**ООО «КРИПТО-ПРО»**

ЖТЯИ.00096-03 97 02

# ПАКМ «КриптоПро HSM»

Версия 2.0 R3

Модуль обеспечения защиты платежных систем

## Команды хоста

2025 г.

ПАКМ «КриптоПро HSM» версия 2.0 R3
Модуль обеспечения защиты платежных систем
Версия ПО: 288111

# Содержание

# 1 Введение

## Локальный мастер-ключ (LMK)

Local Master Key (LMK, локальный мастер-ключ) — главный локальный криптографический ключ HSM, с помощью которого происходит шифрование других криптографических ключей и данных. Общая информация о назначении, поддерживаемых видах LMK, порядке смены LMK и поддержке нескольких LMK содержится в «КриптоПро HSM. Руководство программиста».

## Использование нескольких LMK

HSM поддерживает работу с несколькими установленными LMK. В HSM реализованы следующие механизмы выбора LMK в команде хоста (расположены в порядке уменьшения приоритета):

1. явное указание идентификатора LMK в команде хоста с использованием 2 дополнительных опциональных полей:

| **Параметр** | **Формат** | **Описание** |
|---|---|---|
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |

2. определение идентификатора LMK по номеру TCP-порта, на который была получена команда:

| **Номер TCP-порта** | **Идентификатор используемого LMK** |
|---|---|
| 1500 | Идентификатор по умолчанию |
| 1511 | LMK ID=00 |
| 1512 | LMK ID=01 |
| ... | ... |
| 1520 | LMK ID=09 |

3. определение идентификатора LMK из заголовка Проприетарного Key Block (байты 14-15)

Корректный выбор идентификатора LMK также зависит от выставленных значений настроек безопасности `Ignore LMK ID in Key Block Header`, `Ensure LMK Identifier in command corresponds with host port` (подробнее см. описание настроек безопасности в Прил. Б).

Подробнее механизмы выбора LMK и приоритеты их использования описан в разделе «Использование нескольких LMK» документа «КриптоПро HSM. Руководство программиста».

## Описание форматов полей команды

Следующие разделы документа содержат описание всех доступных команд, направляемых хостом, соответствующие им ответы HSM и коды возможных ошибок. Перечень стандартных ошибок приведен в Прил. А.

Описание команд и ответов представлено в формате таблиц с наименованием параметров (полей), обозначением их формата и описанием.

Следующие условные обозначения используются для описания длины и типа данных в поле команды/ответа (столбец **Формат** таблицы-описания команды/ответа):

| **Длина поля** | |
|---|---|
| L | длина зашифрованного PIN, значение зависит от настройки `PIN length` (см. Прил. Б) |
| m | длина заголовка сообщения, устанавливается при конфигурации HSM |
| n | переменная длина поля |
| **Тип поля** | |
| A | буквенно-цифровой символ (любой не управляющий) |
| H | шестнадцатеричный символ ('0'..'9', 'A'..'F') |
| N | цифра ('0'..'9') |
| C | управляющий символ |
| B | бинарные данные (байт) (0x00..0xFF) |

# 2 Команды управления ключами

Следующие команды хоста используются для управления ключами, включая функции генерации, формирования ключа из компонент, импорта, экспорта и трансляции ключей:

## Доступные типы/использования ключей

Команды генерации и управления ключами 'A0', 'A6' и 'A8' поддерживают работу со следующими типами/использованиями ключей:

### Variant LMK

| Тип | Имя |
|---|---|
| 000 | Зональный мастер-ключ (Zone Master Key, ZMK) |
| 200 | Мастер-ключ VisaCash (KML) |
| 001 | Зональный ключ шифрования PIN (Zone PIN encryption, ZPK) |
| 002 | Ключ проверки PIN (PIN Verification Key, PVK) |
| 002* | Терминальный мастер-ключ (Terminal Master Key, TMK ) |
| 002* | Терминальный ключ шифрования PIN (Terminal PIN Key, TPK) |
| 002* | Terminal Key Register, TKR |
| 302 | Начальный ключ DUKPT (DUKPT Initial Key, IKEY†) |
| 402 | Ключ проверки карты (Card Verification Key, CVK, CSCK) |
| 003 | Терминальный ключ аутентификации (Terminal Authentication Key, TAK) |
| 006 | Watchword key, WWK |
| 008 | Зональный ключ аутентификации (Zone authentication key, ZAK) |
| 009 | Базовый ключ диверсификации DUKPT (DUKPT Base Derivation Key, BDK-1) |
| 609 | Базовый ключ диверсификации DUKPT (DUKPT Base Derivation Key, BDK-2) |
| 809 | Базовый ключ диверсификации DUKPT (DUKPT Base Derivation Key, BDK-3) |
| 909 | Базовый ключ диверсификации DUKPT (DUKPT Base Derivation Key, BDK-4) |
| 109 | Ключ EMV, MK-AC |
| 209 | Ключ EMV, MK-SMI |
| 309 | Ключ EMV, MK-SMC |
| 409 | Ключ EMV, MK-DAC |
| 509 | Ключ EMV, MK-DN |
| 709 | Мастер-ключ DCVV, MK-CVC3 |
| 00A | Ключ шифрования данных, ZEK |
| 00B | Ключ шифрования данных, DEK |
| 30B | Ключ шифрования данных, TEK |
| 30D | Ключ карты для шифрования, CK-ENC |
| 40D | Ключ карты для обеспечения целостности, CK-MAC |
| 50D | Ключ карты для шифрования данных карты, CK-DEK |
| 70D◇ | Терминальный ключ шифрования PIN (Terminal PIN Key, TPK) |
| 80D◇ | Терминальный мастер-ключ (TMK) |
| 90D◇ | Terminal Key Register (TKR) |

### Key Block LMK

| Использование ключа | Имя |
|---|---|
| 01 | WatchWord Key, WWK |
| B0 | Базовый ключ диверсификации DUKPT (DUKPT Base Derivation Key, BDK-1) |
| 41 | Базовый ключ диверсификации DUKPT (DUKPT Base Derivation Key, BDK-2) |
| 42 | Базовый ключ диверсификации DUKPT (DUKPT Base Derivation Key, BDK-3) |
| 43 | Базовый ключ диверсификации DUKPT (DUKPT Base Derivation Key, BDK-4) |
| 44 | Базовый ключ диверсификации DUKPT (DUKPT Base Derivation Key, BDK-5) |
| B1 | Начальный ключ DUKPT (DUKPT Initial Key, IKEY†) |
| C0 | Проверка карты (общий) |
| 11 | Проверка карты (American Express CSC) |
| 12 | Проверка карты (Mastercard CVC) |
| 13 | Проверка карты (Visa CVV) |
| D0 | Шифрование данных (общий) |
| 21 | Шифрование данных (DEK) |
| 22 | Шифрование данных (ZEK) |
| 23 | Шифрование данных (TEK) |
| 24 | Ключ шифрования ключей (Транспортный ключ) |
| 25 | Ключ шифрования данных (CTR Data encryption key, CTRDEK) |
| E0 | Мастер-ключ EMV: Application Cryptogram ($MK_{AC}$) |
| E1 | Мастер-ключ EMV: Secure Messaging для обеспечения конфиденциальности ($MK_{SMC}$) |
| E2 | Мастер-ключ EMV: Secure Messaging для обеспечения целостности ($MK_{SMI}$) |
| E3 | Мастер-ключ EMV: Data Authentication Code ($MK_{DAC}$) |
| E4 | Мастер-ключ EMV: Dynamic Numbers ($MK_{DN}$) |
| E5 | Мастер-ключ EMV: персонализация карт |
| E6 | Мастер-ключ EMV: другое |
| E7 | EMV/Master Personalization Key |
| 31 | VisaCash Master Load Key, KML |
| 32 | Мастер-ключ Dynamic CVV (MK-CVC3) |
| 33 | Мастер-ключ Mobile Remote Management для обеспечения конфиденциальности (M_KEY_CONF) |

| Тип | Имя |
|---|---|
| 607 | Мастер-ключ ZKA (ZKA-MK) |
| 107 | Ключ шифрования ключей (Key encryption Key, KEK) |
| 207 | Master Personalization Key, KMC |

* Если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`.

† IKEY также известен как IPEK.

◇ Если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: Yes`.

*Примечание*: Ограничения операций генерации, импора и экспорта ключей описаны в таблице типов ключей в «КриптоПро HSM. Руководство программиста».

| Использование ключа | Имя |
|---|---|
| 34 | Мастер-ключ Mobile Remote Management для обеспечения целостности (M_KEY_MAC) |
| 35 | Сессионный ключ Mobile Remote Management для обеспечения конфиденциальности (MS_KEY_CONF) |
| 36 | Сессионный ключ Mobile Remote Management для обеспечения целостности (MS_KEY_MAC) |
| 37 | Ключ EMV-карты для криптограмм |
| 38 | Ключ EMV-карты для обеспечения целостности |
| 39 | Ключ EMV-карты для шифрования |
| 40 | EMV Personalization System Key |
| 47 | Сессионный ключ EMV для криптограмм |
| 48 | Сессионный ключ EMV для обеспечения целостности |
| 49 | Сессионный ключ EMV для шифрования |
| K0 | Шифрование ключа или key wrapping (общий) |
| K1 | Ключ защиты Key Block |
| 51 | Шифрование терминальных ключей (Terminal key encryption, TMK) |
| 52 | Шифрование зональных ключей (Zone key encryption, ZMK) |
| 53 | Мастер-ключ ZKA (ZKA-MK) |
| 54 | Ключ шифрования ключей (Key Encryption Key, KEK) |
| 55 | Ключ шифрования ключей (Транспортный ключ) |
| M0 | ISO 16609 MAC алгоритм 1 (с использованием 3-DES) |
| M1 | ISO 9797-1 MAC алгоритм 1 (с использованием 3DES) |
| M2 | ISO 9797-1 MAC алгоритм 2 |
| M3 | ISO 9797-1 MAC алгоритм 3 (с использованием 3DES) |
| M4 | ISO 9797-1 MAC алгоритм 4 |
| M5 | CBC-MAC (с использованием AES) |
| M6 | CMAC (с использованием AES) |
| P0 | Шифрование PIN (общий) |
| 71 | Терминальный ключ шифрования PIN (Terminal PIN encryption, TPK) |
| 72 | Зональный ключ шифрования PIN (Zone PIN encryption, ZPK) |
| 73 | Transaction key scheme Terminal Key Register, TKR |
| V0 | Провека PIN (KPV, другой алгоритм) |
| V1 | Провека PIN (с использованием метода IBM 3624) |
| V2 | Провека PIN (с использованием метода ABA PVV) |

† IKEY также известен как IPEK.

## Интерпретация поля "Идентификатор версии" TR-31 Key Block

Первый байт TR-31 Key Block содержит поле идентификатора версии Key Block, которое идентифицирует формат Key Block и процесс, используемый для его защиты.

В таблице ниже описаны возможные значения идентификатора версии (Version ID) Key Block.

| ID версии Key Block | Описание |
|---|---|
| 'A' | Ключи имитозащиты и шифрования вырабатываются из ключа защиты Key Block с использованием операции XOR. Подробнее см. TR-31:2005. |
| 'B' | Ключи имитозащиты и шифрования вырабатываются из ключа защиты Key Block с использованием CMAC. Подробнее см. раздел 5.3.2.1 TR-31:2010. |
| 'C' | Идентична версии 'A'.<br>Ключи имитозащиты и шифрования вырабатываются из ключа защиты Key Block с использованием операции XOR, аналогичной используемой для версии 'A'. Подробнее см. раздел 5.3.3.1 TR-31:2010. |
| 'D' | Ключи шифрования и аутентификации вырабатываются из ключа защиты Key Block с использованием CMAC в качестве псевдослучайной функции получения 16-байтовых значений MAC. Key Block, полученные с использованием AES KBPK, всегда имеют версию 'D'. Подробнее см. раздел 5.3.2.3 TR-31:2018. |

## [A0] — Генерация ключа

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Определяется по ТТК (Г&Э)**<br>Активности: **generate.{key}.host и export.{key}.host** | |
| Key Block LMK | Авторизация: **При экспорте в формат, отличный от Key Block**<br>Активности: **export.{key}.host** | |

**Описание функции:** Генерация случайного ключа или диверсификация ключа и возврат его хосту в зашифрованном виде под LMK и опционально под ZMK/TMK/BDK (для передачи третьей стороне).

**Авторизация:**

Команда проверяет флаг 'Г' (генерация) для заданного типа ключа в таблице типов ключей (ТТК, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **generate.{key}.host** должна быть авторизована, где 'key' — код типа генерируемого ключа.

Команда проверяет флаг 'Э' (экспорт) для заданного типа ключа в ТТК. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **export.{key}.host** должна быть авторизована, где 'key' — код типа экспортируемого ключа.

Требование авторизации для команды зависит только от ключевой схемы:

| Ключевая схема (ZMK) | Авторизация |
|---|---|
| 'S' (Проприетарный Key Block) | Не требуется |
| 'R' (TR-31 Key Block) | Не требуется |
| 'U', 'T' (Variant) | Требуется |
| 'X', 'Y' (ANSI X9.17) | Требуется |

Если авторизация требуется, HSM должен находиться в авторизованном состоянии, либо активность **export.{key}.host** должна быть авторизована, где 'key' — значение *Использования ключа* экспортируемого ключа.

**Примечания:**

| | |
|---|---|
| TMK может экспортировать только следующие типы ключей:<br><br>Если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`:<br>002 (TPK или TMK)<br>003 (TAK)<br>30B (TEK)<br>302 (IKEY)<br><br>`Enforce key type 002 separation for PCI HSM compliance: Yes`:<br>70D (TPK)<br>80D (TMK)<br>003 (TAK)<br>30B (TEK)<br>302 (IKEY) | TMK с *Использованием ключа* = '51' может экспортировать только Key Block со следующими значениями поля *Использование ключа*:<br><br>'P0', '71' (TPK)<br>'M1', 'M3', 'M5', 'M6' (TAK)<br>'23' (TEK)<br>'51' (TMK)<br>'B1' (IKEY) |

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable X9.17 for export` | `Yes [Y]` | Доступен экспорт ключа в формат X9.17 (X, Y схемы). |
| | `No [N]` | Экспорт ключа в формат X9.17 невозможен. |
| `Key export and import in trusted format only` | `Yes [Y]` | Экспорт ключа в недоверенные форматы невозможен. |
| | `No [N]` | Доступен экспорт ключа в недоверенные форматы (X, Y, U, T схемы). |
| `Enable export of a ZMK` | `Yes [Y]` | Доступен экспорт ZMK. |
| | `No [N]` | Экспорт ZMK невозможен. |
| `Enforce key type 002 separation for PCI HSM compliance`<br>(влияет на параметры: *Тип ключа, ZMK/TMK/Текущий BDK*) | `Yes [Y]` | Для Variant ограничены типы создаваемых ключей с последующим экспортом, см. Примечание выше. TMK зашифрован под LMK 36-37/8. |
| | `No [N]` | Для Variant ограничены типы создаваемых ключей с последующим экспортом, см. Примечание выше. TMK зашифрован под LMK 14-15/0. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'A0' (A-ноль).</td></tr>
<tr><td>Режим</td><td>1 H</td><td>Тип операции:<br>'0': Генерация ключа<br>'1': Генерация ключа и зашифрование под ZMK/TMK/Текущий BDK<br>'A': Диверсификация ключа<br>'B': Диверсификация ключа и зашифрование под ZMK/TMK/Текущий BDK</td></tr>
<tr><td>Тип ключа</td><td>3 H</td><td>Тип генерируемого/диверсифицируемого ключа.<br>В случае генерации нового ключа (Режим = '0' или '1') допустимые значения типов ключей указаны в таблице на странице 14.<br>В случае диверсификации ключа из мастер-ключа (Режим = 'A' или 'B') допустимые значения:
<table>
<tr><th>Тип ключа</th><th>Описание</th><th>Режим диверсификации</th></tr>
<tr><td>302</td><td>IKEY</td><td>0 (DUKPT)</td></tr>
<tr><td>001</td><td>ZPK</td><td>1 (ZKA)</td></tr>
<tr><td>008</td><td>ZAK</td><td>1 (ZKA)</td></tr>
<tr><td>00A</td><td>ZEK</td><td>1 (ZKA)</td></tr>
</table>
</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Ключевая схема (LMK)</td><td>1 A</td><td>Схема шифрования выходного ключа под LMK, подробнее см. таблицу ключевых схем в «КриптоПро HSM. Руководство программиста».</td></tr>
<tr><td>Режим диверсификации ключа</td><td>1 A</td><td>Присутствует только в случае Режима = 'A' или 'B'.<br>Операция для диверсификации ключа.<br>'0': DUKPT - Диверсификация IKEY из мастер-ключа DUKPT<br>'1': ZKA — Диверсификация ключа ZKA из мастер-ключа ZKA</td></tr>
<tr><td>Тип мастер-ключа DUKPT</td><td>1 H</td><td>Присутствует только в случае Режима диверсификации ключа = '0'.<br>Тип мастер-ключа DUKPT для диверсификации начального ключа устройства.<br>'1': BDK-1<br>'2': BDK-2<br>'3': BDK-3<br>'4': BDK-4<br>'5': BDK-5</td></tr>
<tr><td>Мастер-ключ DUKPT</td><td></td><td>Присутствует только в случае Режима диверсификации ключа = '0'.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>Если Тип мастер-ключа DUKPT = '1' — BDK-1, зашифрованный под LMK 28-29.<br>Если Тип мастер-ключа DUKPT = '2' — BDK-2, зашифрованный под LMK 28-29/6.<br>Если Тип мастер-ключа DUKPT = '3' — BDK-3, зашифрованный под LMK 28-29/8.<br>Если Тип мастер-ключа DUKPT = '4' — BDK-4, зашифрованный под LMK 28-29/9.<br>Если Тип мастер-ключа DUKPT = '5' — BDK-5 не поддерживает Variant LMK.</td></tr>
<tr><td></td><td>'S' + n A</td><td>BDK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'B0', '41', '43'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
<tr><td>'42', '44'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>KSN</td><td>15 H<br>или<br>16 H</td><td>Присутствует только в случае Режима диверсификации ключа = '0'.<br>Идентификатор ключевого набора и идентификатор устройства для диверсификации начального ключа, выровненные по правому краю и дополненные при необходимости 0xF.<br>Примечание: поле не содержит значения счетчика транзакций, которое передается как часть значения KSN в данных транзакции от терминала.<br><br>В случае 3DES BDK-1, BDK-2, BDK-3 или BDK-4 размер поля 15 H.<br>Пример 1: Для значений KSI + идентификатор устройства = 303950+12342468 (14 шестнадцатеричных символов) поле содержит значение "F30395012342468".<br><br>В случае AES BDK или 3DES BDK-5 размер поля 16 H.<br>Пример 2: Для BDK ID + идентификатор устройства = 30395059 + 12345678 (16 шестнадцатеричных символов) поле содержит значение "3039505912345678".</td></tr>
<tr><td>Тип мастер-ключа ZKA</td><td></td><td>Присутствует только в случае Режима диверсификации ключа = '1'.</td></tr>
<tr><td></td><td>3 H</td><td>607: Мастер-ключ, зашифрованный под LMK 24-25/6.</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Мастер-ключ ZKA</td><td></td><td>Присутствует только в случае Режима диверсификации ключа = '1'.<br>Допускается использовать только ключ 2DES.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>Мастер-ключ ZKA, зашифрованный под соответствующим LMK, определяемым значением поля Тип мастер-ключа ZKA.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Мастер-ключ ZKA должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'53'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Флаг ZKA RNDI</td><td>1 H</td><td>Присутствует только в случае Режима диверсификации ключа = '1'.<br>'0': диверсификация ключа с использованием переданного в команде RNDI<br>'1': диверсификация ключа с использованием нового RNDI</td></tr>
<tr><td>ZKA RNDI</td><td>32 H</td><td>Присутствует только в случае Флага ZKA RNDI = '0'.<br>Случайное число, используемое для выработки ключа PAC/MAC/DE из мастер-ключа ZKA.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Опционально; может присутствовать только в случае Режима = '1' или 'B'. Если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Флаг ZMK/TMK</td><td>1 N</td><td>Опционально; присутствует, только если присутствует разделитель выше.<br>'0': ZMK (значение по умолчанию, если данное поле отсутствует)<br>'1': TMK</td></tr>
<tr><td>ZMK/TMK/Текущий BDK</td><td></td><td>Присутствует только в случае Режима = '1' или 'B'.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>ZMK, зашифрованный под LMK 04-05.<br>TMK, зашифрованный под LMK 14-15/0 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: No</code>) или LMK 36-37/8 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: Yes</code>).</td></tr>
<tr><td></td><td>'S' + n A</td><td>ZMK/TMK/Текущий BDK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'K0', '51', '52'</td><td>'T', 'A'</td><td>'B', 'E', 'N'</td></tr>
<tr><td>'B0', '41', '43'</td><td>'A'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Серийный номер начального ключа текущего BDK</td><td>16 H</td><td>Присутствует, только если используется текущий BDK.</td></tr>
</table>

| | | |
|---|---|---|
| Ключевая схема (ZMK/TMK/Текущий BDK) | 1 A | Присутствует только в случае *Режима* = '1' или 'B'.<br>Схема шифрования выходного ключа под ZMK/TMK/Текущим BDK, подробнее см. таблицу ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Atalla вариант | 1/2 N | Присутствует только в случае *Режима* = '1' или 'B'.<br>Опционально; используется при работе с оборудованием Atalla. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующие поля присутствуют только в случае генерации (и опционально экспорта) ключа в формате Key Block: | | |
| Разделитель | 1 A | Значение '#'. Обязательное поле в случае генерации Key Block. Если присутствует, следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block. Допустимые значения см. в таблице на странице 14. |
| Алгоритм | 2 A | Алгоритм и длина ключа; первый символ включается в поле *Алгоритм* заголовка Key Block (байт 7).<br>Допустимые значения:<br>'T2': 2DES<br>'T3': 3DES<br>'A1': AES-128<br>'A2': AES-192<br>'A3': AES-256 |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block.<br>Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице режимов использования ключа в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения см. в таблице экспортируемости ключа в «КриптоПро HSM. Руководство программиста». |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Разделитель | 1 A | Значение '&'. Опционально; может присутствовать, только если созданный ключ должен быть экспортирован в формат Key Block. Если присутствует, следующее поле обязательно. |
| Новое значение экспортируемости | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block (байт 11).<br>Допустимое значение: 'N'. |
| Разделитель | 1 A | Значение '!'. Опционально; присутствует только при экспорте ключа в формат TR-31 Key Block. Если присутствует, следующее поле обязательно. |
| Идентификатор (ID) версии Key Block | 1 A | ID версии Key Block (подробнее см. ASC X9 TR 31-2018):<br>'A': Key Block, защищённый методом Key Variant Binding<br>'B': Key Block, защищённый методом Key Derivation Binding<br>'C': Key Block, защищённый методом Key Variant Binding<br>'D': Key Block, защищённый методом AES Key Derivation Binding |
| Следующие поля присутствуют только в случае генерации ключа в формате Variant и экспорта его в формат TR-31: | | |

| | | |
|---|---|---|
| Разделитель | 1 A | Значение '&'. Опционально; может присутствовать, только если сгенерированный ключ должен быть экспортирован. Если присутствует, следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block. Любое допустимое значение TR-31 для указанного типа ключа. Допустимые значения см. в таблице использования ключей в «КриптоПро HSM. Руководство программиста». |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block. Любое допустимое значение для указанного типа ключа. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N' или 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '02'.<br>*Примечание:* допускается использовать только опциональные блоки с идентификатором 'KS' или 'KV'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Допустимые значения: 'KS' или 'KV'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Разделитель | 1 A | Значение '!'. Опционально; может присутствовать, только если созданный ключ должен быть экспортирован в формат TR-31 Key Block. Если присутствует, следующее поле обязательно. |
| Идентификатор (ID) версии Key Block | 1 A | ID версии Key Block (подробнее см. ASC X9 TR 31-2018):<br>'A': Key Block, защищённый методом Key Variant Binding<br>'B': Key Block, защищённый методом Key Derivation Binding<br>'C': Key Block, защищённый методом Key Variant Binding |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'A1'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'06': Недопустимый режим диверсификации ключа<br>'07': Недопустимый тип мастер-ключа DUKPT/ZKA<br>'10': Нарушена четность ZMK/TMK<br>'11': Нарушена четность мастер-ключа DUKPT/ZKA<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Ключ (под LMK) | | Сгенерированный/диверсифицированный ключ, зашифрованный под LMK. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | Ключ, зашифрованный под соответствующим LMK, определяемым значением поля *Тип ключа*. |
| | 'S' + n A | Ключ, зашифрованный под LMK. |
| Ключ (под ZMK/TMK/Текущим BDK) | 'U' или<br>'X' + 32 H<br>или<br>'T' или<br>'Y' + 48 H | Присутствует только в случае *Режима* = '1' или 'B'.<br>Сгенерированный/диверсифицированный ключ, зашифрованный под указанным ZMK/TMK/Текущим BDK. |
| | 'R' + n A<br>или<br>'S' + n A | |
| KCV | 6 H | Проверочное значение ключа. |
| ZKA RNDI | 32 H | Присутствует только в случае *Флага ZKA RNDI* = '1'.<br>Сгенерированное значение RNDI, которое использовалось для выработки ключа PAC/MAC/DE из мастер-ключа ZKA. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [A2] — Генерация и печать компоненты

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Требуется** | |
| Активности: **genprint.{key}.host** | |

**Описание функции:** Генерация случайной компоненты, печать её с помощью подключенного к HSM принтера и возврат зашифрованной компоненты хосту.

**Авторизация:**

| Variant LMK | Key Block LMK |
|---|---|
| HSM должен находиться в авторизованном состоянии, либо активность **genprint.{key}.host** должна быть авторизована, где 'key' — код типа ключа генерируемой компоненты. | HSM должен находиться в авторизованном состоянии, либо активность **genprint.{key}.host** должна быть авторизована, где 'key' — значение *Использования ключа* генерируемой компоненты. |

**Примечания:**

На практике поле *Количество опциональных блоков* должно быть установлено в '00', поскольку любые подобные поля не учитываются при формировании ключевого блока (например, с использованием команды 'A4').

Для выполнения команды принтер должен быть подключен к USB-порту HSM.

На HSM уже должен быть настроен формат печати.

Последовательность ^P определяет место печати открытой компоненты.

^T в формате печати обозначает проверочное значение компоненты.

В команде должно присутствовать как минимум одно поле печати.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'A2'. |
| Тип ключа | 3 H | Тип ключа генерируемой компоненты. Допустимые значения см. в таблице на странице 14. |
| | | Значение 'FFF'. |
| Флаг проверочного значения компоненты | 1 A | Опционально. Если присутствует, показывает, должен ли ответ включать проверочное значение компоненты:<br>'1': не возвращать проверочное значение компоненты<br>'2': вернуть проверочное значение компоненты<br>Если поле отсутствует, используется значение по умолчанию '1'. |
| Ключевая схема (LMK) | 1 A | Схема шифрования ключа под LMK. Список ключевых схем см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Поле печати 0 | n A | Поле печати определяется как *Поле печати 0* в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение ';'. |
| Поле печати 1 | n A | Поле печати определяется как *Поле печати 1* в определении формата печати (не должно содержать символов ';' или '∼'). |
| ... | ... | ... |
| ... | ... | ... |
| Последнее поле печати | n A | *Последнее поле печати*, определенное в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение '∼'. Опционально; должен присутствовать в случае, если присутствует разделитель '%' или '#'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующие поля присутствуют только в случае генерации компоненты в формате Key Block: | | |
| Разделитель | 1 A | Значение '#'. Обязательное поле в случае генерации компоненты в формате Key Block. Если присутствует, следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block. Допустимые значения см. в таблице на странице 14. |
| Алгоритм | 2 A | Алгоритм и длина ключа; первый символ включается в поле *Алгоритм* заголовка Key Block (байт 7).<br>Допустимые значения:<br>'T2': 2DES<br>'T3': 3DES<br>'A1': AES-128<br>'A2': AES-192<br>'A3': AES-256 |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block.<br>Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице режимов использования ключа в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 A | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: 'c0' .. 'c9'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения см. в таблице экспортируемости ключа в «КриптоПро HSM. Руководство программиста». |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '06'. |

| Следующие 3 поля определяются для каждого опционального блока.<br>*Примечание*: Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
|---|---|---|
| Идентификатор блока | 2 A | Любое допустимое значение, кроме '03', '04' и 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'A3'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'16': Принтер не готов/не подключен<br>'18': Определение формата не загружено<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Компонента | | Сгенерированная компонента, зашифрованная под LMK. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | Компонента, зашифрованная под соответствующим LMK, определяемым значением поля *Тип ключа*. |
| | 'S' + n A | Компонента, зашифрованная под LMK. |
| Проверочное значение компоненты (CCV) | 6 H | Проверочное значение компоненты. Присутствует только в случае *Проверочного флага компоненты* = '2'. |
| Код ответа принтера | 2 A | Значение 'AZ'. |
| Код ошибки принтера | 2 H | '00': Без ошибок<br>'41': Внутренняя аппаратная/программная ошибка<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [NE] — Генерация и печать ключа как разделённых компонент

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Требуется** | |
| Активности: **genprint.{key}.host** | |

**Описание функции:** Генерация случайного ключа, печать его в виде двух или трех разделенных компонент с помощью подключенного к HSM принтера и возврат ключа, зашифрованного под LMK, хосту.

**Авторизация:**

| Variant LMK | Key Block LMK |
|---|---|
| HSM должен находиться в авторизованном состоянии, либо активность **genprint.{key}.host** должна быть авторизована, где 'key' — код типа генерируемого ключа/компоненты. | HSM должен находиться в авторизованном состоянии, либо активность **genprint.{key}.host** должна быть авторизована, где 'key' — значение *Использования ключа* генерируемого ключа/компоненты. |

**Примечания:**

Для выполнения команды принтер должен быть подключен к USB-порту HSM.

На HSM уже должен быть настроен формат печати.

Для ключа двойной длины ^P и ^Q в формате печати обозначают первый и второй ключи соответственно.

Для ключа тройной длины ^P, ^Q и ^R — первый, второй и третий ключи.

^T в формате печати обозначает проверочное значение ключа (KCV).

В команде должно присутствовать как минимум одно поле печати.

Команда не поддерживает работу с 256-битными AES ключами.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'NE'. |
| Тип ключа | 3 H | Тип генерируемого ключа. Допустимые значения см. в таблице на странице 14. |
| | | Значение 'FFF'. |
| Ключевая схема (LMK) | 1 A | Схема шифрования ключа под LMK. Список ключевых схем см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Поле печати 0 | n A | Поле печати определяется как *Поле печати 0* в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение ';'. |
| Поле печати 1 | n A | Поле печати определяется как *Поле печати 1* в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение ';'. |
| ... | ... | ... |
| ... | ... | ... |
| Последнее поле печати | n A | *Последнее поле печати*, определенное в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение '∼'. Опционально; должен присутствовать в случае, если присутствует разделитель '%' или '#'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующие поля присутствуют только в случае генерации компонент в формате Key Block: | | |
| Разделитель | 1 A | Значение '#'. Обязательное поле в случае генерации компоненты в формате Key Block. Если присутствует, следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block. Допустимые значения см. в таблице на странице 14. |
| Алгоритм | 2 A | Алгоритм и длина ключа; первый символ включается в поле *Алгоритм* заголовка Key Block (байт 7).<br>Допустимые значения:<br>'T2': 2DES<br>'T3': 3DES<br>'A1': AES-128<br>'A2': AES-192 |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block.<br>Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице режимов использования ключа в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 A | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Любое допустимое значение. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения см. в таблице экспортируемости ключа в «КриптоПро HSM. Руководство программиста». |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока.<br>*Примечание*: Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |

| | | |
|---|---|---|
| Данные блока | n A | Данные блока. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'NF'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'16': Принтер не готов/не подключен<br>'18': Определение формата не загружено<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Ключ | | Сгенерированный ключ, зашифрованный под LMK. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | Ключ, зашифрованный под соответствующим LMK, определяемым значением поля *Тип ключа*. |
| | 'S' + n A | Ключ, зашифрованный под LMK. |
| KCV | 6 H | Проверочное значение ключа. |
| Код ответа принтера | 2 A | Значение 'NZ'. |
| Код ошибки принтера | 2 H | '00': Без ошибок<br>'41': Внутренняя аппаратная/программная ошибка<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [A4] — Формирование ключа из зашифрованных компонент

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Требуется** | |
| Активности: **component.{key}.host** | |

**Описание функции:** Формирование ключа из зашифрованных компонент.

**Авторизация:**

| Variant LMK | Key Block LMK |
|---|---|
| HSM должен находиться в авторизованном состоянии, либо активность **component.{key}.host** должна быть авторизована, где 'key' — код типа формируемого ключа. | HSM должен находиться в авторизованном состоянии, либо активность **component.{key}.host** должна быть авторизована, где 'key' — значение *Использования ключа* формируемого ключа. |

**Примечания:**

Поля *Использование ключа*, *Режим использования*, *Алгоритм* и *Экспортируемость*, определенные после разделителя '#', должны совпадать с соответствующими значениями, определенными для всех компонент ключа.

Любые опциональные блоки, определенные после разделителя '#', будут использованы при формировании нового ключа. Опциональные блоки, содержащиеся в Key Block компонент, будут проигнорированы.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'A4'. |
| Количество компонент | 1 N | Количество компонент ключа.<br>Допустимые значения: '2' .. '9'. |
| Тип ключа | 3 H | Тип генерируемого ключа. Допустимые значения см. в таблице на странице 14. |
| | | Значение 'FFF'. |
| Ключевая схема (LMK) | 1 A | Схема шифрования ключа под LMK. Список ключевых схем см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| 1-я компонента ключа | 'U' + 32 H<br>или<br>'T' + 48 H | Зашифрованная первая компонента ключа. |
| | 'S' + n A | |
| 2-я компонента ключа | 'U' + 32 H<br>или<br>'T' + 48 H | Зашифрованная вторая компонента ключа. |
| | 'S' + n A | |
| ... | ... | ... |
| n-я компонента ключа | 'U' + 32 H<br>или<br>'T' + 48 H | Зашифрованная n-я компонента ключа. |
| | 'S' + n A | |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующая секция применяется только при использовании компонент в формате Key Block: | | |

| | | |
|---|---|---|
| Разделитель | 1 A | Значение '#'. Обязательное поле в случае генерации ключа из Key Block компонент. Если присутствует, следующие поля обязательны. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока.<br>*Примечание*: Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'A5'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Недопустимое число компонент<br>'10': Нарушена четность компоненты<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Ключ (под LMK) | | Сформированный из компонент ключ, зашифрованный под LMK. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | Ключ, зашифрованный под соответствующим LMK, определяемым значением поля *Тип ключа*. |
| | 'S' + n A | Ключ, зашифрованный под LMK. |
| KCV | 6 H | Проверочное значение ключа. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [A6] — Импорт ключа

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Определяется по ТТК (И)**<br>Активности: **import.{key}.host** | |
| Key Block LMK | Авторизация: **При импорте из формата, отличного от Key Block**<br>Активности: **import.{key}.host** | |

**Описание функции:** Импорт ключа, зашифрованного под ZMK.

**Авторизация:**

Команда проверяет флаг 'И' (импорт) для заданного типа ключа в таблице типов ключей (ТТК, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **import.{key}.host** должна быть авторизована, где 'key' — код типа импортируемого ключа.

Требование авторизации для команды зависит только от ключевой схемы:

| Ключевая схема (ZMK) | Авторизация |
|---|---|
| 'S' (Проприетарный Key Block) | Не требуется |
| 'R' (TR-31 Key Block) | Не требуется |
| 'U', 'T' (Variant) | Требуется |
| 'X', 'Y' (ANSI X9.17) | Требуется |

Если авторизация требуется, HSM должен находиться в авторизованном состоянии, либо активность **import.{key}.host** должна быть авторизована, где 'key' — значение *Использования ключа* импортируемого ключа.

**Примечания:** Данная команда не требует, чтобы у импортируемого ключа были выставлены биты четности. Однако команда гарантирует, что у выходного ключа, зашифрованного под LMK, биты четности будут выставлены. В случае нарушения четности у импортируемого ключа команда возвращает код ошибки '01' и далее работает штатно.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce Atalla variant match to variant key type` | `Yes [Y]` | Принудительно проверяется соответствие между Atalla вариантом и типом ключа Variant, см. таблицу ниже. |
| | `No [N]` | Ограничения на соответствие между Atalla вариантом и типом ключа Variant не накладываются. |
| `Enable X9.17 for import` | `Yes [Y]` | Доступен импорт ключа из формата X9.17 (X, Y схемы). |
| | `No [N]` | Импорт ключа из формата X9.17 невозможен. |
| `Key export and import in trusted format only` | `Yes [Y]` | Импорт ключа из недоверенных форматов невозможен. |
| | `No [N]` | Доступен импорт ключа из недоверенных форматов (X, Y, U, T схемы). |

| | | |
|---|---|---|
| `Enable import of a ZMK` | `Yes [Y]` | Доступен импорт ZMK. |
| | `No [N]` | Импорт ZMK невозможен. |
| `Enforce key type 002 separation for PCI HSM compliance` | `Yes [Y]` | См. таблицу ниже. |
| | `No [N]` | См. таблицу ниже. |

| Тип ключа | Atalla вариант | Код типа ключа Variant (*) | Код типа ключа Variant(**) |
|---|---|---|---|
| TPK<br>ZPK | 1 или 01 | 002 LMK 14-15<br>001 LMK 06-07 | 70D LMK 36-37/7<br>001 LMK 06-07 |
| DEK<br>ZEK | 2 или 02 | 00B LMK 32-33<br>00A LMK 30-31 | 00B LMK 32-33<br>00A LMK 30-31 |
| TAK<br>ZAK<br>CVK | 3 или 03 | 003 LMK 16-17<br>008 LMK 26-27<br>402 LMK 14-15/4 | 003 LMK 16-17<br>008 LMK 26-27<br>402 LMK 14-15/4 |
| TMK<br>TPK<br>PVK | 4 или 04 | 002 LMK 14-15<br>002 LMK 14-15<br>002 LMK 14-15 | 80D LMK 36-37/8<br>70D LMK 36-37/7<br>002 LMK 14-15 |
| TMK | 5 или 05 | 002 LMK 14-15 | 80D LMK 36-37/8 |
| BDK-1 | 8 или 08 | 009 LMK 28-29 | 009 LMK 28-29 |
| MK-AC | 9 или 09 | 109 LMK 28-29/1 | 109 LMK 28-29/1 |
| MK-SMI | 9 или 09 | 209 LMK 28-29/2 | 209 LMK 28-29/2 |
| MK-SMC | 9 или 09 | 309 LMK 28-29/3 | 309 LMK 28-29/3 |
| TEK | 26 | 30B LMK 32-33/3 | 30B LMK 32-33/3 |
| BDK-2 | 30 | 609 LMK 28-29/6 | 609 LMK 28-29/6 |
| BDK-3 | 8 или 08 | 809 LMK 28-29/8 | 809 LMK 28-29/8 |
| BDK-4 | 9 или 09 | 909 LMK 28-29/9 | 909 LMK 28-29/9 |
| BDK-5 | н/д | н/д<br>(только Key Block) | н/д<br>(только Key Block) |

* Если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`

** Если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: Yes`

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'A6'.</td></tr>
<tr><td>Тип ключа</td><td>3 H</td><td>Тип импортируемого ключа.<br>Допустимые значения см. в таблице на странице 14.</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>ZMK</td><td></td><td>ZMK, зашифрованный под LMK.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>ZMK, зашифрованный под LMK 04-05.</td></tr>
<tr><td></td><td>'S' + n A</td><td>ZMK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'K0', '52'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>Ключ (под ZMK)</td><td>'U' или<br>'X' + 32 H<br><br>или<br>'T' или<br>'Y' + 48 H<br>или<br>'R' + n A<br>или<br>'S' + n A</td><td>Импортируемый ключ, зашифрованный под ZMK. Ключ может быть в формате X9.17, Variant или Key Block.<br><br>Если ключ в формате Key Block, он должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>Любое допустимое значение</td><td>'T', 'A'</td><td>Любое допустимое значение</td></tr>
</table>
Допустимые значения Использования ключа см. в таблице на странице 14.</td></tr>
<tr><td>Ключевая схема (LMK)</td><td>1 A</td><td>Схема шифрования выходного ключа под LMK, подробнее см. таблицу ключевых схем в «КриптоПро HSM. Руководство программиста».</td></tr>
<tr><td>Atalla вариант</td><td>1/2 N</td><td>Atalla вариант. Опционально; используется при работе с оборудованием Atalla.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае импорта ключа из формата TR-31 при использовании Key Block LMK:</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '#'. Опционально; может присутствовать, только если импортируемый ключ в формате TR-31 Key Block. Если присутствует, следующие поля обязательны.</td></tr>
<tr><td>Новое значение использования ключа</td><td>2 A</td><td>Поле Использование ключа, включаемое в заголовок Key Block.<br>Должно соответствовать значению Использования ключа в заголовке Key Block для Ключа (под ZMK).</td></tr>
<tr><td>Количество опциональных блоков</td><td>2 N</td><td>Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '06'.</td></tr>
<tr><td colspan="3">Следующие 3 поля определяются для каждого опционального блока:<br>Примечание: Если Количество опциональных блоков = '00', следующие 3 поля не присутствуют.</td></tr>
<tr><td>Идентификатор блока</td><td>2 A</td><td>Любое допустимое значение, кроме 'KS', 'KV', 'PB'.</td></tr>
<tr><td>Длина блока</td><td>2 H</td><td>Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует.</td></tr>
<tr><td>Данные блока</td><td>n A</td><td>Данные блока.</td></tr>
</table>

| | | |
|---|---|---|
| Следующие поля присутствуют только в случае импорта ключа из формата, отличного от Key Block (например, X9.17), при использовании Key Block LMK: | | |
| Разделитель | 1 A | Значение '#'. Опционально; присутствует, только если импортируемый ключ в формате, отличном от Key Block. Если присутствует, следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block. Допустимые значения см. в таблице использования ключей в «КриптоПро HSM. Руководство программиста». |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block. Любое допустимое значение для указанного *Использования ключа*. Допустимые значения см. в таблице режимов использования ключей в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N' или 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока.<br>*Примечание*: Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'A7'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Нарушена четность ключа (предупреждение)<br>'10': Нарушена четность ZMK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Ключ (под LMK) | | Импортированный ключ, зашифрованный под LMK. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | Ключ, зашифрованный под соответствующим LMK, определяемым значением поля *Тип ключа*. |
| | 'S' + n A | Ключ, зашифрованный под LMK. |
| KCV | 6 H | Проверочное значение ключа. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [A8] — Экспорт ключа

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Определяется по ТТК (Э)**<br>Активности: **export.{key}.host** | |
| Key Block LMK | Авторизация: **При экспорте в формат, отличный от Key Block**<br>Активности: **export.{key}.host** | |

**Описание функции:** Зашифрование ключа под ZMK или TMK для экспорта.

**Авторизация:**

Команда проверяет флаг 'Э' (экспорт) для заданного типа ключа в таблице типов ключей (ТТК, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **export.{key}.host** должна быть авторизована, где 'key' — код типа экспортируемого ключа.

Требование авторизации для команды зависит только от ключевой схемы:

| Ключевая схема (ZMK) | Авторизация |
|---|---|
| 'S' (Проприетарный Key Block) | Не требуется |
| 'R' (TR-31 Key Block) | Не требуется |
| 'V' (Verifone/GISKE Key Block) | Не требуется |
| 'U', 'T' (Variant) | Требуется |
| 'X', 'Y' (ANSI X9.17) | Требуется |

Если авторизация требуется, HSM должен находиться в авторизованном состоянии, либо активность **export.{key}.host** должна быть авторизована, где 'key' — значение *Использования ключа* экспортируемого ключа.

**Примечания:**

TMK может экспортировать только следующие типы ключей:

Если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`:
002 (TPK)
003 (TAK)
30B (TEK)
302 (IKEY)

`Enforce key type 002 separation for PCI HSM compliance: Yes`:
70D (TPK)
003 (TAK)
30B (TEK)
302 (IKEY)

TMK с *Использованием ключа* = '51' может экспортировать только Key Block со следующими значениями поля *Использование ключа*:
'P0', '71' (TPK)
'M1', 'M3', 'M5', 'M6' (TAK)
'23' (TEK)
'B1' (IKEY)

Key Block, экспортированный в формат Verifone/GISKE Key Block, должен иметь следующие значения поля *Использование ключа*:
'P0', '71' (TPK)
'M1', 'M3' (TAK)

Key Block ZMK (или TMK) должен соответствовать следующему формату:

| Использование ключа | Алгоритм | Режим использования |
|---|---|---|
| 'K0', '51' или '52' | 'T' или 'A' | 'B', 'E' или 'N' |

При экспорте Проприетарного Key Block в формате TR-31 любое значение Проприетарного *Использования ключа* конвертируется в соответствующее значение из стандарта TR-31.

Для экспорта в формат Verifone/GISKE Key Block всегда требуется 2DES/3DES TMK.

Экспорт в формат Verifone/GISKE Key Block поддерживается только для ключей 2DES/3DES TPK или TAK.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable X9.17 for export` | `Yes [Y]` | Доступен экспорт ключа в формат X9.17 (X, Y схемы). |
| | `No [N]` | Экспорт ключа в формат X9.17 невозможен. |
| `Key export and import in trusted format only` | `Yes [Y]` | Экспорт ключа в недоверенные форматы невозможен. |
| | `No [N]` | Доступен экспорт ключа в недоверенные форматы (X, Y, U, T схемы). |
| `Enable export of a ZMK` | `Yes [Y]` | Доступен экспорт ZMK. |
| | `No [N]` | Экспорт ZMK невозможен. |
| `Enforce key type 002 separation for PCI HSM compliance` | `Yes [Y]` | Ограничены типы экспортируемых ключей (Variant), см. Примечание выше. TMK зашифрован под LMK 36-37/8. |
| (влияет на параметры: *Тип ключа*) | `No [N]` | Ограничены типы экспортируемых ключей (Variant), см. Примечание выше. TMK зашифрован под LMK 14-15/0. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'A8'.</td></tr>
<tr><td>Тип ключа</td><td>3 H</td><td>Тип экспортируемого ключа. Допустимые значения см. в таблице на странице 14.</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Опционально.<br>Если присутствует, следующее поле обязательно.</td></tr>
<tr><td>ZMK/TMK флаг</td><td>1 N</td><td>Опционально; присутствует, только если присутствует разделитель выше.<br>'0': ZMK (значение по умолчанию, если поле не объявлено)<br>'1': TMK</td></tr>
<tr><td>ZMK (или TMK)</td><td></td><td>Зональный (или Терминальный) Мастер-Ключ.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>ZMK, зашифрованный под LMK 04-05.<br>TMK, зашифрованный под LMK 14-15/0 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: No</code>) или LMK 36-37/8 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: Yes</code>).</td></tr>
<tr><td></td><td>'S' + n A</td><td>ZMK (или TMK) должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'K0', '51', '52'</td><td>'T', 'A'</td><td>'B', 'E', 'N'</td></tr>
</table></td></tr>
<tr><td>Ключ</td><td></td><td>Экспортируемый ключ, зашифрованный под LMK.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Ключ, зашифрованный под соответствующим LMK, определяемым значением поля Тип ключа.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>Любое допустимое значение</td><td>'T', 'A'</td><td>Любое допустимое значение</td></tr>
</table>
Для экспорта в формат Verifone/GISKE Key Block ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'M0', 'M3'</td><td>'T'</td><td>'N', 'C', 'G'</td></tr>
<tr><td>'P0', '71'</td><td>'T'</td><td>'N', 'B', 'E'</td></tr>
</table></td></tr>
<tr><td>Ключевая схема (ZMK или TMK)</td><td>1 A</td><td>Схема шифрования ключа под ZMK (или TMK). Список ключевых схем см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста».</td></tr>
<tr><td>Atalla вариант</td><td>1/2 N</td><td>Atalla вариант. Опционально; используется при работе с оборудованием Atalla.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае экспорта ключа в формат Key Block (например, TR-31 или Проприетарный Key Block) при использовании Key Block LMK:</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '&'. Опционально; присутствует, только если экспортируемый ключ в формате Key Block. Если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Новое значение экспортируемости</td><td>1 A</td><td>Поле Экспортируемость, включаемое в заголовок Key Block.<br>Допустимое значение: 'N'.</td></tr>
</table>

| | | |
|---|---|---|
| Разделитель | 1 A | Значение '!'. Опционально; присутствует только при экспорте ключа в формат TR-31 Key Block. Если присутствует, следующее поле обязательно. |
| Идентификатор (ID) версии Key Block | 1 A | ID версии Key Block (подробнее см. ASC X9 TR 31-2018):<br>'A': Key Block, защищённый методом Key Variant Binding<br>'B': Key Block, защищённый методом Key Derivation Binding<br>'C': Key Block, защищённый методом Key Variant Binding<br>'D': Key Block, защищённый методом AES Key Derivation Binding |
| Следующие поля присутствуют только в случае экспорта ключа в формат TR-31 при использовании Variant LMK: | | |
| Разделитель | 1 A | Значение '&'. Опционально; присутствует только в случае экспорта ключа в формат TR-31. Если присутствует, следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок TR-31 Key Block. Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице использования ключей в «КриптоПро HSM. Руководство программиста». |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок TR-31 Key Block. Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице режимов использования ключей в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок TR-31 Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок TR-31 Key Block.<br>Допустимые значения: 'N' или 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '02'. |
| Следующие 3 поля определяются для каждого опционального блока.<br>*Примечание*: Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Разделитель | 1 A | Значение '!'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор (ID) версии Key Block | 1 A | ID версии Key Block (подробнее см. ASC X9 TR 31-2018):<br>'A': Key Block, защищённый методом Key Variant Binding<br>'B': Key Block, защищённый методом Key Derivation Binding<br>'C': Key Block, защищённый методом Key Variant Binding |
| Следующие поля присутствуют только в случае экспорта ключа в формат GISKE при использовании Variant LMK: | | |
| Разделитель | 1 A | Значение '&'. Опционально; присутствует только в случае экспорта ключа в формат GISKE. Если присутствует, следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок GISKE Key Block.<br>Допустимые значения: 'P0', 'K0', '00', '10', '20', '30', '40', '50', '60'. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок GISKE Key Block.<br>Допустимые значения: '00' .. '99'. |
| Идентификатор (ID) Key Block | 1 A | Идентификатор Key Block, определяющий первый байт заголовка GISKE Key Block.<br>Допустимые значения: 'A' или '2'. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |

| | | |
|---|---|---|
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'A9'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность ZMK или TMK<br>'11': Нарушена четность ключа<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Ключ (под ZMK или TMK) | 'U' или 'X' + 32 H или 'T' или 'Y' + 48 H или 'R' + n A или 'S' + n A или 'V' + n A | Ключ, зашифрованный под ZMK или TMK. |
| KCV | 6 H | Проверочное значение ключа. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [BY] — Трансляция ZMK (из-под ZMK под LMK)

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Определяется по ТТК (И)**<br>Активности: **import.000.host** | |
| Key Block LMK | Авторизация: **При импорте из формата, отличного от Key Block**<br>Активности: **import.{key}.host** | |

**Описание функции:** Расшифрование ZMK, зашифрованного под ZMK, и последующее зашифрование под LMK.

**Авторизация:**

Команда проверяет флаг 'И' (импорт) для заданного типа ключа в таблице типов ключей (ТТК, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **import.000.host** должна быть авторизована.

Требование авторизации для команды зависит только от ключевой схемы:

| Ключевая схема (ZMK) | Авторизация |
|---|---|
| 'S' (Проприетарный Key Block) | Не требуется |
| 'R' (TR-31 Key Block) | Не требуется |
| 'U', 'T' (Variant) | Требуется |
| 'X', 'Y' (ANSI X9.17) | Требуется |

Если авторизация требуется, HSM должен находиться в авторизованном состоянии, либо активность **import.{key}.host** должна быть авторизована, где 'key' — значение *Использования ключа* импортируемого ключа.

**Примечания:** Данная команда не требует, чтобы у импортируемого ZMK были выставлены биты четности. Однако команда гарантирует, что у выходного ZMK, зашифрованного под LMK, биты четности будут выставлены. В случае нарушения четности у импортируемого ZMK команда возвращает код ошибки '01' и далее работает штатно.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable ZMK translate command` | `Yes [Y]` | Команда доступна. |
| | `No [N]` | Команда недоступна. |
| `Enable X9.17 for import` | `Yes [Y]` | Доступен импорт ключа из формата X9.17 (X, Y схемы). |
| | `No [N]` | Импорт ключа из формата X9.17 невозможен. |
| `Key export and import in trusted format only` | `Yes [Y]` | Импорт ключа из недоверенных форматов невозможен. |
| | `No [N]` | Доступен импорт ключа из недоверенных форматов (X, Y, U, T схемы). |
| `Enable import of a ZMK` | `Yes [Y]` | Команда доступна. |
| | `No [N]` | Команда недоступна. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'BY'.</td></tr>
<tr><td>ZMKi</td><td></td><td>ZMKi, зашифрованный под LMK.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>ZMKi, зашифрованный под LMK 04-05.</td></tr>
<tr><td></td><td>'S' + n A</td><td>ZMKi должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'K0', '52'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>ZMK</td><td>'U' или<br>'X' + 32 H<br>или<br>'T' или<br>'Y' + 48 H<br>или<br>'R' + n A<br>или<br>'S' + n A</td><td>ZMK, зашифрованный под ZMKi. ZMK может быть в формате X9.17, Variant или Key Block.<br>Если ZMK в формате Key Block, ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'K0', '52'</td><td>'T', 'A'</td><td>Любое допустимое значение</td></tr>
</table></td></tr>
<tr><td>Atalla вариант</td><td>1/2 N</td><td>Atalla вариант. Опционально; используется при работе с оборудованием Atalla.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Опционально; если присутствует, следующие 3 поля обязательны.</td></tr>
<tr><td>Зарезервировано</td><td>1 A</td><td>Опционально; если присутствует — значение '0'.</td></tr>
<tr><td>Ключевая схема (LMK)</td><td>1 A</td><td>Опционально. Схема шифрования выходного ключа под LMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста».</td></tr>
<tr><td>Тип KCV</td><td>1 A</td><td>Опционально. Метод вычисления проверочного значения ключа:<br>'0': 16-значный KCV (режим обратной совместимости)<br>'1': 6-значный KCV<br>Примечание: поддерживается генерация только 6-значных KCV.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае импорта ключа из формата TR-31 при использовании Key Block LMK:</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '#'. Опционально; может присутствовать, только если импортируемый ZMK в формате TR-31 Key Block. Если присутствует, следующие поля обязательны.</td></tr>
<tr><td>Новое значение использования ключа</td><td>2 A</td><td>Поле Использование ключа, включаемое в заголовок Key Block.<br>Допустимые значения: 'K0' или '52'.</td></tr>
<tr><td>Количество опциональных блоков</td><td>2 N</td><td>Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '06'.</td></tr>
<tr><td colspan="3">Следующие 3 поля определяются для каждого опционального блока:<br>Примечание: Если Количество опциональных блоков = '00', следующие 3 поля не присутствуют.</td></tr>
<tr><td>Идентификатор блока</td><td>2 A</td><td>Любое допустимое значение, кроме 'KS', 'KV', 'PB'.</td></tr>
</table>

| | | |
|---|---|---|
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Следующие поля присутствуют только в случае импорта ключа из формата, отличного от Key Block (например, X9.17), при использовании Key Block LMK: | | |
| Разделитель | 1 A | Значение '#'. Опционально; присутствует, только если импортируемый ZMK в формате, отличном от Key Block. Если присутствует, следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: 'K0' или '52'. |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block. Любое допустимое значение для указанного *Использования ключа*. Допустимые значения см. в таблице режимов использования ключей в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N' или 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока.<br>*Примечание*: Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'BZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Нарушена четность ZMK (предупреждение)<br>'10': Нарушена четность ZMKi<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| ZMK | | ZMK, зашифрованный под LMK. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | ZMK, зашифрованный под LMK 04-05. |
| | 'S' + n A | ZMK, зашифрованный под LMK. |
| KCV | 6 H | Результат зашифрования 64 бинарных нулей под ZMK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 3 Команды трансляции при смене LMK

Данные, которые хранятся и обрабатываются на хосте, как правило зашифрованы с использованием LMK HSM. Если LMK меняется, соответствующие зашифрованные данные невозможно использовать до их трансляции (перешифрования с использованием нового LMK). Для поддержки этой операции в HSM предусмотрена возможность одновременного хранения старого и нового LMK:

- если текущий LMK является «новым», необходимо загрузить «старый» LMK в хранилище смены ключей (например, с помощью консольной команды LO)
- если текущий LMK является «старым», необходимо загрузить «новый» LMK в хранилище смены ключей (например, с помощью консольной команды LN)

HSM не различает, какой LMK загружен в хранилище смены ключей («старый» или «новый»). Команды, выполняющие трансляцию данных, всегда перешифровывают их из-под «старого» LMK под «новый» LMK.
После того, как соответствующий LMK был загружен в хранилище смены ключей, все данные, хранящиеся на хосте и зашифрованные под «старым» LMK, должны быть переданы на HSM для трансляции.

HSM поддерживает следующие команды хоста для трансляции (перешифрования) PIN/ключей при изменении LMK:

## [BG] — Трансляция PIN и длины PIN

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование PIN, зашифрованного под «старым» LMK, и последующее зашифрование под «новым» LMK. При этом при расшифровании используется значение настройки безопасности `PIN Length` в момент загрузки «старого» LMK, при зашифровании — текущее значение настройки безопасности `PIN length`.
«Старый» или «новый» LMK должен быть предварительно загружен в хранилище смены ключей.

**Примечания:** Команда может использоваться для трансляции только длины PIN (без трансляции самого PIN). В этом случае необходимо загрузить в хранилище смены ключей LMK, совпадающий с текущим.

Значение $L_1$ определяется значением настройки безопасности `PIN length` в момент загрузки «старого» LMK. Значение $L_2$ определяется текущим значением настройки безопасности `PIN length`, установленным с помощью консольной команды CS.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| | **КОМАНДА** | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'BG'. |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| PIN | | PIN, зашифрованный под «старым» LMK. |
| | $L_1$N<br>или<br>$L_1$H | При использовании «старого» 3DES Variant или Key Block LMK длина зашифрованного PIN равна $L_1$ цифр, где $L_1$ определяется значением настройки безопасности `PIN length` в момент загрузки «старого» LMK.<br>$L_1$ должно быть меньше или равно $L_2$. |
| | или<br>'M' + 32 H | При использовании «старого» AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | **ОТВЕТ** | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'BH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| PIN | | PIN, зашифрованный под текущим LMK. |
| | $L_2$N<br>или<br>$L_2$H | При использовании «нового» 3DES Variant или Key Block LMK длина зашифрованного PIN равна $L_2$ цифр, где $L_2$ зависит от текущего значения настройки безопасности `PIN length`. |
| | или<br>'M' + 32 H | При использовании «нового» AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [BW] — Трансляция ключей при смене LMK и смена типа ключей

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Команда используется для выполнения одной из следующих операций:

• Трансляция ключа при смене LMK — расшифрование ключа, зашифрованных под «старым» LMK, и последующее зашифрование его под «новым» LMK.
«Старый» или «новый» LMK должен быть предварительно загружен в хранилище смены ключей.

• Переход от типа ключа 002 (ключи зашифрованы под LMK 14-15/0) к новому типу ключа для разделения ключей в соответствии с PCI HSM.

**Примечания:** Трансляция ключей при смене «старого» Key Block LMK на «новый» Variant LMK не поддерживается.

Если в поле *2-значный код типа ключа* указан код, соответствующий 3-значному коду типа ключа (без средней цифры), поле *3-значный код типа ключа* не должно присутствовать.

Типы ключей, которые необходимо использовать при переходе с типа ключа 002 (если *2-значный код типа ключа* = 'E2' или 'F2'), описаны в «КриптоПро HSM. Руководство программиста».

Возможность смены типа ключа 002 на тип ключа, совместимый с PCI HSM, доступна только в том случае, если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`.

При значении поля *2-значный код типа ключа* = 'E2' (смена типа ключа без смены LMK) используется «текущий» LMK, загрузка LMK в хранилище смены ключей не требуется.

| Алгоритм ключа: | DES | AES |
|---|---|---|
| Метод вычисления KCV: | Зашифрование блока бинарных нулей | Вычисление CMAC от блока бинарных нулей |

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce key type 002 separation for PCI HSM compliance` | `Yes [Y]` | Смена типа ключа 002 на тип ключа, совместимый с PCI HSM, невозможна. |
| | `No [N]` | Доступна смена типа ключа 002 на тип ключа, совместимый с PCI HSM. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'BW'. |
| 2-значный код типа ключа | 2 H | '00' .. '9E': только трансляция ключей (при смене LMK); поле содержит 2-значный код типа ключа, идентичный стандартному 3-значному коду типа ключа, но без средней цифры.<br>'E2': только смена типа ключей с типа 002 на тип ключа, указанный ниже в поле *3-значный код типа ключа*. Это значение может использоваться, только если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No` и в хранилище смены ключей отсутствует LMK.<br>'F2': трансляция ключей (при смене LMK) и смена типа ключей с типа 002 на тип ключа, указанный ниже в поле *3-значный код типа ключа*. Это значение может использоваться, только если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`<br>'FF': только трансляция ключей (при смене LMK); используется тип ключа, указанный ниже в поле *3-значный код типа ключа*. |
| | 2 H | Значение 'FF'. |
| Флаг длины ключа | 1 N | '1': 2DES<br>'2': 3DES |
| | 1 H | Значение 'F'. |
| Ключ | | Ключ, для которого осуществляется трансляция и/или смена типа ключа. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | Ключ, зашифрованный под «старым» LMK, определяемым значением поля *2-значный код типа ключа*. |
| | 'S' + n A | Ключ, зашифрованный под «старым» LMK. |
| Разделитель | 1 A | Значение ';'. Опционально; присутствует только в случае *2-значного кода типа ключа* = 'E2', 'F2' или 'FF'. Если присутствует, следующее поле обязательно. |
| 3-значный код типа ключа | 3 H | В случае *2-значного кода типа ключа* = 'FF' содержит 3-значный код типа транслируемого ключа. Перечень допустимых значений см. в таблице типов ключей в «КриптоПро HSM. Руководство программиста».<br>В случае *2-значного кода типа ключа* = 'E2' или 'F2' содержит 3-значный код типа ключа, в который будет переведен ключ. Тип ключа для старого ключа должен иметь значение 002. Допустимые значения:<br>'002' (PVK, PVVK: смена типа ключа не требуется)<br>'70D' (TPK, PEK)<br>'80D' (TMK, KT, TK, KI, KCA, KMA)<br>'90D' (TKR) |
| | | Значение 'FFF'. |
| Разделитель | 1 A | Значение ';'. Опционально; если присутствует, следующие 3 поля обязательны. |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Ключевая схема (LMK) | 1 A | Опционально. Схема шифрования выходного ключа под LMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |

| | | |
|---|---|---|
| Следующие поля присутствуют только в случае трансляции закрытого ключа, зашифрованного под Variant LMK, в зашифрованный под Key Block LMK: | | |
| Разделитель | 1 A | Значение '#'. Опционально; должен присутствовать в случае трансляции закрытого ключа, зашифрованного под «старым» Variant LMK, в зашифрованный под «новым» Key Block LMK. Если присутствует, следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block.<br>Любое допустимое значение для указанного типа ключа. Должно быть совместимо с существующим типом ключа. Допустимые значения см. в таблице использования ключей в «КриптоПро HSM. Руководство программиста». |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block.<br>Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице режимов использования ключей в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N' или 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Разделитель | 1 A | Значение '!'. Опционально; присутствует только если присутствуют поля *Флаг возврата KCV* и *Тип KCV* ниже. |
| Флаг возврата KCV | 1 A | Опционально; если присутствует — значение '1'. |
| Тип KCV | 1 A | Опционально. Присутствует только если присутствует поле *Флаг возврата KCV*. Метод вычисления проверочного значения ключа.<br>'0': 16-значный KCV (6-значный KCV, дополненный слева 10 символами '0')<br>'1': 6-значный KCV |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'BX'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Недопустимый тип ключа<br>'05': Недопустимая длина ключа<br>'10': Нарушена четность ключа<br>'44': Смена типа ключа недоступна: смена типа ключа запрошена при выставленной настройке `Enforce key type 002 separation for PCI HSM compliance: Yes`<br>'45': Недопустимый целевой тип ключа<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |

| | | |
|---|---|---|
| Ключ | | Транслированный ключ, зашифрованный под LMK. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | Ключ, зашифрованный под «новым» LMK, определяемым значениями полей *2-значный код типа ключа* и *3-значный код типа ключа*. |
| | 'S' + n A | Ключ, зашифрованный под «новым» LMK. |
| KCV | 16/6 H | Опционально; присутствует только если присутствуют поля *Флаг возврата KCV* и *Тип KCV*. Проверочное значение ключа, размер поля зависит от значения поля *Тип KCV*. В случае формата 16 H содержит 6-значный KCV, дополненный слева 10 символами '0'. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [BS] — Очистка хранилища смены ключей

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Удаление ключа из хранилища смены ключей.

**Примечания:** Рекомендуется использовать данную команду после трансляции (расшифрования ключа, зашифрованного под «старым» LMK, и зашифрования под «новым» LMK) ключей, хранящихся на хосте.
Будет очищено хранилище смены ключей, соответствующее LMK с указанным в команде идентификатором.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'BS'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'BT'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 4 Команды управления ключами EMV

Следующие команды хоста используются для управления ключами EMV:

## [KI] — Выработка уникального ключа карты

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Выработка уникального ключа карты из мастер-ключа.

**Примечания:** Команда поддерживает:

- Выработку уникальных ключей для EMV карт
- Генерацию мастер-ключей карт для персонализации с использованием EMV CPS

Команда поддерживает генерацию сеансовых ключей для облачных схем мобильных платежей или HCE:

- ключи ограниченного использования Visa

В соответствии с таблицей ниже, метод диверсификации ключа определяет алгоритм для мастер-ключа, ключа карты и KEK, а также схему зашифрования выработанного ключа под KEK.

| **Метод диверсификации ключа** | **Алгоритм мастер-ключа, ключа карты** | **Алгоритм KEK** | **Ключевая схема (KEK)** |
|---|---|---|---|
| 'A', 'B', 'C', 'D', 'E', 'H' | 3DES | 3DES | 'X' для 112-битовых ключей (ANSI X9.17) |
| 'A', 'B', 'C', 'D', 'H' | 3DES | AES | 'N' для любого ключа AES (NIST SP800-38F Key Wrap) |
| 'I' | AES | AES | 'N' для любого ключа AES (NIST SP800-38F Key Wrap) |
| 'C' | AES | AES | 'N' для любого ключа AES |

| **Метод диверсификации ключа** | **Тип ключа MK (Variant LMK)** | **Использование ключа MK (Key Block LMK)** |
|---|---|---|
| 'A', 'B' | '109', '209', '309', '509', '709', '207' | 'E0', 'E2', 'E1', 'E4', 'E6', '32', 'E7' |
| 'C', 'D' | '207' | 'E7' |
| 'E', 'H' | '109' | 'E0' |
| 'I' | не применимо | '32', 'E0', 'E2', 'E6' |

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Restrict Key Check Value to 6 hex chars` | `Yes [Y]` | Только первые 6 символов KCV содержат проверочное значение ключа, остальные крайние правые символы устанавливаются в '0'. |
| (влияет на параметры: *DK KCV, CK-ENC KCV, CK-MAC KCV, CK-DEK KCV, PSK KCV*) | `No [N]` | Дополнительные ограничения на KCV не накладываются. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'KI'.</td></tr>
<tr><td>Тип MK</td><td></td><td>Тип мастер-ключа.</td></tr>
<tr><td></td><td>3 H</td><td>'109': MK-AC, зашифрованный под LMK 28-29/1<br>'209': MK-SMI, зашифрованный под LMK 28-29/2<br>'309': MK-SMC, зашифрованный под LMK 28-29/3<br>'509': MK-DN, зашифрованный под LMK 28-29/5<br>'709': MK-CVC3 или MK-DCVV, зашифрованный под LMK 28-29/7<br>'207': KMC, зашифрованный под LMK 24-25/2</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>MK</td><td></td><td>Мастер-ключ, из которого вырабатывается уникальный ключ, зашифрованный под LMK.</td></tr>
<tr><td></td><td>32 H<br>или<br>'U' + 32 H<br>или<br>'T' + 48 H</td><td>MK, зашифрованный под соответствующим LMK, определяемым значением поля Тип MK.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E1', 'E4'</td><td>'T'</td><td>'X', 'N'</td></tr>
<tr><td>'32', 'E0', 'E2', 'E6', 'E7'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Метод диверсификации ключа</td><td>1 A</td><td>EMV методы выработки уникального ключа из мастер-ключа.<br>'A': EMV 4.1 Book 2 Option A<br>'B': EMV 4.1 Book 2 Option B<br>'C': EMV CPS для мастер-ключей карт<br>Примечание: При использовании этого метода диверсификации из мастер-ключа будут выработаны 3 ключа (CK-ENC, CK-MAC и CK-DEK) в соответствии с EMV CPS.<br>'D': Generic Personalisation Key Derivation Method<br>'E': Visa Limited Use Key (LUK) (только в случае Тип MK = '109')<br>'H': Visa Limited Use Key (LUK) QR Code (только в случае Тип MK = '109')<br>'I': EMV 4.3 Option 'C' (AES)</td></tr>
<tr><td>Данные для диверсификации</td><td>n N</td><td>В случае Метода диверсификации ключа = 'A', 'B', 'E', 'H' или 'I':<br>Конкатенация PAN и 2-значного PAN Sequence Number.<br>Если PAN Sequence Number не определен, используется значение '00'.</td></tr>
<tr><td></td><td>6 B</td><td>В случае Метода диверсификации ключа = 'C':<br>Данные для диверсификации ключа карты (например, KEYDATA, состоящие из ID мастер-ключа и серийного номера чипа).</td></tr>
<tr><td></td><td>10 B</td><td>В случае Метода диверсификации ключа = 'C' и при использовании AES MK:<br>Данные для диверсификации ключа карты (например, KEYDATA, состоящие из ID мастер-ключа и серийного номера чипа).</td></tr>
<tr><td></td><td>16 B</td><td>В случае Метода диверсификации ключа = 'D':<br>Данные для диверсификации ключа.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
</table>

<table>
<tr><td colspan="3">Следующее поле присутствует только в случае Метода диверсификации ключа = 'E' или 'H':</td></tr>
<tr><td>YHHHHCC</td><td>7 N</td><td>Значение Год/Час/Счетчик, используемое для выработки ключа ограниченного использования (LUK) для генерации криптограммы ограниченного использования (LUC):<br>Y (0-9): последняя значащая цифра текущего года<br>HHHH (0001-8784): количество часов, прошедших с 01 января<br>CC (00-99): значение счетчика</td></tr>
<tr><td colspan="3">Следующие поля присутствуют для всех значений Метода диверсификации ключа:</td></tr>
<tr><td>KEK</td><td></td><td>Транспортный ключ шифрования ключей, зашифрованный под LMK.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>KEK, зашифрованный под LMK 24-25/1.</td></tr>
<tr><td></td><td>'S' + n A</td><td>KEK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'54'</td><td>'T', 'A'</td><td>'B', 'D', 'E', 'N'</td></tr>
</table></td></tr>
<tr><td>Ключевая схема (KEK)</td><td>1 A</td><td>Ключевая схема для зашифрования выработанного ключа под KEK.<br>'X': 3DES KEK (ANSI X9.17)<br>'N': AES KEK (NIST SP800-38F Key Wrap)</td></tr>
<tr><td>Тип KCV</td><td>1 A</td><td>'0': длина KCV 6 байтов<br>'1': длина KCV 3 байта</td></tr>
<tr><td>Atalla вариант</td><td>1/2 N</td><td>Опционально; используется при работе с оборудованием Atalla.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KJ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Недопустимый метод диверсификации ключа<br>'05': Недопустимый тип MK<br>'06': Недопустимые тип MK или данные для диверсификации для указанного метода диверсификации или значения YHHHHCC<br>'10': Нарушена четность MK<br>'11': Нарушена четность KEK<br>'27': Несоответствие значения ключевой схемы (KEK) значению выработанного ключа<br>'DA': Некорректный Key Block KEK<br>'EA': Некорректный Key Block MK<br>'FE': Не поддерживается с Variant LMK<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'DA' или 'EA': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующие 2 поля присутствуют только в случае *Метода диверсификации ключа* = 'A', 'B' или 'H': | | |

| | | |
|---|---|---|
| DK (KEK) | | Выработанный уникальный ключ, зашифрованный под KEK. |
| | 'X' + 16 B<br>или | В случае KEK, отличного от AES. |
| | 'N' + n B | В случае AES KEK. |
| DK KCV | 6 B или 3 B | Проверочное значение ключа DK. |
| Следующие 6 полей присутствуют только в случае *Метода диверсификации ключа* = 'C': | | |
| CK-ENC (KEK) | | Ключ карты для криптограмм, зашифрованный под KEK. |
| | 'X' + 16 B<br>или | В случае KEK, отличного от AES. |
| | 'N' + n B | В случае AES KEK. |
| CK-ENC KCV | 6 B или 3 B | Проверочное значение ключа CK-ENC. |
| CK-MAC (KEK) | | Ключ карты для аутентификации, зашифрованный под KEK. |
| | 'X' + 16 B<br>или | В случае KEK, отличного от AES. |
| | 'N' + n B | В случае AES KEK. |
| CK-MAC KCV | 6 B или 3 B | Проверочное значение ключа CK-MAC. |
| CK-DEK (KEK) | | Ключ карты для шифрования, зашифрованный под KEK. |
| | 'X' + 16 B<br>или | В случае KEK, отличного от AES. |
| | 'N' + n B | В случае AES KEK. |
| CK-DEK KCV | 6 B или 3 B | Проверочное значение ключа CK-DEK. |
| Следующие 2 поля присутствуют только в случае *Метода диверсификации ключа* = 'D': | | |
| PSK (KEK) | | Ключ системы персонализации, зашифрованный под KEK. |
| | 'X' + 16 B<br>или | В случае KEK, отличного от AES. |
| | 'N' + n B | В случае AES KEK. |
| PSK KCV | 6 B или 3 B | Проверочное значение ключа PSK. |
| Следующие 2 поля присутствуют только в случае *Метода диверсификации ключа* = 'E': | | |
| DK (KEK) | 'X' + 16 B | Выработанный уникальный ключ, зашифрованный под KEK. |
| DK KCV | 6 B или 3 B | Проверочное значение ключа DK. |
| Следующие 2 поля присутствуют только в случае *Метода диверсификации ключа* = 'I': | | |
| DK (KEK) | 'N' + n B | Выработанный уникальный ключ, зашифрованный под KEK. |
| DK KCV | 6 B или 3 B | Проверочное значение ключа DK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [L6] — Импорт закрытого ключа

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Требуется**<br>Активности: **import.rsa.host** | |
| Key Block LMK | | Авторизация: **Требуется**<br>Активности: **import.03.host** |

**Описание функции:** Расшифрование закрытого ключа RSA/ECC, зашифрованного под ZMK, и последующее зашифрование под LMK.

**Авторизация:** Авторизация требуется только для импорта ключа RSA, для импорта ключа ECC авторизация не требуется.

**Примечания:** **При импорте закрытого ключа RSA**

Импортируемый закрытый ключ RSA должен быть представлен в формате 5 компонент CRT (p, q, dp, dq, u, где dp = d mod (p-1), dq = d mod (q-1), u = $q^{-1}$ mod p).
Каждая компонента CRT расшифровывается с использованием ключа AES или 3DES ZMK и режима шифрования ECB или CBC.

При импорте ключа, зашифрованного под ZMK, применяются ключи с сопоставимыми значениями силы ключа (key strength) (подробнее см. в NIST SP800-57 часть 1).

Следующая таблица определяет необходимую длину ключей AES или 3DES, используемых для защиты закрытых ключей RSA:

| Длина ключа RSA (в битах) | 3DES ZMK | AES ZMK |
|---|---|---|
| 320 .. 1024 | 112/168-битный | 128/192/256-битный |
| 1025 .. 2048 | только 168-битный | 128/192/256-битный |
| 2049 .. 3072 | н/д | 128/192/256-битный |
| 3073 .. 4096 | н/д | только 192/256-битный |

Следующая таблица определяет допустимые значения Использования ключа и Режима использования выходного Key Block закрытого ключа RSA:

| Использование ключа | Режим использования (допустимые значения) |
|---|---|
| '03' (подпись/управление ключами) | 'D', 'N', 'S' |
| '04' (ICC) | 'N', 'S' |
| '05' (трансляция PIN) | 'D', 'N' |
| '06' (расшифрование данных) | 'D', 'N' |

**При импорте закрытого ключа ECC**

Для закрытых ключей ECC допускается импорт только из-под AES ZMK. Импортируемый закрытый ключ ECC должен быть представлен в формате ASC X9 TR 31-2018.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Key export and import in trusted format only` | `Yes [Y]` | При использовании закрытого ключа RSA возможен импорт ключа только из формата Key Block, команда недоступна. |
| | `No [N]` | Импорт ключа RSA возможен из любого допустимого формата, команда доступна. |
| `Enable import and export of RSA Private Keys` | `Yes [Y]` | Возможен импорт закрытого ключа RSA, команда доступна. |
| | `No [N]` | Импорт закрытого ключа RSA невозможен, команда недоступна. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'L6'.</td></tr>
<tr><td>ZMK</td><td></td><td>Зональный мастер-ключ, используемый для защиты импортируемого закрытого ключа.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>ZMK, зашифрованный под LMK 04-05/0.</td></tr>
<tr><td></td><td>'S' + n A</td><td>ZMK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'K0', 'K1', '52'</td><td>'T', 'A'</td><td>'B', 'D', 'E', 'N'</td></tr>
</table></td></tr>
<tr><td>Формат ключа</td><td>1 N</td><td>Формат импортируемого закрытого ключа:<br>'0': 5 компонент CRT (p, q, dp, dq, u по порядку)<br>'9': ASC X9 TR 31-2018</td></tr>
<tr><td colspan="3">Следующие 2 или 3 поля присутствуют только в случае Формата ключа = '0':</td></tr>
<tr><td>Режим шифрования</td><td>1 N</td><td>Режим шифрования, используемый при расшифровании закрытого ключа, зашифрованного под ZMK:<br>'0': ECB<br>'1': CBC (каждая компонента (плюс любое дополнение) отдельно зашифрована с использованием нулевого IV)</td></tr>
<tr><td>Режим дополнения</td><td>1 N</td><td>Режим дополнения ISO 9797-1:<br>'1': режим дополнения 1 (опционально дополнить 0x00 до длины блока)<br>'2': режим дополнения 2 (обязательно добавить 0x80 и опционально дополнить 0x00 до длины блока)<br>'3': режим дополнения 3 (добавить перед значением байт(ы) длины (содержит значение длины компоненты CRT без дополнений в байтах), опционально дополнить 0x00)</td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Режима дополнения = '3':</td></tr>
</table>

<table>
<tr><td>Байт длины</td><td>1 N</td><td>'0': без BER-кодировки (один байт)<br>'1': BER-кодировка</td></tr>
<tr><td>Длина закрытого ключа</td><td>4 H</td><td>В случае Формата ключа = '0' — длина (в байтах) следующего поля.<br>В случае Формата ключа = '9' — значение 'FFFF'.</td></tr>
<tr><td>Закрытый ключ</td><td></td><td>Закрытый ключ, зашифрованный под ZMK.</td></tr>
<tr><td></td><td>n B</td><td>В случае Формата ключа = '0'.</td></tr>
<tr><td></td><td>'R' + n A</td><td>В случае Формата ключа = '9' закрытый ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'K3'</td><td>'E'</td><td>'X'</td></tr>
<tr><td>'S0'</td><td>'E'</td><td>'S'</td></tr>
<tr><td>'03'</td><td>'E'</td><td>'S', 'X', 'N'</td></tr>
</table>.</td></tr>
<tr><td>Флаг проверки импортированного ключа</td><td>1 N</td><td>Присутствует только в случае Формата ключа = '0'.<br>'0': Проверка закрытого ключа не выполняется<br>'1': Необходима проверка импортированного закрытого ключа</td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае Флага проверки импортированного ключа = '1':</td></tr>
<tr><td>Длина открытого ключа</td><td>4 H</td><td>Длина (в байтах) модуля открытого ключа.</td></tr>
<tr><td>Открытый ключ</td><td>n B</td><td>Модуль открытого ключа (n).</td></tr>
<tr><td>Длина открытой экспоненты</td><td>4 H</td><td>Длина (в байтах) открытой экспоненты.</td></tr>
<tr><td>Открытая экспонента</td><td>n B</td><td>Открытая экспонента (e).</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае использования Key Block LMK:</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '#'.</td></tr>
<tr><td colspan="3">Следующие 5 полей присутствуют только в случае Формата ключа = '0':</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '~'. опционально; если присутствует, следующие 2 поля обязательны.</td></tr>
<tr><td>Использование ключа</td><td>2 A</td><td>Поле Использование ключа, включаемое в заголовок Key Block.<br>Допустимые значения: '03', '04', '05', '06'.<br>Если не указано, используется значение '03'.</td></tr>
<tr><td>Режим использования</td><td>1 A</td><td>Поле Режим использования, включаемое в заголовок Key Block.<br>Допустимые значения: 'D', 'N', 'S'.<br>Если не указано, используется значение 'N'.</td></tr>
<tr><td>Номер версии ключа</td><td>2 N</td><td>Поле Номер версии ключа, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'.</td></tr>
<tr><td>Экспортируемость</td><td>1 A</td><td>Поле Экспортируемость, включаемое в заголовок Key Block.<br>Допустимые значения: 'N', 'S'.</td></tr>
<tr><td>Количество опциональных блоков</td><td>2 N</td><td>Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'.</td></tr>
<tr><td colspan="3">Следующие 3 поля определяются для каждого опционального блока:<br>Примечание: Если Количество опциональных блоков = '00', следующие 3 поля не присутствуют.</td></tr>
<tr><td>Идентификатор блока</td><td>2 A</td><td>Любое допустимое значение, кроме 'PB'.</td></tr>
<tr><td>Длина блока</td><td>2 H</td><td>Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует.</td></tr>
<tr><td>Данные блока</td><td>n A</td><td>Данные блока.</td></tr>
</table>

| | | |
|---|---|---|
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'L7'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Команда отключена согласно конфигурации безопасности<br>'10': Нарушена четность ZMK<br>'80': Ошибка длины закрытого ключа<br>'D1': Некорректный Key Block ZMK<br>'D3': Некорректный формат ключа<br>'D5': Ошибка силы ключа ZMK (ошибка проверки безопасности длины ключа)<br>'D8': Некорректный режим шифрования<br>'D9': Некорректный режим дополнения<br>'DA': Некорректный байт длины<br>'DB': Ошибка длины открытого ключа<br>'DC': Ошибка длины открытой экспоненты<br>'DD': Ошибка длины CRT<br>'DE': Некорректный флаг проверки импортированного ключа<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D1': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Длина закрытого ключа | 4 H | Длина следующего поля. |
| Закрытый ключ | | Закрытый ключ, зашифрованный под LMK. |
| | n B | Закрытый ключ, зашифрованный под LMK 34-35/0. |
| | 'S' + n B | В случае *Формата ключа* = '0' закрытый ключ должен соответствовать следующему формату:<br>Использование ключа: '03' или значение *Использования ключа*, указанное после разделителя '∼'<br>Алгоритм: 'R'<br>Режим использования: 'S' или значение *Режима использования*, указанное после разделителя '∼' |
| | 'S' + n A | В случае *Формата ключа* = '9' закрытый ключ должен соответствовать следующему формату:<br>Использование ключа: '03'<br>Алгоритм: 'E'<br>Режим использования: 'S', 'X', 'N' |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [L8] — Экспорт закрытого ключа

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Требуется**<br>Активности: **export.rsa.host** | |
| Key Block LMK | | Авторизация: **Требуется**<br>Активности: **export.03.host** |

**Описание функции:** Расшифрование закрытого ключа RSA/ECC, зашифрованного под LMK, и последующее зашифрование под ZMK.

**Авторизация:** Авторизация требуется только для экспорта ключа RSA, для экспорта ключа ECC авторизация не требуется.

**Примечания:**

**При экспорте закрытого ключа RSA**

Экспортированный закрытый ключ RSA будет представлен в формате 5 компонент CRT (p, q, dp, dq, u, где dp = d mod (p-1), dq = d mod (q-1), u = $q^{-1}$ mod p).
Каждая компонента CRT зашифровывается с использованием ключа AES или 3DES ZMK и режима шифрования ECB или CBC.

При экспорте ключа и последующем его зашифровании под ZMK применяются ключи с сопоставимыми значениями силы ключа (key strength) (подробнее см. в NIST SP800-57 часть 1).

Следующая таблица определяет необходимую длину ключей AES или 3DES, используемых для защиты закрытых ключей RSA:

| Длина ключа RSA (в битах) | 3DES ZMK | AES ZMK |
|---|---|---|
| 320 .. 1024 | 112/168-битный | 128/192/256-битный |
| 1025 .. 2048 | только 168-битный | 128/192/256-битный |
| 2049 .. 3072 | н/д | 128/192/256-битный |
| 3073 .. 4096 | н/д | только 192/256-битный |

**При экспорте закрытого ключа ECC**

Для закрытых ключей ECC допускается экспорт только под AES ZMK. Экспортированный закрытый ключ ECC будет представлен в формате ASC X9 TR 31-2018.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce PCI HSMv3 Key Equivalence for Key Wrapping`<br>(влияет на параметры: *ZMK, Закрытый ключ*) | `Yes [Y]` | Сила ZMK (key strength) должна быть не меньше силы закрытого ключа. |
| | `No [N]` | Ограничения на силу ZMK не накладываются. |

| | | |
|---|---|---|
| `Key export and import in trusted format only` | `Yes [Y]` | При использовании закрытого ключа RSA возможен экспорт ключа только в формат Key Block, команда недоступна. |
| | `No [N]` | Экспорт ключа RSA возможен в любой допустимый формат, команда доступна. |
| `Enable import and export of RSA Private Keys` | `Yes [Y]` | Экспорт закрытого ключа RSA разрешен, команда доступна. |
| | `No [N]` | Экспорт закрытого ключа RSA невозможен, команда недоступна. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'L8'. |
| ZMK | | Зональный мастер-ключ, используемый для защиты экспортированного закрытого ключа. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | ZMK, зашифрованный под LMK 04-05. |
| | 'S' + n A | ZMK должен соответствовать следующему формату:<br>Использование ключа: 'K0', 'K1', '52'<br>Алгоритм: 'T', 'A'<br>Режим использования: 'B', 'D', 'E', 'N' |
| Формат ключа | 1 N | Формат экспортированного закрытого ключа:<br>'0': 5 компонент CRT (p, q, dp, dq, u по порядку)<br>'9': ASC X9 TR 31-2018 |
| Следующие 2 или 3 поля присутствуют только в случае *Формата ключа* = '0': | | |
| Режим шифрования | 1 N | Режим шифрования, используемый при зашифровании закрытого ключа под ZMK:<br>'0': ECB<br>'1': CBC (каждая компонента (плюс любое дополнение) отдельно зашифрована с использованием нулевого IV) |
| Режим дополнения | 1 N | Режим дополнения ISO 9797-1:<br>'1': режим дополнения 1 (опционально дополнить 0x00 до длины блока)<br>'2': режим дополнения 2 (обязательно добавить 0x80 и опционально дополнить 0x00 до длины блока)<br>'3': режим дополнения 3 (добавить перед значением байт(ы) длины (содержит значение длины компоненты CRT без дополнений в байтах), опционально дополнить 0x00) |
| Следующее поле присутствует только в случае *Режима дополнения* = '3': | | |
| Байт длины | 1 N | '0': без BER-кодировки (один байт)<br>'1': BER-кодировка |
| Длина закрытого ключа | 4 H | Длина (в байтах) следующего поля. |
| | | Значение 'FFFF'. |
| Закрытый ключ | | Закрытый ключ, зашифрованный под LMK. |
| | n B | Закрытый ключ, зашифрованный под LMK 34-35/0. |

<table>
<tr><td></td><td>'S' + n B</td><td>В случае Формата ключа = '0' закрытый ключ должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'03'</td><td>'R'</td><td>'S', 'D', 'N'</td></tr></table></td></tr>
<tr><td></td><td>'S' + n A</td><td>В случае Формата ключа = '9' закрытый ключ должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'03'</td><td>'E'</td><td>'S', 'X', 'N'</td></tr></table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае экспорта ключа в формат ASC X9 TR 31 (Формата ключа = '9'):</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '&'. Опционально; может присутствовать, только если экспортируется ключ ECC. Если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Экспортируемость</td><td>1 A</td><td>Поле Экспортируемость, включаемое в заголовок Key Block.<br>Допустимое значение: 'N'.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'L9'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Команда отключена согласно конфигурации безопасности<br>'10': Нарушена четность ZMK<br>'75': Несоответствие открытого/закрытого ключей<br>'80': Ошибка длины закрытого ключа<br>'D1': Некорректный Key Block ZMK<br>'D3': Некорректный формат ключа<br>'D5': Ошибка силы ключа ZMK (ошибка проверки безопасности длины ключа)<br>'D6': Запрещен экспорт ключей (значение Экспортируемости 'N')<br>'D7': Некорректный Key Block закрытого ключа<br>'D8': Некорректный режим шифрования<br>'D9': Некорректный режим дополнения<br>'DA': Некорректный байт длины<br>'DD': Ошибка длины CRT<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D1' или 'D7': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующие 2 поля присутствуют только в случае *Кода ошибки* = '00': | | |
| Длина закрытого ключа | 4 H | В случае *Формата ключа* = '0' — длина (в байтах) следующего поля.<br>В случае *Формата ключа* = '9' — значение 'FFFF'. |
| Закрытый ключ | n B | Экспортированный закрытый ключ, зашифрованный под ZMK.<br>В случае *Формата ключа* = '0'. |

<table>
<tr><td></td><td>'R' + n A</td><td>В случае Формата ключа = '9' закрытый ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'K3'</td><td>'E'</td><td>'X'</td></tr>
<tr><td>'S0'</td><td>'E'</td><td>'S'</td></tr>
<tr><td>'03'</td><td>'E'</td><td>'N'</td></tr>
</table>.</td></tr>
<tr><td>Символ конца ответа</td><td>1 C</td><td>Значение 0x19. Присутствует, только если присутствует в команде.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Присутствует, только если присутствует в команде. Максимальная длина — 32 символа.</td></tr>
</table>

# 5 Команды управления асимметричными ключами

Следующие команды хоста используются для поддержки операций с ключами RSA и ECC:

## [EI] — Генерация ключевой пары RSA

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Требуется**<br>Активности: **generate.rsa.host** | |
| Key Block LMK | | Авторизация: **Требуется**<br>Активности: **generate.{key}.host** |

**Описание функции:** Генерация ключевой пары RSA.

**Авторизация:** Для всех значений *Индикатора типа ключа*, кроме '3' (ключи ICC), HSM должен находиться в авторизованном состоянии, либо должна быть авторизована соответствующая активность.

При использовании Variant LMK применяется активность **generate.rsa.host**.

При использовании Key Block LMK применяется активность вида **generate.{key}.host**, где 'key' — значение *Использования ключа* генерируемого закрытого ключа RSA.

**Примечания:** Если в команде указана открытая экспонента, её значение должно быть нечётным (т.е. младший бит должен быть равен 1); в противном случае HSM вернёт ошибку.

В случае генерации RSA ключей длиннее 2048 бит необходимо использовать AES Key Block LMK.

В случае Key Block LMK закрытый ключ RSA генерируется в формате Key Block со следующими атрибутами:

| **Поле** | **Значение** |
|---|---|
| Использование ключа | '03' (для *Индикатора типа ключа* = '0', '1', '2')<br>'04' (для *Индикатора типа ключа* = '3')<br>'05' (для *Индикатора типа ключа* = '5')<br>'06' (для *Индикатора типа ключа* = '4') |
| Алгоритм | 'R' |
| Режим использования | 'S' (для *Индикатора типа ключа* = '0' и '3')<br>'D' (для *Индикатора типа ключа* = '1' и '5')<br>'N' (для *Индикатора типа ключа* = '2' и '4') |
| Экспортируемость | 'N' (если явно не указано значение 'S') |

Сгенерированный открытый ключ RSA возвращается в том же формате, что и при использовании Variant LMK.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'EI'. |
| Индикатор типа ключа | 1 N | Определяет предполагаемое использование ключевой пары:<br>'0': Только подпись<br>'1': Только управление ключами<br>'2': Подпись и управление ключами<br>'3': Ключ Integrated Chip Card (ICC)<br>'4': Ключ общего назначения (например, зашифрование/расшифрование TLS/SSL premaster secret)<br>'5': Зашифрование/расшифрование PIN |
| Длина ключа | 4 N | Длина модуля RSA в битах:<br>'0320' .. '2048': если AES Key Block LMK не используется<br>'0320' .. '4096': если используется AES Key Block LMK |
| Метод кодирования открытого ключа | 2 N | '01': DER, ASN.1 (беззнаковое целое)<br>'02': DER, ASN.1 (целое в формате дополнительного кода) |
| Длина открытой экспоненты | 4 N | Опционально. Присутствует, если присутствует открытая экспонента. Длина открытой экспоненты в битах. |
| Открытая экспонента | n B | Опционально. Должно содержать нечётное значение. Если поле отсутствует, используется экспонента по умолчанию 65537. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующие поля присутствуют в случае генерации закрытого ключа Key Block RSA: | | |
| Разделитель | 1 A | Значение '#'. Опционально; должен присутствовать, если используется Key Block LMK. Если присутствует, следующие поля обязательны. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block. Допустимые значение: '00' .. '99'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже. Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Разделитель | 1 A | Значение '&'. Опционально; если присутствует, следующее поле обязательно. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block (байт 11) закрытого ключа.<br>Допустимые значения: 'N' или 'S'. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">ОТВЕТ</td></tr>
<tr><td>Заголовок ответа</td><td>m A</td><td>Заголовок команды, возвращаемый хосту без изменений.</td></tr>
<tr><td>Код ответа</td><td>2 A</td><td>Значение 'EJ'.</td></tr>
<tr><td>Код ошибки</td><td>2 H</td><td>'00': Без ошибок<br>'03': Недопустимый метод кодирования открытого ключа<br>'04': Ошибка длины ключа<br>'05': Недопустимый тип ключа<br>'06': Ошибка длины открытой экспоненты<br>'08': Открытая экспонента четная<br>'47': Алгоритм не лицензирован<br>'48': Требуется более сильный LMK для защиты RSA ключа такой длины<br>'68': Команда недоступна<br>или другой стандартный код ошибки.</td></tr>
<tr><td>Открытый ключ</td><td>n B</td><td>Открытый ключ в формате, определенном в поле Метод кодирования открытого ключа.</td></tr>
<tr><td>Длина закрытого ключа RSA</td><td>4 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
<tr><td>Закрытый ключ RSA</td><td></td><td>Закрытый ключ RSA, зашифрованный под LMK.</td></tr>
<tr><td></td><td>n B</td><td>Закрытый ключ RSA, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B</td><td>Закрытый ключ RSA должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03', '04', '05', '06'</td><td>'R'</td><td>'S', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>Символ конца ответа</td><td>1 C</td><td>Значение 0x19. Присутствует, только если присутствует в команде.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Присутствует, только если присутствует в команде. Максимальная длина — 32 символа.</td></tr>
</table>

## [FY] — Генерация ключевой пары ECC

| Variant LMK ☒ | AES Key Block LMK ☑ |
|---|---|
| Авторизация: **Требуется** | |
| Активности: **generate.03.host** | |

**Описание функции:** Генерация закрытого и открытого ключей ECC с использованием алгоритмов, основанных на эллиптических кривых.

**Примечания:** Команду допускается использовать только с AES Key Block LMK.
Поддерживаются следующие эллиптические кривые:

- FIPS 186-3 – NIST P-256
- FIPS 186-3 – NIST P-384
- FIPS 186-3 – NIST P-521

Выходной закрытый ключ ECC кодируется с идентификатором кривой в формате ASN.1 и зашифровывается под LMK.
Выходной открытый ключ представлен в виде блока SubjectPublicKeyInfo в формате ASN.1 согласно ANSI X9.62.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'FY'. |
| Версия команды | 2 N | Значение '01'. |
| Идентификатор кривой | 2 H | '00': FIPS 186-3 – NIST P-256<br>'01': FIPS 186-3 – NIST P-384<br>'02': FIPS 186-3 – NIST P-521 |
| Разделитель | 1 A | Значение ';'. Опционально; если присутствует, следующее поле обязательно. |
| Метод генерации ключей | 1 N | Метод генерации ключевой пары ECC:<br>'0': ISO 15946-1<br>'1': EMV v4.4 B2.2.4 Key Generation<br>Если поле отсутствует, по умолчанию используется метод ISO 15946-1. |
| Метод кодирования открытого ключа | 2 N | '03': несжатый открытый ключ ECC в формате X9.62 DER, ASN.1 |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Разделитель | 1 A | Значение '#'. |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block.<br>Допустимые значения: 'S', 'X', 'N'. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N', 'E', 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |

| | | |
|---|---|---|
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'FZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'A1': Функция работает только с AES Key Block<br>'D2': Некорректные параметры кривой<br>'D3': Недопустимый метод кодирования ключа<br>'E0': Недопустимый номер версии команды<br>'E1': Недопустимый метод генерации ключей<br>или другой стандартный код ошибки. |
| Длина открытого ключа ECC | 4 N | Длина (в байтах) следующего поля. |
| Открытый ключ ECC | n B | Открытый ключ в формате, определенном в поле *Метод кодирования открытого ключа*. |
| Закрытый ключ ECC | 'S' + n A | Закрытый ключ должен соответствовать следующему формату:<br>Использование ключа: '03'; Алгоритм: 'E'; Режим использования: 'S', 'X', 'N' |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [EK] — Загрузка закрытого ключа

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Загрузка закрытого ключа, зашифрованного под LMK, в защищенную от НСД память HSM.

**Примечания:** Хостовое приложение должно гарантировать, что ранее загруженный закрытый ключ не будет случайно перезаписан этой командой.
После загрузки ключа при его использовании по индексу в хранилище в команде требуется явно указывать соответствующий идентификатор LMK.

| Параметр | Формат | Описание |
|---|---|---|
| | | **КОМАНДА** |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'EK'. |
| Индекс ключа | 2 N | Индекс загружаемого в память HSM закрытого ключа (используется, если требуется хранить несколько ключей).<br>Допустимые значения: '00' .. '20'. |
| Длина закрытого ключа | 4 N | Длина (в байтах) следующего поля. |
| | 4 H | Значение 'FFFF'. |
| Закрытый ключ | | Загружаемый в HSM для хранения закрытый ключ. |
| | n B | Закрытый ключ, зашифрованный под LMK 34-35. |
| | 'S' + n B<br>или<br>'S' + n A | Закрытый ключ должен соответствовать следующему формату: |

| Использование ключа | Алгоритм | Режим использования |
|---|---|---|
| '03', '04', '05', '06' | 'R' | 'S', 'D', 'N' |
| '03' | 'E' | 'S', 'X', 'N' |

| | | |
|---|---|---|
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'EL'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Недопустимый индекс ключа<br>'04': Недостаточно памяти для хранения закрытого ключа<br>'47': Алгоритм не лицензирован<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [EM] — Трансляция закрытого ключа

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование закрытого ключа RSA или ECC, зашифрованного под «старым» LMK, и последующее зашифрование под «новым» LMK.
«Старый» или «новый» LMK должен быть предварительно загружен в хранилище смены ключей.

**Примечания:** Подробнее о поддержке алгоритмов RSA и ECC см. в «КриптоПро HSM. Руководство программиста».

При трансляции закрытого ключа RSA, зашифрованного ранее под Variant LMK, в зашифрованный под Key Block LMK он пересоздается в формате Проприетарного Key Block со следующими атрибутами:

| **Поле** | **Значение** |
|---|---|
| Использование ключа | '03', '04', '05' или '06' |
| Алгоритм | 'R' |
| Режим использования | Выводится из типа исходного ключа |
| Экспортируемость | 'N' (если явно не указано значение 'S') |
| Длина ключа | Определяется длиной исходного ключа |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'EM'. |
| Длина закрытого ключа | 4 N | Длина (в байтах) следующего поля. |
| | 4 H | Значение 'FFFF'. |
| Закрытый ключ | | Транслируемый закрытый ключ. |
| | n B | Закрытый ключ, зашифрованный под LMK 34-35. |
| | 'S' + n B<br>или<br>'S' + n A | Закрытый ключ должен соответствовать следующему формату:<br>Использование ключа: '03', '04', '05', '06' — Алгоритм: 'R' — Режим использования: 'S', 'D', 'N'<br>Использование ключа: '03' — Алгоритм: 'E' — Режим использования: 'S', 'X', 'N' |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующие поля присутствуют только в случае трансляции закрытого ключа, зашифрованного под Variant LMK, в зашифрованный под Key Block LMK: | | |
| Разделитель | 1 A | Значение '#'. Опционально; должен присутствовать в случае трансляции закрытого ключа, зашифрованного под Variant LMK, в зашифрованный под Key Block LMK. Если присутствует, следующие поля обязательны. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block. Допустимые значение: '00' .. '99'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже. Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Разделитель | 1 A | Значение '&'. Опционально; если присутствует, следующее поле обязательно. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block (байт 11) транслированного закрытого ключа.<br>Допустимые значения: 'N' или 'S'. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'EN'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'47': Алгоритм не лицензирован<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Длина закрытого ключа | 4 N | Длина (в байтах) следующего поля. |
| | 4 H | Значение 'FFFF'. |

<table>
<tr><td>Закрытый ключ</td><td></td><td>Транслированный закрытый ключ.</td></tr>
<tr><td></td><td>n B</td><td>Закрытый ключ, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B<br>или<br>'S' + n A</td><td>Закрытый ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03', '04', '05', '06'</td><td>'R'</td><td>'S', 'D', 'N'</td></tr>
<tr><td>'03'</td><td>'E'</td><td>'S', 'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Символ конца ответа</td><td>1 C</td><td>Значение 0x19. Присутствует, только если присутствует в команде.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Присутствует, только если присутствует в команде. Максимальная длина — 32 символа.</td></tr>
</table>

## [EO] — Импорт открытого ключа

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Variant LMK | Авторизация: **Требуется**<br>Активности: **import.rsa.host** |
| Key Block LMK | Авторизация: **Требуется**<br>Активности: **import.02.host** |

**Описание функции:** Импорт открытого ключа RSA или ECC с помощью вычисления MAC для ключа. В случае использование Key Block LMK импортированный открытый ключ будет в формате Key Block.

**Примечания:** Функция может использоваться, например, для защиты открытого ключа ЦС.
Подробнее о поддержке алгоритмов RSA и ECC см. в «КриптоПро HSM. Руководство программиста».

В случае импорта открытого ключа RSA или ECC с использованием Key Block LMK, импортированный открытый ключ RSA или ECC возвращается в формате Key Block со следующими атрибутами:

| **Поле** | **Значение** |
|---|---|
| Использование ключа | '02' |
| Алгоритм | 'R', 'E' |
| Режим использования | Указывается в команде после *Разделителя* '#' |
| Экспортируемость | Указывается в команде после *Разделителя* '#' |
| Длина ключа | Определяется входным ключом |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'EO'. |
| Метод кодирования открытого ключа | 2 N | '01': открытый ключ RSA в формате DER, ASN.1 (беззнаковое целое)<br>'02': открытый ключ RSA в формате DER, ASN.1 (целое в формате дополнительного кода)<br>'03': несжатый открытый ключ ECC в формате X9.62 DER, ASN.1 |
| Открытый ключ | n B | Открытый ключ в формате, определенном выше в поле *Метод кодирования открытого ключа*. |
| Данные для аутентификации | n B | Опционально. Дополнительные данные для вычисления MAC (не должны содержать символы ';' и '∼'). |
| Разделитель | 1 A | Значение '∼'. Опционально; присутствует, если присутствует разделитель '%' или '#' ниже. Признак конца полей *Открытый ключ* и/или *Данные для аутентификации*. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующие поля присутствуют только в случае использования Key Block LMK: | | |
| Разделитель | 1 A | Значение '#'. Опционально; должен присутствовать, если используется Key Block LMK. Если присутствует, следующие поля обязательны. |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block.<br>Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице режимов использования ключей в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Любое допустимое значение. Допустимые значения см. в таблице экспортируемости ключа в «КриптоПро HSM. Руководство программиста». |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'EP'. |

<table>
<tr><td>Код ошибки</td><td>2 H</td><td>'00': Без ошибок<br>'03': Недопустимый метод кодирования открытого ключа<br>'04': Открытый ключ не соответствует правилам кодирования<br>'47': Алгоритм не лицензирован<br>'68': Команда недоступна<br>или другой стандартный код ошибки.</td></tr>
<tr><td>MAC</td><td>4 B</td><td>MAC, вычисленный для открытого ключа и данных аутентификации с использованием LMK 36-37.</td></tr>
<tr><td>Открытый ключ</td><td></td><td>Импортированный открытый ключ.</td></tr>
<tr><td></td><td>n B</td><td>Открытый ключ, DER в формате ASN.1 (последовательность модуля и экспоненты).</td></tr>
<tr><td></td><td>'S' + n B<br>или<br>'S' + n A</td><td>Открытый ключ хранится в формате Key Block (без шифрования), включая значение MAC.<br>Импортированный открытый ключ RSA должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'02'</td><td>'R'</td><td>'V', 'E', 'N'</td></tr>
</table>
Импортированный открытый ключ ECC должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'02'</td><td>'E'</td><td>'V', 'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Символ конца ответа</td><td>1 C</td><td>Значение 0x19. Присутствует, только если присутствует в команде.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Присутствует, только если присутствует в команде. Максимальная длина — 32 символа.</td></tr>
</table>

## [EQ] — Проверка открытого ключа

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка открытого ключа RSA.

**Примечания:** Команда не поддерживает открытые ключи ECC.
Подробнее о поддержке алгоритма RSA см. в «КриптоПро HSM. Руководство программиста».

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'EQ'. |
| Следующие 4 поля присутствуют только в случае Variant LMK: | | |
| MAC | 4 B | MAC, вычисленный для открытого ключа и данных аутентификации с использованием LMK 36-37. |
| Открытый ключ | n B | Открытый ключ; DER в формате ASN.1 (последовательность модуля и экспоненты). |
| Данные для аутентификации | n B | Опционально. Дополнительные данные для вычисления MAC (не должны содержать символы ';' и '∼'). |
| Разделитель | 1 A | Значение '∼'. Опционально; должен присутствовать, только если присутствует разделитель '%' ниже. Признак конца предыдущих полей. |
| Следующее поле присутствует только в случае Key Block LMK: | | |
| Открытый ключ | 'S' + n B | Открытый ключ должен соответствовать следующему формату:<br>Использование ключа: '02'; Алгоритм: 'R'; Режим использования: 'E', 'N', 'V' |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'ER'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'04': Открытый ключ не соответствует правилам кодирования<br>'47': Алгоритм не лицензирован<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [ES] — Проверка сертификата и импорт открытого ключа

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка сертификата и импорт открытого ключа RSA, содержащегося в сертификате.

**Примечания:** Команда не поддерживает использование закрытых/открытых ключей ECC.
Команда позволяет (опционально) проверить соответствие открытого ключа в сертификате закрытому ключу, зашифрованному под LMK.
Подробнее о поддержке алгоритма RSA см. в «КриптоПро HSM. Руководство программиста».

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce minimum key strength of 1024-bits for RSA signature verification` (влияет на параметры: *Открытый ключ*) | `Yes [Y]` | Длина открытого ключа RSA должна быть не менее 1024 бит. |
| | `No [N]` | Ограничения на длину ключа не накладываются. |
| `Enforce minimum key strength of 2048-bits for RSA` (влияет на параметры: *Открытый ключ, Закрытый ключ*) | `Yes [Y]` | Длины открытого и закрытого ключей RSA должны быть не менее 2048 бит. |
| | `No [N]` | Ограничения на длину ключа не накладываются. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'ES'.</td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае Variant LMK:</td></tr>
<tr><td>MAC</td><td>4 B</td><td>MAC, вычисленный для открытого ключа и данных аутентификации с использованием LMK 36-37.</td></tr>
<tr><td>Открытый ключ</td><td>n B</td><td>Открытый ключ, используемый для проверки сертификата. DER в формате ASN.1 (последовательность модуля и экспоненты).</td></tr>
<tr><td>Данные для аутентификации</td><td>n B</td><td>Опционально. Дополнительные данные для вычисления MAC (не должны содержать символы ';' и '~').</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Признак конца поля Данные для аутентификации.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае Key Block LMK:</td></tr>
<tr><td>Открытый ключ</td><td>'S' + n B</td><td>Открытый ключ для проверки сертификата должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'02'</td><td>'R'</td><td>'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Длина сертификата</td><td>4 N</td><td>Длина сертификата (в байтах).</td></tr>
<tr><td>Смещение данных для хэширования</td><td>4 N</td><td>Смещение до первого байта данных сертификата, которые используются при вычислении хэш-значения.</td></tr>
<tr><td>Длина данных для хэширования</td><td>4 N</td><td>Длина (в байтах) данных сертификата, которые используются при вычислении хэш-значения.</td></tr>
<tr><td>Смещение подписи</td><td>4 N</td><td>Смещение до первого байта подписи, содержащейся в данных сертификата.</td></tr>
<tr><td>Длина подписи</td><td>4 N</td><td>Длина (в байтах) подписи, содержащейся в данных сертификата.</td></tr>
<tr><td>Сертификат</td><td>n B</td><td>Данные сертификата для проверки.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Признак конца поля Сертификат.</td></tr>
<tr><td>Идентификатор алгоритма хэширования</td><td>2 N</td><td>Алгоритм хэширования данных сертификата:<br>'01': SHA-1<br>'02': MD5<br>'03': ISO 10118-2<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512</td></tr>
<tr><td>Идентификатор алгоритма подписи</td><td>2 N</td><td>Алгоритм подписи данных сертификата:<br>'01': RSA</td></tr>
<tr><td>Идентификатор режима дополнения подписи</td><td>2 N</td><td>'01': PKCS#1 v2.2 method EMSA-PKCS1-v1_5</td></tr>
<tr><td>Метод кодирования открытого ключа</td><td>2 N</td><td>Метод кодирования открытого ключа, содержащегося в сертификате.<br>'01': DER, ASN.1 (беззнаковое целое)<br>'02': DER, ASN.1 (целое в формате дополнительного кода)</td></tr>
<tr><td>Смещение открытого ключа</td><td>4 N</td><td>Смещение до первого байта открытого ключа, содержащегося в сертификате.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае использования Variant LMK:</td></tr>
<tr><td>Данные для аутентификации</td><td>n B</td><td>Опционально. Дополнительные данные для вычисления MAC (не должны содержать символ ';').</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Признак конца поля Данные для аутентификации.</td></tr>
<tr><td rowspan="3">Длина закрытого ключа</td><td></td><td>Опционально; присутствует, только если присутствует поле Закрытый ключ.</td></tr>
<tr><td>4 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td>4 H</td><td>Значение 'FFFF'.</td></tr>
</table>

<table>
<tr><td>Закрытый ключ</td><td></td><td>Опционально. Закрытый ключ, который проверяется на соответствие открытому ключу, содержащемуся в сертификате.</td></tr>
<tr><td></td><td>n B</td><td>Закрытый ключ, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B</td><td>Закрытый ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03'</td><td>'R'</td><td>'S', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае использования Key Block LMK:</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '#'. Опционально; должен присутствовать, если используется Key Block LMK. Если присутствует, следующие поля обязательны.</td></tr>
<tr><td>Режим использования</td><td>1 A</td><td>Поле Режим использования, включаемое в заголовок Key Block.<br>Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице режимов использования ключей в «КриптоПро HSM. Руководство программиста».<br>Примечание: указанное значение должно соответствовать значению Режима использования закрытого ключа (если он присутствует в команде).</td></tr>
<tr><td>Номер версии ключа</td><td>2 N</td><td>Поле Номер версии ключа, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'.</td></tr>
<tr><td>Экспортируемость</td><td>1 A</td><td>Поле Экспортируемость, включаемое в заголовок Key Block.<br>Любое допустимое значение. Допустимые значения см. в таблице экспортируемости ключа в «КриптоПро HSM. Руководство программиста».</td></tr>
<tr><td>Количество опциональных блоков</td><td>2 N</td><td>Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'.</td></tr>
<tr><td colspan="3">Следующие 3 поля определяются для каждого опционального блока:<br>Примечание: Если Количество опциональных блоков = '00', следующие 3 поля не присутствуют.</td></tr>
<tr><td>Идентификатор блока</td><td>2 A</td><td>Любое допустимое значение, кроме 'PB'.</td></tr>
<tr><td>Длина блока</td><td>2 H</td><td>Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует.</td></tr>
<tr><td>Данные блока</td><td>n A</td><td>Данные блока.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'ET'. |

| | | |
|---|---|---|
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'02': Ошибка проверки сертификата<br>'03': Недопустимый метод кодирования открытого ключа<br>'04': Открытый ключ не соответствует правилам кодирования<br>'05': Недопустимый идентификатор алгоритма шифрования<br>'06': Недопустимый идентификатор алгоритма подписи<br>'07': Недопустимый идентификатор режима дополнения<br>'47': Алгоритм не лицензирован<br>'68': Команда недоступна<br>'76': Длина подписи не равна длине модуля открытого ключа<br>'77': Ошибка расшифрованных данных<br>'78': Ошибка длины закрытого ключа<br>'79': Ошибка идентификатора объекта алгоритма хэширования<br>'80': Ошибка длины сертификата<br>'81': Недопустимый заголовок сертификата<br>или другой стандартный код ошибки. |
| MAC | 4 B | MAC, вычисленный для открытого ключа и данных аутентификации с использованием LMK 36-37. |
| Открытый ключ | | Импортированный открытый ключ. |
| | n B | Открытый ключ, DER в формате ASN.1 (последовательность модуля и экспоненты). |
| | 'S' + n B | Открытый ключ хранится в формате Key Block (без шифрования), включая значение MAC. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [EU] — Трансляция открытого ключа

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Трансляция открытого ключа RSA или ECC, защищенного с использованием «старого» LMK, в защищенный с использованием «нового» LMK.
«Старый» или «новый» LMK должен быть предварительно загружен в хранилище смены ключей.

**Примечания:** Подробнее о поддержке алгоритмов RSA и ECC см. в «КриптоПро HSM. Руководство программиста».

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'EU'.</td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае «старого» Variant LMK:</td></tr>
<tr><td>MAC</td><td>4 B</td><td>MAC, вычисленный для открытого ключа и данных аутентификации с использованием «старого» LMK 36-37.</td></tr>
<tr><td>Открытый ключ</td><td>n B</td><td>Открытый ключ; DER в формате ASN.1 (последовательность модуля и экспоненты).</td></tr>
<tr><td>Данные для аутентификации</td><td>n B</td><td>Опционально. Дополнительные данные для вычисления MAC (не должны содержать символы ';' и '∼').</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '∼'. Опционально; присутствует, если присутствует разделитель '%' или '#' ниже. Признак конца полей Открытый ключ и/или Данные для аутентификации.</td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае «старого» Key Block LMK:</td></tr>
<tr><td>Открытый ключ</td><td>'S' + n B<br>или<br>'S' + n A</td><td>Открытый ключ должен быть в формате Key Block (с использованием «старого» LMK) и соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'02'</td><td>'R'</td><td>'V', 'E', 'N'</td></tr>
<tr><td>'02'</td><td>'E'</td><td>'V', 'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае трансляции открытого ключа, защищенного с использованием «старого» Variant LMK, в защищенный с использованием «нового» Key Block LMK:</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '#'. Опционально; должен присутствовать, если используются «старый» Variant LMK и «новый» Key Block LMK. Если присутствует, следующие поля обязательны.</td></tr>
<tr><td>Режим использования</td><td>1 A</td><td>Поле Режим использования, включаемое в заголовок Key Block.<br>Любое допустимое значение для указанных Использования ключа и Алгоритма. Допустимые значения см. в таблице режимов использования ключей в «КриптоПро HSM. Руководство программиста».</td></tr>
<tr><td>Номер версии ключа</td><td>2 N</td><td>Поле Номер версии ключа, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'.</td></tr>
</table>

| | | |
|---|---|---|
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Любое допустимое значение. Допустимые значения см. в таблице экспортируемости ключа в «КриптоПро HSM. Руководство программиста». |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'EV'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'04': Открытый ключ не соответствует правилам кодирования<br>'47': Алгоритм не лицензирован<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| MAC | 4 B | MAC, вычисленный для открытого ключа и данных аутентификации с использованием «нового» LMK 36-37. |
| Открытый ключ | 'S' + n B<br>или<br>'S' + n A | Транслированный открытый ключ хранится в формате Key Block (без шифрования), включая значение MAC.<br>Открытый ключ должен соответствовать следующему формату:<br>Использование ключа: '02'<br>Алгоритм: 'R'<br>Режим использования: 'V', 'E', 'N'<br>Использование ключа: '02'<br>Алгоритм: 'E'<br>Режим использования: 'V', 'X', 'N' |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [GI] — Импорт ключа или данных, зашифрованных под открытым ключом RSA

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Требуется** | |
| Активности: **command.gi.host** | |

**Описание функции:** Расшифрование импортируемого ключа DES, AES или HMAC, зашифрованного под открытым ключом RSA, и последующее зашифрование под LMK.

Команда также может использоваться для расшифрования данных, используется ключевая пара RSA, созданная ранее с помощью команды 'EI' с Индикатором типа ключа = '4'.

**Примечания:** Типы ключей и ограничения на импорт ключей описаны в таблице типов ключей в «КриптоПро HSM. Руководство программиста».

Подробнее о поддержке алгоритма RSA см. в «КриптоПро HSM. Руководство программиста».

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Restrict Key Check Value to 6 hex chars` (влияет на параметры: *KCV*) | `Yes [Y]` | Только первые 6 символов KCV содержат проверочное значение ключа, остальные крайние правые символы устанавливаются в '0'. |
| | `No [N]` | Дополнительные ограничения на KCV не накладываются. |
| `Enable import of a ZMK` (влияет на параметры: *Тип ключа*) | `Yes [Y]` | Доступен импорт ZMK. |
| | `No [N]` | Импорт ZMK невозможен. |
| `Enforce minimum key strength of 1024-bits for RSA signature verification` (влияет на параметры: *Открытый ключ*) | `Yes [Y]` | Длина открытого ключа RSA должна быть не менее 1024 бит. |
| | `No [N]` | Ограничения на длину ключа не накладываются. |
| `Enforce minimum key strength of 2048-bits for RSA` (влияет на параметры: *Открытый ключ, Закрытый ключ*) | `Yes [Y]` | Длины открытого и закрытого ключей RSA должны быть не менее 2048 бит. |
| | `No [N]` | Ограничения на длину ключа не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'GI'. |
| Идентификатор алгоритма шифрования | 2 A | Идентификатор алгоритма расшифрования ключа.<br>'01': RSA |
| Идентификатор режима дополнения | 2 N | '01': PKCS#1 v2.2 method EME-PKCS1-v1_5<br>'02': PKCS#1 v2.2 method EME-OAEP |
| Функция генерации маски (MGF) | 2 N | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP).<br>'01': MGF1 (как определено в PKCS#1 v2.2) |
| Хэш-функция в MGF | 2 N | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP).<br>'01': SHA-1<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| Длина OAEP Label | 2 N | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP).<br>Если используется схема дополнения OAEP без значения Label, поле должно иметь значение '00', а следующее поле должно отсутствовать. |
| OAEP Label | n B | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP). |
| Разделитель OAEP Label | 1 A | Значение ';'. Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP). |
| Тип ключа | 4 N | Параметры ключа LMK, используемого для шифрования импортированного ключа.<br>Формат 'PPVV', где PP обозначает ключевую пару LMK, VV — номер варианта LMK.<br>В случае ключей HMAC — значение '3401'.<br>В случае расшифрования данных (например, TLS/SSL premaster secret) с использованием ключа RSA с Индикатором типа ключа = '4' — значение '3400'. |
| | 4 H | Значение 'FFFF'. |
| Следующие поля присутствуют, только если для импортируемого ключа указывается значение подписи: | | |
| Индикатор подписи | 1 A | Значение '='. Присутствует, только если присутствуют поля подписи ниже. |
| Идентификатор алгоритма хэширования | 2 N | '01': SHA-1<br>'02': MD5<br>'03': ISO 10118-2<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| Идентификатор алгоритма подписи | 2 N | '01': RSA |
| Идентификатор режима дополнения подписи | 2 N | '01': PKCS#1 v2.2 method EMSA-PKCS1-v1_5 |
| Смещение зашифрованного ключа | 4 N | Смещение (в байтах) до первого байта зашифрованного импортируемого ключа в поле *Блок данных*. |
| Длина зашифрованного ключа | 4 N | Длина (в байтах) зашифрованного импортируемого ключа в поле *Блок данных*. |
| Длина подписи | 4 N | Длина (в байтах) следующего поля. |

<table>
<tr><td>Подпись</td><td>n B</td><td>Подпись, подтверждающая подлинность зашифрованного импортируемого ключа.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Признак конца поля Подпись.</td></tr>
<tr><td>MAC</td><td>4 B</td><td>MAC, вычисленный для открытого ключа и данных аутентификации с использованием LMK 36-37.</td></tr>
<tr><td>Открытый ключ</td><td></td><td>Открытый ключ, используемый для проверки подписи</td></tr>
<tr><td></td><td>n B</td><td>Открытый ключ (DER) в формате ASN.1 (последовательность модуля и экспоненты)</td></tr>
<tr><td></td><td>'S' + n B</td><td>Открытый ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'02'</td><td>'R'</td><td>'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Данные для аутентификации</td><td>n B</td><td>Опционально. Дополнительные данные для вычисления MAC (не должны содержать символы ';' и '~').</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Признак конца поля Данные для аутентификации.</td></tr>
<tr><td>Длина блока данных</td><td>4 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td>Блок данных</td><td>n B</td><td>Блок данных может содержать:<br>• зашифрованный импортируемый ключ<br>• данные (например, TLS/SSL premaster secret), если используется ключ RSA с Индикатором типа ключа = '4'<br>Примечание: формат зашифрованного ключа описан в «КриптоПро HSM. Руководство программиста».</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Признак конца поля Блок данных.</td></tr>
<tr><td>Флаг закрытого ключа</td><td>2 N</td><td>Указывает расположение закрытого ключа, используемого для расшифрования импортируемого ключа.<br>'00' .. '20' : индекс ключа в хранилище<br>'99' : используется ключ, переданный в команде</td></tr>
<tr><td>Длина закрытого ключа</td><td></td><td>Опционально; присутствует только в случае Флага закрытого ключа = '99'.</td></tr>
<tr><td></td><td>4 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
<tr><td>Закрытый ключ</td><td></td><td>Опционально; присутствует только в случае Флага закрытого ключа = '99'.<br>Закрытый ключ, используемый для расшифрования импортируемого ключа.</td></tr>
<tr><td></td><td>n B</td><td>Закрытый ключ, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B</td><td>Закрытый ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03'</td><td>'R'</td><td>'D', 'N'</td></tr>
</table></td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае импорта ключа DES/AES:</td></tr>
<tr><td>1) Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует, только если присутствуют следующие поля.</td></tr>
<tr><td>2) Тип импортируемого ключа</td><td>1 A</td><td>'0': 3DES<br>'1': AES</td></tr>
<tr><td>3) Ключевая схема (LMK)</td><td>1 A</td><td>Схема шифрования импортируемого ключа под LMK.</td></tr>
<tr><td>4) Тип KCV</td><td>1 A</td><td>Опционально. Метод вычисления проверочного значения ключа.<br>'0': 16-значный KCV<br>'1': 6-значный KCV</td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае импорта ключа HMAC:</td></tr>
<tr><td>1) Разделитель</td><td>1 A</td><td>Присутствует, только если присутствуют следующие поля.</td></tr>
<tr><td></td><td></td><td>Значение '#' или '|' (ASCII 0x7C)</td></tr>
<tr><td></td><td></td><td>Значение '|' (ASCII 0x7C)</td></tr>
</table>

| | | |
|---|---|---|
| 2) Идентификатор алгоритма хэширования | 2 N | '01': SHA-1<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| 3) Использование ключа HMAC | 2 N | '01': Генерация HMAC<br>'02': Проверка HMAC<br>'03': Генерация и проверка HMAC |
| 4) Формат ключа HMAC | 2 N | Формат ключа HMAC, зашифрованного под LMK.<br>'00': HMAC Key<br>'04': HMAC Key Block |
| Разделитель | 1 A | Значение '='. Присутствует, только если присутствует следующее поле. |
| Тип Key Data Block | 2 N | Присутствует, только если присутствует разделитель выше. Если поле отсутствует, используется тип Key Data Block по умолчанию '01'.<br>'01': Стандартный Key Data Block<br>'02': Шаблон Key Data Block (формат шаблона определяется ниже)<br>'03': Неформатированный Key Data Block<br>'04': Key Data Block в формате ASN.1<br>Key Data Block типа '01', '02' или '03' может использоваться для импорта DES/AES ключей.<br>Key Data Block типа '02', '03' или '04' может использоваться для импорта HMAC ключей. |
| Следующие поля присутствуют только в случае *Tuna Key Data Block* = '02': | | |
| Длина шаблона Key Data Block | 4 N | Длина следующего поля. |
| Шаблон Key Data Block | n H | Key Data Block в кодировке DER в формате ASN.1. Данные ключа заполнены нулями. |
| Разделитель | 1 A | Значение ';'. |
| Длина ключа | | Длина ключа в Key Data Block. |
| | 2 A | Для ключей DES/AES размер поля 2 A. |
| | 4 N | Для ключей HMAC размер поля 4 N. |
| Смещение ключа | 4 N | Смещение до первого байта значения ключа в Key Data Block. |
| Длина проверочного значения | 2 N | Присутствует только в случае импорта ключей DES/AES.<br>Длина (в байтах) проверочного значения.<br>Допустимые значения: '00' .. '08'. Если проверочное значение не используется, поле имеет значение '00'.<br>Если проверочное значение указано, HSM выполнит проверку с использованием извлеченного ключа.<br>В случае *Tuna Key Data Block* = '02' проверочное значение должно располагаться в Key Data Block в соответствии со значением поля *Смещение проверочного значения* ниже. |
| Смещение проверочного значения | 4 N | Присутствует только в случае импорта ключей DES/AES.<br>Смещение до первого байта проверочного значения в Key Data Block. Если *Длина проверочного значения* = '00', поле игнорируется. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующие поля присутствуют только в случае импорта ключа DES/AES и использования Key Block LMK: | | |
| Разделитель | 1 A | Значение '#'. Опционально; присутствует только в случае импорта ключа DES/AES и возврате его в формате Key Block. Если присутствует, следующие поля обязательны. |

| | | |
|---|---|---|
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block.<br>Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице использования ключей в «КриптоПро HSM. Руководство программиста». |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block.<br>Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице режимов использования ключей в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N' или 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Следующие поля присутствуют только в случае импорта ключа HMAC и использования Key Block LMK: | | |
| Разделитель | 1 A | Значение '#'. Опционально; присутствует только в случае импорта ключа HMAC и возврате его в формате Key Block. Если присутствует, следующие поля обязательны. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N' или 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'GJ'. |

| | | |
|---|---|---|
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'02': Ошибка проверки подписи<br>'03': Недопустимый тип закрытого ключа<br>'04': Недопустимый флаг закрытого ключа<br>'05': Недопустимый тип ключа<br>'06': Недопустимый идентификатор алгоритма шифрования<br>'07': Недопустимый идентификатор режима дополнения<br>'50': Открытый ключ не соответствует правилам кодирования<br>'51': Недопустимый идентификатор алгоритма хэширования подписи<br>'52': Недопустимый идентификатор подписи<br>'53': Недопустимый идентификатор режима дополнения подписи<br>'54': Недопустимое значение смещения зашифрованного ключа<br>'55': Недопустимое значение длины зашифрованного ключа<br>'56': Несоответствие подписи/длины подписи<br>'57': Недопустимый тип KCV<br>'58': Недопустимый идентификатор алгоритма хэширования HMAC<br>'59': Недопустимое значение использования ключа HMAC<br>'60': Недопустимое значение формата ключа HMAC<br>'68': Команда недоступна<br>'76': Длина подписи не равна длине модуля открытого ключа<br>'77': Ошибка расшифрованных данных<br>'78': Ошибка длины закрытого ключа<br>'79': Ошибка идентификатора объекта алгоритма хэширования<br>'80': Ошибка длины блока данных<br>'81': Недопустимый тип Key Data Block<br>'83': Ошибка формата Key Block<br>'85': Недопустимое значение OAEP MGF<br>'86': Недопустимая функция хэширования OAEP MGF<br>'87': Ошибка OAEP Label<br>или другой стандартный код ошибки. |
| Следующие 3 поля присутствуют только в случае импорта ключа DES/AES: | | |
| 1) IV | 16 H | Опционально; присутствует только в случае *Tuna Key Data Block* = '01'.<br>Вектор инициализации для ключа DES/AES.<br>*Примечание:* вектор инициализации длиннее 16 H будет усечен. |
| 2) Ключ | | Импортированный ключ DES/AES, зашифрованный под LMK. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | Ключ, зашифрованный под соответствующим LMK, определяемым значением поля *Тип ключа*. |
| | 'S' + n A | Ключ, зашифрованный под LMK. |
| 3) KCV | 16/6 H | Проверочное значение для импортированного ключа.<br>Размер поля определяется значением поля *Tun KCV*. Если поле *Tun KCV* отсутствует, используется размер поля по умолчанию 16 H. |
| Следующие 2 поля присутствуют только в случае импорта ключа HMAC: | | |
| 1) Длина ключа HMAC | 4 N | Длина (в байтах) следующего поля. |
| | 4 H | Значение 'FFFF'. |
| 2) Ключ | | Импортированный ключ HMAC, зашифрованный под LMK. |
| | n B | Ключ HMAC, зашифрованный под LMK 34-35/1. |
| | n A | Ключ HMAC, зашифрованный под LMK. |
| Следующие 2 поля присутствуют только в случае импорта данных (например, TLS/SSL premaster secret) с использование ключа RSA с Индикатором типа ключа = '4': | | |
| Длина данных TLS | 4 N | Длина следующего поля. |
| Данные TLS | n B | Данные или незашифрованный TLS/SSL premaster secret. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |

| | | |
|---|---|---|
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [GK] — Экспорт ключа, зашифрованного под открытым ключом RSA

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Variant LMK | Авторизация: **Определяется по ТТК (Э)**<br>Активности: **export.{key}.host** |
| Key Block LMK | Авторизация: **Не требуется** |

**Описание функции:** Расшифрование ключа DES, AES или HMAC, зашифрованного под LMK, и последующее зашифрование под открытым ключом RSA.

**Авторизация:** Команда проверяет флаг 'Э' (экспорт) для заданного типа ключа в таблице типов ключей (ТТК, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **export.{key}.host** должна быть авторизована, где 'key' — код типа экспортируемого ключа.

**Примечания:** Типы ключей и ограничения на экспорт ключей описаны в таблице типов ключей в «КриптоПро HSM. Руководство программиста».
Подробнее о поддержке алгоритма RSA см. в «КриптоПро HSM. Руководство программиста».

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Restrict Key Check Value to 6 hex chars`<br>(влияет на параметры: *KCV*) | `Yes [Y]` | Только первые 6 символов KCV содержат проверочное значение ключа, остальные крайние правые символы игнорируются. |
| | `No [N]` | Дополнительные ограничения на KCV не накладываются. |
| `Enable export of a ZMK`<br>(влияет на параметры: *Тип ключа*) | `Yes [Y]` | Доступен экспорт ZMK. |
| | `No [N]` | Экспорт ZMK невозможен. |
| `Enforce minimum key strength of 2048-bits for RSA`<br>(влияет на параметры: *Открытый ключ, Закрытый ключ*) | `Yes [Y]` | Длины открытого и закрытого ключей RSA должны быть не менее 2048 бит. |
| | `No [N]` | Ограничения на длину ключа не накладываются. |
| `Enforce NIST recommendations when encrypting AES keys using RSA`<br>(влияет на параметры: *Идентификатор режима дополнения*) | `Yes [Y]` | Сила ключа (key strength) RSA должна быть не меньше силы экспортируемого ключа AES (подробнее см. в NIST SP800-57). Поле *Идентификатор режима дополнения* должно иметь значение '02' (PKCS#1 v2.2 method EME-OAEP). |
| | `No [N]` | Ограничения NIST на экспорт ключей не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'GK'. |
| Идентификатор алгоритма шифрования | 2 A | Идентификатор алгоритма зашифрования ключа.<br>'01': RSA |
| Идентификатор режима дополнения | 2 N | '01': PKCS#1 v2.2 method EME-PKCS1-v1_5<br>'02': PKCS#1 v2.2 method EME-OAEP |
| Функция генерации маски (MGF) | 2 N | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP).<br>'01': MGF1 (как определено в PKCS#1 v2.2) |
| Хэш-функция в MGF | 2 N | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP).<br>'01': SHA-1<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| Длина OAEP Label | 2 N | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP).<br>Если используется схема дополнения OAEP без значения Label, поле должно иметь значение '00', а следующее поле должно отсутствовать. |
| OAEP Label | n B | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP). |
| Разделитель OAEP Label | 1 A | Значение ';'. Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP). |
| Тип ключа | 4 N | Параметры ключа LMK, используемого для шифрования экспортируемого ключа.<br>Формат 'PPVV', где PP обозначает ключевую пару LMK, VV — номер варианта LMK.<br>В случае ключей HMAC — значение '3401'. |
| | 4 H | Значение 'FFFF'. |
| Следующие поля присутствуют, только если для экспортируемого ключа указывается значение подписи: | | |
| Индикатор подписи | 1 A | Значение '='. Присутствует, только если присутствуют поля подписи ниже. |
| Идентификатор алгоритма хэширования | 2 N | '01': SHA-1<br>'02': MD5<br>'03': ISO 10118-2<br>'04': Без хэширования<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| Идентификатор алгоритма подписи | 2 N | '01': RSA |
| Идентификатор режима дополнения подписи | 2 N | '01': PKCS#1 v2.2 method EMSA-PKCS1-v1_5 |
| Длина блока данных header | 4 N | Длина (в байтах) следующего поля.<br>Если *Блок данных header* не указывается — значение '0000'. |
| Блок данных header | n B | Блок данных, добавляемых перед зашифрованным ключом перед вычислением подписи. |
| Разделитель | 1 A | Значение ';'. |
| Длина блока данных footer | 4 N | Длина (в байтах) следующего поля.<br>Если *Блок данных footer* не указывается — значение '0000'. |

<table>
<tr><td>Блок данных footer</td><td>n B</td><td>Блок данных, добавляемых после зашифрованного ключа перед вычислением подписи.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td>Флаг закрытого ключа</td><td>2 N</td><td>Указывает расположение закрытого ключа, используемого для вычисления подписи.<br>'00' .. '20' : индекс ключа в хранилище<br>'99' : используется ключ, переданный в команде</td></tr>
<tr><td>Длина закрытого ключа</td><td></td><td>Опционально; присутствует только в случае Флага закрытого ключа = '99'.</td></tr>
<tr><td></td><td>4 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
<tr><td>Закрытый ключ</td><td></td><td>Опционально; присутствует только в случае Флага закрытого ключа = '99'.<br>Закрытый ключ для вычисления подписи.</td></tr>
<tr><td></td><td>n B</td><td>Закрытый ключ, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B</td><td>Закрытый ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03'</td><td>'R'</td><td>'S', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Опционально; присутствует только в случае Флага закрытого ключа = '99'.</td></tr>
<tr><td colspan="3">Следующие 3 поля присутствуют только в случае экспорта ключа DES/AES:</td></tr>
<tr><td>Флаг ключа DES</td><td>1 N</td><td>Длина ключа DES:<br>'1': 2DES<br>'2': 3DES</td></tr>
<tr><td></td><td>1 A</td><td>Значение 'F'.</td></tr>
<tr><td>Ключ DES/AES (под LMK)</td><td></td><td>Экспортируемый ключ DES/AES, зашифрованный под LMK.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Ключ, зашифрованный под соответствующим LMK, определяемым значением поля Тип ключа.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ, зашифрованный под LMK.</td></tr>
<tr><td>KCV</td><td></td><td>Проверочное значение ключа DES/AES.</td></tr>
<tr><td></td><td>16 H</td><td>Для ключей DES размер поля 16 H.</td></tr>
<tr><td></td><td>6 H</td><td>Для ключей AES размер поля 6 H.</td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае экспорта ключа HMAC:</td></tr>
<tr><td>Формат ключа HMAC</td><td>2 N</td><td>Формат ключа HMAC, зашифрованного под LMK.</td></tr>
<tr><td></td><td></td><td>'00': HMAC Key</td></tr>
<tr><td></td><td></td><td>'04': HMAC Key Block</td></tr>
<tr><td>Длина ключа HMAC</td><td>4 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
<tr><td>Ключ</td><td></td><td>Экспортируемый ключ HMAC, зашифрованный под LMK.</td></tr>
<tr><td></td><td>n B</td><td>Ключ HMAC, зашифрованный под LMK 34-35/1.</td></tr>
<tr><td></td><td>n A</td><td>Ключ HMAC, зашифрованный под LMK.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае Variant LMK:</td></tr>
<tr><td>MAC</td><td>4 B</td><td>MAC, вычисленный для открытого ключа и данных аутентификации с использованием LMK 36-37/0.</td></tr>
<tr><td>Открытый ключ</td><td>n B</td><td>Открытый ключ, используемый для зашифрования экспортируемого ключа. DER в формате ASN.1 (последовательность модуля и экспоненты).</td></tr>
<tr><td>Данные для аутентификации</td><td>n B</td><td>Опционально. Дополнительные данные для вычисления MAC (не должны содержать символы ';' и '~').</td></tr>
</table>

<table>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '~'. Опционально; должен присутствовать, если присутствует Разделитель '%' ниже.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае Key Block LMK:</td></tr>
<tr><td>Открытый ключ</td><td>'S' + n B</td><td>Открытый ключ, используемый для зашифрования экспортируемого ключа; должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'02'</td><td>'R'</td><td>'E', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует, только если присутствует следующее поле.</td></tr>
<tr><td>Тип Key Data Block</td><td>2 N</td><td>Присутствует, только если присутствует разделитель выше. Если поле отсутствует, используется тип Key Data Block по умолчанию '01'.<br>'01': Стандартный Key Data Block<br>'02': Шаблон Key Data Block (формат шаблона определяется ниже)<br>'03': Неформатированный Key Data Block<br>'04': Key Data Block в формате ASN.1<br>Key Data Block типа '01', '02' или '03' может использоваться для импорта DES/AES ключей.<br>Key Data Block типа '02', '03' или '04' может использоваться для импорта HMAC ключей.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае Tuna Key Data Block = '02':</td></tr>
<tr><td>Длина шаблона Key Data Block</td><td>4 N</td><td>Длина следующего поля.</td></tr>
<tr><td>Шаблон Key Data Block</td><td>n H</td><td>Key Data Block в кодировке DER в формате ASN.1. Данные ключа и проверочного значения (при наличии) заполнены нулями.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td>Смещение ключа</td><td>4 N</td><td>Смещение до первого байта значения ключа в Key Data Block.</td></tr>
<tr><td>Длина проверочного значения</td><td>2 N</td><td>Присутствует только в случае экспорта ключей DES/AES.<br>Длина (в байтах) проверочного значения.<br>Допустимые значения: '00' .. '08'. Если проверочное значение не используется, поле имеет значение '00'.<br>Если длина проверочного значения указана, HSM сгенерирует проверочное значение и вставит его в Key Data Block в соответствии со значением Смещение проверочного значения ниже.</td></tr>
<tr><td>Смещение проверочного значения</td><td>4 N</td><td>Присутствует только в случае экспорта ключей DES/AES.<br>Смещение внутри Key Data Block для вставки сгенерированного проверочного значения. Если Длина проверочного значения = '00', поле игнорируется.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'GL'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'02': Ошибка проверки KCV<br>'03': Недопустимый тип закрытого ключа<br>'04': Недопустимый флаг закрытого ключа<br>'05': Недопустимый тип ключа<br>'06': Недопустимый идентификатор алгоритма шифрования<br>'07': Недопустимый идентификатор режима дополнения<br>'10': Нарушена четность ключа DES<br>'50': Открытый ключ не соответствует правилам кодирования<br>'51': Недопустимый идентификатор алгоритма хэширования подписи<br>'52': Недопустимый идентификатор подписи<br>'53': Недопустимый идентификатор режима дополнения подписи<br>'54': Ошибка блока данных header<br>'55': Ошибка блока данных footer<br>'56': Недопустимый флаг ключа DES<br>'60': Недопустимое значение формата ключа HMAC<br>'68': Команда недоступна<br>'78': Ошибка длины закрытого ключа<br>'81': Недопустимый тип Key Data Block<br>'85': Недопустимое значение OAEP MGF<br>'86': Недопустимая функция хэширования OAEP MGF<br>'87': Ошибка OAEP Label<br>или другой стандартный код ошибки. |
| IV | 16 H | Опционально; присутствует только в случае *Tuna Key Data Block* = '01'.<br>Вектор инициализации для ключа DES/AES. |
| Длина зашифрованного ключа | 4 N | Длина (в байтах) следующего поля. |
| Зашифрованный ключ | n B | Экспортированный ключ, зашифрованный под открытым ключом RSA. |
| Длина подписи | 4 N | Длина (в байтах) следующего поля. Присутствует, только если в команде присутствует поле *Индикатор подписи*. |
| Подпись | n B | Подпись от конкатенации *Блока данных header*, *Зашифрованного ключа* и *Блока данных footer*. Присутствует, только если в команде присутствует поле *Индикатор подписи*. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [QE] — Генерация запроса на сертификат

| Variant LMK ☒ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Создание запроса на выпуск сертификата (CSR) путем подписи информации о субъекте и открытом ключе с помощью соответствующего закрытого ключа для создания самоподписанного сертификата в формате PKCS#10.

**Примечания:** Входными данными команды могут являться отдельные поля Subject (тогда команда сама формирует поле Subject в кодировке DER) или готовый шаблон Subject в кодировке DER. Например:

```
30 6b                                   ; SEQUENCE (6b байт)
   31 0b                                ; SET (b байт)
   |  30 09                             ; SEQUENCE (9 байт)
   |     06 03                          ; OBJECT_ID (3 байт)
   |     |  55 04 06
   |     |     ; 2.5.4.6 Страна или регион (C)
   |     13 02                          ; PRINTABLE_STRING (2 байт)
   |        52 55                                          ; RU
   |           ; "RU"
   31 0f                                ; SET (f байт)
   |  30 0d                             ; SEQUENCE (d байт)
   |     06 03                          ; OBJECT_ID (3 байт)
   |     |  55 04 08
   |     |     ; 2.5.4.8 Область, штат (S)
   |     13 06                          ; PRINTABLE_STRING (6 байт)
   |        4d 4f 53 43 4f 57                              ; MOSCOW
   |           ; "MOSCOW"
   31 0f                                ; SET (f байт)
   |  30 0d                             ; SEQUENCE (d байт)
   |     06 03                          ; OBJECT_ID (3 байт)
   |     |  55 04 07
   |     |     ; 2.5.4.7 Размещение (L)
   |     13 06                          ; PRINTABLE_STRING (6 байт)
   |        4d 4f 53 43 4f 57                              ; MOSCOW
   |           ; "MOSCOW"
   31 12                                ; SET (12 байт)
   |  30 10                             ; SEQUENCE (10 байт)
   |     06 03                          ; OBJECT_ID (3 байт)
   |     |  55 04 0a
   |     |     ; 2.5.4.10 Организация (O)
   |     13 09                          ; PRINTABLE_STRING (9 байт)
   |        43 52 59 50 54 4f 50 52  4f                    ; CRYPTOPRO
   |           ; "CRYPTOPRO"
   31 12                                ; SET (12 байт)
   |  30 10                             ; SEQUENCE (10 байт)
   |     06 03                          ; OBJECT_ID (3 байт)
   |     |  55 04 0b
   |     |     ; 2.5.4.11 Подразделение (OU)
   |     13 09                          ; PRINTABLE_STRING (9 байт)
   |        43 52 59 50 54 4f 50 52  4f                    ; CRYPTOPRO
   |           ; "CRYPTOPRO"
   31 12                                ; SET (12 байт)
```

```
30 10                                ; SEQUENCE (10 байт)
   06 03                             ; OBJECT_ID (3 байт)
   |  55 04 03
   |     ; 2.5.4.3 Обычное имя (CN)
   13 09                             ; PRINTABLE_STRING (9 байт)
     43 52 59 50 54 4f 50 52  4f    ; CRYPTOPRO
```

Если в команде указывается Subject в кодировке DER, он должен содержать непустое подмножество следующих полей:

2.5.4.3 - commonName
2.5.4.4 - surname
2.5.4.5 - serialNumber
2.5.4.6 - countryName
2.5.4.7 - localityName
2.5.4.8 - stateOrProvinceName
2.5.4.10 - organizationName
2.5.4.11 - organizationUnitName
2.5.4.12 - title
2.5.4.41 - name
2.5.4.42 - givenName
2.5.4.43 - initials
2.5.4.44 - generationQualifier
2.5.4.46 - distinguishedNameQualifier
2.5.4.65 - pseudonym
0.9.2342.19200300.100.1.25 - domainComponent

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce minimum key strength of 2048-bits for RSA` | `Yes [Y]` | Длины закрытого ключа RSA должна быть не менее 2048 бит. |
| (влияет на параметры: *Закрытый ключ*) | `No [N]` | Ограничения на длину ключа не накладываются. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'QE'.</td></tr>
<tr><td>Тип CSR</td><td>1 N</td><td>Формат запроса на выпуск сертификата:<br>'0': PKCS#10</td></tr>
<tr><td>Выходной формат CSR</td><td>1 N</td><td>'0': PEM в кодировке Base64<br>'1': Шестнадцатеричная кодировка DER</td></tr>
<tr><td>Идентификатор алгоритма подписи</td><td>2 N</td><td>Алгоритм подписи запроса на сертификат:<br>'01': RSA<br>'02': ECC</td></tr>
<tr><td>Метод кодирования открытого ключа</td><td>2 N</td><td>В случае Идентификатора алгоритма подписи = '01' (RSA):<br>'01': открытый ключ RSA в кодировке DER, ASN.1 (беззнаковое целое)<br>'02': открытый ключ RSA в кодировке DER, ASN.1 (целое в формате дополнительного кода)<br><br>В случае Идентификатора алгоритма подписи = '02' (ECC):<br>'03': открытый ключ ECC в кодировке DER, ASN.1 в формате X9.62</td></tr>
<tr><td>Открытый ключ</td><td>n B</td><td>Открытый ключ в формате, определенном выше в поле Метод кодирования открытого ключа.</td></tr>
<tr><td>Закрытый ключ</td><td>'S' + n A</td><td>Закрытый ключ субъекта должен быть в формате Key Block LMK и соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03', '06'</td><td>'R'</td><td>'S', 'D', 'N'</td></tr>
<tr><td>'03'</td><td>'E'</td><td>'S', 'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Идентификатор режима дополнения</td><td>2 N</td><td>Присутствует только в случае Идентификатора алгоритма подписи = '01' (RSA). Режим дополнения, используемый при генерации подписи:<br>'01': PKCS#1 v2.2 method EMSA-PKCS1-v1_5<br>'04': PKCS#1 v2.2 method EMSA-PSS</td></tr>
<tr><td>Идентификатор алгоритма хэширования</td><td>2 N</td><td>Алгоритм хэширования, используемый в CSR:<br>'01': SHA-1 (только RSA)<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512</td></tr>
<tr><td>Функция генерации маски (MGF)</td><td>1 N</td><td>Присутствует только в случае Идентификатора режима дополнения = '04'.<br>'1': MGF1 (как определено в PKCS#1 v2.1)</td></tr>
<tr><td>Тип данных Subject</td><td>1 N</td><td>'0': использовать указанный шаблон<br>'1': явно указать Subject в команде</td></tr>
<tr><td colspan="3">Следующие 3 поля присутствуют только в случае Типа данных Subject = '0':</td></tr>
<tr><td>Длина шаблона Subject</td><td>4 N</td><td>Длина следующего поля.</td></tr>
<tr><td>Шаблон Subject</td><td>n H</td><td>Subject в кодировке DER, ASN.1.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td colspan="3">Следующие 12 полей присутствуют только в случае Типа данных Subject = '1':</td></tr>
<tr><td>Обычное имя (CN)</td><td>n A</td><td>Допустимая длина: от 1 до 64 символов.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td>Организация (O)</td><td>n A</td><td>Допустимая длина: от 1 до 64 символов.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td>Подразделение (OU)</td><td>n A</td><td>Допустимая длина: от 1 до 64 символов.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td>Размещение (L)</td><td>n A</td><td>Допустимая длина: от 1 до 64 символов.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
</table>

| | | |
|---|---|---|
| Область, штат (S) | n A | Допустимая длина: от 1 до 64 символов. |
| Разделитель | 1 A | Значение ';'. |
| Страна/регион (C) | 2 A | Код страны ISO. |
| Разделитель | 1 A | Значение ';'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'QF'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'05': Недопустимый идентификатор алгоритма хэширования<br>'07': Недопустимый идентификатор режима дополнения<br>'D2': Недопустимые параметры кривой<br>'E0': Недопустимый тип CSR<br>'E1': Недопустимый выходной формат CSR<br>'E2': Недопустимый формат открытого ключа<br>'E4': Недопустимый открытый ключ<br>'E5': Ошибка Key Block закрытого ключа<br>'E6': Недопустимое значение MGF<br>'E7': Недопустимый тип данных Subject<br>'E8': Данные Subject не соответствуют правилам кодирования DER<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'E5': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующее 2 поля присутствует только в случае *Кода ошибки* = '00': | | |
| Длина CSR | 4 N | Длина запроса на выпуск сертификата. |
| CSR | n A<br>или<br>n H | Если *Выходной формат CSR* = '0'.<br><br>Если *Выходной формат CSR* = '1'. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [IG] — Выработка ключей с использованием протокола согласования ключей на эллиптических кривых (ECKA)

Команда вырабатывает набор общих ключей с использованием протокола согласования ключей на эллиптических кривых (Elliptic Curve Key Agreement Algorithm, ECKA). Поддерживаются протоколы ECKA-EG (ElGamal Key Agreement, схема Эль-Гамаля) с использованием эфемерного/статического ключа или ECKA-DH (Diffie-Hellman Key Agreement, протокол Диффи-Хеллмана) с использованием только эфемерных ключей.

Команда 'IG' имеет три режима работы (инициирование, выполнение, завершение) для каждой из двух поддерживаемых схем (ECKA-EG и ECKA-DH), и каждая из этих 6 возможных комбинаций описана в этом разделе как отдельная команда:

| | |
|---|---|
| Инициирование ECKA-EG | 103 |
| Выполнение ECKA-EG | 105 |
| Завершение ECKA | 110 |
| Инициирование ECKA-DH | 114 |
| Выполнение ECKA-DH | 116 |
| Завершение ECKA-DH | 121 |

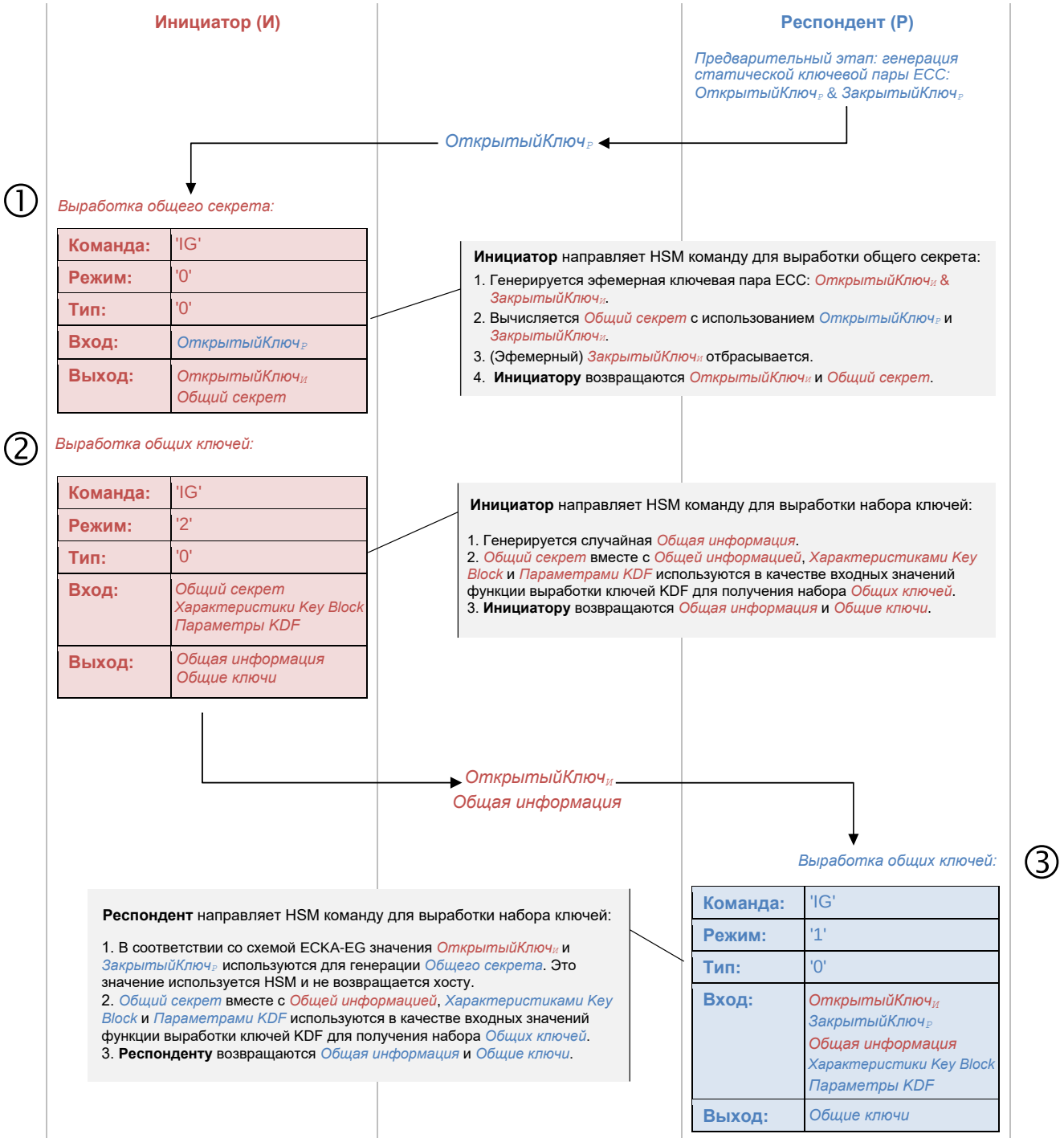
Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce PCI HSMv3 Key Equivalence for Key Wrapping` | `Yes [Y]` | Выработка ключей с большей силой, чем у переданных в команде ключей ECC, невозможна. |
| | `No [N]` | Ограничения на силу вырабатываемых ключей не накладываются. |

### Пример ECKA-EG

Ниже представлен пример совместной выработки набора ключей с использованием схемы ECKA-EG двумя независимыми сторонами (**Инициатором** и **Респондентом**) с разными HSM. **Инициатор** использует эфемерную ключевую пару ECC, **Респондент** — статическую.

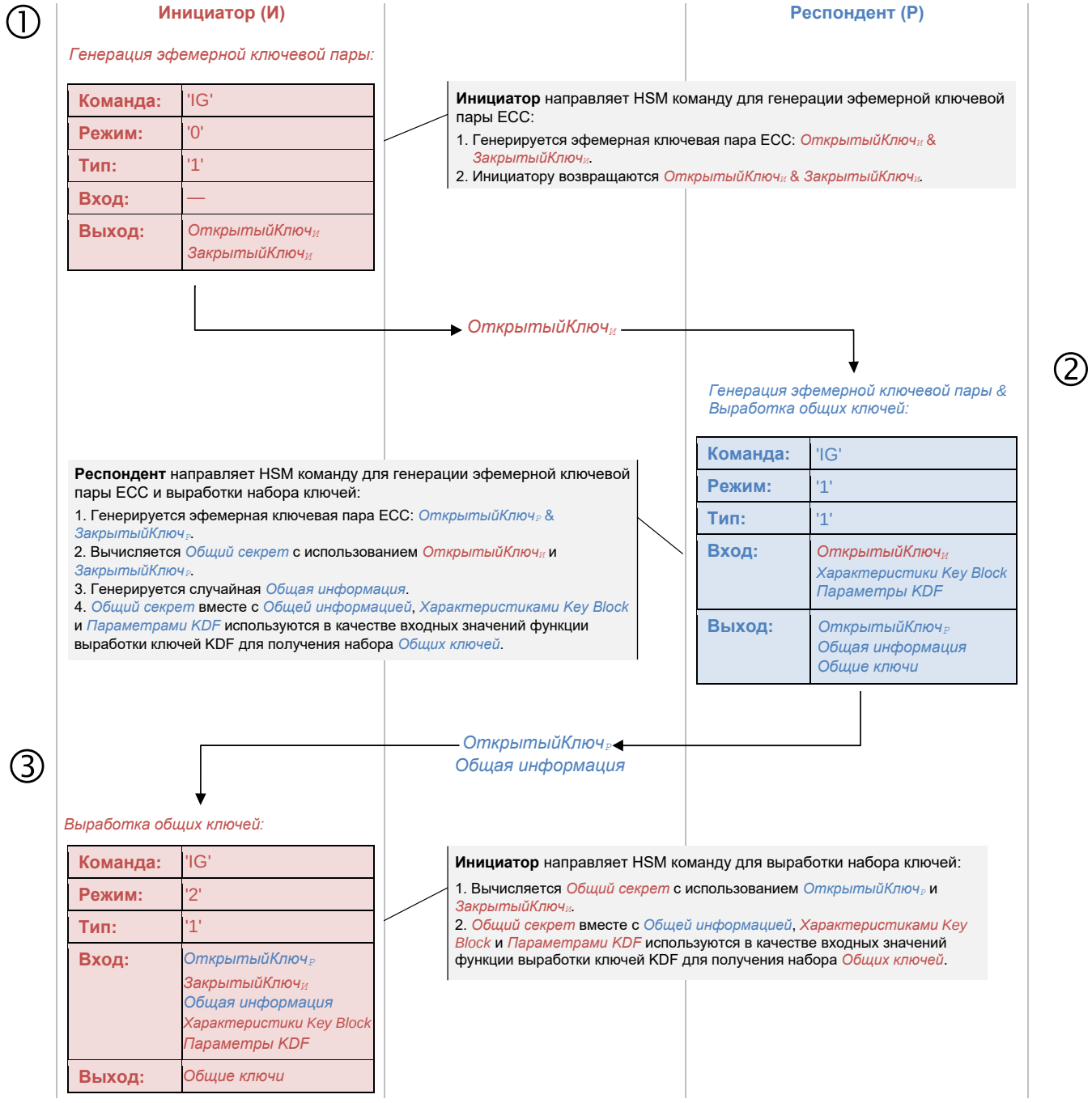
Обратите внимание, что **Инициатор** и **Респондент** должны использовать одинаковый набор входных параметров (*Общая информация, Характеристики Key Block, Параметры KDF* и т.д., за исключением ключей ECC) для успешной выработки одинаковых ключей.



### Пример ECKA-DH

Ниже представлен пример совместной выработки набора ключей с использованием схемы ECKA-DH двумя независимыми сторонами (**Инициатором** и **Респондентом**) с разными HSM. И **Инициатор**, и **Респондент** используют эфемерные ключевые пары ECC.

Обратите внимание, что **Инициатор** и **Респондент** должны использовать одинаковый набор входных параметров (*Общая информация, Характеристики Key Block, Параметры KDF* и т.д., за исключением ключей ECC) для успешной выработки одинаковых ключей.



## [IG] — Выработка ключа с использованием ECKA-EG (Инициатор: выработка общего секрета)

| Variant LMK ☒ | AES Key Block LMK ☑ |
|---|---|

**Описание функции:** Выработка и возврат хосту общего секрета с использованием схемы ECKA-EG. Инициатор процесса согласования ключей использует эфемерную ключевую пару ECC, Респондент — статическую.

Перед вызовом команды Инициатору необходимо получить статический открытый ключ ECC Респондента.

Общий секрет вычисляется путем умножения точки эллиптической кривой статического открытого ключа Респондента и эфемерного закрытого ключа Инициатора. Эфемерный открытый ключ Инициатора возвращается в ответе для последующей передачи Респонденту.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'IG'.</td></tr>
<tr><td>Режим</td><td>1 N</td><td>'0': Инициатор: Инициирование ECKA-EG</td></tr>
<tr><td>Тип согласования ключей</td><td>1 N</td><td>'0': Эфемерный-статический (Эль-Гамаль)</td></tr>
<tr><td>Метод кодирования открытого ключа</td><td>2 N</td><td>Метод кодирования статического открытого ключа Респондента:<br>'03': X9.62 ASN.1<br>'04': несжатый открытый ключ<br>'05': ISO 7816<br>'06': открытый ключ в формате Key Block</td></tr>
<tr><td>Идентификатор кривой</td><td>2 H</td><td>Присутствует только в случае Метода кодирования открытого ключа = '04' или '05'. Эллиптическая кривая, соответствующая статическому открытому ключу Респондента:<br>'00': FIPS 186-3 — NIST P-256<br>'01': FIPS 186-3 — NIST P-384<br>'02': FIPS 186-3 — NIST P-521</td></tr>
<tr><td>Длина открытого ключа</td><td>4 N</td><td>Присутствует только в случае Метода кодирования открытого ключа = '04'. Длина (в байтах) следующего поля.</td></tr>
<tr><td>Открытый ключ</td><td></td><td>Статический открытый ключ Респондента.</td></tr>
<tr><td></td><td>n B</td><td>В случае Метода кодирования открытого ключа = '03', '04', '05' — открытый ключ в соответствующем формате.</td></tr>
<tr><td></td><td>или<br>'S' + n A</td><td>В случае Метода кодирования открытого ключа = '06' ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'02'</td><td>'E'</td><td>'X', 'N'</td></tr>
</table>
</td></tr>
<tr><td>Метод кодирования выходного открытого ключа</td><td>2 N</td><td>'03': X9.62 ASN.1<br>'04': несжатый открытый ключ<br>'05': ISO 7816</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
</table>

| | | |
|---|---|---|
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'IH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки SHS CMAC<br>'56': Ошибка разделителя (конец определения всех ключей)<br>'79': Недопустимый идентификатор алгоритма хэширования<br>'A1': Недопустимая схема LMK<br>'A5': Несоответствие значения длины ключа алгоритму<br>'B2': Ошибка разделителя (конец определения ключа)<br>'D0': Недопустимый режим<br>'D1': Недопустимый тип согласования ключей<br>'D2': Недопустимый идентификатор кривой<br>'D3': Ошибка Key Block открытого ключа<br>'D4': Недопустимый открытый ключ<br>'D5': Кривая не поддерживается<br>'D6': Недопустимый входной формат открытого ключа<br>'D7': Открытый ключ не соответствует правилам кодирования ASN.1<br>'D8': Открытый ключ не соответствует формату TLV<br>'D9': Ошибка Key Block закрытого ключа<br>'DA': Недопустимая длина общей информации<br>'DB': Открытый ключ представлен не в несжатом формате<br>'DD': Недопустимая функция KDF<br>'DE': Недопустимый режим хэширования<br>'DF': Недопустимая длина модификатора входа хэш-функции (соли)<br>'E0': Недопустимая опция хэширования<br>'E1': Недопустимый флаг общей информации<br>'E2': Недопустимое количество SHS<br>'E3': Недопустимый флаг диверсификации ключа<br>'E4': Недопустимое количество ключей<br>'E5': Недопустимое значение модификатора входа хэш-функции (соли)<br>'E8': Недопустимая длина общего секрета<br>'E9': Недопустимое значение SHS<br>'EA': Недостаточная сила кривой ECC для выработки ключей<br>'EB': Недопустимый выходной формат открытого ключа<br>'EC': Недопустимое значение силы ключа в SHS<br>'ED': Длины общего секрета различны<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D3' или 'D9': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Длина открытого ключа | 4 N | Длина (в байтах) следующего поля. |
| Открытый ключ | n B | Эфемерный открытый ключ Инициатора в формате, определенном в поле *Метод кодирования выходного открытого ключа.* |
| Длина SHS | 3 N | Длина (в байтах) следующего поля. |
| SHS | n B | Общий секрет, зашифрованный под LMK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

**[IG] — Выработка ключа с использованием ECKA-EG (Респондент: выработка общего секрета/общих ключей)**

| Variant LMK ☒ | AES Key Block LMK ☑ |
|---|---|

**Описание функции:** Выработка и возврат хосту общего секрета или набора общих ключей, выработанных с использованием схемы ECKA-EG. Инициатор процесса согласования ключей использует эфемерную ключевую пару ECC, Респондент — статическую.

Общий секрет вычисляется путем умножения точки эллиптической кривой эфемерного открытого ключа Инициатора и статического закрытого ключа Респондента.

Набор общих ключей опционально вырабатывается из общего секрета с использованием функции выработки ключей KDF. Поддерживается возможность выработки до 99 общих ключей (DES/AES/HMAC).

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'IG'. |
| Режим | 1 N | '1': Респондент: Выполнение ECKA-EG |
| Тип согласования ключей | 1 N | '0': Эфемерный-статический (Эль-Гамаль) |
| Метод кодирования открытого ключа | 2 N | Метод кодирования эфемерного открытого ключа Инициатора:<br>'03': X9.62 ASN.1<br>'04': несжатый открытый ключ<br>'05': ISO 7816 |
| Идентификатор кривой | 2 H | Присутствует только в случае *Метода кодирования открытого ключа* = '04' или '05'. Эллиптическая кривая, соответствующая эфемерному открытому ключу Инициатора:<br>'00': FIPS 186-3 — NIST P-256<br>'01': FIPS 186-3 — NIST P-384<br>'02': FIPS 186-3 — NIST P-521 |
| Длина открытого ключа | 4 N | Присутствует только в случае *Метода кодирования открытого ключа* = '04'. Длина (в байтах) следующего поля. |
| Открытый ключ | n B | Эфемерный открытый ключ Инициатора в соответствующем формате. |
| Закрытый ключ | 'S' + n A | Статический закрытый ключ Респондента, зашифрованный под LMK, должен соответствовать следующему формату:<br>Использование ключа: '03'; Алгоритм: 'E'; Режим использования: 'X', 'N' |
| Флаг диверсификации ключа | 1 N | '0': вывести только значение общего секрета<br>'1': выполнить выработку общих ключей |
| Следующие поля присутствуют только в случае *Флага диверсификации ключа* = '1': | | |
| Функция KDF | 1 N | '0': HKDF (RFC 5869)<br>'1': Single Step KDF (NIST SP800-56A)<br>'2': KDF (ANSI X9.63) |
| Идентификатор алгоритма хэширования | 2 N | Алгоритм хэширования, используемый в KDF:<br>'06': SHA-256 |
| Следующие 4 поля присутствуют только в случае *Функции KDF* = '0' (HKDF): | | |

| | | |
|---|---|---|
| Режим хэширования | 1 N | '0': включить эфемерный открытый ключ в KDF |
| Длина модификатора входа хэш-функции («соли») | 2 N | Длина следующего поля, должна быть чётной. Если модификатор входа хэш-функции («соль») не требуется, поле должно иметь значение '00'. |
| Модификатор входа хэш-функции («соль») | n H | Значение модификатора входа хэш-функции («соли»), используемое в KDF. |
| Разделитель | 1 A | Значение ';'. |
| Опция хэширования | 1 N | Присутствует только в случае *Функции KDF* = '1' (Single Step KDF).<br>'1': использовать функцию $H(x) = hash(x)$ |
| Флаг общей информации | 1 N | '0': использовать значение общей информации, переданное в команде<br>'1': использовать случайное значение общей информации |
| Длина общей информации | 3 N | В случае *Флага общей информации* = '0' — длина (в шестнадцатеричных символах) следующего поля.<br>В случае *Флага общей информации* = '1' — длина (в шестнадцатеричных символах) случайно генерируемого значения общей информации.<br>Должно содержать чётное значение.<br>Если значение общей информации не требуется, поле должно иметь значение '000'. |
| Общая информация | n H | Присутствует только в случае *Флага общей информации* = '0'.<br>Значение, известное двум сторонам, используемое в KDF.<br>*Например*, при использовании в качестве общей информации строки "Cryptopro" значение поля будет представлено следующей последовательностью шестнадцатеричных символов: 43727970746F70726F. Значение предыдущего поля при этом равно '018' (18 шестнадцатеричных символов).<br>*Примечание:* при обмене общей информацией необходимо убедиться, что системы обеих сторон настроены на одинаковое представление информации (ASCII-символы или байтовая строка). |
| Разделитель | 1 A | Присутствует только в случае *Флага общей информации* = '0'.<br>Значение ';'. |
| Количество ключей | 2 N | Количество вырабатываемых ключей, должно быть больше '00'. |
| Следующие поля (до поля *Разделитель (конец определения всех ключей)*) повторяются для каждого ключа: | | |
| Длина ключа | 5 N | Длина (в битах) ключа. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block. Любое допустимое значение, совместимое со значениями *Алгоритма* и *Режима использования* ниже. |
| Алгоритм | 2 A | Поле *Алгоритм*, первый символ включается в заголовок Key Block (байт 7).<br>'T2': 2DES<br>'T3': 3DES<br>'A1': AES-128<br>'A2': AES-192<br>'A3': AES-256<br>'H0': HMAC |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block. Любое допустимое значение, совместимое со значениями *Использования ключа* и *Алгоритма* выше. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N', 'E', 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |

| | | |
|---|---|---|
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Разделитель (конец определения ключа) | 1 A | Значение ';'. Признак конца определения характеристик одного вырабатываемого ключа. |
| Разделитель (конец определения всех ключей) | 1 A | Значение ':'. Признак конца определений характеристик всех вырабатываемых ключей. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'IH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки SHS CMAC<br>'56': Ошибка разделителя (конец определения всех ключей)<br>'79': Недопустимый идентификатор алгоритма хэширования<br>'A1': Недопустимая схема LMK<br>'A5': Несоответствие значения длины ключа алгоритму<br>'B2': Ошибка разделителя (конец определения ключа)<br>'D0': Недопустимый режим<br>'D1': Недопустимый тип согласования ключей<br>'D2': Недопустимый идентификатор кривой<br>'D3': Ошибка Key Block открытого ключа<br>'D4': Недопустимый открытый ключ<br>'D5': Кривая не поддерживается<br>'D6': Недопустимый входной формат открытого ключа<br>'D7': Открытый ключ не соответствует правилам кодирования ASN.1<br>'D8': Открытый ключ не соответствует формату TLV<br>'D9': Ошибка Key Block закрытого ключа<br>'DA': Недопустимая длина общей информации<br>'DB': Открытый ключ представлен не в несжатом формате<br>'DD': Недопустимая функция KDF<br>'DE': Недопустимый режим хэширования<br>'DF': Недопустимая длина модификатора входа хэш-функции (соли)<br>'E0': Недопустимая опция хэширования<br>'E1': Недопустимый флаг общей информации<br>'E2': Недопустимое количество SHS<br>'E3': Недопустимый флаг диверсификации ключа<br>'E4': Недопустимое количество ключей<br>'E5': Недопустимое значение модификатора входа хэш-функции (соли)<br>'E8': Недопустимая длина общего секрета<br>'E9': Недопустимое значение SHS<br>'EA': Недостаточная сила кривой ECC для выработки ключей<br>'EB': Недопустимый выходной формат открытого ключа<br>'EC': Недопустимое значение силы ключа в SHS<br>'ED': Длины общего секрета различны<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D3' или 'D9': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующие 2 поля присутствуют только в случае *Флага диверсификации ключа* = '0': | | |
| Длина SHS | 3 N | Длина (в байтах) следующего поля. |
| SHS | n B | Общий секрет, зашифрованный под LMK. |
| Следующие поля присутствуют только в случае *Флага диверсификации ключа* = '1': | | |
| Следующие 2 поля повторяются для каждого ключа: | | |
| Ключ | 'S' + n A | Выработанный ключ, зашифрованный под LMK. |
| KCV | 3 B | Проверочное значение выработанного ключа. |
| Общая информация | n H | Присутствует только в случае *Флага общей информации* = '1'.<br>Случайно сгенерированное значение общей информации, используемое в KDF. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |

| | | |
|---|---|---|
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [IG] — Выработка ключа с использованием ECKA-EG/DH (Выработка общих ключей)

| Variant LMK ☒ | AES Key Block LMK ☑ |
|---|---|

**Описание функции:** Возврат хосту набора выработанных ключей с использованием схемы ECKA-EG или ECKA-DH.

Вызов команды может использоваться и Инициатором, и Респондентом для выработки общих ключей из одного или нескольких общих секретов, которые были получены в предыдущих ответах на команду 'IG'.

Набор общих ключей вырабатывается из общего(-их) секрета(-ов) с использованием функции выработки ключей KDF. Поддерживается возможность выработки до 99 общих ключей (DES/AES/HMAC).

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'IG'. |
| Режим | 1 N | '2': Инициатор/Респондент: Завершение ECKA |
| Тип согласования ключей | 1 N | '0': Эфемерный-статический (Эль-Гамаль) или Эфемерный-эфемерный (Диффи-Хеллман) |
| Количество SHS | 1 N | Количество общих секретов, из которых вырабатываются общие ключи. |
| Следующие 3 поля повторяются для каждого SHS: | | |
| Длина SHS | 3 N | Длина (в байтах) следующего поля. |
| SHS | n B | Общий секрет, зашифрованный под LMK. |
| Разделитель | 1 A | Значение ';'. |
| Функция KDF | 1 N | '0': HKDF (RFC 5869)<br>'1': Single Step KDF (NIST SP800-56A)<br>'2': KDF (ANSI X9.63) |
| Идентификатор алгоритма хэширования | 2 N | Алгоритм хэширования, используемый в KDF:<br>'06': SHA-256 |
| Следующие поля присутствуют только в случае *Функции KDF* = '0' (HKDF): | | |
| Метод кодирования открытого ключа | 2 N | Метод кодирования открытого ключа Инициатора:<br>'03': X9.62 ASN.1<br>'04': несжатый открытый ключ<br>'05': ISO 7816 |
| Длина открытого ключа | 4 N | Присутствует только в случае *Метода кодирования открытого ключа* = '04'.<br>Длина (в байтах) следующего поля. |
| Открытый ключ | n B | Открытый ключ Инициатора, используемый в KDF. |
| Режим хэширования | 1 N | '0': включить эфемерный открытый ключ в KDF |
| Длина модификатора входа хэш-функции («соли») | 2 N | Длина следующего поля, должна быть чётной. Если модификатор входа хэш-функции («соль») не требуется, поле должно иметь значение '00'. |
| Модификатор входа хэш-функции («соль») | n H | Значение модификатора входа хэш-функции («соли»), используемое в KDF. |
| Разделитель | 1 A | Значение ';'. |
| Опция хэширования | 1 N | Присутствует только в случае *Функции KDF* = '1' (Single Step KDF).<br>'1': использовать функцию $H(x) = hash(x)$ |

| | | |
|---|---|---|
| Флаг общей информации | 1 N | '0': использовать значение общей информации, переданное в команде<br>'1': использовать случайное значение общей информации |
| Длина общей информации | 3 N | В случае *Флага общей информации* = '0' — длина (в шестнадцатеричных символах) следующего поля.<br>В случае *Флага общей информации* = '1' — длина (в шестнадцатеричных символах) случайно генерируемого значения общей информации.<br>Должно содержать чётное значение.<br>Если значение общей информации не требуется, поле должно иметь значение '000'. |
| Общая информация | n H | Присутствует только в случае *Флага общей информации* = '0'.<br>Значение, известное двум сторонам, используемое в KDF.<br>*Например*, при использовании в качестве общей информации строки "Cryptopro" значение поля будет представлено следующей последовательностью шестнадцатеричных символов: 43727970746F70726F. Значение предыдущего поля при этом равно '018' (18 шестнадцатеричных символов).<br>*Примечание:* при обмене общей информацией необходимо убедиться, что системы обеих сторон настроены на одинаковое представление информации (ASCII-символы или байтовая строка). |
| Разделитель | 1 A | Присутствует только в случае *Флага общей информации* = '0'.<br>Значение ';'. |
| Количество ключей | 2 N | Количество вырабатываемых ключей, должно быть больше '00'. |
| Следующие поля (до поля *Разделитель (конец определения всех ключей)*) повторяются для каждого ключа: | | |
| Длина ключа | 5 N | Длина (в битах) ключа. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block. Любое допустимое значение, совместимое со значениями *Алгоритма* и *Режима использования* ниже. |
| Алгоритм | 2 A | Поле *Алгоритм*, первый символ включается в заголовок Key Block (байт 7).<br>'T2': 2DES<br>'T3': 3DES<br>'A1': AES-128<br>'A2': AES-192<br>'A3': AES-256<br>'H0': HMAC |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block. Любое допустимое значение, совместимое со значениями *Использования ключа* и *Алгоритма* выше. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N', 'E', 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Разделитель (конец определения ключа) | 1 A | Значение ';'. Признак конца определения характеристик одного вырабатываемого ключа. |

| | | |
|---|---|---|
| Разделитель (конец определения всех ключей) | 1 A | Значение ':'. Признак конца определений характеристик всех вырабатываемых ключей. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'IH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки SHS CMAC<br>'56': Ошибка разделителя (конец определения всех ключей)<br>'79': Недопустимый идентификатор алгоритма хэширования<br>'A1': Недопустимая схема LMK<br>'A5': Несоответствие значения длины ключа алгоритму<br>'B2': Ошибка разделителя (конец определения ключа)<br>'D0': Недопустимый режим<br>'D1': Недопустимый тип согласования ключей<br>'D2': Недопустимый идентификатор кривой<br>'D3': Ошибка Key Block открытого ключа<br>'D4': Недопустимый открытый ключ<br>'D5': Кривая не поддерживается<br>'D6': Недопустимый входной формат открытого ключа<br>'D7': Открытый ключ не соответствует правилам кодирования ASN.1<br>'D8': Открытый ключ не соответствует формату TLV<br>'D9': Ошибка Key Block закрытого ключа<br>'DA': Недопустимая длина общей информации<br>'DB': Открытый ключ представлен не в несжатом формате<br>'DD': Недопустимая функция KDF<br>'DE': Недопустимый режим хэширования<br>'DF': Недопустимая длина модификатора входа хэш-функции (соли)<br>'E0': Недопустимая опция хэширования<br>'E1': Недопустимый флаг общей информации<br>'E2': Недопустимое количество SHS<br>'E3': Недопустимый флаг диверсификации ключа<br>'E4': Недопустимое количество ключей<br>'E5': Недопустимое значение модификатора входа хэш-функции (соли)<br>'E8': Недопустимая длина общего секрета<br>'E9': Недопустимое значение SHS<br>'EA': Недостаточная сила кривой ECC для выработки ключей<br>'EB': Недопустимый выходной формат открытого ключа<br>'EC': Недопустимое значение силы ключа в SHS<br>'ED': Длины общего секрета различны<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D3' или 'D9': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующие 2 поля повторяются для каждого ключа: | | |
| Ключ | 'S' + n A | Выработанный ключ, зашифрованный под LMK. |

| | | |
|---|---|---|
| KCV | 3 B | Проверочное значение выработанного ключа. |
| Общая информация | n H | Присутствует только в случае *Флага общей информации* = '1'.<br>Случайно сгенерированное значение общей информации, используемое в KDF. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

**[IG] — Выработка ключа с использованием ECKA-DH (Инициатор: генерация эфемерной ключевой пары)**

| Variant LMK ☒ | AES Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация и возврат хосту эфемерной ключевой пары, необходимой Инициатору для инициирования процесса согласования ключей с использованием схемы ECKA-DH. И Инициатор, и Респондент используют эфемерную ключевую пару ECC.

После генерации эфемерный открытый ключ Инициатора должен быть передан Респонденту.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'IG'. |
| Режим | 1 N | '0': Инициатор: Инициирование ECKA-DH |
| Тип согласования ключей | 1 N | '1': Эфемерный-эфемерный (Диффи-Хеллман) |
| Идентификатор кривой | 2 H | Эллиптическая кривая для выходного эфемерного открытого ключа Инициатора:<br>'00': FIPS 186-3 — NIST P-256<br>'01': FIPS 186-3 — NIST P-384<br>'02': FIPS 186-3 — NIST P-521 |
| Метод кодирования выходного открытого ключа | 2 N | Метод кодирования выходного эфемерного открытого ключа Инициатора:<br>'03': X9.62 ASN.1<br>'04': несжатый открытый ключ<br>'05': ISO 7816 |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'IH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки SHS CMAC<br>'56': Ошибка разделителя (конец определения всех ключей)<br>'79': Недопустимый идентификатор алгоритма хэширования<br>'A1': Недопустимая схема LMK<br>'A5': Несоответствие значения длины ключа алгоритму<br>'B2': Ошибка разделителя (конец определения ключа)<br>'D0': Недопустимый режим<br>'D1': Недопустимый тип согласования ключей<br>'D2': Недопустимый идентификатор кривой<br>'D3': Ошибка Key Block открытого ключа<br>'D4': Недопустимый открытый ключ<br>'D5': Кривая не поддерживается<br>'D6': Недопустимый входной формат открытого ключа<br>'D7': Открытый ключ не соответствует правилам кодирования ASN.1<br>'D8': Открытый ключ не соответствует формату TLV<br>'D9': Ошибка Key Block закрытого ключа<br>'DA': Недопустимая длина общей информации<br>'DB': Открытый ключ представлен не в несжатом формате<br>'DD': Недопустимая функция KDF<br>'DE': Недопустимый режим хэширования<br>'DF': Недопустимая длина модификатора входа хэш-функции (соли)<br>'E0': Недопустимая опция хэширования<br>'E1': Недопустимый флаг общей информации<br>'E2': Недопустимое количество SHS<br>'E3': Недопустимый флаг диверсификации ключа<br>'E4': Недопустимое количество ключей<br>'E5': Недопустимое значение модификатора входа хэш-функции (соли)<br>'E8': Недопустимая длина общего секрета<br>'E9': Недопустимое значение SHS<br>'EA': Недостаточная сила кривой ECC для выработки ключей<br>'EB': Недопустимый выходной формат открытого ключа<br>'EC': Недопустимое значение силы ключа в SHS<br>'ED': Длины общего секрета различны<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D3' или 'D9': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Длина открытого ключа | 4 N | Длина (в байтах) следующего поля. |
| Открытый ключ | n B | Эфемерный открытый ключ Инициатора в формате, определенном в поле *Метод кодирования выходного открытого ключа.* |
| Закрытый ключ | 'S' + n A | Эфемерный закрытый ключ Инициатора, зашифрованный под LMK, должен соответствовать следующему формату:<br>Использование ключа: '03'; Алгоритм: 'E'; Режим использования: 'X' |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

**[IG] — Выработка ключа с использованием ECKA-DH (Респондент: выработка общего секрета/общих ключей)**

| Variant LMK ☒ | AES Key Block LMK ☑ |
|---|---|

**Описание функции:** Выработка и возврат хосту общего секрета или набора общих ключей, выработанных с использованием схемы ECKA-DH. И Инициатор, и Респондент используют эфемерную ключевую пару ECC.

Общий секрет вычисляется путем умножения точки эллиптической кривой эфемерного открытого ключа Инициатора и эфемерного закрытого ключа Респондента.

Набор общих ключей опционально вырабатывается из общего секрета с использованием функции выработки ключей KDF. Поддерживается возможность выработки до 99 общих ключей (DES/AES/HMAC).

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'IG'. |
| Режим | 1 N | '1': Респондент: Выполнение ECKA-DH |
| Тип согласования ключей | 1 N | '1': Эфемерный-эфемерный (Диффи-Хеллман) |
| Метод кодирования открытого ключа | 2 N | Метод кодирования эфемерного открытого ключа Инициатора:<br>'03': X9.62 ASN.1<br>'04': несжатый открытый ключ<br>'05': ISO 7816 |
| Идентификатор кривой | 2 H | Присутствует только в случае *Метода кодирования открытого ключа* = '04' или '05'. Эллиптическая кривая, соответствующая эфемерному открытому ключу Инициатора:<br>'00': FIPS 186-3 — NIST P-256<br>'01': FIPS 186-3 — NIST P-384<br>'02': FIPS 186-3 — NIST P-521 |
| Длина открытого ключа | 4 N | Присутствует только в случае *Метода кодирования открытого ключа* = '04'. Длина (в байтах) следующего поля. |
| Открытый ключ | n B | Эфемерный открытый ключ Инициатора в соответствующем формате. |
| Метод кодирования выходного открытого ключа | 2 N | Метод кодирования выходного эфемерного открытого ключа Респондента:<br>'03': X9.62 ASN.1<br>'04': несжатый открытый ключ<br>'05': ISO 7816 |
| Флаг диверсификации ключа | 1 N | '0': вывести только значение общего секрета<br>'1': выполнить выработку общих ключей |
| Следующие поля присутствуют только в случае *Флага диверсификации ключа* = '1': | | |
| Функция KDF | 1 N | '0': HKDF (RFC 5869)<br>'1': Single Step KDF (NIST SP800-56A)<br>'2': KDF (ANSI X9.63) |
| Идентификатор алгоритма хэширования | 2 N | Алгоритм хэширования, используемый в KDF:<br>'06': SHA-256 |
| Следующие 4 поля присутствуют только в случае *Функции KDF* = '0' (HKDF): | | |
| Режим хэширования | 1 N | '0': включить эфемерный открытый ключ в KDF |

| | | |
|---|---|---|
| Длина модификатора входа хэш-функции («соли») | 2 N | Длина следующего поля, должна быть чётной. Если модификатор входа хэш-функции («соль») не требуется, поле должно иметь значение '00'. |
| Модификатор входа хэш-функции («соль») | n H | Значение модификатора входа хэш-функции («соли»), используемое в KDF. |
| Разделитель | 1 A | Значение ';'. |
| Опция хэширования | 1 N | Присутствует только в случае *Функции KDF* = '1' (Single Step KDF).<br>'1': использовать функцию $H(x) = hash(x)$ |
| Флаг общей информации | 1 N | '0': использовать значение общей информации, переданное в команде<br>'1': использовать случайное значение общей информации |
| Длина общей информации | 3 N | В случае *Флага общей информации* = '0' — длина (в шестнадцатеричных символах) следующего поля.<br>В случае *Флага общей информации* = '1' — длина (в шестнадцатеричных символах) случайно генерируемого значения общей информации.<br>Должно содержать чётное значение.<br>Если значение общей информации не требуется, поле должно иметь значение '000'. |
| Общая информация | n H | Присутствует только в случае *Флага общей информации* = '0'.<br>Значение, известное двум сторонам, используемое в KDF.<br>*Например*, при использовании в качестве общей информации строки "Cryptopro" значение поля будет представлено следующей последовательностью шестнадцатеричных символов: 43727970746F70726F.<br>Значение предыдущего поля при этом равно '018' (18 шестнадцатеричных символов).<br>*Примечание:* при обмене общей информацией необходимо убедиться, что системы обеих сторон настроены на одинаковое представление информации (ASCII-символы или байтовая строка). |
| Разделитель | 1 A | Присутствует только в случае *Флага общей информации* = '0'.<br>Значение ';'. |
| Количество ключей | 2 N | Количество вырабатываемых ключей, должно быть больше '00'. |
| Следующие поля (до поля *Разделитель (конец определения всех ключей)*) повторяются для каждого ключа: | | |
| Длина ключа | 5 N | Длина (в битах) ключа. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block. Любое допустимое значение, совместимое со значениями *Алгоритма* и *Режима использования* ниже. |
| Алгоритм | 2 A | Поле *Алгоритм*, первый символ включается в заголовок Key Block (байт 7).<br>'T2': 2DES<br>'T3': 3DES<br>'A1': AES-128<br>'A2': AES-192<br>'A3': AES-256<br>'H0': HMAC |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block. Любое допустимое значение, совместимое со значениями *Использования ключа* и *Алгоритма* выше. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N', 'E', 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |

| | | |
|---|---|---|
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Разделитель (конец определения ключа) | 1 A | Значение ';'. Признак конца определения характеристик одного вырабатываемого ключа. |
| Разделитель (конец определения всех ключей) | 1 A | Значение ':'. Признак конца определений характеристик всех вырабатываемых ключей. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'IH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки SHS CMAC<br>'56': Ошибка разделителя (конец определения всех ключей)<br>'79': Недопустимый идентификатор алгоритма хэширования<br>'A1': Недопустимая схема LMK<br>'A5': Несоответствие значения длины ключа алгоритму<br>'B2': Ошибка разделителя (конец определения ключа)<br>'D0': Недопустимый режим<br>'D1': Недопустимый тип согласования ключей<br>'D2': Недопустимый идентификатор кривой<br>'D3': Ошибка Key Block открытого ключа<br>'D4': Недопустимый открытый ключ<br>'D5': Кривая не поддерживается<br>'D6': Недопустимый входной формат открытого ключа<br>'D7': Открытый ключ не соответствует правилам кодирования ASN.1<br>'D8': Открытый ключ не соответствует формату TLV<br>'D9': Ошибка Key Block закрытого ключа<br>'DA': Недопустимая длина общей информации<br>'DB': Открытый ключ представлен не в несжатом формате<br>'DD': Недопустимая функция KDF<br>'DE': Недопустимый режим хэширования<br>'DF': Недопустимая длина модификатора входа хэш-функции (соли)<br>'E0': Недопустимая опция хэширования<br>'E1': Недопустимый флаг общей информации<br>'E2': Недопустимое количество SHS<br>'E3': Недопустимый флаг диверсификации ключа<br>'E4': Недопустимое количество ключей<br>'E5': Недопустимое значение модификатора входа хэш-функции (соли)<br>'E8': Недопустимая длина общего секрета<br>'E9': Недопустимое значение SHS<br>'EA': Недостаточная сила кривой ECC для выработки ключей<br>'EB': Недопустимый выходной формат открытого ключа<br>'EC': Недопустимое значение силы ключа в SHS<br>'ED': Длины общего секрета различны<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D3' или 'D9': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Длина открытого ключа | 4 N | Длина (в байтах) следующего поля. |
| Открытый ключ | n B | Эфемерный открытый ключ Респондента в формате, определенном в поле *Метод кодирования выходного открытого ключа.* |
| Следующие 2 поля присутствуют только в случае *Флага диверсификации ключа* = '0': | | |
| Длина SHS | 3 N | Длина (в байтах) следующего поля. |
| SHS | n B | Общий секрет, зашифрованный под LMK. |
| Следующие поля присутствуют только в случае *Флага диверсификации ключа* = '1': | | |
| Следующие 2 поля повторяются для каждого ключа: | | |
| Ключ | 'S' + n A | Выработанный ключ, зашифрованный под LMK. |
| KCV | 3 B | Проверочное значение выработанного ключа. |

| | | |
|---|---|---|
| Общая информация | n H | Присутствует только в случае *Флага общей информации* = '1'.<br>Случайно сгенерированное значение общей информации, используемое в KDF. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [IG] — Выработка ключа с использованием ECKA-DH (Инициатор: выработка общих ключей)

| Variant LMK ☒ | AES Key Block LMK ☑ |
|---|---|

**Описание функции:** Возврат хосту набора ключей, выработанных с использованием схемы ECKA-DH.

Вызов команды выполняется Инициатором для локальной выработки общего секрета и последующей выработки и возврата хосту набора общих ключей.

Набор общих ключей вырабатывается из общего секрета с использованием функции выработки ключей KDF. Поддерживается возможность выработки до 99 общих ключей (DES/AES/HMAC).

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'IG'. |
| Режим | 1 N | '2': Инициатор: Завершение ECKA-DH |
| Тип согласования ключей | 1 N | '1': Эфемерный-эфемерный (Диффи-Хеллман) |
| Метод кодирования открытого ключа | 2 N | Метод кодирования эфемерного открытого ключа Респондента:<br>'03': X9.62 ASN.1<br>'04': несжатый открытый ключ<br>'05': ISO 7816 |
| Идентификатор кривой | 2 H | Присутствует только в случае *Метода кодирования открытого ключа* = '04' или '05'. Эллиптическая кривая, соответствующая эфемерному открытому ключу Респондента:<br>'00': FIPS 186-3 — NIST P-256<br>'01': FIPS 186-3 — NIST P-384<br>'02': FIPS 186-3 — NIST P-521 |
| Длина открытого ключа | 4 N | Присутствует только в случае *Метода кодирования открытого ключа* = '04'. Длина (в байтах) следующего поля. |
| Открытый ключ | n B | Эфемерный открытый ключ Респондента в соответствующем формате. |
| Закрытый ключ | 'S' + n A | Эфемерный закрытый ключ Инициатора (полученный в ответе предыдущего вызова 'IG' с параметрами *Режим* = '0', *Тип согласования ключей* = '1'), зашифрованный под LMK, должен соответствовать следующему формату:<br>Использование ключа: '03'; Алгоритм: 'E'; Режим использования: 'X', 'N' |
| Функция KDF | 1 N | '0': HKDF (RFC 5869)<br>'1': Single Step KDF (NIST SP800-56A)<br>'2': KDF (ANSI X9.63) |
| Идентификатор алгоритма хэширования | 2 N | Алгоритм хэширования, используемый в KDF:<br>'06': SHA-256 |
| Следующие 7 полей присутствуют только в случае *Функции KDF* = '0' (HKDF): | | |
| Метод кодирования открытого ключа KDF | 2 N | '03': X9.62 ASN.1<br>'04': несжатый открытый ключ<br>'05': ISO 7816 |
| Длина открытого ключа KDF | 4 N | Присутствует только в случае *Метода кодирования открытого ключа KDF* = '04'. Длина (в байтах) следующего поля. |

| | | |
|---|---|---|
| Открытый ключ | n B | Открытый ключ Инициатора, используемый в KDF. |
| Режим хэширования | 1 N | '0': включить эфемерный открытый ключ в KDF |
| Длина модификатора входа хэш-функции («соли») | 2 N | Длина следующего поля, должна быть чётной. Если модификатор входа хэш-функции («соль») не требуется, поле должно иметь значение '00'. |
| Модификатор входа хэш-функции («соль») | n H | Значение модификатора входа хэш-функции («соли»), используемое в KDF. |
| Разделитель | 1 A | Значение ';'. |
| Опция хэширования | 1 N | Присутствует только в случае *Функции KDF* = '1' (Single Step KDF).<br>'1': использовать функцию $H(x) = hash(x)$ |
| Флаг общей информации | 1 N | '0': использовать значение общей информации, переданное в команде<br>'1': использовать случайное значение общей информации |
| Длина общей информации | 3 N | В случае *Флага общей информации* = '0' — длина (в шестнадцатеричных символах) следующего поля.<br>В случае *Флага общей информации* = '1' — длина (в шестнадцатеричных символах) случайно генерируемого значения общей информации.<br>Должно содержать чётное значение.<br>Если значение общей информации не требуется, поле должно иметь значение '000'. |
| Общая информация | n H | Присутствует только в случае *Флага общей информации* = '0'.<br>Значение, известное двум сторонам, используемое в KDF.<br>*Например*, при использовании в качестве общей информации строки "Cryptopro" значение поля будет представлено следующей последовательностью шестнадцатеричных символов: 43727970746F70726F. Значение предыдущего поля при этом равно '018' (18 шестнадцатеричных символов).<br>*Примечание:* при обмене общей информацией необходимо убедиться, что системы обеих сторон настроены на одинаковое представление информации (ASCII-символы или байтовая строка). |
| Разделитель | 1 A | Присутствует только в случае *Флага общей информации* = '0'.<br>Значение ';'. |
| Количество ключей | 2 N | Количество вырабатываемых ключей, должно быть больше '00'. |
| Следующие поля (до поля *Разделитель (конец определения всех ключей)*) повторяются для каждого ключа: | | |
| Длина ключа | 5 N | Длина (в битах) ключа. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block. Любое допустимое значение, совместимое со значениями *Алгоритма* и *Режима использования* ниже. |
| Алгоритм | 2 A | Поле *Алгоритм*, первый символ включается в заголовок Key Block (байт 7).<br>'T2': 2DES<br>'T3': 3DES<br>'A1': AES-128<br>'A2': AES-192<br>'A3': AES-256<br>'H0': HMAC |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block. Любое допустимое значение, совместимое со значениями *Использования ключа* и *Алгоритма* выше. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N', 'E', 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже.<br>Допустимые значения: '00' .. '08'. |

| | | |
|---|---|---|
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Разделитель (конец определения ключа) | 1 A | Значение ';'. Признак конца определения характеристик одного вырабатываемого ключа. |
| Разделитель (конец определения всех ключей) | 1 A | Значение ':'. Признак конца определений характеристик всех вырабатываемых ключей. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'IH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки SHS CMAC<br>'56': Ошибка разделителя (конец определения всех ключей)<br>'79': Недопустимый идентификатор алгоритма хэширования<br>'A1': Недопустимая схема LMK<br>'A5': Несоответствие значения длины ключа алгоритму<br>'B2': Ошибка разделителя (конец определения ключа)<br>'D0': Недопустимый режим<br>'D1': Недопустимый тип согласования ключей<br>'D2': Недопустимый идентификатор кривой<br>'D3': Ошибка Key Block открытого ключа<br>'D4': Недопустимый открытый ключ<br>'D5': Кривая не поддерживается<br>'D6': Недопустимый входной формат открытого ключа<br>'D7': Открытый ключ не соответствует правилам кодирования ASN.1<br>'D8': Открытый ключ не соответствует формату TLV<br>'D9': Ошибка Key Block закрытого ключа<br>'DA': Недопустимая длина общей информации<br>'DB': Открытый ключ представлен не в несжатом формате<br>'DD': Недопустимая функция KDF<br>'DE': Недопустимый режим хэширования<br>'DF': Недопустимая длина модификатора входа хэш-функции (соли)<br>'E0': Недопустимая опция хэширования<br>'E1': Недопустимый флаг общей информации<br>'E2': Недопустимое количество SHS<br>'E3': Недопустимый флаг диверсификации ключа<br>'E4': Недопустимое количество ключей<br>'E5': Недопустимое значение модификатора входа хэш-функции (соли)<br>'E8': Недопустимая длина общего секрета<br>'E9': Недопустимое значение SHS<br>'EA': Недостаточная сила кривой ECC для выработки ключей<br>'EB': Недопустимый выходной формат открытого ключа<br>'EC': Недопустимое значение силы ключа в SHS<br>'ED': Длины общего секрета различны<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D3' или 'D9': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующие 2 поля повторяются для каждого ключа: | | |
| Ключ | 'S' + n A | Выработанный ключ, зашифрованный под LMK. |
| KCV | 3 B | Проверочное значение выработанного ключа. |
| Общая информация | n H | Присутствует только в случае *Флага общей информации* = '1'.<br>Случайно сгенерированное значение общей информации, используемое в KDF. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [B8] — Экспорт ключа в формат TR-34

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Определяется по ТТК (Э)**<br>Активности: **export.{key}.host** | |
| Key Block LMK | | Авторизация: **Требуется**<br>Активности: **export.{key}.host** |

**Описание функции:** Экспорт симметричного ключа с использованием асимметричных методов с единого узла распространения ключей (Key Distribution Host, KDH) на устройство, принимающее ключи (Key Receiving Device, KRD).

Поддерживаются следующие типы симметричных ключей:

- 112/168-битные ключи DES
- 128-битные ключи AES

**Авторизация:**

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Команда проверяет флаг 'Э' (экспорт) для заданного типа ключа в таблице типов ключей (ТТК, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **export.{key}.host** должна быть авторизована, где 'key' — код типа экспортируемого ключа. | HSM должен находиться в авторизованном состоянии, либо активность **export.{key}.host** должна быть авторизована, где 'key' — значение *Использования ключа* экспортируемого ключа. |

**Примечания:** Подробнее о поддержке алгоритма RSA см. в «КриптоПро HSM. Руководство программиста».

Выходной Key Block TR-34 включает в себя заголовок Key Block TR-31, но не включает полного Key Block, поэтому поле длины Key Block в заголовке всегда имеет значение '0000'. В случае *Идентификатора схемы* = '0' команда вычисляет хэш-значение для enveloped data, не включая поля длины и тега SEQUENCE.

В случае *Идентификатора схемы* = '1' команда вычисляет хэш-значение для enveloped data, включая поля длины и тега SEQUENCE.
*Идентификатор схемы* = '2' аналогичен *Идентификатору схемы* = '1', однако в ответе поле `encryptedContent` в формате ASN.1 является элементом того же уровня, что и поле `contentEncryptionAlgorithm`, а не является его частью.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable export of a ZMK` | `Yes [Y]` | Доступен экспорт ZMK. |
| (влияет на параметры: *Тип ключа*) | `No [N]` | Экспорт ZMK невозможен. |
| `Enforce minimum key strength of 2048-bits for RSA` | `Yes [Y]` | Длина модуля закрытого ключа KDH должна быть не менее 2048 бит. |
| (влияет на параметры: *Закрытый ключ KDH*) | `No [N]` | Ограничения на длину модуля закрытого ключа KDH не накладываются. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'B8'.</td></tr>
<tr><td>Идентификатор схемы</td><td>1 N</td><td>'0': X9 TR-34:2012<br>'1': X9 TR-34:2019<br>'2': X9 TR-34:2019 (включая поправку: <code>encryptedContent</code> и <code>contentEncryptionAlgorithm</code> являются элементами одного уровня).</td></tr>
<tr><td>Тип ключа</td><td>3 H</td><td>Тип экспортируемого ключа. Перечень допустимых значений см. в таблице типов ключей.</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Ключ</td><td></td><td>Ключ, экспортируемый с KDH на KRD, зашифрованный под LMK.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Ключ, зашифрованный под соответствующим LMK, определяемым значением поля Тип ключа.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>Любое допустимое значение</td><td>'T', 'A'</td><td>Любое допустимое значение</td></tr>
</table></td></tr>
<tr><td>KDH Credential</td><td>n B</td><td>Уникальное имя и серийный номер сертификата в BER-кодировке для идентификации KDH.<br>KDH Credential::= SEQUENCE{<br>issuer Name,<br>serialNumber CertificateSerialNumber<br>}</td></tr>
<tr><td>Алгоритм зашифрования ключа</td><td>2 N</td><td>'00': 3DES-CBC<br>'01': AES128-CBC</td></tr>
<tr><td>Алгоритм зашифрования ключа экспорта</td><td>2 N</td><td>'00': RSA OAEP</td></tr>
<tr><td>Количество получателей KRD</td><td>2 N</td><td>Допустимое значение: '01'.</td></tr>
<tr><td colspan="3">Следующие поля повторяются для каждого получателя KRD:</td></tr>
<tr><td>KRD Credential</td><td>n B</td><td>Уникальное имя и серийный номер сертификата в BER-кодировке для идентификации получателя KRD.<br>KRD Credential::= SEQUENCE{<br>issuer Name,<br>serialNumber CertificateSerialNumber<br>}</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае Алгоритма зашифрования ключа экспорта = '00':</td></tr>
<tr><td>Открытый ключ KRD</td><td>n B</td><td>Открытый ключ KRD, BER в формате ASN.1 (последовательность модуля и экспоненты). Длина модуля — 2048 бит, значение экспоненты — 65537.</td></tr>
<tr><td>Длина OAEP Label</td><td>2 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td>OAEP Label</td><td>n B</td><td>Опционально; присутствует только в случае Длины OAEP Label ≠ '00'.</td></tr>
<tr><td>Разделитель OAEP Label</td><td>1 A</td><td>Значение ';'. Опционально; присутствует, только если присутствует предыдущее поле.</td></tr>
</table>

<table>
<tr><td>Флаг закрытого ключа</td><td>2 N</td><td>Указывает расположение закрытого ключа, используемого для генерации подписи:<br>'00' .. '20': индекс ключа в хранилище<br>'99': используется ключ, переданный в команде</td></tr>
<tr><td>Длина закрытого ключа KDH</td><td></td><td>Опционально; присутствует только в случае Флага закрытого ключа = '99'.</td></tr>
<tr><td></td><td>4 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
<tr><td>Закрытый ключ KDH</td><td></td><td>Опционально; присутствует только в случае Флага закрытого ключа = '99'.<br>Закрытый ключ, используемый для генерации подписи.</td></tr>
<tr><td></td><td>n B</td><td>Закрытый ключ, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B</td><td>Закрытый ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03'</td><td>'R'</td><td>'S', 'N'</td></tr>
</table></td></tr>
<tr><td>Идентификатор режима дополнения</td><td>2 N</td><td>'01': PKCS#1 v2.2 method EMSA-PKCS1-v1_5</td></tr>
<tr><td>Идентификатор алгоритма хэширования</td><td>1 N</td><td>'0': SHA-256</td></tr>
<tr><td>Длина случайных данных</td><td>2 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td>Случайные данные</td><td>n B</td><td>Опционально; присутствует только в случае Длины случайных данных ≠ '00'. Случайные данные, полученные от KRD.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае использования Variant LMK:</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '&'. Опционально; должен присутствовать в случае экспорта ключа, зашифрованного под Variant LMK. Если присутствует, следующие поля обязательны.</td></tr>
<tr><td>Использование ключа</td><td>2 A</td><td>Поле Использование ключа, включаемое в заголовок TR-34 Key Block экспортированного ключа. Любое допустимое значение для указанного типа ключа. Допустимые значения см. в таблице использования ключей.</td></tr>
<tr><td>Режим использования</td><td>1 A</td><td>Поле Режим использования, включаемое в заголовок TR-34 Key Block экспортированного ключа. Любое допустимое значение для указанного Использования ключа. Допустимые значения см. в таблице режимов использования ключей.</td></tr>
<tr><td>Номер версии ключа</td><td>2 N</td><td>Поле Номер версии ключа, включаемое в заголовок TR-34 Key Block экспортированного ключа.<br>Допустимые значения: '00' .. '99'.</td></tr>
<tr><td>Экспортируемость</td><td>1 A</td><td>Поле Экспортируемость, включаемое в заголовок TR-34 Key Block экспортированного ключа.<br>Допустимые значения: 'N' или 'S'.</td></tr>
<tr><td>Количество опциональных блоков</td><td>2 N</td><td>Количество опциональных блоков, включаемых в заголовок TR-34 Key Block экспортированного ключа.<br>Допустимые значения: '00' .. '02'.</td></tr>
<tr><td colspan="3">Следующие 3 поля определяются для каждого опционального блока.<br>Примечание: Если Количество опциональных блоков = '00', следующие 3 поля не присутствуют.</td></tr>
<tr><td>Идентификатор блока</td><td>2 A</td><td>Допустимые значения: 'KS' или 'KV'.</td></tr>
<tr><td>Длина блока</td><td>2 H</td><td>Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует.</td></tr>
</table>

| | | |
|---|---|---|
| Данные блока | n A | Данные блока. |
| Разделитель | 1 A | Значение '!'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор (ID) версии Key Block | 1 A | ID версии Key Block (подробнее см. ASC X9 TR 31-2018):<br>'A': Key Block, защищённый методом Key Variant Binding 2005<br>'B': Key Block, защищённый методом Key Derivation Binding 2010<br>'C': Key Block, защищённый методом Key Variant Binding 2010<br>'D': Key Block, защищённый методом AES Key Derivation Binding |
| Следующие поля присутствуют только в случае использования Key Block LMK: | | |
| Разделитель | 1 A | Значение '&'. Опционально; если присутствует, следующее поле обязательно. |
| Новое значение экспортируемости | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block. Допустимое значение: 'N'. |
| Разделитель | 1 A | Значение '!'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор (ID) версии Key Block | 1 A | ID версии Key Block (подробнее см. ASC X9 TR 31-2018):<br>'A': Key Block, защищённый методом Key Variant Binding 2005<br>'B': Key Block, защищённый методом Key Derivation Binding 2010<br>'C': Key Block, защищённый методом Key Variant Binding 2010<br>'D': Key Block, защищённый методом AES Key Derivation Binding |
| Разделитель | 1 A | Значение '*'. Опционально; если присутствует, следующее поле обязательно. |
| Новое использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block. Используется в случае *Ключа* с *Использованием ключа* = '51', '52' или '54'. Допустимые значения: 'K0' или 'K1'. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'B9'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Недопустимый тип ключа<br>'D1': Недопустимый идентификатор схемы<br>'D3': Ошибка Key Block ключа<br>'D4': Недопустимое количество получателей<br>'D5': KDH Credential не соответствует правилам кодирования BER<br>'D6': Недопустимый алгоритм зашифрвоания ключа<br>'D7': Недопустимый алгоритм зашифрования ключа экспорта<br>'D8': KRD Credential не соответствует правилам кодирования BER<br>'D9': Открытый ключ KRD не соответствует правилам кодирования BER<br>'DA': Недопустимая длина модуля или значение экспоненты открытого ключа KRD<br>'DB': Недопустимая длина OAEP Label<br>'DC': Ошибка Key Block закрытого ключа KDH<br>'DD': Недопустимый идентификатор режима дополнения<br>'DE': Недопустимый идентификатор алгоритма хэширования<br>'DF': Недопустимая длина случайных данных<br>'E0': Недопустимый идентификатор версии Key Block<br>'E1': Недопустимое новое значение экспортируемости или новое использование ключа<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D3' или 'DC': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |

| Следующее 5 полей присутствуют только в случае *Кода ошибки* = '00': | | |
|---|---|---|
| Аутентифицированные атрибуты | n B | Строка в BER-кодировке, содержащая следующие атрибуты, для которых было вычислено и подписано хэш-значение SHA-256:<br>• случайные данные<br>• заголовок Key Block<br>• хэш-значение, вычисленное для enveloped data |
| KCV | 3 B | Проверочное значение экспортированного ключа. |
| Enveloped data | n B | Данные в BER-кодировке. |
| Длина подписи | 4 N | Длина (в байтах) следующего поля. |
| Подпись | n B | Значение подписи для данных в поле *Аутентифицированные атрибуты*. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 6 Команды генерации PIN и Offset

Команды 'EE', 'JA', 'BK' и 'FW' поддерживают возможность проверки, является ли сгенерированный/выработанный или установленный пользователем PIN «слабым» (т.е. легко подбираемые нарушителем). HSM поддерживает 3 метода выявления «слабых» PIN:

• путем проверки наличия PIN в глобальном списке «слабых» PIN, загруженного в HSM с помощью команды 'BM'
• путем проверки наличия PIN в локальном списке «слабых» PIN, который передается в команде генерации или выработки нового PIN
• путем проверки PIN на соответствие определенным правилам — PIN считается «слабым», если выполняется хотя бы одно из условий:
  – больше 50% цифр PIN одинаковые (например, 1111, 0222, 3301 и т.п.)
  – если весь PIN является последовательностью чисел, расположенных в порядке возрастания или убывания (например, 1234, 8765 и т.п.)

Следующие команды хоста используются для генерации PIN/Offset:

## [EE] — Выработка PIN с использованием метода IBM 3624

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация PIN длиной от 4 до 12 цифр с использованием метода IBM 3624 (IBM Offset Method).

**Примечания:** PIN вырабатывается из значения IBM Offset в дополнение к другим данным.

По умолчанию предполагается использование зашифрованных таблиц децимализации, однако возможно использование незашифрованных таблиц децимализации (см. описание настройки `Decimalization Table`). Рекомендуется использование зашифрованных таблиц децимализации.

Команда никогда не возвращает код ошибки 00 в случае успеха, так как ключи PVK с алгоритмом DES не поддерживаются. Вместо кода 00 в случае успеха возвращается код ошибки 02 (используется ключ PVK с алгоритмом 2DES или 3DES).

Опционально команда гарантирует, что сгенерированный PIN отсутствует в списке «слабых» PIN (см. описание настройки `Enable Weak PIN checking`).

При использовании 3DES LMK PIN-блок, зашифрованный под LMK, формируется в результате криптографического преобразования PIN и номера карты (PAN).

В случае AES LMK используется формат PIN-блока ISO Format 4.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Decimalization tables`<br>(влияет на параметры: *Таблица децимализации*) | `Encrypted [E]`<br>`(по умолчанию)` | Таблица децимализации, подаваемая на вход, должна быть зашифрована (с помощью консольной команды ED) и состоять из 16 шестнадцатеричных символов (для Variant LMK или 3DES Key Block LMK) или 'L' + 32 шестнадцатеричных символов (для AES Key Block LMK). |

| | | |
|---|---|---|
| | `Plaintext [P]` | Таблица децимализации, подаваемая на вход, должна быть незашифрована и состоять из 16 десятичных символов. |
| `Enable Decimalization Table checks` | `Yes [Y]` `(по умолчанию)` | Выполняется проверка таблицы децимализации, подаваемой на вход: таблица децимализации должна содержать не менее 8 различных цифр, и каждая цифра должна повторяться не более 4 раз. Если требование не выполняется, возвращается ошибка 25. |
| | `No [N]` | Проверка таблицы децимализации не выполняется. |
| `Enable Weak PIN checking`<br>(влияет на параметры: *Разделитель, Количество «слабых» PIN, Длина «слабых» PIN, Список «слабых» PIN*) | `Yes [Y]` | Выполнение команды зависит от следующих настроек безопасности:<br>• `Check new PINs using global list of weak PINs: [Yes/No]`<br>• `Check new PINs using local list of weak PINs: [Yes/No]`<br>*Примечание:* перед проверкой локального списка «слабых» PIN проверяется соответствие длины проверяемого PIN параметру *Длина «слабых» PIN*.<br>• `Check new PINs using rules: [Yes/No]`<br>Если в результате проверки PIN присутствует в каком-либо списке «слабых» PIN, возвращается код ошибки 86. Если не прошла проверка PIN по правилам, возвращается код ошибки 85. |
| | `No [N]` `(по умолчанию)` | При генерации PIN не проверяются локальный и глобальный списки «слабых» PIN. Если в команде передается локальный список «слабых» PIN, возвращается код ошибки 15. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **КОМАНДА** |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'EE'. |
| PVK | | PVK, используемый для генерации PIN. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | PVK, зашифрованный под LMK 14-15/0. |
| | 'S' + n A | PVK должен соответствовать следующему формату:<br>Использование ключа: 'V1'; Алгоритм: 'T'; Режим использования: 'C', 'G', 'N' |
| Offset | 12 H | Значение Offset, выровненное по левому краю и дополненное 'F'. |
| Проверочная длина | 2 N | Количество цифр в значении Offset. |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| Таблица децимализации | 16 N<br>или | 16 N при использовании незашифрованной таблицы децимализации. |
| | 16 H<br>или | 16 H при использовании зашифрованной таблицы децимализации и Variant LMK или 3DES Key Block LMK. |
| | 'L' + 32 H | 'L' + 32 H при использовании зашифрованной таблицы децимализации и AES Key Block LMK. |
| Данные для проверки PIN | 12 A | Пользовательские данные, состоящие из шестнадцатиричных символов и символа 'N', который указывает HSM, где расположить последние 5 цифр PAN. |
| | или | или |
| | 'P' + 16 H | Пользовательские данные, состоящие из ASCII символа 'P', дополненного 16 шестнадцатеричными цифрами, которые будут использоваться в качестве входа для алгоритма генерации PIN. |
| Разделитель | 1 A | Значение '*'. Присутствует, только если присутствуют поля ниже. |
| Количество «слабых» PIN | 2 N | Количество PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '00' .. '99'. |
| Длина «слабых» PIN | 2 N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Длина каждого PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '04' .. '12'. |
| Список «слабых» PIN | n N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Список «слабых» PIN. Длина поля вычисляется как *Количество «слабых» PIN * Длина «слабых» PIN.* |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'EF'. |
| Код ошибки | 2 H | '02': Без ошибок<br>'06': Недопустимая длина Offset<br>'10': Нарушена четность PVK<br>'68': Команда недоступна<br>'81': Несоответствие длины PIN<br>'86': PIN присутствует в списке «слабых» PIN<br>или другой стандартный код ошибки. |
| PIN | | Сгенерированный PIN, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [JA] — Генерация случайного PIN

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация случайного PIN длиной от 4 до 12 цифр.

**Примечания:** Если длина PIN не указана в команде, генерируется 4-значный PIN.

При использовании 3DES LMK указанная в команде длина PIN не должна превышать значение, установленное консольной командой CS.

Опционально команда гарантирует, что сгенерированный PIN отсутствует в списке «слабых» PIN.

При использовании 3DES LMK PIN-блок, зашифрованный под LMK, формируется в результате криптографического преобразования PIN и номера карты (PAN).

В случае AES LMK используется формат PIN-блока ISO Format 4.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *Длина PIN, PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |

| | | |
|---|---|---|
| `Enable Weak PIN checking`<br>(влияет на параметры: *Разделитель, Количество «слабых» PIN, Длина «слабых» PIN, Список «слабых» PIN*) | `Yes [Y]` | Выполнение команды зависит от следующих настроек безопасности:<br>• `Check new PINs using global list of weak PINs: [Yes/No]`<br>• `Check new PINs using local list of weak PINs: [Yes/No]`<br>*Примечание:* перед проверкой локального списка «слабых» PIN проверяется соответствие длины проверяемого PIN параметру *Длина «слабых» PIN*.<br>• `Check new PINs using rules: [Yes/No]`<br>Если в результате проверки PIN присутствует в каком-либо списке «слабых» PIN, возвращается код ошибки 86. Если не прошла проверка PIN по правилам, возвращается код ошибки 85. |
| | `No [N]`<br>`(по умолчанию)` | При генерации PIN не проверяются локальный и глобальный списки «слабых» PIN. Если в команде передается локальный список «слабых» PIN, возвращается код ошибки 15. |

| Параметр | Формат | Описание |
|---|---|---|
| | **КОМАНДА** | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'JA'. |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| Длина PIN | 2 N | Опционально; если отсутствует, генерируется 4-значный PIN.<br>Допустимые значения: '04' .. '12'. |
| Разделитель | 1 A | Значение '*'. Присутствует, только если присутствуют поля ниже. |
| Количество «слабых» PIN | 2 N | Количество PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '00' .. '99'. |
| Длина «слабых» PIN | 2 N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Длина каждого PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '04' .. '12'. |
| Список «слабых» PIN | n N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Список «слабых» PIN. Длина поля вычисляется как *Количество «слабых» PIN * Длина «слабых» PIN*. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'JB'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Некорректное количество «слабых» PIN<br>'68': Команда недоступна<br>'81': Несоответствие длины PIN<br>или другой стандартный код ошибки. |
| PIN | | Сгенерированный PIN, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [DE] — Генерация IBM Offset (для PIN, зашифрованного под LMK)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация PIN Offset с использованием метода IBM 3624 (IBM Offset Method). PIN, для которого вычисляется Offset, должен быть зашифрован под LMK.

**Примечания:** По умолчанию предполагается использование зашифрованных таблиц децимализации, однако возможно использование незашифрованных таблиц децимализации (см. описание настройки `Decimalization Table`). Рекомендуется использование зашифрованных таблиц децимализации.

По умолчанию проверяется корректность таблицы децимализации в соответствии со следующим правилом: "таблица децимализации должна состоять из 16 цифр, при этом должна содержать не менее 8 различных цифр, и каждая цифра может повторяться не более 4 раз". Если данные требования не выполнены, возвращается ошибка 25. Проверка корректности таблицы может быть отключена (см. описание настройки `Decimalization Table checks`). Отключение данной проверки не рекомендуется.

Команда никогда не возвращает код ошибки 00 в случае успеха, так как ключи PVK с алгоритмом DES не поддерживаются. Вместо кода 00 в случае успеха возвращается код ошибки 02 (используется ключ PVK с алгоритмом 2DES или 3DES).

При использовании 3DES LMK PIN-блок, зашифрованный под LMK, формируется в результате криптографического преобразования PIN и номера карты (PAN).

В случае AES LMK используется формат PIN-блока ISO Format 4.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |

| | | |
|---|---|---|
| `Decimalization tables`<br><br>(влияет на параметры: *Таблица децимализации*) | `Encrypted [E]` `(по умолчанию)` | Таблица децимализации, подаваемая на вход, должна быть зашифрована (с помощью консольной команды ED) и состоять из 16 шестнадцатеричных символов (для Variant LMK или 3DES Key Block LMK) или 'L' + 32 шестнадцатеричных символов (для AES Key Block LMK). |
| | `Plaintext [P]` | Таблица децимализации, подаваемая на вход, должна быть незашифрована и состоять из 16 десятичных символов. |
| `Enable Decimalization Table checks` | `Yes [Y]` `(по умолчанию)` | Выполняется проверка таблицы децимализации, подаваемой на вход: таблица децимализации должна содержать не менее 8 различных цифр, и каждая цифра должна повторяться не более 4 раз. Если требование не выполняется, возвращается ошибка 25. |
| | `No [N]` | Проверка таблицы децимализации не выполняется. |
| `Enable variable length PIN offset`<br><br>(влияет на параметры: *Offset*) | `Yes [Y]` | Длина сгенерированного Offset соответствует длине входного PIN. |
| | `No [N]` `(по умолчанию)` | Длина генерируемого Offset определяется значением параметра *Проверочная длина*. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'DE'. |
| PVK | | PVK, используемый для генерации Offset. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | PVK, зашифрованный под LMK 14-15/0. |
| | 'S' + n A | PVK должен соответствовать следующему формату:<br>Использование ключа: 'V1'; Алгоритм: 'T'; Режим использования: 'C', 'G', 'N' |
| PIN | | PIN, для которого генерируется Offset, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Проверочная длина | 2 N | Если выставлена настройка `Enable variable length PIN offset: No`, определяет длину генерируемого значения Offset. |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| Таблица децимализации | 16 N<br>или | 16 N при использовании незашифрованной таблицы децимализации. |

| | | |
|---|---|---|
| | 16 H<br>или | 16 H при использовании зашифрованной таблицы децимализации и Variant LMK или 3DES Key Block LMK. |
| | 'L' + 32 H | 'L' + 32 H при использовании зашифрованной таблицы децимализации и AES Key Block LMK. |
| Данные для проверки PIN | 12 A | Пользовательские данные, состоящие из шестнадцатиричных символов и символа 'N', который указывает HSM, где расположить последние 5 цифр PAN. |
| | или | или |
| | 'P' + 16 H | Пользовательские данные, состоящие из ASCII символа 'P', дополненного 16 шестнадцатеричными цифрами, которые будут использоваться в качестве входа для алгоритма генерации PIN. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'DF'. |
| Код ошибки | 2 H | '02': Без ошибок<br>'10': Нарушена четность PVK<br>'68': Команда недоступна<br>'81': Несоответствие длины PIN<br>или другой стандартный код ошибки. |
| Offset | 12 H | Сгенерированное значение Offset, выровненное по левому краю и дополненное 'F'. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [BK] — Генерация IBM Offset (для терминального PIN, зашифрованного под ZPK/TPK)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация PIN Offset с использованием метода IBM 3624 (IBM Offset Method). PIN, для которого вычисляется Offset, должен быть представлен в виде зашифрованного PIN-блока.

**Примечания:** По умолчанию предполагается использование зашифрованных таблиц децимализации, однако возможно использование незашифрованных таблиц децимализации (см. описание настройки `Decimalization Table`). Рекомендуется использование зашифрованных таблиц децимализации.

По умолчанию проверяется корректность таблицы децимализации в соответствии со следующим правилом: "таблица децимализации должна состоять из 16 цифр, при этом должна содержать не менее 8 различных цифр, и каждая цифра может повторяться не более 4 раз". Если данные требования не выполнены, возвращается ошибка 25. Проверка корректности таблицы может быть отключена (см. описание настройки `Decimalization Table checks`). Отключение данной проверки не рекомендуется.

Команда никогда не возвращает код ошибки 00 в случае успеха, так как ключи PVK с алгоритмом DES не поддерживаются. Вместо кода 00 в случае успеха возвращается код ошибки 02 (используется ключ PVK с алгоритмом 2DES или 3DES).

Опционально команда проверяет наличие переданного в команде PIN в списке «слабых» PIN.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Decimalization tables` | `Encrypted [E]` `(по умолчанию)` | Таблица децимализации, подаваемая на вход, должна быть зашифрована (с помощью консольной команды ED) и состоять из 16 шестнадцатеричных символов (для Variant LMK или 3DES Key Block LMK) или 'L' + 32 шестнадцатеричных символов (для AES Key Block LMK). |
| | `Plaintext [P]` | Таблица децимализации, подаваемая на вход, должна быть незашифрована и состоять из 16 десятичных символов. |
| `Enable Decimalization Table checks` | `Yes [Y]` `(по умолчанию)` | Выполняется проверка таблицы децимализации, подаваемой на вход: таблица децимализации должна содержать не менее 8 различных цифр, и каждая цифра должна повторяться не более 4 раз. Если требование не выполняется, возвращается ошибка 25. |
| | `No [N]` | Проверка таблицы децимализации не выполняется. |
| `Enable variable length PIN offset` | `Yes [Y]` | Длина сгенерированного Offset соответствует длине входного PIN. |
| (влияет на параметры: *Offset*) | `No [N]` `(по умолчанию)` | Длина генерируемого Offset определяется значением параметра *Проверочная длина*. |

| | | |
|---|---|---|
| `Enable Weak PIN checking`<br>(влияет на параметры: *Разделитель, Количество «слабых» PIN, Длина «слабых» PIN, Список «слабых» PIN*) | `Yes [Y]` | Выполнение команды зависит от следующих настроек безопасности:<br>• `Check new PINs using global list of weak PINs: [Yes/No]`<br>• `Check new PINs using local list of weak PINs: [Yes/No]`<br>*Примечание:* перед проверкой локального списка «слабых» PIN проверяется соответствие длины проверяемого PIN параметру *Длина «слабых» PIN*.<br>• `Check new PINs using rules: [Yes/No]`<br>Если в результате проверки PIN присутствует в каком-либо списке «слабых» PIN, возвращается код ошибки 86. Если не прошла проверка PIN по правилам, возвращается код ошибки 85. |
| | `No [N]`<br>`(по умолчанию)` | При генерации PIN не проверяются локальный и глобальный списки «слабых» PIN. Если в команде передается локальный список «слабых» PIN, возвращается код ошибки 15. |
| `Restrict PIN block usage for PCI HSM Compliance`<br>(влияет на параметры: *Код формата PIN-блока*) | `Yes [Y]` | Допускается использовать только определенные форматы PIN-блока в соответствии с требованиями ISO 9564/ANSI X9.8 и PCI HSM. |
| | `No [N]` | Ограничения на формат PIN-блока не накладываются. |
| `Enforce key type 002 separation for PCI HSM compliance`<br>(влияет на параметры: *Тип ключа шифрования PIN-блока, Ключ шифрования PIN-блока*) | `Yes [Y]` | TPK зашифрован под LMK 36-37/7. |
| | `No [N]` | TPK зашифрован под LMK 14-15/0. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'BK'.</td></tr>
<tr><td rowspan="3">Тип ключа шифрования PIN-блока</td><td rowspan="3">3 H</td><td>Если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: No</code>:<br>'001': ZPK (зашифрованный под LMK 06-07/0)<br>'002': TPK (зашифрованный под LMK 14-15/0)</td></tr>
<tr><td>Если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: Yes</code>:<br>'001': ZPK (зашифрованный под LMK 06-07/0)<br>'70D': TPK (зашифрованный под LMK 36-37/7)</td></tr>
<tr><td>Значение 'FFF'.</td></tr>
<tr><td rowspan="3">Ключ шифрования PIN-блока</td><td></td><td>Ключ, под которым зашифрован PIN-блок (ZPK или TPK).</td></tr>
<tr><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Ключ шифрования PIN-блока, зашифрованный под соответствующим LMK, определяемым значением поля Тип ключа шифрования PIN-блока.</td></tr>
<tr><td>'S' + n A</td><td>Ключ шифрования PIN-блока должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'P0', '71', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td rowspan="3">PVK</td><td></td><td>PVK, используемый для генерации Offset.</td></tr>
<tr><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>PVK, зашифрованный под LMK 14-15/0.</td></tr>
<tr><td>'S' + n A</td><td>PVK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'V1'</td><td>'T'</td><td>'C', 'G', 'N'</td></tr>
</table></td></tr>
<tr><td>PIN-блок</td><td>16 H<br>или<br>32 H</td><td>PIN-блок, для которого генерируется Offset, зашифрованный под Ключом шифрования PIN-блока.<br>Если Ключ шифрования PIN-блока DES, то размер поля 16H.<br>Если Ключ шифрования PIN-блока AES, то размер поля 32H.</td></tr>
<tr><td>Код формата PIN-блока</td><td>2 N</td><td>Код формата PIN-блока.<br>Если выставлена настройка <code>Restrict PIN block usage for PCI compliance: Yes</code>, допускаются только следующие значения:<br>'01': ISO format 0<br>'47': ISO format 3<br>'48': ISO format 4</td></tr>
<tr><td>Проверочная длина</td><td>2 N</td><td>Если выставлена настройка <code>Enable variable length PIN offset: No</code>, определяет длину генерируемого значения Offset.</td></tr>
<tr><td rowspan="4">Номер карты (PAN)</td><td></td><td>Номер карты (PAN), используемый при формировании PIN-блока.</td></tr>
<tr><td>n N</td><td>Если Код формата PIN-блока = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель.</td></tr>
<tr><td>или</td><td></td></tr>
<tr><td>12 N</td><td>Для всех остальных значений поля Код формата PIN-блока:<br>12 крайних правых цифр PAN, за исключением контрольной цифры.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует, только если Код формата PIN-блока = '48'.</td></tr>
</table>

| | | |
|---|---|---|
| Таблица децимализации | 16 N<br>или | 16 N при использовании незашифрованной таблицы децимализации. |
| | 16 H<br>или | 16 H при использовании зашифрованной таблицы децимализации и Variant LMK или 3DES Key Block LMK. |
| | 'L' + 32 H | 'L' + 32 H при использовании зашифрованной таблицы децимализации и AES Key Block LMK. |
| Данные для проверки PIN | 12 A | Пользовательские данные, состоящие из шестнадцатиричных символов и символа 'N', который указывает HSM, где расположить последние 5 цифр PAN. |
| | или | или |
| | 'P' + 16 H | Пользовательские данные, состоящие из ASCII символа 'P', дополненного 16 шестнадцатеричными цифрами, которые будут использоваться в качестве входа для алгоритма генерации PIN. |
| Разделитель | 1 A | Значение '*'. Присутствует, только если присутствуют поля ниже. |
| Количество «слабых» PIN | 2 N | Количество PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '00' .. '99'. |
| Длина «слабых» PIN | 2 N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Длина каждого PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '04' .. '12'. |
| Список «слабых» PIN | n N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Список «слабых» PIN. Длина поля вычисляется как *Количество «слабых» PIN * Длина «слабых» PIN*. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'BL'. |
| Код ошибки | 2 H | '02': Без ошибок<br>'03': Некорректное количество «слабых» PIN<br>'10': Нарушена четность TPK или ZPK<br>'11': Нарушена четность PVK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>'81': Несоответствие длины PIN<br>'86': PIN присутствует в списке «слабых» PIN<br>или другой стандартный код ошибки. |
| Offset | 12 H | Сгенерированное значение Offset, выровненное по левому краю и дополненное 'F'. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [DG] — Генерация ABA PVV (для PIN, зашифрованного под LMK)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация 4-значного PVV с использованием метода ABA. PIN, для которого вычисляется PVV, должен быть зашифрован под LMK.

**Примечания:** При использовании 3DES LMK PIN-блок, зашифрованный под LMK, формируется в результате криптографического преобразования PIN и номера карты (PAN).

В случае AES LMK используется формат PIN-блока ISO Format 4.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **КОМАНДА** |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'DG'. |
| PVK | | PVK, используемый для генерации PVV. |
| | 32 H<br>или<br>'U' + 32 H | PVK, зашифрованный под LMK 14-15/0. |
| | 'S' + n A | PVK является ключом 2DES и должен соответствовать следующему формату:<br>Использование ключа: 'V2'; Алгоритм: 'T'; Режим использования: 'C', 'G', 'N' |
| PIN | | PIN, для которого вычисляется PVV, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| PVKI | 1 N | Индекс ключа проверки PIN.<br>В соответствии с определением Visa допустимые значения '0' .. '6'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'DH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность PVK<br>'27': Алгоритм PVK отличен от 2DES<br>'68': Команда недоступна<br>'81': Несоответствие длины PIN<br>или другой стандартный код ошибки. |
| PVV | 4 N | Сгенерированное значение PVV. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [FW] — Генерация ABA PVV (для PIN, выбранного пользователем)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация 4-значного PVV с использованием метода ABA. PIN, для которого вычисляется PVV, должен быть зашифрован под ключом шифрования PIN-блока.

**Примечания:** Опционально команда проверяет, что выбранный пользователем PIN отсутствует в списке «слабых» PIN.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable Weak PIN checking`<br>(влияет на параметры: *Разделитель, Количество «слабых» PIN, Длина «слабых» PIN, Список «слабых» PIN*) | `Yes [Y]` | Выполнение команды зависит от следующих настроек безопасности:<br>• `Check new PINs using global list of weak PINs: [Yes/No]`<br>• `Check new PINs using local list of weak PINs: [Yes/No]`<br>*Примечание:* перед проверкой локального списка «слабых» PIN проверяется соответствие длины проверяемого PIN параметру *Длина «слабых» PIN*.<br>• `Check new PINs using rules: [Yes/No]`<br>Если в результате проверки PIN присутствует в каком-либо списке «слабых» PIN, возвращается код ошибки 86. Если не прошла проверка PIN по правилам, возвращается код ошибки 85. |
| | `No [N]`<br>`(по умолчанию)` | Для передаваемого PIN не проверяются локальный и глобальный списки «слабых» PIN. Если в команде передается локальный список «слабых» PIN, возвращается код ошибки 15. |
| `Restrict PIN block usage for PCI HSM Compliance`<br>(влияет на параметры: *Код формата PIN-блока*) | `Yes [Y]` | Допускается использовать только определенные форматы PIN-блока в соответствии с требованиями ISO 9564/ANSI X9.8 и PCI HSM. |
| | `No [N]` | Ограничения на формат PIN-блока не накладываются. |
| `Enforce key type 002 separation for PCI HSM compliance`<br>(влияет на параметры: *Тип ключа шифрования PIN-блока, Ключ шифрования PIN-блока*) | `Yes [Y]` | TPK зашифрован под LMK 36-37/7. |
| | `No [N]` | TPK зашифрован под LMK 14-15/0. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'FW'.</td></tr>
<tr><td rowspan="4">Тип ключа шифрования PIN-блока</td><td rowspan="4">3 H</td><td>Если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: No</code>:<br>'001': ZPK (зашифрованный под LMK 06-07/0)<br>'002': TPK (зашифрованный под LMK 14-15/0)</td></tr>
<tr><td>Если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: Yes</code>:<br>'001': ZPK (зашифрованный под LMK 06-07/0)<br>'70D': TPK (зашифрованный под LMK 36-37/7)</td></tr>
<tr><td>Значение 'FFF'.</td></tr>
<tr><td>Ключ, под которым зашифрован PIN-блок (ZPK или TPK).</td></tr>
<tr><td rowspan="2">Ключ шифрования PIN-блока</td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Ключ шифрования PIN-блока, зашифрованный под соответствующим LMK, определяемым значением поля Тип ключа шифрования PIN-блока.</td></tr>
<tr><td>'S' + n A</td><td>Ключ шифрования PIN-блока должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'P0', '71', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>PVK</td><td></td><td>PVK, используемый для генерации PVV.</td></tr>
<tr><td rowspan="2">32 H<br>или<br>'U' + 32 H</td><td rowspan="2">PVK, зашифрованный под LMK 14-15/0.</td></tr>
<tr><td>'S' + n A</td><td>PVK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'V2'</td><td>'T'</td><td>'C', 'G', 'N'</td></tr>
</table></td></tr>
<tr><td>PIN-блок</td><td>16 H<br>или<br>32 H</td><td>PIN, для которого генерируется PVV, зашифрованный под Ключом шифрования PIN-блока.<br>Если Ключ шифрования PIN-блока DES, то размер поля 16H.<br>Если Ключ шифрования PIN-блока AES, то размер поля 32H.</td></tr>
<tr><td>Код формата PIN-блока</td><td>2 N</td><td>Код формата PIN-блока.<br>Если выставлена настройка <code>Restrict PIN block usage for PCI compliance: Yes</code>, допускаются только следующие значения:<br>'01': ISO format 0<br>'47': ISO format 3<br>'48': ISO format 4</td></tr>
<tr><td rowspan="3">Номер карты (PAN)</td><td rowspan="3">n N<br><br>или<br><br>12 N</td><td rowspan="3">Номер карты (PAN), используемый при формировании PIN-блока.<br>Если Код формата PIN-блока = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель.<br>Для всех остальных значений поля Код формата PIN-блока:<br>12 крайних правых цифр PAN, за исключением контрольной цифры.</td></tr>
<tr></tr>
<tr></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует, только если Код формата PIN-блока = '48'.</td></tr>
<tr><td>PVKI</td><td>1 N</td><td>Индекс ключа проверки PIN.<br>В соответствии с определением Visa допустимые значения '0' .. '6'.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '*'. Присутствует, только если присутствуют поля ниже.</td></tr>
</table>

| | | |
|---|---|---|
| Количество «слабых» PIN | 2 N | Количество PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '00' .. '99'. |
| Длина «слабых» PIN | 2 N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Длина каждого PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '04' .. '12'. |
| Список «слабых» PIN | n N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Список «слабых» PIN. Длина поля вычисляется как *Количество «слабых» PIN * Длина «слабых» PIN.* |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'FX'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность TPK или ZPK<br>'11': Нарушена четность PVK<br>'27': Алгоритм PVK отличен от 2DES<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>'81': Несоответствие длины PIN<br>'86': PIN присутствует в списке «слабых» PIN<br>или другой стандартный код ошибки. |
| PVV | 4 N | Сгенерированное значение PVV. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [BM] — Загрузка списка «слабых» PIN

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Загрузка глобального списка «слабых» PIN в память HSM.

**Примечания:** Существует 9 уникальных списков «слабых» PIN, каждый из которых содержит перечень PIN определенной длины (4 .. 12). Все PIN в списке должны иметь одинаковую длину. В каждом списке может храниться до 99 PIN.

Команды, поддерживающие функцию проверки PIN с использованием списка «слабых» PIN, проверяют наличие PIN в глобальном списке «слабых» PIN, загруженном данной командой, только если выставлена настройка безопасности `Check new PINs using global list of weak PINs: Yes`.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'BM'. |
| Количество «слабых» PIN | 2 N | Количество PIN в глобальном списке «слабых» PIN ниже.<br>Допустимые значения: '00' .. '99'. |
| Длина «слабых» PIN | 2 N | Длина каждого PIN в глобальном списке «слабых» PIN ниже.<br>Допустимые значения: '04' .. '12'. |
| Список «слабых» PIN | n N | Глобальный список «слабых» PIN. Длина поля вычисляется как *Количество «слабых» PIN * Длина «слабых» PIN*. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'BN'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'41': Ошибка хранилища данных<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 7 Команды печати PIN-конвертов

HSM поддерживает функцию печати PIN-конвертов с использованием подключенного к HSM принтера.

PIN-конверты могут использоваться для безопасной передачи сгенерированного PIN держателю карты. Также конверты используются при необходимости передачи данных запроса о присвоении PIN (PIN Solicitation) в случае, когда держателю карты предоставляется возможность самостоятельно выбрать PIN (без использования устройств ввода для установки PIN). В этом случае передача заранее сгенерированного PIN держателю карты не требуется, достаточно только запроса PIN.

Данные, напечатанные в PIN-конвертах, недоступны хосту. Для подтверждения корректности печати данных HSM возвращает хосту соответствующие проверочные значения.

Для конфигурации принтера используется консольная команда CP.

Следующие команды хоста используются для поддержки операций печати PIN-конвертов:

## [PE] — Печать PIN/PIN и данных запроса

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Требуется** | |
| Активности: **pin.mailer.host** | |

**Описание функции:** Печать PIN/PIN и данных запроса с помощью подключенного к HSM принтера.

**Примечания:** Для выполнения команды принтер должен быть подключен к USB-порту HSM.
На HSM уже должен быть настроен формат печати.
В команде должно присутствовать как минимум одно поле печати.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'PE'. |
| Тип документа | 1 A | 'A': печать 1-ого документа (в формате 2 документа на листе)<br>'B': печать 2-ого документа (в формате 2 документа на листе)<br>'C': печать документа (в формате 1 документ на листе) |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| PIN | | PIN, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Поле печати 0 | n A | Поле печати определяется как *Поле печати 0* в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение ';'. |
| Поле печати 1 | n A | Поле печати определяется как *Поле печати 1* в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение ';'. |
| ... | ... | ... |
| ... | ... | ... |
| Последнее поле печати | n A | *Последнее поле печати*, определенное в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение '∼'. Опционально; должен присутствовать, если присутствует разделитель '%' ниже. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'PF'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'16': Принтер не готов/не подключен<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Проверочные значения PIN и ссылочного номера | L + 12 N | Проверочные значения PIN и ссылочного номера, вычисленные с использованием LMK. |

| | | |
|---|---|---|
| Код ответа принтера | 2 A | Значение 'PZ'. |
| Код ошибки принтера | 2 H | '00': Без ошибок<br>'41': Внутренняя аппаратная/программная ошибка<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [OA] — Печать запроса о присвоении PIN

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Требуется** | |
| Активности: **pin.mailer.host** | |

**Описание функции:** Печать запроса о присвоении PIN с помощью подключенного к HSM принтера.

**Примечания:** Для выполнения команды принтер должен быть подключен к USB-порту HSM.
На HSM уже должен быть настроен формат печати.
В команде должно присутствовать как минимум одно поле печати.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'OA'. |
| Тип документа | 1 A | 'A': печать 1-ого документа (в формате 2 документа на листе)<br>'B': печать 2-ого документа (в формате 2 документа на листе)<br>'C': печать документа (в формате 1 документ на листе) |
| Номер карты (PAN) | 12 N | 12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Поле печати 0 | n A | Поле печати определяется как *Поле печати 0* в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение ';'. |
| Поле печати 1 | n A | Поле печати определяется как *Поле печати 1* в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение ';'. |
| ... | ... | ... |
| ... | ... | ... |
| Последнее поле печати | n A | *Последнее поле печати*, определенное в определении формата печати (не должно содержать символов ';' или '∼'). |
| Разделитель | 1 A | Значение '∼'. Опционально; должен присутствовать, если присутствует разделитель '%' ниже. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'OB'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'16': Принтер не готов/не подключен<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |

| | | |
|---|---|---|
| Проверочное значение ссылочного номера | 12 N | Проверочное значение ссылочного номера, вычисленное с использованием LMK. |
| Код ответа принтера | 2 A | Значение 'OZ'. |
| Код ошибки принтера | 2 H | '00': Без ошибок<br>'41': Внутренняя аппаратная/программная ошибка или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [PG] — Криптографическая проверка команды печати PIN/PIN и данных запроса

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка корректности команды 'PE'.

**Примечания:** Рекомендуется проверять корректность команды 'PE', выполняемой одним HSM, с помощью команды 'PG', выполняемой другим HSM.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'PG'. |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| PIN | | PIN, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Проверочные значения PIN и ссылочного номера | L + 12 N | Проверочные значения PIN и ссылочного номера, вычисленные с использованием LMK. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'PH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [RC] — Криптографическая проверка команды печати запроса о присвоении PIN

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка корректности команды 'OA'.

**Примечания:** Рекомендуется проверять корректность команды 'OA', выполняемой одним HSM, с помощью команды 'RC', выполняемой другим HSM.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'RC'. |
| Номер карты (PAN) | 12 N | 12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Проверочное значение ссылочного номера | 12 N | Проверочное значение ссылочного номера, вычисленное с использованием LMK. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'RD'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 8 Команды обработки запросов PIN

Держателю карту может предоставляться возможность самостоятельно выбрать и назначить PIN. В этом случае он должен вернуть форму, содержащую выбранный PIN, и ссылочный номер, который используется вместо номера карты (PAN) для обеспечения безопасности. Ссылочный номер является результатом криптографического преобразования 10 последних цифр номера карты (PAN) за исключением контрольной цифры.

HSM обрабатывает полученные данные и возвращает хосту зашифрованный PIN и 10 последних цифр номера карты PAN за исключением контрольной цифры. Хост может сопоставить полученное от HSM и сохраненное значение номера карты (PAN) и сохранить зашифрованный PIN для последующей обработки.

Ссылочный номер является единственной ссылкой на PIN держателя карты, который вводится вручную. Поэтому необходимо обеспечивать корректность ввода PIN, например, с помощью двойного ввода или визуального сравнения значений.

В отличие от PIN корректность ссылочного номера может контролироваться хостом. Ссылочный номер состоит из 10 цифр и 2 контрольных цифр, которые могут быть верифицированы хостом во время или после ввода данных.

Данные запросов PIN обрабатываются HSM пакетно. Количество введенных записей должно быть больше или равно минимальному размеру пакета, установленному при настройке HSM. Каждый пакет содержит как минимум одну запись, которая состоит из 12-значного ссылочного номера (полученного из возвращенного конверта) и соответствующего PIN, выбранного держателем карты.

После загрузки пакета данных для каждой записи HSM зашифровывает PIN с использованием LMK 02-03 и расшифровывает ссылочный номер, получая значение 10 крайних правых цифр номера карты (PAN) за исключением контрольной цифры. Зашифрованный PIN и номер карты (PAN) возвращаются хосту.

HSM поддерживает следующую команду хоста для обработки данных запросов PIN:

| | |
|---|---|
| [QC] — Обработка данных запросов PIN | 161 |

## [QC] — Обработка данных запросов PIN

| Variant LMK ☒ | 3DES Key Block LMK ☑ |
|---|---|

**Описание функции:** Обработка группы запросов PIN.

**Примечания:** Данные запросов PIN обрабатываются пакетно. Количество передаваемых в команде записей должно быть больше или равно минимальному размеру пакета, установленному в настройке безопасности `Solicitation batch size` при конфигурации HSM, и меньше 1260.

Каждый пакет состоит как минимум из одной логической записи, которая включает 12-значный ссылочный номер и выбранный держателем карты PIN.

Ссылочный номер состоит из 10 цифр и 2 контрольных цифр.

HSM зашифровывает PIN под LMK 02-03 и расшифровывает ссылочный номер, получая значение 10 крайних правых цифр номера карты (PAN) за исключением контрольной цифры.

В ответе HSM возвращает хосту зашифрованный PIN и 10 последних цифр соответствующего номера карты (PAN). Порядок записей в ответе 'QD' случаен, таким образом выходные записи нельзя сопоставить с входными записями в команде.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *Данные запроса*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *Обработанные данные*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *Обработанные данные*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *Обработанные данные*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Solicitation batch size` | `[1-1024]` | Минимальное количество записей, включаемых в один пакет. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'QC'. |
| Данные запроса 1 | n N | 12-значный ссылочный номер<br>Выбранный PIN (от 4 до 12 цифр)<br>Значение ';' (разделитель) |
| Данные запроса 2 | n N | 12-значный ссылочный номер<br>Выбранный PIN (от 4 до 12 цифр)<br>Значение ';' (разделитель) |
| ... | ... | ... |
| Данные последнего запроса | n N | 12-значный ссылочный номер<br>Выбранный PIN (от 4 до 12 цифр)<br>Значение ';' (разделитель) |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'QD'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'30': Недопустимый ссылочный номер<br>'31': Недостаточное количество записей для пакета<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Обработанные данные 1 | n A | 10 крайних правых цифр номера карты (PAN) и PIN, зашифрованный под LMK. |
| Обработанные данные 2 | n A | 10 крайних правых цифр номера карты (PAN) и PIN, зашифрованный под LMK. |
| ... | ... | ... |
| Последние обработанные данные | n A | 10 крайних правых цифр номера карты (PAN) и PIN, зашифрованный под LMK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 9 Команды форматирования документов для печати

Бланки (конверты) для защищенной передачи PIN и других конфиденциальных данных печатаются с помощью принтера, подключенного напрямую к USB-порту HSM. Перед отправкой команды печати документа (например, 'PE') на HSM должен быть настроен формат печати.

Полный перечень поддерживаемых символов форматирования приведен в «КриптоПро HSM. Руководство программиста».

HSM поддерживает следующие команды хоста для настройки форматов печатаемых документов:

## [PA] — Загрузка данных форматирования в HSM

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Загрузка данных форматирования в HSM.

**Примечания:** HSM может хранить до 299 символов и констант.

Команда должна вызываться перед каждым обращением к принтеру, за исключением случаев печати 2-го документа на одном листе (подробнее см. описание команд 'PE' и 'OA'.)

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'PA'. |
| Данные форматирования | n A | Строка форматирования, состоящая из символов и констант (подробное описание см. в «КриптоПро HSM. Руководство программиста»).<br>Задание пустой строки удаляет строку форматирования. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'PB'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [LI] — Переопределение текстовых значений для цифр PIN

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Переопределение текстовых значений цифр PIN для печати PIN словами.

**Примечания:** По умолчанию текстовые значения для цифр PIN, используемые HSM для печати PIN словами, установлены на английском языке (ONE, TWO, THREE, ...).

Данная команда используется для переопределения текстовых значений для цифр PIN на другом языке.

В команде должны быть указаны значения для всех цифр PIN (от 0 до 9).

Допустимые значения полей *Длина*: от 0 до F (HEX), где 0 соответствует длине $16_{10}$.

Текстовая строка, соответствующая цифре PIN, должна быть указана в команде в кодировке UTF-8 в шестнадцатеричной системе счисления. Например, строка 'НОЛЬ', соответствующая цифре 0 на русском языке, должны быть передана в виде 'd09dd09ed09bd0ac'.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'LI'. |
| Цифра 0 | n B | Строка, соответствующая цифре 0, в кодировке UTF-8 в HEX. |
| Длина | 1 H | Длина строки в следующем поле. |
| Цифра 1 | n B | Строка, соответствующая цифре 1, в кодировке UTF-8 в HEX. |
| ... | ... | ... |
| ... | ... | ... |
| Длина | 1 H | Длина строки в следующем поле. |
| Цифра 9 | n B | Строка, соответствующая цифре 9, в кодировке UTF-8 в HEX. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'LJ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 10 Команды работы с незашифрованными PIN

ИСПОЛЬЗОВАНИЕ КОМАНД РАБОТЫ С НЕЗАШИФРОВАННЫМИ PIN СОПРОВОЖДАЕТСЯ ЗНАЧИТЕЛЬНЫМИ РИСКАМИ ИБ.

HSM поддерживает следующие команды хоста для операций с незашифрованными PIN:

## [BA] — Зашифрование PIN

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Требуется** | |
| Активности: **pin.clear.host** | |

**Описание функции:** Зашифрование PIN.

**Предупреждение:** ИСПОЛЬЗОВАНИЕ КОМАНДЫ СОПРОВОЖДАЕТСЯ ЗНАЧИТЕЛЬНЫМИ РИСКАМИ ИБ.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Encrypt clear PINs` | `Yes [Y]` | Команда доступна. |
| | `No [N]` | Команда недоступна. |
| `PIN length` (влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm` (влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A` (влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm` (влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **КОМАНДА** |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'BA'. |
| PIN | L H | Незашифрованный PIN, выровненный по левому краю и дополненный 'F' до максимальной длины PIN (L). Значение L (допустимые значения: 5 .. 13) устанавливается с помощью консольной команды CS. |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'BB'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| PIN | | PIN, зашифрованный под LMK. |
| | L N<br>или<br>L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [NG] — Расшифрование PIN

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Требуется** | |
| Активности: **pin.clear.host** | |

**Описание функции:** Расшифрование PIN, зашифрованного под LMK, и возврат хосту ссылочного номера (reference number).

**Примечания:** Ссылочный номер может использоваться в процессе обработки данных запроса PIN.

**Предупреждение:** ИСПОЛЬЗОВАНИЕ КОМАНДЫ СОПРОВОЖДАЕТСЯ ЗНАЧИТЕЛЬНЫМИ РИСКАМИ ИБ.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Select clear PINs` | `Yes [Y]` | Команда доступна. |
| | `No [N]` | Команда недоступна. |
| `PIN length` (влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm` (влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A` (влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm` (влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'NG'. |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| PIN | | PIN, зашифрованный под LMK. |
| | L N<br>или<br>L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'NH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| PIN | L H | Незашифрованный PIN, выровненный по левому краю и дополненный 'F'. |
| Ссылочный номер | 12 N | Ссылочный номер, полученный в результате зашифрования PAN под LMK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 11 Команды CVC/CVV

CVC/CVV (Card Verification Code/Card Verification Value) — код проверки подлинности платежной карты, для генерации которого используются определенные поля данных, например, номер карты (PAN), срок действия карты, сервисный код и ключ проверки/генерации CVC/CVV (CVK, Card Verification Key).

CVC/CVV как правило наносятся на оборотную сторону платежной карты. В процессе транзакции CVC/CVV передается HSM, который заново вычисляет CVV и сравнивает его с полученным значением для подтверждения подлинности карты.

Следующие команды хоста используются для поддержки операций с CVC/CVV:

## [CW] — Генерация CVV/CVC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация CVV или CVC.

**Примечания:** Команда может использоваться для генерации:

- Visa CVV1 или Mastercard CVC1 для кодирования на магнитную полосу карты;
- Visa CVV2 или Mastercard CVC2 для печати на полосе для подписи карты;
- Visa iCVV или Mastercard Chip CVC для записи на EMV-карту с чипом;
- Visa CAVV или Mastercard AAV для использования в протоколе 3-D Secure.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'CW'.</td></tr>
<tr><td>CVK A/B</td><td></td><td>Ключ CVK A/B, используемый для вычисления CVV/CVC.</td></tr>
<tr><td></td><td>32 H<br>или<br>'U' + 32 H</td><td>CVK A/B, зашифрованный под LMK 14-15/4.</td></tr>
<tr><td></td><td>'S' + n A</td><td>CVK A/B должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'C0', '12', '13'</td><td>'T'</td><td>'C', 'G', 'N'</td></tr>
</table></td></tr>
<tr><td>Номер карты (PAN)</td><td>8 – 19 N</td><td>Номер карты (PAN).</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td>Срок действия карты</td><td>4 N</td><td>В случае генерации:<br>CAVV/AAV — 4-значное случайное число (UN), выработанное на основе идентификатора транзакции (в соответствии с протоколом 3-D Secure).<br>Иначе — срок действия карты.</td></tr>
<tr><td>Сервисный код</td><td>3 N</td><td>В случае генерации:<br>Visa CVV1 или Mastercard CVC1 — сервисный код карты.<br>Visa CVV2 или Mastercard CVC2 — значение '000'.<br>Visa iCVV или Mastercard Chip CVC — значение '999'.<br>CAVV/AAV — 1-значный код результата аутентификации + 2-значный код результата вторичной аутентификации (в соответствии с протоколом 3-D Secure).</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'CX'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность CVK A/B<br>'27': Алгоритм CVK отличен от 2DES<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| CVV | 3 N | Сгенерированное значение CVV/CVC. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [CY] — Проверка CVV/CVC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка CVV или CVC.

**Примечания:** Команда может использоваться для проверки:

- Visa CVV1 или Mastercard CVC1, закодированного на магнитной полосе карты;
- Visa CVV2 или Mastercard CVC2, напечатанного на полосе для подписи карты;
- Visa iCVV или Mastercard Chip CVC, записанного на EMV-карте с чипом;
- Visa CAVV или Mastercard AAV, используемого в протоколе 3-D Secure.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'CY'.</td></tr>
<tr><td>CVK A/B</td><td></td><td>Ключ CVK A/B, используемый для проверки CVV/CVC.</td></tr>
<tr><td></td><td>32 H<br>или<br>'U' + 32 H</td><td>CVK A/B, зашифрованный под LMK 14-15/4.</td></tr>
<tr><td></td><td>'S' + n A</td><td>CVK A/B должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'C0', '12', '13'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>CVV</td><td>3 N</td><td>CVV/CVC для проверки.</td></tr>
<tr><td>Номер карты (PAN)</td><td>8 – 19 N</td><td>Номер карты (PAN).</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td>Срок действия карты</td><td>4 N</td><td>В случае проверки:<br>CAVV/AAV — 4-значное случайное число (UN), выработанное на основе идентификатора транзакции (в соответствии с протоколом 3-D Secure).<br>Иначе — срок действия карты.</td></tr>
<tr><td>Сервисный код</td><td>3 N</td><td>В случае проверки:<br>Visa CVV1 или Mastercard CVC1 — сервисный код карты.<br>Visa CVV2 или Mastercard CVC2 — значение '000'.<br>Visa iCVV или Mastercard Chip CVC — значение '999'.<br>CAVV/AAV — 1-значный код результата аутентификации + 2-значный код результата вторичной аутентификации (в соответствии с протоколом 3-D Secure).</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'CZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки CVV/CVC<br>'10': Нарушена четность CVK A/B<br>'27': Алгоритм CVK отличен от 2DES<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [QY] — Генерация динамического CVV

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация динамического CVV (dCVV).

**Примечания:** Команда поддерживает схемы генерации dCVV.

При генерации DK-DCVV команда всегда добавляет нулевой байт к переданному номеру карты (PAN).

Для *Идентификатора схемы* = '0' единственное допустимое значение *Сервисного кода* — '998'. В случае других значений команда вернет код ошибки 07.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'QY'.</td></tr>
<tr><td>Идентификатор схемы</td><td>1 N</td><td>'0': Visa dCVV<br>'1': Visa Authentication Value (AV)<br>'5': Visa dCVV2 Time Based</td></tr>
<tr><td>MK</td><td></td><td>Мастер-ключ для выработки ключа карты.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>MK-AC, зашифрованный под LMK 28-29/1.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK-AC должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E0'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Метод диверсификации ключа</td><td>1 A</td><td>'A': EMV 4.1 Book 2 Option A<br>'B': EMV 4.1 Book 2 Option B</td></tr>
<tr><td>Номер карты (PAN)</td><td>8 – 19 N</td><td>Номер карты (PAN).<br>Примечание: если длина PAN ≤ 16 цифр, применяется метод EMV Option A и HSM при необходимости дополнит значение до 16 цифр соответствующим образом.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Признак конца поля Номер карты (PAN).</td></tr>
<tr><td colspan="3">Следующие 3 поля присутствуют только в случае Идентификатора схемы = '0' (Visa dCVV):</td></tr>
<tr><td>Срок действия карты</td><td>4 N</td><td>Срок действия карты.</td></tr>
<tr><td>Сервисный код</td><td>3 N</td><td>Сервисный код карты, используемый для генерации dCVV.<br>Допустимое значение: '998'.</td></tr>
<tr><td>ATC</td><td>6 N</td><td>Счетчик транзакций.<br>Если длина ATC для Track2 < 6 цифр, ATC должен быть выровнен по правому краю и дополнен слева нулями. При генерации криптограммы будут использованы 4 крайних правых (наименее значимых) цифры ATC.</td></tr>
<tr><td colspan="3">Следующие 3 поля присутствуют только в случае Идентификатора схемы = '1' (Visa AV):</td></tr>
<tr><td>Длина данных транзакции</td><td>2 H</td><td>Длина следующего поля. Допустимые значения: '01' .. FF.</td></tr>
<tr><td>Данные транзакции</td><td>n B</td><td>Данные переменной длины. Если длина данных не кратна 8 байтам, данные дополняются в конце нулями.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Признак конца поля Данные транзакции.</td></tr>
<tr><td colspan="3">Следующие 2 поля присутствуют только в случае Идентификатора схемы = '5' (Visa dCVV2):</td></tr>
</table>

| | | |
|---|---|---|
| Срок действия карты | 4 N | Срок действия карты в формате ГГММ. |
| TWU | 6 N | Единица измерения временного окна (в секундах). |
| Текущее время | 8 H | Количество секунд, прошедших с полуночи (00:00:00 UTC) 1 января 1970 года. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'QZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'05': Недопустимый идентификатор схемы или метод диверсификации ключа<br>'07': Недопустимый сервисный код<br>'10': Нарушена четность MK<br>или другой стандартный код ошибки. |
| dCVV/AV/dCVV2 | 3 N<br>или<br>8 B<br>или<br>3 N | В случае *Идентификатора схемы* = '0' — вычисленное значение dCVV.<br><br>В случае *Идентификатора схемы* = '1' — вычисленное значение AV.<br><br>В случае *Идентификатора схемы* = '5' — вычисленное значение dCVV2. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [PM] — Проверка динамического CVV/CVC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Опционально (см. описание)** | |
| Активности: **diagnostic.host** | |

**Описание функции:** Проверка динамически сгенерированного CVV/CVC.

**Примечания:** Значения следующих полей команды формируются на основе данных EMV "Track2 Equivalent Data", указанных в авторизационном сообщении, полученном от бесконтактной смарт-карты:

- Номер карты (PAN)
- Срок действия карты
- Сервисный код
- ATC
- DCVV

Ниже приведены примечания для разных платежных систем и используемых схем:

| | |
|---|---|
| Visa (dCVV) | Для вычисления UDK используется нулевой PSN. Команда добавит ноль к переданному номеру карты (PAN) при генерации DK-AC. |
| Visa (dCVV2) | Команда поддерживает проверку динамического CVV с использованием алгоритма Visa dCVV2. Ключ карты вырабатывается из мастер-ключа MK-DCVV с использованием данных диверсификации, затем вычисляется значение dCVV2 и сравнивается со значением, переданным в команде. |
| Visa (LUC) | Метод Visa, применяемый в облачных схемах платежей, используется ключ ограниченного использования (LUK) для генерации криптограммы ограниченного использования (LUC). |
| Mastercard (CVC3) | Если в команде не указан PSN, команда добавит ноль к переданному номеру карты (PAN) при генерации DK-CVC3.<br>Для проверки CVC3 требуется IVCVC3, который представляет собой значение MAC, вычисленное для статической части Track1 или Track2 с использованием DK-CVC3. Значение IVCVC3 может быть передано в команде в соответствующем поле или вычислено в процессе проверки CVC3 из переданных в команде данных Track1 или Track2. |
| Mastercard (PINCVC3) | Является вариантом стандартной схемы CVC3. Приложение Mastercard Mobile PayPass M/Chip генерирует PINCVC3 вместо CVC3 в случаях, когда PIN был введен на мобильных устройствах. В вычислениях PINCVC3 используется специальный вектор инициализации PINIVCVC3. В остальном вычисления PINCVC3 и CVC3 аналогичны. |
| American Express ExpressPay Cryptogram | Схема бесконтактных платежей American Express использует динамически сгенерированную 5-значную криптограмму. |
| JCB Dynamic CAV | Команда поддерживает проверку динамического CAV (dCAV) с использованием сессионного ключа проверки динамического CAV. |

Для удобства разработки приложений хоста вычисленный динамический CVV включается в данные ответа в случае возврата кода ошибки 01 при условии, что HSM находится в авторизованном состоянии.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'PM'. |
| Идентификатор схемы | 1 N | '0': Visa<br>'1': Mastercard<br>'2': American Express<br>'5': Visa dCVV2<br>'6': JCB Contactless Mobile Payment Application |
| Версия | 1 N | Для *Идентификатора схемы* = '0' (Visa):<br>'0': проверка Visa DCVV<br>'1': проверка Visa LUC<br>'2': проверка Visa LUC (со значением, переданным хостом)<br>'3': проверка Visa LUC (с проверкой состояния потребительского устройства)<br><br>Для *Идентификатора схемы* = '1' (Mastercard):<br>'0': проверка PayPass CVC3 (IVCVC3 передается в команде, PSN=00)<br>'1': проверка PayPass CVC3 (PSN и IVCVC3 передаются в команде)<br>'2': проверка PayPass CVC3 (PSN передается в команде, IVCVC3 вычисляется из переданных в команде данных магнитной полосы)<br>'3': проверка PayPass PINCVC3 (PSN передается в команде, PINIVCVC3 вычисляется из переданных в команде данных магнитной полосы)<br>'4': проверка HCE CVC3 (PSN передается в команде, PINIVCVC3 вычисляется из переданных в команде данных магнитной полосы)<br><br>Для *Идентификатора схемы* = '2' (American Express):<br>'0': метод проверки ExpressPay (в соответствии со спецификацией ExpressPay 2.0)<br><br>Для *Идентификатора схемы* = '5' (Visa dCVV2):<br>'0': Visa dCVV2<br><br>Для *Идентификатора схемы* = '6' (JCB Contactless):<br>'0': метод проверки JCB J/Speedy (в соответствии со спецификацией JCB IC Card Application Specification v3.0) |
| MK-DCVV | | Мастер-ключ, из которого вырабатывается ключ карты. |
| | 'U' + 32 H | Для *Идентификатора схемы* = '0', '2' или '5' — MK-AC, зашифрованный под LMK 28-29/1.<br>Для *Идентификатора схемы* = '1' и *Версии* = '0', '1', '2' или '3' — MK-CVC3, зашифрованный под LMK 28-29/7.<br>Для *Идентификатора схемы* = '1' и *Версии* = '4' — MK-AC, зашифрованный под LMK 28-29/1.<br>Для *Идентификатора схемы* = '6' — MK-DCVV, зашифрованный под LMK 28-29/7. |

<table>
<tr><td></td><td>'S' + n A</td><td>Для Идентификатора схемы = '0', '2' или '5' MK-DCVV должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E0'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table>
Для Идентификатора схемы = '1' и Версии = '0', '1', '2' или '3' MK-DCVV должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E6', '32'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table>
Для Идентификатора схемы = '1' и Версии = '4' MK-DCVV должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E0'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table>
Для Идентификатора схемы = '6' MK-DCVV должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E6'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Метод диверсификации ключа</td><td>1 A</td><td>Метод выработки ключа карты из мастер-ключа:<br>Для Идентификатора схемы = '0', '1' (Версия = '0', '1', '2' или '3'), '2' или '5':<br>'A': EMV 4.1 Book 2 Option A method<br>'B': EMV 4.1 Book 2 Option B method<br>Для Идентификатора схемы = '1' и Версии = '4':<br>'4': выработка ключа карты из мастер-ключа с использованием EMV 4.1 Book 2 Option A и последующая выработка сессионного ключа с сипользованием EMV Common Session Key derivation<br>Для Идентификатора схемы = '6':<br>'A': EMV Option 'A' Method и JCB Session Key Derivation</td></tr>
<tr><td>Номер карты (PAN)</td><td>n N</td><td>Для Идентификатора схемы = '0', '1', '2' или '5' длина PAN 8-19 цифр.<br>Для Идентификатора схемы = '6' длина PAN 16 цифр.<br>Примечание: если длина PAN $\leq$ 16 цифр, применяется метод EMV Option A и HSM при необходимости дополнит значение до 16 цифр соответствующим образом.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Признак конца поля Номер карты (PAN).</td></tr>
<tr><td>PAN Sequence Number (PSN)</td><td>2 N</td><td>Присутствует только в случае:<br>Идентификатора схемы = '0' и Версии = '3'<br>Идентификатора схемы = '1' Версии = '1', '2', '3' или '4'<br>Идентификатора схемы = '2'<br>Идентификатора схемы = '6'<br>Если PAN Sequence Number не определен, используется значение '00'.</td></tr>
<tr><td>Флаг модификации PSN</td><td>1 N</td><td>Присутствует только в случае Идентификатора схемы = '1' и Версии = '4'.<br>'0': в команде передается немодифицированный PSN<br>'1': в команде передается модифицированный PSN</td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае Идентификатора схемы = '0' (Visa) и Версии = '0' (DCVV):</td></tr>
<tr><td>Срок действия карты</td><td>4 N</td><td>Срок действия карты.</td></tr>
<tr><td>Сервисный код</td><td>3 N</td><td>Сервисный код карты (Track2).</td></tr>
<tr><td>ATC</td><td>6 N</td><td>Счетчик транзакций.<br>Если длина ATC для Track2 $<$ 6 цифр, ATC должен быть выровнен по правому краю и дополнен слева нулями. При проверке криптограммы будут использованы 4 крайних правых (наименее значимых) цифры ATC.</td></tr>
</table>

| | | |
|---|---|---|
| dCVV | 3 N | Проверяемое значение dCVV. |
| Следующие 2 поля присутствуют только в случае *Идентификатора схемы* = '0' (Visa) и *Версии* = '1' (LUC): | | |
| YHHHHCC | 7 N | Значение Год/Час/Счетчик, используемое для выработки LUK для генерации LUC:<br>Y (0-9): последняя значащая цифра текущего года<br>HHHH (0001-8784): количество часов, прошедших с 01 января<br>CC (00-99): значение счетчика |
| LUC | 6 N | Проверяемая криптограмма. |
| Следующие 3 поля присутствуют только в случае *Идентификатора схемы* = '0' (Visa) и *Версии* = '2' (LUC со значением, переданным хостом): | | |
| YHHHHCC | 7 N | Значение Год/Час/Счетчик, используемое для выработки LUK для генерации LUC:<br>Y (0-9): последняя значащая цифра текущего года<br>HHHH (0001-8784): количество часов, прошедших с 01 января<br>CC (00-99): значение счетчика |
| Значение для LUC | 16 N | Значение для генерации криптограммы с использованием LUK. |
| LUC | 3 N | Проверяемая криптограмма. |
| Следующие 4 поля присутствуют только в случае *Идентификатора схемы* = '0' (Visa) и *Версии* = '3' (проверка LUC с проверкой состояния потребительского устройства): | | |
| YHHHHCC | 7 N | Значение Год/Час/Счетчик, используемое для выработки LUK для генерации LUC:<br>Y (0-9): последняя значащая цифра текущего года<br>HHHH (0001-8784): количество часов, прошедших с 01 января<br>CC (00-99): значение счетчика |
| Уровень уязвимости | 1 N | Состояние потребительского устройства при проверке LUC.<br>'0': нормальное<br>'1': уязвимое |
| ATC | 6 N | Счетчик транзакций.<br>При проверке криптограммы будут использованы 4 крайних правых (наименее значимых) цифры ATC. |
| LUC | 3 N | Проверяемая криптограмма. |
| Следующие 4 поля присутствуют только в случае *Идентификатора схемы* = '1' (Mastercard) и *Версии* = '0' или '1': | | |
| IVCVC3 | 5 N | Статические данные эмитента. Максимальное значение: 65535 (2 байта). |
| UN | 10 N<br>или<br>8 H | Случайное число (Unpredictable Number), генерируемое терминалом для карты во время PayPass-транзакции. Вне зависимости от формата поля используется 4-байтовое двоичное число. HSM определяет длину поля (и соответствующий тип) на основании количества символов, передаваемых в команде.<br>Например, для использования 4-байтового значения 0x00000256 допускается передавать в команде одно из следующих значений:<br>в BCD формате (8 H) — '00000256' → 0x00000256<br>в десятичном формате (10 N) — '0000000598' → 0x00000256 |
| ATC | 5 N | Значение счетчика транзакций в десятичном формате. Максимальное значение: 65535 (2 байта). |
| CVC3/PINCVC3 | 5 A | Проверяемое значение CVC3 или PINCVC3.<br>Первые символы поля (максимум 2) могут содержать значение 'X' — признак, что длина CVC3/PINCVC3 меньше 5 цифр. Символы 'X' не участвуют в сравнении преданного в команде и вычисленного значений CVC3/PINCVC3. Например, переданное в команде значение 'XX123' соответствует вычисленному значению '87123'.<br>Максимальное значение: 65535 (2 байта). |
| Следующие поля присутствуют только в случае *Идентификатора схемы* = '1' (Mastercard) и *Версии* = '2', '3' или '4': | | |

| | | |
|---|---|---|
| Длина Track | 3 N | Длина следующего поля. |
| Track | n B | Статические данные Track1 или Track2. |
| UN | 10 N<br>или<br>8 H | Случайное число (Unpredictable Number), генерируемое терминалом для карты во время PayPass-транзакции. Вне зависимости от формата поля используется 4-байтовое двоичное число. Максимальное значение: 4294967295 (4 байта). |
| ATC | 5 N | Значение счетчика транзакций в десятичном формате. Максимальное значение: 65535 (2 байта). |
| CVC3/PINCVC3 | 5 A | Проверяемое значение CVC3 или PINCVC3.<br>Первые символы поля (максимум 2) могут содержать значение 'X' — признак, что длина CVC3/PINCVC3 меньше 5 цифр. Символы 'X' не участвуют в сравнении преданного в команде и вычисленного значений CVC3/PINCVC3. Например, переданное в команде значение 'XX123' соответствует вычисленному значению '87123'.<br>Максимальное значение: 65535 (2 байта). |
| Маска CVC | 8 B | Присутствует только в случае *Версии* = '4'.<br>Маска для проверки вычисленного значения CVC3. Например, маска 0xFFFF0000 00000000 указывает, что сравниваться будут 2 крайних левых (наиболее значимых) байта CVC3. |
| Следующие поля присутствуют только в случае *Идентификатора схемы* = '2' (American Express) и *Версии* = '0' (ExpressPay): | | |
| Длина данных транзакции | 2 H | Длина следующего поля. Допустимые значения: '01' .. FF. |
| Данные транзакции | n B | Данные переменной длины. Если длина данных не кратна 8 байтам, данные дополняются в конце нулями. |
| Разделитель | 1 A | Значение ';'. Признак конца поля *Данные транзакции*. |
| Криптограмма | 5 N | Проверяемое значение криптограммы. |
| Следующие поля присутствуют только в случае *Идентификатора схемы* = '5' (Visa dCVV2): | | |
| Срок действия карты | 4 N | Срок действия карты в формате ГГММ. |
| TWU | 6 N | Единица измерения временного окна (в секундах). |
| Текущее время | 8 H | Количество секунд, прошедших с полуночи (00:00:00 UTC) 1 января 1970 года. |
| dCVV2 | 3 N | Проверяемое значение dCVV2. |
| Следующие поля присутствуют только в случае *Идентификатора схемы* = '6' (JCB): | | |
| Срок действия карты | 4 N | Срок действия карты в формате ММГГ. |
| Сервисный код | 3 N | Сервисный код карты. |
| ATC | 5 N | Значение счетчика транзакций в десятичном формате. |
| CVS для дискреционных данных | 1 N | Допустимые значения: '1'..'4'. |
| dCAV | 3 N | Проверяемое значение динамического CAV. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |

| | | |
|---|---|---|
| Код ответа | 2 A | Значение 'PN'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки криптограммы<br>'05': Недопустимый идентификатор схемы, версия или метод диверсификации ключа<br>'06': Недопустимое значение YHHHHCC<br>'10': Нарушена четность MK-DCVV<br>'52': Недопустимый CVS для дискреционных данных<br>'68': Команда недоступна<br>'E9': Недопустимая маска CVC3<br>'EA': Недопустимый флаг модификации PSN<br>'EB': Недопустимый уровень уязвимости<br>или другой стандартный код ошибки. |
| Диагностические данные | | Вычисленное значение (корректное) криптограммы. Присутствует только в случае *Кода ошибки* = '01' и если HSM находится в авторизованном состоянии. |
| | 3 N | Для *Идентификатора схемы* = '0' и *Версии* = '0' или '2' — вычисленное корректное значение dCVV или LUC соответственно.<br>Для *Идентификатора схемы* = '5' — вычисленное корректное значение dCVV2.<br>Для *Идентификатора схемы* = '6' — вычисленное корректное значение dCAV. |
| | 5 N | Для *Идентификатора схемы* = '1' и *Версии* = '0', '1' или '2' — вычисленное корректное значение CVC3.<br>Для *Идентификатора схемы* = '1' и *Версии* = '3' или '4' — вычисленное корректное значение PINCVC3.<br>Для *Идентификатора схемы* = '2' — вычисленное корректное значение криптограммы. |
| | 6 N | Для *Идентификатора схемы* = '0' и *Версии* = '1' — вычисленное корректное значение LUC. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [RY] — Генерация CSC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация 5-значного, 4-значного и 3-значного CSC для карт American Express.

**Примечания:** Команда поддерживает 3 алгоритма вычисления CSC:

- Classic CSC Algorithm (CSC Version 1.0);
- Enhanced CSC Algorithm (CSC Version 2.0);
- American Express Verification Value (AEVV).

| Параметр | Формат | Описание |
|---|---|---|
| | | **КОМАНДА** |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'RY'. |
| Режим | 1 N | Значение '3'. |
| Флаг | 1 N | Алгоритм вычисления CSC:<br>'0': Classic CSC Algorithm (CSC Version 1.0)<br>'2': Enhanced CSC Algorithm (CSC Version 2.0)<br>'3': American Express Verification Value (AEVV) |
| CSCK | | Ключ CSCK, используемый для вычисления CSC. |
| | 'U' + 32 H | CSCK, зашифрованный под LMK 14-15/4. |
| | 'S' + n A | CSCK должен соответствовать следующему формату: |

| Использование ключа | Алгоритм | Режим использования |
|---|---|---|
| 'C0', '11' | 'T' | 'C', 'G', 'N' |

| | | |
|---|---|---|
| Номер карты (PAN) | 19 N | Номер карты (PAN), выровненный по левому краю и дополненный '0' в случае длины меньшей 19. |
| Срок действия карты | 4 N | В случае *Флага* = '0' или '2' — срок действия карты в формате ГГММ.<br>В случае *Флага* = '3' — 4-значное случайное число (UN), выработанное на основе идентификатора транзакции (в соответствии с протоколом 3-D Secure). |
| Сервисный код | 3 N | Присутствует только в случае *Флага* = '2' или '3'.<br>В случае *Флага* = '2' — сервисный код карты.<br>В случае *Флага* = '3' — 1-значный код результата аутентификации + 2-значный код результата вторичной аутентификации (в соответствии с процессом AEVV). |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'RZ'. |

| | | |
|---|---|---|
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность CSCK<br>'27': Алгоритм CSCK отличен от 2DES<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Режим | 1 N | Значение '3'. |
| 5-значный CSC/iCSC | 5 N | Присутствует только в случае *Флага* = '0' или '2'. |
| 4-значный CSC/iCSC | 4 N | Присутствует только в случае *Флага* = '0' или '2'. |
| 3-значный CSC/iCSC/AEVV | 3 N | В случае *Флага* = '0' или '2' — 3-значный CSC/iCSC.<br>В случае *Флага* = '3' — 3-значный AEVV. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [RY] — Проверка CSC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка 5-значного, 4-значного и 3-значного CSC для карт American Express.

**Примечания:** Команда поддерживает 3 алгоритма вычисления CSC:

- Classic CSC Algorithm (CSC Version 1.0);
- Enhanced CSC Algorithm (CSC Version 2.0);
- American Express Verification Value (AEVV).

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'RY'.</td></tr>
<tr><td>Режим</td><td>1 N</td><td>Значение '4'.</td></tr>
<tr><td>Флаг</td><td>1 N</td><td>Алгоритм вычисления CSC:<br>'0': Classic CSC Algorithm (CSC Version 1.0)<br>'2': Enhanced CSC Algorithm (CSC Version 2.0)<br>'3': American Express Verification Value (AEVV)</td></tr>
<tr><td>CSCK</td><td></td><td>Ключ CSCK, используемый для проверки CSC.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>CSCK, зашифрованный под LMK 14-15/4.</td></tr>
<tr><td></td><td>'S' + n A</td><td>CSCK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'C0', '11'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Номер карты (PAN)</td><td>19 N</td><td>Номер карты (PAN), выровненный по левому краю и дополненный '0' в случае длины меньшей 19.</td></tr>
<tr><td>Срок действия карты</td><td>4 N</td><td>В случае Флага = '0' или '2' — срок действия карты в формате ГГММ.<br>В случае Флага = '3' — 4-значное случайное число (UN), выработанное на основе идентификатора транзакции (в соответствии с протоколом 3-D Secure).</td></tr>
<tr><td>Сервисный код</td><td>3 N</td><td>Присутствует только в случае Флага = '2' или '3'.<br>В случае Флага = '2' — сервисный код карты.<br>В случае Флага = '3' — 1-значный код результата аутентификации + 2-значный код результата вторичной аутентификации (в соответствии с процессом AEVV).</td></tr>
<tr><td>5-значный CSC/iCSC</td><td>5 H</td><td>Присутствует только в случае Флага = '0' или '2'.<br>Если проверка 5-значного CSC не требуется — значение 'FFFFF'.</td></tr>
<tr><td>4-значный CSC/iCSC</td><td>4 H</td><td>Присутствует только в случае Флага = '0' или '2'.<br>Если проверка 4-значного CSC не требуется — значение 'FFFF'.</td></tr>
<tr><td>3-значный CSC/iCSC/AEVV</td><td>3 H</td><td>В случае Флага = '0' или '2' поле игнорируется, если установлено значение 'FFF'.<br>В случае Флага = '3' — 3-значный AEVV.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
</table>

| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |
|---|---|---|

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'RZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки CSC<br>'10': Нарушена четность CSCK<br>'27': Алгоритм CSCK отличен от 2DES<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Режим | 1 N | Значение '4'. |
| Результат проверки 5-значного CSC/iCSC | 1 N | Присутствует только в случае *Флага* = '0' или '2'.<br>'0': Без ошибок<br>'1': Значение CSC не передано<br>'2': Ошибка проверки |
| Результат проверки 4-значного CSC/iCSC | 1 N | Присутствует только в случае *Флага* = '0' или '2'.<br>'0': Без ошибок<br>'1': Значение CSC не передано<br>'2': Ошибка проверки |
| Результат проверки 3-значного CSC/iCSC/AEVV | 1 N | '0': Без ошибок<br>'1': Значение CSC не передано<br>'2': Ошибка проверки |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 12 Команды изменения PIN

Процесс изменения PIN включает обязательную проверку текущего PIN перед обработкой нового PIN.

Текущий и новый PIN-блоки зашифрованы под одним и тем же ключом (ключом шифрования PIN-блока) TPK или ZPK, в зависимости от того, откуда получен PIN — ATM, PIN pad и т.п. или эквайера соответственно. Функции изменения PIN поддерживают изменение PIN, полученного от "терминала" или "системы обмена".

Следующие команды хоста используются для поддержки операции изменения PIN:

## [DU] — Проверка PIN и генерация IBM Offset (для нового PIN, выбранного пользователем)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка текущего PIN и, в случае успеха, генерация Offset с использованием метода IBM 3624 (IBM Offset Method) для нового PIN, выбранного пользователем. Текущий и новый PIN должны быть зашифрованы под ключом шифрования PIN-блока.

**Примечания:** По умолчанию предполагается использование зашифрованных таблиц децимализации, однако возможно использование незашифрованных таблиц децимализации (см. описание настройки `Decimalization Table`). Рекомендуется использование зашифрованных таблиц децимализации.

По умолчанию проверяется корректность таблицы децимализации в соответствии со следующим правилом: "таблица децимализации должна состоять из 16 цифр, при этом должна содержать не менее 8 различных цифр, и каждая цифра может повторяться не более 4 раз". Если данные требования не выполнены, возвращается ошибка 25. Проверка корректности таблицы может быть отключена (см. описание настройки `Enable Decimalization Table checks`). Отключение данной проверки не рекомендуется.

Команда никогда не возвращает код ошибки 00 в случае успеха, так как ключи PVK с алгоритмом DES не поддерживаются. Вместо кода 00 в случае успеха возвращается код ошибки 02 (используется ключ PVK с алгоритмом 2DES или 3DES).

Опционально команда гарантирует, что новый PIN отсутствует в списке «слабых» PIN (см. описание настройки `Enable Weak PIN checking`).

Процесс изменения PIN включает проверку текущего PIN и генерацию значения Offset для нового PIN. Команда выполняет обе эти функции.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Decimalization tables`<br>(влияет на параметры: *Таблица децимализации*) | `Encrypted [E]`<br>`(по умолчанию)` | Таблица децимализации, подаваемая на вход, должна быть зашифрована (с помощью консольной команды ED) и состоять из 16 шестнадцатеричных символов (для Variant LMK или 3DES Key Block LMK) или 'L' + 32 шестнадцатеричных символов (для AES Key Block LMK). |
| | `Plaintext [P]` | Таблица децимализации, подаваемая на вход, должна быть незашифрована и состоять из 16 десятичных символов. |
| `Enable Decimalization Table checks` | `Yes [Y]`<br>`(по умолчанию)` | Выполняется проверка таблицы децимализации, подаваемой на вход: таблица децимализации должна содержать не менее 8 различных цифр, и каждая цифра должна повторяться не более 4 раз. Если требование не выполняется, возвращается ошибка 25. |
| | `No [N]` | Проверка таблицы децимализации не выполняется. |
| `Enable variable length PIN offset`<br>(влияет на параметры: *Новый Offset*) | `Yes [Y]` | Длина сгенерированного Offset соответствует длине нового PIN. |
| | `No [N]`<br>`(по умолчанию)` | Длина генерируемого Offset для нового PIN определяется значением параметра *Проверочная длина*. |

| | | |
|---|---|---|
| `Enable Weak PIN checking`<br>(влияет на параметры: *Разделитель, Количество «слабых» PIN, Длина «слабых» PIN, Список «слабых» PIN*) | `Yes [Y]` | Выполнение команды зависит от следующих настроек безопасности:<br>• `Check new PINs using global list of weak PINs: [Yes/No]`<br>• `Check new PINs using local list of weak PINs: [Yes/No]`<br>*Примечание:* перед проверкой локального списка «слабых» PIN проверяется соответствие длины проверяемого PIN параметру *Длина «слабых» PIN*.<br>• `Check new PINs using rules: [Yes/No]`<br>Если в результате проверки PIN присутствует в каком-либо списке «слабых» PIN, возвращается код ошибки 86. Если не прошла проверка PIN по правилам, возвращается код ошибки 85. |
| | `No [N]`<br>`(по умолчанию)` | При генерации PIN не проверяются локальный и глобальный списки «слабых» PIN. Если в команде передается локальный список «слабых» PIN, возвращается код ошибки 15. |
| `Restrict PIN block usage for PCI HSM compliance`<br>(влияет на параметры: *Код формата PIN-блока*) | `Yes [Y]` | Допускается использовать только определенные форматы PIN-блока в соответствии с требованиями ISO 9564/ANSI X9.8 и PCI HSM. |
| | `No [N]` | Ограничения на формат PIN-блока не накладываются. |
| `Enforce key type 002 separation for PCI HSM compliance`<br>(влияет на параметры: *Тип ключа шифрования PIN-блока, Ключ шифрования PIN-блока*) | `Yes [Y]` | ТРК зашифрован под LMK 36-37/7. |
| | `No [N]` | ТРК зашифрован под LMK 14-15/0. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'DU'.</td></tr>
<tr><td>Тип ключа шифрования PIN-блока</td><td>3 H</td><td>Если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: No</code>:<br>'001': ZPK (зашифрованный под LMK 06-07/0)<br>'002': TPK (зашифрованный под LMK 14-15/0)<br>Если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: Yes</code>:<br>'001': ZPK (зашифрованный под LMK 06-07/0)<br>'70D': TPK (зашифрованный под LMK 36-37/7)</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Ключ шифрования PIN-блока</td><td></td><td>Ключ, под которым зашифрованы PIN-блоки (ZPK или TPK).</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Ключ шифрования PIN-блока, зашифрованный под соответствующим LMK, определяемым значением поля Тип ключа шифрования PIN-блока.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ шифрования PIN-блока должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'P0', '71', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr></table></td></tr>
<tr><td>PVK</td><td></td><td>PVK, используемый для генерации Offset.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>PVK, зашифрованный под LMK 14-15/0.</td></tr>
<tr><td></td><td>'S' + n A</td><td>PVK должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'V1'</td><td>'T'</td><td>'C', 'N'</td></tr></table></td></tr>
<tr><td>Текущий PIN-блок</td><td>16 H<br>или<br>32 H</td><td>Текущий PIN, зашифрованный под Ключом шифрования PIN-блока.<br>Если Ключ шифрования PIN-блока DES, то размер поля 16H.<br>Если Ключ шифрования PIN-блока AES, то размер поля 32H.</td></tr>
<tr><td>Код формата PIN-блока</td><td>2 N</td><td>Код формата PIN-блока.<br>Если выставлена настройка <code>Restrict PIN block usage for PCI compliance: Yes</code>, допускаются только следующие значения:<br>'01': ISO format 0<br>'47': ISO format 3<br>'48': ISO format 4</td></tr>
<tr><td>Проверочная длина</td><td>2 N</td><td>Если выставлена настройка <code>Enable variable length PIN offset: No</code>, определяет длину генерируемого значения Offset для нового PIN.</td></tr>
<tr><td>Номер карты (PAN)</td><td></td><td>Номер карты (PAN), используемый при формировании PIN-блока.</td></tr>
<tr><td></td><td>n N<br><br>или<br><br>12 N</td><td>Если Код формата PIN-блока = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель.<br>Для всех остальных значений поля Код формата PIN-блока:<br>12 крайних правых цифр PAN, за исключением контрольной цифры.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует, только если Код формата PIN-блока = '48'.</td></tr>
<tr><td>Таблица децимализации</td><td>16 N<br>или</td><td>16 N при использовании незашифрованной таблицы децимализации.</td></tr>
</table>

| | | |
|---|---|---|
| | 16 H<br>или | 16 H при использовании зашифрованной таблицы децимализации и Variant LMK или 3DES Key Block LMK. |
| | 'L' + 32 H | 'L' + 32 H при использовании зашифрованной таблицы децимализации и AES Key Block LMK. |
| Данные для проверки PIN | 12 A | Пользовательские данные, состоящие из шестнадцатиричных символов и символа 'N', который указывает HSM, где расположить последние 5 цифр PAN. |
| | или | или |
| | 'P' + 16 H | Пользовательские данные, состоящие из ASCII символа 'P', дополненного 16 шестнадцатеричными цифрами, которые будут использоваться в качестве входа для алгоритма генерации PIN. |
| Текущий Offset | 12 H | Значение Offset для текущего PIN, выровненное по левому краю и дополненное 'F'. |
| Новый PIN-блок | 16 H<br>или<br>32 H | Новый PIN, зашифрованный под Ключом шифрования PIN-блока.<br>Если Ключ шифрования PIN-блока DES, то размер поля 16H.<br>Если Ключ шифрования PIN-блока AES, то размер поля 32H. |
| Разделитель | 1 A | Значение '*'. Присутствует, только если присутствуют поля ниже. |
| Количество «слабых» PIN | 2 N | Количество PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '00' .. '99'. |
| Длина «слабых» PIN | 2 N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Длина каждого PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '04' .. '12'. |
| Список «слабых» PIN | n N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Список «слабых» PIN. Длина поля вычисляется как *Количество «слабых» PIN * Длина «слабых» PIN.* |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'DV'. |
| Код ошибки | 2 H | '01': Ошибка проверки PIN<br>'02': Без ошибок<br>'03': Некорректное количество «слабых» PIN<br>'06': Недопустимая длина Offset<br>'10': Нарушена четность TPK или ZPK<br>'11': Нарушена четность PVK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>'81': Несоответствие длины PIN<br>'86': PIN присутствует в списке «слабых» PIN<br>или другой стандартный код ошибки. |
| Текущий Offset | 12 H | Сгенерированное значение Offset для нового PIN, выровненное по левому краю и дополненное 'F'. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [CU] — Проверка PIN и генерация ABA PVV (для нового PIN, выбранного пользователем)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка текущего PIN и, в случае успеха, генерация PVV (с использованием метода ABA PVV) для нового PIN, выбранного пользователем. Текущий и новый PIN должны быть зашифрованы под ключом шифрования PIN-блока.

**Примечания:** Опционально команда гарантирует, что новый PIN отсутствует в списке «слабых» PIN (см. описание настройки `Enable Weak PIN checking`).

Процесс изменения PIN включает проверку текущего PIN и генерацию значения PVV для нового PIN. Команда выполняет обе эти функции.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable Weak PIN checking`<br>(влияет на параметры: *Разделитель, Количество «слабых» PIN, Длина «слабых» PIN, Список «слабых» PIN*) | `Yes [Y]` | Выполнение команды зависит от следующих настроек безопасности:<br>• `Check new PINs using global list of weak PINs: [Yes/No]`<br>• `Check new PINs using local list of weak PINs: [Yes/No]`<br>*Примечание:* перед проверкой локального списка «слабых» PIN проверяется соответствие длины проверяемого PIN параметру *Длина «слабых» PIN*.<br>• `Check new PINs using rules: [Yes/No]`<br>Если в результате проверки PIN присутствует в каком-либо списке «слабых» PIN, возвращается код ошибки 86. Если не прошла проверка PIN по правилам, возвращается код ошибки 85. |
| | `No [N]`<br>`(по умолчанию)` | При генерации PIN не проверяются локальный и глобальный списки «слабых» PIN. Если в команде передается локальный список «слабых» PIN, возвращается код ошибки 15. |
| `Restrict PIN block usage for PCI HSM compliance`<br>(влияет на параметры: *Код формата PIN-блока*) | `Yes [Y]` | Допускается использовать только определенные форматы PIN-блока в соответствии с требованиями ISO 9564/ANSI X9.8 и PCI HSM. |
| | `No [N]` | Ограничения на формат PIN-блока не накладываются. |
| `Enforce key type 002 separation for PCI HSM compliance`<br>(влияет на параметры: *Тип ключа шифрования PIN-блока, Ключ шифрования PIN-блока*) | `Yes [Y]` | TPK зашифрован под LMK 36-37/7. |
| | `No [N]` | TPK зашифрован под LMK 14-15/0. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'CU'.</td></tr>
<tr><td>Тип ключа шифрования PIN-блока</td><td>3 H</td><td>Если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: No</code>:<br>'001': ZPK (зашифрованный под LMK 06-07/0)<br>'002': TPK (зашифрованный под LMK 14-15/0)<br>Если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: Yes</code>:<br>'001': ZPK (зашифрованный под LMK 06-07/0)<br>'70D': TPK (зашифрованный под LMK 36-37/7)<br>Значение 'FFF'.</td></tr>
<tr><td>Ключ шифрования PIN-блока</td><td></td><td>Ключ, под которым зашифрованы PIN-блоки (ZPK или TPK).</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Ключ шифрования PIN-блока, зашифрованный под соответствующим LMK, определяемым значением поля Тип ключа шифрования PIN-блока.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ шифрования PIN-блока должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'P0', '71', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr></table></td></tr>
<tr><td>PVK</td><td></td><td>PVK, используемый для генерации PVV.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>PVK, зашифрованный под LMK 14-15/0.</td></tr>
<tr><td></td><td>'S' + n A</td><td>PVK должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'V2'</td><td>'T'</td><td>'C', 'N'</td></tr></table></td></tr>
<tr><td>Текущий PIN-блок</td><td>16 H<br>или<br>32 H</td><td>Текущий PIN, зашифрованный под Ключом шифрования PIN-блока.<br>Если Ключ шифрования PIN-блока DES, то размер поля 16H.<br>Если Ключ шифрования PIN-блока AES, то размер поля 32H.</td></tr>
<tr><td>Код формата PIN-блока</td><td>2 N</td><td>Код формата PIN-блока.<br>Если выставлена настройка <code>Restrict PIN block usage for PCI compliance: Yes</code>, допускаются только следующие значения:<br>'01': ISO format 0<br>'47': ISO format 3<br>'48': ISO format 4</td></tr>
<tr><td>Номер карты (PAN)</td><td></td><td>Номер карты (PAN), используемый при формировании PIN-блока.</td></tr>
<tr><td></td><td>n N<br><br>или<br><br>12 N</td><td>Если Код формата PIN-блока = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или<br>13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель.<br>Для всех остальных значений поля Код формата PIN-блока:<br>12 крайних правых цифр PAN, за исключением контрольной цифры.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует, только если Код формата PIN-блока = '48'.</td></tr>
<tr><td>PVKI</td><td>1 N</td><td>Индекс ключа проверки PIN.<br>В соответствии с определением Visa допустимые значения '0' .. '6'.</td></tr>
<tr><td>Текущий PVV</td><td>4 N</td><td>Значение PVV для текущего PIN.</td></tr>
<tr><td>Новый PIN-блок</td><td>16 H<br>или<br>32 H</td><td>Новый PIN, зашифрованный под Ключом шифрования PIN-блока.<br>Если Ключ шифрования PIN-блока DES, то размер поля 16H.<br>Если Ключ шифрования PIN-блока AES, то размер поля 32H.</td></tr>
</table>

| | | |
|---|---|---|
| Разделитель | 1 A | Значение '*'. Присутствует, только если присутствуют поля ниже. |
| Количество «слабых» PIN | 2 N | Количество PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '00' .. '99'. |
| Длина «слабых» PIN | 2 N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Длина каждого PIN в списке «слабых» PIN ниже.<br>Допустимые значения: '04' .. '12'. |
| Список «слабых» PIN | n N | Присутствует, только если *Количество «слабых» PIN* > '00'.<br>Список «слабых» PIN. Длина поля вычисляется как *Количество «слабых» PIN * Длина «слабых» PIN.* |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'CV'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки PIN<br>'03': Некорректное количество «слабых» PIN<br>'10': Нарушена четность TPK или ZPK<br>'11': Нарушена четность PVK<br>'27': Алгоритм PVK отличен от 2DES<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>'81': Несоответствие длины PIN<br>'86': PIN присутствует в списке «слабых» PIN<br>или другой стандартный код ошибки. |
| Новый PVV | 4 N | Сгенерированное значение PVV для нового PIN. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 13 Команды проверки PIN

Для проверки PIN он должен быть передан HSM в формате 16-значного PIN-блока. HSM поддерживает несколько форматов PIN-блока, которые определяются двухзначным кодом формата PIN-блока (подробнее см. раздел «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста»).

HSM поддерживает следующие методы проверки PIN:
- IBM 3624 (IBM Offset Method)
- ABA PVV
- сравнение PIN

Полученный HSM PIN-блок зашифрован под ключом шифрования PIN-блока TPK или ZPK, в зависимости от того, откуда получен PIN — ATM, PIN pad и т.п. или эквайера соответственно. Функции проверки PIN поддерживают проверку PIN, полученного от "терминала" или "системы обмена".

Следующие команды хоста используются для поддержки операции проверки PIN:



Команды проверки PIN, используемые при обработке транзакций DUKPT, приведены в разд. 15.

## [DA] — Проверка PIN, зашифрованного под TPK, с использованием метода IBM 3624

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка PIN, зашифрованного под TPK и полученного от локального терминала (например, ATM, PIN pad, и т.д.), с использованием метода IBM 3624 (IBM Offset Method).

**Примечания:** По умолчанию предполагается использование зашифрованных таблиц децимализации, однако возможно использование незашифрованных таблиц децимализации (см. описание настройки `Decimalization Table`). Рекомендуется использование зашифрованных таблиц децимализации.

По умолчанию проверяется корректность таблицы децимализации в соответствии со следующим правилом: "таблица децимализации должна состоять из 16 цифр, при этом должна содержать не менее 8 различных цифр, и каждая цифра может повторяться не более 4 раз". Если данные требования не выполнены, возвращается ошибка 25. Проверка корректности таблицы может быть отключена (см. описание настройки `Enable Decimalization Table checks`). Отключение данной проверки не рекомендуется.

Команда никогда не возвращает код ошибки 00 в случае успеха, так как ключи PVK с алгоритмом DES не поддерживаются. Вместо кода 00 в случае успеха возвращается код ошибки 02 (используется ключ PVK с алгоритмом 2DES или 3DES).

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Decimalization tables`<br>(влияет на параметры: *Таблица децимализации*) | `Encrypted [E]`<br>`(по умолчанию)` | Таблица децимализации, подаваемая на вход, должна быть зашифрована (с помощью консольной команды ED) и состоять из 16 шестнадцатеричных символов (для Variant LMK или 3DES Key Block LMK) или 'L' + 32 шестнадцатеричных символов (для AES Key Block LMK). |
| | `Plaintext [P]` | Таблица децимализации, подаваемая на вход, должна быть незашифрована и состоять из 16 десятичных символов. |
| `Enable Decimalization Table checks` | `Yes [Y]`<br>`(по умолчанию)` | Выполняется проверка таблицы децимализации, подаваемой на вход: таблица децимализации должна содержать не менее 8 различных цифр, и каждая цифра должна повторяться не более 4 раз. Если требование не выполняется, возвращается ошибка 25. |
| | `No [N]` | Проверка таблицы децимализации не выполняется. |
| `Enforce key type 002 separation for PCI HSM compliance`<br>(влияет на параметры: *TPK*) | `Yes [Y]` | TPK зашифрован под LMK 36-37/7. |
| | `No [N]` | TPK зашифрован под LMK 14-15/0. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'DA'.</td></tr>
<tr><td>TPK</td><td></td><td>TPK, под которым зашифрован PIN-блок</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>TPK, зашифрованный под LMK 14-15/0 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: No</code>)<br>или LMK 36-37/7 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: Yes</code>).</td></tr>
<tr><td></td><td>'S' + n A</td><td>TPK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'P0', '71'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>PVK</td><td></td><td>PVK, используемый для проверки PIN-блока.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>PVK, зашифрованный под LMK 14-15/0.</td></tr>
<tr><td></td><td>'S' + n A</td><td>PVK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'V1'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Максимальная длина PIN</td><td>2 N</td><td>Значение '12'.</td></tr>
<tr><td>PIN-блок</td><td>16 H<br>или<br>32 H</td><td>PIN-блок, зашифрованный под TPK.<br>Если TPK DES, то размер поля 16H.<br>Если TPK AES, то размер поля 32H.</td></tr>
<tr><td>Код формата PIN-блока</td><td>2 N</td><td>Код формата PIN-блока.</td></tr>
<tr><td>Проверочная длина</td><td>2 N</td><td>Количество правых цифр значения Offset, которые необходимо проверить.</td></tr>
<tr><td>Номер карты (PAN)</td><td></td><td>Номер карты (PAN), используемый при формировании PIN-блока.</td></tr>
<tr><td></td><td>n N<br><br>или<br><br>12 N</td><td>Если поле Код формата PIN-блока = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или<br>13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель.<br>Для всех остальных значений поля Код формата PIN-блока:<br>12 крайних правых цифр PAN, за исключением контрольной цифры.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует, только если Код формата PIN-блока = '48'</td></tr>
<tr><td>Таблица децимализации</td><td>16 N<br>или<br><br>16 H<br>или<br><br>'L' + 32 H</td><td>16 N при использовании незашифрованной таблицы децимализации.<br><br>16 H при использовании зашифрованной таблицы децимализации и Variant LMK или 3DES Key Block LMK.<br><br>'L' + 32 H при использовании зашифрованной таблицы децимализации и AES Key Block LMK.</td></tr>
<tr><td>Данные для проверки PIN</td><td>12 A<br><br>или<br><br>'P' + 16 H</td><td>Пользовательские данные, состоящие из шестнадцатиричных символов и символа 'N', который указывает HSM, где расположить последние 5 цифр PAN.<br><br>или<br><br>Пользовательские данные, состоящие из ASCII символа 'P', дополненного 16 шеснадцатиричными цифрами, которые будут использоваться в качестве входа для алгоритма генерации PIN.</td></tr>
<tr><td>Offset</td><td>12 H</td><td>Значение Offset, выровненное по левому краю и дополненное 'F'.</td></tr>
</table>

| | | |
|---|---|---|
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'DB'. |
| Код ошибки | 2 H | '01': Ошибка проверки PIN<br>'02': Без ошибок<br>'10': Нарушена четность TPK<br>'11': Нарушена четность PVK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [EA] — Проверка PIN, зашифрованного под ZPK, с использованием метода IBM 3624

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка PIN, зашифрованного под ZPK и полученного через систему обмена, с использованием метода IBM 3624 (IBM Offset Method).

**Примечания:** По умолчанию предполагается использование зашифрованных таблиц децимализации, однако возможно использование незашифрованных таблиц децимализации (см. описание настройки `Decimalization Table`). Рекомендуется использование зашифрованных таблиц децимализации.

По умолчанию проверяется корректность таблицы децимализации в соответствии со следующим правилом: "таблица децимализации должна состоять из 16 цифр, при этом, должна содержать не менее 8 различных цифр, и каждая цифра может повторяться не более 4 раз". Если данные требования не выполнены, возвращается ошибка 25. Проверка корректности таблицы может быть отключена (см. описание настройки `Decimalization Table checks`). Отключение данной проверки не рекомендуется.

Команда никогда не возвращает код ошибки 00 в случае успеха, так как ключи PVK с алгоритмом DES не поддерживаются. Вместо кода 00 в случае успеха возвращается код ошибки 02 (используется ключ PVK с алгоритмом 2DES или 3DES).

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Decimalization tables`<br>(влияет на параметры: *Таблица децимализации*) | `Encrypted [E]`<br>`(по умолчанию)` | Таблица децимализации, подаваемая на вход, должна быть зашифрована (с помощью консольной команды ED) и состоять из 16 шестнадцаритичных символов (для Variant LMK или 3DES Key Block LMK) или 'L' + 32 шестнадцаритичных символов (для AES Key Block LMK). |
| | `Plaintext [P]` | Таблица децимализации, подаваемая на вход, должна быть незашифрована и состоять из 16 десятичных символов. |
| `Enable Decimalization Table checks` | `Yes [Y]`<br>`(по умолчанию)` | Выполняется проверка таблицы децимализации, подаваемой на вход: таблица децимализации должна содержать не менее 8 различных цифр, и каждая цифра должна повторяться не более 4 раз. Если требование не выполняется, возвращается ошибка 25. |
| | `No [N]` | Проверка таблицы децимализации не выполняется. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'EA'.</td></tr>
<tr><td>ZPK</td><td></td><td>ZPK, под которым зашифрован PIN-блок</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>ZPK, зашифрованный под LMK 06-07</td></tr>
<tr><td></td><td>'S' + n A</td><td>ZPK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'P0', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>PVK</td><td></td><td>PVK, используемый для проверки PIN-блока.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>PVK, зашифрованный под LMK 14-15/0.</td></tr>
<tr><td></td><td>'S' + n A</td><td>PVK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'V1'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Максимальная длина PIN</td><td>2 N</td><td>Значение '12'.</td></tr>
<tr><td>PIN-блок</td><td>16 H<br>или<br>32 H</td><td>PIN-блок, зашифрованный под ZPK.<br>Если ZPK DES, то размер поля 16H.<br>Если ZPK AES, то размер поля 32H.</td></tr>
<tr><td>Код формата PIN-блока</td><td>2 N</td><td>Код формата PIN-блока.</td></tr>
<tr><td>Проверочная длина</td><td>2 N</td><td>Количество правых цифр значения Offset, которые необходимо проверить.</td></tr>
<tr><td>Номер карты (PAN)</td><td></td><td>Номер карты (PAN), используемый при формировании PIN-блока.</td></tr>
<tr><td></td><td>nN<br><br>или<br><br>12 N</td><td>Если поле Код формата PIN-блока = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или<br>13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель.<br>Для всех остальных значений поля Код формата PIN-блока:<br>12 крайних правых цифр PAN, за исключением контрольной цифры.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует, только если Код формата PIN-блока = '48'</td></tr>
<tr><td>Таблица декомализации</td><td>16 N<br>или<br><br>16 H<br>или<br><br>'L' + 32 H</td><td>16 N при использовании незашифрованной таблицы декомализации.<br><br>16 H при использовании зашифрованной таблицы декомализации и Variant LMK или 3DES Key Block LMK.<br><br>'L' + 32 H при использовании зашифрованной таблицы декомализации и AES Key Block LMK.</td></tr>
<tr><td>Данные для проверки PIN</td><td>12 A<br><br>или<br><br>'P' + 16 H</td><td>Пользовательские данные, состоящие из шестнадцатиричных символов и символа 'N', который указывает HSM, где расположить последние 5 цифр PAN.<br><br>или<br><br>Пользовательские данные, состоящие из ASCII символа 'P', дополненного 16 шеснадцатиричными цифрами, которые будут использоваться в качестве входа для алгоритма генерации PIN.</td></tr>
<tr><td>Offset</td><td>12 H</td><td>Значение Offset, выровненное по левому краю и дополненное 'F'.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
</table>

| | | |
|---|---|---|
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'EB'. |
| Код ошибки | 2 H | '01': Ошибка проверки PIN<br>'02': Без ошибок<br>'10': Нарушена четность ZPK<br>'11': Нарушена четность PVK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [DC] — Проверка PIN, зашифрованного под TPK, с использованием метода ABA PVV

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка PIN, зашифрованного под TPK и полученного от локального терминала (например, ATM, PIN pad, и т.д.), с использованием метода ABA PVV.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce key type 002 separation for PCI HSM compliance` (влияет на параметры: *TPK*) | `Yes [Y]` | TPK зашифрован под LMK 36-37/7. |
| | `No [N]` | TPK зашифрован под LMK 14-15/0. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'DC'. |
| TPK | | TPK, под которым зашифрован PIN-блок |
| | 'U' + 32 H<br>или<br>'T' + 48 H | TPK, зашифрованный под LMK 14-15/0 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`)<br>или LMK 36-37/7 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: Yes`). |
| | 'S' + n A | TPK должен соответствовать следующему формату:<br>Использование ключа: 'P0', '71' \| Алгоритм: 'T', 'A' \| Режим использования: 'B', 'D', 'N' |
| PVK | | PVK, используемый для проверки PVV. |
| | 'U' + 32 H | PVK, зашифрованный под LMK 14-15/0. |
| | 'S' + n A | PVK должен соответствовать следующему формату:<br>Использование ключа: 'V2' \| Алгоритм: 'T' \| Режим использования: 'C', 'V', 'N' |
| PIN-блок | 16 H<br>или<br>32 H | PIN-блок, зашифрованный под TPK.<br>Если TPK DES, то размер поля 16H.<br>Если TPK AES, то размер поля 32H. |
| Код формата PIN-блока | 2 N | Код формата PIN-блока. |
| Номер карты (PAN) | | Номер карты (PAN), используемый при формировании PIN-блока. |
| | n N<br><br>или | Если поле *Код формата PIN-блока* = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | 12 N | Для всех остальных значений поля *Код формата PIN-блока*:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует, только если *Код формата PIN-блока* = '48' |
| PVKI | 1 N | Индекс ключа проверки PIN. |
| PVV | 4 N | PVV для PIN. |

| | | |
|---|---|---|
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'DD'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки PIN<br>'10': Нарушена четность TPK<br>'11': Нарушена четность PVK<br>'27': Алгоритм PVK отличен от 2DES<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [EC] — Проверка PIN, зашифрованного под ZPK, с использованием метода ABA PVV

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка PIN, зашифрованного под ZPK и полученного через систему обмена, с использованием метода ABA PVV.
Команда поддерживает проверку PIN-блоков, сформированных с использованием токена вместо настоящего номера карты (PAN). Для использования данного функционала должна быть выставлена соответствующая настройка (см. ниже).

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable use of Tokens in PIN Verification` (влияет на параметры: *Разделитель проверочного номера карты (PAN), Проверочный номер карты (PAN)*) | `Yes [Y]` | Доступна проверка PIN-блоков, сформированных с использованием токенов вместо настоящего номера карты (PAN). |
| | `No [N]` | Проверка PIN-блоков, сформированных с использованием токенов вместо настоящего номера карты (PAN), невозможна. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'EC'.</td></tr>
<tr><td>ZPK</td><td></td><td>ZPK, под которым зашифрован PIN-блок</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>ZPK, зашифрованный под LMK 06-07</td></tr>
<tr><td></td><td>'S' + n A</td><td>ZPK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'P0', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>PVK</td><td></td><td>PVK, используемый для проверки PVV.</td></tr>
<tr><td></td><td>32 H<br>или<br>'U' + 32 H</td><td>PVK, зашифрованный под LMK 14-15/0.</td></tr>
<tr><td></td><td>'S' + n A</td><td>PVK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'V2'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>PIN-блок</td><td>16 H<br>или<br>32 H</td><td>PIN-блок, зашифрованный под ZPK.<br>Если ZPK DES, то размер поля 16H.<br>Если ZPK AES, то размер поля 32H.</td></tr>
<tr><td>Код формата PIN-блока</td><td>2 N</td><td>Код формата PIN-блока.</td></tr>
<tr><td>Номер карты (PAN)/токен</td><td></td><td>Содержит токен, если PIN-блок использует токен вместо настоящего номера карты (PAN); в противном случае содержит номер карты (PAN).</td></tr>
</table>

| | | |
|---|---|---|
| | nN<br><br>или<br><br>12 N | Если поле *Код формата PIN-блока* = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель.<br>Для всех остальных значений поля *Код формата PIN-блока*:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует, только если *Код формата PIN-блока* = '48' |
| Следующие 2 поля присутствуют, если PIN-блок был сформирован с использованием токена вместо настоящего номера карты (PAN). Для формирования PVV необходимо значение PAN. | | |
| Разделитель проверочного номера карты (PAN) | 1 A | Опционально. Принимает значение ';'. Если присутствует, должно присутствовать и следующее поле.<br>Допускается использовать, только если выставлена настройка `Enable use of Tokens in PIN Verification: Yes`. |
| Проверочный номер карты (PAN) | 12 N | Присутствует, только если присутствует *Разделитель проверочного номера карты (PAN)*.<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| PVKI | 1 N | Индекс ключа проверки PIN. |
| PVV | 4 N | PVV для PIN. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'ED'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки PIN<br>'10': Нарушена четность ZPK<br>'11': Нарушена четность PVK<br>'17': Проверка PIN с помощью токена отключена;<br>'27': Алгоритм PVK отличен от 2DES<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [BC] — Проверка терминального PIN методом сравнения

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка PIN, полученного от ATM (терминала и т.п.), путем сравнения его со значением из базы данных хоста.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce key type 002 separation for PCI HSM compliance`<br>(влияет на параметры: *TPK*) | `Yes [Y]` | TPK зашифрован под LMK 36-37/7. |
| | `No [N]` | TPK зашифрован под LMK 14-15/0. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'BC'. |
| TPK | | TPK, под которым зашифрован PIN-блок. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | TPK, зашифрованный под LMK 14-15/0 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`) или LMK 36-37/7 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: Yes`). |
| | 'S' + n A | TPK должен соответствовать следующему формату:<br>Использование ключа: 'P0', '71'<br>Алгоритм: 'T', 'A'<br>Режим использования: 'B', 'D', 'N' |
| PIN-блок | 16 H<br>или<br>32 H | PIN-блок, содержащий проверяемый PIN, зашифрованный под TPK.<br>Если TPK DES, то размер поля 16H.<br>Если TPK AES, то размер поля 32H. |
| Код формата PIN-блока | 2 N | Код формата PIN-блока. |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| PIN | | PIN из базы данных хоста, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'BD'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки PIN<br>'10': Нарушена четность TPK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |

| | | |
|---|---|---|
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [BE] — Проверка PIN, полученного через систему обмена, методом сравнения

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка PIN, полученного через систему обмена, путем сравнения его со значением из базы данных хоста.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'BE'. |
| ZPK | | ZPK, под которым зашифрован PIN-блок. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | ZPK, зашифрованный под LMK 06-07. |
| | 'S' + n A | ZPK должен соответствовать следующему формату:<br>Использование ключа: 'P0', '72'<br>Алгоритм: 'T', 'A'<br>Режим использования: 'B', 'D', 'N' |
| PIN-блок | 16 H<br>или<br>32 H | PIN-блок, содержащий проверяемый PIN, зашифрованный под ZPK.<br>Если ZPK DES, то размер поля 16H.<br>Если ZPK AES, то размер поля 32H. |
| Код формата PIN-блока | 2 N | Код формата PIN-блока. |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| PIN | | PIN из базы данных хоста, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'BF'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки PIN<br>'10': Нарушена четность ZPK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 14 Команды трансляции PIN

Для трансляции PIN он должен быть передан HSM в формате 16-значного PIN-блока. HSM поддерживает несколько форматов PIN-блока, которые определяются двухзначным кодом формата PIN-блока (подробнее см. раздел «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста»).

Трансляция PIN подразумевает расшифрование PIN-блока, переданного в зашифрованном виде на HSM, перевод PIN-блока из одного формата в другой (опционально) и зашифрование PIN-блока под целевым ключом для дальнейшего использования хостом.

Команда 'QK' может использоваться для трансляции PIN, зашифрованного под LMK, когда номер карты (PAN) должен быть изменен, но старый PIN не изменяется. Рекомендуется использовать эту команду вместо небезопасной схемы трансляции PIN в промежуточный формат PIN-блока без привязки к номеру карты (PAN) и последующей трансляции в PIN-блок, включающий новый номер карты (PAN).

Следующие команды хоста используются для поддержки операции трансляции PIN:



Команда трансляции PIN, используемая при обработке транзакций DUKPT, приведена в разд. 15.

## [CC] — Трансляция PIN (из-под ZPK под ZPK)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование PIN-блока, зашифрованного под исходным ZPK, перевод PIN-блока из одного формата в другой и последующее зашифрование под целевым ZPK.

Команда поддерживает трансляцию PIN-блоков, сформированных с использованием токена вместо номера карты (PAN). Для использования данного функционала должна быть выставлена соответствующая настройка (см. ниже).

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable PIN Block Format 34 as output format for PIN translations to ZPK` | `Yes [Y]` | Доступно использование формата PIN-блока 34 в качестве возвращаемого. |
| | `No [N]` | Использование формата PIN-блока 34 в качестве возвращаемого не допускается. |
| `Enable use of Tokens in PIN Translation` (влияет на параметры: *Разделитель целевого номера карты (PAN), Целевой номер карты (PAN)*) | `Yes [Y]` | Доступна трансляция PIN-блоков, сформированных с использованием токенов вместо настоящего номера карты (PAN). |
| | `No [N]` | Трансляция PIN-блоков, сформированных с использованием токенов вместо настоящего номера карты (PAN), невозможна. |
| `Restrict PIN block usage for PCI HSM Compliance` (влияет на параметры: *Код формата возвращаемого PIN-блока*) | `Yes [Y]` | Доступна трансляция PIN-блока только в определенные форматы в соответствии с требованиями ISO 9564/ANSI X9.8 и PCI HSM. |
| | `No [N]` | Ограничения на форматы PIN-блоков не накладываются. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'CC'.</td></tr>
<tr><td>Исходный ZPK</td><td></td><td>ZPK, под которым зашифрован PIN-блок.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Исходный ZPK, зашифрованный под LMK 06-07.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Исходный ZPK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'P0', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>Целевой ZPK</td><td></td><td>ZPK, под которым будет зашифрован PIN-блок.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Целевой ZPK, зашифрованный под LMK 06-07.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Целевой ZPK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'P0', '72'</td><td>'T', 'A'</td><td>'B', 'E', 'N'</td></tr>
</table></td></tr>
<tr><td>Максимальная длина PIN</td><td>2 N</td><td>Допустимые значения: '04' .. '12'.</td></tr>
<tr><td>Исходный PIN-блок</td><td>16 H<br>или<br>32 H</td><td>Исходный PIN-блок, зашифрованный под Исходным ZPK.<br>Если Исходный ZPK DES, то размер поля 16H.<br>Если Исходный ZPK AES, то размер поля 32H.</td></tr>
<tr><td>Код формата исходного PIN-блока</td><td>2 N</td><td>Код формата исходного PIN-блока. Допустимые значения см. в главе «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста».</td></tr>
<tr><td>Код формата возвращаемого PIN-блока</td><td>2 N</td><td>Код формата возвращаемого PIN-блока. Допустимые значения см. в главе «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста».<br>Выбор формата возвращаемого PIN-блока ограничен, если выставлена настройка <code>Restrict PIN block usage for PCI compliance: Yes</code>.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют, только если Исходный PIN-блок и Возвращаемый PIN-блок используют одинаковый номер карты (PAN):</td></tr>
<tr><td>Номер карты (PAN)</td><td></td><td>Номер карты (PAN), используемый при формировании Исходного PIN-блока и Возвращаемого PIN-блока.</td></tr>
<tr><td></td><td>n N</td><td>Если Код формата исходного PIN-блока = '48' или Код формата возвращаемого PIN-блока = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель.</td></tr>
<tr><td></td><td>или<br>12 N</td><td>Для всех остальных значений полей Код формата исходного PIN-блока и Код формата возвращаемого PIN-блока:<br>12 крайних правых цифр PAN, за исключением контрольной цифры.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует только в случае Кода формата исходного PIN-блока = '48' или Кода формата возвращаемого PIN-блока = '48'.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют, если Исходный PIN-блок был сформирован с использованием токена, а Возвращаемый PIN-блок должен быть сформирован с использованием настоящего номера карты (PAN):</td></tr>
<tr><td>Исходный номер карты (PAN)</td><td></td><td>Номер карты (PAN), используемый при формировании Исходного PIN-блока.</td></tr>
</table>

| | | |
|---|---|---|
| | n N | Если *Код формата исходного PIN-блока* = '48':<br>12 крайних правых цифр Исходного PAN, за исключением контрольной цифры, или 13-19 цифр Исходного PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений поля *Код формата исходного PIN-блока*:<br>12 крайних правых цифр Исходного PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Кода формата исходного PIN-блока* = '48'. |
| Разделитель целевого номера карты (PAN) | 1 A | Значение ';'. Обязательное поле. |
| Целевой номер карты (PAN) | | Номер карты (PAN), используемый при формировании Возвращаемого PIN-блока. |
| | n N | Если *Код формата возвращаемого PIN-блока* = '48':<br>12 крайних правых цифр Целевого PAN, за исключением контрольной цифры, или 13-19 цифр Целевого PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений поля *Код формата возвращаемого PIN-блока*:<br>12 крайних правых цифр Целевого PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Кода формата возвращаемого PIN-блока* = '48'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'CD'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность исходного ZPK<br>'11': Нарушена четность целевого ZPK<br>'17': Трансляция PIN с использованием токена недоступна<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Длина PIN | 2 N | Длина возвращаемого PIN. |
| Возвращаемый PIN-блок | 16 H<br>или<br>32 H | Возвращаемый PIN-блок, зашифрованный под Целевым ZPK.<br>Если Целевой ZPK DES, то размер поля 16H.<br>Если Целевой ZPK AES, то размер поля 32H. |
| Код формата возвращаемого PIN-блока | 2 N | Соответствует указанному в команде значению. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [CA] — Трансляция PIN (из-под TPK под ZPK/BDK(3DES DUKPT))

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование PIN-блока, зашифрованного под TPK, перевод PIN-блока из одного формата в другой и последующее зашифрование под ZPK или BDK для передачи на другой узел.

Команда поддерживает трансляцию PIN-блоков, сформированных с использованием токена вместо номера карты (PAN). Для использования данного функционала должна быть выставлена соответствующая настройка (см. ниже).

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable PIN Block Format 34 as output format for PIN translations to ZPK` | `Yes [Y]` | Доступно использование формата PIN-блока 34 в качестве возвращаемого. |
| | `No [N]` | Использование формата PIN-блока 34 в качестве возвращаемого не допускается. |
| `Enable use of Tokens in PIN Translation` (влияет на параметры: *Разделитель целевого номера карты (PAN), Целевой номер карты (PAN)*) | `Yes [Y]` | Доступна трансляция PIN-блоков, сформированных с использованием токенов вместо настоящего номера карты (PAN). |
| | `No [N]` | Трансляция PIN-блоков, сформированных с использованием токенов вместо настоящего номера карты (PAN), невозможна. |
| `Restrict PIN block usage for PCI HSM Compliance` (влияет на параметры: *Код формата возвращаемого PIN-блока*) | `Yes [Y]` | Доступна трансляция PIN-блока только в определенные форматы в соответствии с требованиями ISO 9564/ANSI X9.8 и PCI HSM. |
| | `No [N]` | Ограничения на форматы PIN-блоков не накладываются. |
| `Enforce key type 002 separation for PCI HSM compliance` (влияет на параметры: *Исходный TPK*) | `Yes [Y]` | Исходный TPK зашифрован под LMK 36-37/7. |
| | `No [N]` | Исходный TPK зашифрован под LMK 14-15/0. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'CA'.</td></tr>
<tr><td>Исходный TPK</td><td></td><td>TPK, под которым зашифрован PIN-блок.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>TPK, зашифрованный под LMK 14-15/0 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: No</code>) или LMK 36-37/7 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: Yes</code>).</td></tr>
<tr><td></td><td>'S' + n A</td><td>TPK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'P0', '71'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>Флаг целевого ключа</td><td>1 A</td><td>Опциональное поле. Допустимые значения:<br>'*': Целевой ключ — BDK-1<br>'∼': Целевой ключ — BDK-2<br>Если поле отсутствует, в качестве Целевого ключа используется ZPK.</td></tr>
<tr><td>Целевой ключ</td><td></td><td>Ключ, под которым будет зашифрован PIN-блок. Поддерживаются следующие типы ключей: ZPK, BDK-1 и BDK-2.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Если поле Флаг целевого ключа отсутствует — ZPK, зашифрованный под LMK 06-07.<br>В случае Флага целевого ключа = '*' — BDK-1, зашифрованный под LMK 28-29.<br>В случае Флага целевого ключа = '∼' — BDK-2, зашифрованный под LMK 28-29/6.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ должен соответствовать одному из следующих форматов:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'P0', '72'</td><td>'T', 'A'</td><td>'B', 'E', 'N'</td></tr>
<tr><td>'B0', '41'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Дескриптор целевого KSN</td><td>3 H</td><td>Присутствует, только если тип Целевого ключа BDK-1 или BDK-2.<br>Дескриптор Целевого KSN.<br>1-я цифра: Длина идентификатора Целевого ключа ('0' — 'F')<br>2-я цифра: Значение '0'<br>3-я цифра: Длина идентификатора устройства ('0' — 'F')</td></tr>
<tr><td>Целевой KSN</td><td>12 – 20 H</td><td>Присутствует, только если тип Целевого ключа BDK-1 или BDK-2.<br>Серийный номер целевого ключа, предоставляемый хостом, который эмулирует терминал DUKPT.</td></tr>
<tr><td>Максимальная длина PIN</td><td>2 N</td><td>Допустимые значения: '04' .. '12'.</td></tr>
<tr><td>Исходный PIN-блок</td><td>16 H<br>или<br>32 H</td><td>Исходный PIN-блок, зашифрованный под Исходным TPK.<br>Если Исходный TPK DES, то размер поля 16H.<br>Если Исходный TPK AES, то размер поля 32H.</td></tr>
<tr><td>Код формата исходного PIN-блока</td><td>2 N</td><td>Код формата исходного PIN-блока. Допустимые значения см. в главе «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста».</td></tr>
<tr><td>Код формата возвращаемого PIN-блока</td><td>2 N</td><td>Код формата возвращаемого PIN-блока. Допустимые значения см. в главе «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста».<br>Выбор формата возвращаемого PIN-блока ограничен, если выставлена настройка <code>Restrict PIN block usage for PCI compliance: Yes</code>.</td></tr>
</table>

| | | |
|---|---|---|
| Следующие поля присутствуют, только если Исходный PIN-блок и Возвращаемый PIN-блок используют одинаковый номер карты (PAN): | | |
| Номер карты (PAN) | | Номер карты (PAN), используемый при формировании Исходного PIN-блока и Возвращаемого PIN-блока. |
| | n N | Если *Код формата исходного PIN-блока* = '48' или *Код формата возвращаемого PIN-блока* = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений полей *Код формата исходного PIN-блока* и *Код формата возвращаемого PIN-блока*:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Кода формата исходного PIN-блока* = '48' или *Кода формата возвращаемого PIN-блока* = '48'. |
| Следующие поля присутствуют, если Исходный PIN-блок был сформирован с использованием токена, а Возвращаемый PIN-блок должен быть сформирован с использованием настоящего номера карты (PAN): | | |
| Исходный номер карты (PAN) | | Номер карты (PAN), используемый при формировании Исходного PIN-блока. |
| | n N | Если *Код формата исходного PIN-блока* = '48':<br>12 крайних правых цифр Исходного PAN, за исключением контрольной цифры, или 13-19 цифр Исходного PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений поля *Код формата исходного PIN-блока*:<br>12 крайних правых цифр Исходного PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Кода формата исходного PIN-блока* = '48'. |
| Разделитель целевого номера карты (PAN) | 1 A | Значение ';'. Обязательное поле. |
| Целевой номер карты (PAN) | | Номер карты (PAN), используемый при формировании Возвращаемого PIN-блока. |
| | n N | Если *Код формата возвращаемого PIN-блока* = '48':<br>12 крайних правых цифр Целевого PAN, за исключением контрольной цифры, или 13-19 цифр Целевого PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений поля *Код формата возвращаемого PIN-блока*:<br>12 крайних правых цифр Целевого PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Кода формата возвращаемого PIN-блока* = '48'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'CB'. |

| | | |
|---|---|---|
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность исходного TPK<br>'11': Нарушена четность целевого ключа<br>'17': Трансляция PIN с использованием токена недоступна<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Длина PIN | 2 N | Длина возвращаемого PIN. |
| Возвращаемый PIN-блок | 16 H<br>или<br>32 H | Возвращаемый PIN-блок, зашифрованный под Целевым ключом.<br>Если Целевой ключ DES, размер поля 16H.<br>Если Целевой ключ AES, размер поля 32H. |
| Код формата возвращаемого PIN-блока | 2 N | Соответствует указанному в команде значению. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [JE] — Трансляция PIN (из-под ZPK под LMK)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование PIN-блока, зашифрованного под ZPK, и последующее зашифрование под LMK.

**Примечания:** PIN, зашифрованный под LMK, формируется в результате криптографического преобразования PIN и номера карты (PAN).

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length` (влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm` (влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A` (влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованные эмитентом, хранятся в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm` (влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованные эмитентом под AES LMK, хранятся в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Restrict PIN block usage for PCI HSM Compliance` | `Yes [Y]` | При использовании Variant LMK, 3DES Key Block LMK или AES Key Block LMK при выставленной настройке `Enforce legacy AES PIN encryption algorithm: Yes` (см. выше) PIN-блок будет переведен в формат, отличный от ISO-форматов, и команда будет возвращать ошибку 23, если исходный формат PIN-блока отличен от формата "Diebold & IBM ATM". |
| | `No [N]` | Ограничения на форматы PIN-блоков не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'JE'. |
| Исходный ZPK | | ZPK, под которым зашифрован PIN-блок. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | Исходный ZPK, зашифрованный под LMK 06-07. |
| | 'S' + n A | Исходный ZPK должен соответствовать следующему формату:<br>Использование ключа: 'P0', '72'<br>Алгоритм: 'T', 'A'<br>Режим использования: 'B', 'D', 'N' |
| PIN-блок | 16 H<br>или<br>32 H | PIN-блок, зашифрованный под Исходным ZPK.<br>Если Исходный ZPK DES, то размер поля 16H.<br>Если Исходный ZPK AES, то размер поля 32H. |
| Код формата PIN-блока | 2 N | Код формата PIN-блока. Допустимые значения см. в главе «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста». |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'JF'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность ZPK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| PIN | | PIN, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [JC] — Трансляция PIN (из-под TPK под LMK)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование PIN-блока, зашифрованного под TPK, и последующее зашифрование под LMK.

**Примечания:** PIN, зашифрованный под LMK, формируется в результате криптографического преобразования PIN и номера карты (PAN).

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Restrict PIN block usage for PCI HSM Compliance` | `Yes [Y]` | При использовании Variant LMK, 3DES Key Block LMK или AES Key Block LMK при выставленной настройке `Enforce legacy AES PIN encryption algorithm: Yes` (см. выше) PIN-блок будет переведен в формат, отличный от ISO-форматов, и команда будет возвращать ошибку 23, если исходный формат PIN-блока отличен от формата "Diebold & IBM ATM". |
| | `No [N]` | Ограничения на форматы PIN-блоков не накладываются. |
| `Enforce key type 002 separation for PCI HSM compliance`<br>(влияет на параметры: *Исходный TPK*) | `Yes [Y]` | Исходный TPK зашифрован под LMK 36-37/7. |
| | `No [N]` | Исходный TPK зашифрован под LMK 14-15/0. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'JC'. |
| Исходный TPK | | TPK, под которым зашифрован PIN-блок. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | TPK, зашифрованный под LMK 14-15/0 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`) или LMK 36-37/7 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: Yes`). |
| | 'S' + n A | TPK должен соответствовать следующему формату:<br>Использование ключа: 'P0', '71'<br>Алгоритм: 'T', 'A'<br>Режим использования: 'B', 'D', 'N' |
| PIN-блок | 16 H<br>или<br>32 H | PIN-блок, зашифрованный под Исходным TPK.<br>Если Исходный TPK DES, то размер поля 16H.<br>Если Исходный TPK AES, то размер поля 32H. |
| Код формата PIN-блока | 2 N | Код формата PIN-блока. Допустимые значения см. в главе «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста». |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'JD'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность TPK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| PIN | | PIN, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [JG] — Трансляция PIN (из-под LMK под ZPK)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование PIN-блока, зашифрованного под LMK, и последующее зашифрование под ZPK.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enable PIN Block Format 34 as output format for PIN translations to ZPK` | `Yes [Y]` | Доступно использование формата PIN-блока 34 в качестве возвращаемого. |
| | `No [N]` | Использование формата PIN-блока 34 в качестве возвращаемого не допускается. |
| `Restrict PIN block usage for PCI compliance` | `Yes [Y]` | PIN-блок будет переведен из формата, содержащего PAN, и команда будет возвращать ошибку 23, если формат возвращаемого PIN-блока не будет включать в себя PAN. |
| | `No [N]` | Ограничения на форматы PIN-блоков не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'JG'. |
| Целевой ZPK | | ZPK, под которым будет зашифрован PIN-блок. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | Целевой ZPK, зашифрованный под LMK 06-07. |
| | 'S' + n A | Целевой ZPK должен соответствовать следующему формату:<br>Использование ключа: 'P0', '72'<br>Алгоритм: 'T', 'A'<br>Режим использования: 'B', 'E', 'N' |
| Код формата PIN-блока | 2 N | Код формата PIN-блока. Допустимые значения см. в главе «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста». |
| Номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| PIN | | PIN, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или<br>'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'JH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'11': Нарушена четность ZPK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| PIN-блок | 16 H<br>или<br>32 H | PIN-блок, зашифрованный под Целевым ZPK.<br>Если Целевой ZPK DES, то размер поля 16H.<br>Если Целевой ZPK AES, то размер поля 32H. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [QK] — Трансляция номера карты для PIN, зашифрованного под LMK

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Изменение номера карты (PAN) для PIN-блока, зашифрованного под LMK 02-03. Клиентский PIN не изменяется. Для использования команды должна быть выставлена настройка `Enable translation of account number for LMK encrypted PINs: Yes`.

**Примечания:** PIN, зашифрованный под LMK, формируется в результате криптографического преобразования PIN и номера карты (PAN). Таким образом, при изменении номера карты (PAN) изменяется и PIN, зашифрованный под LMK.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `PIN length`<br>(влияет на параметры: *PIN*) | `[4-12]` | Длина PIN. |
| `PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `[A]` | Зашифрованный PIN представлен в десятичном виде. |
| | `[B]` | Зашифрованный PIN представлен в шестнадцатеричном виде. |
| `Enforce legacy PIN encryption algorithm A`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. выше). PIN, зашифрованный эмитентом, хранится в legacy формате. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enforce legacy AES PIN encryption algorithm`<br>(влияет на параметры: *PIN*) | `Yes [Y]` | PIN, зашифрованный эмитентом под AES LMK, хранится в legacy формате: вместо формата 'M' + 32 H используется 'J' + 32 H. |
| | `No [N]` | Дополнительные ограничения на формат зашифрованного PIN не накладываются. |
| `Enable translation of account number for LMK encrypted PINs` | `Yes [Y]` | Доступна трансляция номера карты (PAN) для зашифрованных под LMK PIN. |
| | `No [N]` | Трансляция номера карты (PAN) для зашифрованных под LMK PIN невозможна. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'QK'. |
| PIN | | PIN, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или 'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Старый номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или 12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| Новый номер карты (PAN) | n N | При использовании AES Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или 12 N | При использовании 3DES Variant или Key Block LMK:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует в случае, если используется AES Key Block LMK.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'QL'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| PIN | | PIN, зашифрованный под LMK. |
| | L N или L H | При использовании 3DES Variant или Key Block LMK длина зашифрованного PIN — L цифр, где L зависит от значения настройки `PIN Length`. |
| | или 'M' + 32 H | При использовании AES Key Block LMK это поле должно состоять из символа 'M' с последующими 32 шестнадцатеричными цифрами. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [AQ] — Трансляция PIN (из-под RSA под ZPK/TPK)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование PIN-блока, зашифрованного с использованием ключа RSA, перевод PIN-блока из одного формата в другой и последующее зашифрование под 3DES ZPK или TPK.

**Примечания:** *Закрытый ключ*, передаваемый в команде, должен иметь Тип ключа = 5 (зашифрование/расшифрование PIN).

Команда аналогична команде 'GI', однако вместо расшифрованных открытых данных возвращает PIN-блок, зашифрованный под указанным в команде ZPK/TPK.

Команда поддерживает трансляцию PIN-блоков, сформированных с использованием токена вместо номера карты (PAN).

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable use of Tokens in PIN Translation` (влияет на параметры: *Разделитель целевого номера карты (PAN), Целевой номер карты (PAN)*) | `Yes [Y]` | Доступна трансляция PIN-блоков, сформированных с использованием токенов вместо настоящего номера карты (PAN). |
| | `No [N]` | Трансляция PIN-блоков, сформированных с использованием токенов вместо настоящего номера карты (PAN), невозможна. |
| `Restrict PIN block usage for PCI compliance` | `Yes [Y]` | Доступна трансляция PIN-блока только в определенные форматы в соответствии с требованиями ISO 9564/ANSI X9.8 и PCI HSM. |
| | `No [N]` | Ограничения на форматы PIN-блоков не накладываются. |
| `Enforce minimum key strength of 2048-bits for RSA` (влияет на параметры: *Закрытый ключ*) | `Yes [Y]` | Длина закрытого ключа (RSA) должна быть не менее 2048 бит. |
| | `No [N]` | Ограничения на длину ключа не накладываются. |
| `Enforce key type 002 separation for PCI HSM compliance` (влияет на параметры: *TPK*) | `Yes [Y]` | TPK зашифрован под LMK 36-37/7. |
| | `No [N]` | TPK зашифрован под LMK 14-15/0. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'AQ'. |
| Идентификатор режима дополнения | 2 N | '01': PKCS#1 v2.2 method EME-PKCS1-v1_5<br>'02': PKCS#1 v2.2 method EME-OAEP |
| Функция генерации маски (MGF) | 2 N | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP).<br>'01': MGF1 (как определено в PKCS#1 v2.2) |
| Хэш-функция в MGF | 2 N | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP).<br>'01': SHA-1<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| Длина OAEP Label | 2 N | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP).<br>Если используется схема дополнения OAEP без значения Label, поле должно иметь значение '00', а следующее поле должно отсутствовать. |
| OAEP Label | n B | Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP). |
| Разделитель OAEP Label | 1 A | Значение ';'. Опционально; присутствует только в случае *Идентификатора режима дополнения* = '02' (OAEP). |
| Длина исходного PIN-блока | 4 N | Длина следующего поля. |
| Исходный PIN-блок | n B | PIN-блок, зашифрованный под открытым ключом. |
| Разделитель | 1 A | Значение ';'. Признак конца поля *Исходный PIN-блок*. |
| Флаг закрытого ключа | 2 N | Указывает расположение закрытого ключа.<br>'00' .. '20' : индекс ключа в хранилище<br>'99' : используется ключ, переданный в команде |
| Длина закрытого ключа | | Опционально; присутствует только в случае *Флага закрытого ключа* = '99'. |
| | 4 N | Длина (в байтах) следующего поля. |
| | 4 H | Значение 'FFFF'. |
| Закрытый ключ | | Опционально; присутствует только в случае *Флага закрытого ключа* = '99'. |
| | n B | Закрытый ключ, зашифрованный под LMK 34-35. |
| | 'S' + n B | Закрытый ключ должен соответствовать следующему формату:<br>Использование ключа: '05' \| Алгоритм: 'R' \| Режим использования: 'D', 'N' |
| Флаг целевого ключа | 1 N | '0': ZPK<br>'1': TPK |
| ZPK | | Присутствует только в случае *Флага целевого ключа* = '0'. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | ZPK, зашифрованный под LMK 06-07. |
| | 'S' + n A | ZPK должен соответствовать следующему формату:<br>Использование ключа: 'P0', '72' \| Алгоритм: 'T' \| Режим использования: 'B', 'E', 'N' |
| TPK | | Присутствует только в случае *Флага целевого ключа* = '1'. |

| | | |
|---|---|---|
| | 'U' + 32 H<br>или<br>'T' + 48 H | TPK, зашифрованный под LMK 14-15/0 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`) или LMK 36-37/7 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: Yes`). |
| | 'S' + n A | TPK должен соответствовать следующему формату:<br>Использование ключа: 'P0', '71'; Алгоритм: 'T'; Режим использования: 'B', 'E', 'N' |
| Код формата исходного PIN-блока | 2 N | '01': ISO 9564-1 & ANSI X9.8 формат 0<br>'05': ISO 9564-1 формат 1<br>'47': ISO 9564-1 & ANSI X9.8 формат 3 |
| Код формата возвращаемого PIN-блока | 2 N | '01': ISO 9564-1 & ANSI X9.8 формат 0<br>'03': Diebold & IBM ATM<br>'05': ISO 9564-1 формат 1<br>'47': ISO 9564-1 & ANSI X9.8 формат 3 |
| Номер карты (PAN)/токен | | Если Исходный PIN-блок использует токен вместо настоящего номера карты (PAN), это поле будет содержать номер токена. В противном случае поле будет содержать значение PAN. |
| | 12 N | 12 крайних правых цифр PAN/токена, за исключением контрольной цифры. |
| Следующие поля присутствуют, если Исходный PIN-блок был сформирован с использованием токена, а Возвращаемый PIN-блок должен быть сформирован с использованием настоящего номера карты (PAN): | | |
| Разделитель целевого номера карты (PAN) | 1 A | Значение ';'. Опционально; если присутствует, то следующее поле обязательно. |
| Целевой номер карты (PAN) | 12 N | 12 крайних правых цифр целевого PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'AR'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Недопустимый тип закрытого ключа<br>'04': Недопустимый флаг закрытого ключа<br>'07': Недопустимый идентификатор режима дополнения<br>'11': Нарушена четность ZPK или TPK<br>'17': Трансляция PIN с использованием токена недоступна<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>'76': Длина исходного PIN-блока не равна длине модуля закрытого ключа<br>'77': Ошибка расшифрованных данных<br>'78': Ошибка длины закрытого ключа<br>'85': Недопустимое значение OAEP MGF<br>'86': Недопустимая функция хэширования OAEP MGF<br>'87': Ошибка OAEP Label<br>или другой стандартный код ошибки. |
| Длина PIN | 2 N | Длина возвращаемого PIN. |

| | | |
|---|---|---|
| Возвращаемый PIN-блок | 16 H | PIN-блок, зашифрованный под ZPK или TPK в формате, определенном в поле *Код формата возвращаемого PIN-блока*. |
| Код формата возвращаемого PIN-блока | 2 N | Соответствует указанному в команде значению. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 15 Команды обработки транзакций DUKPT (X9.24)

Следующие команды хоста используются для поддержки операций DUKPT:



Указанные выше команды используются для обработки транзакций, полученных от терминалов с поддержкой схемы управления ключами DUKPT в соответствии с X9.24. Согласно DUKPT, терминал и HSM вырабатывают ключ транзакций из BDK и данных транзакции. Затем к ключу транзакции применяются соответствующие варианты для получения рабочих ключей проверки PIN, аутентификации данных.

В данном разделе описывается схема DUKPT только применительно к шифрованию PIN и аутентификации данных. Команды, поддерживающие DUKPT для шифрования данных, описаны в разделе разд. 17

В X9.24-3:2017 определены 2 метода выработки ключей аутентификации данных:

- Двунаправленный метод — для аутентификации данных, передаваемых от терминала к хосту и от хоста к терминалу, используется один ключ. Данный метод поддерживает BDK-1.
- Однонаправленный метод — для аутентификации данных, передаваемых от терминала к хосту и от хоста к терминалу, используются два разных ключа. Данный метод поддерживают BDK-2 и BDK-4.

При получении транзакции (т.е. при получении "запросных" данных транзакции от терминала, или (опционально) отправка "ответных" данных транзакции терминалу) используется BDK-1, если требуются двунаправленные ключи "терминал-эквайер", и BDK-2, если требуются однонаправленные ключи "терминал-эквайер".

Для поставщиков платежных услуг (payment service provider, PSP), которые эмулируют функцию терминала (путем передачи "запросных" данных транзакции эквайеру или (опционально) получения "ответных" данных транзакции от эквайера) используется BDK-1, если требуются двунаправленные ключи "PSP-эквайер", и BDK-4, если требуются однонаправленные ключи "PSP-эквайер".

Подробное описание схемы DUKPT и её применения в HSM см. в «КриптоПро HSM. Руководство программиста».

## Типы BDK, используемые в командах шифрования PIN и генерации/проверки MAC

### 3DES BDK

В таблице ниже приведены различные значения вариантов, применяемых к ключу транзакции в процессе выработки рабочих ключей шифрования PIN/аутентификации данных из ключа 3DES BDK.

<table>
<tr><th colspan="2">Тип 3DES BDK</th><th>Описание</th></tr>
<tr><td rowspan="2">BDK-1</td><td>BDK, зашифрованный под LMK 28-29.</td><td rowspan="2">Значения вариантов для диверсифицированного ключа транзакций:<table><tr><th>Ключевая функция</th><th>Вариант</th></tr><tr><td>Шифрование PIN</td><td>00 00 00 00 00 00 00 FF</td></tr><tr><td>Проверка "запросного" MAC</td><td>00 00 00 00 00 00 FF 00</td></tr><tr><td>Генерация "ответного" MAC</td><td>00 00 00 00 00 00 FF 00</td></tr></table>Созданные таким методом ключи являются двунаправленными.</td></tr>
<tr><td>BDK со значением Использование ключа = 'B0'.</td></tr>
<tr><td rowspan="2">BDK-2</td><td>BDK, зашифрованный под LMK 28-29/6.</td><td rowspan="2">Значения вариантов для диверсифицированного ключа транзакций:<table><tr><th>Ключевая функция</th><th>Вариант</th></tr><tr><td>Шифрование PIN</td><td>00 00 00 00 00 00 00 FF</td></tr><tr><td>Проверка "запросного" MAC</td><td>00 00 00 00 00 00 FF 00</td></tr><tr><td>Генерация "ответного" MAC</td><td>00 00 00 00 FF 00 00 00</td></tr></table>Созданные таким методом ключи являются однонаправленными.</td></tr>
<tr><td>BDK со значением Использование ключа = '41'.</td></tr>
<tr><td rowspan="2">BDK-4</td><td>BDK, зашифрованный под LMK 28-29/9.</td><td rowspan="2">Значения вариантов для диверсифицированного ключа транзакций:<table><tr><th>Ключевая функция</th><th>Вариант</th></tr><tr><td>Шифрование PIN</td><td>00 00 00 00 00 00 00 FF</td></tr><tr><td>Генерация "запросного" MAC</td><td>00 00 00 00 00 00 FF 00</td></tr><tr><td>Проверка "ответного" MAC</td><td>00 00 00 00 FF 00 00 00</td></tr></table>Созданные таким методом ключи являются однонаправленными.</td></tr>
<tr><td>BDK со значением Использование ключа = '43'.</td></tr>
</table>

**AES BDK**

В таблице ниже приведены различные значения *Индикатора использования ключа*, используемые при выработке рабочих ключей шифрования PIN/аутентификации данных из ключа AES BDK.

<table>
<tr><th colspan="2">Тип AES BDK</th><th>Описание</th></tr>
<tr><td>BDK-1</td><td>BDK со значением Использование ключа = 'B0'.</td><td>Значения Индикатора использования ключа, используемые при диверсификации ключа шифрования PIN/аутентификации сообщений:
<table>
<tr><th>Ключевая функция</th><th>Индикатор использования ключа</th></tr>
<tr><td>Шифрование PIN</td><td>0x1000</td></tr>
<tr><td>Проверка "запросного" MAC</td><td>0x2002</td></tr>
<tr><td>Генерация "ответного" MAC</td><td>0x2002</td></tr>
</table>
Созданные таким методом ключи являются двунаправленными.</td></tr>
<tr><td>BDK-2</td><td>BDK со значением Использование ключа = '41'.</td><td>Значения Индикатора использования ключа, используемые при диверсификации ключа шифрования PIN/аутентификации сообщений:
<table>
<tr><th>Ключевая функция</th><th>Индикатор использования ключа</th></tr>
<tr><td>Шифрование PIN</td><td>0x1000</td></tr>
<tr><td>Проверка "запросного" MAC</td><td>0x2000</td></tr>
<tr><td>Генерация "ответного" MAC</td><td>0x2001</td></tr>
</table>
Созданные таким методом ключи являются однонаправленными.</td></tr>
<tr><td>BDK-4</td><td>BDK со значением Использование ключа = '43'.</td><td>Значения Индикатора использования ключа, используемые при диверсификации ключа шифрования PIN/аутентификации сообщений:
<table>
<tr><th>Ключевая функция</th><th>Индикатор использования ключа</th></tr>
<tr><td>Шифрование PIN</td><td>0x1000</td></tr>
<tr><td>Генерация "запросного" MAC</td><td>0x2000</td></tr>
<tr><td>Проверка "ответного" MAC</td><td>0x2001</td></tr>
</table>
Созданные таким методом ключи являются однонаправленными.</td></tr>
</table>

## [G0] — Трансляция PIN (из-под BDK под BDK/ZPK (3DES и AES DUKPT))

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование PIN-блока, зашифрованного под BDK, и последующее зашифрование под ZPK или другим BDK для передачи на другой узел.

Команда поддерживает трансляцию PIN-блоков, сформированных с использованием токена вместо номера карты (PAN). Для использования данного функционала должна быть выставлена соответствующая настройка (см. ниже).

**Примечания:** Команда поддерживает изменение формата PIN-блока.

Команда выполняет ту же функцию, что и команды 'CA' и 'CC', за исключением того, что хост предоставляет HSM информацию, необходимую для вычисления текущего ключа. *Исходный PIN-блок* и *Исходный KSN* получены с PIN-pad.

При использовании 3DES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-1:2009. Дополнительную информацию об использовании 3DES BDK с командами шифрования PIN см. в таблице на странице 233.

При использовании AES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-3:2017. При этом у диверсифицированного ключа шифрования/расшифрования PIN индикатор использования ключа имеет значение "Шифрование PIN". Дополнительную информацию об использовании AES BDK с командами шифрования PIN см. в таблице на странице 234.

В качестве *Исходного ключа* может использоваться BDK-1 или BDK-2.

В качестве *Целевого ключа* может использоваться BDK-1, BDK-2 или BDK-4.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable PIN Block Format 34 as output format for PIN translations to ZPK` | `Yes [Y]` | Доступно использование формата PIN-блока 34 в качестве возвращаемого. |
| | `No [N]` | Использование формата PIN-блока 34 в качестве возвращаемого не допускается. |
| `Enable use of Tokens in PIN Translation` (влияет на параметры: *Разделитель целевого номера карты (PAN), Целевой номер карты (PAN)*) | `Yes [Y]` | Доступна трансляция PIN-блоков, сформированных с использованием токенов вместо настоящего номера карты (PAN). |
| | `No [N]` | Трансляция PIN-блоков, сформированных с использованием токенов вместо настоящего номера карты (PAN), невозможна. |
| `Restrict PIN block usage for PCI compliance` (влияет на параметры: *Код формата возвращаемого PIN-блока*) | `Yes [Y]` | Доступна трансляция PIN-блока только в определенные форматы в соответствии с требованиями ISO 9564/ANSI X9.8 и PCI HSM. |
| | `No [N]` | Ограничения на форматы PIN-блоков не накладываются. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'G0' (G-ноль).</td></tr>
<tr><td>Флаг исходного ключа</td><td>1 A</td><td>Значение '~' (0x7E). Опционально; если присутствует, исходный ключ — BDK-2.</td></tr>
<tr><td>Исходный ключ</td><td></td><td>Ключ, используемый для расшифрования Исходного PIN-блока.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>Если поле Флаг исходного ключа отсутствует — BDK-1, зашифрованный под LMK 28-29.<br>Если поле Флаг исходного ключа присутствует — BDK-2, зашифрованный под LMK 28-29/6.</td></tr>
<tr><td></td><td>'S' + n A</td><td>BDK-1 или BDK-2, соответствующий следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'B0', '41'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Флаг целевого ключа</td><td>1 A</td><td>Опционально; допустимые значения:<br>'*': Целевой ключ — BDK-1<br>'~': Целевой ключ — BDK-2<br>'!': Целевой ключ — BDK-4<br>Если поле отсутствует, в качестве целевого ключа используется ZPK.</td></tr>
<tr><td>Целевой ключ</td><td></td><td>Ключ, используемый для зашифрования Возвращаемого PIN-блока.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Если поле Флаг целевого ключа отсутствует — ZPK, зашифрованный под LMK 06-07.<br>Если Флаг целевого ключа = '*' — BDK-1, зашифрованный под LMK 28-29.<br>Если Флаг целевого ключа = '~' — BDK-2, зашифрованный под LMK 28-29/6.<br>Если Флаг целевого ключа = '!' — BDK-4, зашифрованный под LMK 28-29/9.</td></tr>
<tr><td></td><td>'S' + n A</td><td>ZPK или BDK-1, BDK-2, BDK-4, соответствующий одному из следующих форматов:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'P0', '72'</td><td>'T', 'A'</td><td>'B', 'E', 'N'</td></tr>
<tr><td>'B0', '41', '43'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Дескриптор исходного KSN</td><td>3 H</td><td>Дескриптор исходного KSN (в следующем поле).<br>В случае Исходного ключа AES BDK-1 или BDK-2 — значение '000'.<br>1-я цифра: Длина идентификатора исходного ключа ('0' — 'F')<br>2-я цифра: Значение '0'<br>3-я цифра: Длина идентификатора устройства ('0' — 'F')</td></tr>
<tr><td>Исходный KSN</td><td>12 - 20 H<br>или<br>24 H</td><td>Серийный номер исходного ключа, полученный от PIN-pad.<br>В случае Исходного ключа 3DES размер поля 12-20 H.<br>Для Исходного ключа AES BDK-1 или BDK-2 размер поля 24 H.</td></tr>
<tr><td>Дескриптор целевого KSN</td><td>3 H</td><td>Присутствует, только если Целевой ключ — BDK.<br>Дескриптор целевого KSN (в следующем поле).<br>В случае Целевого ключа AES BDK-1 или BDK-4 — значение '000'.<br>1-я цифра: Длина идентификатора целевого ключа ('0' — 'F')<br>2-я цифра: Значение '0'<br>3-я цифра: Длина идентификатора устройства ('0' — 'F')</td></tr>
<tr><td>Целевой KSN</td><td>12 - 20 H<br>или<br>24 H</td><td>Присутствует, только если Целевой ключ — BDK.<br>Серийный номер целевого ключа, предоставляемый хостом, который эмулирует терминал DUKPT.<br>В случае Целевого ключа 3DES BDK-1, BDK-2 или BDK-4 размер поля 12-20 H.<br>Для Целевого ключа AES BDK-1 или BDK-4 размер поля 24 H.</td></tr>
</table>

| | | |
|---|---|---|
| Исходный PIN-блок | 16 H<br>или<br>32 H | Исходный PIN-блок, зашифрованный под *Исходным ключом*, полученный от POS-терминала.<br>В случае *Исходного ключа* DES размер поля 16 H.<br>Для *Исходного ключа* AES размер поля 32 H. |
| Код формата исходного PIN-блока | 2 N | Код формата исходного PIN-блока. Допустимые значения см. в главе «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста». |
| Код формата возвращаемого PIN-блока | 2 N | Код формата возвращаемого PIN-блока. Допустимые значения см. в главе «Форматы PIN-блоков» документа «КриптоПро HSM. Руководство программиста». Выбор формата возвращаемого PIN-блока ограничен, если выставлена настройка `Restrict PIN block usage for PCI compliance: Yes`. |
| Следующие поля присутствуют, только если Исходный PIN-блок и Возвращаемый PIN-блок используют одинаковый номер карты (PAN): | | |
| Номер карты (PAN) | | Номер карты (PAN), используемый при формировании Исходного PIN-блока и Возвращаемого PIN-блока. |
| | n N | Если *Код формата исходного PIN-блока* = '48' или *Код формата возвращаемого PIN-блока* = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений полей *Код формата исходного PIN-блока* и *Код формата возвращаемого PIN-блока*:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Кода формата исходного PIN-блока* = '48' или *Кода формата возвращаемого PIN-блока* = '48'. |
| Следующие поля присутствуют, если Исходный PIN-блок был сформирован с использованием токена, а Возвращаемый PIN-блок должен быть сформирован с использованием настоящего номера карты (PAN): | | |
| Исходный номер карты (PAN) | | Номер карты (PAN), используемый при формировании Исходного PIN-блока. |
| | n N | Если *Код формата исходного PIN-блока* = '48':<br>12 крайних правых цифр Исходного PAN, за исключением контрольной цифры, или 13-19 цифр Исходного PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений поля *Код формата исходного PIN-блока*:<br>12 крайних правых цифр Исходного PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Кода формата исходного PIN-блока* = '48'. |
| Разделитель целевого номера карты (PAN) | 1 A | Значение ';'. Обязательное поле. |
| Целевой номер карты (PAN) | | Номер карты (PAN), используемый при формировании Возвращаемого PIN-блока. |
| | n N | Если *Код формата возвращаемого PIN-блока* = '48':<br>12 крайних правых цифр Целевого PAN, за исключением контрольной цифры, или 13-19 цифр Целевого PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений поля *Код формата возвращаемого PIN-блока*:<br>12 крайних правых цифр Целевого PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Кода формата возвращаемого PIN-блока* = '48'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |

| | | |
|---|---|---|
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'G1'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность исходного ключа<br>'11': Нарушена четность целевого ключа<br>'17': Трансляция PIN с использованием токена недоступна<br>'27': Недопустимая длина 3DES BDK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Длина PIN | 2 N | Длина возвращаемого PIN. |
| Возвращаемый PIN-блок | 16 H<br>или<br>32 H | Возвращаемый PIN-блок, зашифрованный под *Целевым ключом*, в формате, определенном в поле *Код формата возвращаемого PIN-блока*.<br>В случае *Целевого ключа* DES размер поля 16H.<br>Для *Целевого ключа* AES размер поля 32H. |
| Код формата возвращаемого PIN-блока | 2 N | Соответствует указанному в команде значению. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [GO] — Проверка PIN, зашифрованного под BDK, с использованием метода IBM 3624 (3DES и AES DUKPT))

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции**

Проверка PIN, зашифрованного под BDK, с использованием метода IBM 3624 (IBM Offset Method).
Команда опционально проверяет MAC с использованием ключа MAC (DUKPT).

**Примечания**

Команда выполняет ту же функцию, что и команды 'DA' и 'EA', за исключением того, что хост предоставляет HSM информацию, необходимую для вычисления текущего ключа. *PIN-блок* и *KSN* получены с DUKPT-терминала.

При использовании 3DES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-1:2009.
В случае проверки MAC HSM вырабатывает ключ транзакции из переданного в команде BDK:

- При использовании BDK-1 данные для проверки MAC могут быть данными "запроса" или "ответа" (в обоих случаях диверсифицированный ключ будет одинаковым).
- При использовании BDK-2 данные для проверки MAC считаются данными "запроса".

Дополнительную информацию об использовании 3DES BDK с командами шифрования PIN и проверки MAC см. в таблице на странице 233.

При использовании AES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-3:2017. У диверсифицированного ключа расшифрования PIN индикатор использования ключа имеет значение "Шифрование PIN".

В случае проверки MAC HSM вырабатывает ключ транзакции из переданного в команде BDK:

- При использовании BDK-1 у диверсифицированного ключа проверки MAC индикатор использования ключа имеет значение "Аутентификация сообщения, двунаправленная".
- При использовании BDK-2 у диверсифицированного ключа проверки MAC индикатор использования ключа имеет значение "Аутентификация сообщения, проверка".

Дополнительную информацию об использовании AES BDK с командами шифрования PIN и проверки MAC см. в таблице на странице 234.

Ключ MAC используется для проверки MAC, полученного от терминала.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Decimalization tables`<br>(влияет на параметры: *Таблица децимализации*) | `Encrypted [E]`<br>`(по умолчанию)` | Таблица децимализации, подаваемая на вход, должна быть зашифрована (с помощью консольной команды ED) и состоять из 16 шестнадцаритичных символов (для Variant LMK или 3DES Key Block LMK) или 'L' + 32 шестнадцаритичных символов (для AES Key Block LMK). |
| | `Plaintext [P]` | Таблица децимализации, подаваемая на вход, должна быть незашифрована и состоять из 16 десятичных символов. |
| `Enable Decimalization Table checks` | `Yes [Y]`<br>`(по умолчанию)` | Выполняется проверка таблицы децимализации, подаваемой на вход: таблица децимализации должна содержать не менее 8 различных цифр, и каждая цифра должна повторяться не более 4 раз. Если требование не выполняется, возвращается ошибка 25. |
| | `No [N]` | Проверка таблицы децимализации не выполняется. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'GO'.</td></tr>
<tr><td>Режим</td><td>1 N</td><td>'0': Только проверка PIN (с использованием двунаправленного ключа PIN)<br>'1': Проверка PIN и проверка MAC<br>'2': Только проверка PIN (с использованием однонаправленного ключа PIN)</td></tr>
<tr><td>Режим MAC</td><td>1 A</td><td>Присутствует только в случае Режима = '1'.<br>'1' & 'A': Проверка 8-байтового MAC<br>'2' & 'B': Проверка 4-байтового MAC (крайние левые 4 байта)<br>'3' & 'C': Проверка 4-байтового MAC (крайние правые 4 байта)<br><br>Значения '1' .. '3' используются для режима проверки MAC с использованием двунаправленного ключа MAC, значения 'A' .. 'C' — проверки MAC с использованием однонаправленного ключа MAC.</td></tr>
<tr><td>Алгоритм MAC</td><td>1 N</td><td>Присутствует только в случае Режима = '1'.<br>'1': ANSI X9.19 (только 3DES BDK)<br>'2': CBC MAC (только AES BDK)<br>'3': CMAC (только AES BDK)</td></tr>
<tr><td>BDK</td><td></td><td>BDK, используемый для расшифрования PIN-блока и проверки MAC (опционально).</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>Если Режим = '0' или Режим = '1' и Режим MAC = '1' .. '3' — BDK-1, зашифрованный под LMK 28-29.<br>Если Режим = '2' или Режим = '1' и Режим MAC = 'A' .. 'C' — BDK-2, зашифрованный под LMK 28-29/6.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Если Режим = '0' или Режим = '1' и Режим MAC = '1' .. '3' — BDK-1, соответствующий следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'B0'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table>
Если Режим = '2' или Режим = '1' и Режим MAC = 'A' .. 'C' — BDK-2, соответствующий следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'41'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>PVK</td><td></td><td>PVK, используемый для проверки PIN клиента.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>PVK, зашифрованный под LMK 14-15/0.</td></tr>
<tr><td></td><td>'S' + n A</td><td>PVK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'V1'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Дескриптор KSN</td><td>3 H</td><td>Дескриптор KSN (в следующем поле).<br>В случае AES BDK-1 или BDK-2 — значение '000'.</td></tr>
<tr><td>KSN</td><td>12 - 20 H<br>или<br>24 H</td><td>Серийный номер ключа, полученный от PIN-pad .<br>В случае 3DES BDK-1 или BDK-2 размер поля 12-20 H.<br>Для AES BDK-1 или BDK-2 размер поля 24 H.</td></tr>
<tr><td>PIN-блок</td><td>16 H<br>или<br>32 H</td><td>Зашифрованный PIN-блок, полученный от POS-терминала.<br>В случае 3DES BDK размер поля 16 H.<br>Для AES BDK размер поля 32 H.</td></tr>
</table>

| | | |
|---|---|---|
| Код формата PIN-блока | 2 N | '01': ANSI X9.8 формат 0<br>'05': ISO 9564-1 формат 1, ANSI X9.8 формат 1<br>'47': ISO 9564-1 формат 3<br>'48': ISO 9564-1 формат 4 |
| Проверочная длина | 2 N | Число правых цифр значения IBM offset, которые необходимо проверить. |
| Номер карты (PAN) | | Номер карты, используемый при формировании PIN-блока. |
| | n N | Если *Код формата PIN-блока* = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений поля *Код формата PIN-блока*:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует, только если *Код формата PIN-блока* = '48'.<br>*Примечание:* разделитель может отсутствовать при использовании PAN длины 12. |
| Таблица децимализации | 16 N<br>или | 16 N при использовании незашифрованной таблицы децимализации. |
| | 16 H<br>или | 16 H при использовании зашифрованной таблицы децимализации и Variant LMK или 3DES Key Block LMK. |
| | 'L' + 32 H | 'L' + 32 H при использовании зашифрованной таблицы децимализации и AES Key Block LMK. |
| Данные для проверки PIN | 12 A | Пользовательские данные, состоящие из шестнадцатеричных символов и символа 'N', который указывает HSM, где расположить последние 5 цифр PAN. |
| | или | или |
| | 'P' + 16 H | Пользовательские данные, состоящие из ASCII символа 'P', дополненного 16 шестнадцатеричными цифрами, которые будут использоваться в качестве входа для алгоритма генерации PIN. |
| IBM offset | 12 H | Значение IBM offset, выровненное по левому краю и дополненное 'F'. |
| MAC | 8 H<br>или<br>16 H | Присутствует только в случае *Режима* = '1'.<br>Проверяемое значение MAC.<br>В случае *Режима MAC* = '1' или 'A' размер поля 16 H.<br>В случае *Режима MAC* = '2', '3', 'B' или 'C' размер поля 8 H. |
| Длина сообщения | 4 N | Присутствует только в случае *Режима* = '1'.<br>Длина (в байтах) следующего поля, должна быть кратна 8 байтам. |
| Сообщение | n B | Присутствует только в случае *Режима* = '1'.<br>Сообщение, для которого проверяется значение MAC. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'GP'. |

| | | |
|---|---|---|
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки PIN<br>'10': Нарушена четность BDK<br>'11': Нарушена четность PVK<br>'27': Алгоритм BDK отличен от 2DES<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Код ошибки MAC | 2 N | Присутствует только в случае *Режима* = '1'.<br>'00': Без ошибок<br>'01': Ошибка проверки MAC |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [GQ] — Проверка PIN, зашифрованного под BDK, с использованием метода ABA PVV (3DES и AES DUKPT))

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции**

Проверка PIN, зашифрованного под BDK, с использованием метода ABA PVV.
Команда опционально проверяет MAC с использованием ключа MAC (DUKPT).

Команда поддерживает проверку PIN-блоков, сформированных с использованием токена вместо номера карты (PAN). Для использования данного функционала должна быть выставлена соответствующая настройка (см. ниже).

**Примечания**

Команда выполняет ту же функцию, что и команды 'DC' и 'EC', за исключением того, что хост предоставляет HSM информацию, необходимую для вычисления текущего ключа. *PIN-блок* и *KSN* получены с DUKPT-терминала.

При использовании 3DES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-1:2009.
В случае проверки MAC HSM вырабатывает ключ транзакции из переданного в команде BDK:

- При использовании BDK-1 данные для проверки MAC могут быть данными "запроса" или "ответа" (в обоих случаях диверсифицированный ключ будет одинаковым).
- При использовании BDK-2 данные для проверки MAC считаются данными "запроса".

Дополнительную информацию об использовании 3DES BDK с командами шифрования PIN и проверки MAC см. в таблице на странице 233.

При использовании AES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-3:2017. У диверсифицированного ключа расшифрования PIN индикатор использования ключа имеет значение "Шифрование PIN".

В случае проверки MAC HSM вырабатывает ключ транзакции из переданного в команде BDK:

- При использовании BDK-1 у диверсифицированного ключа проверки MAC индикатор использования ключа имеет значение "Аутентификация сообщения, двунаправленная".
- При использовании BDK-2 у диверсифицированного ключа проверки MAC индикатор использования ключа имеет значение "Аутентификация сообщения, проверка".

Дополнительную информацию об использовании AES BDK с командами шифрования PIN и проверки MAC см. в таблице на странице 234.

Ключ MAC используется для проверки MAC, полученного от терминала.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable use of Tokens in PIN Verification` (влияет на параметры: *Разделитель проверочного номера карты (PAN), Проверочный номер карты (PAN)*) | `Yes [Y]` | Доступна проверка PIN-блоков, сформированных с использование токенов вместо настоящего номера карты (PAN). |
| | `No [N]` | Проверка PIN-блоков, сформированных с использование токенов вместо настоящего номера карты (PAN), невозможна. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'GQ'.</td></tr>
<tr><td>Режим</td><td>1 N</td><td>'0': Только проверка PIN (с использованием двунаправленного ключа PIN)<br>'1': Проверка PIN и проверка MAC<br>'2': Только проверка PIN (с использованием однонаправленного ключа PIN)</td></tr>
<tr><td>Режим MAC</td><td>1 A</td><td>Присутствует только в случае Режима = '1'.<br>'1' & 'A': Проверка 8-байтового MAC<br>'2' & 'B': Проверка 4-байтового MAC (крайние левые 4 байта)<br>'3' & 'C': Проверка 4-байтового MAC (крайние правые 4 байта)<br>Значения '1' .. '3' используются для режима проверки MAC с использованием двунаправленного ключа MAC, значения 'A' .. 'C' — проверки MAC с использованием однонаправленного ключа MAC.</td></tr>
<tr><td>Алгоритм MAC</td><td>1 N</td><td>Присутствует только в случае Режима = '1'.<br>'1': ANSI X9.19 (только 3DES BDK)<br>'2': CBC MAC (только AES BDK)<br>'3': CMAC (только AES BDK)</td></tr>
<tr><td>BDK</td><td></td><td>BDK, используемый для расшифрования PIN-блока и проверки MAC (опционально).</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>Если Режим = '0' или Режим = '1' и Режим MAC = '1' .. '3' — BDK-1, зашифрованный под LMK 28-29.<br>Если Режим = '2' или Режим = '1' и Режим MAC = 'A' .. 'C' — BDK-2, зашифрованный под LMK 28-29/6.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Если Режим = '0' или Режим = '1' и Режим MAC = '1' .. '3' — BDK-1, соответствующий следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'B0'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table>
Если Режим = '2' или Режим = '1' и Режим MAC = 'A' .. 'C' — BDK-2, соответствующий следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'41'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>PVK</td><td></td><td>PVK, используемый для проверки PIN клиента.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>PVK, зашифрованный под LMK 14-15/0.</td></tr>
<tr><td></td><td>'S' + n A</td><td>PVK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'V2'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Дескриптор KSN</td><td>3 H</td><td>Дескриптор KSN (в следующем поле).<br>В случае AES BDK-1 или BDK-2 — значение '000'.</td></tr>
<tr><td>KSN</td><td>12 - 20 H<br>или<br>24 H</td><td>Серийный номер ключа, полученный от PIN-pad .<br>В случае 3DES BDK-1 или BDK-2 размер поля 12-20 H.<br>Для AES BDK-1 или BDK-2 размер поля 24 H.</td></tr>
<tr><td>PIN-блок</td><td>16 H<br>или<br>32 H</td><td>Зашифрованный PIN-блок, полученный от POS-терминала.<br>В случае DES BDK размер поля 16 H.<br>Для AES BDK размер поля 32 H.</td></tr>
<tr><td>Код формата PIN-блока</td><td>2 N</td><td>'01': ANSI X9.8 формат 0<br>'05': ISO 9564-1 формат 1, ANSI X9.8 формат 1<br>'47': ISO 9564-1 формат 3<br>'48': ISO 9564-1 формат 4</td></tr>
</table>

| | | |
|---|---|---|
| Номер карты (PAN)/токен | | Если *Исходный PIN-блок* использует токен вместо настоящего номера карты (PAN), поле содержит номер токена. В противном случае поле содержит значение PAN. |
| | n N | Если *Код формата PIN-блока* = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений поля *Код формата PIN-блока*:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Кода формата PIN-блока* = '48'. |
| Следующие 2 поля присутствуют, если PIN-блок был сформирован с использованием токена вместо настоящего номера карты (PAN), и для формирования PVV необходимо значение PAN: | | |
| Разделитель проверочного номера карты (PAN) | 1 A | Значение ';'. Опционально; если присутствует, следующее поле обязательно.<br>Допускается использовать, только если выставлена настройка `Enable use of Tokens in PIN Verification: Yes`. |
| Проверочный номер карты (PAN) | 12 N | Присутствует, только если присутствует предыдущее поле.<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| PVKI | 1 N | Индекс ключа проверки PIN. |
| PVV | 4 N | Значение PVV с карты или из базы данных. |
| MAC | 8 H<br>или<br>16 H | Присутствует только в случае *Режима* = '1'.<br>Проверяемое значение MAC.<br>В случае *Режима MAC* = '1' или 'A' размер поля 16 H.<br>В случае *Режима MAC* = '2', '3', 'B' или 'C' размер поля 8 H. |
| Длина сообщения | 4 N | Присутствует только в случае *Режима* = '1'.<br>Длина (в байтах) следующего поля, должна быть кратна 8 байтам. |
| Сообщение | n B | Присутствует только в случае *Режима* = '1'.<br>Сообщение, для которого проверяется значение MAC. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'GR'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки PIN<br>'10': Нарушена четность BDK<br>'11': Нарушена четность PVK<br>'17': Проверка PIN с использованием токена недоступна<br>'27': Некорректная длина 3DES BDK<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| Код ошибки MAC | 2 N | Присутствует только в случае *Режима* = '1'.<br>'00': Без ошибок<br>'01': Ошибка проверки MAC |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |

| | | |
|---|---|---|
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [GW] — Генерация/проверка MAC (3DES и AES DUKPT))

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции** Генерация или проверка MAC для сообщения с использованием ключа MAC, выработанного из BDK в соответствии с DUKPT.

**Примечания** При использовании 3DES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-1:2009:

- При использовании BDK-1 данные для генерации/проверки MAC могут быть данными "запроса" или "ответа" (в обоих случаях диверсифицированный ключ будет одинаковым).
- При использовании BDK-2 данные для генерации MAC считаются данными "ответа", а данные для проверки MAC считаются данными "запроса".
- При использовании BDK-4 данные для генерации MAC считаются данными "запроса", а данные для проверки MAC считаются данными "ответа".

Дополнительную информацию об использовании 3DES BDK с командами генерации/проверки MAC см. в таблице на странице 233.

При использовании AES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-3:2017:

- При использовании BDK-1 у диверсифицированного ключа генерации/проверки MAC индикатор использования ключа имеет значение "Аутентификация сообщения, двунаправленная".
- При использовании BDK-2 или BDK-4 у диверсифицированного ключа генерации MAC индикатор использования ключа имеет значение "Аутентификация сообщения, генерация".
- При использовании BDK-2 или BDK-4 у диверсифицированного ключа проверки MAC индикатор использования ключа имеет значение "Аутентификация сообщения, проверка".

Дополнительную информацию об использовании AES BDK с командами генерации/проверки MAC см. в таблице на странице 234.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'GW'.</td></tr>
<tr><td>Режим MAC</td><td>1 A</td><td>'1', 'A', 'G': Проверка 8-байтового MAC<br>'2', 'B', 'H': Проверка Approval MAC (крайние левые 4 байта)<br>'3', 'C', 'I': Проверка Decline MAC (крайние правые 4 байта)<br>'4', 'D', 'J': Генерация 8-байтового MAC<br>'5', 'E', 'K': Генерация Approval MAC (крайние левые 4 байта)<br>'6', 'F', 'L': Генерация Decline MAC (крайние правые 4 байта)<br><br>Значения '1' .. '6' используются в случае BDK-1 (двунаправленные ключи MAC)<br>Значения 'A' .. 'C' используются в случае BDK-2 (однонаправленные "запросные" ключи MAC)<br>Значения 'D' .. 'F' используются в случае BDK-2 (однонаправленные "ответные" ключи MAC)<br>Значения 'G' .. 'I' используются в случае BDK-4 (однонаправленные "ответные" ключи MAC)<br>Значения 'J' .. 'L' используются в случае BDK-4 (однонаправленные "запросные" ключи MAC)</td></tr>
<tr><td>Алгоритм MAC</td><td>1 N</td><td>'1': ANSI X9.19 (только 3DES BDK)<br>'2': AS2805.4.1 (2001) (только 3DES BDK)<br>'3': CBC MAC (только AES BDK)<br>'4': CMAC (только AES BDK)</td></tr>
<tr><td>BDK</td><td></td><td>BDK, используемый для выработки ключа MAC.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>Если Режим MAC = '1' .. '6' — BDK-1, зашифрованный под LMK 28-29.<br>Если Режим MAC = 'A' .. 'F' — BDK-2, зашифрованный под LMK 28-29/6.<br>Если Режим MAC = 'G' .. 'L' — BDK-4, зашифрованный под LMK 28-29/9.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Если Режим MAC = '1' .. '6' — BDK-1, соответствующий следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'B0'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table>
Если Режим MAC = 'A' .. 'F' — BDK-2, соответствующий следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'41'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table>
Если Режим MAC = 'G' .. 'L' — BDK-4, соответствующий следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'43'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Дескриптор KSN</td><td>3 H</td><td>Дескриптор KSN (в следующем поле).<br>В случае AES BDK-1, BDK-2 или BDK-4 — значение '000'.</td></tr>
<tr><td>KSN</td><td>12 - 20 H<br>или<br>24 H</td><td>Серийный номер ключа, полученный от PIN-pad .<br>В случае 3DES BDK-1, BDK-2 или BDK-4 размер поля 12-20 H.<br>Для AES BDK-1, BDK-2 или BDK-4 размер поля 24 H.</td></tr>
<tr><td>MAC</td><td>8 H<br>или<br>16 H</td><td>Присутствует только в случае Режима MAC = '1', '2', '3', 'A', 'B', 'C', 'G', 'H', 'I' .<br>Проверяемое значение MAC.<br>В случае Режима MAC = '1', 'A' или 'G' размер поля 16 H.<br>В случае Режима MAC = '2', '3', 'B', 'C', 'H' или 'I' размер поля 8 H.</td></tr>
</table>

| | | |
|---|---|---|
| Длина сообщения | 4 N | Длина (в байтах) следующего поля.<br>В случае *Алгоритма MAC* = '1' или '2' должна быть кратна 8 байтам.<br>В случае *Алгоритма MAC* = '3' должна быть кратна 16 байтам. |
| Сообщение | n B | Сообщение, для которого генерируется/проверяется значение MAC. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'GX'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| MAC | 8 H<br>или<br>16 H | Присутствует только в случае *Режима MAC* = '4', '5', '6', 'D', 'E', 'F', 'J', 'K', 'L' .<br>Сгенерированное значение MAC.<br>В случае *Режима MAC* = '4', 'D' или 'J' размер поля 16 H.<br>В случае *Режима MAC* = '5', '6', 'E', 'F', 'K' или 'L' размер поля 8 H. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 16 Команды обеспечения целостности сообщений

MAC (Message Authentication Code, код аутентификации сообщения, имитовставка) используется для обеспечения целостности сообщения и аутентификации отправителя. Для вычисления MAC используются определенные поля сообщения и ключ MAC.

При получении сообщения принимающая сторона вычисляет MAC и сравнивает его с полученным значением MAC, вычисленным отправителем.

Пользователь выбирает несколько параметров:

- поля сообщения, используемые при вычислении MAC
- порядок этих полей
- формат этих полей

При обработке транзакций за корректность форматирования данных отвечает хост. На HSM передаются данные переменной длины для вычисления MAC и HSM использует полученные данные в том виде, в котором получил их, дополненные до длины блока в случае необходимости.

Следующие команды хоста используются для обеспечения целостности сообщений:

## [M6] — Генерация MAC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация MAC для сообщения с использованием TAK или ZAK.
Команда поддерживает различные алгоритмы вычисления MAC и режимы дополнения (подробнее см. описание команды).

**Примечания:** Данные, для которых вычисляется значение MAC, могут быть переданы в HSM в различных форматах в соответствии со значением, указанным в поле *Флаг формата входных данных*.

При использовании Key Block значение поля Использование ключа определяет доступные алгоритмы вычисления MAC и режимы дополнения:

| Использование ключа | Алгоритм | Допустимые алгоритмы MAC | Допустимые режимы дополнения |
|---|---|---|---|
| 'M1' | 'T' | ISO 9797 MAC алгоритм 1 | • Без дополнения<br>• ISO 9797 режим дополнения 1<br>• ISO 9797 режим дополнения 2<br>• ISO 9797 режим дополнения 3 |
| 'M3' | 'T' | ISO 9797 MAC алгоритм 3 | |
| 'M5' | 'A' | CBC MAC | |
| 'M6' | 'A' | CMAC | дополнение AES CMAC |

Максимальное значение поля *Длина сообщения* зависит от формата входных данных, при этом максимальная длина всей команды ограничена 32 КБ.

В случае вычисления MAC для сообщения, состоящего из нескольких блоков, промежуточные значения IV будут зашифрованы с использованием ключа, выработанного из ключа MAC.

При генерации MAC для нескольких блоков сообщения (*Флаг режима* = '1', '2' или '3') ограничена минимальная длина каждого блока сообщения:

• в случае ключа 3DES: минимальная длина блока сообщения 24 байта (бинарные данные) или 48 шестнадцатеричных символов;
• в случае ключа AES: минимальная длина блока сообщения 48 байтов (бинарные данные) или 96 шестнадцатеричных символов.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'M6'.</td></tr>
<tr><td>Флаг режима</td><td>1 N</td><td>'0': Единственный блок сообщения<br>'1': Первый блок сообщения из нескольких блоков<br>'2': Промежуточный блок сообщения из нескольких блоков<br>'3': Последний блок сообщения из нескольких блоков</td></tr>
<tr><td>Флаг формата входных данных</td><td>1 N</td><td>'0': Бинарные данные<br>'1': Бинарные данные в шестнадцатеричном формате<br>'2': Текстовые данные</td></tr>
<tr><td>Размер MAC</td><td>1 N</td><td>'0': 8 шестнадцатеричных символов<br>'1': 16 шестнадцатеричных символов</td></tr>
<tr><td>Алгоритм MAC</td><td>1 N</td><td>'1': ISO 9797 MAC алгоритм 1 (только DES)<br>'3': ISO 9797 MAC алгоритм 3 (= ANSI X9.19 если используется с ключом 2DES) (только DES)<br>'5': CBC-MAC (только AES)<br>'6': CMAC (только AES)</td></tr>
<tr><td>Режим дополнения</td><td>1 N</td><td>В случае Алгоритма MAC = '1', '3' или '5':<br>'0': Без дополнения (общая длина сообщения должна быть кратна 8 байтам для Алгоритма MAC = '1' или '3', 16 байтам для Алгоритма MAC = '5')<br>'1': ISO 9797 режим дополнения 1 (дополнить 0x00)<br>'2': ISO 9797 режим дополнения 2 (добавить 0x80 и дополнить 0x00)<br>'3': ISO 9797 режим дополнения 3 (добавить перед сообщением значение длины, дополнить 0x00)<br>Примечание: если Режим дополнения = '3', Флаг режима должен иметь значение '0'.<br>В случае Алгоритма MAC = '6':<br>'4': дополнение AES CMAC</td></tr>
<tr><td>Тип ключа</td><td>3 H</td><td>Тип используемого ключа:<br>'003': TAK, зашифрованный под LMK 16-17<br>'008': ZAK, зашифрованный под LMK 26-27</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Ключ MAC</td><td></td><td>Ключ MAC, используемый совместно с IV (в соответствующих случаях) для генерации MAC.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>TAK или ZAK (в соответствии со значением Тип ключа).</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'M1'</td><td>'T'</td><td>'C', 'G', 'N'</td></tr>
<tr><td>'M3'</td><td>'T'</td><td>'C', 'G', 'N'</td></tr>
<tr><td>'M5', 'M6'</td><td>'A'</td><td>'C', 'G', 'N'</td></tr>
</table></td></tr>
<tr><td>IV</td><td>16 H<br>или<br>32 H</td><td>Присутствует только в случае Флага режима = '2' или '3'.<br>Промежуточный вектор инициализации.<br>При генерации MAC для промежуточного или последнего блока сообщения используется значение IV, возвращаемое в ответе при генерации MAC для предыдущего блока.<br>В случае ключа 3DES размер поля 16 H.<br>Для ключа AES размер поля 32 H.</td></tr>
<tr><td>Длина сообщения</td><td>4 H</td><td>Длина (в байтах) следующего поля. Максимальное значение: 0x7D00 (32000) байт.</td></tr>
</table>

| | | |
|---|---|---|
| Сообщение | | Сообщение, для которого вычисляется значение MAC. |
| | n B | В случае *Флага формата входных данных* = '0' (бинарные данные):<br>Если *Флаг режима* = '1' или '2':<br>n должно быть кратно 8 при использовании ключа DES<br>n должно быть кратно 16 при использовании ключа AES |
| | или<br>n H | В случае *Флага формата входных данных* = '1' (бинарные данные в шестнадцатеричном формате):<br>Если *Флаг режима* = '1' или '2':<br>n должно быть кратно 16 при использовании ключа DES<br>n должно быть кратно 32 при использовании ключа AES |
| | или<br>n A | В случае *Флага формата входных данных* = '2' (текстовые данные):<br>Если *Флаг режима* = '1' или '2':<br>n должно быть кратно 8 при использовании ключа DES<br>n должно быть кратно 16 при использовании ключа AES |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | **ОТВЕТ** | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'M7'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'02': Недопустимый флаг режима<br>'03': Недопустимый флаг формата входных данных<br>'04': Недопустимый размер MAC или алгоритм MAC<br>'05': Недопустимый тип ключа<br>'06': Недопустимая длина сообщения<br>'09': Недопустимый режим дополнения<br>'10': Нарушена четность ключа MAC<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| IV | 16 H<br>или<br>32 H | Присутствует только в случае *Флага режима* = '1' или '2'.<br>Промежуточный вектор инициализации.<br>При генерации MAC для нескольких блоков данных этот IV должен подаваться как входной в команде генерации MAC для следующего блока.<br>В случае ключа 3DES размер поля 16 H.<br>Для ключа AES размер поля 32 H. |
| MAC | 8 H<br>или<br>16 H | Присутствует только в случае *Флага режима* = '0' или '3'.<br>Вычисленное значение MAC.<br>Длина поля определяется значением поля *Размер MAC*. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [M8] — Проверка MAC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка MAC для сообщения с использованием TAK или ZAK.
Команда поддерживает различные алгоритмы вычисления MAC и режимы дополнения (подробнее см. описание команды).

**Примечания:** Данные, для которых проверяется MAC, могут быть переданы в HSM в различных форматах в соответствии со значением, указанным в поле *Флаг формата входных данных*.

При использовании Key Block значение поля Использование ключа определяет доступные алгоритмы вычисления MAC и режимы дополнения:

| Использование ключа | Алгоритм | Допустимые алгоритмы MAC | Допустимые режимы дополнения |
|---|---|---|---|
| 'M1' | 'T' | ISO 9797 MAC алгоритм 1 | • Без дополнения<br>• ISO 9797 режим дополнения 1<br>• ISO 9797 режим дополнения 2<br>• ISO 9797 режим дополнения 3 |
| 'M3' | 'T' | ISO 9797 MAC алгоритм 3 | |
| 'M5' | 'A' | CBC MAC | |
| 'M6' | 'A' | CMAC | дополнение AES CMAC |

Максимальное значение поля *Длина сообщения* зависит от формата входных данных, при этом максимальная длина всей команды ограничена 32 КБ.

В случае проверки MAC для сообщения, состоящего из нескольких блоков, промежуточные значения IV будут зашифрованы с использованием ключа, выработанного из ключа MAC.

При проверке MAC для нескольких блоков сообщения (*Флаг режима* = '1', '2' или '3') ограничена минимальная длина каждого блока сообщения:

• в случае ключа 3DES: минимальная длина блока сообщения 24 байта (бинарные данные) или 48 шестнадцатеричных символов;
• в случае ключа AES: минимальная длина блока сообщения 48 байтов (бинарные данные) или 96 шестнадцатеричных символов.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'M8'.</td></tr>
<tr><td>Флаг режима</td><td>1 N</td><td>'0': Единственный блок сообщения<br>'1': Первый блок сообщения из нескольких блоков<br>'2': Промежуточный блок сообщения из нескольких блоков<br>'3': Последний блок сообщения из нескольких блоков</td></tr>
<tr><td>Флаг формата входных данных</td><td>1 N</td><td>'0': Бинарные данные<br>'1': Бинарные данные в шестнадцатеричном формате<br>'2': Текстовые данные</td></tr>
<tr><td>Размер MAC</td><td>1 N</td><td>'0': 8 шестнадцатеричных символов<br>'1': 16 шестнадцатеричных символов</td></tr>
<tr><td>Алгоритм MAC</td><td>1 N</td><td>'1': ISO 9797 MAC алгоритм 1 (только DES)<br>'3': ISO 9797 MAC алгоритм 3 (= ANSI X9.19 если используется с ключом 2DES) (только DES)<br>'5': CBC-MAC (только AES)<br>'6': CMAC (только AES)</td></tr>
<tr><td>Режим дополнения</td><td>1 N</td><td>В случае Алгоритма MAC = '1', '3' или '5':<br>'0': Без дополнения (общая длина сообщения должна быть кратна 8 байтам для Алгоритма MAC = '1' или '3', 16 байтам для Алгоритма MAC = '5')<br>'1': ISO 9797 режим дополнения 1 (дополнить 0x00)<br>'2': ISO 9797 режим дополнения 2 (добавить 0x80 и дополнить 0x00)<br>'3': ISO 9797 режим дополнения 3 (добавить перед сообщением значение длины, дополнить 0x00)<br>Примечание: если Режим дополнения = '3', Флаг режима должен иметь значение '0'.<br>В случае Алгоритма MAC = '6':<br>'4': дополнение AES CMAC</td></tr>
<tr><td>Тип ключа</td><td>3 H</td><td>Тип используемого ключа:<br>'003': TAK, зашифрованный под LMK 16-17<br>'008': ZAK, зашифрованный под LMK 26-27</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Ключ MAC</td><td></td><td>Ключ MAC, используемый совместно с IV (в соответствующих случаях) для проверки MAC.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>TAK или ZAK (в соответствии со значением Тип ключа).</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'M1'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr>
<tr><td>'M3'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr>
<tr><td>'M5', 'M6'</td><td>'A'</td><td>'C', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>IV</td><td>16 H<br>или<br>32 H</td><td>Присутствует только в случае Флага режима = '2' или '3'.<br>Промежуточный вектор инициализации.<br>При проверке MAC для промежуточного или последнего блока сообщения используется значение IV, возвращаемое в ответе при проверке MAC для предыдущего блока.<br>В случае ключа 3DES размер поля 16 H.<br>Для ключа AES размер поля 32 H.</td></tr>
<tr><td>Длина сообщения</td><td>4 H</td><td>Длина (в байтах) следующего поля. Максимальное значение: 0x7D00 (32000) байт.</td></tr>
</table>

| | | |
|---|---|---|
| Сообщение | | Сообщение, для которого проверяется значение MAC. |
| | n B | В случае *Флага формата входных данных* = '0' (бинарные данные):<br>Если *Флаг режима* = '1' или '2':<br>n должно быть кратно 8 при использовании ключа DES<br>n должно быть кратно 16 при использовании ключа AES |
| | или<br>n H | В случае *Флага формата входных данных* = '1' (бинарные данные в шестнадцатеричном формате):<br>Если *Флаг режима* = '1' или '2':<br>n должно быть кратно 16 при использовании ключа DES<br>n должно быть кратно 32 при использовании ключа AES |
| | или<br>n A | В случае *Флага формата входных данных* = '2' (текстовые данные):<br>Если *Флаг режима* = '1' или '2':<br>n должно быть кратно 8 при использовании ключа DES<br>n должно быть кратно 16 при использовании ключа AES |
| MAC | 8 H<br>или<br>16 H | Присутствует только в случае *Флага режима* = '0' или '3'.<br>Проверяемое значение MAC.<br>Длина поля определяется значением поля *Размер MAC*. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'M9'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'02': Недопустимый флаг режима<br>'03': Недопустимый флаг формата входных данных<br>'04': Недопустимый размер MAC или алгоритм MAC<br>'05': Недопустимый тип ключа<br>'06': Недопустимая длина сообщения<br>'09': Недопустимый режим дополнения<br>'10': Нарушена четность ключа MAC<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| IV | 16 H<br>или<br>32 H | Присутствует только в случае *Флага режима* = '1' или '2'.<br>Промежуточный вектор инициализации.<br>При проверке MAC для нескольких блоков данных этот IV должен подаваться как входной в команде проверки MAC для следующего блока.<br>В случае ключа 3DES размер поля 16 H.<br>Для ключа AES размер поля 32 H. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [MY] — Проверка и трансляция MAC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка MAC для сообщения с использованием TAK, ZAK или BDK и, в случае успеха, генерация MAC для этого сообщения с использованием другого TAK или ZAK.
Команда поддерживает различные алгоритмы вычисления MAC и режимы дополнения (подробнее см. описание команды).

**Примечания:** Данные, для которых проверяется и транслируется значение MAC, могут быть переданы в HSM в различных форматах в соответствии со значением, указанным в поле *Флаг формата входных данных*.

При использовании Key Block значение поля Использование ключа определяет доступные алгоритмы вычисления MAC и режимы дополнения:

| Использование ключа | Алгоритм | Допустимые алгоритмы MAC |
|---|---|---|
| 'M1' | 'T' | ISO 9797 MAC алгоритм 1 |
| 'M3' | 'T' | ISO 9797 MAC алгоритм 3 |
| 'M5' | 'A' | CBC MAC |
| 'M6' | 'A' | CMAC |
| 'B0', '41', '43' | 'T' | • ISO 9797 MAC алгоритм 1<br>• ISO 9797 MAC алгоритм 3 |
| 'B0', '41', '43' | 'A' | • CBC MAC<br>• CMAC |

Для ISO 9797 MAC алгоритмы 1 и 3 и AES CBC MAC допускается использовать следующие режимы дополнения:

- Без дополнения
- ISO 9797 режим дополнения 1
- ISO 9797 режим дополнения 2
- ISO 9797 режим дополнения 3

Для AES CMAC допускается использовать только режим дополнения AES CMAC.

В качестве *Исходного ключа MAC* для проверки значения MAC может использоваться BDK (Использование ключа = 'B0', '41', '43').

При использовании 3DES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-1:2009:

• При использовании BDK-1 данные, для которых проверяется MAC, могут быть данными "запроса" или "ответа" (в обоих случаях диверсифицированный ключ будет одинаковым).
• При использовании BDK-2 данные, для которых проверяется MAC, считаются данными "запроса".
• При использовании BDK-4 данные, для которых проверяется MAC, считаются данными "ответа".

При использовании AES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-3:2017:

• При использовании BDK-1 у диверсифицированного ключа индикатор использования ключа имеет значение "Аутентификация сообщений, двунаправленная".
• При использовании BDK-2 или BDK-4 у диверсифицированного ключа индикатор использования ключа имеет значение "Аутентификация сообщений, проверка".

Максимальное значение поля *Длина сообщения* зависит от формата входных данных, при этом максимальная длина всей команды ограничена 32 КБ.

В случае проверки или генерации MAC для сообщения, состоящего из нескольких блоков, промежуточные значения IV будут зашифрованы с использованием ключа, выработанного из ключа MAC.

При генерации или проверке MAC для нескольких блоков сообщения (*Флаг режима* = '1', '2' или '3') ограничена минимальная длина каждого блока сообщения:

• в случае ключа 3DES: минимальная длина блока сообщения 24 байта (бинарные данные) или 48 шестнадцатеричных символов;
• в случае ключа AES: минимальная длина блока сообщения 48 байтов (бинарные данные) или 96 шестнадцатеричных символов.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'MY'.</td></tr>
<tr><td>Флаг режима</td><td>1 N</td><td>'0': Единственный блок сообщения<br>'1': Первый блок сообщения из нескольких блоков<br>'2': Промежуточный блок сообщения из нескольких блоков<br>'3': Последний блок сообщения из нескольких блоков</td></tr>
<tr><td>Флаг формата входных данных</td><td>1 N</td><td>'0': Бинарные данные<br>'1': Бинарные данные в шестнадцатеричном формате<br>'2': Текстовые данные</td></tr>
<tr><td>Исходный размер MAC</td><td>1 N</td><td>'0': 8 шестнадцатеричных символов<br>'1': 16 шестнадцатеричных символов</td></tr>
<tr><td>Исходный алгоритм MAC</td><td>1 N</td><td>'1': ISO 9797 MAC алгоритм 1 (только DES)<br>'3': ISO 9797 MAC алгоритм 3 (= ANSI X9.19 если используется с ключом 2DES) (только DES)<br>'5': CBC-MAC (только AES)<br>'6': CMAC (только AES)</td></tr>
<tr><td>Исходный режим дополнения</td><td>1 N</td><td>В случае Исходного алгоритма MAC = '1', '3' или '5':<br>'0': Без дополнения (общая длина сообщения должна быть кратна 8 байтам для Исходного алгоритма MAC = '1' или '3', 16 байтам для Исходного алгоритма MAC = '5')<br>'1': ISO 9797 режим дополнения 1 (дополнить 0x00)<br>'2': ISO 9797 режим дополнения 2 (добавить 0x80 и дополнить 0x00)<br>'3': ISO 9797 режим дополнения 3 (добавить перед сообщением значение длины, дополнить 0x00)<br>Примечание: если Исходный режим дополнения = '3', Флаг режима должен иметь значение '0'.<br>В случае Исходного алгоритма MAC = '6':<br>'4': дополнение AES CMAC</td></tr>
<tr><td>Тип исходного ключа</td><td>3 H</td><td>'003': TAK, зашифрованный под LMK 16-17<br>'008': ZAK, зашифрованный под LMK 26-27</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Исходный ключ MAC</td><td></td><td>Исходный ключ MAC, используемый совместно с Исходным IV (в соответствующих случаях) для проверки MAC.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>TAK или ZAK (в соответствии со значением Тип исходного ключа).</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'M1', 'M3'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr>
<tr><td>'M5', 'M6'</td><td>'A'</td><td>'C', 'V', 'N'</td></tr>
<tr><td>'B0', '41', '43'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Дескриптор исходного KSN</td><td>3 H</td><td>Присутствует, только если Исходный ключ MAC — BDK.<br>Дескриптор исходного KSN (в следующем поле).<br>Если Исходный ключ MAC AES BDK-1, BDK-2 или BDK-4, поле должно содержать значение '000'.</td></tr>
<tr><td>Исходный KSN</td><td>12-20 H<br>или<br>24 H</td><td>Присутствует, только если Исходный ключ MAC — BDK.<br>Серийный номер ключа, полученный от PIN-pad.<br>Если Исходный ключ MAC — 3DES BDK-1, BDK-2 или BDK-4, размер поля 12-20 H.<br>Если Исходный ключ MAC — AES BDK-1, BDK-2 или BDK-4, размер поля 24 H.</td></tr>
</table>

| | | |
|---|---|---|
| Целевой размер MAC | 1 N | '0': 8 шестнадцатеричных символов<br>'1': 16 шестнадцатеричных символов |
| Целевой алгоритм MAC | 1 N | '1': ISO 9797 MAC алгоритм 1 (только DES)<br>'3': ISO 9797 MAC алгоритм 3 (= ANSI X9.19 если используется с ключом 2DES) (только DES)<br>'5': CBC-MAC (только AES)<br>'6': CMAC (только AES) |
| Целевой режим дополнения | 1 N | В случае *Целевого алгоритма MAC* = '1', '3' или '5':<br>'0': Без дополнения (общая длина сообщения должна быть кратна 8 байтам для *Целевого алгоритма MAC* = '1' или '3', 16 байтам для *Целевого алгоритма MAC* = '5')<br>'1': ISO 9797 режим дополнения 1 (дополнить 0x00)<br>'2': ISO 9797 режим дополнения 2 (добавить 0x80 и дополнить 0x00)<br>'3': ISO 9797 режим дополнения 3 (добавить перед сообщением значение длины, дополнить 0x00)<br>*Примечание:* если *Целевой режим дополнения* = '3', *Флаг режима* должен иметь значение '0'.<br>В случае *Целевого алгоритма MAC* = '6':<br>'4': дополнение AES CMAC |
| Тип целевого ключа | 3 H | '003': TAK, зашифрованный под LMK 16-17<br>'008': ZAK, зашифрованный под LMK 26-27 |
| | | Значение 'FFF'. |
| Целевой ключ MAC | | Целевой ключ MAC, используемый совместно с *Целевым IV* (в соответствующих случаях) для генерации нового MAC. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | TAK или ZAK (в соответствии со значением *Тип целевого ключа*). |
| | 'S' + n A | Ключ должен соответствовать следующему формату:<br>Использование ключа: 'M1', 'M3' / 'M5', 'M6'<br>Алгоритм: 'T' / 'A'<br>Режим использования: 'C', 'G', 'N' |
| Исходный IV | 16 H<br>или<br>32 H | Присутствует только в случае *Флага режима* = '2' или '3'.<br>Промежуточный вектор инициализации, используемый при проверке MAC.<br>При проверке MAC для промежуточного или последнего блока сообщения используется значение IV, возвращаемое в ответе при проверке MAC для предыдущего блока.<br>В случае *Исходного ключа MAC* 3DES размер поля 16 H.<br>Для *Исходного ключа MAC* AES размер поля 32 H. |
| Целевой IV | 16 H<br>или<br>32 H | Присутствует только в случае *Флага режима* = '2' или '3'.<br>Промежуточный вектор инициализации, используемый при генерации MAC.<br>При генерации MAC для промежуточного или последнего блока сообщения используется значение IV, возвращаемое в ответе при генерации MAC для предыдущего блока.<br>В случае *Целевого ключа MAC* 3DES размер поля 16 H.<br>Для *Целевого ключа MAC* AES размер поля 32 H. |
| Длина сообщения | 4 H | Длина (в байтах) следующего поля. Максимальное значение: 0x7D00 (32000) байт. |
| Сообщение | | Сообщение, для которого проверяется значение *Исходный MAC* и генерируется *Целевой MAC*. |
| | n B | В случае *Флага формата входных данных* = '0' (бинарные данные):<br>Если *Флаг режима* = '1' или '2':<br>n должно быть кратно 8 при использовании ключа DES<br>n должно быть кратно 16 при использовании ключа AES |

| | | |
|---|---|---|
| | или<br>n H | В случае *Флага формата входных данных* = '1' (бинарные данные в шестнадцатеричном формате):<br>Если *Флаг режима* = '1' или '2':<br>n должно быть кратно 16 при использовании ключа DES<br>n должно быть кратно 32 при использовании ключа AES |
| | или<br>n A | В случае *Флага формата входных данных* = '2' (текстовые данные):<br>Если *Флаг режима* = '1' или '2':<br>n должно быть кратно 8 при использовании ключа DES<br>n должно быть кратно 16 при использовании ключа AES |
| Исходный MAC | 8 H<br>или<br>16 H | Присутствует только в случае *Флага режима* = '0' или '3'.<br>Значение MAC, проверяемое с использованием *Исходного ключа MAC*.<br>Длина поля определяется значением поля *Исходный размер MAC*. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'MZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'02': Недопустимый флаг режима<br>'03': Недопустимый флаг формата входных данных<br>'04': Недопустимый исходный размер MAC или исходный алгоритм MAC<br>'05': Недопустимый тип исходного ключа<br>'06': Недопустимая длина сообщения<br>'07': Недопустимый целевой размер MAC или целевой алгоритм MAC<br>'08': Недопустимый тип целевого ключа<br>'09': Недопустимый исходный режим дополнения<br>'10': Нарушена четность исходного ключа MAC<br>'11': Нарушена четность целевого ключа MAC<br>'34': Недопустимый целевой режим дополнения<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Исходный IV | 16 H<br>или<br>32 H | Присутствует только в случае *Флага режима* = '1' или '2'.<br>Промежуточный вектор инициализации, используемый при проверке MAC.<br>При проверке MAC для нескольких блоков данных этот IV должен подаваться как входной в команде для следующего блока.<br>В случае *Исходного ключа MAC* 3DES размер поля 16 H.<br>Для *Исходного ключа MAC* AES размер поля 32 H. |
| Целевой IV | 16 H<br>или<br>32 H | Присутствует только в случае *Флага режима* = '1' или '2'.<br>Промежуточный вектор инициализации, используемый при генерации MAC.<br>При генерации MAC для нескольких блоков данных этот IV должен подаваться как входной в команде для следующего блока.<br>В случае *Целевого ключа MAC* 3DES размер поля 16 H.<br>Для *Целевого ключа MAC* AES размер поля 32 H. |
| Целевой MAC | 8 H<br>или<br>16 H | Присутствует только в случае *Флага режима* = '0' или '3'.<br>Значение MAC, вычисленное с использованием *Целевого ключа MAC*.<br>Длина поля определяется значением поля *Целевой размер MAC*. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |

| | | |
|---|---|---|
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [EW] — Генерация подписи RSA/ECC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация подписи сообщения с использованием закрытого ключа алгоритмов RSA/ECDSA.

**Примечания:** Подробнее о поддержке алгоритмов RSA и ECC см. в «КриптоПро HSM. Руководство программиста».

| Идентификатор алгоритма хэширования | Алгоритм хэширования | Минимальная длина закрытого ключа RSA (EMSA-PKCS1-v1_5) | Минимальная длина закрытого ключа RSA (EMSA-PSS) | Кривая ECC |
|---|---|---|---|---|
| '01' | SHA-1 | 368 бит | 336 бит | н/д |
| '02' | MD5 | 360 бит | н/д | н/д |
| '03' | ISO 10118-2 | 320 бит | н/д | н/д |
| '04' | Без хэширования | 320 бит | н/д | н/д |
| '05' | SHA-224 | 464 бит | 464 бит | н/д |
| '06' | SHA-256 | 496 бит | 528 бит | P-256 |
| '07' | SHA-384 | 624 бит | 784 бит | P-384 |
| '08' | SHA-512 | 752 бит | 1040 бит | P-521 |

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce minimum key strength of 2048-bits for RSA` | `Yes [Y]` | Длины закрытого ключа (RSA) должна быть не менее 2048 бит. |
| (влияет на параметры: *Закрытый ключ*) | `No [N]` | Ограничения на длину ключа не накладываются. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'EW'.</td></tr>
<tr><td>Идентификатор алгоритма хэширования</td><td>2 N</td><td>Алгоритм хэширования сообщения:<br>'01': SHA-1<br>'02': MD5<br>'03': ISO 10118-2<br>'04': Без хэширования<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512</td></tr>
<tr><td>Идентификатор алгоритма подписи</td><td>2 N</td><td>Алгоритм подписи сообщения:<br>'01': RSA<br>'02': ECDSA</td></tr>
<tr><td>Идентификатор режима дополнения</td><td>2 N</td><td>Присутствует только в случае Идентификатора алгоритма подписи = '01'.<br>'01': PKCS#1 v2.2 method EMSA-PKCS1-v1_5<br>'04': PKCS#1 v2.2 method EMSA-PSS</td></tr>
<tr><td>Формат подписи</td><td>1 N</td><td>Присутствует только в случае Идентификатора алгоритма подписи = '02'.<br>'0': Простой формат (конкатенация r, s)<br>'1': ANSI X9.62 ASN.1 (SEQUENCE {r INTEGER, s INTEGER})</td></tr>
<tr><td>Длина сообщения</td><td>4 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td>Сообщение</td><td>n B</td><td>Подписываемое сообщение.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Признак конца поля Сообщение.</td></tr>
<tr><td>Флаг закрытого ключа</td><td>2 N</td><td>Указывает расположение закрытого ключа, используемого для генерации подписи.<br>'00' .. '20' : индекс ключа в хранилище<br>'99' : используется ключ, переданный в команде</td></tr>
<tr><td>Длина закрытого ключа</td><td></td><td>Опционально; присутствует только в случае Флага закрытого ключа = '99'.</td></tr>
<tr><td></td><td>4 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
<tr><td>Закрытый ключ</td><td></td><td>Опционально; присутствует только в случае Флага закрытого ключа = '99'.<br>Закрытый ключ, используемый для генерации подписи.</td></tr>
<tr><td></td><td>n B</td><td>Закрытый ключ, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B<br>или<br>'S' + n A</td><td>Закрытый ключ должен соответствовать следующему формату:<br>Если Идентификатор алгоритма подписи = '01' (RSA):
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03', '06'</td><td>'R'</td><td>'S', 'N'</td></tr>
</table>
Если Идентификатор алгоритма подписи = '02' (ECDSA):
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03'</td><td>'E'</td><td>'S', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'EX'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Недопустимый тип закрытого ключа<br>'04': Недопустимый флаг закрытого ключа<br>'05': Недопустимый идентификатор алгоритма хэширования<br>'06': Недопустимый идентификатор алгоритма подписи<br>'07': Недопустимый идентификатор режима дополнения<br>'47': Алгоритм не лицензирован<br>'68': Команда недоступна<br>'74': Недопустимый синтаксис digest info (только в режиме Без хэширования)<br>'78': Ошибка длины закрытого ключа<br>'80': Ошибка длины сообщения<br>'DB': Закрытый ключ больше порядка кривой<br>'DC': Недопустимое значение формата подписи<br>или другой стандартный код ошибки. |
| Длина подписи | 4 N | Длина (в байтах) следующего поля. |
| Подпись | n B | Вычисленное значение подписи. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [EY] — Проверка подписи RSA/ECC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка подписи сообщения с использованием открытого ключа алгоритмов RSA/ECDSA.

**Примечания:** Подробнее о поддержке алгоритмов RSA и ECC см. в «КриптоПро HSM. Руководство программиста».

| Идентификатор алгоритма хэширования | Алгоритм хэширования | Минимальная длина закрытого ключа RSA (EMSA-PKCS1-v1_5) | Минимальная длина закрытого ключа RSA (EMSA-PSS) | Кривая ECC |
|---|---|---|---|---|
| '01' | SHA-1 | 368 бит | 336 бит | н/д |
| '02' | MD5 | 360 бит | н/д | н/д |
| '03' | ISO 10118-2 | 320 бит | н/д | н/д |
| '04' | Без хэширования | 320 бит | н/д | н/д |
| '05' | SHA-224 | 464 бит | 464 бит | н/д |
| '06' | SHA-256 | 496 бит | 528 бит | P-256 |
| '07' | SHA-384 | 624 бит | 784 бит | P-384 |
| '08' | SHA-512 | 752 бит | 1040 бит | P-521 |

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce minimum key strength of 1024-bits for RSA signature verification` (влияет на параметры: *Открытый ключ*) | `Yes [Y]` | Длина открытого ключа RSA должна быть не менее 1024 бит. |
| | `No [N]` | Ограничения на длину ключа не накладываются. |
| `Enforce minimum key strength of 2048-bits for RSA` (влияет на параметры: *Закрытый ключ*) | `Yes [Y]` | Длины закрытого ключа (RSA) должна быть не менее 2048 бит. |
| | `No [N]` | Ограничения на длину ключа не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'EY'. |
| Идентификатор алгоритма хэширования | 2 N | Алгоритм хэширования сообщения:<br>'01': SHA-1<br>'02': MD5<br>'03': ISO 10118-2<br>'04': Без хэширования<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| Идентификатор алгоритма подписи | 2 N | Алгоритм проверки подписи сообщения:<br>'01': RSA<br>'02': ECDSA |
| Идентификатор режима дополнения | 2 N | Присутствует только в случае *Идентификатора алгоритма подписи* = '01'.<br>'01': PKCS#1 v2.2 method EMSA-PKCS1-v1_5<br>'04': PKCS#1 v2.2 method EMSA-PSS |
| Формат подписи | 1 N | Присутствует только в случае *Идентификатора алгоритма подписи* = '02'.<br>'0': Простой формат (конкатенация r, s)<br>'1': ANSI X9.62 ASN.1 (SEQUENCE {r INTEGER, s INTEGER}) |
| Длина подписи | 4 N | Длина (в байтах) следующего поля. |
| Подпись | n B | Значение подписи для проверки. |
| Разделитель | 1 A | Значение ';'. Признак конца поля *Подпись*. |
| Длина сообщения | 4 N | Длина (в байтах) следующего поля. |
| Сообщение | n B | Проверяемое сообщение. |
| Разделитель | 1 A | Значение ';'. Признак конца поля *Сообщение*. |
| Следующие 4 поля присутствуют только в случае Variant LMK: | | |
| MAC | 4 B | MAC, вычисленный для открытого ключа и данных аутентификации с использованием LMK 36-37. |
| Открытый ключ | n B | Открытый ключ, используемый для проверки подписи. DER в формате ASN.1 (последовательность модуля и экспоненты). |
| Данные для аутентификации | n B | Опционально. Дополнительные данные для вычисления MAC (не должны содержать символы ';' и '~'). |
| Разделитель | 1 A | Значение '~'. Опционально; должен присутствовать, если присутствует *Разделитель* '%' ниже. |
| Следующее поле присутствуют только в случае Key Block LMK: | | |
| Открытый ключ | 'S' + n B<br>или<br>'S' + n A | Открытый ключ для проверки подписи, должен соответствовать следующему формату:<br>Использование ключа: '02'<br>Алгоритм: 'R', 'E'<br>Режим использования: 'V', 'N' |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'EZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'02': Ошибка проверки подписи<br>'04': Открытый ключ не соответствует правилам кодирования<br>'05': Недопустимый идентификатор алгоритма хэширования<br>'06': Недопустимый идентификатор алгоритма подписи<br>'07': Недопустимый идентификатор режима дополнения<br>'47': Алгоритм не лицензирован<br>'68': Команда недоступна<br>'74': Недопустимый синтаксис digest info (только в режиме Без хэширования)<br>'76': Длина подписи не равна длине модуля открытого ключа<br>'77': Ошибка расшифрованных данных<br>'79': Ошибка идентификатора объекта алгоритма хэширования<br>'80': Ошибка длины сообщения<br>'DB': Параметры подписи (r, s) больше порядка кривой<br>'DC': Недопустимое значение формата подписи<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [GM] — Вычисление значения хэш-функции для блока данных

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Вычисление значения хэш-функции для блока данных.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'GM'. |
| Идентификатор алгоритма хэширования | 2 N | '01': SHA-1<br>'02': MD5<br>'03': ISO 10118-2<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| Длина данных | 5 N | Длина данных, для которых вычисляется значение хэш-функции. |
| Данные | n B | Данные, для которых вычисляется значение хэш-функции. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'GN'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'05': Недопустимый идентификатор алгоритма хэширования<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Значение хэш-функции | n B | Вычисленное значение хэш-функции (длина поля зависит от используемого алгоритма хэширования). |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 17 Команды шифрования сообщений

Следующие команды хоста используются для операций шифрования данных:



Указанные команды обеспечивают функции шифрования и расшифрования и предназначены для защиты передаваемых (например, данных транзакций) и хранящихся данных.

Команды поддерживают 4 типа ключей:

• TEK, терминальный ключ шифрования — используется терминалом и хост-системой (например, банкоматом/PIN-pad и эквайером) для защиты передаваемых данных
• ZEK, зональный ключ шифрования — используется двумя разными зонами (например, эквайером и коммутатором) для защиты передаваемых данных
• DEK, ключ шифрования данных — существует только в пределах одной зоны (например, эквайера), используется для защиты хранящихся данных
• BDK, базовый ключ диверсификации — используются в терминалах, поддерживающих DUKPT, для шифрования "запросных" (от терминала к хосту) или "ответных" (от хоста к терминалу) сообщений; терминал и HSM вырабатывают ключ транзакции из BDK в соответствии с DUKPT

В X9.24-3:2017 определены 2 метода выработки ключей шифрования данных:

• Двунаправленный метод — для шифрования данных, передаваемых от терминала к хосту и от хоста к терминалу, используется один ключ. Данный метод поддерживают BDK-1 и BDK-3.
• Однонаправленный метод — для шифрования данных, передаваемых от терминала к хосту и от хоста к терминалу, используются два разных ключа. Данный метод поддерживают BDK-2 и BDK-4.

Описание схемы DUKPT и её применения в HSM см. в разделе «Схема управления ключами транзакций» документа «КриптоПро HSM. Руководство программиста».

## Типы BDK, используемые в командах шифрования сообщения

### 3DES BDK

В таблице ниже приведены различные значения вариантов, применяемых к ключу транзакции в процессе выработки рабочих ключей шифрования данных из ключа 3DES BDK.

<table>
<tr><th colspan="2">Тип 3DES BDK</th><th>Описание</th></tr>
<tr><td rowspan="2">BDK-1</td><td>BDK, зашифрованный под LMK 28-29.</td><td rowspan="2">Значения вариантов для диверсифицированного ключа транзакций:<table><tr><th>Ключевая функция</th><th>Вариант</th></tr><tr><td>Зашифрование/расшифрование данных "запроса"</td><td>00 00 00 00 00 FF 00 00</td></tr><tr><td>Зашифрование/расшифрование данных "ответа"</td><td>00 00 00 00 00 FF 00 00</td></tr></table>Созданные таким методом ключи шифрования являются двунаправленными.</td></tr>
<tr><td>BDK со значением Использование ключа = 'B0'.</td></tr>
<tr><td rowspan="2">BDK-2</td><td>BDK, зашифрованный под LMK 28-29/6.</td><td rowspan="2">Значения вариантов для диверсифицированного ключа транзакций:<table><tr><th>Ключевая функция</th><th>Вариант</th></tr><tr><td>Расшифрование данных "запроса"</td><td>00 00 00 00 00 FF 00 00</td></tr><tr><td>Зашифрование данных "ответа"</td><td>00 00 00 FF 00 00 00 00</td></tr></table>Созданные таким методом ключи шифрования являются однонаправленными.</td></tr>
<tr><td>BDK со значением Использование ключа = '41'.</td></tr>
<tr><td rowspan="2">BDK-3</td><td>BDK, зашифрованный под LMK 28-29/8.</td><td rowspan="2">Значения вариантов для диверсифицированного ключа транзакций:<table><tr><th>Ключевая функция</th><th>Вариант</th></tr><tr><td>Зашифрование/расшифрование данных "запроса"</td><td>00 00 00 00 00 00 00 FF</td></tr><tr><td>Зашифрование/расшифрование данных "ответа"</td><td>00 00 00 00 00 00 00 FF</td></tr></table>Созданные таким методом ключи шифрования являются двунаправленными.</td></tr>
<tr><td>BDK со значением Использование ключа = '42'.</td></tr>
<tr><td rowspan="2">BDK-4</td><td>BDK, зашифрованный под LMK 28-29/9.</td><td rowspan="2">Значения вариантов для диверсифицированного ключа транзакций:<table><tr><th>Ключевая функция</th><th>Вариант</th></tr><tr><td>Зашифрование данных "запроса"</td><td>00 00 00 00 00 FF 00 00</td></tr><tr><td>Расшифрование данных "ответа"</td><td>00 00 00 FF 00 00 00 00</td></tr></table>Созданные таким методом ключи шифрования являются однонаправленными.</td></tr>
<tr><td>BDK со значением Использование ключа = '43'.</td></tr>
</table>

**AES BDK**

В таблице ниже приведены различные значения *Индикатора использования ключа*, используемые при выработке рабочих ключей шифрования данных из ключа AES BDK.

<table>
<tr><th colspan="2">Тип AES BDK</th><th>Описание</th></tr>
<tr><td>BDK-1</td><td>BDK со значением Использование ключа = 'B0'.</td><td>Значения Индикатора использования ключа, используемые при диверсификации ключа шифрования:
<table>
<tr><th>Ключевая функция</th><th>Индикатор использования ключа</th></tr>
<tr><td>Зашифрование/расшифрование данных "запроса"</td><td>0x3002</td></tr>
<tr><td>Зашифрование/расшифрование данных "ответа"</td><td>0x3002</td></tr>
</table>
Созданные таким методом ключи шифрования являются двунаправленными.</td></tr>
<tr><td>BDK-2</td><td>BDK со значением Использование ключа = '41'.</td><td>Значения Индикатора использования ключа, используемые при диверсификации ключа шифрования:
<table>
<tr><th>Ключевая функция</th><th>Индикатор использования ключа</th></tr>
<tr><td>Расшифрование данных "запроса"</td><td>0x3000</td></tr>
<tr><td>Зашифрование данных "ответа"</td><td>0x3001</td></tr>
</table>
Созданные таким методом ключи шифрования являются однонаправленными.</td></tr>
<tr><td>BDK-4</td><td>BDK со значением Использование ключа = '43'.</td><td>Значения Индикатора использования ключа, используемые при диверсификации ключа шифрования:
<table>
<tr><th>Ключевая функция</th><th>Индикатор использования ключа</th></tr>
<tr><td>Зашифрование данных "запроса"</td><td>0x3000</td></tr>
<tr><td>Расшифрование данных "ответа"</td><td>0x3001</td></tr>
</table>
Созданные таким методом ключи шифрования являются однонаправленными.</td></tr>
</table>

## [M0] — Зашифрование блока данных

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции** Зашифрование блока данных.

**Примечания**

В качестве ключа зашифрования может использоваться BDK. Команда поддерживает ключи BDK-1, BDK-2, BDK-3 и BDK-4.
При использовании 3DES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-1:2009:

- При использовании BDK-1 или BDK-3 данные для зашифрования могут быть данными "запроса" или "ответа" (в обоих случаях диверсифицированный ключ зашифрования будет одинаковым).
- При использовании BDK-2 данные для зашифрования считаются данными "ответа".
- При использовании BDK-4 данные для зашифрования считаются данными "запроса".

Дополнительную информацию об использовании 3DES BDK с командами шифрования сообщений см. в таблице на странице 271.

При использовании AES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-3:2017:

- При использовании BDK-1 у диверсифицированного ключа зашифрования индикатор использования ключа имеет значение "Шифрование данных, двунаправленное".
- При использовании BDK-2 или BDK-4 у диверсифицированного ключа зашифрования индикатор использования ключа имеет значение "Шифрование данных, зашифрование".

Дополнительную информацию об использовании AES BDK с командами шифрования сообщений см. в таблице на странице 272.

Если в качестве ключа зашифрования используется ZEK или TEK, содержимое открытого сообщения должно соответствовать ограничениям, накладываемым настройкой безопасности `ZEK/TEK encryption`.
При использовании DEK или BDK ограничения на содержимое сообщения не накладываются.

Данные для зашифрования могут быть переданы в HSM в различных форматах в соответствии со значением, указанным в поле *Флаг формата входных данных*.

К входному сообщению не применяется процедура дополнения. Для всех режимов, кроме CTR, длина входного сообщения должна быть кратна размеру блока (для бинарных сообщений) или кратна удвоенному размеру блока (для сообщений в шестнадцатеричном формате). При использовании ключа 3DES размер блока равен 8. При использовании ключа AES размер блока равен 16.

Дополнительную информацию о DUKPT см. в разделе «Схема управления ключами транзакций» документа «КриптоПро HSM. Руководство программиста».

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable ZEK/TEK encryption of ASCII data or Binary data or None` (влияет на параметры: *Данные сообщения*) | `ASCII [A]` | При использовании для зашифрования ZEK или TEK незашифрованное сообщение должно содержать только ASCII-символы (0x20-0x7F). |
| | `Binary [B]` | Ограничения на формат незашифрованного сообщения не накладываются. |
| | `None [N]` | Зашифрование с использованием ZEK или TEK не допускается. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'M0' (M-ноль).</td></tr>
<tr><td>Флаг режима</td><td>2 N</td><td>Режим шифрования:<br>'00': ECB<br>'01': CBC (требуется IV)<br>'02': CFB8 (требуется IV)<br>'03': CFB64 (требуется IV)<br>'05': OFB (требуется IV)<br>'06': CTR (требуется IV)</td></tr>
<tr><td>Флаг формата входных данных</td><td>1 N</td><td>'0': Бинарные данные<br>'1': Бинарные данные в шестнадцатеричном формате<br>'2': Текстовые данные</td></tr>
<tr><td>Флаг формата выходных данных</td><td>1 N</td><td>'0': Бинарные данные<br>'1': Бинарные данные в шестнадцатеричном формате</td></tr>
<tr><td>Тип ключа</td><td>3 H</td><td>'009': BDK-1 (зашифрованный под LMK 28-29)<br>'609': BDK-2 (зашифрованный под LMK 28-29/6)<br>'809': BDK-3 (зашифрованный под LMK 28-29/8)<br>'909': BDK-4 (зашифрованный под LMK 28-29/9)<br>Примечание: в случае использования указанных выше типов ключей команда также должна включать опциональные поля Дескриптор KSN и KSN.<br>'00A': ZEK (зашифрованный под LMK 30-31)<br>'00B': DEK (зашифрованный под LMK 32-33)<br>'30B': TEK (зашифрованный под LMK 32-33/3)</td></tr>
<tr><td rowspan="4">Ключ</td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td></td><td>Ключ, используемый совместно с IV (в соответствующих режимах) для зашифрования входного сообщения.<br>Примечание: В случае Флага режима = '06' содержит CTRDEK (Использование ключа = '25').</td></tr>
<tr><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>BDK, ZEK, DEK или TEK, в соответствии со значением поля Тип ключа.</td></tr>
<tr><td>'S' + n A</td><td>Ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'B0', '41', '43'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
<tr><td>'42'</td><td>'T'</td><td>'X', 'N'</td></tr>
<tr><td>'D0', '21', '22', '23'</td><td>'T', 'A'</td><td>'B', 'E', 'N'</td></tr>
<tr><td>'25'</td><td>'A'</td><td>'B', 'E', 'N'</td></tr>
</table></td></tr>
<tr><td>Дескриптор KSN</td><td>3 H</td><td>Присутствует только в случае Типа ключа BDK.<br>Дескриптор серийного номера ключа (в следующем поле).<br>В случае AES BDK-1, BDK-2 или BDK-4 — значение '000'.</td></tr>
<tr><td>KSN</td><td>12 - 20 H<br>или<br>24 H</td><td>Присутствует только в случае Типа ключа BDK.<br>Серийный номер ключа, полученный от PIN-pad, включая счетчик транзакций.<br>В случае 3DES BDK-1, BDK-2, BDK-3 или BDK-4 размер поля 12-20 H.<br>Для AES BDK-1, BDK-2 или BDK-4 размер поля 24 H.</td></tr>
</table>

| | | |
|---|---|---|
| IV | 16 H<br>или<br>32 H | Присутствует только в случае *Флага режима* = '01', '02', '03', '05' или '06'.<br>Входной вектор инициализации, используемый совместно с ключом зашифрования. При зашифровании первого блока значение начального IV должно быть установлено вызывающей стороной; зачастую начальный IV имеет значение {00 00 00 00 00 00 00 00}.<br>В случае *Флага режима* ≠ '06' (CTR), для каждого следующего блока используется значение IV, возвращаемое в ответе при зашифровании предыдущего блока.<br>В случае ключа 3DES размер поля 16 H.<br>Для ключа AES размер поля 32 H. |
| Смещение счетчика | 3 N | Присутствует только в случае *Флага режима* = '06' (CTR).<br>Смещение в битах от наименьшего значащего бита IV до начала значения счетчика.<br>Допустимое значение: '000'. |
| Длина счетчика | 3 N | Присутствует только в случае *Флага режима* = '06' (CTR).<br>Длина счетчика в битах. Должна быть кратна 8 битам. Минимальное значение: 8 бит. |
| Флаг режима OFB | 1 N | Присутствует только в случае *Флага режима* = '05' (OFB).<br>'1': OFB8<br>'8': OFB64 |
| Длина сообщения | 4 H | Длина (в байтах) следующего поля. Максимальное значение: 0x7D00 (32000) байт. |
| Данные сообщения | | Данные для зашифрования. Длина и тип данных зависят от значения поля *Флаг формата входных данных*: |
| | n B | В случае *Флага формата входных данных* = '0' (бинарные данные):<br>Если *Флаг режима* ≠ '06' (CTR):<br>n должно быть кратно 8 при использовании ключа 3DES<br>n должно быть кратно 16 при использовании ключа AES |
| | или<br>n H | В случае *Флага формата входных данных* = '1' (бинарные данные в шестнадцатеричном формате):<br>Если *Флаг режима* ≠ '06' (CTR):<br>n должно быть кратно 16 при использовании ключа 3DES<br>n должно быть кратно 32 при использовании ключа AES |
| | или<br>n A | В случае *Флага формата входных данных* = '2' (текстовые данные):<br>Если *Флаг режима* ≠ '06' (CTR):<br>n должно быть кратно 8 при использовании ключа 3DES<br>n должно быть кратно 16 при использовании ключа AES |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'M1'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'02': Недопустимое значение флага режима<br>'03': Недопустимое значение флага формата входных данных<br>'04': Недопустимое значение флага формата выходных данных<br>'05': Недопустимый тип ключа<br>'06': Недопустимое значение длины сообщения<br>'10': Нарушена четность ключа зашифрования<br>'68': Команда недоступна<br>'D3': Недопустимое значение длины счетчика<br>'D4': Недопустимое значение смещения счетчика<br>или другой стандартный код ошибки. |
| IV | 16 H<br>или<br>32 H | Присутствует только в случае *Флага режима* = '01', '02', '03' или '05'.<br>Выходной IV. При зашифровании нескольких блоков данных этот IV должен подаваться как входной в команде зашифрования следующего блока.<br>В случае ключа 3DES размер поля 16 H.<br>Для ключа AES размер поля 32 H. |
| Длина сообщения | 4 H | Длина (в байтах) следующего поля. |
| Зашифрованное сообщение | | Зашифрованные данные. Длина и тип данных зависят от значения поля *Флаг формата выходных данных*: |
| | n B | В случае *Флага формата выходных данных* = '0' (бинарные данные):<br>Если *Флаг режима* ≠ '06' (CTR):<br>n должно быть кратно 8 при использовании ключа 3DES<br>n должно быть кратно 16 при использовании ключа AES |
| | или<br>n H | В случае *Флага формата выходных данных* = '1' (бинарные данные в шестнадцатеричном формате):<br>Если *Флаг режима* ≠ '06' (CTR):<br>n должно быть кратно 16 при использовании ключа 3DES<br>n должно быть кратно 32 при использовании ключа AES |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [M2] — Расшифрование блока данных

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции** Расшифрование блока данных.

**Примечания**

В качестве ключа расшифрования может использоваться BDK. Команда поддерживает ключи BDK-1, BDK-2, BDK-3 и BDK-4.
При использовании 3DES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-1:2009:

- При использовании BDK-1 или BDK-3 данные для расшифрования могут быть данными "запроса" или "ответа" (в обоих случаях диверсифицированный ключ расшифрования будет одинаковым).
- При использовании BDK-2 данные для расшифрования считаются данными "запроса".
- При использовании BDK-4 данные для расшифрования считаются данными "ответа".

Дополнительную информацию об использовании 3DES BDK с командами шифрования сообщений см. в таблице на странице 271.

При использовании AES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-3:2017:

- При использовании BDK-1 у диверсифицированного ключа расшифрования индикатор использования ключа имеет значение "Шифрование данных, двунаправленное".
- При использовании BDK-2 или BDK-4 у диверсифицированного ключа расшифрования индикатор использования ключа имеет значение "Шифрование данных, расшифрование".

Дополнительную информацию об использовании AES BDK с командами шифрования сообщений см. в таблице на странице 272.

Если в качестве ключа расшифрования используется ZEK или TEK, содержимое расшифрованного сообщения должно соответствовать ограничениям, накладываемым настройкой безопасности `ZEK/TEK encryption`.
При использовании DEK или BDK ограничения на содержимое сообщения не накладываются.

Данные для расшифрования могут быть переданы в HSM в различных форматах в соответствии со значением, указанным в поле *Флаг формата входных данных*.

К входному сообщению не применяется процедура дополнения. Для всех режимов, кроме CTR, длина входного сообщения должна быть кратна размеру блока (для бинарных сообщений) или кратна удвоенному размеру блока (для сообщений в шестнадцатеричном формате). При использовании ключа 3DES размер блока равен 8. При использовании ключа AES размер блока равен 16.

Дополнительную информацию о DUKPT см. в разделе «Схема управления ключами транзакций» документа «КриптоПро HSM. Руководство программиста».

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable ZEK/TEK encryption of ASCII data or Binary data or None` (влияет на параметры: *Зашифрованное сообщение*) | `ASCII [A]` | При использовании для расшифрования ZEK или TEK зашифрованное сообщение должно содержать только ASCII-символы (0x20-0x7F). |
| | `Binary [B]` | Ограничения на формат зашифрованного сообщения не накладываются. |
| | `None [N]` | Расшифрование с использованием ZEK или TEK не допускается. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'M2'.</td></tr>
<tr><td>Флаг режима</td><td>2 N</td><td>Режим расшифрования:<br>'00': ECB<br>'01': CBC (требуется IV)<br>'02': CFB8 (требуется IV)<br>'03': CFB64 (требуется IV)<br>'05': OFB (требуется IV)<br>'06': CTR (требуется IV)</td></tr>
<tr><td>Флаг формата входных данных</td><td>1 N</td><td>'0': Бинарные данные<br>'1': Бинарные данные в шестнадцатеричном формате</td></tr>
<tr><td>Флаг формата выходных данных</td><td>1 N</td><td>'0': Бинарные данные<br>'1': Бинарные данные в шестнадцатеричном формате<br>'2': Текстовые данные</td></tr>
<tr><td rowspan="3">Тип ключа</td><td rowspan="3">3 H</td><td>'009': BDK-1 (зашифрованный под LMK 28-29)<br>'609': BDK-2 (зашифрованный под LMK 28-29/6)<br>'809': BDK-3 (зашифрованный под LMK 28-29/8)<br>'909': BDK-4 (зашифрованный под LMK 28-29/9)<br>Примечание: в случае использования указанных выше типов ключей команда также должна включать опциональные поля Дескриптор KSN и KSN.</td></tr>
<tr><td>'00A': ZEK (зашифрованный под LMK 30-31)<br>'00B': DEK (зашифрованный под LMK 32-33)<br>'30B': TEK (зашифрованный под LMK 32-33/3)</td></tr>
<tr><td>Значение 'FFF'.</td></tr>
<tr><td rowspan="3">Ключ</td><td></td><td>Ключ, используемый совместно с IV (в соответствующих режимах) для расшифрования входного сообщения.<br>Примечание: В случае Флага режима = '06' содержит CTRDEK (Использование ключа = '25').</td></tr>
<tr><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>BDK, ZEK, DEK или TEK, в соответствии со значением поля Тип ключа.</td></tr>
<tr><td>'S' + n A</td><td>Ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'B0', '41', '43'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
<tr><td>'42'</td><td>'T'</td><td>'X', 'N'</td></tr>
<tr><td>'D0', '21', '22', '23'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr>
<tr><td>'25'</td><td>'A'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>Дескриптор KSN</td><td>3 H</td><td>Присутствует только в случае Типа ключа BDK.<br>Дескриптор серийного номера ключа (в следующем поле).<br>В случае AES BDK-1, BDK-2 или BDK-4 — значение '000'.</td></tr>
<tr><td>KSN</td><td>12 - 20 H<br>или<br>24 H</td><td>Присутствует только в случае Типа ключа BDK.<br>Серийный номер ключа, полученный от PIN-pad, включая счетчик транзакций.<br>В случае 3DES BDK-1, BDK-2, BDK-3 или BDK-4 размер поля 12-20 H.<br>Для AES BDK-1, BDK-2 или BDK-4 размер поля 24 H.</td></tr>
</table>

| | | |
|---|---|---|
| IV | 16 H<br>или<br>32 H | Присутствует только в случае *Флага режима* = '01', '02', '03', '05' или '06'.<br>Входной вектор инициализации, используемый совместно с ключом расшифрования. При расшифровании первого блока значение этого начального IV должно совпадать со значением начального IV, используемого для зашифрования первого блока открытого сообщения.<br>В случае *Флага режима* ≠ '06' (CTR), для каждого следующего блока используется значение IV, возвращаемое в ответе при расшифровании предыдущего блока.<br>В случае ключа 3DES размер поля 16 H.<br>Для ключа AES размер поля 32 H. |
| Смещение счетчика | 3 N | Присутствует только в случае *Флага режима* = '06' (CTR).<br>Смещение в битах от наименьшего значащего бита IV до начала значения счетчика.<br>Допустимое значение: '000'. |
| Длина счетчика | 3 N | Присутствует только в случае *Флага режима* = '06' (CTR).<br>Длина счетчика в битах. Должна быть кратна 8 битам. Минимальное значение: 8 бит. |
| Флаг режима OFB | 1 N | Присутствует только в случае *Флага режима* = '05' (OFB).<br>'1': OFB8<br>'8': OFB64 |
| Длина сообщения | 4 H | Длина (в байтах) следующего поля. Максимальное значение: 0x7D00 (32000) байт. |
| Зашифрованное сообщение | | Зашифрованные данные для расшифрования. Длина и тип данных зависят от значения поля *Флаг формата входных данных*: |
| | n B | В случае *Флага формата входных данных* = '0' (бинарные данные):<br>Если *Флаг режима* ≠ '06' (CTR):<br>n должно быть кратно 8 при использовании ключа 3DES<br>n должно быть кратно 16 при использовании ключа AES |
| | или<br>n H | В случае *Флага формата входных данных* = '1' (бинарные данные в шестнадцатеричном формате):<br>Если *Флаг режима* ≠ '06' (CTR):<br>n должно быть кратно 16 при использовании ключа 3DES<br>n должно быть кратно 32 при использовании ключа AES |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'M3'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'02': Недопустимое значение флага режима<br>'03': Недопустимое значение флага формата входных данных<br>'04': Недопустимое значение флага формата выходных данных<br>'05': Недопустимый тип ключа<br>'06': Недопустимое значение длины сообщения<br>'10': Нарушена четность ключа расшифрования<br>'68': Команда недоступна<br>'D3': Недопустимое значение длины счетчика<br>'D4': Недопустимое значение смещения счетчика<br>или другой стандартный код ошибки. |
| IV | 16 H<br>или<br>32 H | Присутствует только в случае *Флага режима* = '01', '02', '03' или '05'.<br>Выходной IV. При расшифровании нескольких блоков данных этот IV должен подаваться как входной в команде расшифрования следующего блока.<br>В случае ключа 3DES размер поля 16 H.<br>Для ключа AES размер поля 32 H. |
| Длина сообщения | 4 H | Длина (в байтах) следующего поля. |
| Расшифрованное сообщение | | Расшифрованные данные. Длина и тип данных зависят от значения поля *Флаг формата выходных данных*: |
| | n B | В случае *Флага формата выходных данных* = '0' (бинарные данные):<br>Если *Флаг режима* ≠ '06' (CTR):<br>n должно быть кратно 8 при использовании ключа 3DES<br>n должно быть кратно 16 при использовании ключа AES |
| | или<br>n H | В случае *Флага формата выходных данных* = '1' (бинарные данные в шестнадцатеричном формате):<br>Если *Флаг режима* ≠ '06' (CTR):<br>n должно быть кратно 16 при использовании ключа 3DES<br>n должно быть кратно 32 при использовании ключа AES |
| | или<br>n A | В случае *Флага формата выходных данных* = '2' (текстовые данные):<br>Если *Флаг режима* ≠ '06' (CTR):<br>n должно быть кратно 8 при использовании ключа 3DES<br>n должно быть кратно 16 при использовании ключа AES |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [M4] — Трансляция блока данных

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции** Расшифрование блока данных, зашифрованного под одним ключом, и последующее зашифрование под другим ключом.

**Примечания** В качестве исходного ключа (расшифрования) и/или целевого ключа (зашифрования) может использоваться BDK.
Команда поддерживает ключи BDK-1, BDK-2, BDK-3 и BDK-4.

При использовании исходного ключа (расшифрования) 3DES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-1:2009:

- При использовании BDK-1 или BDK-3 данные для расшифрования могут быть данными "запроса" или "ответа" (в обоих случаях диверсифицированный ключ расшифрования будет одинаковым).
- При использовании BDK-2 данные для расшифрования считаются данными "запроса".
- При использовании BDK-4 данные для расшифрования считаются данными "ответа".

При использовании исходного ключа (расшифрования) AES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-3:2017:

- При использовании BDK-1 у диверсифицированного ключа расшифрования индикатор использования ключа имеет значение "Шифрование данных, двунаправленное".
- При использовании BDK-2 или BDK-4 у диверсифицированного ключа расшифрования индикатор использования ключа имеет значение "Шифрование данных, расшифрование".

При использовании целевого ключа (зашифрования) 3DES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-1:2009:

- При использовании BDK-1 или BDK-3 данные для зашифрования могут быть данными "запроса" или "ответа" (в обоих случаях диверсифицированный ключ зашифрования будет одинаковым).
- При использовании BDK-2 данные для зашифрования считаются данными "ответа".
- При использовании BDK-4 данные для зашифрования считаются данными "запроса".

При использовании целевого ключа (зашифрования) AES BDK для DUKPT-диверсификации ключа используется метод ANSI X9.24-3:2017:

- При использовании BDK-1 у диверсифицированного ключа зашифрования индикатор использования ключа имеет значение "Шифрование данных, двунаправленное".
- При использовании BDK-2 или BDK-4 у диверсифицированного ключа зашифрования индикатор использования ключа имеет значение "Шифрование данных, зашифрование".

Дополнительную информацию об использовании 3DES BDK с командами шифрования сообщений см. в таблице на странице 271.

Дополнительную информацию об использовании AES BDK с командами шифрования сообщений см. в таблице на странице 272.

Если в качестве исходного или целевого ключа используется ZEK или TEK, содержимое открытого сообщения должно соответствовать ограничениям, накладываемым настройкой безопасности `ZEK/TEK encryption`.

Транслируемые данные могут быть переданы в HSM в различных форматах в соответствии со значением, указанным в поле *Флаг формата входных данных*.
Выходные данные после трансляции могут быть возвращены хосту в различных форматах в соответствии со значением, указанным в поле *Флаг формата выходных данных*.

Дополнительную информацию о DUKPT см. в разделе «Схема управления ключами транзакций» документа «КриптоПро HSM. Руководство программиста».

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable ZEK/TEK encryption of ASCII data or Binary data or None` (влияет на параметры: *Зашифрованное сообщение*) | `ASCII [A]` | При использовании для расшифрования ZEK или TEK зашифрованное сообщение должно содержать только ASCII-символы (0x20-0x7F). |
| | `Binary [B]` | Ограничения на формат зашифрованного сообщения не накладываются. |
| | `None [N]` | Расшифрование с использованием ZEK или TEK не допускается. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'M4'. |
| Исходный флаг режима | 2 N | Режим расшифрования:<br>'00': ECB<br>'01': CBC (требуется IV)<br>'02': CFB8 (требуется IV)<br>'03': CFB64 (требуется IV) |
| Целевой флаг режима | 2 N | Режим зашифрования:<br>'00': ECB<br>'01': CBC (требуется IV)<br>'02': CFB8 (требуется IV)<br>'03': CFB64 (требуется IV) |
| Флаг формата входных данных | 1 N | '0': Бинарные данные<br>'1': Бинарные данные в шестнадцатеричном формате |
| Флаг формата выходных данных | 1 N | '0': Бинарные данные<br>'1': Бинарные данные в шестнадцатеричном формате |
| Тип исходного ключа | 3 H | Тип исходного ключа (расшифрования).<br>'009': BDK-1 (зашифрованный под LMK 28-29)<br>'609': BDK-2 (зашифрованный под LMK 28-29/6)<br>'809': BDK-3 (зашифрованный под LMK 28-29/8)<br>'909': BDK-4 (зашифрованный под LMK 28-29/9)<br>*Примечание:* в случае использования указанных выше типов ключей команда также должна включать опциональные поля *Дескриптор исходного KSN* и *Исходный KSN*.<br>'00A': ZEK (зашифрованный под LMK 30-31)<br>'00B': DEK (зашифрованный под LMK 32-33)<br>'30B': TEK (зашифрованный под LMK 32-33/3) |
| | | Значение 'FFF'. |
| Исходный ключ | | Ключ, используемый совместно с *Исходным IV* (в соответствующих режимах) для расшифрования входного сообщения. |
| | 'U' + 32 H<br>или<br>'T' + 48 H | BDK, ZEK, DEK или TEK, в соответствии со значением поля *Тип исходного ключа*. |
| | 'S' + n A | Ключ должен соответствовать следующему формату: |

| Использование ключа | Алгоритм | Режим использования |
|---|---|---|
| 'B0', '41', '43' | 'T', 'A' | 'X', 'N' |
| '42' | 'T' | 'X', 'N' |
| 'D0', '21', '22', '23' | 'T', 'A' | 'B', 'D', 'N' |

<table>
<tr><td>Дескриптор исходного KSN</td><td>3 H</td><td>Присутствует, только если Тип исходного ключа — BDK.<br>Дескриптор исходного KSN (в следующем поле).<br>В случае Исходного ключа AES BDK-1, BDK-2 или BDK-4 — значение '000'.</td></tr>
<tr><td>Исходный KSN</td><td>12 - 20 H<br>или<br>24 H</td><td>Присутствует, только если Тип исходного ключа — BDK.<br>Серийный номер исходного ключа, полученный от PIN-pad, включая счетчик транзакций.<br>В случае Исходного ключа 3DES BDK-1, BDK-2, BDK-3 или BDK-4 размер поля 12-20 H.<br>Для Исходного ключа AES BDK-1, BDK-2 или BDK-4 размер поля 24 H.</td></tr>
<tr><td>Тип целевого ключа</td><td>3 H</td><td>Тип целевого ключа (зашифрования).<br>'009': BDK-1 (зашифрованный под LMK 28-29)<br>'609': BDK-2 (зашифрованный под LMK 28-29/6)<br>'809': BDK-3 (зашифрованный под LMK 28-29/8)<br>'909': BDK-4 (зашифрованный под LMK 28-29/9)<br>Примечание: в случае использования указанных выше типов ключей команда также должна включать опциональные поля Дескриптор целевого KSN и Целевой KSN.<br>'00A': ZEK (зашифрованный под LMK 30-31)<br>'00B': DEK (зашифрованный под LMK 32-33)<br>'30B': TEK (зашифрованный под LMK 32-33/3)</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Целевой ключ</td><td></td><td>Ключ, используемый совместно с Целевым IV (в соответствующих режимах) для зашифрования расшифрованного сообщения.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>BDK, ZEK, DEK или TEK, в соответствии со значением поля Тип целевого ключа.</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'B0', '41', '43'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
<tr><td>'42'</td><td>'T'</td><td>'X', 'N'</td></tr>
<tr><td>'D0', '21', '22', '23'</td><td>'T', 'A'</td><td>'B', 'E', 'N'</td></tr>
</table></td></tr>
<tr><td>Дескриптор целевого KSN</td><td>3 H</td><td>Присутствует, только если Тип целевого ключа — BDK.<br>Дескриптор целевого KSN (в следующем поле).<br>В случае Целевого ключа AES BDK-1, BDK-2 или BDK-4 — значение '000'.</td></tr>
<tr><td>Целевой KSN</td><td>12 - 20 H<br>или<br>24 H</td><td>Присутствует, только если Тип целевого ключа — BDK.<br>Серийный номер целевого ключа, полученный от PIN-pad, включая счетчик транзакций.<br>В случае Целевого ключа 3DES BDK-1, BDK-2, BDK-3 или BDK-4 размер поля 12-20 H.<br>Для Целевого ключа AES BDK-1, BDK-2 или BDK-4 размер поля 24 H.</td></tr>
<tr><td>Исходный IV</td><td>16 H<br>или<br>32 H</td><td>Присутствует только в случае Исходного флага режима = '01', '02', '03'.<br>Входной вектор инициализации, используемый совместно с исходным ключом (расшифрования). При трансляции первого блока значение этого начального IV должно совпадать со значением начального IV, используемого для зашифрования первого блока исходного сообщения.<br>Для каждого следующего блока используется значение исходного IV, возвращаемое в ответе при трансляции предыдущего блока.<br>В случае Исходного ключа 3DES размер поля 16 H.<br>Для Исходного ключа AES размер поля 32 H.</td></tr>
</table>

| | | |
|---|---|---|
| Целевой IV | 16 H<br>или<br>32 H | Присутствует только в случае *Целевого флага режима* = '01', '02', '03'.<br>Входной вектор инициализации, используемый совместно с целевым ключом (зашифрования). При трансляции первого блока значение начального IV должно быть установлено вызывающей стороной; зачастую начальный IV имеет значение {00 00 00 00 00 00 00 00}.<br>Для каждого следующего блока используется значение целевого IV, возвращаемое в ответе при трансляции предыдущего блока.<br>В случае *Целевого ключа* 3DES размер поля 16 H.<br>Для *Целевого ключа* AES размер поля 32 H. |
| Длина сообщения | 4 H | Длина (в байтах) следующего поля. Максимальное значение: 0x7D00 (32000) байт. |
| Зашифрованное сообщение | | Транслируемое сообщение, которое расшифровывается с использованием *Исходного ключа*. Длина и тип данных зависят от значения поля *Флаг формата входных данных*: |
| | n B | В случае *Флага формата входных данных* = '0' (бинарные данные):<br>n должно быть кратно 8 при использовании ключа 3DES<br>n должно быть кратно 16 при использовании ключа AES |
| | или<br>n H | В случае *Флага формата входных данных* = '1' (бинарные данные в шестнадцатеричном формате):<br>n должно быть кратно 16 при использовании ключа 3DES<br>n должно быть кратно 32 при использовании ключа AES |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'M5'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'02': Недопустимое значение исходного флага режима<br>'03': Недопустимое значение флага формата входных данных<br>'04': Недопустимое значение флага формата выходных данных<br>'05': Недопустимый тип исходного ключа<br>'06': Недопустимое значение длины сообщения<br>'07': Недопустимое значение целевого флага режима<br>'08': Недопустимый тип целевого ключа<br>'10': Нарушена четность исходного ключа расшифрования<br>'11': Нарушена четность целевого ключа зашифрования<br>'35': Недопустимый формат сообщения<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Исходный IV | 16 H<br>или<br>32 H | Присутствует только в случае *Исходного флага режима* = '01', '02', '03'.<br>Выходной IV, вычисленный с использованием исходного ключа. При трансляции нескольких блоков данных этот IV должен подаваться как входной в команде трансляции следующего блока.<br>В случае *Исходного ключа* 3DES размер поля 16 H.<br>Для *Исходного ключа* AES размер поля 32 H. |

| | | |
|---|---|---|
| Целевой IV | 16 H<br>или<br>32 H | Присутствует только в случае *Целевого флага режима* = '01', '02', '03'.<br>Выходной IV, вычисленный с использованием целевого ключа. При трансляции нескольких блоков данных этот IV должен подаваться как входной в команде трансляции следующего блока.<br>В случае *Целевого ключа* 3DES размер поля 16 H.<br>Для *Целевого ключа* AES размер поля 32 H. |
| Длина сообщения | 4 H | Длина (в байтах) следующего поля. |
| Транслированное сообщение | | Сообщение, зашифрованное с использованием *Целевого ключа*. Длина и тип данных зависят от значения поля *Флаг формата выходных данных*: |
| | n B | В случае *Флага формата выходных данных* = '0' (бинарные данные):<br>n должно быть кратно 8 при использовании ключа 3DES<br>n должно быть кратно 16 при использовании ключа AES |
| | или<br>n H | В случае *Флага формата выходных данных* = '1' (бинарные данные в шестнадцатеричном формате):<br>n должно быть кратно 16 при использовании ключа 3DES<br>n должно быть кратно 32 при использовании ключа AES |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 18 Команды HMAC

HSM поддерживает следующие команды хоста для операций с HMAC:

## [L0] — Генерация закрытого ключа HMAC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация закрытого ключа HMAC.

**Примечания:** Функция генерирует закрытый ключ для вычисления кода аутентификации сообщений, использующего хэш-функции с ключом (HMAC). Максимальная длина ключа, сгенерированного с помощью этой команды, ограничена 4096 байтами. Ключ HMAC можно использовать только в качестве входных данных для функций HMAC и недопустимо использовать с другими функциями HSM.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'L0' (L-ноль). |
| Идентификатор алгоритма хэширования | 2 N | '01': SHA-1<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| | 2 H | Значение 'FF'. |
| Использование ключа HMAC | 2 N | '01': Генерация HMAC<br>'02': Проверка HMAC<br>'03': Генерация и проверка HMAC |
| | 2 H | Значение 'FF'. |
| Длина ключа HMAC | 4 N | Длина ключа HMAC в байтах. Должна быть $\geq$ L/2, где L — длина выхода хэш-функции в байтах (например, L = 20 в случае SHA-1). |
| Формат ключа HMAC | 2 N | Определяет формат хранимого ключа. |
| | | '00': HMAC Key |
| | | '04': HMAC Key Block |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующие поля присутствуют только в случае генерации Key Block: | | |
| Разделитель | 1 A | Значение '#'. Обязательное поле в случае генерации Key Block. Если присутствует, то следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block (байты 5-6). Допустимые значения:<br>'61': SHA-1<br>'62': SHA-224<br>'63': SHA-256<br>'64': SHA-384<br>'65': SHA-512 |
| Алгоритм | 2 A | Поле *Алгоритм*, первый символ включается в заголовок Key Block (байт 7). Допустимое значение:<br>'H0': HMAC |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block. Допустимые значения см. в таблице режимов использования ключа в «КриптоПро HSM. Руководство программиста». |

| | | |
|---|---|---|
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block. Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block. Допустимые значения см. в таблице экспортируемости ключа в «КриптоПро HSM. Руководство программиста». |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже. Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор опционального блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина опционального блока | 2 H | Количество символов в опциональном блоке (включая идентификатор и длину). Допустимые значения: 0x04 .. 0xFF. Если значение 0x04, следующее поле отсутствует. |
| Данные опционального блока | n A | Данные опционального блока. Отсутствует, если длина блока 0x04. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'L1'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Ошибка длины ключа<br>'05': Некорректный идентификатор алгоритма хэширования<br>'06': Некорректное значение использования ключа<br>'07': Некорректное значение формата ключа<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Длина ключа HMAC | 4 N | Длина в байтах следующего поля |
| | 4 H | Значение 'FFFF'. |
| Ключ HMAC | | Сгенерированный ключ HMAC. *Примечание:* ключ не имеет префикса с символом ключевой схемы. |
| | n B | Ключ HMAC, зашифрованный под LMK 34-35/1. |
| | n A | Ключ HMAC, зашифрованный под LMK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [LQ] — Генерация HMAC для блока данных

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация HMAC для блока данных.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Minimum HMAC length in bytes` (влияет на параметры: *HMAC*) | `[5-64]` | Минимальная длина HMAC, который может генерировать HSM. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **КОМАНДА** |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'LQ'. |
| Идентификатор алгоритма хэширования | 2 N | '01': SHA-1<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| | 2 H | Значение 'FF'. |
| Длина HMAC | 4 N | Длина выхода HMAC (t) в байтах. Должна удовлетворять (Минимальная длина HMAC $\leq$ t $\leq$ L), где L — длина выхода хэш-функции (например, L = 20 в случае SHA-1), Минимальная длина HMAC задается с помощью консольной команды CS (Configure Security). |
| Формат ключа HMAC | 2 N | Определяет формат хранимого ключа. |
| | | '00': HMAC Key |
| | | '04': HMAC Key Block |
| Длина ключа HMAC | 4 N | Длина в байтах следующего поля. |
| | 4 H | Значение 'FFFF'. |
| Ключ HMAC | | Ключ, используемый для вычисления HMAC. *Примечание:* ключ не имеет префикса с символом ключевой схемы. |
| | n B | Ключ HMAC, зашифрованный под LMK 34-35/1. |
| | n A | Ключ HMAC должен соответствовать следующему формату: |

| Использование ключа | Алгоритм | Режим использования |
|---|---|---|
| '61' – '65' | 'H' | 'C', 'G', 'N' |

| | | |
|---|---|---|
| Разделитель | 1 A | Значение ';'. Присутствует только в случае Variant LMK. |
| Длина данных | 5 N | Длина сообщения для аутентификации. |
| Данные сообщения | n B | Данные для аутентификации. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |

| | | |
|---|---|---|
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'LR'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Ошибка длины HMAC<br>'05': Некорректный идентификатор алгоритма хэширования<br>'06': Некорректное значение использования ключа<br>'07': Некорректное значение формата ключа<br>'08': Ошибка ключа HMAC<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Длина HMAC | 4 N | Длина выхода HMAC (t) в байтах, как определена в команде. |
| HMAC | n B | Сгенерированное значение HMAC. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [LS] — Проверка HMAC для блока данных

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка HMAC для блока данных.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Minimum HMAC length in bytes` (влияет на параметры: *HMAC*) | `[5-64]` | Минимальная длина HMAC, который может проверять HSM. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **КОМАНДА** |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'LS'. |
| Идентификатор алгоритма хэширования | 2 N | '01': SHA-1<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| | 2 H | Значение 'FF'. |
| Длина HMAC | 4 N | Длина HMAC для проверки (t) в байтах. Должна удовлетворять (Минимальная длина HMAC $\leq$ t $\leq$ L), где L — длина выхода хэш-функции (например, L = 20 в случае SHA-1), Минимальная длина HMAC задается с помощью консольной команды CS (Configure Security). |
| HMAC | n B | HMAC для проверки. |
| Формат ключа HMAC | 2 N | Определяет формат хранимого ключа. |
| | | '00': HMAC Key |
| | | '04': HMAC Key Block |
| Длина ключа HMAC | 4 N | Длина в байтах следующего поля. |
| | 4 H | Значение 'FFFF'. |
| Ключ HMAC | | Ключ, используемый для проверки переданного HMAC. *Примечание:* ключ не имеет префикса с символом ключевой схемы. |
| | n B | Ключ HMAC, зашифрованный под LMK 34-35/1. |
| | n A | Ключ HMAC должен соответствовать следующему формату: |

| Использование ключа | Алгоритм | Режим использования |
|---|---|---|
| '61' – '65' | 'H' | 'C', 'V', 'N' |

| | | |
|---|---|---|
| Разделитель | 1 A | Значение ';'. Присутствует только в случае Variant LMK. |
| Длина данных | 5 N | Длина сообщения для аутентификации. |
| Данные сообщения | n B | Данные для аутентификации. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |

| | | |
|---|---|---|
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'LT'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки HMAC<br>'04': Ошибка длины HMAC<br>'05': Некорректный идентификатор алгоритма хэширования<br>'06': Некорректное значение использования ключа<br>'07': Некорректное значение формата ключа<br>'08': Ошибка ключа HMAC<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [LU] — Импорт ключа HMAC, зашифрованного под ZMK

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Не требуется** | |
| Key Block LMK | Авторизация: **При импорте из формата, отличного от Key Block**<br>Активности: **import.{key}.host** | |

**Описание функции:** Импорт ключа HMAC, зашифрованного под зональным мастер-ключом (ZMK).

**Авторизация:** При импорте из формата, отличного от Key Block, HSM должен находиться в авторизованном состоянии, либо активность **import.{key}.host** должна быть авторизована, где 'key' — значение *Использования ключа* импортируемого ключа HMAC.

**Примечания:** Ключ HMAC, зашифрованный с помощью ZMK, должен иметь длину, кратную 8 байтам.

Для использования транспортных форматов 01, 02 или 03 должны быть выставлены соответствующие настройки (см. ниже).

При использовании транспортного формата 03 (X9.17) длина ключа HMAC должна быть строго кратна 8 байтам.

Импорт HMAC из транспортного формата 04 (Key Block) возможен только в случае использования Key Block LMK.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable PKCS#11 import and export for HMAC keys` | `Yes [Y]` | Доступно использование транспортных форматов 01, 02 (PKCS#11). |
| (влияет на параметры: *Транспортный формат*) | `No [N]` | Использование транспортных форматов 01, 02 (PKCS#11) не допускается. |
| `Enable ANSI X9.17 import and export for HMAC keys` | `Yes [Y]` | Доступно использование транспортного формата 03 (X9.17). |
| (влияет на параметры: *Транспортный формат*) | `No [N]` | Использование транспортного формата 03 (X9.17) не допускается. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'LU'.</td></tr>
<tr><td>ZMK</td><td></td><td>Зональный мастер-ключ, используемый для расшифрования ключа HMAC (ZMK).</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>ZMK, зашифрованный под LMK 04-05.</td></tr>
<tr><td></td><td>'S' + n A</td><td>ZMK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'K0', '52'</td><td>'T'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>Длина ключа HMAC (ZMK)</td><td>4 N</td><td>Если Транспортный формат = '00', '01', '02' или '03', это поле задает длину следующего поля (в байтах).</td></tr>
<tr><td></td><td>4 H</td><td>Если Транспортный формат = '04', значение 'FFFF'.</td></tr>
<tr><td>Ключ HMAC (ZMK)</td><td></td><td>Импортируемый ключ HMAC, зашифрованный под ZMK. Примечание: ключ не имеет префикса с символом ключевой схемы.</td></tr>
<tr><td></td><td>n B</td><td>Для всех транспортных форматов, отличных от Key Block (Транспортный формат ≠ '04').</td></tr>
<tr><td></td><td>n A</td><td>В случае Транспортного формата = '04' ключ HMAC (ZMK) должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'61' – '65'</td><td>'H'</td><td>'C', 'G', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует только в случае Транспортного формата = '00', '01', '02' или '03'.</td></tr>
<tr><td>Транспортный формат</td><td>2 N</td><td>Формат ключа HMAC (ZMK).<br>'00': проприетарный формат<br>'01': PKCS#11 ECB<br>'02': PKCS#11 CBC<br>'03': X9.17<br>'04': Key Block (недоступен для Variant LMK).</td></tr>
<tr><td>Формат ключа HMAC (LMK)</td><td>2 N</td><td>Определяет формат ключа HMAC, зашифрованного под LMK.</td></tr>
<tr><td></td><td></td><td>'00': HMAC Key</td></tr>
<tr><td></td><td></td><td>'04': HMAC Key Block</td></tr>
<tr><td>Идентификатор алгоритма хэширования</td><td>2 N или 2 H</td><td>Присутствует только в случае Транспортного формата = '01', '02' или '03'.<br>'01': SHA-1<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512</td></tr>
<tr><td>Использование ключа HMAC</td><td>2 N или 2 H</td><td>Присутствует только в случае Транспортного формата = '01', '02' или '03'.<br>'01': Генерация HMAC<br>'02': Проверка HMAC<br>'03': Генерация и проверка HMAC</td></tr>
<tr><td>Длина ключа HMAC</td><td>4 N</td><td>Присутствует только в случае Транспортного формата = '01', '02' или '03'. Длина ключа HMAC в байтах. Должна быть ≥ L/2, где L — длина выхода хэш-функции в байтах (например, L = 20 в случае SHA-1).</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
</table>

| | | |
|---|---|---|
| Следующие поля присутствуют только в случае генерации Key Block: | | |
| Разделитель | 1 A | Значение '#'. Обязательное поле в случае импорта в формат HMAC Key Block, если *Транспортный формат* ≠ '04'. Если присутствует, то следующие поля обязательны. |
| Использование ключа | 2 A | Поле *Использование ключа*, включаемое в заголовок Key Block (байты 5-6). Допустимые значения:<br>'61': SHA-1<br>'62': SHA-224<br>'63': SHA-256<br>'64': SHA-384<br>'65': SHA-512<br>*Примечание:* При импорте ключа из формата '00' значение поля должно быть согласовано со значением *Идентификатора алгоритма хэширования* импортируемого ключа. |
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block. Допустимые значения см. в таблице режимов использования ключа в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block. Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block. Допустимые значения: 'N' или 'S' (подробнее см. в таблице экспортируемости ключа в «КриптоПро HSM. Руководство программиста»). |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже. Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор опционального блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина опционального блока | 2 H | Количество символов в опциональном блоке (включая идентификатор и длину). Допустимые значения: 0x04 .. 0xFF. Если значение 0x04, следующее поле отсутствует. |
| Данные опционального блока | n A | Данные опционального блока. Отсутствует, если длина блока 0x04. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'LV'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Недопустимый транспортный формат<br>'04': Ошибка длины HMAC<br>'05': Некорректный идентификатор алгоритма хэширования<br>'06': Некорректное значение использования ключа<br>'07': Некорректное значение формата ключа<br>'08': Ошибка ключа HMAC<br>'10': Нарушена четность ZMK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Длина ключа HMAC | 4 N | Длина в байтах следующего поля. |
| | 4 H | Значение 'FFFF'. |

| | | |
|---|---|---|
| Ключ HMAC (LMK) | | Импортированный ключ HMAC. *Примечание:* ключ не имеет префикса с символом ключевой схемы. |
| | n B | Ключ HMAC, зашифрованный под LMK 34-35/1. |
| | n A | Ключ HMAC, зашифрованный под LMK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [LW] — Экспорт ключа HMAC с зашифрованием под ZMK

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Определяется по ТТК (Э)**<br>Активности: **export.hmac.host** | |
| Key Block LMK | Авторизация: **При экспорте в формат, отличный от Key Block**<br>Активности: **export.{key}.host** | |

**Описание функции:** Экспорт ключа HMAC с зашифрованием под зональным мастер-ключом (ZMK).

**Авторизация:**

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Команда проверяет флаг 'Э' (экспорт) для заданного типа ключа в таблице типов ключей (ТТК, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **export.hmac.host** должна быть авторизована. | При экспорте в формат, отличный от Key Block, HSM должен находиться в авторизованном состоянии, либо активность **export.{key}.host** должна быть авторизована, где 'key' — значение *Использования ключа* экспортируемого ключа HMAC. |

**Примечания:** Ключ HMAC, зашифрованный с помощью ZMK, должен иметь длину, кратную 8 байтам.

Для использования транспортных форматов 01, 02 или 03 должны быть выставлены соответствующие настройки (см. ниже).

При использовании транспортного формата 03 (X9.17) длина ключа HMAC должна быть строго кратна 8 байтам.

Экспорт HMAC в транспортный формат 04 (Key Block) возможен только в случае использования Key Block LMK.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable PKCS#11 import and export for HMAC keys` | `Yes [Y]` | Доступно использование транспортных форматов 01, 02 (PKCS#11). |
| (влияет на параметры: *Транспортный формат*) | `No [N]` | Использование транспортных форматов 01, 02 (PKCS#11) не допускается. |
| `Enable ANSI X9.17 import and export for HMAC keys` | `Yes [Y]` | Доступно использование транспортного формата 03 (X9.17). |
| (влияет на параметры: *Транспортный формат*) | `No [N]` | Использование транспортного формата 03 (X9.17) не допускается. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'LW'.</td></tr>
<tr><td>ZMK</td><td></td><td>Зональный мастер-ключ, используемый для зашифрования ключа HMAC (ZMK).</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>ZMK, зашифрованный под LMK 04-05.</td></tr>
<tr><td></td><td>'S' + n A</td><td>ZMK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'K0', '52'</td><td>'T'</td><td>'B', 'E', 'N'</td></tr>
</table></td></tr>
<tr><td>Формат ключа HMAC (LMK)</td><td>2 N</td><td>Определяет формат ключа HMAC, зашифрованного под LMK.</td></tr>
<tr><td></td><td></td><td>'00': HMAC Key</td></tr>
<tr><td></td><td></td><td>'04': HMAC Key Block</td></tr>
<tr><td>Транспортный формат</td><td>2 N</td><td>Формат ключа HMAC (ZMK).<br>'00': проприетарный формат<br>'01': PKCS#11 ECB<br>'02': PKCS#11 CBC<br>'03': X9.17<br>'04': Key Block (недоступен для Variant LMK).</td></tr>
<tr><td>Длина ключа HMAC (LMK)</td><td>4 N</td><td>Длина в байтах следующего поля.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
<tr><td>Ключ HMAC (LMK)</td><td></td><td>Экспортируемый ключ HMAC. Примечание: ключ не имеет префикса с символом ключевой схемы.</td></tr>
<tr><td></td><td>n B</td><td>Ключ HMAC, зашифрованный под LMK 34-35/1.</td></tr>
<tr><td></td><td>n A</td><td>Ключ HMAC должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'61' – '65'</td><td>'H'</td><td>'C', 'G', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае экспорта в формат Key Block (например, TR-31) при использовании Key Block LMK:</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '&'. Опционально; присутствует только если экспортируемый ключ в формате Key Block. Если присутствует, то следующее поле обязательно.</td></tr>
<tr><td>Экспортируемость</td><td>1 A</td><td>Поле Экспортируемость, включаемое в заголовок Key Block. Допустимое значение: 'N'.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'LX'. |

| | | |
|---|---|---|
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Недопустимый транспортный формат<br>'07': Некорректное значение формата ключа<br>'08': Ошибка ключа HMAC<br>'10': Нарушена четность ZMK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Длина ключа HMAC (ZMK) | 4 N | Если *Транспортный формат* = '00', '01', '02' или '03', это поле задает длину следующего поля (в байтах). |
| | 4 H | Если *Транспортный формат* = '04', значение 'FFFF'. |
| Ключ HMAC (ZMK) | | Экспортированный ключ HMAC, зашифрованный под ZMK в указанном транспортном формате. *Примечание:* ключ не имеет префикса с символом ключевой схемы. |
| | n B | Для всех транспортных форматов, отличных от Key Block (*Транспортный формат* $\neq$ '04'). |
| | n A | В случае *Транспортного формата* = '04'. |
| Идентификатор алгоритма хэширования | 2 N | Присутствует только в случае *Транспортного формата* = '01', '02' или '03'.<br>'01': SHA-1<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512 |
| Использование ключа HMAC | 2 N | Присутствует только в случае *Транспортного формата* = '01', '02' или '03'.<br>'01': Генерация HMAC<br>'02': Проверка HMAC<br>'03': Генерация и проверка HMAC |
| Длина ключа HMAC | 4 N | Присутствует только в случае *Транспортного формата* = '01', '02' или '03'. Длина ключа HMAC в байтах. Должна быть $\geq$ L/2, где L — длина выхода хэш-функции в байтах (например, L = 20 в случае SHA-1). |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

## [LY] — Трансляция ключа HMAC

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование ключа HMAC, зашифрованного под старым LMK, и последующее зашифрование под новым LMK.

**Примечания:** Эта команда может также использоваться для смены формата хранения ключа HMAC. При переводе ключей в формат Key Block команда ограничивает выбор значений *Режима использования* для совпадения со значением *Использование ключа HMAC*, определенного при создании ключа (например, с использованием команды 'L0').

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'LY'.</td></tr>
<tr><td>Входной формат ключа HMAC</td><td>2 N</td><td>Определяет формат входного ключа HMAC, зашифрованного под старым LMK.</td></tr>
<tr><td></td><td></td><td>'00': HMAC Key</td></tr>
<tr><td></td><td></td><td>'04': HMAC Key Block</td></tr>
<tr><td>Выходной формат ключа HMAC</td><td>2 N</td><td>Определяет формат выходного ключа HMAC, зашифрованного под текущим LMK.</td></tr>
<tr><td></td><td></td><td>'00': HMAC Key</td></tr>
<tr><td></td><td></td><td>'04': HMAC Key Block</td></tr>
<tr><td>Длина ключа HMAC</td><td>4 N</td><td>Длина в байтах следующего поля.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
<tr><td>Ключ HMAC</td><td></td><td>Ключ HMAC, зашифрованный под старым LMK. Примечание: ключ не имеет префикса с символом ключевой схемы.</td></tr>
<tr><td></td><td>n B</td><td>Ключ HMAC, зашифрованный под старым LMK 34-35/1.</td></tr>
<tr><td></td><td>n A</td><td>Ключ HMAC должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'61' – '65'</td><td>'H'</td><td>'C', 'G', 'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае трансляции из-под Variant LMK под Key Block LMK:</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '#'. Обязательное поле в случае трансляции в формат Key Block. Если присутствует, то следующие поля обязательны.</td></tr>
<tr><td>Использование ключа</td><td>2 A</td><td>Поле Использование ключа, включаемое в заголовок Key Block (байты 5-6).<br>Допустимые значения:<br>'61': SHA-1<br>'62': SHA-224<br>'63': SHA-256<br>'64': SHA-384<br>'65': SHA-512<br>Примечание: При трансляции ключа из формата '00' значение поля должно быть согласовано со значением Идентификатора алгоритма хэширования входного ключа.</td></tr>
</table>

| | | |
|---|---|---|
| Режим использования | 1 A | Поле *Режим использования*, включаемое в заголовок Key Block. Допустимые значения см. в таблице режимов использования ключа в «КриптоПро HSM. Руководство программиста». |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block. Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block. Допустимые значения см. в таблице экспортируемости ключа в «КриптоПро HSM. Руководство программиста». |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже. Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор опционального блока | 2 A | Любое допустимое значение, кроме 'PB'. |
| Длина опционального блока | 2 H | Количество символов в опциональном блоке (включая идентификатор и длину). Допустимые значения: 0x04 .. 0xFF. Если значение 0x04, следующее поле отсутствует. |
| Данные опционального блока | n A | Данные опционального блока. Отсутствует, если длина блока 0x04. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'LZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Недопустимый формат выходного ключа<br>'07': Недопустимый формат входного ключа<br>'08': Ошибка ключа HMAC<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Длина ключа HMAC | 4 N | Длина в байтах следующего поля. |
| | 4 H | Значение 'FFFF'. |
| Ключ HMAC | | Транслированный ключ HMAC, зашифрованный под текущим LMK. *Примечание:* ключ не имеет префикса с символом ключевой схемы. |
| | n B | Ключ HMAC, зашифрованный под LMK 34-35/1. |
| | n A | Ключ HMAC, зашифрованный под LMK. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

# 19 Вспомогательные команды

Следующие команды хоста используются для различных вспомогательных операций:

## [B2] — Echo

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Возврат указанных в команде данных обратно пользователю.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'B2'. |
| Длина данных | 4 H | Длина (в байтах) следующего поля. |
| Данные | n B | Пользовательские данные. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'B3'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Данные | n B | Пользовательские данные, соответствующие указанным в команде. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [RA] — Отмена авторизации активностей

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Отмена авторизации указанных активностей (или отмена авторизованного состояния HSM).

**Примечания:** Выполняется отмена авторизации только активностей, соответствующих указанному в команде LMK.

Отмена авторизации активностей с помощью этой команды регистрируется в журнале аудита.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce Authorization` | `Yes [Y]` | Команда выполняется в соответствии с описанием. |
| | `No [N]` | Команда не выполняет никаких действий. |
| `Enable multiple authorized activities` (влияет на параметры: *Флаг режима*) | `Yes [Y]` | Команда отменяет авторизацию активностей в соответствии со значением *Флага режима*. |
| | `No [N]` | Команда отменяет авторизованное состояние HSM. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'RA'. |
| Флаг режима | 2 H | Опционально. Если отсутствует, команда отменяет авторизацию всех активностей. Если присутствует, допустимые значения:<br>'00': Отмена авторизации всех активностей<br>'01': Отмена авторизации активностей, указанных ниже в команде<br>'02' .. 'FF': Зарезервировано |
| Следующие поля присутствуют только в случае *Флага режима* = '01': | | |
| Количество активностей | 3 N | Количество активностей (N) ниже. |
| Активность 1 | n A | Название активности (ASCII-символы) в формате `<категория>.[<подкатегория>].[<интерфейс>]` |
| Разделитель 1 | 1 A | Значение ';'. |
| Активность 2 | n A | Название активности (ASCII-символы) в формате `<категория>.[<подкатегория>].[<интерфейс>]` |
| Разделитель 2 | 1 A | Значение ';'. |
| ... | ... | ... |
| Активность N | n A | Название активности (ASCII-символы) в формате `<категория>.[<подкатегория>].[<интерфейс>]` |
| Разделитель N | 1 A | Значение ';'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'RB'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Недопустимое значение флага режима<br>'02': Настройка `Enable multiple authorized activities` выключена<br>'03': Указанная в команде активность не авторизована<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Флага режима* = '01': | | |
| Количество авторизованных активностей | 3 N | Количество авторизованных активностей после выполнения данной команды. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [BU] — Генерация проверочного значения ключа (KCV)

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Опционально (см. описание)**<br>Активности: **generate.{key}.host** | |
| Key Block LMK | Авторизация: **Не требуется** | |

**Описание функции:** Генерация проверочного значения (KCV) для ключа, зашифрованного под LMK.

**Авторизация:**

Для поддерживаемых в команде типов ключей:

- Генерация 6-значного KCV не требует авторизации
- Для генерации 16-значного KCV — HSM должен находиться в авторизованном состоянии, либо активность **generate.{key}.host** должна быть авторизована, где 'key' — код типа ключа, для которого вычисляется KCV.

**Примечания:**

Команда с помощью таблицы типов ключей проверяет, допускается ли использовать указанный тип ключа. Если указан недопустимый тип ключа, возвращается ошибка.

Если в поле *2-значный код типа ключа* указан код, соответствующий 3-значному коду типа ключа (без средней цифры), поле *3-значный код типа ключа* не должно присутствовать.

| Алгоритм ключа: | DES | AES | HMAC |
|---|---|---|---|
| Метод вычисления KCV: | Зашифрование блока бинарных нулей | Вычисление CMAC от блока бинарных нулей | Вычисление HMAC от сообщения нулевой длины |

При использовании команды с Variant LMK количество значимых символов возвращаемого значения KCV зависит от настройки безопасности (см. ниже). В случае использования Key Block LMK значение *KCV* всегда содержит 6 значимых цифр; в случае запроса 16-значного KCV крайние правые символы устанавливаются в '0'.

Команда не поддерживает работу с ключами HMAC, зашифрованными под Key Block LMK.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Restrict Key Check Value to 6 hex chars`<br>(влияет на параметры: *KCV*) | `Yes [Y]` | Только первые 6 символов параметра *KCV* содержат проверочное значение ключа, остальные крайние правые символы устанавливаются в '0'. |
| | `No [N]` | Дополнительные ограничения на KCV не накладываются. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'BU'.</td></tr>
<tr><td rowspan="2">2-значный код типа ключа</td><td>2 H</td><td>'00' .. '9E': поле содержит 2-значный код типа ключа, идентичный стандартному 3-значному коду типа ключа, но без средней цифры.<br>'FF': используется тип ключа, указанный ниже в поле 3-значный код типа ключа.</td></tr>
<tr><td>2 H</td><td>Значение 'FF'.</td></tr>
<tr><td rowspan="2">Флаг длины ключа</td><td>1 N</td><td>'1': 2DES<br>'2': 3DES<br>'3': HMAC</td></tr>
<tr><td>1 H</td><td>Значение 'F'.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют во всех случаях, кроме использования ключа HMAC (2-значный код типа ключа = '1C', Флаг длины ключа = '3'), зашифрованного под Variant LMK:</td></tr>
<tr><td rowspan="3">Ключ</td><td></td><td>Ключ, для которого вычисляется значение KCV.</td></tr>
<tr><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Ключ, зашифрованный под соответствующим LMK, определяемым значением поля 2-значный код типа ключа.</td></tr>
<tr><td>'S' + n A</td><td>Ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>Любое допустимое значение</td><td>Любое допустимое значение</td><td>Любое допустимое значение</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует только в случае 2-значного кода типа ключа = 'FF'. Если присутствует, следующее поле обязательно.</td></tr>
<tr><td rowspan="2">3-значный код типа ключа</td><td>3 H</td><td>В случае 2-значного кода типа ключа = 'FF' содержит 3-значный код типа ключа, для которого вычисляется значение KCV. Перечень допустимых значений см. в таблице типов ключей.</td></tr>
<tr><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Опционально; если присутствует, следующие 3 поля обязательны.</td></tr>
<tr><td>Зарезервировано</td><td>1 A</td><td>Опционально; если присутствует — значение '0'.</td></tr>
<tr><td>Зарезервировано</td><td>1 A</td><td>Опционально; если присутствует — значение '0'.</td></tr>
<tr><td>Тип KCV</td><td>1 A</td><td>Опционально. Метод вычисления проверочного значения ключа.<br>'0': 16-значный KCV (режим обратной совместимости, значение по умолчанию)<br>'1': 6-значный KCV</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае использования ключа HMAC (2-значный код типа ключа = '1C', Флаг длины ключа = '3'), зашифрованного под Variant LMK:</td></tr>
<tr><td>Идентификатор алгоритма хэширования</td><td>2 N</td><td>'01': SHA-1<br>'05': SHA-224<br>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512</td></tr>
<tr><td>Длина ключа HMAC</td><td>4 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td>Ключ HMAC</td><td>n B</td><td>Ключ, используемый для вычисления HMAC.<br>Примечание: ключ не имеет префикса с символом ключевой схемы.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
</table>

| | | |
|---|---|---|
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'BV'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Недопустимый тип ключа<br>'05': Недопустимая длина ключа<br>'10': Нарушена четность ключа<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| KCV | 16/6 H | Проверочное значение ключа, размер поля зависит от значения поля *Тип KCV*. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [LO] — Трансляция таблицы децимализации (из-под старого LMK под новый LMK)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование таблицы децимализации, зашифрованной под старым LMK, и последующее зашифрование под новым LMK.
«Старый» или «новый» LMK должен быть предварительно загружен в хранилище смены ключей.

**Примечания:** Команда предназначена для упрощения процесса смены LMK для эмитентов или обработчиков транзакций, которые используют большое количество таблиц децимализации.

По умолчанию предполагается использование зашифрованных таблиц децимализации, однако, возможно использование незашифрованных таблиц децимализации (см. описание настройки `Decimalization Table`). Рекомендуется использование зашифрованных таблиц децимализации.

Трансляция таблиц децимализации при смене «старого» Key Block LMK на «новый» Variant LMK не поддерживается.
Трансляция таблиц децимализации при смене «старого» Key Block AES LMK на «новый» DES LMK не поддерживается.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable Decimalization Table checks` | `Yes [Y]` `(по умолчанию)` | Выполняется проверка таблицы децимализации, подаваемой на вход: таблица децимализации должна содержать не менее 8 различных цифр, и каждая цифра должна повторяться не более 4 раз. Если требование не выполняется, возвращается ошибка 25. |
| | `No [N]` | Проверка таблицы децимализации не выполняется. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'LO'. |
| Таблица децимализации (под старым LMK) | 16 H<br>или | 16 H при использовании Variant LMK или 3DES Key Block LMK. |
| | 'L' + 32 H | 'L' + 32 H при использовании AES Key Block LMK. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'LP'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Таблица децимализации (под новым LMK) | 16 H<br>или | 16 H при использовании Variant LMK или 3DES Key Block LMK. |
| | 'L' + 32 H | 'L' + 32 H при использовании AES Key Block LMK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [NK] — Объединение команд

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Объединение и отправка нескольких команд в одном пакете.

**Примечания:** Команда позволяет объединять до 99 хостовых команд (называемых подкомандами) и отправлять их HSM в одном командном сообщении. HSM извлекает подкоманды, выполняет их по отдельности (как если бы они были отправлены хостом независимо), объединяет ответы и отправляет их хосту в одном ответном сообщении.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'NK'. |
| Флаг заголовка подкоманд | 1 N | '0': подкоманды без заголовка<br>'1': подкоманды с заголовком |
| Количество подкоманд | 2 N | Допустимые значения: '01' .. '99'. |
| **Подкоманда 1** | | |
| Длина | 4 N | Длина полей ниже в этой подкоманде. |
| Заголовок подкоманды | m A | Присутствует только в случае *Флага заголовка подкоманд* = '1'. |
| Код подкоманды | 2 A | Код подкоманды. |
| Параметры | ? | Входные параметры в соответствии с описанием подкоманды. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| **Подкоманда 2** | | |
| Длина | 4 N | Длина полей ниже в этой подкоманде. |
| Заголовок подкоманды | m A | Присутствует только в случае *Флага заголовка подкоманд* = '1'. |
| Код подкоманды | 2 A | Код подкоманды. |
| Параметры | ? | Входные параметры в соответствии с описанием подкоманды. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| ... | ... | ... |
| **Подкоманда N** | | |
| Длина | 4 N | Длина полей ниже в этой подкоманде. |
| Заголовок подкоманды | m A | Присутствует только в случае *Флага заголовка подкоманд* = '1'. |
| Код подкоманды | 2 A | Код подкоманды. |
| Параметры | ? | Входные параметры в соответствии с описанием подкоманды. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'NL'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'51': Недопустимый заголовок подкоманды<br>'52': Недопустимое значение количества подкоманд<br>'53': Недопустимое значение длины в подкоманде<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Количество подкоманд | 2 N | Количество выполняемых подкоманд. |
| **Подкоманда 1** | | |
| Длина | 4 N | Длина полей ниже в этой подкоманде. |
| Заголовок ответа подкоманды | m A | Присутствует только в случае *Флага заголовка подкоманд* = '1'. |
| Код ответа подкоманды | 2 A | Код ответа подкоманды. |
| Код ошибки | 2 H | Код ошибки в соответствии с описанием подкоманды. |
| Параметры | ? | Выходные параметры в соответствии с описанием подкоманды. |
| **Подкоманда 2** | | |
| Длина | 4 N | Длина полей ниже в этой подкоманде. |
| Заголовок ответа подкоманды | m A | Присутствует только в случае *Флага заголовка подкоманд* = '1'. |
| Код ответа подкоманды | 2 A | Код ответа подкоманды. |
| Код ошибки | 2 H | Код ошибки в соответствии с описанием подкоманды. |
| Параметры | ? | Выходные параметры в соответствии с описанием подкоманды. |
| ... | ... | ... |
| **Подкоманда N** | | |
| Длина | 4 N | Длина полей ниже в этой подкоманде. |
| Заголовок ответа подкоманды | m A | Присутствует только в случае *Флага заголовка подкоманд* = '1'. |
| Код ответа подкоманды | 2 A | Код ответа подкоманды. |
| Код ошибки | 2 H | Код ошибки в соответствии с описанием подкоманды. |
| Параметры | ? | Выходные параметры в соответствии с описанием подкоманды. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [CS] — Изменение заголовка Key Block

| Variant LMK ☒ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Опционально (см. описание)** | |
| Активности: **misc.host** | |

**Описание функции:** Изменение определённых полей в заголовке Key Block.

**Авторизация:** Авторизация требуется, если изменяется значение поля *Статус ключа*.

**Примечания:** Команда поддерживает только следующие изменения полей в заголовке Key Block:

| Поле заголовка Key Block | Старое значение | Новое значение |
|---|---|---|
| Экспортируемость | E, S | N |
| Статус ключа | P | E, L, R |
| | L | E, R |
| Режим использования | B, N | D, E |
| Режим использования | C, N | G, V |

Изменение значения поля *Режим использования* доступно только для симметричных ключей.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'CS'. |
| Исходный ключ | 'S' + n A<br>или<br>'S' + n B | Ключ в формате Key Block, для которого изменяется поле заголовка. |
| Изменяемое поле | 1 N | Флаг изменяемого поля, допустимые значения:<br>'0': Статус ключа<br>'1': Режим использования<br>'2': Экспортируемость |
| Старое значение | n A | Значение поля, которое необходимо изменить (не должно содержать символа ';'). |
| Разделитель | 1 A | Значение ';'. |
| Новое значение | n A | Новое значение поля (не должно содержать символа '%'). |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'CT'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'B7': Недопустимое изменяемое поле<br>'B8': Недопустимое старое значение<br>'B9': Недопустимое новое значение<br>'BA': Поле *Статус ключа* отсутствует в заголовке Key Block<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Изменённый ключ | 'S' + n A<br>или<br>'S' + n B | Ключ в формате Key Block с изменённым полем заголовка. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [N0] — Генерация случайного значения

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация случайного значения длиной до 256 байтов.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'N0' (N-ноль). |
| Длина случайного значения | 3 N | Десятичное число, допустимые значения: '001' .. '256'. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'N1'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Недопустимая длина случайного значения<br>или другой стандартный код ошибки. |
| Случайное значение | n B | Сгенерированное случайное значение, длина определяется значением поля *Длина случайного значения*. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 20 Команды диагностики

Следующие команды хоста используются для поддержки операций диагностики HSM:

## [NC] — Выполнение диагностики HSM

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Тестирование ПО и LMK, возврат хосту проверочного значения (KCV) для указанного LMK.

**Примечания:** Команда возвращает то же проверочное значение LMK, что и консольная команда V.

| Параметр | Формат | Описание |
|---|---|---|
| | | **КОМАНДА** |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'NC'. |
| Тип LMK | 1 A | Опционально; если поле отсутствует, используется значение по умолчанию '0'.<br>'0': возврат проверочного значения текущего LMK<br>'1': возврат проверочного значения LMK в хранилище смены ключей |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'ND'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| KCV | 16 N | Проверочное значение LMK. Совпадает со значением, возвращаемым консольной командой V. |
| Версия прошивки | 9 A | Номер версии прошивки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [NO] — Получение информации о состоянии HSM

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Возврат хосту информации о состоянии HSM.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'NO'. |
| Флаг режима | 2 H | '00': возврат информации о состоянии HSM<br>'01': возврат информации о соответствии PCI HSM<br>'50': возврат информации о состоянии ключа активации ПАКМ |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'NP'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Следующие 6 полей присутствуют только в случае *Флага режима* = '00': | | |
| Зарезервировано | 1 N | Значение '3'. |
| Сетевой протокол | 1 N | '1': TCP |
| Зарезервировано | 2 N | Значение '64'. |
| Версия прошивки | 9 A | Номер версии прошивки. |
| Зарезервировано | 1 N | Зарезервировано. |
| Зарезервировано | 4 A | Зарезервировано. |
| Следующие 2 поля присутствуют только в случае *Флага режима* = '01': | | |
| Соответствие PCI HSM | 1 N | '0': не выставлены некоторые настройки безопасности, которые относятся к соответствию PCI HSM (например, `Enforce key type 002 separation for PCI HSM compliance`)<br>'1': все настройки безопасности, которые относятся к соответствию PCI HSM, выставлены корректно<br>'2': не выставлены некоторые настройки безопасности, которые относятся к соответствию PCI HSM (настройка `Enforce key type 002 separation for PCI HSM compliance` не относится к таким настройкам) |
| Зарезервировано | 10 A | Зарезервировано. |
| Следующее поле присутствует только в случае *Флага режима* = '50': | | |
| Состояние ключа активации ПАКМ | 1 N | '0': ключ не активирован (HSM неактивен)<br>'1': ключ активирован (HSM активен) |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [NI] — Получение информации о сетевой активности

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Возврат хосту информации о сетевой активности на сетевых интерфейсах HSM.

Данные сведения могут быть полезны при настройке устройства, а также использоваться для обнаружения и анализа нетипичной сетевой активности.

HSM собирает информацию о каждом конечном устройстве, которое с ним взаимодействует.

Для TCP пакетов HSM возвращает следующие сведения:

- Локальный TCP-порт
- Удаленные IP-адрес и TCP-порт
- Статус TCP-соединения

Для UDP пакетов:

- Локальный UDP-порт
- Удаленные IP-адрес и UDP-порт

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'NI'. |
| Интерфейс | 1 A | '1': интерфейс eth0<br>'2': интерфейс eth1<br>'3': интерфейс eth2 (при наличии)<br>'4': интерфейс eth3 (при наличии)<br>'X': все интерфейсы |
| Статистика Ethernet | 1 N | '0': не возвращать статистические данные (количество пакетов, байтов, ошибок)<br>'1': возвращать статистические данные |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'NJ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'68': Команда недоступна<br>'82': Недопустимое значение поля *Статистика Ethernet* или другой стандартный код ошибки. |
| Количество записей | 4 N | Количество записей ниже. |
| **Запись 1** | | |
| Протокол | 1 N | '0': TCP<br>'1': UDP |
| Локальный порт | 4 H | Номер порта HSM. |
| Удаленный адрес | 8 H | IP-адрес удаленного узла. Например, C1F06541 = 193.240.101.65. |
| Удаленный порт | 4 H | Номер порта на удаленном узле. |

| | | |
|---|---|---|
| Статус TCP-соединения | 1 N | '0': установлено (ESTABLISHED)<br>'1': закрыто (CLOSED) |
| Зарезервировано | 8 N | Значение '00000000'. |
| **Запись 2** | | |
| Протокол | 1 N | ... |
| Локальный порт | 4 H | ... |
| Удаленный адрес | 8 H | ... |
| Удаленный порт | 4 H | ... |
| Статус TCP-соединения | 1 N | ... |
| Зарезервировано | 8 N | ... |
| ... | ... | ... |
| **Запись N** | | |
| Протокол | 1 N | ... |
| Локальный порт | 4 H | ... |
| Удаленный адрес | 8 H | ... |
| Удаленный порт | 4 H | ... |
| Статус TCP-соединения | 1 N | ... |
| Зарезервировано | 8 N | ... |
| Следующие поля присутствуют только в случае *Статистики Ethernet* = '1': | | |
| Отправлено байтов | 16 H | Общее количество байтов, отправленных с указанного интерфейса. |
| Получено байтов | 16 H | Общее количество байтов, полученных на указанном интерфейсе. |
| Отправлено пакетов | 8 H | Общее количество пакетов, отправленных с указанного интерфейса. |
| Получено пакетов | 16 H | Общее количество пакетов, полученных на указанном интерфейсе. |
| Зарезервировано | 8 H | Значение '00000000'. |
| Зарезервировано | 8 H | Значение '00000000'. |
| Отброшено пакетов при отправке | 8 H | Общее количество пакетов, отброшенных при отправке с указанного интерфейса. |
| Отброшено пакетов при получении | 8 H | Общее количество пакетов, отброшенных при получении на указанном интерфейсе. |
| Ошибки при отправке | 8 H | Общее количество ошибок, обнаруженных при отправке пакетов с указанного интерфейса. |
| Ошибки при получении | 8 H | Общее количество ошибок, обнаруженных при получении пакетов на указанном интерфейсе. |
| Зарезервировано | 8 H | Значение '00000000'. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [J2] — Получение статистики загруженности HSM

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Возврат статистики загруженности HSM в виде списка интервалов уровня загрузки (например, от 10% до 20%), с указанием, сколько секунд HSM был загружен в этом интервале. Данная статистика ведётся со времени последнего сброса.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'J2'. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'J3'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка выполнения команды<br>или другой стандартный код ошибки. |
| Серийный номер | 12 A | Серийный номер HSM, возвращающего данные. |
| Дата начала | 6 N | Дата последнего сброса статистики, в формате YYMMDD. |
| Время начала | 6 N | Время последнего сброса статистики, в формате HHMMSS. |
| Дата окончания | 6 N | Дата окончания сбора статистики, в формате YYMMDD. |
| Время окончания | 6 N | Время окончания сбора статистики, в формате HHMMSS. |
| Дата отчёта | 6 N | Текущая дата, в формате YYMMDD. |
| Время отчёта | 6 N | Текущее время, в формате HHMMSS.<br>*Примечание:* если текущие время и дата равны времени и дате окончания, в настоящий момент статистика продолжает собираться. |
| Продолжительность сбора статистики | 10 N | Общее число секунд, в течение которых собиралась статистика. |
| Следующие 4 поля повторяются 11 раз, для интервалов 000-010, 010-020, . . . , 090-100, 100-100.<br>*Примечание:* подразумевается, что для первых 10 интервалов нижняя граница включена в интервал, верхняя не включена, а в интервал 100-100 попадают секунды, когда была зафиксирована полная загрузка HSM.<br>Например, '0200300000001234' означает, что 1234 секунды за время сбора статистики сервер HSM был загружен от 20% до 30%. | | |
| Начало интервала (%) | 3 N | Начало интервала измерения, в процентах.<br>Допустимые значения: '000' .. '100'. |
| Конец интервала (%) | 3 N | Число от «начала интервала» до 100, конец интервала измерения, в процентах.<br>Допустимые значения: '000' .. '100'. |
| Количество секунд | 10 N | Число секундных периодов, в течение которых загруженность HSM находилась в данном интервале. |
| Разделитель | 1 A | Значение ';'. |

| | | |
|---|---|---|
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [J4] — Получение статистики использования HSM

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** При использовании функции без параметров возвращает количество вызовов каждой команды хоста (**сокращённый ответ**).

При использовании функции с опциональным параметром *Расширение* возвращает статистику загруженности HSM в виде списка интервалов уровня загрузки (например, от 10% до 20%), с указанием, сколько секунд HSM был загружен в этом интервале (**расширенный ответ**).

Также в расширенном варианте функция возвращает для каждой команды хоста:

1. Количество вызовов команды.
2. Количество успешных (вернувших код ошибки '00') вызовов команды.
3. Значение TPS, вычисленное как количество вызовов, поделённое на сумму времён их исполнения. Данная величина удобна для оценки максимальной производительности HSM.
4. Значение Successful TPS, вычисленное как количество успешных вызовов, поделённое на сумму времён их исполнения. Данная величина удобна для оценки максимальной производительности HSM.
5. Значение Average TPS, вычисленное как количество вызовов, поделённое на число секундных интервалов, в которые попадал хотя бы один из них. Данная величина удобна для оценки производительности HSM в реальных системах и в нагрузочных тестах.
6. Значение Successful Average TPS, вычисленное как количество успешных вызовов, поделённое на число секундных интервалов, в которые попадал хотя бы один из них. Данная величина удобна для оценки производительности HSM в реальных системах и в нагрузочных тестах.

Статистика ведётся с момента последнего сброса.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'J4'. |
| Расширение | 1 N | Опционально. Если отсутствует, команда возвращает количество вызовов каждой команды хоста (**сокращённый ответ**). Если присутствует и равен '1', возвращает **расширенный ответ** (см. Примечание выше). При любом другом значении возвращается ошибка. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

**Сокращённый ответ:**

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'J5'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка выполнения команды<br>или другой стандартный код ошибки. |
| Серийный номер | 12 A | Серийный номер HSM, возвращающего данные. |
| Дата начала | 6 N | Дата последнего сброса статистики, в формате YYMMDD. |
| Время начала | 6 N | Время последнего сброса статистики, в формате HHMMSS. |
| Дата окончания | 6 N | Дата окончания сбора статистики, в формате YYMMDD. |
| Время окончания | 6 N | Время окончания сбора статистики, в формате HHMMSS. |
| Дата отчёта | 6 N | Текущая дата, в формате YYMMDD. |
| Время отчёта | 6 N | Текущее время, в формате HHMMSS.<br>*Примечание:* если текущие время и дата равны времени и дате окончания, в настоящий момент статистика продолжает собираться. |
| Продолжительность сбора статистики | 10 N | Общее число секунд, в течение которых собиралась статистика. |
| Следующие 2 поля повторяются до конца сообщения.<br>*Примечание:* в полях ниже перечисляются все хотя бы раз выполненные команды (если команда не выполнялась ни разу, она не указывается); коды команд упорядочены по алфавиту. | | |
| Код команды | 2 A | Код команды. |
| Число команд | 12 N | Количество выполненных за время сбора статистики команд с указанным выше кодом команды. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

**Расширенный ответ:**

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'J5'. |

| | | |
|---|---|---|
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка выполнения команды<br>или другой стандартный код ошибки. |
| Серийный номер | 12 A | Серийный номер HSM, возвращающего данные. |
| Дата начала | 6 N | Дата последнего сброса статистики, в формате YYMMDD. |
| Время начала | 6 N | Время последнего сброса статистики, в формате HHMMSS. |
| Дата окончания | 6 N | Дата окончания сбора статистики, в формате YYMMDD. |
| Время окончания | 6 N | Время окончания сбора статистики, в формате HHMMSS. |
| Дата отчёта | 6 N | Текущая дата, в формате YYMMDD. |
| Время отчёта | 6 N | Текущее время, в формате HHMMSS.<br>*Примечание:* если текущие время и дата равны времени и дате окончания, в настоящий момент статистика продолжает собираться. |
| Продолжительность сбора статистики | 10 N | Общее число секунд, в течение которых собиралась статистика. |

Следующие 4 поля повторяются 11 раз, для интервалов 000-010, 010-020, . . . , 090-100, 100-100.

*Примечание:* подразумевается, что для первых 10 интервалов нижняя граница включена в интервал, верхняя не включена, а в интервал 100-100 попадают секунды, когда была зафиксирована полная загрузка HSM.
Например, '0200300000001234' означает, что 1234 секунды за время сбора статистики сервер HSM был загружен от 20% до 30%.

| | | |
|---|---|---|
| Начало интервала (в %) | 3 N | Число от 0 до 100, начало интервала измерения, в процентах. |
| Конец интервала (в %) | 3 N | Число от «начала интервала» до 100, конец интервала измерения, в процентах. |
| Количество секунд | 10 N | Число секундных периодов, в течение которых загруженность HSM находилась в данном интервале. |
| Разделитель | 1 A | Значение ';'. |

Следующие 7 полей повторяются до конца сообщения.

*Примечание:* в полях ниже перечисляются все хотя бы раз выполненные команды (если команда не выполнялась ни разу, она не указывается); коды команд упорядочены по алфавиту.

| | | |
|---|---|---|
| Код команды | 2 A | Код команды. |
| Число команд | 12 N | Количество выполненных за время сбора статистики команд с указанным выше кодом команды. |
| Число успешных команд | 12 N | Количество выполненных за время сбора статистики успешных (вернувших код ошибки '00') команд с указанным выше кодом команды. |
| TPS | 7 N 1 A 2 N | Значение TPS, вычисленное как количество вызовов, поделённое на общее время их исполнения.<br>Первое число (7 N) содержит целую часть значения TPS; допустимые значения: '0000000' .. '1000000'.<br>Далее указывается разделитель (1 A), значение '.'.<br>Второе число (2 N) содержит сотые доли значения TPS; допустимые значения: '00' .. '99'. |
| Successful TPS | 7 N 1 A 2 N | Значение Successful TPS, вычисленное как количество успешных вызовов, поделённое на общее время их исполнения.<br>Первое число (7 N) содержит целую часть значения Successful TPS; допустимые значения: '0000000' .. '1000000'.<br>Далее указывается разделитель (1 A), значение '.'.<br>Второе число (2 N) содержит сотые доли значения Successful TPS; допустимые значения: '00' .. '99'. |

| | | |
|---|---|---|
| Average TPS | 7 N 1 A 2 N | Значение Average TPS, вычисленное как количество вызовов, поделённое на число секундных интервалов, в которые попадал хотя бы один из них.<br>Первое число (7 N) содержит целую часть значения Average TPS; допустимые значения: '0000000' .. '1000000'.<br>Далее указывается разделитель (1 A), значение '.'.<br>Второе число (2 N) содержит сотые доли значения Average TPS; допустимые значения: '00' .. '99'. |
| Successful Average TPS | 7 N 1 A 2 N | Значение Successful Average TPS, вычисленное как количество успешных вызовов, поделённое на число секундных интервалов, в которые попадал хотя бы один из них.<br>Первое число (7 N) содержит целую часть значения Average TPS; допустимые значения: '0000000' .. '1000000'.<br>Далее указывается разделитель (1 A), значение '.'.<br>Второе число (2 N) содержит сотые доли значения Average TPS; допустимые значения: '00' .. '99'. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [J6] — Сброс статистики использования HSM

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Сброс накопленных данных о загруженности HSM и о количестве и времени выполнения команд, которые возвращаются в командах J2, J4, JO и в консольной команде UTILSTATS (подробнее см. «КриптоПро HSM. Команды консоли»).

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'J6'. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'J7'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка выполнения команды<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [J8] — Получение статистики работоспособности HSM

**Описание функции:** Получение накопленных данных (статистики) о работоспособности HSM с момента последнего сброса данных (за исключением периодов, когда сбор статистики был приостановлен).

**Примечания:** Сброс накопленных данных статистики может быть выполнен с помощью консольной команды HEALTHSTATS.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'J8'. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'J9'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка выполнения команды<br>или другой стандартный код ошибки. |
| Серийный номер | 12 A | Серийный номер HSM. |
| Дата начала | 6 N | Дата начала сбора статистики (дата последнего сброса статистики), в формате YYMMDD. |
| Время начала | 6 N | Время начала сбора статистики (время последнего сброса статистики), в формате HHMMSS. |
| Дата окончания | 6 N | Дата окончания сбора статистики, в формате YYMMDD. |
| Время окончания | 6 N | Время окончания сбора статистики, в формате HHMMSS. |
| Дата отчёта | 6 N | Текущая дата, в формате YYMMDD. |
| Время отчёта | 6 N | Текущее время, в формате HHMMSS.<br>*Примечание:* если текущие время и дата равны времени и дате окончания, в настоящий момент статистика продолжает собираться. |
| Количество перезапусков HSM | 10 N | Количество перезапусков HSM с момента последнего сброса статистики. |
| Количество вскрытий корпуса HSM | 10 N | Количество обнаруженных вскрытий корпуса HSM. |
| Превышение лимита ошибочных проверок PIN (в минуту) | 7 N | Количество превышений лимита ошибок проверки PIN в минуту с момента последнего сброса статистики. |
| Превышение лимита ошибочных проверок PIN (в час) | 5 N | Количество превышений лимита ошибок проверки PIN в час с момента последнего сброса статистики. |
| Количество PIN-атак | 8 N | Количество обнаруженных атак на PIN с момента последнего сброса статистики. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [JK] — Проверка работоспособности HSM

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Получение текущего статуса различных характеристик работоспособности HSM.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'JK'. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'JL'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка выполнения команды<br>или другой стандартный код ошибки. |
| Серийный номер | 12 A | Серийный номер HSM. |
| Системная дата | 6 N | Текущая дата, в формате YYMMDD. |
| Системное время | 6 N | Текущее время, в формате HHMMSS. |
| Статус консоли | 1 N | Текущий статус работы службы обработки консольных команд:<br>0: неизвестно<br>1: работает<br>2: не работает |
| Статус web-интерфейса администрирования | 1 N | Текущий статус работы web-интерфейса администрирования:<br>0: неизвестно<br>1: работает<br>2: не работает |
| Статус сетевого интерфейса eth0 | 1 N | Текущий статус работы сетевого интерфейса eth0:<br>0: неизвестно<br>1: работает<br>2: не работает<br>3: не сконфигурирован для работы с хостом |
| Статус сетевого интерфейса eth1 | 1 N | Текущий статус работы сетевого интерфейса eth1:<br>0: неизвестно<br>1: работает<br>2: не работает<br>3: не сконфигурирован для работы с хостом |
| Зарезервировано | 1 N | Значение '0'. |
| Зарезервировано | 1 N | Значение '0'. |
| Зарезервировано | 1 N | Значение '1'. |
| Количество LMK | 2 N | Количество LMK в основном хранилище. |
| Количество тестовых LMK | 2 N | Количество тестовых LMK в основном хранилище. |

| | | |
|---|---|---|
| Количество LMK в хранилище смены ключей | 2 N | Количество LMK в хранилище смены ключей («новых» и «старых»). |
| Следующие 8 полей повторяются для каждого LMK из основного хранилища: | | |
| Идентификатор LMK | 2 N | Идентификатор LMK в основном хранилище. |
| Авторизация | 1 N | Состояние авторизации для указанного LMK:<br>0: LMK не авторизован<br>1: LMK авторизован |
| Количество авторизованных активностей | 2 N | Количество авторизованных активностей (в случае авторизованного LMK). |
| Схема | 1 A | 'V': Variant LMK<br>'K': Key Block LMK |
| Алгоритм | 1 N | 0: 2DES<br>1: 3DES<br>2: AES-256 |
| Статус | 1 A | 'L': рабочий LMK<br>'T': тестовый LMK |
| Комментарии | 0 .. 40 A | Строка с комментариями. |
| Разделитель | 1 A | Значение '0x14'. |
| Разделитель | 1 A | Значение '0x15'. Признак конца полей характеристик LMK. |
| Превышение лимита ошибочных проверок PIN | 1 N | Индикатор превышения установленного количества ошибок при проверке PIN в минуту/час:<br>0: не превышен (или не включен)<br>1: превышен |
| Превышение лимита атак на PIN | 1 N | Индикатор превышения установленного лимита атак на PIN (с последующим удалением LMK):<br>0: не превышен (или не включен)<br>1: превышен |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 21 Команды процессинга по чиповым картам EMV

Раздел посвящен командам хоста, которые используются для поддержки онлайн обработки транзакций различных платежных схем в соответствии с международным стандартом EMV.

Следующие команды хоста используются для поддержки операций чиповых карт EMV:

## Порядок именования ключей

Разные платежные системы имеют собственные соглашения об именах используемых в HSM ключей. Ниже представлена сводная таблица соответствия наименований ключей.

| Описание ключа | Наименования ключа, используемое в документации | Наименование ключа в спецификации Visa | Наименование ключа в спецификации Mastercard |
|---|---|---|---|
| Мастер-ключ эмитента для генерации и проверки Application Cryptogram | MK-AC | DMK | Issuer MK |
| Мастер-ключ эмитента для обеспечения целостности передаваемых данных | MK-SMI | DMK | Issuer MK |
| Мастер-ключ эмитента для обеспечения конфиденциальности передаваемых данных | MK-SMC | DMK | Issuer MK |
| Мастер-ключ эмитента для вычисления и проверки Data Authentication Code (DAC) | MK-DAC | - | Issuer MK |
| Мастер-ключ эмитента для генерации Dynamic Number (DN) | MK-DN | - | Issuer MK |
| Диверсифицированный ключ для генерации и проверки Application Cryptogram | DK-AC | UDK | ICC MK |
| Диверсифицированный ключ для обеспечения целостности передаваемых данных | DK-SMI | UDK | ICC MK |
| Диверсифицированный ключ для обеспечения конфиденциальности передаваемых данных | DK-SMC | UDK | ICC MK |
| Диверсифицированный ключ для генерации Dynamic Number (DN) | DK-DN | - | ICC MK |

## [KQ] — Проверка ARQC и/или генерация ARPC (с использованием статического или MasterCard Proprietary SKD метода)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Опционально (см. описание)** | |
| Активности: **diagnostic.host** | |

**Описание функции:** Проверка ARQC (или TC/AAC) и, опционально, генерация ARPC. Команда также может использоваться только для генерации ARPC.

**Примечания:** Для вывода диагностических данных требуется авторизованное состояние HSM.

Поле *Диагностические данные* содержит сгенерированное значение ARQC, которое возвращается хосту, если не прошла проверка переданного в команде значения ARQC.
Поле *Диагностические данные MAC* содержит вычисленный MAC для дискреционных данных, который возвращаются хосту, если не прошла проверка переданного в команде MAC для дискреционных данных.

Команда поддерживает следующие методы генерации криптограмм:

| Приложение | Идентификатор схемы |
|---|---|
| Visa VIS (CVN 10 или 17) | '0' |
| Mastercard M/Chip (CVN 10 или 11) | '1' |
| American Express AEIPS (CVN 01 или 02) | '2' |

За применение методов дополнения, соответствующих используемой схеме, отвечает хост, добавляя необходимое дополнение в конец передаваемых данных перед отправкой на HSM. Для некоторых схем необходимо добавить в конец данных байт 0x80. Если длина данных, переданных хостом, кратна 8 байтам, дальнейшее дополнение не требуется; в противном случае данные дополняются нулями.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'KQ'.</td></tr>
<tr><td>Флаг режима</td><td>1 N</td><td>'0': Только проверка ARQC<br>'1': Проверка ARQC и генерация ARPC<br>'2': Только генерация ARPC<br>'3': Проверка ARQC и MAC для дискреционных данных (требуется использовать Идентификатор схемы = '0')<br>'4': Проверка ARQC и MAC для дискреционных данных, генерация ARPC (требуется использовать Идентификатор схемы = '0')</td></tr>
<tr><td>Идентификатор схемы</td><td>1 N</td><td>Методы диверсификации ключей карты:<br>'0': EMV Option 'A' ICC Master Key Derivation (Visa VIS)<br>'1': EMV Option 'A' ICC Master Key Derivation и Mastercard Proprietary Session Key Derivation (Mastercard M/Chip)<br>'2': EMV Option 'A' ICC Master Key Derivation (American Express AEIPS)</td></tr>
<tr><td>MK-AC</td><td></td><td>Мастер-ключ эмитента для генерации и проверки Application Cryptogram.</td></tr>
<tr><td></td><td>32 H или 'U' + 32 H</td><td>MK-AC, зашифрованный под LMK 28-29/1.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK-AC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'E0'</td><td>'T'</td><td>'X', 'N'</td></tr></table></td></tr>
<tr><td>MK-SMI</td><td></td><td>Присутствует только в случае Флага режима = '3' или '4' и Идентификатора схемы = '0'.<br>Мастер-ключ эмитента для обеспечения целостности передаваемых данных.</td></tr>
<tr><td></td><td>32 H или 'U' + 32 H</td><td>MK-SMI, зашифрованный под LMK 28-29/2.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK-AC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'E2'</td><td>'T'</td><td>'X', 'N'</td></tr></table></td></tr>
<tr><td>Номер карты (PAN)/PAN Sequence Number</td><td>8 B</td><td>Предварительно отформатированный PAN/PSN.</td></tr>
<tr><td>ATC</td><td>2 B</td><td>Счетчик транзакций.</td></tr>
<tr><td>UN</td><td>4 B</td><td>Unpredictable Number. Присутствует для всех режимов, используется только в случае Идентификатора схемы = '1'.</td></tr>
<tr><td>Длина данных транзакции</td><td>2 H</td><td>Присутствует только в случае Флага режима = '0', '1', '3' или '4'.<br>Длина следующего поля. Допустимые значения: '01' .. 'FF'.</td></tr>
<tr><td>Данные транзакции</td><td>n B</td><td>Присутствует только в случае Флага режима = '0', '1', '3' или '4'.<br>Данные переменной длины.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует только в случае Флага режима = '0', '1', '3' или '4'. Признак конца поля Данные транзакции.</td></tr>
<tr><td>ARQC/TC/AAC</td><td>8 B</td><td>Проверяемое и/или используемое для генерации ARPC значение ARQC/TC/AAC.</td></tr>
<tr><td>ARC</td><td>2 B</td><td>Присутствует только в случае Флага режима = '1', '2' или '4'.<br>Authorisation Response Code для генерации ARPC.</td></tr>
<tr><td>MAC для дискреционных данных</td><td>4 B</td><td>Присутствует только в случае Флага режима = '3' или '4' и Идентификатора схемы = '0'.</td></tr>
<tr><td>Длина дискреционных данных</td><td>2 N</td><td>Присутствует только в случае Флага режима = '3' или '4' и Идентификатора схемы = '0'.<br>Длина следующего поля, должна быть кратна 8 байтам.</td></tr>
</table>

| | | |
|---|---|---|
| Дискреционные данные | n B | Присутствует только в случае *Флага режима* = '3' или '4' и *Идентификатора схемы* = '0'.<br>Дискреционные данные, для которых вычисляется MAC. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KR'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки ARQC/TC/AAC (предупреждение)<br>'03': Флаг режима = '3' или '4', однако Идентификатор схемы ≠ '0'<br>'04': Некорректное значение флага режима<br>'05': Некорректный идентификатор схемы<br>'06': Ошибка проверки MAC для дискреционных данных (предупреждение)<br>'10': Нарушена четность MK-AC<br>'11': Нарушена четность MK-SMI<br>'68': Команда недоступна<br>'80': Ошибка длины данных транзакции<br>'82': Некорректная длина MAC для данных транзакции<br>или другой стандартный код ошибки. |
| ARPC | 8 B | Сгенерированное значение ARPC. Присутствует только в случае *Флага режима* = '1', '2' или '4' и отсутствия ошибки. |
| Диагностические данные | 8 B | Сгенерированное значение ARQC/TC/AAC. Присутствует только в случае *Флага режима* = '0', '1', '3' или '4', *Кода ошибки* = '01' и если HSM находится в авторизованном состоянии. |
| Диагностические данные MAC | 8 B | Вычисленный MAC для дискреционных данных. Присутствует только в случае *Флага режима* = '3' или '4', *Кода ошибки* = '06' и если HSM находится в авторизованном состоянии. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [KW] — Проверка ARQC и/или генерация ARPC (с использованием метода EMV или Cloud-Based SKD)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Опционально (см. описание)** | |
| Активности: **diagnostic.host** | |

**Описание функции:** Проверка ARQC (или TC/AAC) и, опционально, генерация ARPC. Команда также может использоваться только для генерации ARPC.

**Примечания:** Для вывода диагностических данных требуется авторизованное состояние HSM.

Поле *Диагностические данные* содержит сгенерированное значение ARQC, которое возвращается хосту, если не прошла проверка переданного в команде значения ARQC.

Команда выполняет ту же функцию, что и команда 'KQ', однако с использованием методов EMV2000 или EMV Common Session Key Derivation для генерации сессионного ключа.

Команда поддерживает следующие методы генерации криптограмм:

| Приложение | Идентификатор схемы |
|---|---|
| Visa VIS (CVN 14) | '0' |
| Visa VIS (CVN 18 или '22') | '2' или '3' |
| Visa VCP (CVN '43') | '4' |
| Visa VCP QR Code (CVN 44) | '8' |
| Mastercard M/Chip (CVN 12 или 13) (EMV 2000) | '0' |
| Mastercard M/Chip (CVN 14 или 15) (EMV CSK) | '2' |
| Mastercard MCBP | '5' |
| American Express (CVN 05, 07 и MPVV) | '6' |
| Discover D-PAS (05 или 06) | '2' |
| Indonesian National Standard Chip Card Specification (NSICCS) | '2' |
| EMV Option 'C' Card Key Generation и EMV CSK | '9' |
| JCB (CVN 01) | 'A' |
| JCB (CVN 02) | 'B' |
| JCB (CVN 04) | '2' |
| Union Pay (ver. 4.2) | 'C' |

За применение методов дополнения, соответствующих используемой схеме, отвечает хост, добавляя необходимое дополнение в конец передаваемых данных перед отправкой на HSM. Для некоторых схем необходимо добавить в конец данных байт 0x80.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'KW'. |
| Флаг режима | 1 H | '0': Только проверка ARQC<br>'1': Проверка ARQC и генерация ARPC (EMV 4.x Method 1)<br>'2': Только генерация ARPC (EMV 4.x Method 1)<br>'3': Проверка ARQC и генерация ARPC (EMV 4.x Method 2)<br>'4': Только генерация ARPC (EMV 4.x Method 2)<br>'7': Только проверка American Express MPVV |
| Идентификатор схемы | 1 A | Методы диверсификации ключей карты:<br>'0': EMV Option 'A' Card Key Derivation и EMV2000 Session Key Derivation<br>'1': EMV Option 'B' Card Key Derivation и EMV2000 Session Key Derivation<br>'2': EMV Option 'A' Card Key Derivation и EMV Common Session Key Derivation (также используется Indonesian National Standard Chip Card Specification (NSICCS) и JCB (CVN 04))<br>'3': EMV Option 'B' Card Key Derivation и EMV Common Session Key Derivation<br>'4': Visa Cloud-Based Payments с использованием EMV Option 'A' Card Key Derivation и Limited Use Key (допускается только в случае *Флага режима* = '0')<br>'5': Mastercard Cloud-Based Payments с использованием EMV Option 'A' Card Key Derivation и EMV Common Session Key Derivation (допускается только в случае *Флага режима* = '0', '1' или '3')<br>'6': American Express Cloud-Based Payments (допускается только в случае *Флага режима* = '0' или '7')<br>'8': Visa Cloud-Based Payments, QR Code, с использованием EMV Option 'A' Card Key Derivation и Limited Use Key (допускается только в случае *Флага режима* = '0')<br>'9': EMV Option 'C' Card Key Derivation и EMV Common Session Key Derivation<br>'A': JCB (CVN 01): EMV Option 'A' Card Key Derivation без Session Key Derivation<br>'B': JCB (CVN 02): EMV Option 'A' Card Key Derivation и JCB Session Key Derivation<br>'C': Union Pay (ver. 4.2): EMV Option 'A' Card Key Derivation и Union Pay Session Key Derivation (допускается только в случае *Флага режима* = '0', '1' или '2') |
| MK-AC | | Мастер-ключ эмитента для формирования и проверки Application Cryptogram (или MPVV в случае *Флага режима* = '7'). |
| | 'U' + 32 H | MK-AC, зашифрованный под LMK 28-29/1. |
| | 'S' + n A | MK-AC должен соответствовать следующему формату:<br>Использование ключа: 'E0'<br>Алгоритм: 'T', 'A'<br>Режим использования: 'X', 'N' |
| IV-AC | 16 B | Присутствует только в случае *Идентификатора схемы* = '0' или '1'.<br>IV для метода диверсификации сессионного ключа EMV2000. |
| Длина номера карты (PAN) | 2 N | Присутствует только в случае *Идентификатора схемы* = '1', '3', '6' или '9'.<br>Длина (в байтах) следующего поля. Допустимые значения: '08' .. '32'. |

| | | |
|---|---|---|
| Номер карты (PAN)/PAN Sequence Number | 8 B или n B | В случае *Идентификатора схемы* = '0', '2', '4', '5', '8', 'A', 'B' или 'C' это поле имеет фиксированную длину 8 байтов и содержит предварительно отформатированный PAN/PSN.<br>В случае *Идентификатора схемы* = '1', '3', '6' или '9' длина поля определяется значением поля *Длина номера карты (PAN)*.<br>*Примечание:* Поле должно содержать четное число символов (следовательно, целое число байтов), при необходимости дополненное слева '0').<br>*Примечание:* За корректность дополнения PAN/PSN (при необходимости) отвечает хост. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Идентификатора схемы* = '1', '3', '6' или '9'. Признак конца поля *Номер карты (PAN)/PAN Sequence Number*. |
| Параметры ветвления/высоты дерева | 1 N | Присутствует только в случае *Идентификатора схемы* = '0' или '1'.<br>'0': коэффициент ветвления 2; высота дерева 16<br>'1': коэффициент ветвления 4; высота дерева 8 |
| ATC | 2 B | Присутствует только в случае *Идентификатора схемы* = '0', '1', '2', '3', '5', '6', '9', 'B' или 'C'.<br>Значение ATC, предоставленное картой, используется для генерации сессионных ключей.<br>В случае Truncated AC — ATC последней транзакции, сохраненной в БД хоста. |
| Флаг дополнения | 1 N | Присутствует только в случае *Флага режима* = '0' или '1' и *Идентификатора схемы* = 'C'. Признак применения процедуры дополнения к данным транзакции.<br>'0': входные данные транзакции не были дополнены и, если они не кратны 8, должны быть дополнены при обработке в команде<br>'1': входные данные транзакции были дополнены и должны быть кратны 8, процедура дополнения в команде не применяется |
| YHHHHCC | 7 N | Присутствует только в случае *Идентификатора схемы* = '4' или '8'.<br>Значение Год/Час/Счетчик, используемое для выработки ключа ограниченного использования (LUK) для генерации ARQC:<br>Y (0-9): последняя значащая цифра текущего года<br>HHHH (0001-8784): количество часов, прошедших с 01 января<br>CC (00-99): значение счетчика |
| Метод диверсификации UDK | 1 A | Присутствует только в случае *Идентификатора схемы* = '6'.<br>'A': EMV Option 'A'<br>'B': EMV Option 'B' |
| Метод диверсификации сессионного ключа | 1 A | Присутствует только в случае *Идентификатора схемы* = '6'.<br>'1': EMV Common Session Key Derivation |
| Метод проверки ARQC | 2 N | Присутствует только в случае *Идентификатора схемы* = '6'.<br>'01': Method 1<br>'03': Method 2 |
| Длина данных транзакции | 2 H | Присутствует только в случае *Флага режима* = '0', '1' или '3'.<br>Длина следующего поля. Допустимые значения: '01' .. 'FF'. |
| Данные транзакции | n B | Присутствует только в случае *Флага режима* = '0', '1' или '3'.<br>Данные переменной длины.<br>Для всех значений *Идентификатора схемы*, кроме '9' и 'C', если входные данные транзакции кратны 8, дополнение данных не производится, иначе применяется дополнение нулями 0x00.<br>Для *Идентификатора схемы* = '9' дополнение данных не требуется.<br>Для *Идентификатора схемы* = 'C' данные дополняются согласно описанию поля *Флаг дополнения*. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Флага режима* = '0', '1' или '3'. Признак конца поля *Данные транзакции*. |

| | | |
|---|---|---|
| Маска ARQC | 8 B | Присутствует только в случае *Идентификатора схемы* = '5' или '6'.<br>Маска для проверки ARQC или MPVV длиной меньше 8 байт. Например, маска 0xFFFFFFFF00000000 указывает, что сравниваться будут первые (крайние слева) 4 байта ARQC. |
| ARQC/TC/AAC или MPVV | 8 B | Проверяемое и/или используемое для генерации ARPC значение ARQC/TC/AAC или MPVV. Если длина ARQC/TC/AAC или MPVV меньше 8 байт, используется дополнение нулями 0x00. |
| ARC | 2 B | Присутствует только в случае *Флага режима* = '1' или '2'.<br>Authorisation Response Code для генерации ARPC. |
| CSU | 4 B | Присутствует только в случае *Флага режима* = '3' или '4'.<br>Card Status Update, используемый для генерации ARPC для карт Common Core Definitions (CCD). |
| Длина проприетарных данных аутентификации | 1 N | Присутствует только в случае *Флага режима* = '3' или '4'.<br>Длина следующего поля. Допустимые значения: '0' .. '8'. |
| Проприетарные данные аутентификации | 0 .. 8 B | Присутствует, только если предыдущее поле содержит ненулевое значение.<br>Опциональные данные эмитента, включаемые в передаваемые на карту данные аутентификации эмитента онлайн-транзакции. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KX'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки ARQC/TC/AAC (предупреждение)<br>'03': Некорректный флаг дополнения<br>'04': Некорректное значение флага режима<br>'05': Некорректный идентификатор схемы<br>'06': Некорректное значение YHHHHCC<br>'10': Нарушена четность MK-AC<br>'52': Некорректное значение параметра ветвления/высоты дерева<br>'68': Команда недоступна<br>'F1': Некорректный метод диверсификации ключа<br>'F2': Некорректный метод проверки ARQC<br>'F3': Алгоритм MK-AC отличен от AES<br>'F5': Некорректный метод диверсификации сессионного ключа<br>'82': Длина данных транзакции не кратна 8 байтам<br>или другой стандартный код ошибки. |
| APRC | 8 B | Сгенерированное значение APRC. Присутствует только в случае *Флага режима* = '1', '2', '3' или '4' и отсутствия ошибки. В случае *Флага режима* = '3' или '4' содержит 4-байтовый ARPC и 4-байтовый CSU. |
| Диагностические данные | 8 B | Сгенерированное значение ARQC/TC/AAC или MPVV. Присутствует только в случае *Кода ошибки* = '01' и если HSM находится в авторизованном состоянии. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [KU] — Генерация Secure Message (EMV 3.1.1)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация сообщения (Secure Message) с обеспечением целостности для данных, передаваемых от эмитента обратно карте. Опционально команда поддерживает обеспечение конфиденциальности при обмене сообщениями. В этом случае данные сообщения представлены в зашифрованном с использованием транспортного ключа виде — команда сначала расшифровывает данные с помощью транспортного ключа, а затем повторно зашифровывает их с использованием сеансового ключа.

**Примечания:** Команда также может использоваться для изменения или разблокировки PIN.

При изменении PIN эмитент проверяет текущий PIN, а затем принимает новый PIN в формате PIN-блока. Этот PIN-блок, зашифрованный под зональным или терминальным ключом, транслируется из стандартного для ATM формата PIN-блока в формат, специфичный для конкретного приложения, и зашифровывается под сессионным ключом.

Для разблокировки PIN необходимо использовать *Флаг режима* = '0' (обеспечение только целостности) с указанием EMV PIN Unblock APDU в поле *Незашифрованное сообщение*.

Команда поддерживает следующие методы генерации криптограмм:

| Приложение | Идентификатор схемы |
|---|---|
| Visa VIS (CVN 10) | '0' |
| Mastercard M/Chip (CVN 10 или 11) | '1' |
| American Express AEIPS (CVN 01) | '2' |
| JCB (CVN 01) | '3' |
| JCB (CVN 02) | '4' |
| JCB (CVN 04) | '5' |
| Union Pay (ver. 4.2) | '6' |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'KU'. |
| Флаг режима | 1 N | '0': Только целостность<br>'1': Целостность и конфиденциальность, с использованием одного мастер-ключа эмитента<br>'2': Целостность и конфиденциальность, с использованием разных мастер-ключей эмитента<br>'3': Целостность и трансляция PIN-блока для изменения PIN, с использованием одного мастер-ключа эмитента<br>'4': Целостность и трансляция PIN-блока для изменения PIN, с использованием разных мастер-ключей эмитента |
| Идентификатор схемы | 1 N | '0': Visa VIS<br>'1': Mastercard M/Chip<br>'2': American Express AEIPS<br>'3': JCB (CVN 01): EMV Option 'A' ICC Master Key Derivation без генерации сессионного ключа<br>'4': JCB (CVN 02): EMV Option 'A' ICC Master Key Derivation и JCB Session Key Derivation<br>'5': JCB (CVN 04): EMV Option 'A' ICC Master Key Derivation с EMV 4.x Common Session Key Derivation<br>'6': Union Pay (ver. 4.2): EMV Option 'A' ICC Master Key Derivation и Union Pay Session Key Derivation<br><br>*Примечание:* значения '3', '4' и '5' (JCB) допускается использовать только в случае *Флага режима* = '0', '1' или '2'. |
| MK-SMI | | Мастер-ключ эмитента для обеспечения целостности, используемый для вычисления MAC. |
| | 'U' + 32 H | MK-SMI, зашифрованный под LMK 28-29/2. |
| | 'S' + n A | MK-SMI должен соответствовать следующему формату:<br>Использование ключа: 'E2'; Алгоритм: 'T'; Режим использования: 'X', 'N' |
| Номер карты (PAN)/PAN Sequence Number | 8 B | Предварительно отформатированный PAN/PSN. |
| Данные для генерации сессионного ключа целостности | 8 B<br>или | Для *Идентификатора схемы* = '0' или '2' — значение ATC (2 байта), выровненное по правому краю и дополненное 6 нулевыми байтами слева.<br>Для *Идентификатора схемы* = '1' — случайное число RANDi.<br>Для *Идентификатора схемы* = '5' — значение Application Cryptogram, возвращаемое картой в ответ на первую команду GENERATE AC. |
| | 2 B | Для *Идентификатора схемы* = '3', '4' или '6' — значение ATC. |
| Флаг дополнения | 1 N | Присутствует только в случае *Идентификатора схемы* = '6'.<br>Признак применения процедуры дополнения к данным в поле *Незашифрованное сообщение*.<br>'0': входные данные сообщения не были дополнены и должны быть дополнены при обработке в команде<br>'1': входные данные сообщения были дополнены и должны быть кратны 8, процедура дополнения в команде не применяется |
| Длина незашифрованного сообщения | 4 H | Длина (в байтах) следующего поля. |
| Незашифрованное сообщение | n B | Данные сообщения. |
| Разделитель | 1 A | Значение ';'. |

<table>
<tr><td>MK-SMC</td><td></td><td>Присутствует только в случае Флага режима = '2' или '4'. Мастер-ключ эмитента для обеспечения конфиденциальности, используемый для зашифрования сообщения.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>MK-SMC, зашифрованный под LMK 28-29/3.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK-SMC должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E1'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>TK</td><td></td><td>Присутствует только в случае Флага режима = '1' или '2' и Идентификатора схемы ≠ '6'.<br>Транспортный ключ, используемый для расшифрования передаваемого в команде зашифрованного сообщения.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>TK, зашифрованный под LMK 30-31.</td></tr>
<tr><td></td><td>'S' + n A</td><td>TK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'D0', '22'</td><td>'T'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td>Данные для генерации сессионного ключа конфиденциальности</td><td>8 B</td><td>Присутствует только в случае Флага режима = '1', '2', '3' или '4' и Идентификатора схемы = '0', '1' или '2'.<br>Для Идентификатора схемы = '0' или '2' — значение ATC (2 байта), выровненное по правому краю и дополненное 6 нулевыми байтами слева.<br>Для Идентификатора схемы = '1' — случайное число RANDc.</td></tr>
<tr><td>Смещение</td><td>4 H</td><td>Присутствует только в случае Флага режима = '1', '2', '3' или '4'.<br>Смещение (в байтах) внутри Незашифрованного сообщения для вставки результата перешифрования поля Зашифрованное сообщение.<br>В случае Флага режима = '3' или '4' — значение смещения внутри Незашифрованного сообщения для вставки нового PIN-блока.<br>Допустимые значения: 0000 .. Длина незашифрованного сообщения.<br>Если смещение = n, зашифрованные данные вставляются после n-го байта данных незашифрованного сообщения (т.е. если длина незашифрованного сообщения = 0039, и смещение = 39, зашифрованные данные располагаются в конце данных незашифрованного сообщения).</td></tr>
<tr><td colspan="3">Следующие 3 поля присутствуют только в случае Флага режима = '1', '2', '3', '4' и Идентификатора схемы ≠ '6':</td></tr>
<tr><td>Длина зашифрованного сообщения</td><td>4 H</td><td>Длина (в байтах) следующего поля. Допустимые значения: 8, 16, 24 или 32.</td></tr>
<tr><td>Зашифрованное сообщение</td><td>n B</td><td>Примечание: к расшифрованному сообщению не применяется дополнительная процедура дополнения перед повторным зашифрованием.<br>В случае Флага режима = '1' или '2' — сообщение, передаваемое карте, зашифрованное под TK.<br>В случае Флага режима = '3' или '4':<br>• если Код формата возвращаемого PIN-блока ≠ '42' — новый PIN-блок, зашифрованный под ключом шифрования исходного PIN-блока.<br>• если Код формата возвращаемого PIN-блока = '42' — конкатенация текущего PIN-блока, зашифрованного под ключом шифрования исходного PIN-блока, и нового PIN-блока, зашифрованного под ключом шифрования исходного PIN-блока.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td colspan="3">Следующие 3 поля присутствуют только в случае Флага режима = '1', '2' и Идентификатора схемы = '6':</td></tr>
<tr><td>Длина данных для зашифрования</td><td>4 H</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td>Данные для зашифрования</td><td>n B</td><td>Данные для зашифрования.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
</table>

<table>
<tr><td colspan="3">Следующие поля присутствуют только в случае Флага режима = '3' или '4':</td></tr>
<tr><td>Тип ключа шифрования исходного PIN-блока</td><td>1 N</td><td>'0': ZPK<br>'1': TPK</td></tr>
<tr><td></td><td>1 H</td><td>Значение 'F'.</td></tr>
<tr><td>Ключ шифрования исходного PIN-блока</td><td></td><td>Ключ шифрования исходного PIN-блока, используемый для расшифрования нового PIN-блока, передаваемого в поле Зашифрованное сообщение.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Ключ шифрования PIN-блока, зашифрованный под соответствующим LMK, определяемым значением поля Тип ключа шифрования исходного PIN-блока:<br>ZPK, зашифрованный под LMK 06-07<br>TPK, зашифрованный под LMK 14-15/0 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: No</code>) или LMK 36-37/7 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: Yes</code>).</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ шифрования PIN-блока должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'P0', '71', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr></table></td></tr>
<tr><td>Код формата исходного PIN-блока</td><td>2 N</td><td>Код формата исходного PIN-блока.<br>Примечание: код формата '48' допускается использовать только в случае Идентификатора схемы ≠ '6'.</td></tr>
<tr><td>Код формата возвращаемого PIN-блока</td><td>2 N</td><td>Присутствует только в случае Идентификатора схемы ≠ '6'.<br>'34': Стандартный формат PIN-блока EMV (ISO 9564-1 format 2)<br>'35': Europay/Mastercard Pay Now & Pay Later<br>'41': Формат Visa для изменения PIN без использования текущего PIN<br>'42': Формат Visa для изменения PIN с использованием текущего PIN</td></tr>
<tr><td>Номер карты (PAN)</td><td></td><td>Присутствует только в случае Идентификатора схемы ≠ '6'.<br>Номер карты (PAN), используемый при формировании PIN-блока.</td></tr>
<tr><td></td><td>n N</td><td>Если Код формата исходного PIN-блока = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель.</td></tr>
<tr><td></td><td>или<br>12 N</td><td>Для всех остальных значений поля Код формата исходного PIN-блока:<br>12 крайних правых цифр PAN, за исключением контрольной цифры.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Присутствует только в случае Идентификатора схемы ≠ '6' и Кода формата исходного PIN-блока = '48'.</td></tr>
<tr><td>MK-AC</td><td></td><td>Присутствует только в случае Идентификатора схемы ≠ '6' и Кода формата возвращаемого PIN-блока = '41' или '42'.<br>Мастер-ключ эмитента для генерации и проверки Application Cryptogram (требуется для генерации PIN-блоков при смене PIN для Visa).</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>MK-AC, зашифрованный под LMK 28-29/1.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK-AC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'E0'</td><td>'T'</td><td>'X', 'N'</td></tr></table></td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае Флага режима = '3' или '4' и Идентификатора схемы = '6':</td></tr>
<tr><td>Номер карты (PAN)</td><td>12 N</td><td>12 крайних правых цифр PAN, за исключением контрольной цифры.</td></tr>
<tr><td>Формат возвращаемого PIN-блока</td><td>1 N</td><td>'1': возвращаемый PIN-блок с текущим (старым) PIN<br>'2': возвращаемый PIN-блок без текущего (старого) PIN</td></tr>
<tr><td>Исходный новый PIN-блок</td><td>16 H</td><td>PIN-блок, зашифрованный под ключом шифрования исходного PIN-блока.</td></tr>
</table>

| | | |
|---|---|---|
| Исходный текущий PIN-блок | 16 H | Присутствует только в случае *Формата возвращаемого PIN-блока* = '1'.<br>PIN-блок, зашифрованный под ключом шифрования исходного PIN-блока. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KV'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Недопустимый флаг дополнения<br>'04': Недопустимый флаг режима<br>'05': Недопустимый идентификатор схемы<br>'06': Недопустимое значение смещения<br>'07': Недопустимая длина зашифрованного сообщения<br>'08': Ошибка длины зашифрованного сообщения<br>'09': Нарушена четность TK или ZPK/TPK<br>'10': Нарушена четность MK-SMI<br>'11': Нарушена четность MK-SMC<br>'23': Недопустимый код формата исходного PIN-блока<br>'50': Недопустимый тип ключа шифрования исходного PIN-блока<br>'51': Нарушена четность MK-AC (в случае *Идентификатора схемы* ≠ '6')<br>'51': Недопустимый формат возвращаемого PIN-блока (в случае *Идентификатора схемы* = '6')<br>'52': Ошибка длины PIN (в новом PIN-блоке)<br>'53': Недопустимый формат исходного текущего PIN-блока<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>'80': Ошибка длины незашифрованного сообщения<br>'81': Ошибка длины данных для зашифрования<br>'82': Длина незашифрованного сообщения не кратна 8 байтам<br>или другой стандартный код ошибки. |
| Следующие поля присутствуют только в случае *Идентификатора схемы* = '6': | | |
| MAC | 8 H | 4-байтовое значение MAC. |
| Зашифрованный возвращаемый новый PIN-блок | 32 H | Присутствует только в случае *Флага режима* = '3' или '4'. |
| Длина зашифрованного сообщения | 4 H | Присутствует только в случае *Флага режима* = '1' или '2'.<br>Длина (в байтах) следующего поля. |
| Зашифрованное сообщение | n B | Присутствует только в случае *Флага режима* = '1' или '2'. |
| Следующие поля присутствуют только в случае *Идентификатора схемы* ≠ '6': | | |
| MAC | 8 B | 8-байтовое значение MAC. |
| Длина повторно зашифрованного сообщения | 4 H | Присутствует только в случае *Флага режима* = '1', '2', '3' или '4'.<br>Длина (в байтах) следующего поля. |
| Повторно зашифрованное сообщение | n B | Присутствует только в случае *Флага режима* = '1', '2', '3' или '4'. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |

| | | |
|---|---|---|
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [KY] — Генерация Secure Message (EMV 4.x)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация сообщения (Secure Message) с обеспечением целостности для данных, передаваемых от эмитента обратно карте. Опционально, команда поддерживает обеспечение конфиденциальности при обмене сообщениями. В этом случае данные сообщения представлены в зашифрованном с использованием транспортного ключа виде — команда сначала расшифровывает данные с помощью транспортного ключа, а затем повторно зашифровывает их с использованием сеансового ключа.

**Примечания:** Команда выполняет ту же функцию, что и команда 'KU', однако с использованием методов EMV2000 или EMV Common Session Key Derivation для генерации сессионного ключа.

Команда поддерживает следующие методы генерации криптограмм:

| Приложение | Идентификатор схемы |
|---|---|
| Visa VIS (CVN 14) | '0' |
| Visa VIS (CVN '22') | '9' |
| Visa VIS (CVN 18) | 'A' |
| Mastercard M/Chip (CVN 12 или 13) | '1' |
| Mastercard M/Chip (CVN 14 или 15) | '6' |
| Discover D-PAS (CVN 05 или 06) | '6' |

Команда 'KU' поддерживает режимы работы (*Флаг режима* = '1' и '3'), позволяющие использовать один мастер-ключ эмитента для обеспечения целостности и конфиденциальности сообщения. Данная возможность предусмотрена для поддержки M/Chip 2.1. Спецификация M/Chip 4 рекомендует использовать разные ключи для обеспечения целостности и конфиденциальности. В соответствии с данной рекомендацией команда 'KY' не позволяет генерировать ключи для обеспечения целостности и конфиденциальности из одного мастер-ключа.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'KY'.</td></tr>
<tr><td>Флаг режима</td><td>1 N</td><td>'0': Только целостность<br>'2': Целостность и конфиденциальность<br>'4': Целостность и изменение PIN<br>'5': Только целостность (метод диверсификации ключа определяется значением поля Идентификатор схемы)<br>Примечание: в случае Флага режима = '0' используются методы EMV 4.x Option 'A' ICC Master Key Derivation и EMV2000 Session Key Derivation. Для других режимов метод диверсификации ключа определяется значением поля Идентификатор схемы.</td></tr>
<tr><td>Идентификатор схемы</td><td>1 N</td><td>Присутствует только в случае Флага режима = '2', '4' или '5'.<br>Используемые методы диверсификации ключа и дополнения.<br>'0': Visa VIS с использованием EMV 4.x Option 'A' ICC Master Key Derivation и EMV2000 Session Key Derivation<br>'1': Mastercard M/Chip с использованием EMV 4.x Option 'A' ICC Master Key Derivation и EMV2000 Session Key Derivation<br>'4': CCD с использованием EMV 4.x Option 'B' ICC Master Key Derivation и EMV2000 Session Key Derivation<br>'5': Visa VIS и Indonesian National Standard Chip Card Specification (NSICCS) с использованием EMV 4.x Option 'A' ICC Master Key Derivation и EMV Common Session Key Derivation<br>'6': Mastercard M/Chip и Discover D-PAS с использованием EMV 4.x Option 'A' ICC Master Key Derivation и EMV Common Session Key Derivation<br>'7': CCD с использованием EMV 4.x Option 'B' ICC Master Key Derivation и EMV Common Session Key Derivation<br>'8': CCD с использованием EMV 4.x Option 'C' ICC Master Key Derivation EMV AES Common Session Key Derivation (допускается только в случае Флага режима = '5')<br>'9': Visa VIS 1.6 с использованием EMV 4.3 Option 'B' ICC master Key derivation и EMV Common Session Key Generation.<br>'A': Visa VIS 1.6 с использованием EMV 4.3 Option 'B' ICC master Key derivation и XOR Session Key Generation.<br>Примечание: в случае Флага режима = '5' определяет только метод диверсификации ключа, т.к. дополнение не применяется.</td></tr>
<tr><td>MK-SMI</td><td></td><td>Мастер-ключ эмитента для обеспечения целостности, используемый для вычисления MAC.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>MK-SMI, зашифрованный под LMK 28-29/2.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK-SMI должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E2'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>IV-SMI</td><td>16 B</td><td>Присутствует только в случае Флага режима = '0' или Идентификатора схемы = '0', '1', '4'.<br>Вектор инициализации, используемый при диверсификации сессионного ключа обеспечения целостности.</td></tr>
<tr><td>Длина номера карты (PAN)</td><td>2 N</td><td>Присутствует только в случае Идентификатора схемы = '4', '7', '8', '9', 'A'.<br>Длина (в байтах) следующего поля. Допустимые значения: '01' .. '19'.<br>Примечание: если поле Номер карты (PAN)/PAN Sequence Number содержит нечетное число символов, он должен быть дополнен слева '0' (до целого числа байтов).</td></tr>
</table>

| | | |
|---|---|---|
| Номер карты (PAN)/PAN Sequence Number | | Конкатенация PAN и PAN Sequence Number. |
| | 8 B | В случае *Флага режима* = '0' или *Флага режима* ≠ '0' и *Идентификатора схемы* = '0', '1', '5', '6' — предварительно отформатированный PAN/PSN (в BCD формате) длиной 8 байтов.<br>*Примечание:* PAN/PSN должен быть дополнен до 8 байтов (согласно EMV Option A), за корректность дополнения PAN/PSN (при необходимости) отвечает хост. |
| | или n B | В случае *Флага режима* ≠ '0' и *Идентификатора схемы* = '4', '7', '8', '9', 'A' — PAN/PSN (в BCD формате), длина поля определяется значением поля *Длина номера карты (PAN)*.<br>*Примечание:* Поле должно содержать четное число символов (следовательно, целое число байтов), при необходимости дополненное слева '0'. PAN/PSN затем используется согласно EMV Option B.<br>*Примечание:* Если длина PAN < 8 байт, то HSM дополнит поле до 8 байтов, если это необходимо, в соответствии с EMV Option A. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Идентификатора схемы* = '4', '7', '8', '9', 'A'. Признак конца поля *Номер карты (PAN)/PAN Sequence Number*. |
| Параметры ветвления/высоты дерева | 1 N | Присутствует только в случае *Флага режима* = '0' или *Идентификатора схемы* = '0', '1', '4'.<br>'0': коэффициент ветвления 2; высота дерева 16<br>'1': коэффициент ветвления 4; высота дерева 8 |
| ATC | 2 B | Присутствует только в случае *Флага режима* = '0' или *Идентификатора схемы* = '0', '1', '4', 'A'.<br>Значение ATC, полученное от карты; используется для генерации сессионного ключа. |
| Application Cryptogram | 8 B | Присутствует только в случае *Идентификатора схемы* = '5', '6', '7', '8', '9'.<br>Значение Application Cryptogram, возвращаемое картой в ответ на первую команду GENERATE AC. |
| Длина незашифрованного сообщения | 4 H | Длина (в байтах) следующего поля. |
| Незашифрованное сообщение | n B | Данные сообщения. |
| Разделитель | 1 A | Значение ';'. |
| MK-SMC | | Присутствует только в случае *Флага режима* = '2', '4'.<br>Мастер-ключ эмитента для обеспечения конфиденциальности, используемый для зашифрования сообщения. |
| | 'U' + 32 H | MK-SMC, зашифрованный под LMK 28-29/3. |
| | 'S' + n A | MK-SMC должен соответствовать следующему формату:<br>Использование ключа: 'E1'; Алгоритм: 'T'; Режим использования: 'X', 'N' |
| IV-SMC | 16 B | Присутствует только в случае *Флага режима* = '2', '4' и *Идентификатора схемы* = '0', '1', '4'.<br>Вектор инициализации, используемый при диверсификации сессионного ключа обеспечения конфиденциальности. |

<table>
<tr><td>ТК</td><td></td><td>Присутствует только в случае Флага режима = '2'.<br>Транспортный ключ, используемый для расшифрования передаваемого в команде зашифрованного сообщения.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>ТК, зашифрованный под LMK 30-31.</td></tr>
<tr><td></td><td>'S' + n A</td><td>ТК должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'D0', '22'</td><td>'T'</td><td>'B', 'D', 'N'</td></tr></table></td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае Флага режима = '2' или '4':</td></tr>
<tr><td>Смещение</td><td>4 H</td><td>Смещение (в байтах) внутри Незашифрованного сообщения для вставки результата перешифрования поля Зашифрованное сообщение. В случае Флага режима = '4' — значение смещения внутри Незашифрованного сообщения для вставки нового PIN-блока.<br>Допустимые значения: 0000 .. Длина незашифрованного сообщения.<br>Если смещение = n, зашифрованные данные вставляются после n-го байта данных незашифрованного сообщения (т.е. если длина незашифрованного сообщения = 0039, и смещение = 39, зашифрованные данные располагаются в конце данных незашифрованного сообщения)</td></tr>
<tr><td>Длина зашифрованного сообщения</td><td>4 H</td><td>Длина (в байтах) следующего поля. Допустимые значения: 8, 16, 24 или 32.</td></tr>
<tr><td>Зашифрованное сообщение</td><td>n B</td><td>Примечание: к расшифрованному сообщению не применяется дополнительная процедура дополнения перед повторным зашифрованием.<br>В случае Флага режима = '2' — сообщение, передаваемое карте, зашифрованное под ТК.<br>В случае Флага режима = '4':<br>• если Код формата возвращаемого PIN-блока ≠ '42' — новый PIN-блок, зашифрованный под ключом шифрования исходного PIN-блока.<br>• если Код формата возвращаемого PIN-блока = '42' — конкатенация текущего PIN-блока, зашифрованного под ключом шифрования исходного PIN-блока, и нового PIN-блока, зашифрованного под ключом шифрования исходного PIN-блока.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае Флага режима = '4':</td></tr>
<tr><td>Тип ключа шифрования исходного PIN-блока</td><td>1 N</td><td>'0': ZPK<br>'1': TPK</td></tr>
<tr><td></td><td>1 H</td><td>Значение 'F'.</td></tr>
<tr><td>Ключ шифрования исходного PIN-блока</td><td></td><td>Ключ шифрования исходного PIN-блока, используемый для расшифрования PIN-блока, передаваемого в поле Зашифрованное сообщение.</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Ключ шифрования PIN-блока, зашифрованный под соответствующим LMK, определяемым значением поля Тип ключа шифрования исходного PIN-блока:<br>ZPK, зашифрованный под LMK 06-07<br>TPK, зашифрованный под LMK 14-15/0 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: No</code>) или LMK 36-37/7 (если выставлена настройка <code>Enforce key type 002 separation for PCI HSM compliance: Yes</code>).</td></tr>
<tr><td></td><td>'S' + n A</td><td>Ключ шифрования PIN-блока должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'P0', '71', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr></table></td></tr>
<tr><td>Код формата исходного PIN-блока</td><td>2 N</td><td>Код формата исходного PIN-блока.</td></tr>
</table>

| | | |
|---|---|---|
| Код формата возвращаемого PIN-блока | 2 N | '34': Стандартный формат PIN-блока EMV (ISO 9564-1 format 2)<br>'35': Europay/Mastercard Pay Now & Pay Later<br>'41': Формат Visa для изменения PIN без использования текущего PIN<br>'42': Формат Visa для изменения PIN с использованием текущего PIN |
| Номер карты (PAN) | | Номер карты (PAN), используемый при формировании PIN-блока. |
| | n N | Если *Код формата исходного PIN-блока* = '48':<br>12 крайних правых цифр PAN, за исключением контрольной цифры, или 13-19 цифр PAN, включая контрольную цифру.<br>В данном случае в следующем поле должен присутствовать разделитель. |
| | или<br>12 N | Для всех остальных значений поля *Код формата исходного PIN-блока*:<br>12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Кода формата исходного PIN-блока* = '48'. |
| MK-AC | | Присутствует только в случае *Кода формата возвращаемого PIN-блока* = '41' или '42'.<br>Мастер-ключ эмитента для генерации и проверки Application Cryptogram (требуется для генерации PIN-блоков при смене PIN для Visa). |
| | 'U' + 32 H | MK-AC, зашифрованный под LMK 28-29/1. |
| | 'S' + n A | MK-AC должен соответствовать следующему формату:<br>Использование ключа: 'E0'; Алгоритм: 'T'; Режим использования: 'X', 'N' |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Недопустимый флаг режима<br>'05': Недопустимый идентификатор схемы<br>'06': Недопустимое значение смещения<br>'07': Недопустимая длина зашифрованного сообщения<br>'08': Ошибка длины зашифрованного сообщения<br>'09': Нарушена четность TK или ZPK/TPK<br>'10': Нарушена четность MK-SMI<br>'11': Нарушена четность MK-SMC<br>'23': Недопустимый код формата PIN-блока<br>'50': Недопустимый тип ключа шифрования исходного PIN-блока<br>'51': Нарушена четность MK-AC<br>'52': Некорректное значение параметра ветвления/высоты дерева<br>'68': Команда недоступна<br>'69': Формат PIN-блока недоступен<br>или другой стандартный код ошибки. |
| MAC | 8 B | Вычисленное значение MAC. |
| Длина повторно зашифрованного сообщения | 4 H | Присутствует только в случае *Флага режима* = '2' или '4'.<br>Длина (в байтах) следующего поля. |

| | | |
|---|---|---|
| Повторно зашифрованное сообщение | n B | Присутствует только в случае *Флага режима* = '2' или '4'. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [K2] — Проверка Truncated Application Cryptogram (Mastercard CAP)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Опционально (см. описание)** | |
| Активности: **diagnostic.host** | |

**Описание функции:** Проверка Truncated Application Cryptogram (Mastercard CAP).

**Примечания:** Команда поддерживает:

- EMV 4.1 methods A и B для выработки мастер-ключей карты
- EMV 3.1.1 и EMV 4.1 (включая EMV Common Session Key Derivation) для выработки сессионных ключей карты.

Эта команда совместима со спецификацией Visa DPA.

Для вывода диагностических данных требуется авторизованное состояние HSM.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'K2'. |
| Флаг режима | 1 H | '0': Проверка Truncated AC и проверка MAC |
| Идентификатор схемы | 2 N | '00': Mastercard CAP<br>'01': Mastercard CAP с TDS |
| Метод диверсификации мастер-ключа карты | 1 N | '0': EMV 4.1 Master Key Derivation Option A<br>'1': EMV 4.1 Master Key Derivation Option B |
| Метод диверсификации сессионного ключа карты | 1 N | '0': Сессионный ключ не диверсифицируется<br>'1': Mastercard (M/Chip 2.1 Method)<br>'2': EMV 4.1 (EMV2000) Method<br>'3': EMV 4.1 (EMV Common Session Key Derivation Method) |
| MK-AC | | Мастер-ключ эмитента для формирования и проверки Application Cryptogram. |
| | 'U' + 32 H | MK-AC, зашифрованный под LMK 28-29/1. |
| | 'S' + n A | MK-AC должен соответствовать следующему формату:<br>Использование ключа: 'E0'; Алгоритм: 'T'; Режим использования: 'X', 'N' |
| IV-AC | 16 B | Присутствует только в случае *Метода диверсификации сессионного ключа карты* = '2'. IV для метода диверсификации сессионного ключа EMV2000. |
| Длина номера карты (PAN) | 2 N | Присутствует только в случае *Метода диверсификации сессионного ключа карты* = '1'. Длина (в байтах) следующего поля. Допустимые значения: '01' .. '99'. |

| | | |
|---|---|---|
| Номер карты (PAN)/PAN Sequence Number | 8 B или n B | В случае *Метода диверсификации мастер-ключа карты* = '0' это поле имеет фиксированную длину 8 байтов и содержит предварительно отформатированный PAN/PSN (в BCD формате).<br>*Примечание:* PAN/PSN должен быть дополнен до 8 байтов (согласно EMV Option A).<br>В случае *Метода диверсификации мастер-ключа карты* = '1' поле содержит PAN/PSN (в BCD формате).<br>*Примечание:* Поле должно содержать четное число символов (следовательно, целое число байтов), при необходимости дополненное слева '0').<br>*Примечание:* Если *Длина PAN* < 8 байт, то HSM дополнит поле до 8 байтов, если это необходимо, в соответствии с EMV Option A. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае*Метода диверсификации мастер-ключа карты* = '1'. |
| Параметры ветвления/высоты дерева | 1 N | Присутствует только в случае *Метода диверсификации сессионного ключа карты* = '2'.<br>'0': коэффициент ветвления 2; высота дерева 16<br>'1': коэффициент ветвления 4; высота дерева 8 |
| ATC | 2 B | Значение ATC, полученное хостом на основе следующей информации:<br>ATC последней транзакции, сохраненной в БД хоста;<br>ATC, предоставленный картой в сообщении SecureCode. |
| UN | 4 B | Unpredictable Number. Присутствует только в случае *Метода диверсификации сессионного ключа карты* = '1'. |
| Длина данных транзакции | 2 H | Допустимые значения: '01' .. 'FF'. |
| Данные транзакции | n B | Данные переменной длины. Если длина данных кратна 8 байтам, дополнение не требуется; в противном случае данные дополняются нулями.<br>*Примечание:* За применение альтернативных методов дополнения (при необходимости) отвечает хост. |
| Разделитель | 1 A | Значение ';'. |
| Truncated AC | 8 B | Криптограмма для проверки. Поле содержит усеченную EMV-криптограмму из сообщения SecureCode. Поле должно быть выравнено по правому краю и при необходимости дополнено слева нулями до 8 байт. HSM генерирует криптограмму из подаваемых на вход данных транзакции, усекает ее с использованием указанного IPB и сравнивает со значением в данном поле. |
| IPB | 8 B | Битовая маска эмитента. |
| IPB MAC | 4 B | MAC, сгенерированный с помощью консольной команды MI. Данный MAC защищает от неавторизованных действий с IPB. |
| Длина данных TDS | 4 N | Присутствует только в случае *Идентификатора схемы* = '01'. Допустимые значения: '0002' .. '9998'. |
| Данные TDS | n H | Присутствует только в случае *Идентификатора схемы* = '01'. Данные TDS.<br>*Примечание:* За корректность дополнения данных TDS (согласно EMV 4.x Book 2 Appendix A1.2) отвечает хост. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'K3'. |

| | | |
|---|---|---|
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки ARQC/TC/AAC<br>'04': Некорректное значение флага режима<br>'05': Некорректный идентификатор схемы<br>'10': Нарушена четность MK<br>'52': Некорректное значение параметра ветвления/высоты дерева<br>'82': Ошибка проверки IPB MAC<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Диагностические данные | 8 B | Truncated AC, сгенерированная HSM. Поле должно быть выравнено по правому краю и при необходимости дополнено слева нулями до 8 байт. Присутствует только в случае *Кода ошибки* = '01' и если HSM находится в авторизованном состоянии. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [KS] — Проверка Data Authentication Code (DAC) или Dynamic Number (DN) (EMV 3.1.1)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Авторизация: **Опционально (см. описание)** | |
| Активности: **diagnostic.host** | |

**Описание функции:** Проверка Data Authentication Code (DAC) или Dynamic Number (DN).

**Примечания:** Для вывода диагностических данных требуется авторизованное состояние HSM.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'KS'.</td></tr>
<tr><td>Флаг режима</td><td>1 H</td><td>'0': Проверка DAC<br>'1': Проверка DN</td></tr>
<tr><td>Идентификатор схемы</td><td>1 H</td><td>'1': Mastercard M/Chip</td></tr>
<tr><td>MK-DAC</td><td></td><td>Мастер-ключ эмитента для вычисления и проверки DAC. Присутствует только в случае Флага режима = '0'.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>MK-DAC, зашифрованный под LMK 28-29/4.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK-DAC должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E3'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>MK-DN</td><td></td><td>Мастер-ключ эмитента для вычисления и проверки DN. Присутствует только в случае Флага режима = '1'.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>MK-DN, зашифрованный под LMK 28-29/5.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK-DN должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E4'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Номер карты (PAN)/PAN Sequence Number</td><td>8 B</td><td>Предварительно отформатированный PAN/PSN. Присутствует в обоих режимах '0' и '1'.</td></tr>
<tr><td>DAC</td><td>2 B</td><td>DAC для проверки. Присутствует только в случае Флага режима = '0'.</td></tr>
<tr><td>DN</td><td>2 B</td><td>DN для проверки. Присутствует только в случае Флага режима = '1'.</td></tr>
<tr><td>ATC</td><td>2 B</td><td>Счетчик транзакций. Присутствует только в случае Флага режима = '1'.</td></tr>
<tr><td>UN</td><td>4 B</td><td>Unpredictable Number. Присутствует только в случае Флага режима = '1'.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KT'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки DAC или DN<br>'04': Некорректное значение флага режима<br>'05': Некорректный идентификатор схемы<br>'10': Нарушена четность МК<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Диагностические данные | 2 B | Вычисленное значение DAC или DN (в зависимости от выбранного режима). Присутствует только в случае *Кода ошибки* = '01' и если HSM находится в авторизованном состоянии. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [K0] — Расшифрование зашифрованных счетчиков (EMV 4.x)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Расшифрование и возврат значений счетчиков, которые эмитент может опционально включать в данные приложения эмитента.

**Примечания:** Эмитент может включать значения следующих оффлайн-счетчиков в данные приложения эмитента:

- Offline Cumulative Transaction Amount (OCTA) (6 байт);
- Offline Consecutive Transaction Number (OCTN) (1 байт).

Эти счетчики могут опционально включаться эмитентом в зашифрованном виде. Команда проверит данные зашифрованных счетчиков и вернет расшифрованные значения.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'K0' (K-ноль). |
| Метод диверсификации мастер-ключа карты | 1 N | '0': M/Chip 4 с использованием EMV 4.x ICC Master Key Derivation Option A и EMV2000 Session Key Derivation<br>'1': M/Chip 4 с использованием EMV 4.x ICC Master Key Derivation Option B и EMV2000 Session Key Derivation<br>'2': M/Chip 4 с использованием EMV 4.x ICC Master Key Derivation Option A и EMV Common Session Key Derivation<br>'3': M/Chip 4 с использованием EMV 4.x ICC Master Key Derivation Option B и EMV Common Session Key Derivation<br>'4': M/Chip 4 с использованием EMV 4.x ICC Master Key Derivation Option A и M/Chip 2.1 Proprietary Session Key Derivation<br>'5': M/Chip 4 с использованием EMV 4.x ICC Master Key Derivation Option B и M/Chip 2.1 Proprietary Session Key Derivation |
| MK-AC | | Мастер-ключ эмитента для формирования и проверки Application Cryptogram. |
| | 'U' + 32 H | MK-AC, зашифрованный под LMK 28-29/1. |
| | 'S' + n A | MK-AC должен соответствовать следующему формату:<br>Использование ключа: 'E0'; Алгоритм: 'T'; Режим использования: 'X', 'N' |
| IV-AC | 16 B | Присутствует только в случае *Метода диверсификации мастер-ключа карты* = '0' или '1'. Вектор инициализации для диверсификации сессионного ключа EMV2000 Application Cryptogram. |
| Длина номера карты (PAN) | 2 N | Присутствует только в случае *Метода диверсификации мастер-ключа карты* = '1', '3' или '5'. Длина (в байтах) следующего поля. Допустимые значения: '01' .. '99'.<br>*Примечание:* Поле содержит количество байтов, необходимых для хранения значения PAN/PSN. Если значение PAN/PSN содержит нечетное количество символов, необходимо дополнить его слева '0'. |

| | | |
|---|---|---|
| Номер карты (PAN)/PAN Sequence Number | 8 B или n B | В случае *Метода диверсификации мастер-ключа карты* = '0', '2' или '4' это поле имеет фиксированную длину 8 байтов и содержит предварительно отформатированный PAN/PSN (в BCD формате).<br>*Примечание:* PAN/PSN должен быть дополнен до 8 байтов (согласно EMV Option A).<br><br>В случае *Метода диверсификации мастер-ключа карты* = '1', '3' или '5' поле содержит PAN/PSN (в BCD формате). Длина поля определяется значением поля *Длина номера карты (PAN)*.<br>*Примечание:* Поле должно содержать четное количество символов (следовательно, целое число байтов), при необходимости дополненное слева '0'. PAN/PSN затем используется согласно EMV Option B.<br>*Примечание:* Если *Длина номера карты (PAN)* < 8 байт, то HSM дополнит поле до 8 байтов, если это необходимо, в соответствии с EMV Option A. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Метода диверсификации мастер-ключа карты* = '1', '3' или '5'. Признак конца поля *Номер карты (PAN)/PAN Sequence Number*. |
| Параметры ветвления/высоты дерева | 1 N | Присутствует только в случае *Метода диверсификации мастер-ключа карты* = '0' или '2'.<br>'0': коэффициент ветвления 2; высота дерева 16<br>'1': коэффициент ветвления 4; высота дерева 8 |
| UN | 4 B | Unpredictable Number. Присутствует только в случае *Метода диверсификации мастер-ключа карты* = '4' или '5'. |
| ATC | 2 B | Значение ATC, полученное от карты. Используется для генерации сессионного ключа. |
| Зашифрованные счетчики | 8 B | Зашифрованные данные счетчиков, содержащие значения OCTA и OCTN. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'K1'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки зашифрованного счетчика<br>'05': Некорректный метод диверсификации ключа<br>'10': Нарушена четность MK<br>'52': Некорректное значение параметра ветвления/высоты дерева<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| OCTA | 6 B | Расшифрованное значение счетчика Offline Cumulated Transaction Amount. |
| OCTN | 1 B | Расшифрованное значение счетчика Offline Consecutive Transaction Number. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 22 Команды подготовки данных для бесконтактных карт

Следующая команда хоста используется для генерации данных, необходимых для эмиссии бесконтактных карт:

| | |
|---|---|
| [NY] — Генерация IVCVC3 и статического CVC3 | 360 |

## [NY] — Генерация IVCVC3 и статического CVC3

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация IVCVC3 и CVC3 или PINIVCVC3 и PINCVC3.

**Примечания:** При использовании технологии Mastercard PayPass для персонализации карты требуется значение IVCVC3. Для вычисления статического CVC3 требуется IVCVC3, который представляет собой значение MAC, вычисленное для статической части Track1 или Track2 с использованием DK-CVC3. Команда вычисляет IVCVC3 и CVC3 из переданных в команде данных Track1 или Track2.

При использовании технологии MasterCard Mobile PayPass для вычисления значения PINCVC3 требуется значение PINIVCVC3. Согласно спецификации Mastercard Mobile PayPass M/Chip:

*PINIVCVC3 — проприетарные статические данные эмитента, используемые для генерации криптограммы CVC3 в случае поддержки считывателем расширений Mobile и при условии успешной оффлайн-проверки PIN.*
*Вектор инициализации PIN (PINIVCVC3) = вектор инициализации (IVCVC3) XOR '9559'.*

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'NY'.</td></tr>
<tr><td>Идентификатор схемы</td><td>1 N</td><td>'1': Mastercard PayPass (IVCVC3 и CVC3)<br>'2': Mastercard PayPass (PINIVCVC3 и PINCVC3)</td></tr>
<tr><td>MK-CVC3</td><td></td><td>Мастер-ключ эмитента для вычисления CVC3.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>MK-CVC3, зашифрованный под LMK 28-29/7.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK-CVC3 должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E0', 'E6', '32'</td><td>'T'</td><td>'X', 'N'</td></tr>
</table></td></tr>
<tr><td>Метод диверсификации ключа</td><td>1 A</td><td>'A': EMV 4.1 Book 2 Option A<br>'B': EMV 4.1 Book 2 Option B</td></tr>
<tr><td>Данные для диверсификации</td><td>n N</td><td>Конкатенация PAN и 2-значного PAN Sequence Number. Длина PAN 8-19 цифр.<br>Если PAN Sequence Number не определен, используется значение '00'.<br>Примечание: если длина PAN ≤ 16 цифр, применяется метод EMV Option A и HSM при необходимости дополнит значение до 16 цифр соответствующим образом.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td>Длина Track</td><td>3 N</td><td>Длина следующего поля.</td></tr>
<tr><td>Track</td><td>n B</td><td>Статические данные Track1 или Track2.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'.</td></tr>
<tr><td>UN</td><td>8 N</td><td>Случайное число, которое генерируется терминалом и передается карте во время PayPass транзакции.</td></tr>
<tr><td>ATC</td><td>5 N</td><td>Счетчик транзакций. Максимальное значение: 65535 (2 байта).</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
</table>

| | | |
|---|---|---|
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'NZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Недопустимый метод диверсификации ключа<br>'05': Недопустимый идентификатор схемы<br>'10': Нарушена четность MK-CVC3<br>'EA': Ошибка Key Block MK-CVC3<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае Кода ошибки = 'EA': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| IVCVC3/PINIVCVC3 | 5 N | Вычисленное значение IVCVC3 или PINIVCVC3. |
| Статический CVC3/PINCVC3 | 5 N | Вычисленное значение CVC3 или PINCVC3.<br>Если требуется 3- или 4-значный CVC3/PINCVC3, приложение может обрезать возвращаемое значение. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 23 Команды подготовки данных для карт EMV

Следующие команды хоста используются для поддержки генерации данных, требуемых для карт EMV:

## [KE] — Генерация ключевой пары RSA и сертификата открытого ключа эмитента

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|
| Variant LMK | Авторизация: **Требуется**<br>Активности: **generate.rsa.host** |
| Key Block LMK | Авторизация: **Требуется**<br>Активности: **generate.03.host** |

**Описание функции:** Генерация пары ключей RSA эмитента и возврат хосту самоподписанного сертификата открытого ключа эмитента в формате, соответствующем идентификатору схемы, указанному в команде. Также возможна генерация самоподписанного сертификата с использованием ранее сгенерированной ключевой пары; в этом случае проверяется соответствие закрытого и открытого ключей друг другу.

**Примечания:** Для закрытого ключа эмитента будет установлен тип ключа 2 (Подпись и Управление ключами). По умолчанию используется открытая экспонента 65537 ($2^{16} + 1$). В случае указания открытой экспоненты в команде допустимы значения 3 или 65537; в противном случае HSM вернет ошибку и команда не будет обработана.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'KE'. |
| Идентификатор схемы | 1 N | '0': Visa VSDC<br>'1': Mastercard<br>'2': American Express AEIPS V4.1<br>'3': JCB<br>'4': Union Pay |
| Флаг режима | 1 N | '0': Генерация ключевой пары и сертификата эмитента с использованием сильных простых чисел<br>'1': Генерация только сертификата (на основе ранее сгенерированной ключевой пары)<br>'2': Генерация ключевой пары и сертификата эмитента |
| Идентификатор алгоритма хэширования | 2 N | '01': SHA-1 |
| Идентификатор алгоритма подписи | 2 N | '01': RSA |
| Следующие 5 полей присутствуют только в случае *Флага режима* = '0' или '2' (генерация ключевой пары и сертификата): | | |
| Длина ключа | 4 N | Длина модуля в битах (должна быть кратна 8); минимальное значение = 0400, максимальное значение = 2040. |
| Данные для аутентификации | n B | Опционально. Дополнительные данные для вычисления MAC открытого ключа эмитента (не должны содержать символ ';'). |
| Разделитель | 1 A | Значение ';'. Обязательное поле. |
| Длина открытой экспоненты | 4 N | Опционально. Длина открытой экспоненты в битах. Присутствует, если присутствует следующее поле. |

| | | |
|---|---|---|
| Открытая экспонента | n B | Опционально. Должна соответствовать ограничениям, указанным в примечании к команде. Если поле отсутствует, используется экспонента по умолчанию 65537. |
| Следующие 4 поля присутствуют только в случае *Флага режима* = '1' (генерация только сертификата): | | |
| Длина закрытого ключа эмитента | 4 N | Длина закрытого ключа эмитента в байтах. |
| | 4 H | Значение 'FFFF'. |
| Закрытый ключ эмитента | n B | Закрытый ключ эмитента, зашифрованный под LMK 34-35. |
| | 'S' + n B | Закрытый ключ эмитента должен соответствовать следующему формату:<br>Использование ключа: '03'; Алгоритм: 'R'; Режим использования: 'S', 'D', 'N' |
| Разделитель | 1 A | Значение ';'. Обязательное поле. |
| Открытый ключ эмитента | n B | Открытый ключ эмитента (DER, беззнаковый) в формате ASN.1 (последовательность модуля и экспоненты). |
| Разделитель | 1 A | Значение ';'. Обязательное поле. |
| Идентификатор эмитента (BIN) | 8 H | Крайние левые 3-8 цифр PAN, дополненные справа 0xF. |
| Дата окончания срока действия сертификата | 4 N | Дата окончания срока действия сертификата (ММГГ). |
| Следующие 2 поля присутствуют в случае *Идентификатора схемы* = '0' (Visa VSDC), '2' (American Express AEIPS V4.1) или '4' (Union Pay) и содержат данные для включения в самоподписанный сертификат (см. Прил. B): | | |
| Идентификатор сервиса | 8 H | Идентификатор сервиса Visa/American Express/Union Pay, при необходимости дополненный справа 0x0. |
| Tracking Number | 6 N | Уникальный номер (Tracking Number) в соответствии с используемой схемой. |
| Следующие 2 поля присутствуют в случае *Идентификатора схемы* = '1' (Mastercard) или '3' (JCB) и содержат данные для включения в самоподписанный сертификат (см. Прил. B): | | |
| Серийный номер сертификата | 6 H | Уникальный номер сертификата. |
| Индекс открытого ключа эмитента | 6 H | Уникальный идентификатор открытого ключа эмитента. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующие поля присутствуют только в случае Key Block LMK: | | |
| Разделитель | 1 A | Значение '&'. Опционально, может присутствовать только в случае генерации экспортируемого ключа; если присутствует, то следующее поле обязательно. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block (байт 11) в случае экспортируемого ключа.<br>Допустимые значения: 'N' или 'S'. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KF'. |

<table>
<tr><td>Код ошибки</td><td>2 H</td><td>'00': Без ошибок<br>'05': Некорректный идентификатор схемы или флаг режима<br>'06': Некорректный идентификатор алгоритма хэширования или подписи или другой стандартный код ошибки.<br><br>Только для Флага режима = '0' или '2':<br>'03': Некорректная длина ключа<br>'07': Некорректная длина открытой экспоненты<br>'08': Недопустимое значение открытой экспоненты<br><br>Только для Флага режима = '1':<br>'02': Открытый ключ не соответствует правилам кодирования<br>'09': Некорректная пара открытый/закрытый ключ<br>'E8': Некорректный Key Block закрытого ключа<br>'E9': Некорректный Key Block открытого ключа</td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Кода ошибки = 'E8' или 'E9':</td></tr>
<tr><td>Дополнительный код ошибки</td><td>2 H</td><td>Дополнительный код ошибки Key Block.</td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае Флага режима = '0' или '2' (генерация ключевой пары и сертификата):</td></tr>
<tr><td>MAC</td><td>4 B</td><td>Присутствует только в случае Variant LMK. Значение MAC для открытого ключа эмитента и данных аутентификации, вычисленное с использованием LMK 36-37.</td></tr>
<tr><td>Открытый ключ эмитента</td><td>n B</td><td>Открытый ключ эмитента (DER, беззнаковый) в формате ASN.1 (последовательность модуля и экспоненты).</td></tr>
<tr><td></td><td>'S' + n B</td><td>Открытый ключ эмитента должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'02'</td><td>'R'</td><td>'V'</td></tr></table></td></tr>
<tr><td>Длина закрытого ключа эмитента</td><td>4 N</td><td>Присутствует только в случае Variant LMK. Длина закрытого ключа эмитента в байтах.</td></tr>
<tr><td>Закрытый ключ эмитента</td><td>n B</td><td>Закрытый ключ эмитента, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B</td><td>Закрытый ключ эмитента должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'03'</td><td>'R'</td><td>'S'</td></tr></table></td></tr>
<tr><td>Длина сертификата</td><td>4 N</td><td>Длина самоподписанного сертификата в байтах.</td></tr>
<tr><td>Самоподписанный сертификат открытого ключа эмитента</td><td>n B</td><td>Самоподписанный сертификат открытого ключа эмитента, формат сертификата зависит от используемой схемы (см. Прил. B).</td></tr>
<tr><td>Длина хэш-значения</td><td>2 N</td><td>Длина (количество шестнадцатиричных символов) результата хэш-функции в следующем поле; зависит от алгоритма хэширования, определенного в команде. Для алгоритма SHA-1 значение '40'.</td></tr>
<tr><td>Хэш-значение</td><td>n H</td><td>Значение хэш-функции для данных самоподписанного сертификата открытого ключа, в соответствии с используемой схемой.</td></tr>
<tr><td>Символ конца ответа</td><td>1 C</td><td>Значение 0x19. Присутствует, только если присутствует в команде.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Присутствует, только если присутствует в команде. Максимальная длина — 32 символа.</td></tr>
</table>

## [KG] — Проверка сертификата открытого ключа эмитента

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Проверка сертификата открытого ключа эмитента, полученного от УЦ, и возврат хосту открытого ключа с соответствующим MAC. Опционально проверяется соответствие открытого ключа из сертификата закрытому ключу.

**Примечания:** Файл сертификата открытого ключа эмитента состоит из открытых неподписанных данных, подписанных данных сертификата открытого ключа и, опционально (для схем American Express, Visa и Union Pay), отсоединенной подписи.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce minimum key strength of 1024-bits for RSA signature verification` (влияет на параметры: *Закрытый ключ эмитента*) | `Yes [Y]` | Длина закрытого ключа (RSA) должна быть не менее 1024 бит. |
| | `No [N]` | Ограничения на длину ключа не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| | | **КОМАНДА** |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'KG'. |
| Идентификатор схемы | 1 N | '0': Visa VSDC<br>'1': Mastercard<br>'2': American Express AEIPS V4.1<br>'3': JCB<br>'4': Union Pay |
| MAC открытого ключа УЦ | 4 B | Значение MAC для открытого ключа УЦ и данных аутентификации, вычисленное с использованием LMK 36-37. |
| Открытый ключ УЦ | | Открытый ключ УЦ под LMK. |
| | n B | Открытый ключ УЦ (DER, беззнаковый) в формате ASN.1 (последовательность модуля и экспоненты). |
| | 'S' + n B | Открытый ключ УЦ должен соответствовать следующему формату:<br>Использование ключа: '02'; Алгоритм: 'R'; Режим использования: 'N', 'V' |
| Данные для аутентификации УЦ | n B | Опционально. Дополнительные данные для вычисления MAC открытого ключа УЦ (не должны содержать символ ';'). |
| Разделитель | 1 A | Значение ';'. Обязательное поле. |
| Длина сертификата | 4 N | Длина сертификата эмитента в байтах. |
| Сертификат эмитента | n B | Сертификат эмитента, формат сертификата зависит от используемой схемы (см. Прил. B). В случае *Идентификатора схемы* = '0', '2' или '4' может включать отсоединенную подпись. |
| Разделитель | 1 A | Значение ';'. Обязательное поле. |

| | | |
|---|---|---|
| Данные для аутентификации эмитента | n B | Опционально. Дополнительные данные для вычисления MAC открытого ключа эмитента (не должны содержать символ ';'). |
| Разделитель | 1 A | Значение ';'. Обязательное поле. |
| Длина закрытого ключа эмитента | | Опционально, присутствует только в случае наличия закрытого ключа эмитента. |
| | 4 N | Длина закрытого ключа эмитента в байтах. |
| | 4 H | Значение 'FFFF'. |
| Закрытый ключ эмитента | | Опционально, присутствует только в случае наличия закрытого ключа эмитента. |
| | n B | Закрытый ключ эмитента, зашифрованный под LMK 34-35. |
| | 'S' + n B | Закрытый ключ эмитента должен соответствовать следующему формату:<br>Использование ключа: '03'; Алгоритм: 'R'; Режим использования: 'S', 'D', 'N' |
| Разделитель | 1 A | Значение ';'. Обязательное поле. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'05': Некорректный идентификатор схемы<br>'06': Некорректный идентификатор алгоритма хэширования<br>'07': Ошибка проверки хэш-значения сертификата<br>'08': Открытый ключ УЦ не соответствует правилам кодирования<br>'09': Недопустимая пара открытый ключ/закрытый ключ<br>'76': Некорректная длина открытого ключа<br>'78': Некорректная длина закрытого ключа<br>'80': Некорректная длина сертификата<br>'81': Некорректный формат сертификата<br>'E8': Некорректный Key Block закрытого ключа<br>'E9': Некорректный Key Block открытого ключа<br>или другой стандартный код ошибки.<br><br>Только для *Идентификатора схемы* = '0', '2' или '4':<br>'52': Некорректный заголовок расширения сертификата<br>'53': Некорректный формат отсоединенной подписи<br>'54': Некорректная длина отсоединенной подписи<br>'55': Некорректная отсоединенная подпись |
| Следующее поле присутствует только в случае *Кода ошибки* = 'E8' или 'E9': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| MAC | 4 B | Значение MAC для открытого ключа эмитента и данных аутентификации, вычисленное с использованием LMK 36-37. |

<table>
<tr><td>Открытый ключ эмитента</td><td>n B</td><td>Открытый ключ эмитента (DER, беззнаковый) в формате ASN.1 (последовательность модуля и экспоненты).</td></tr>
<tr><td></td><td>'S' + n B</td><td>Открытый ключ эмитента должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'02'</td><td>'R'</td><td>'E'</td></tr></table></td></tr>
<tr><td>Длина хэш-значения</td><td>2 N</td><td>Длина (количество шестнадцатиричных символов) результата хэш-функции в следующем поле; зависит от алгоритма хэширования, определенного в сертификате.</td></tr>
<tr><td>Хэш-значение</td><td>n H</td><td>Значение хэш-функции, вычисляемое для проверки открытого ключа эмитента.</td></tr>
<tr><td>Идентификатор эмитента</td><td>8 H</td><td>Идентификатор эмитента из сертификата открытого ключа эмитента.</td></tr>
<tr><td>Дата окончания срока действия сертификата</td><td>4 N</td><td>Дата окончания срока действия сертификата (ММГГ) из сертификата открытого ключа эмитента.</td></tr>
<tr><td>Серийный номер сертификата</td><td>6 H</td><td>Серийный номер сертификата открытого ключа эмитента.</td></tr>
<tr><td colspan="3">Следующие 2 поля присутствуют, если Идентификатор схемы = '0', '2' или '4' (подробнее см. Прил. B):</td></tr>
<tr><td>Длина хэш-значения отсоединенной подписи</td><td>2 N</td><td>Длина (количество шестнадцатиричных символов) результата хэш-функции в следующем поле; зависит от алгоритма хэширования, определенного в отсоединенной подписи.<br>Если в сертификате отсутствует отсоединенная подпись, значение поля '00', а следующее поле отсутствует.</td></tr>
<tr><td>Хэш-значение отсоединенной подписи</td><td>n H</td><td>Значение хэш-функции в отсоединенной подписи сертификата эмитента.</td></tr>
<tr><td>Символ конца ответа</td><td>1 C</td><td>Значение 0x19. Присутствует, только если присутствует в команде.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Присутствует, только если присутствует в команде. Максимальная длина — 32 символа.</td></tr>
</table>

## [KM] — Генерация подписи для аутентификации по статическим данным

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация подписи данных карты с использованием закрытого ключа эмитента.

**Примечания:** Поддерживается автоматическая генерация DAC (для схем Mastercard).

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'KM'.</td></tr>
<tr><td>Идентификатор алгоритма хэширования</td><td>2 N</td><td>'01': SHA-1</td></tr>
<tr><td>DAC</td><td>2 B</td><td>Код аутентификации (Data Authentication Code). Значение указывается всегда, но оно игнорируется в случае вычисления DAC (если указаны параметры MK<sub>DAC</sub> и Номера карты (PAN)/PAN Sequence Number).</td></tr>
<tr><td>Длина данных</td><td>4 N</td><td>Длина статических данных, используемых для аутентификации.</td></tr>
<tr><td>Данные для аутентификации</td><td>n B</td><td>Статические данные для аутентификации.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Обязательное поле.</td></tr>
<tr><td>Флаг закрытого ключа эмитента</td><td>2 N</td><td>Указывает расположение закрытого ключа эмитента. Если флаг = '99', используется ключ, переданный в команде; другое значение флага = индекс ключа.</td></tr>
<tr><td>Длина закрытого ключа эмитента</td><td></td><td>Присутствует только в случае Флага закрытого ключа эмитента = '99'.</td></tr>
<tr><td></td><td>4 N</td><td>Длина в байтах поля Закрытый ключ эмитента.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
<tr><td>Закрытый ключ эмитента</td><td></td><td>Присутствует только в случае Флага закрытого ключа эмитента = '99'.</td></tr>
<tr><td></td><td>n B</td><td>Закрытый ключ эмитента, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B</td><td>Закрытый ключ эмитента должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03'</td><td>'R'</td><td>'S', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Опционально; если присутствует, то следующие 2 поля обязательны (необходимы для вычисления DAC).</td></tr>
<tr><td colspan="3">Следующие 2 поля присутствуют, если присутствует разделитель выше:</td></tr>
<tr><td>MK<sub>DAC</sub></td><td></td><td>Мастер-ключ эмитента для вычисления DAC.</td></tr>
<tr><td></td><td>32 H или 'U' + 32 H</td><td>MK<sub>DAC</sub>, зашифрованный под LMK 28-29/4.</td></tr>
<tr><td></td><td>'S' + n A</td><td>MK<sub>DAC</sub> должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'E3'</td><td>'T'</td><td>'B', 'X', 'N'</td></tr>
</table></td></tr>
</table>

| | | |
|---|---|---|
| Номер карты (PAN)/PAN Sequence Number | 16 N | Конкатенация PAN (14 правых цифр) и двузначного PSN. При необходимости может быть дополнено нулями слева. При отсутствии значения PSN берется значение '00'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KN'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Некорректное значение флага закрытого ключа эмитента<br>'06': Некорректный идентификатор алгоритма хэширования<br>'10': Нарушена четность $MK_{DAC}$<br>'E8': Некорректный Key Block закрытого ключа эмитента<br>'E9': Некорректный Key Block $MK_{DAC}$<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'E8' или 'E9': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [KO] — Генерация ключевой пары RSA и сертификата открытого ключа карты

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация пары ключей RSA и выпуск запрашиваемого сертификата открытого ключа карты, подписанного закрытым ключом эмитента. Также возможно формирование сертификата с использованием открытого ключа, сгенерированного ранее, и экспорт соответствующего закрытого ключа в указанном формате; в этом случае проверяется соответствие закрытого и открытого ключей друг другу. Тип ключа для закрытого ключа карты должен быть равен 3 (ICC).

**Примечания:** По умолчанию используется открытая экспонента 65537 ($2^{16} + 1$). В случае указания открытой экспоненты в команде допустимы значения 3 или 65537; в противном случае HSM вернет ошибку и команда не будет обработана. Прил. Г содержит описание форматов кодировки закрытых ключей.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'KO'. |
| Идентификатор схемы | 1 N | '0': Visa VSDC<br>'1': Mastercard<br>'2': American Express AEIPS V4.1<br>'3': JCB<br>'4': Union Pay |
| Тип сертификата | 1 N | '0': Сертификат открытого ключа карты<br>'1': Сертификат открытого ключа для шифрования PIN карты |
| Флаг режима | 1 N | '0': Генерация ключевой пары и сертификата с использованием сильных простых чисел<br>'1': Генерация только сертификата (на основе переданного открытого ключа) и экспорт переданного закрытого ключа под KEK в указанном формате<br>'2': Генерация ключевой пары и сертификата |
| Флаг типа ключа | 1 N | '0': Ключи q > p<br>'2': Ключи p > q<br>*Примечание:* Для передаваемых в команде ключей, сгенерированных ранее, производится проверка соответствия типа ключа указанному и, в случае несоответствия, модификация параметров ключа для удовлетворения данному условию. |
| Следующее поле присутствует только в случае *Флага режима* = '0' или '2' (генерация ключевой пары и сертификата): | | |
| Длина ключа | 4 N | Длина модуля в битах (должна быть кратна 8); минимальное значение = 0400, максимальное значение = 2040. |
| Выходной формат закрытого ключа | 2 N | '03': 5 компонент CRT (Китайская теорема об остатках), зашифрованные в режиме CBC под KEK (см. Прил. Г)<br>'04': закрытая экспонента (d) и модуль (n), зашифрованные под KEK (см. Прил. Г)<br>'05': 5 компонент CRT, зашифрованные под KEK (формат 03) и закрытая экспонента (d) и модуль (n), зашифрованные под KEK (формат 04) |
| Разделитель | 1 A | Значение ';'. Опционально; если присутствует, то следующее поле обязательно. |

<table>
<tr><td>Режим выравнивания</td><td>1 N</td><td>Присутствует, если присутствует предыдущее поле.<br>'0': Дополнить байтами '00' блоки компонент CRT или модуля и закрытой экспоненты до длины, кратной 8 байт (для DES KEK) или 16 байт (для AES KEK).<br>Примечание: Режим по умолчанию для ключа в формате модуль/экспонента, если режим выравнивания не указан.<br>'1': Для DES KEK дополнить блоки компонент CRT или модуля и экспоненты 4 байтами (8000 0000) или 8 байтами (8000 0000 0000 0000) до длины, кратной 8 байт. Для AES KEK дополнить блоки компонент CRT или модуля и экспоненты 4 байтами (8000 0000) , 8 байтами (8000 0000 0000 0000), 12 байтами (8000 0000 0000 0000 0000 0000) или 16 байтами (8000 0000 0000 0000 0000 0000 0000 0000) до длины, кратной 16 байт.<br>Примечание: Режим используется только в случае использования соответствующих длин ключей.<br>'2': Дополнить обязательным байтом '80' и необходимым количеством байтов '00' блоки компонент CRT или модуля и экспоненты до длины, кратной 8 байт (для DES KEK) или 16 байт (для AES KEK).<br>Примечание: Режим по умолчанию для ключа в формате компонент CRT, если режим выравнивания не указан и блоки компонент CRT изначально не кратны 8 байт (для DES KEK) или 16 байт (для AES KEK).</td></tr>
<tr><td>KEK</td><td></td><td>Ключ шифрования ключа, используемый для зашифрования компонент закрытого ключа карты</td></tr>
<tr><td></td><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>KEK, зашифрованный под LMK 24-25/1.</td></tr>
<tr><td></td><td>'S' + n B</td><td>KEK должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'54'</td><td>'T', 'A'</td><td>'B', 'E', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае Выходного формата закрытого ключа = '04' или '05' (содержит модуль и экспоненту):</td></tr>
<tr><td>Режим шифрования</td><td>1 N</td><td>Режим шифрования модуля и экспоненты (в случае Выходного формата закрытого ключа = '05' также компонент CRT.)<br>'0': ECB<br>'1': CBC</td></tr>
<tr><td>IV</td><td>8 B<br>или<br>16 B</td><td>Вектор инициализации, присутствует только в случае Режима шифрования = '1'. Если алгоритм KEK = 'A', длина IV 16 байт, в противном случае 8 байт.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Опционально; если присутствует, то следующее поле обязательно.</td></tr>
<tr><td>Наличие поля длины модуля и закрытой экспоненты</td><td>1 N</td><td>Присутствует, только если присутствует предыдущее поле.<br>Примечание: Значение параметра не меняет формат полей зашифрованных закрытых модуля и экспоненты, а лишь указывает, предшествует ли зашифрованным данным значение длины. Если в команде отсутствует это и предыдущее поля, значение длины не будет добавлено в выходных данных.<br>'0': поле со значением длины не добавляется перед полями с зашифрованными закрытыми модулем и экспонентой в выходных данных (значение по умолчанию)<br>'1': поле со значением длины добавляется перед полями с зашифрованными закрытыми модулем и экспонентой в выходных данных</td></tr>
</table>

<table>
<tr><td>Число байтов для определения длины</td><td>1 N</td><td>Число байтов, используемых для указания длины незашифрованных компонент ключа (описание формата см. в Прил. Г). Допустимые значения: '0', '1', '2'. В случае значения '0' параметр длины не добавляется в выходные данные. В случае Выходного формата закрытого ключа = '03' (только компоненты CRT) используется значение '1'. Параметр применим для любых компонент ключа (компонент CRT, модуля и экспоненты).</td></tr>
<tr><td colspan="3">Следующие 3 поля присутствуют только в случае Флага режима = '0' или '2' (генерация ключевой пары и сертификата):</td></tr>
<tr><td>Длина открытой экспоненты</td><td>4 N</td><td>Опционально. Длина открытой экспоненты в битах. Присутствует, если присутствует следующее поле.</td></tr>
<tr><td>Открытая экспонента</td><td>n B</td><td>Опционально. Должна соответствовать ограничениям, указанным в примечании к команде. Если поле отсутствует, используется экспонента по умолчанию 65537.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Обязательное поле.</td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае Флага режима = '1' (генерация только сертификата):</td></tr>
<tr><td>Длина закрытого ключа карты</td><td>4 N</td><td>Длина закрытого ключа карты в байтах.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
<tr><td>Закрытый ключ карты</td><td>n B</td><td>Закрытый ключ карты, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B</td><td>Закрытый ключ карты должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'04'</td><td>'R'</td><td>'S', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Обязательное поле.</td></tr>
<tr><td>Открытый ключ карты</td><td>n B</td><td>Открытый ключ карты (DER, беззнаковый) в формате ASN.1 (последовательность модуля и экспоненты).</td></tr>
<tr><td>Идентификатор алгоритма хэширования</td><td>2 N</td><td>'01': SHA-1</td></tr>
<tr><td>Идентификатор алгоритма подписи</td><td>2 N</td><td>'01': RSA</td></tr>
<tr><td>Номер карты (PAN)</td><td>20 H</td><td>Значение номера карты (PAN) для включения в сертификат, выровненное по левому краю и дополненное при необходимости справа 0xF.</td></tr>
<tr><td>Дата окончания срока действия сертификата</td><td>4 N</td><td>Дата окончания срока действия сертификата (ММГГ) для включения в сертификат.</td></tr>
<tr><td>Серийный номер сертификата</td><td>6 H</td><td>Серийный номер сертификата для включения в сертификат.</td></tr>
<tr><td>Длина данных</td><td>3 N</td><td>Длина статических данных для аутентификации. Присутствует только в случае Типа сертификата = '0'.</td></tr>
<tr><td>Данные для аутентификации</td><td>n B</td><td>Статические данные для аутентификации. Присутствует только в случае Типа сертификата = '0'.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Обязательное поле.</td></tr>
<tr><td>Флаг закрытого ключа эмитента</td><td>2 N</td><td>Указывает расположение закрытого ключа эмитента. Если флаг = '99', используется ключ, переданный в команде; другое значение флага = индекс ключа.</td></tr>
<tr><td colspan="3">Следующие 2 поля присутствуют только в случае Флаг закрытого ключа эмитента = '99' (передача ключа в команде):</td></tr>
<tr><td>Длина закрытого ключа эмитента</td><td>4 N</td><td>Длина закрытого ключа эмитента в байтах.</td></tr>
<tr><td></td><td>4 H</td><td>Значение 'FFFF'.</td></tr>
</table>

<table>
<tr><td>Закрытый ключ эмитента</td><td>n B</td><td>Закрытый ключ эмитента, зашифрованный под LMK 34-35.</td></tr>
<tr><td></td><td>'S' + n B</td><td>Закрытый ключ эмитента должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'03'</td><td>'R'</td><td>'S', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KP'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Некорректный флаг закрытого ключа эмитента<br>'05': Некорректный идентификатор схемы, флаг режима или тип сертификата<br>'06': Некорректный идентификатор алгоритма хэширования или подписи<br>'09': Некорректное значение длины закрытых модуля и экспоненты<br>'10': Нарушена четность KEK<br>'51': Некорректный флаг типа ключа RSA<br>'52': Некорректный выходной формат закрытого ключа<br>'53': Некорректный режим шифрования<br>'54': Некорректный режим выравнивания<br>'58': Некорректное применение обязательного выравнивания (результат не кратен 8/16 байтам)<br>'60': Некорректное значение наличия поля длины закрытых модуля и экспоненты<br>'DA': Некорректный Key Block KEK<br>'ED': Некорректный Key Block закрытого ключа эмитента<br>или другой стандартный код ошибки.<br><br>Только для *Флага режима* = '0' или '2':<br>'03': Некорректная длина ключа<br>'07': Некорректная длина открытой экспоненты<br>'08': Недопустимое значение открытой экспоненты<br><br>Только для *Флага режима* = '1':<br>'02': Открытый ключ не соответствует правилам кодирования<br>'55': Некорректная длина закрытого ключа карты<br>'56': Некорректный закрытый ключ карты<br>'57': Некорректная пара открытый/закрытый ключ<br>'59': Тип закрытого ключа не равен 3 (ICC)<br>'E8': Некорректный Key Block закрытого ключа карты<br>'E9': Некорректный Key Block открытого ключа карты |
| Следующее поле присутствует только в случае *Кода ошибки* = 'DA', 'E8', 'E9' или 'ED': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующие 6 полей присутствуют только в случае *Выходного формата закрытого ключа* = '03' или '05' (содержит компоненты CRT): | | |

| | | |
|---|---|---|
| Длина компонент закрытого ключа карты | 1 B | Длина в байтах каждого из 5 следующих полей. |
| p (KEK) | n B | Простое число p, зашифрованное под KEK. |
| q (KEK) | n B | Простое число q, зашифрованное под KEK. |
| dp (KEK) | n B | Число dp = d mod (p-1), зашифрованное под KEK. |
| dq (KEK) | n B | Число dq = d mod (q-1), зашифрованное под KEK. |
| u (KEK) | n B | Число u = $q^{-1}$ mod p, зашифрованное под KEK. |
| Следующие 2 или 4 поля присутствуют только в случае *Выходного формата закрытого ключа* = '04' или '05' (содержит модуль и экспоненту): | | |
| Длина зашифрованной закрытой экспоненты | 2 B | Присутствует только если *Наличие поля длины закрытых модуля и экспоненты* = '1'. Длина зашифрованного блока закрытой экспоненты. |
| Экспонента закрытого ключа карты (KEK) | n B | Экспонента закрытого ключа карты, представленного в формате экспонента/модуль (см. Прил. Г), зашифрованная под KEK |
| Длина зашифрованного закрытого модуля | 2 B | Присутствует только если *Наличие поля длины закрытых модуля и экспоненты* = '1'. Длина зашифрованного блока закрытого модуля. |
| Модуль закрытого ключа карты | n B | Модуль закрытого ключа карты, представленного в формате экспонента/модуль (см. Прил. Г), зашифрованный под KEK |
| Длина сертификата карты (ICC) | 2 H | Длина в байтах сертификата карты в следующем поле. |
| Сертификат карты (ICC) | n B | Подписанный сертификат карты (формат см. в Прил. В). |
| Длина остатка открытого ключа карты (ICC) | 2 H | Длина в байтах остатка открытого ключа в следующем поле. Может быть 0, если $N_{IC} \leq N_I - 42$, где $N_I$ — длина модуля открытого ключа эмитента, $N_{IC}$ — длина модуля открытого ключа карты (ICC). |
| Остаток открытого ключа карты (ICC) | n B | Остаток открытого ключа карты. Присутствует, только если предыдущее поле содержит ненулевое значение. |
| Длина экспоненты открытого ключа карты (ICC) | 2 H | Длина в байтах экспоненты открытого ключа в следующем поле. |
| Экспонента открытого ключа карты (ICC) | n B | Экспонента открытого ключа карты. |
| Длина модуля открытого ключа карты (ICC) | 4 H | Длина в байтах модуля открытого ключа в следующем поле. |
| Модуль открытого ключа карты (ICC) | n B | Модуль открытого ключа карты. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [KK] — Импорт самоподписанного сертификата УЦ

| | Variant LMK ☑ | Key Block LMK ☑ |
|---|---|---|
| Variant LMK | Авторизация: **Требуется**<br>Активности: **import.rsa.host** | |
| Key Block LMK | | Авторизация: **Требуется**<br>Активности: **import.02.host** |

**Описание функции:** Проверка самоподписанного сертификата УЦ и возврат хосту открытого ключа УЦ с соответствующими MAC и датой окончания срока действия сертификата. Для схем Mastercard и JCB функция дополнительно возвращает серийный номер сертификата и значение хэш-функции для проверки переданного открытого ключа УЦ.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'KK'. |
| Идентификатор схемы | 1 N | '0': Visa VSDC<br>'1': Mastercard<br>'2': American Express AEIPS V4.1<br>'3': JCB<br>'4': Union Pay |
| Длина сертификата | 4 N | Длина самоподписанного сертификата УЦ в байтах. |
| Самоподписанный сертификат УЦ | n B | Самоподписанный сертификат УЦ, формат сертификата зависит от используемой схемы (см. Прил. B). |
| Разделитель | 1 A | Значение ';'. Обязательное поле. |
| Данные для аутентификации | n B | Опционально. Дополнительные данные для вычисления MAC открытого ключа УЦ (не должны содержать символ ';'). |
| Разделитель | 1 A | Значение ';'. Присутствует, только если присутствует предыдущее поле. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Следующие поля присутствуют только в случае Key Block LMK: | | |
| Разделитель | 1 A | Значение '#'. |
| Номер версии ключа | 2 N | Поле *Номер версии ключа*, включаемое в заголовок Key Block.<br>Допустимые значения: '00' .. '99'. |
| Экспортируемость | 1 A | Поле *Экспортируемость*, включаемое в заголовок Key Block.<br>Допустимые значения: 'N', 'E' или 'S'. |
| Количество опциональных блоков | 2 N | Количество опциональных блоков ниже. Должно присутствовать, если присутствует *Разделитель* выше.<br>Допустимые значения: '00' .. '08'. |
| Следующие 3 поля определяются для каждого опционального блока:<br>*Примечание:* Если *Количество опциональных блоков* = '00', следующие 3 поля не присутствуют. | | |
| Идентификатор блока | 2 A | Любое допустимое значение, кроме 'PB'. |

| | | |
|---|---|---|
| Длина блока | 2 H | Количество символов в блоке (включая идентификатор и длину блока).<br>Допустимые значения: 0x04 .. 0xFF.<br>Если значение 0x04, следующее поле отсутствует. |
| Данные блока | n A | Данные блока. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KL'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'05': Некорректный идентификатор схемы<br>'06': Некорректный идентификатор алгоритма хэширования или подписи<br>'07': Ошибка проверки хэш-значения сертификата<br>'08': Несоответствие исходных и подписанных данных сертификата<br>'80': Некорректная длина сертификата<br>'81': Некорректный формат сертификата<br>или другой стандартный код ошибки. |
| MAC | 4 B | Значение MAC для открытого ключа УЦ и данных аутентификации, вычисленное с использованием LMK 36-37. |
| Открытый ключ УЦ | | Открытый ключ УЦ под LMK. |
| | n B | Открытый ключ УЦ (DER, беззнаковый) в формате ASN.1 (последовательность модуля и экспоненты). |
| | 'S' + n B | Открытый ключ УЦ должен соответствовать следующему формату:<br>Использование ключа: '02'; Алгоритм: 'R'; Режим использования: 'V' |
| Дата окончания срока действия сертификата | 4 N | Дата окончания срока действия сертификата (ММГГ) из сертификата УЦ. |
| Следующие 3 поля присутствуют, если *Идентификатор схемы* = '1' или '3' (подробнее см. Прил. B): | | |
| Серийный номер сертификата | 6 H | Серийный номер сертификата УЦ. |
| Длина хэш-значения | 2 N | Длина (количество шестнадцатиричных символов) результата хэш-функции в следующем поле; зависит от алгоритма хэширования, определенного в сертификате. |
| Хэш-значение | n H | Значение хэш-функции, вычисляемое для проверки открытого ключа УЦ (включая идентификатор сертификата, индекс открытого ключа, модуль и экспоненту). |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [IK] — Подпись данных (EMV)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Генерация электронной подписи для сообщения с использованием закрытого ключа RSA в соответствии с EMV Book 2 и возврат хосту подписанного сообщения.

**Примечания:** К сообщению не применяется процедура дополнения. Его длина должна быть равна длине модуля используемого закрытого ключа, в противном случае будет возвращена ошибка.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'IK'. |
| Флаг режима | 1 N | '0': Без форматирования и выравнивания данных сообщения |
| Идентификатор алгоритма подписи | 2 N | '01': RSA |
| Длина сообщения | 4 N | Длина сообщения в байтах. |
| Данные сообщения | n B | Подписываемое сообщение. |
| Разделитель | 1 A | Значение ';'. Признак конца поля *Данные сообщения*. |
| Флаг закрытого ключа | 2 N | Указывает расположение закрытого ключа. Если флаг = '99', используется ключ, переданный в команде; другое значение флага = индекс ключа. |
| Следующие 2 поля присутствуют только в случае *Флага закрытого ключа* = '99': | | |
| Длина закрытого ключа | 4 N | Длина в байтах поля *Закрытый ключ*. |
| | 4 H | Значение 'FFFF'. |
| Закрытый ключ | n B | Закрытый ключ, зашифрованный под LMK 34-35. |
| | 'S' + n B | Закрытый ключ должен соответствовать следующему формату: |

| Использование ключа | Алгоритм | Режим использования |
|---|---|---|
| '03' | 'R' | 'S', 'N' |

| | | |
|---|---|---|
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'. Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'IL'. |

| | | |
|---|---|---|
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Некорректный флаг закрытого ключа<br>'05': Некорректный флаг режима<br>'06': Некорректный идентификатор алгоритма подписи<br>'27': Несоответствие длин закрытого ключа и сообщения<br>'D1': Некорректный Key Block закрытого ключа<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D1': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующие 2 поля присутствует только в случае *Кода ошибки* = '00': | | |
| Длина сообщения | 4 N | Длина подписанного сообщения в байтах. |
| Данные подписанного сообщения | n B | Подписанное сообщение. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [IM] — Восстановление данных (EMV)

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Восстановление данных сообщения из подписанного сообщения с использованием открытого ключа RSA в соответствии с EMV Book 2 и возврат хосту восстановленного сообщения.

**Примечания:** Для восстановленного сообщения не выполняются проверка или удаление дополнения.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'IM'. |
| Флаг режима | 1 N | '0': Без форматирования и выравнивания данных сообщения |
| Идентификатор алгоритма подписи | 2 N | '01': RSA |
| Длина сообщения | 4 N | Длина сообщения в байтах. |
| Данные сообщения | n B | Подписанное сообщение. |
| Разделитель | 1 A | Значение ';'. Признак конца поля *Данные сообщения*. |
| MAC открытого ключа | 4 B | Присутствует только в случае Variant LMK. Значение MAC для открытого ключа и данных аутентификации, вычисленное с использованием LMK 36-37. |
| Открытый ключ | n B | Открытый ключ (DER) в формате ASN.1 (последовательность модуля и экспоненты). |
| | 'S' + n B | Открытый ключ должен соответствовать следующему формату:<br>Использование ключа: '02'; Алгоритм: 'R'; Режим использования: 'V', 'N' |
| Данные для аутентификации | n B | Присутствует только в случае Variant LMK. Опционально; дополнительные данные для вычисления MAC открытого ключа (не должны содержать символ ';'). |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'IN'. |

| | | |
|---|---|---|
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки MAC<br>'04': Открытый ключ не соответствует правилам кодирования<br>'05': Некорректный флаг режима<br>'06': Некорректный идентификатор алгоритма подписи<br>'D2': Некорректный Key Block открытого ключа<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D2': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующие 2 поля присутствует только в случае *Кода ошибки* = '00': | | |
| Длина восстановленного сообщения | 4 N | Длина восстановленного сообщения в байтах. |
| Данные восстановленного сообщения | n B | Восстановленное сообщение. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 24 Команды персонализации чиповых карт

Следующие команды хоста используются для поддержки операций персонализации чиповых карт:

## [IC] — Установка безопасного соединения с чиповой картой

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Поддержка установки безопасного соединения с двусторонней аутентификацией с чиповой картой в соответствии с EMV Common Personalization Specification (CPS) и Global Platform (GP) Secure Channel Protocol 2 (SCP02) и Secure Channel Protocol 3 (SCP03).

Команда поддерживает следующие протоколы:

- Secure Channel Protocol 02 (SCP02) "i" = 0x15
- Secure Channel Protocol 02 (SCP02) "i" = 0x55
- Поддержка специального процесса для карт с магнитной полосой Mastercard PayPass
- Поддержка метода статической персонализации, при котором приложение карты персонализируется с помощью единственного PSK
- Secure Channel Protocol 03 (SCP03)

**Примечания:** В соответствии с EMV CPS и GP SCP02 существует 2 метода установки безопасного соединения с приложением карты для персонализации: Indirect (Explicit) Method и Direct (Implicit) Method.

Команда поддерживает только Indirect (Explicit) Method. В этом методе процессу подготовки данных не требуется обладать информацией о процессе, используемом для установки безопасного сеанса персонализации с картой. Таким образом, существует 2 зоны безопасности: зона безопасности между процессом подготовки данных и процессом персонализации и зона безопасности между процессом персонализации и картой.

Процесс персонализации устанавливает безопасный сеанс с картой с помощью команд INITIALISE UPDATE и EXTERNAL AUTHENTICATE. В рамках этого процесса генерируются сеансовые ключи и криптограммы, необходимые для установки безопасного сеанса с картой.

Команда использует ответы INITIALISE UPDATE для генерации данных для команды EXTERNAL AUTHENTICATE, а также для выработки ключей, необходимых для персонализации карты. Ключи возвращаются в зашифрованном под LMK виде для использования командой 'IE'. Команда поддерживает специальные параметры Global Platform для Уровня безопасности, включающего использование R-MAC. Если в команде определена опция, включающая использование R-MAC, ключ R-MAC также будет выработан и возвращен в зашифрованном под LMK виде. Этот ключ будет обрабатываться как «ZAK», чтобы сообщения от карты можно было проверить с помощью команды 'M8'.

Для метода Mastercard PayPass Magnetic Stripe команда вырабатывает только ключ персонализации KD, который используется для аутентификации сообщений, отправленных карте, и защиты конфиденциальных данных. Ключ возвращается в зашифрованном под LMK виде для использования командой 'IE'.

C-MAC — MAC команды APDU, вычисляемый хостом.

R-MAC — MAC ответа APDU, вычисляемый картой.

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">КОМАНДА</td></tr>
<tr><td>Заголовок команды</td><td>m A</td><td>Должен быть возвращен хосту без изменений.</td></tr>
<tr><td>Код команды</td><td>2 A</td><td>Значение 'IC'.</td></tr>
<tr><td>Метод установки безопасного соединения</td><td>1 N</td><td>'0': Indirect (Explicit) инициация защищенного канала системой персонализации, ключи карты вырабатываются из KMC (Global Platform SCP02 "i" = 0x15)<br>'1': Indirect (Explicit) инициация защищенного канала системой персонализации, ключи карты передаются в команде (Global Platform SCP02 "i" = 0x15)<br>'2': Mastercard PayPass Magnetic Stripe, ключ PERSO вырабатывается из KMC<br>'4': Indirect (Explicit) инициация защищенного канала системой персонализации, ключи карты вырабатываются из KMC (Global Platform SCP02 "i" = 0x55)<br>'5': Indirect (Explicit) инициация защищенного канала системой персонализации, ключи карты передаются в команде (Global Platform SCP02 "i" = 0x55)<br>'6': Indirect (Explicit) инициация защищенного канала Open Platform системой персонализации с использованием единственного ключа PSK (статическая аутентификация)<br>'7': Secure Channel Protocol 03 (SCP03)</td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Метода установки безопасного соединения = '6' или '7':</td></tr>
<tr><td>Режим генерации ключей карты</td><td>1 N</td><td>'0': Ключ(и) карты вырабатываются из мастер-ключа KMC (недоступно для Метода установки безопасного соединения = '7')<br>'1': Ключи карты передаются в команде</td></tr>
<tr><td colspan="3">Следующие 2 поля присутствуют только в случае Метода установки безопасного соединения = '0', '2', '4' или Метода установки безопасного соединения = '6' и Режима генерации ключей карты = '0':</td></tr>
<tr><td rowspan="3">KMC</td><td></td><td>Мастер-ключ персонализации.</td></tr>
<tr><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>KMC, зашифрованный под LMK 24-25/2.</td></tr>
<tr><td>'S' + n A</td><td>KMC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'E7'</td><td>'T'</td><td>'X', 'N'</td></tr></table></td></tr>
<tr><td>Данные для диверсификации</td><td>6 B<br><br>16 B</td><td>Данные для генерации статических диверсифицированных ключей карты.<br>В случае Метода установки безопасного соединения = '0' или '4' — 6 наименьших значащих байтов KEYDATA, обычно возвращаемых в ответ на команду INITIALISE UPDATE.<br>В случае Метода установки безопасного соединения = '6' — данные для диверсификации PSK.</td></tr>
<tr><td colspan="3">Следующие 3 поля присутствуют только в случае Метода установки безопасного соединения = '1' или '5':</td></tr>
<tr><td rowspan="3">CK-ENC</td><td></td><td>Ключ карты для генерации сеансового ключа шифрования.</td></tr>
<tr><td>'U' + 32 H</td><td>CK-ENC, зашифрованный под LMK 36-37/3.</td></tr>
<tr><td>'S' + n A</td><td>CK-ENC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'37'</td><td>'T'</td><td>'X', 'N'</td></tr></table></td></tr>
<tr><td rowspan="2">CK-MAC</td><td></td><td>Ключ карты для генерации сеансового ключа аутентификации.</td></tr>
<tr><td>'U' + 32 H</td><td>CK-MAC, зашифрованный под LMK 36-37/4.</td></tr>
</table>

<table>
<tr><td></td><td>'S' + n A</td><td>CK-MAC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'38'</td><td>'T'</td><td>'X', 'N'</td></tr></table></td></tr>
<tr><td>CK-DEK</td><td></td><td>Ключ карты для генерации сеансового ключа шифрования данных карты.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>CK-DEK, зашифрованный под LMK 36-37/5.</td></tr>
<tr><td></td><td>'S' + n A</td><td>CK-DEK должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'39'</td><td>'T'</td><td>'X', 'N'</td></tr></table></td></tr>
<tr><td colspan="3">Следующие 3 поля присутствуют только в случае Режима генерации ключей карты = '1':</td></tr>
<tr><td>PSK</td><td></td><td>Присутствует только в случае Метода установки безопасного соединения = '6'.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>PSK, зашифрованный под LMK 24-25/5.</td></tr>
<tr><td></td><td>'S' + n A</td><td>PSK должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'40'</td><td>'T'</td><td>'N'</td></tr></table></td></tr>
<tr><td>CK-ENC</td><td>'S' + n A</td><td>Присутствует только в случае Метода установки безопасного соединения = '7'. Ключ карты для криптограмм.<br>CK-ENC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'37'</td><td>'A'</td><td>'X'</td></tr></table></td></tr>
<tr><td>CK-MAC</td><td>'S' + n A</td><td>Присутствует только в случае Метода установки безопасного соединения = '7'. Ключ карты для аутентификации.<br>CK-MAC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'38'</td><td>'A'</td><td>'X'</td></tr></table></td></tr>
<tr><td>Ключевая схема (LMK)</td><td>1 A</td><td>Значение 'U'.</td></tr>
<tr><td colspan="3">Следующие 2 поля присутствуют только в случае Метода установки безопасного соединения = '0', '1', '4', '5', '6' (SCP02):</td></tr>
<tr><td>Host Challenge</td><td>8 B</td><td>Случайное число, сгенерированное системой персонализации и указанное в команде INITIALISE UPDATE, отправленной карте.</td></tr>
<tr><td>Sequence Counter</td><td>2 B</td><td>Значение счетчика, возвращаемое в ответ на команду INITIALISE UPDATE, отправленную карте, которое используется для диверсификации сессионных ключей карты.</td></tr>
<tr><td colspan="3">Следующие 3 поля присутствуют только в случае Метода установки безопасного соединения = '7' (SCP03):</td></tr>
<tr><td>Режим генерации Card Challenge</td><td>1 N</td><td>'0': случайный (Card Challenge и криптограмма передаются в команде)<br>'1': предиктивный (Card Challenge и криптограмма генерируются командой)</td></tr>
<tr><td>Host Challenge</td><td>8 B</td><td>Случайное число, сгенерированное системой персонализации.</td></tr>
<tr><td>Sequence Counter</td><td>3 B</td><td>Значение счетчика, возвращаемое в ответ на команду INITIALISE UPDATE, отправленную карте, которое используется для диверсификации сессионных ключей карты.</td></tr>
<tr><td colspan="3">Следующие 2 поля присутствуют только в случае Метода установки безопасного соединения = '0', '1' или '6' (SCP02 i='15'):</td></tr>
<tr><td>Card Challenge</td><td>6 B</td><td>Случайное число, сгенерированное картой в ответ на команду INITIALISE UPDATE.</td></tr>
</table>

| | | |
|---|---|---|
| Криптограмма карты | 8 B | Криптограмма, сгенерированная картой в ответ на команду INITIALISE UPDATE, которая используется хостом для аутентификации карты. |
| Следующие 2 поля присутствуют только в случае *Метода установки безопасного соединения* = '7' и *Режима генерации Card Challenge* = '0' (SCP03): | | |
| Card Challenge | 8 B | Случайное число, сгенерированное картой в ответ на команду INITIALISE UPDATE. |
| Криптограмма карты | 8 B | Криптограмма, сгенерированная картой в ответ на команду INITIALISE UPDATE, которая используется хостом для аутентификации карты. |
| Следующие 3 поля присутствуют только в случае *Метода установки безопасного соединения* = '4', '5' (SCP02 i='55') или *Метода установки безопасного соединения* = '7' и *Режима генерации Card Challenge* = '1': | | |
| Длина AID | 2 N | Длина следующего поля (должна быть четной). |
| AID | n H | Идентификатор приложения, который используется для генерации псевдослучайного значения Card Challenge. |
| Разделитель | 1 A | Значение ';'. |
| Следующие поля присутствуют только в случае *Метода установки безопасного соединения* = '0', '1', '4', '5', '6', '7': | | |
| Начальный заголовок APDU | 5 B | Начальный заголовок APDU для команды EXTERNAL AUTHENTICATE [CLA, INS, P1, P2, Lc]; как правило используется значение [0x80, 0x82, 0x00, 0x00, 0x10]. |
| Уровень безопасности | 1 B | Уровень безопасности, устанавливаемый для всех команд безопасного обмена сообщениями, вызываемых после команды EXTERNAL AUTHENTICATE.<br>В случае *Метода установки безопасного соединения* = '0', '1', '4', '5', '6' (SCP02) допустимые значения:<br>0x00: Без защиты обмена сообщениями<br>0x01: C-MAC<br>0x03: Шифрование и C-MAC<br>0x10: R-MAC<br>0x11: C-MAC и R-MAC<br>0x13: Шифрование, C-MAC и R-MAC<br>В случае *Метода установки безопасного соединения* = '7' (SCP03) допустимые значения:<br>0x00: Без защиты обмена сообщениями<br>0x01: C-MAC<br>0x03: Шифрование команды и C-MAC<br>0x11: C-MAC и R-MAC<br>0x13: Шифрование команды, C-MAC и R-MAC<br>0x33: Шифрование команды, C-MAC, R-MAC и шифрование ответа |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

<table>
<tr><th>Параметр</th><th>Формат</th><th>Описание</th></tr>
<tr><td colspan="3">ОТВЕТ</td></tr>
<tr><td>Заголовок ответа</td><td>m A</td><td>Заголовок команды, возвращаемый хосту без изменений.</td></tr>
<tr><td>Код ответа</td><td>2 A</td><td>Значение 'ID'.</td></tr>
<tr><td>Код ошибки</td><td>2 H</td><td>'00': Без ошибок<br>'05': Недопустимый метод установки безопасного соединения<br>'06': Недопустимый уровень безопасности<br>'07': Ошибка проверки криптограммы карты<br>'08': Нарушена четность CK-DEK<br>'09': Недопустимый режим генерации ключей карты<br>'10': Нарушена четность KMC, PSK или CK-MAC<br>'11': Нарушена четность CK-ENC<br>'37': Недопустимый режим генерации Card Challenge<br>'80': Ошибка длины AID<br>'E4': Ошибка Key Block KMC<br>'E5': Ошибка Key Block CK-ENC<br>'E6': Ошибка Key Block CK-MAC<br>'E7': Ошибка Key Block CK-DEK<br>'E8': Ошибка Key Block PSK<br>или другой стандартный код ошибки.</td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Кода ошибки = 'E4', 'E5', 'E6', 'E7' или 'E8':</td></tr>
<tr><td>Дополнительный код ошибки</td><td>2 H</td><td>Дополнительный код ошибки Key Block.</td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае Метода установки безопасного соединения = '0', '1', '4', '5' или '6' (SCP02):</td></tr>
<tr><td>Заголовок APDU</td><td>5 B</td><td>Заголовок APDU для команды EXTERNAL AUTHENTICATE [CLA, INS, P1, P2, Lc].</td></tr>
<tr><td>Криптограмма хоста</td><td>8 B</td><td>Криптограмма хоста для команды EXTERNAL AUTHENTICATE, используемая картой для аутентификации хоста.</td></tr>
<tr><td>Криптограмма карты</td><td>8 B</td><td>Присутствует только в случае Метода установки безопасного соединения = '4' или '5'.<br>Криптограмма, сгенерированная картой, используемая хостом для аутентификации карты.</td></tr>
<tr><td>C-MAC</td><td>8 B</td><td>C-MAC для команды EXTERNAL AUTHENTICATE, используемый в качестве начального C-MAC в команде 'IE'.</td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае Метода установки безопасного соединения = '0', '1', '4' или '5':</td></tr>
<tr><td>SK-ENC</td><td></td><td>Сессионный ключ для криптограмм и шифрования сообщений карты (данных APDU).</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>SK-ENC, зашифрованный под LMK 24-25/3.</td></tr>
<tr><td></td><td>'S' + n A</td><td>SK-ENC должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'47'</td><td>'T'</td><td>'B'</td></tr>
</table></td></tr>
<tr><td>SK-MAC</td><td></td><td>Сессионный ключ для аутентификации сообщений карты (C-MAC).</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>SK-MAC, зашифрованный под LMK 24-25/4.</td></tr>
<tr><td></td><td>'S' + n A</td><td>SK-MAC должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'48'</td><td>'T'</td><td>'G'</td></tr>
</table></td></tr>
<tr><td>SK-DEK</td><td></td><td>Сессионный ключ шифрования конфиденциальных данных карты (например, ключей и PIN).</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>SK-DEK, зашифрованный под LMK 24-25/5.</td></tr>
</table>

<table>
<tr><td></td><td>'S' + n A</td><td>SK-DEK должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'49'</td><td>'T'</td><td>'B'</td></tr></table></td></tr>
<tr><td>SK-RMAC</td><td></td><td>Присутствует только в случае Уровня безопасности = 0x10, 0x11 или 0x13. Сессионный ключ для аутентификации ответов карты (R-MAC).</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>SK-RMAC, зашифрованный под LMK 26-27.</td></tr>
<tr><td></td><td>'S' + n A</td><td>SK-RMAC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'48'</td><td>'T'</td><td>'V'</td></tr></table></td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Метода установки безопасного соединения = '6' и Режима генерации ключей карты = '0':</td></tr>
<tr><td>PSK</td><td></td><td>Ключ системы персонализации.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>PSK, зашифрованный под LMK 24-25/5.</td></tr>
<tr><td></td><td>'S' + n A</td><td>PSK должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'40'</td><td>'T'</td><td>'N'</td></tr></table></td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Метода установки безопасного соединения = '2' (Mastercard PayPass Magnetic Stripe):</td></tr>
<tr><td>KD-PERSO</td><td></td><td>Ключ персонализации KD для аутентификации сообщений и шифрования конфиденциальных данных.</td></tr>
<tr><td></td><td>'U' + 32 H</td><td>PSK, зашифрованный под LMK 24-25/5.</td></tr>
<tr><td></td><td>'S' + n A</td><td>PSK должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'40'</td><td>'T'</td><td>'N'</td></tr></table></td></tr>
<tr><td colspan="3">Следующие поля присутствуют только в случае Метода установки безопасного соединения = '7' (SCP03):</td></tr>
<tr><td>Заголовок APDU</td><td>5 B</td><td>Заголовок APDU для команды EXTERNAL AUTHENTICATE [CLA, INS, P1, P2, Lc].</td></tr>
<tr><td>Криптограмма хоста</td><td>8 B</td><td>Криптограмма хоста для команды EXTERNAL AUTHENTICATE, используемая картой для аутентификации хоста.</td></tr>
<tr><td>C-MAC</td><td>8 B</td><td>C-MAC для команды EXTERNAL AUTHENTICATE.</td></tr>
<tr><td>C-MAC Chaining</td><td>16 B</td><td>Начальный C-MAC, используемый в команде 'IE'.</td></tr>
<tr><td>Криптограмма карты</td><td>8 B</td><td>Присутствует только в случае Режима генерации Card Challenge = '1'. Сгенерированная криптограмма карты.</td></tr>
<tr><td>SK-MAC</td><td>'S' + n A</td><td>Сессионный ключ для аутентификации сообщений карты (C-MAC). SK-MAC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'48'</td><td>'A'</td><td>'G'</td></tr></table></td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Уровня безопасности = 0x03, 0x13 или 0x33:</td></tr>
<tr><td>SK-ENC</td><td>'S' + n A</td><td>Сессионный ключ для криптограмм и шифрования сообщений карты. SK-ENC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'47'</td><td>'A'</td><td>'B'</td></tr></table></td></tr>
</table>

<table>
<tr><td colspan="3">Следующее поле присутствует только в случае Уровня безопасности = 0x11, 0x13 или 0x33:</td></tr>
<tr><td>SK-RMAC</td><td>'S' + n A</td><td>Сессионный ключ для аутентификации ответов карты (R-MAC).<br>SK-RMAC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'48'</td><td>'A'</td><td>'V'</td></tr></table></td></tr>
<tr><td>Символ конца ответа</td><td>1 C</td><td>Значение 0x19. Присутствует, только если присутствует в команде.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Присутствует, только если присутствует в команде. Максимальная длина — 32 символа.</td></tr>
</table>

## [IE] — Подготовка сообщений для безопасного соединения с чиповой картой

| Variant LMK ☑ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Подготовка сообщения персонализации для передачи на чиповую карту после успешной установки безопасного соединения с картой в соответствии с EMV Common Personalization Specification (CPS), Global Platform (GP) Secure Channel Protocol 2 (SCP02) и Secure Channel Protocol 3 (SCP03).

Команда поддерживает следующие протоколы:

- Secure Channel Protocol 02 (SCP02) "i" = 0x15
- Secure Channel Protocol 02 (SCP02) "i" = 0x55
- Поддержка специального процесса для карт с магнитной полосой Mastercard PayPass
- Поддержка метода статической персонализации, при котором приложение карты персонализируется с помощью единственного PSK
- Secure Channel Protocol 03 (SCP03)

**Примечания:** В соответствии с EMV CPS и GP SCP02 существует 2 метода передачи данных персонализации приложению карты: Indirect (Explicit) Method и Direct (Implicit) Method.

Команда поддерживает только Indirect (Explicit) Method. В этом методе данные карты подготавливаются процессом подготовки данных и передаются процессу персонализации для записи на карту. Процесс персонализации расшифровывает конфиденциальные данные (например, ключи приложения или PIN), зашифрованные под KEK (или другим соответствующим ключом), повторно зашифровывает их под SK-DEK и генерирует сообщения APDU, передаваемые карте. При необходимости безопасной передачи данных сообщения защищаются с использованием MAC (C-MAC) и опционально зашифровываются с использованием сессионных ключей, сгенерированных в процессе установки безопасного соединения.

Команда формирует сообщения APDU, при необходимости перешифровывая конфиденциальные данные с использованием ключа карты.

Команда поддерживает как полное отсутствие, так и включение одной или нескольких групп данных (Data Groupings, DG) в одно сообщение APDU, а также длины команд для расширенного APDU. Поддерживаются все команды Global Platform, включая STORE DATA и PUT KEY. В зависимости от Уровня безопасности, установленного в параметрах команды, команда может генерировать C-MAC для сообщения и зашифровывать элементы данных APDU.

Если установленный *Уровень безопасности* предполагает использование C-MAC или шифрования, бит 3 байта CLA будет автоматически установлен в 1 (в этом случае, как правило, байт имеет значение 0x84), в противном случае устанавливается значение 0. В C-MAC, который генерируется в соответствии со спецификацией GP, номера логических каналов в байте CLA (биты 1 и 2) всегда устанавливаются в 0, независимо от их значений, установленных в начальном заголовке APDU (это правило не применяется к картам с магнитной полосой Mastercard PayPass и процессу генерации EMV CPS C-MAC), однако исходные значения будут сохранены для дальнейшего вывода. В другие биты CLA-байта изменения не вносятся. Команда поддерживает специальные опции GP для генерации C-MAC с зашифрованными ICV и модифицированными/немодифицированными APDU.

В случае карт с магнитной полосой Mastercard PayPass команда формирует сообщение APDU и выполняет трансляцию ключа KD-CVC3 (расшифровывает KD-CVC3, зашифрованный под ключом процесса подготовки данных, и повторно зашифровывает под ключом карты). Также для APDU сообщения вычисляется MAC с использованием ключа карты.

C-MAC — MAC команды APDU, вычисляемый хостом.

В соответствии со спецификацией Global Platform, STORE DATA APDU определяется значением INS = 0xE2 и битом 8 байта CLA, установленными в начальном заголовке APDU.

STORE DATA APDU формируются в соответствии с дополнительными правилами:

• Объекты данных представлены в DGI кодировке: 2 байта DGI с последующим индикатором длины.
Для поддержки команды APPEND RECORD в соответствии с ISO 7816, которая также использует значение INS = 0xE2, добавлен дополнительный опциональный флаг *Идентификатор версии GP*, отключающий кодирование DGI, если имеет значение '99'.
• Значение P2 будет увеличиваться с каждым дополнительным сообщением APDU, созданным в результате превышения длиной данных APDU максимальной длины команды.
• Индикатор последней команды STORE DATA (бит 8) параметра P1 последнего сгенерированного APDU устанавливается для *Режима вывода* = '2' или '3' (не применяется в случае карт с магнитной полосой Mastercard PayPass).

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'IE'. |
| Метод установки безопасного соединения | 1 N | '0': Indirect (Explicit) инициация защищенного канала системой персонализации<br>'2': Mastercard PayPass Magnetic Stripe<br>*Примечание:* KD-PERSO, используемый для шифрования в группах данных, также используется для генерации MAC; будет создан единственный APDU с полем длины (Lc), содержащим 1 байт.<br>'6': Indirect (Explicit) инициация защищенного канала Open Platform системой персонализации с использованием единственного ключа PSK (SCP02)<br>'7': Secure Channel Protocol 03 (SCP03) |
| Следующее поле присутствует только в случае *Метода установки безопасного соединения* = '0', '6' или '7': | | |
| Уровень безопасности | 1 B | Уровень безопасности, устанавливаемый для всех сообщений карты, создаваемых данной командой. Должен соответствовать уровню, установленному командой EXTERNAL AUTHENTICATE.<br>В случае *Метода установки безопасного соединения* = '0' или '6' (SCP02) допустимые значения:<br>0x00: Без защиты обмена сообщениями<br>0x01: C-MAC<br>0x03: Шифрование и C-MAC<br>0x10: R-MAC<br>0x11: C-MAC и R-MAC<br>0x13: Шифрование команды, C-MAC и R-MAC<br>В случае *Метода установки безопасного соединения* = '7' (SCP03) допустимые значения:<br>0x00: Без защиты обмена сообщениями<br>0x01: C-MAC<br>0x03: Шифрование команды и C-MAC<br>0x11: C-MAC и R-MAC<br>0x13: Шифрование команды, C-MAC и R-MAC<br>0x33: Шифрование команды, C-MAC, R-MAC и шифрование ответа |
| Следующее поле присутствует только в случае *Метода установки безопасного соединения* = '0' или '6' (SCP02) и *Уровня безопасности* = 0x01, 0x03, 0x11 или 0x13: | | |
| SK-MAC или PSK | | Сессионный ключ для аутентификации сообщений карты (C-MAC) или мастер-ключ персонализации. |

| | | |
|---|---|---|
| | 'U' + 32 H | В случае *Метода установки безопасного соединения* = '0' — SK-MAC, зашифрованный под LMK 24-25/4.<br>В случае *Метода установки безопасного соединения* = '6' — PSK, зашифрованный под LMK 24-25/5. |
| | 'S' + n A | Ключ должен соответствовать следующему формату:<br>Использование ключа: Алгоритм: Режим использования<br>'48' (SK-MAC): 'T': 'G'<br>'40' (PSK): 'T': 'N' |
| Начальный C-MAC | 8 B | C-MAC предыдущей команды APDU или EXTERNAL AUTHENICATE для первого C-MAC. |
| Флаг шифрования ICV | 1 N | Признак шифрования предыдущего C-MAC для использования его в качестве ICV (опция GP):<br>'0': не шифровать предыдущие C-MAC перед его использованием в качестве ICV<br>'1': шифровать предыдущие C-MAC перед его использованием в качестве ICV |
| Флаг C-MAC | 1 N | В случае использования процесса генерации C-MAC и опций в соответствии с Global Platform (предыдущий C-MAC используется в качестве IV для MAC):<br>'0': изменить APDU перед генерацией C-MAC (установить бит признака безопасного соединения в CLA в 1 и включить длину C-MAC в байт Lc)<br>'1': не изменять APDU перед генерацией C-MAC<br>В случае использования процесса генерации C-MAC и опций в соответствии с EMV (предыдущий C-MAC добавляется перед данными MAC, используется нулевой IV):<br>'9': изменить APDU перед генерацией C-MAC (установить бит признака безопасного соединения в CLA в 1 и включить длину C-MAC в байт Lc) |
| Следующее поле присутствует только в случае *Метода установки безопасного соединения* = '0' и *Уровня безопасности* = 0x03 или 0x13: | | |
| SK-ENC | | Сессионный ключ для криптограмм и шифрования сообщений карты (APDU). |
| | 'U' + 32 H | SK-ENC, зашифрованный под LMK 24-25/3. |
| | 'S' + n A | SK-ENC должен соответствовать следующему формату:<br>Использование ключа: Алгоритм: Режим использования<br>'47': 'T': 'B' |
| Следующие 3 поля присутствует только в случае *Метода установки безопасного соединения* = '7' (SCP03) и *Уровня безопасности* ≠ 0x00: | | |
| SK-MAC | 'S' + n A | Сессионный ключ для аутентификации сообщений карты (C-MAC) (при необходимости, зашифрованный под LMK).<br>SK-MAC должен соответствовать следующему формату:<br>Использование ключа: Алгоритм: Режим использования<br>'48': 'A': 'G' |
| C-MAC Chaining | 16 B | Значение C-MAC Chaining, полученное от предыдущей APDU команды, или начальный C-MAC, возвращаемый командой EXTERNAL AUTHENTICATE. |
| Текущее значение счетчика ICV | 6 N | Счетчик устанавливается в 1 после успешной команды EXTERNAL AUTHENTICATE и увеличивается для каждой последующей APDU команды с обеспечением безопасного соединения. |
| Следующее поле присутствует только в случае *Метода установки безопасного соединения* = '7' (SCP03) и *Уровня безопасности* = 0x03, 0x13 или 0x33: | | |

<table>
<tr><td>SK-ENC</td><td>'S' + n A</td><td>Сессионный ключ криптограмм и шифрования сообщений карты (APDU) (при необходимости, зашифрованный под LMK).<br>SK-ENC должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'47'</td><td>'A'</td><td>'B'</td></tr></table></td></tr>
<tr><td>Начальный заголовок APDU</td><td>4 B</td><td>Начальный заголовок APDU для команды [CLA, INS, P1, P2].<br>Примечание: Lc генерируется командой автоматически.<br>Значения следующих элементов заголовка должны быть установлены хостом:<br>CLA: бит 8 со значением 1 (для команды GP) или 0 (для ISO 7816)<br>CLA: биты 1 и 2 со значением логического канала (по умолчанию 00)<br>INS: код команды<br>P1: зависит от значения INS<br>P2: зависит от значения INS</td></tr>
<tr><td>Длина команды</td><td>1 N</td><td>Максимальная длина команды.<br>'0': Lc = 1 байт, максимальная длина всей команды (включая заголовок APDU) — 255 байт<br>'1': Lc = 1 байт, максимальная длина — 255 байт<br>Примечание: если передаваемые группы данных не помещаются в одну команду, будет создано несколько команд. Метод установки безопасного соединения = '2' поддерживает только одну команду.<br>'2': Lc = 2 байта, максимальная длина — 65535 байт (не допускатеся использовать в случае Метода установки безопасного соединения = '2'.<br>Примечание: в этом случае перед длиной добавляются дополнительные байты 0x00 до общей длины 3 байта; будет создана только одна команда.</td></tr>
<tr><td>Количество DG</td><td>2 N</td><td>В случае STORE DATA APDU — количество отдельных DGI, которые должны быть объединены в одну команду STORE DATA APDU.<br>Для других APDU — количество элементов данных, которые объединяются для формирования данных APDU.<br>Примечание: в случае Метода установки безопасного соединения = '2' должно быть больше нуля.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Режим вывода</td><td>1 N</td><td>Опционально; должно отсутствовать в случае Метода установки безопасного соединения = '2'.<br>'0': поместить все DGI в один APDU<br>'1': поместить каждый DGI в отдельный APDU<br>'2': поместить все DGI в один APDU и автоматически установить индикатор последней команды STORE DATA (бит 8) в P1 последнего сформированного APDU<br>'3': поместить каждый DGI в отдельный APDU и автоматически установить индикатор последней команды STORE DATA (бит 8) в P1 последнего сформированного APDU</td></tr>
<tr><td colspan="3">Следующие поля (до поля Разделитель (конец всех DG)) повторяются для каждой группы данных (DG):</td></tr>
<tr><td>DGI</td><td>2 B</td><td>Идентификатор группы данных.<br>Примечание: применяется только в случае STORE DATA APDU, в противном случае должно быть установлено нулевое значение.</td></tr>
</table>

<table>
<tr><td>Флаг типа DG</td><td>1 A</td><td>Тип данных в группе данных:<br>'0': открытые данные<br>'1': ключ(и), зашифрованные под KEK (режим ECB)<br>'2': ключ, зашифрованный под KEK (режим CBC)<br>'3': PIN-блок, зашифрованный под ZPK<br>'4': открытые данные, которые будут зашифрованы под SK-DEK (длина должна бать кратна 8 байтам)<br>'5': ключ, зашифрованный под LMK<br>Примечание: зашифрованные ключи и PIN-блоки должны быть представлены в формате, требуемом картой, т.к. преобразование форматов выполняться не будет.<br>Если для Флага типа DGI = '1' указаны несколько ключей, они должны быть конкатенированы без индикаторов Ключевой схемы. Все ключи должны иметь тип и длину, соответствующие значению параметра Ключевая схема (KEK).</td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Флага типа DG = '1', '2' или '3':</td></tr>
<tr><td rowspan="3">Ключ расшифрования</td><td></td><td>Ключ расшифрования данных DG. Опционально; должно присутствовать только для первой группы данных, в случае, если нескольким группам данных требуется один и тот же ключ.</td></tr>
<tr><td>'U' + 32 H<br>или<br>'T' + 48 H</td><td>Если Флаг типа DG = '1' или '2' — KEK, зашифрованный под LMK 24-25/1.<br>Если Флаг типа DG = '3' — ZPK, зашифрованный под LMK 06-07.</td></tr>
<tr><td>'S' + n A</td><td>Ключ расшифрования должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'54' (KEK)</td><td>'T'</td><td>'B', 'D', 'E', 'N'</td></tr>
<tr><td>'72' (ZPK)</td><td>'T'</td><td>'B', 'D', 'N'</td></tr>
</table></td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае Флага типа DG = '1', '2', '3' или '4':</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Обязательное поле.</td></tr>
<tr><td>Ключевая схема (KEK)</td><td>1 A</td><td>Ключевая схема в случае, если ключи зашифровываются под KEK. Присутствует только в случае Флага типа DG = '1'.<br>Опционально; значение по умолчанию 'X'. Должно присутствовать только для первой группы данных, в случае, если несколько групп данных использует одну и ту же ключевую схему.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Обязательное поле.</td></tr>
<tr><td>IV</td><td>8 B</td><td>Вектор инициализации для режима расшифования CBC. Присутствует только в случае Флага типа DG = '2'.</td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Метода установки безопасного соединения = '0', '2' или '6' и Флага типа DG = '1', '2', '3', '4' или '5':</td></tr>
<tr><td rowspan="3">SK-DEK/KD-PERSO/ PSK (если ранее не загружен)</td><td></td><td>Сессионный ключ шифрования конфиденциальных данных карты (например, ключей приложения или PIN), зашифрованных под LMK.<br>Опционально; в случае Флага типа DG = '1', '2', '3' или '4' должно присутствовать только для первой группы данных, в случае, если нескольким группам данных требуется один и тот же указанный ключ.</td></tr>
<tr><td>'U' + 32 H</td><td>Сессионный ключ, зашифрованный под LMK 24-25/5.</td></tr>
<tr><td>'S' + n A</td><td>Сессионный ключ должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'49' (SK-DEK)</td><td>'T'</td><td>'E', 'B'</td></tr>
<tr><td>'40' (PSK)</td><td>'T'</td><td>'N'</td></tr>
</table></td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Метода установки безопасного соединения = '7' и Флага типа DG = '1', '2', '3', '4' или '5':</td></tr>
</table>

<table>
<tr><td>CK-DEK</td><td>'S' + n A</td><td>Ключ карты для шифрования данных карты.<br>CK-DEK должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'39'</td><td>'A'</td><td>'B'</td></tr></table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение ';'. Обязательное поле.</td></tr>
<tr><td colspan="3">Следующее поле присутствует только в случае Флага типа DG = '5':</td></tr>
<tr><td>Код типа ключа</td><td>3 H</td><td>Параметры ключа LMK, используемого для шифрования ключа, передаваемого в данных DG.<br>'30D': CK-ENC, зашифрованный под LMK 36-37/3<br>'40D': CK-MAC, зашифрованный под LMK 36-37/4<br>'50D': CK-DEK, зашифрованный под LMK 36-37/5<br>'507': PSK, зашифрованный под LMK 24-25/5</td></tr>
<tr><td></td><td></td><td>Значение 'FFF'.</td></tr>
<tr><td>Длина DG</td><td>2 B</td><td>Длина группы данных. Значение игнорируется в случае Флага типа DG = '5'.</td></tr>
<tr><td>Данные DG</td><td>n B</td><td>В случае Флага типа DG = '0', '1', '2' или '4'.</td></tr>
<tr><td></td><td>16 H</td><td>В случае Флага типа DG = '3' содержит PIN-блок.<br>Примечание: в этом случае Длина DG = 08.</td></tr>
<tr><td></td><td>'S' + n A</td><td>В случае Флага типа DG = '5' содержит ключ, зашифрованный под LMK.<br>Для Key Block LMK и Метода установки безопасного соединения = '0' или '6' допустимые значения:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'37' (CK-ENC)</td><td>'T'</td><td>'X'</td></tr><tr><td>'38' (CK-MAC)</td><td>'T'</td><td>'X'</td></tr><tr><td>'39' (CK-DEK)</td><td>'T'</td><td>'X'</td></tr><tr><td>'40' (PSK)</td><td>'T'</td><td>'N'</td></tr></table>Для Key Block LMK и Метода установки безопасного соединения = '7' допустимые значения:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'37' (CK-ENC)</td><td>'A', 'T'</td><td>'X'</td></tr><tr><td>'38' (CK-MAC)</td><td>'A', 'T'</td><td>'X'</td></tr><tr><td>'39' (CK-DEK)</td><td>'T'</td><td>'X'</td></tr><tr><td>'39' (CK-DEK)</td><td>'A'</td><td>'B'</td></tr><tr><td>'40' (PSK)</td><td>'T'</td><td>'N'</td></tr></table></td></tr>
<tr><td>Разделитель (конец DG)</td><td>1 A</td><td>Значение ';'. Обязательное поле. Признак конца группы данных.</td></tr>
<tr><td>Разделитель (конец всех DG)</td><td>1 A</td><td>Значение ':'. Обязательное поле. Признак конца всех групп данных.</td></tr>
<tr><td>Разделитель (версия GP)</td><td>1 A</td><td>Значение '$'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор версии GP</td><td>2 N</td><td>Признак соответствия команды спецификации GP Card Specification:<br>'01': команда соответствует GP Card Specification 2.2<br>'99': команда не соответствует GP Card Specification</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'IF'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'05': Недопустимый метод установки безопасного соединения<br>'06': Недопустимый уровень безопасности<br>'07': Недопустимый флаг типа DG<br>'08': Нарушена четность SK-DEK<br>'09': Нарушена четность ключа расшифрования<br>'10': Нарушена четность PSK или SK-MAC<br>'11': Нарушена четность SK-ENC<br>'50': Недопустимый флаг шифрования ICV<br>'51': Недопустимый флаг C-MAC<br>'52': Недопустимая длина команды<br>'53': Не доступен требуемый ключ расшифрования<br>'54': Не доступен требуемый SK-DEK<br>'55': Длина APDU превысила ограничения<br>'56': Ошибка блока DG (разделитель)<br>'57': Превышен максимальное количество сообщений APDU<br>'58': Недопустимый код типа ключа<br>'DA': Ошибка Key Block ключа расшифрования<br>'E1': Ошибка Key Block SK-MAC<br>'E2': Ошибка Key Block SK-ENC<br>'E3': Ошибка Key Block SK-DEK/KD-PERSO<br>'E8': Ошибка Key Block PSK<br>'F2': Недопустимый идентификатор версии GP<br>'F3': Ошибка Key Block в случае Флага типа ключа = '5'<br>'F4': Недопустимый режим вывода<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'DA', 'E1', 'E2', 'E3' или 'E8': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующие поля присутствуют только в случае *Метода установки безопасного соединения* = '0' или '6': | | |
| Количество сообщений APDU | | Количество сгенерированных команд.<br>*Примечание:* если *Длина команды* = '2', будет возвращена единственная команда. |
| | 1 N | В случае Режима вывода = '0' или '2'. |
| | 2 N | В случае Режима вывода = '1' или '3'. |
| Следующее 3 поля повторяются для каждого сообщения APDU: | | |
| Заголовок APDU | 5 или 7 B (если *Длина команды* = '2') | Заголовок APDU для команды [CLA, INS, P1, P2, Lc].<br>*Примечание:* если *Длина команды* = '2', байт Lc принимает значение 0x00, после него добавляются дополнительные 2 байта, т.е. всего 3 байта содержат значение длины блока данных. |
| Блок данных APDU | n B | Данные APDU (длиной Lc) — группы данных (DG) и MAC (при необходимости).<br>*Примечание:* последние 8 байт последнего (или единственного) блока данных APDU могут содержать значение C-MAC (если выбран соответствующий режим), который используется в качестве начального C-MAC для следующей команды 'IE'. |
| Разделитель (конец APDU) | 1 A | Значение ';'. |
| Разделитель (конец всех APDU) | 1 A | Значение ':'. |

| | | |
|---|---|---|
| Следующие 2 поля присутствуют только в случае *Метода установки безопасного соединения* = '2': | | |
| Заголовок APDU | 5 B | Заголовок APDU для команды [CLA, INS, P1, P2, Lc]. |
| Блок данных APDU | n B | Данные APDU (длиной Lc). |
| Следующие 2 поля присутствуют только в случае *Метода установки безопасного соединения* = '7' и *Уровня безопасности* $\neq$ 0x00: | | |
| C-MAC Chaining | 16 B | Значение C-MAC, вычисленное для последнего APDU сообщения. |
| Последнее значение счетчика ICV | 6 N | Значение ICV, используемое в последнем APDU сообщении. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 25 Команды JSON Web Token (JWT)

Следующие команды хоста используются для поддержки операций кодирования/декодирования JSON Web Token (JWT) с использованием JSON Web Signature (JWS) и JSON Web Encryption (JWE):

## [JW] — Кодирование JWT

| Variant LMK ☒ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Создание JSON Web Token (JWT) в виде закодированного блока JSON Web Encryption (JWE) или JSON Web Signature (JWS).

При использовании JWE команда создает полезные данные (payload), которые содержат зашифрованный и защищенный с использованием MAC открытый текст, для формирования JWE-кодированного блоба в виде JWE Compact Serialization, соответствующего следующему формату:

BASE64URL (UTF8 (JWE Protected Header)) || '.' || BASE64URL (JWE Encrypted Key) || '.' || BASE64URL (JWE Initialization Vector) || '.' || BASE64URL (JWE Ciphertext) || '.' || BASE64URL (JWE Authentication Tag)

При использовании JWS команда подписывает полезные данные (payload) для формирования JWS-кодированного блоба в виде JWS Compact Serialization, соответствующего следующему формату:

BASE64URL (UTF8 (JWS Protected Header)) || '.' || BASE64URL (JWS Payload) || '.' || BASE64URL (JWS Signature)

Команда поддерживает следующие механизмы JWE для шифрования ключа:
`"alg": "A128KW", "A192KW", "A256KW"`
`"alg": "A128GCMKW", "A192GCMKW", "A256GCMKW"`
`"alg": "RSA1_5"`
`"alg": "ECDH-ES"`

Команда поддерживает следующие механизмы JWE для шифрования:
`"enc": "A128GCM", "A192GCM", "A256GCM"`
`"enc": "A128CBC-HS256", "A192CBC-HS384", "A256CBC-HS512"`

Команда поддерживает следующие механизмы JWS для генерации подписи:
`"alg": "RS256", "RS384", "RS512"`
`"alg": "PS256", "PS384", "PS512"`
`"alg": "ES256", "ES384", "ES512"`

**Примечания:** При использовании JWE с механизмом `"ECDH-ES"` поле BASE64URL (JWE Encrypted Key) JWE-кодированного блоба отсутствует.

При использовании JWS с механизмом генерации подписи `"ES256"`, `"ES384"`, `"ES512"` алгоритм хэширования должен соответствовать эллиптической кривой закрытого ключа (SHA-256 для P-256, SHA-384 для P-384, SHA-512 для P-521).

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce PCI HSMv3 Key Equivalence for Key Wrapping`<br>(влияет на параметры: *Длина CEK, Ключ шифрования ключа/Открытый ключ получателя*) | `Yes [Y]` | Если для шифрования ключа используется ключ RSA, его сила (key strength) должна быть не меньше силы ключа CEK.<br>Если для шифрования используется диверсифицированный ключ, его сила (key strength) не может быть больше силы исходных ключей ECC, переданных в команде. |
| | `No [N]` | Ограничения на силу ключа не накладываются. |

| | | |
|---|---|---|
| `Enforce minimum key strength of 2048-bits for RSA` | `Yes [Y]` | Длины ключа шифрования ключей (RSA) и ключа подписи (RSA) должны быть не менее 2048 бит. |
| (влияет на параметры: *Ключ шифрования ключа, Ключ подписи*) | `No [N]` | Ограничения на длину ключей не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'JW'. |
| Формат JWT | 1 N | '0': JWE (Compact Serialisation)<br>'1': JWS (Compact Serialisation) |
| Разделитель заголовка | 1 A | Значение '='. Опционально; если присутствуют, следующие 2 поля обязательны. |
| Следующие 2 поля присутствуют, только если присутствует *Разделитель заголовка*: | | |
| Длина Protected Header | 4 N | Длина JWE/JWS Protected Header. |
| Protected Header | n B | JWE/JWS Protected Header в формате JSON. |
| Следующие 4 поля присутствуют только в случае *Формата JWT* = '0': | | |
| Режим шифрования | 1 N | Режим шифрования и MAC, используемые для защиты полезных данных (payload):<br>'0': AES CBC с использованием HMAC SHA2<br>'1': AES GCM |
| Флаг IV | 1 N | '0': Генерировать случайный вектор инициализации |
| Флаг CEK | 1 N | '1': Генерировать случайный CEK<br>'9': Сформировать CEK из общего производного ключа |
| Длина CEK | 2 N | Длина (в байтах) CEK. Допустимые значения: 16, 24 или 32. |
| Следующие 2 или 3 поля присутствуют только в случае *Формата JWT* = '0' и *Флага CEK* = '1': | | |
| Режим шифрования CEK | 1 N | '0': AES<br>'1': AES GCM<br>'2': PKCS#1 v2.2 method EME-PKCS1-v1_5 |
| Ключ шифрования ключа | 'S' + n A<br>или<br>'S' + n B | В случае *Режима шифрования CEK* = '0' ключ должен соответствовать следующему формату:<br>Использование ключа: 'K0' / Алгоритм: 'A' / Режим использования: 'B', 'E', 'D'<br>В случае *Режима шифрования CEK* = '1' ключ должен соответствовать следующему формату:<br>Использование ключа: '24' / Алгоритм: 'A' / Режим использования: 'B', 'E', 'D'<br>В случае *Режима шифрования CEK* = '2' ключ должен соответствовать следующему формату:<br>Использование ключа: '02' / Алгоритм: 'R' / Режим использования: 'E', 'N' |
| Тип Key Block | 2 N | Присутствует только в случае *Режима шифрования CEK* = '2'.<br>'03': Неформатированный Key Block |
| Следующее поле присутствуют только в случае *Формата JWT* = '0' и *Флага CEK* = '9': | | |

<table>
<tr><td>Открытый ключ получателя</td><td>'S' + n A</td><td>Ключ должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'02'</td><td>'E'</td><td>'X', 'N'</td></tr></table></td></tr>
<tr><td colspan="3">Следующие 4 поля присутствуют только в случае Формата JWT = '1':</td></tr>
<tr><td>Идентификатор алгоритма подписи</td><td>1 N</td><td>'1': RSA<br>'2': ECDSA</td></tr>
<tr><td>Идентификатор режима дополнения</td><td>2 N</td><td>Присутствует только в случае Идентификатора алгоритма подписи = '1'.<br>'01': PKCS#1 v2.2 method EMSA-PKCS1-v1_5<br>'04': PKCS#1 v2.2 method EMSA-PSS</td></tr>
<tr><td>Идентификатор алгоритма хэширования</td><td>2 N</td><td>'06': SHA-256<br>'07': SHA-384<br>'08': SHA-512</td></tr>
<tr><td>Ключ подписи</td><td>'S' + n B<br>или<br>'S' + n A</td><td>В случае Идентификатора алгоритма подписи = '1' ключ должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'03'</td><td>'R'</td><td>'S', 'N'</td></tr></table>В случае Идентификатора алгоритма подписи = '2' ключ должен соответствовать следующему формату:<table><tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr><tr><td>'03'</td><td>'E'</td><td>'S', 'N'</td></tr></table></td></tr>
<tr><td>Количество сообщений</td><td>2 N</td><td>Количество сообщений, включаемых в полезные данные (payload).</td></tr>
<tr><td colspan="3">Следующие 4 поля повторяются для каждого сообщения:</td></tr>
<tr><td>Тип сообщения</td><td>2 N</td><td>'00': незашифрованный JWT</td></tr>
<tr><td>Длина сообщения</td><td>6 N</td><td>Длина (в байтах) следующего поля.</td></tr>
<tr><td>Сообщение</td><td>n B</td><td>Открытый текст.</td></tr>
<tr><td>Разделитель сообщения</td><td>1 A</td><td>Значение ';'. Обязательное поле.</td></tr>
<tr><td>Разделитель (конец всех сообщений)</td><td>1 A</td><td>Значение ':'. Обязательное поле.</td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'JX'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'38': Недопустимый тип Key Block<br>'D1': Недопустимый формат JWT<br>'D2': Недопустимое сообщение<br>'D3': Недопустимый режим шифрования<br>'D4': Недопустимый формат JSON в заголовке<br>'D6': Недопустимый режим шифрования CEK<br>'D7': Ошибка Key Block ключа шифрования ключа<br>'D9': Недопустимая длина сообщения<br>'DB': Недопустимая длина CEK<br>'DE': Достигнута максимальная длина сообщения<br>'DF': Недопустимый идентификатор режима дополнения<br>'E1': Недопустимое количество сообщений<br>'E2': Недопустимый флаг IV<br>'E3': Недопустимый идентификатор алгоритма подписи<br>'E4': Недопустимый идентификатор алгоритма хэширования<br>'E5': Ошибка Key Block ключа подписи<br>'E6': Недопустимый флаг CEK<br>'E9': Недопустимая длина заголовка<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D7' или 'E5': | | |
| Дополнительный код ошибки (Key Block) | 2 H | Дополнительный код ошибки Key Block. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'D2' или 'D9': | | |
| Дополнительный код ошибки (сообщение) | 2 H | Номер сообщения, в котором обнаружена ошибка. |
| Следующие поля присутствует только в случае отсутствия ошибки выполнения команды (*Код ошибки* = '00'): | | |
| Длина JWT | 6 N | Длина следующего поля. |
| JWT | n A | В случае *Формата JWT* = '0' — JWT в формате JWE:<br>BASE64URL(UTF8(JWE Protected Header)) \|\| '.' \|\|<br>BASE64URL(JWE Encrypted Key) \|\| '.' \|\|<br>BASE64URL(JWE Initialization Vector) \|\| '.' \|\|<br>BASE64URL(JWE Ciphertext) \|\| '.' \|\|<br>BASE64URL(JWE Authentication Tag)<br>В случае *Формата JWT* = '1' — JWT в формате JWS:<br>BASE64URL (UTF8 (JWS Protected Header)) \|\| '.' \|\|<br>BASE64URL (JWS Payload) \|\| '.' \|\|<br>BASE64URL (JWS Signature) |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [JY] — Декодирование JWT

| Variant LMK ☒ | Key Block LMK ☑ |
|---|---|

**Описание функции:** Декодирование JSON Web Token (JWT) в формате JSON Web Encryption (JWE) и возврат хосту расшифрованного сообщения, или декодирование JWT в формате JSON Web Signature (JWS) и проверка подписи.

JWE-кодированный блоб в виде JWE Compact Serialization соответствует следующему формату:

BASE64URL (UTF8 (JWE Protected Header)) || '.' || BASE64URL (JWE Encrypted Key) || '.' || BASE64URL (JWE Initialization Vector) || '.' || BASE64URL (JWE Ciphertext) || '.' || BASE64URL (JWE Authentication Tag)

JWS-кодированный блоб в виде JWS Compact Serialization соответствует следующему формату:

BASE64URL (UTF8 (JWS Protected Header)) || '.' || BASE64URL (JWS Payload) || '.' || BASE64URL (JWS Signature)

Перед вызовом команды заголовок JWE Protected Header необходимо перевести из двоичного формата с кодировкой Base64 в строковый формат для определения значения поля «alg», указывающего, какой ключ расшифрования ключа необходимо использовать в команде.

Команда поддерживает следующие механизмы JWE для расшифрования ключа:
`"alg": "A128KW", "A192KW", "A256KW"`
`"alg": "A128GCMKW", "A192GCMKW", "A256GCMKW"`
`"alg": "RSA1_5"`
`"alg": "ECDH-ES"`

Команда поддерживает следующие механизмы JWE для расшифрования:
`"enc": "A128GCM", "A192GCM", "A256GCM"`
`"enc": "A128CBC-HS256", "A192CBC-HS384", "A256CBC-HS512"`

Команда поддерживает следующие механизмы JWS для проверки подписи:
`"alg": "RS256", "RS384", "RS512"`
`"alg": "PS256", "PS384", "PS512"`
`"alg": "ES256", "ES384", "ES512"`

**Примечания:** При использовании JWE с механизмом `"ECDH-ES"` поле BASE64URL (JWE Encrypted Key) JWE-кодированного блоба отсутствует.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce PCI HSMv3 Key Equivalence for Key Wrapping` (влияет на параметры: *Закрытый ключ получателя*) | `Yes [Y]` | Если для расшифрования используется диверсифицированный ключ, его сила (key strength) не может быть больше силы исходных ключей ECC, переданных в команде. |
| | `No [N]` | Ограничения на силу ключа не накладываются. |
| `Enforce minimum key strength of 1024-bits for RSA signature verification` (влияет на параметры: *Ключ проверки подписи*) | `Yes [Y]` | Длина ключа проверки подписи (RSA) должна быть не менее 1024 бит. |
| | `No [N]` | Ограничения на длину ключа не накладываются. |

| | | |
|---|---|---|
| `Enforce minimum key strength of 2048-bits for RSA` | `Yes [Y]` | Длины ключа расшифрования ключей (RSA) и ключа проверки подписи (RSA) должны быть не менее 2048 бит. |
| (влияет на параметры: *Ключ проверки подписи*) | `No [N]` | Ограничения на длину ключа не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'JY'. |
| Формат JWT | 1 N | '0': JWE (Compact Serialisation)<br>'1': JWS (Compact Serialisation) |
| Длина JWT | 6 N | Длина следующего поля. |
| JWT | n A | В случае *Формата JWT* = '0' — JWT в формате JWE.<br>В случае *Формата JWT* = '1' — JWT в формате JWS. |
| Разделитель | 1 A | Значение ';'. |
| Следующие 2 поля (*Ключ расшифрования ключа* ИЛИ *Закрытый ключ получателя* и *Тип Key Block*) присутствуют только в случае *Формата JWT* = '0': | | |
| Ключ расшифрования ключа | 'S' + n A<br>или<br>'S' + n B | Ключ для расшифрования JWE Encrypted Key.<br>Если 'alg' имеет значение A128/192/256GCMKW, ключ должен соответствовать следующему формату:<br>Использование ключа: '24' / Алгоритм: 'A' / Режим использования: 'B', 'E', 'D'<br>Если 'alg' имеет значение A128/192/256KW, ключ должен соответствовать следующему формату:<br>Использование ключа: 'K0' / Алгоритм: 'A' / Режим использования: 'B', 'E', 'D'<br>Если 'alg' имеет значение RSA1_5, ключ должен соответствовать следующему формату:<br>Использование ключа: '03' / Алгоритм: 'R' / Режим использования: 'D', 'N' |
| ИЛИ | | |
| Закрытый ключ получателя | 'S' + n A | Если 'alg' имеет значение ECDH-ES, ключ должен соответствовать следующему формату:<br>Использование ключа: '03' / Алгоритм: 'E' / Режим использования: 'X', 'N' |
| Тип Key Block | 2 N | Присутствует, только если 'alg' имеет значение RSA1_5.<br>'03': Неформатированный Key Block |

<table>
<tr><td colspan="3">Следующее поле присутствует только в случае Формата JWT = '1':</td></tr>
<tr><td>Ключ проверки подписи</td><td>'S' + n B<br>или<br>'S' + n A</td><td>Если 'alg' имеет значение RS256/384/512 или PS256/384/512, ключ для проверки подписи JWS Signature должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'02'</td><td>'R'</td><td>'V', 'N'</td></tr>
</table>
Если 'alg' имеет значение ES256/384/512, ключ для проверки подписи JWS Signature должен соответствовать следующему формату:
<table>
<tr><th>Использование ключа</th><th>Алгоритм</th><th>Режим использования</th></tr>
<tr><td>'02'</td><td>'E'</td><td>'V', 'N'</td></tr>
</table></td></tr>
<tr><td>Разделитель</td><td>1 A</td><td>Значение '%'. Опционально; если присутствует, следующее поле обязательно.</td></tr>
<tr><td>Идентификатор LMK</td><td>2 N</td><td>Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле.</td></tr>
<tr><td>Символ конца команды</td><td>1 C</td><td>Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер.</td></tr>
<tr><td>Трейлер</td><td>n A</td><td>Опционально. Максимальная длина — 32 символа.</td></tr>
</table>

| Параметр | Формат | Описание |
|---|---|---|
| | | **ОТВЕТ** |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'JZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'02': Ошибка проверки подписи JWS<br>'38': Недопустимый тип Key Block<br>'D1': Недопустимый формат JWT<br>'D2': Недопустимая длина JWT<br>'D3': Данные JWT не соответствуют указанному формату JWT<br>'D4': Недопустимый формат JSON в заголовке<br>'D5': Отсутствует поле 'enc' в заголовке<br>'D6': Отсутствует поле 'alg' в заголовке<br>'D7': Недопустимое значение 'alg'<br>'D8': Недопустимое значение 'enc'<br>'DA': Недопустимое значение 'kty'<br>'DB': Параметры подписи (r, s) больше порядка кривой<br>'DF': Ошибка Key Block ключа расшифрования ключа<br>'E0': Недопустимая длина ключа расшифрования ключа<br>'E1': Недопустимая длина вектора инициализации JWE<br>'E2': Отсутствует поле 'tag' или 'iv' в заголовке<br>'E4': Недопустимая длина CEK<br>'E6': Ошибка проверки JWE Authentication Tag<br>'E8': Ошибка Key Block ключа проверки подписи<br>'EA': Недостаточная сила кривой ECC для выработки ключей<br>или другой стандартный код ошибки. |
| Следующее поле присутствует только в случае *Кода ошибки* = 'DF' или 'E8': | | |
| Дополнительный код ошибки | 2 H | Дополнительный код ошибки Key Block. |
| Следующие поля присутствует только в случае отсутствия ошибки выполнения команды (*Код ошибки* = '00') и *Формата JWT* = '0': | | |
| Длина сообщения | 6 N | Длина следующего поля. |
| Сообщение | n B | Расшифрованный JWT. |

| | | |
|---|---|---|
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 26 Устаревшие команды управления ключами

Для управления ключами в HSM поддерживаются следующие устаревшие (legacy) команды хоста:

## [HA] — Генерация TAK

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|
| Авторизация: **Определяется по TTK (Э)** | |
| Активности: **export.003.host** | |

**Описание функции:** Генерация случайного TAK и возврат его хосту в зашифрованном виде под TMK и LMK 16-17.

**Авторизация:** Команда проверяет флаг 'Э' (экспорт) для заданного типа ключа в таблице типов ключей (TTK, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **export.003.host** должна быть авторизована.

**Примечания:** Поля *Ключевая схема (TMK)* и *Ключевая схема (LMK)* могут содержать значение '0', однако не могут быть равны нулю одновременно.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable X9.17 for export` | `Yes [Y]` | Доступен экспорт ключа в формат X9.17 (X, Y схемы). |
| | `No [N]` | Экспорт ключа в формат X9.17 невозможен. |
| `Key export and import in trusted format only` | `Yes [Y]` | Экспорт ключа в недоверенные форматы невозможен. |
| | `No [N]` | Доступен экспорт ключа в недоверенные форматы (X, Y, U, T схемы). |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'HA'. |
| TMK | 'U' + 32 H<br>или<br>'T' + 48 H | TMK, зашифрованный под LMK 14-15/0 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`) или LMK 36-37/8 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: Yes`). |
| Разделитель | 1 A | Значение ';'. |
| Ключевая схема (TMK) | 1 A | Схема шифрования ключа под TMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Ключевая схема (LMK) | 1 A | Схема шифрования ключа под LMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Зарезервировано | 1 A | Значение '0'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'HB'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность TMK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| TAK (под TMK) | 'U' или<br>'X' + 32 H<br>или<br>'T' или<br>'Y' + 48 H | TAK, зашифрованный под TMK. |
| TAK (под LMK) | 'U' + 32 H<br>или<br>'T' + 48 H | TAK, зашифрованный под LMK 16-17. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [HC] — Генерация TMK, TPK или PVK

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|
| Авторизация: **Определяется по ТТК (Э)** | |
| Активности: **export.002.host** | |

**Описание функции:** Генерация случайного ключа и возврат его хосту в зашифрованном виде под TMK (TPK или PVK) и LMK 14-15.

**Авторизация:** Команда проверяет флаг 'Э' (экспорт) для заданного типа ключа в таблице типов ключей (ТТК, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **export.002.host** должна быть авторизована.

**Примечания:** Поля *Ключевая схема (TMK)* и *Ключевая схема (LMK)* могут содержать значение '0', однако не могут быть равны нулю одновременно.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable X9.17 for export` | `Yes [Y]` | Доступен экспорт ключа в формат X9.17 (X, Y схемы). |
| | `No [N]` | Экспорт ключа в формат X9.17 невозможен. |
| `Key export and import in trusted format only` | `Yes [Y]` | Экспорт ключа в недоверенные форматы невозможен. |
| | `No [N]` | Доступен экспорт ключа в недоверенные форматы (X, Y, U, T схемы). |
| `Enforce key type 002 separation for PCI HSM compliance` | `Yes [Y]` | Команда недоступна. |
| | `No [N]` | Команда доступна. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'HC'. |
| Текущий TMK, TPK или PVK | 'U' + 32 H<br>или<br>'T' + 48 H | Текущий TMK, TPK или PVK, зашифрованный под LMK 14-15. |
| Разделитель | 1 A | Значение ';'. |
| Ключевая схема (TMK) | 1 A | Схема шифрования ключа под TMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Ключевая схема (LMK) | 1 A | Схема шифрования ключа под LMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Зарезервировано | 1 A | Значение '0'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'HD'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность TMK, TPK или PVK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Новый ключ (под текущим ключом) | 'U' или<br>'X' + 32 H<br>или<br>'T' или<br>'Y' + 48 H | Сгенерированный ключ, зашифрованный под текущим ключом. |
| Новый ключ (под LMK) | 'U' + 32 H<br>или<br>'T' + 48 H | Сгенерированный ключ, зашифрованный под LMK 14-15. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [AE] — Трансляция TMK, TPK или PVK (из-под LMK под TMK/TPK/PVK)

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|
| Авторизация: **Определяется по ТТК (Э)** | |
| Активности: **export.002.host** | |

**Описание функции:** Расшифрование сохраненного TMK, TPK или PVK, зашифрованного под LMK 14-15, и последующее зашифрование под текущим TMK (TPK или PVK).

**Авторизация:** Команда проверяет флаг 'Э' (экспорт) для заданного типа ключа в таблице типов ключей (ТТК, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **export.002.host** должна быть авторизована.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable X9.17 for export` | `Yes [Y]` | Доступен экспорт ключа в формат X9.17 (X, Y схемы). |
| | `No [N]` | Экспорт ключа в формат X9.17 невозможен. |
| `Key export and import in trusted format only` | `Yes [Y]` | Экспорт ключа в недоверенные форматы невозможен. |
| | `No [N]` | Доступен экспорт ключа в недоверенные форматы (X, Y, U, T схемы). |
| `Enforce key type 002 separation for PCI HSM compliance` | `Yes [Y]` | Команда недоступна. |
| | `No [N]` | Команда доступна. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'AE'. |
| Текущий TMK, TPK или PVK | 'U' + 32 H<br>или<br>'T' + 48 H | Текущий TMK, TPK или PVK, зашифрованный под LMK 14-15. |
| Сохраненный TMK, TPK или PVK | 'U' + 32 H<br>или<br>'T' + 48 H | Сохраненный TMK, TPK или PVK, зашифрованный под LMK 14-15. |
| Разделитель | 1 A | Значение ';'. Опционально; если присутствует, следующие 3 поля обязательны. |
| Ключевая схема (TMK) | 1 A | Опционально. Схема шифрования ключа под TMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'AF'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность текущего TMK, TPK или PVK<br>'11': Нарушена четность сохраненного TMK, TPK или PVK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| Сохраненный ключ, зашифрованный под текущим ключом | 'U' или<br>'X' + 32 H<br>или<br>'T' или<br>'Y' + 48 H | Сохраненный TMK, TPK или PVK, зашифрованный под текущим TMK, TPK или PVK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [AG] — Трансляция TAK (из-под LMK под TMK)

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|
| Авторизация: **Определяется по ТТК (Э)** | |
| Активности: **export.003.host** | |

**Описание функции:** Расшифрование TAK, зашифрованного под LMK, и последующее зашифрование под TMK для передачи ключа терминалу.

**Авторизация:** Команда проверяет флаг 'Э' (экспорт) для заданного типа ключа в таблице типов ключей (ТТК, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **export.003.host** должна быть авторизована.

**Примечания:** Данная команда заменятся командой 'A8'.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable X9.17 for export` | `Yes [Y]` | Доступен экспорт ключа в формат X9.17 (X, Y схемы). |
| | `No [N]` | Экспорт ключа в формат X9.17 невозможен. |
| `Key export and import in trusted format only` | `Yes [Y]` | Экспорт ключа в недоверенные форматы невозможен. |
| | `No [N]` | Доступен экспорт ключа в недоверенные форматы (X, Y, U, T схемы). |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'AG'. |
| TMK | 'U' + 32 H<br>или<br>'T' + 48 H | TMK, зашифрованный под LMK 14-15/0 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`) или LMK 36-37/8 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: Yes`). |
| TAK | 'U' + 32 H<br>или<br>'T' + 48 H | TAK, зашифрованный под LMK 16-17. |
| Разделитель | 1 A | Значение ';'. Опционально; если присутствует, следующие 3 поля обязательны. |
| Ключевая схема (TMK) | 1 A | Опционально. Схема шифрования ключа под TMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'AH'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность TMK<br>'11': Нарушена четность TAK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| TAK (TMK) | 'U' или<br>'X' + 32 H<br>или<br>'T' или<br>'Y' + 48 H | TAK, зашифрованный под TMK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [OE] — Генерация и печать TMK, TPK или PVK

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|
| Авторизация: **Требуется** | |
| Активности: **genprint.002.host** | |

**Описание функции:** Генерация TMK, TPK или PVK, возврат его хосту в зашифрованном виде под LMK 14-15 и печать с помощью подключенного к HSM принтера.

**Авторизация:** HSM должен находиться в авторизованном состоянии, либо активность **genprint.002.host** должна быть авторизована.

**Примечания:** Данная команда заменяется командой 'NE'.

Для выполнения команды принтер должен быть подключен к USB-порту HSM.

На HSM уже должен быть настроен формат печати.

В команде должно присутствовать как минимум одно поле печати.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce key type 002 separation for PCI HSM compliance` | `Yes [Y]` | Команда недоступна. |
| | `No [N]` | Команда доступна. |

| Параметр | Формат | Описание |
|---|---|---|
| | **КОМАНДА** | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'OE'. |
| Поле печати 0 | n A | Поле печати определяется как *Поле печати 0* в определении формата печати (не должно содержать символов ';', '\|' или '~'). |
| Разделитель | 1 A | Значение ';'. |
| Поле печати 1 | n A | Поле печати определяется как *Поле печати 1* в определении формата печати (не должно содержать символов ';', '\|' или '~'). |
| Разделитель | 1 A | Значение ';'. |
| ... | ... | ... |
| ... | ... | ... |
| Последнее поле печати | n A | *Последнее поле печати*, определенное в определении формата печати (не должно содержать символов ';', '\|' или '~'). |
| Разделитель | 1 A | Значение '\|'. Опционально; если присутствует, следующие 3 поля обязательны. |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Ключевая схема (LMK) | 1 A | Опционально. Схема шифрования ключа под LMK. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Разделитель | 1 A | Значение '~'. Опционально; присутствует, если присутствует разделитель '%' ниже. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |

| | | |
|---|---|---|
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'OF'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'16': Принтер не готов/не подключен<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| TMK, TPK или PVK | 'U' + 32 H<br>или<br>'T' + 48 H | TMK, TPK или PVK, зашифрованный под LMK 14-15. |
| Код ответа принтера | 2 A | Значение 'OZ'. |
| Код ошибки принтера | 2 H | '00': Без ошибок<br>'41': Внутренняя аппаратная/программная ошибка<br>или другой стандартный код ошибки. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [AY] — Трансляция CVK (из-под старого LMK под новый LMK)

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|

**Описание функции:** Расшифрование CVK, зашифрованного под старым LMK, и последующее зашифрование под новым LMK.

**Примечания:** Данная команда заменяется командой 'BW'.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'AY'. |
| CVK A/B | 'U' + 32 H | CVK A/B, зашифрованный под старым LMK 14-15/4. |
| Разделитель | 1 A | Значение ';'. Опционально; если присутствует, следующие 3 поля обязательны. |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Ключевая схема (LMK) | 1 A | Опционально. Схема шифрования выходного ключа под LMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'AZ'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность CVK A/B<br>'11': Нарушена четность ZPK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| CVK A/B | 'U' + 32 H | CVK A/B, зашифрованный под новым LMK 14-15/4. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [FE] — Трансляция TMK, TPK или PVK (из-под LMK под ZMK)

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|
| Авторизация: **Определяется по TTK (Э)** | |
| Активности: **export.002.host** | |

**Описание функции:** Расшифрование TMK, TPK или PVK, зашифрованного под LMK, и последующее зашифрование под ZMK.

**Авторизация:** Команда проверяет флаг 'Э' (экспорт) для заданного типа ключа в таблице типов ключей (TTK, см. «КриптоПро HSM. Руководство программиста») для определения необходимости авторизации. Если значение флага 'A', HSM должен находиться в авторизованном состоянии, либо активность **export.002.host** должна быть авторизована.

**Примечания:** Данная команда заменятся командой 'A8'.

Команда используется для передачи ключа другой стороне.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enable X9.17 for export` | `Yes [Y]` | Доступен экспорт ключа в формат X9.17 (X, Y схемы). |
| | `No [N]` | Экспорт ключа в формат X9.17 невозможен. |
| `Restrict Key Check Value to 6 hex chars` (влияет на параметры: *KCV*) | `Yes [Y]` | Только первые 6 символов параметра *KCV* содержат проверочное значение ключа, остальные крайние правые символы устанавливаются в '0'. |
| | `No [N]` | Дополнительные ограничения на KCV не накладываются. |
| `Key export and import in trusted format only` | `Yes [Y]` | Экспорт ключа в недоверенные форматы невозможен. |
| | `No [N]` | Доступен экспорт ключа в недоверенные форматы (X, Y, U, T схемы). |
| `Enforce key type 002 separation for PCI HSM compliance` | `Yes [Y]` | Команда недоступна. |
| | `No [N]` | Команда доступна. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'FE'. |
| ZMK | 'U' + 32 H<br>или<br>'T' + 48 H | ZMK, зашифрованный под LMK 04-05. |
| TMK, TPK или PVK | 'U' + 32 H<br>или<br>'T' + 48 H | TMK, TPK или PVK, зашифрованный под LMK 14-15. |
| Atalla вариант | 1/2 N | Опционально; используется при работе с оборудованием Atalla. |
| Разделитель | 1 A | Значение ';'. Опционально; если присутствует, следующие 3 поля обязательны. |
| Ключевая схема (ZMK) | 1 A | Опционально. Схема шифрования ключа под ZMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Тип KCV | 1 A | Опционально. Метод вычисления проверочного значения ключа:<br>'0': 16-значный KCV (режим обратной совместимости, значение по умолчанию)<br>'1': 6-значный KCV |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'FF'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность ZMK<br>'11': Нарушена четность TMK, TPK или PVK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| TMK, TPK или PVK | 'U' или<br>'X' + 32 H<br>или<br>'T' или<br>'Y' + 48 H | Транслированный TMK, TPK или PVK, зашифрованный под ZMK. |
| KCV | 16/6 H | Результат зашифрования 64 бинарных нулей под ключом. Размер поля зависит от значения *Тип KCV*, указываемого в команде. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [KC] — Трансляция ZPK (из-под старого LMK под новый LMK)

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|

**Описание функции:** Расшифрование ZPK, зашифрованного под старым LMK, и последующее зашифрование под новым LMK.
«Старый» или «новый» LMK должен быть предварительно загружен в хранилище смены ключей.

**Примечания:** Данная команда заменяется командой 'BW'.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'KC'. |
| ZPK | 'U' + 32 H<br>или<br>'T' + 48 H | ZPK, зашифрованный под старым LMK. |
| Разделитель | 1 A | Значение ';'. Опционально; если присутствует, следующие 3 поля обязательны. |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Ключевая схема (LMK) | 1 A | Опционально. Схема шифрования выходного ключа под LMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KD'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'10': Нарушена четность ZPK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| ZPK | 'U' + 32 H<br>или<br>'T' + 48 H | ZPK, зашифрованный под новым LMK. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [FA] — Трансляция ZPK (из-под ZMK под LMK)

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|

**Описание функции:** Расшифрование ZPK, зашифрованного под ZMK, и последующее зашифрование под LMK.

**Примечания:** Данная команда заменяется командой 'A6'.
Команда используется для получения ключа от другой стороны.

Данная команда не требует, чтобы у ZPK были выставлены биты четности. Однако команда гарантирует, что у выходного ключа, зашифрованного под LMK, биты четности будут выставлены. В случае нарушения четности ZPK команда возвращает код ошибки '01' и далее работает штатно.

Команда проверяет ZPK после расшифрования, чтобы убедиться, что ключ (за исключением битов четности) ненулевой (не равен 0x0000 0000 0000 0000), в противном случае команда завершается с ошибкой '11' (Нулевой ZPK).

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce Atalla variant match to variant key type` | `Yes [Y]` | Принудительно проверяется соответствие между Atalla вариантом и типом ключа Variant, см. таблицу ниже. |
| | `No [N]` | Ограничения на соответствие между Atalla вариантом и типом ключа Variant не накладываются. |
| `Enable X9.17 for import` | `Yes [Y]` | Доступен импорт ключа из формата X9.17 (X, Y схемы). |
| | `No [N]` | Импорт ключа из формата X9.17 невозможен. |
| `Restrict Key Check Value to 6 hex chars` (влияет на параметры: *KCV*) | `Yes [Y]` | Только первые 6 символов параметра *KCV* содержат проверочное значение ключа, остальные крайние правые символы устанавливаются в '0'. |
| | `No [N]` | Дополнительные ограничения на KCV не накладываются. |
| `Key export and import in trusted format only` | `Yes [Y]` | Импорт ключа из недоверенных форматов невозможен. |
| | `No [N]` | Доступен импорт ключа из недоверенных форматов (X, Y, U, T схемы). |

| Тип ключа | Atalla вариант | Код типа ключа Variant |
|---|---|---|
| ZPK | 1 или 01 | 001 LMK 06-07 |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'FA'. |
| ZMK | 'U' + 32 H<br>или<br>'T' + 48 H | ZMK, зашифрованный под LMK 04-05. |
| ZPK | 'U' или<br>'X' + 32 H<br>или<br>'T' или<br>'Y' + 48 H | ZPK, зашифрованный под ZMK. |
| Atalla вариант | 1/2 N | Опционально; используется при работе с оборудованием Atalla. |
| Разделитель | 1 A | Значение ';'. Опционально; если присутствует, следующие 3 поля обязательны. |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Ключевая схема (LMK) | 1 A | Опционально. Схема шифрования ключа под LMK или значение '0'. Допустимые значения см. в таблице ключевых схем в «КриптоПро HSM. Руководство программиста». |
| Тип KCV | 1 A | Опционально. Метод вычисления проверочного значения ключа:<br>'0': 16-значный KCV (режим обратной совместимости, значение по умолчанию)<br>'1': 6-значный KCV |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'FB'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Нарушена четность ZPK (предупреждение)<br>'10': Нарушена четность ZMK<br>'11': Нулевой ZPK<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| ZPK | 'U' + 32 H<br>или<br>'T' + 48 H | Транслированный ZPK, зашифрованный под LMK 06-07. |
| KCV | 16/6 H | Результат зашифрования 64 бинарных нулей под ZPK. Размер поля зависит от значения *Тип KCV*, указываемого в команде. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [KA] — Генерация проверочного значения ключа (KCV)

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|

**Описание функции:** Генерация проверочного значения ключа (KCV) для ключей ZMK, ZPK, TMK, TPK, TKR, PVK, TAK.

**Примечания:** Данная команда заменяется командой 'BU'.

Команда может использоваться для проверки ключа, полученного HSM от другой стороны. HSM генерирует значение KCV путем зашифрования 64 бинарных нулей под указанным в команде ключом.

Выполнение данной команды зависит от следующих настроек безопасности (см. консольную команду CS):

| | | |
|---|---|---|
| `Enforce key type 002 separation for PCI HSM compliance` | `Yes [Y]` | Команда недоступна. |
| | `No [N]` | Команда доступна. |
| `Restrict Key Check Value to 6 hex chars` (влияет на параметры: *KCV*) | `Yes [Y]` | Только первые 6 символов параметра *KCV* содержат проверочное значение ключа, остальные символы устанавливаются в '0'. |
| | `No [N]` | Дополнительные ограничения на KCV не накладываются. |

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'KA'. |
| Ключ | 'U' + 32 H<br>или<br>'T' + 48 H | Ключ ZMK, ZPK, TMK, TPK, TKR, PVK или TAK, зашифрованный под соответствующим LMK. |
| Тип ключа | 2 N | '00': ZMK<br>'01': ZPK<br>'02': TMK, TPK, TKR или PVK<br>'03': TAK |
| Разделитель | 1 A | Значение ';'. Опционально; если присутствует, следующие 3 поля обязательны. |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Зарезервировано | 1 A | Опционально; если присутствует — значение '0'. |
| Тип KCV | 1 A | Опционально. Метод вычисления проверочного значения ключа:<br>'0': 16-значный KCV (режим обратной совместимости, значение по умолчанию)<br>'1': 6-значный KCV |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'KB'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'04': Недопустимый тип ключа<br>'10': Нарушена четность ключа<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| KCV | 16/6 H | Результат зашифрования 64 бинарных нулей под ключом. Размер поля зависит от значения *Тип KCV*, указываемого в команде. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 27 Устаревшие команды обеспечения целостности сообщений

Для обеспечения целостности сообщений в HSM поддерживаются следующие устаревшие (legacy) команды хоста:

## [MS] — Генерация MAC (MAB) с использованием метода ANSI X9.19 для больших сообщений

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|

**Описание функции:** Генерация MAB для больших сообщений с использованием ключа TAK или ZAK.

**Примечания:**

Данная команда заменяется командой 'M6'.

Используемый алгоритм MAC — ANSI X9.19 с дополнением нулями.

Команда поддерживает работу с данными в бинарном и шестнадцатеричном форматах.

Если блок сообщения является первым или промежуточным (*Номер блока сообщения* = '1' или '2'), он должен быть кратен 8 байтам.

В случае вычисления MAC для сообщения, состоящего из нескольких блоков, промежуточные значения MAB будут зашифрованы под ключом, выработанным из ключа MAC.

При генерации MAC для нескольких блоков сообщения (если *Номер блока сообщения* = '1', '2' или '3') минимальная длина каждого блока сообщения 24 байта (бинарные/текстовые данные) или 48 шестнадцатеричных символов.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'MS'. |
| Номер блока сообщения | 1 N | Номер обрабатываемого блока сообщения:<br>'0': Единственный блок<br>'1': Первый блок<br>'2': Промежуточный блок<br>'3': Последний блок |
| Тип ключа | 1 N | '0': TAK<br>'1': ZAK |
| Длина ключа | 1 N | '1': 2DES |
| Тип данных сообщения | 1 N | '0': Бинарные<br>'1': Шестнадцатеричные |
| Ключ | 'U' + 32 H<br>или<br>'T' + 48 H | Ключ, зашифрованный под соответствующим LMK (TAK — под LMK 16-17, ZAK — под LMK 26-27). |
| IV | 16 H | Вектор инициализации. Присутствует только в случае *Номера блока сообщения* = '2' или '3'. |
| Длина блока сообщения | 4 H | В случае *Типа данных сообщения* = '0' (бинарные данные) — длина следующего поля.<br>В случае *Типа данных сообщения* = '1' (шестнадцатеричные данные) — половина длины следующего поля. |
| Блок сообщения | n B или n H | Блок данных сообщения в бинарном или шестнадцатеричном формате. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |

| | | |
|---|---|---|
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'MT'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Недопустимый тип данных сообщения<br>'04': Недопустимый тип ключа<br>'05': Недопустимый номер блока сообщения<br>'06': Недопустимая длина ключа<br>'68': Команда недоступна<br>или другой стандартный код ошибки. |
| MAB | 16 H | Если *Номер блока сообщения* = '1' или '2' — используется в качестве IV для следующего блока.<br>Если *Номер блока сообщения* = '0' или '3' — значение MAC. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# 28 Устаревшие команды UnionPay

Для поддержки операций с картами платежной системы UnionPay (CUP) в HSM поддерживаются следующие устаревшие (legacy) команды хоста:

| | |
|---|---|
| [JS] — Проверка ARQC и/или генерация ARPC (UnionPay) | 430 |
| [JU] — Генерация Secure Message (UnionPay) | 432 |

## [JS] — Проверка ARQC и/или генерация ARPC (UnionPay)

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|
| Авторизация: **Опционально (см. описание)** | |
| Активности: **diagnostic.host** | |

**Описание функции:** Проверка ARQC (или TC/AAC) и, опционально, генерация ARPC. Команда также может использоваться только для генерации ARPC.

**Примечания:** Данная команда заменяется командой 'KW'.

Для вывода диагностических данных требуется авторизованное состояние HSM.

Поле *Диагностические данные* содержит сгенерированное значение ARQC, которое возвращается хосту, если не прошла проверка переданного в команде значения ARQC.

В соответствии со спецификацией UnionPay (см. JR/T 0025.5-2010, приложение D.2) данные для вычисления ARQC должны быть дополнены. Если длина данных кратна 8 байтам, они дополняются в конце байтами 0x80 00 00 00 00 00 00 00. Если длина данных не кратна 8 байтам, данные дополняются в конце одним байтом 0x80 и байтами 0x00 (от 0 до 7) до длины, кратной 8 байтам.

Поле *Флаг дополнения* позволяет приложению контролировать, применяется ли описанная выше процедура дополнения к данным транзакции в команде.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'JS'. |
| Флаг режима | 1 H | '0': Только проверка ARQC<br>'1': Проверка ARQC и генерация ARPC<br>'2': Только генерация ARPC |
| Метод диверсификации ключа | 1 N | '1': CUP Card Key Derivation method (CUP ver. 4.2) |
| MK-AC | 'U' + 32 H | Мастер-ключ эмитента для формирования и проверки Application Cryptogram, зашифрованный под LMK 28-29/1. |
| Номер карты (PAN)/PAN Sequence Number | 8 B | Предварительно отформатированный PAN/PSN. |
| ATC | 2 B | Счетчик транзакций. |
| Флаг дополнения | 1 N | Признак применения процедуры дополнения к данным транзакции.<br>'0': входные данные транзакции не были дополнены и должны быть дополнены при обработке в команде<br>'1': входные данные транзакции были дополнены и должны быть кратны 8, процедура дополнения в команде не применяется |
| Длина данных транзакции | 2 H | Присутствует только в случае *Флага режима* = '0' или '1'.<br>Длина следующего поля. Допустимые значения: '01' .. 'FF'. |
| Данные транзакции | n B | Присутствует только в случае *Флага режима* = '0' или '1'.<br>Данные переменной длины. |
| Разделитель | 1 A | Значение ';'. Присутствует только в случае *Флага режима* = '0' или '1'.<br>Признак конца поля *Данные транзакции*. |
| ARQC/TC/AAC | 8 B | Проверяемое и/или используемое для генерации ARPC значение ARQC/TC/AAC. |

| | | |
|---|---|---|
| ARC | 2 B | Присутствует только в случае *Флага режима* = '1' или '2'.<br>Authorisation Response Code для генерации ARPC. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'JT'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'01': Ошибка проверки ARQC/TC/AAC (предупреждение)<br>'03': Некорректное значение флага дополнения<br>'04': Некорректное значение флага режима<br>'05': Некорректный метод диверсификации ключа<br>'10': Нарушена четность MK-AC<br>'68': Команда недоступна<br>'80': Ошибка длины данных<br>'82': Длина данных транзакции не кратна 8 байтам<br>или другой стандартный код ошибки. |
| APRC | 8 B | Присутствует только в случае *Флага режима* = '1', или '2' и отсутствия ошибки. Сгенерированное значение APRC. |
| Диагностические данные | 8 B | Присутствует только в случае *Кода ошибки* = '01' и если HSM находится в авторизованном состоянии. Сгенерированное значение ARQC/TC/AAC. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

## [JU] — Генерация Secure Message (UnionPay)

| Variant LMK ☑ | Key Block LMK ☒ |
|---|---|

**Описание функции:** Генерация сообщения (Secure Message) с обеспечением целостности для данных, передаваемых от эмитента обратно карте. Опционально, команда поддерживает обеспечение конфиденциальности при обмене сообщениями или при оффлайн изменении PIN.

**Примечания:** Данная команда заменяется командой 'KU'.

В соответствии со спецификацией UnionPay (см. JR/T 0025.5-2010, приложение C.2.4) данные для вычисления MAC должны быть дополнены. Если длина данных кратна 8 байтам, они дополняются в конце байтами 0x80 00 00 00 00 00 00 00. Если длина данных не кратна 8 байтам, данные дополняются в конце одним байтом 0x80 и байтами 0x00 (от 0 до 7) до длины, кратной 8 байтам.

Поле *Флаг дополнения* позволяет приложению контролировать, применяется ли описанная выше процедура дополнения к данным транзакции в команде.

| Параметр | Формат | Описание |
|---|---|---|
| **КОМАНДА** | | |
| Заголовок команды | m A | Должен быть возвращен хосту без изменений. |
| Код команды | 2 A | Значение 'JU'. |
| Флаг режима | 1 N | '0': Только целостность<br>'1': Целостность и конфиденциальность, с использованием одного мастер-ключа эмитента<br>'2': Целостность и конфиденциальность, с использованием разных мастер-ключей эмитента<br>'3': Целостность и конфиденциальность для изменения PIN, с использованием одного мастер-ключа эмитента.<br>'4': Целостность и конфиденциальность для изменения PIN, с использованием разных мастер-ключей эмитента. |
| Идентификатор схемы | 1 N | '1': CUP с использованием Card Key Derivation method (CUP ver. 4.2) |
| MK-SMI | 'U' + 32 H | Мастер-ключ эмитента для обеспечения целостности, зашифрованный под LMK 28-29/2. |
| Номер карты (PAN)/PAN Sequence Number | 8 B | Предварительно отформатированный PAN/PSN. |
| ATC | 2 B | Счетчик транзакций. |
| Флаг дополнения | 1 N | Признак применения процедуры дополнения к данным в поле *Незашифрованное сообщение*.<br>'0': входные данные сообщения не были дополнены и должны быть дополнены при обработке в команде<br>'1': входные данные сообщения были дополнены и должны быть кратны 8, процедура дополнения в команде не применяется |
| Длина незашифрованного сообщения | 4 H | Длина (в байтах) следующего поля. |
| Незашифрованное сообщение | n B | Данные сообщения, для которых вычисляется значение MAC. |
| Разделитель | 1 A | Значение ';'. |

| | | |
|---|---|---|
| MK-SMC | 'U' + 32 H | Присутствует только в случае *Флага режима* = '2' или '4'.<br>Мастер-ключ эмитента для обеспечения конфиденциальности, зашифрованный под LMK 28-29/3. |
| Смещение | 4 H | Присутствует только в случае *Флага режима* = '1', '2', '3' или '4'.<br>Смещение (в байтах) внутри *Незашифрованного сообщения* для вставки зашифрованного нового PIN-блока или результата зашифрования поля *Данные для зашифрования*.<br>Допустимые значения: 0000 .. *Длина незашифрованного сообщения*.<br>Если смещение = n, зашифрованные данные вставляются после n-го байта данных незашифрованного сообщения (т.е. если длина незашифрованного сообщения = 0039, и смещение = 39, зашифрованные данные располагаются в конце данных незашифрованного сообщения). |
| Следующие 3 поля присутствуют только в случае *Флага режима* = '1' или '2': | | |
| Длина данных для зашифрования | 4 H | Длина (в байтах) следующего поля. |
| Данные для зашифрования | n B | Данные для зашифрования. |
| Разделитель | 1 A | Значение ';'. |
| Следующие поля присутствуют только в случае *Флага режима* = '3' или '4': | | |
| Тип ключа шифрования исходного PIN-блока | 1 N | '0': ZPK<br>'1': TPK |
| Ключа шифрования исходного PIN-блока | 'U' + 32 H<br>или<br>'T' + 48 H | Ключ шифрования PIN-блока, зашифрованный под соответствующим LMK, определяемым значением поля *Тип ключа шифрования исходного PIN-блока*:<br>ZPK, зашифрованный под LMK 06-07/0<br>TPK, зашифрованный под LMK 14-15/0 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: No`) или LMK 36-37/7 (если выставлена настройка `Enforce key type 002 separation for PCI HSM compliance: Yes`). |
| Код формата исходного PIN-блока | 2 N | Код формата исходного PIN-блока. |
| Номер карты (PAN) | 12 N | 12 крайних правых цифр PAN, за исключением контрольной цифры. |
| Формат выходного PIN-блока | 1 N | '1': выходной PIN-блок с текущим (старым) PIN<br>'2': выходной PIN-блок без текущего (старого) PIN |
| Исходный новый PIN-блок | 16 H | Исходный новый PIN-блок. |
| Исходный текущий PIN-блок | 16 H | Присутствует только в случае *Формата выходного PIN-блока* = '1'.<br>Исходный текущий (старый) PIN-блок. |
| Разделитель | 1 A | Значение '%'. Опционально; если присутствует, следующее поле обязательно. |
| Идентификатор LMK | 2 N | Допустимые значения: '00' .. '09'.<br>Присутствует, только если присутствует предыдущее поле. |
| Символ конца команды | 1 C | Значение 0x19. Опционально. Должен присутствовать, если в команде передается трейлер. |
| Трейлер | n A | Опционально. Максимальная длина — 32 символа. |

| Параметр | Формат | Описание |
|---|---|---|
| **ОТВЕТ** | | |
| Заголовок ответа | m A | Заголовок команды, возвращаемый хосту без изменений. |
| Код ответа | 2 A | Значение 'JV'. |
| Код ошибки | 2 H | '00': Без ошибок<br>'03': Недопустимый флаг дополнения<br>'04': Недопустимый флаг режима<br>'05': Недопустимый идентификатор схемы<br>'06': Недопустимое значение смещения<br>'09': Нарушена четность ZPK/TPK<br>'10': Нарушена четность MK-SMI<br>'11': Нарушена четность MK-SMC<br>'23': Недопустимый код формата исходного PIN-блока<br>'50': Недопустимый тип ключа шифрования исходного PIN-блока<br>'51': Недопустимый формат выходного PIN-блока<br>'52': Недопустимый формат исходного нового PIN-блока<br>'53': Недопустимый формат исходного текущего PIN-блока<br>'80': Ошибка длины незашифрованного сообщения<br>'81': Ошибка длины данных для зашифрования<br>'82': Длина незашифрованного сообщения не кратна 8 байтам<br>или другой стандартный код ошибки. |
| MAC | 8 H | Вычисленное значение MAC. |
| Зашифрованный возвращаемый новый PIN-блок | 32 H | Присутствует только в случае *Флага режима* = '3' или '4'. |
| Следующие 2 поля присутствуют только в случае *Флага режима* = '1' или '2': | | |
| Длина зашифрованного сообщения | 4 H | Длина (в байтах) следующего поля. |
| Зашифрованное сообщение | n B | Зашифрованное сообщение. |
| Символ конца ответа | 1 C | Значение 0x19. Присутствует, только если присутствует в команде. |
| Трейлер | n A | Присутствует, только если присутствует в команде. Максимальная длина — 32 символа. |

# Приложение A Коды ошибок

В таблице приведены стандартные коды ошибок, которые HSM может возвращать хосту в случае ошибки выполнения команды.

Некоторые коды ошибок могут иметь несколько интерпретаций в зависимости от выполняемой команды хоста, в описании таких кодов возможные причины ошибки перечислены через "или".

Таблица 1. Коды ошибок

| Код | Описание ошибки |
|---|---|
| 00 | Без ошибки |
| 01 | Ошибка проверки (верификации) значения или предупреждение о нарушении четности импортированного ключа |
| 02 | Некорректная длина ключа для используемого алгоритма |
| 03 | Недопустимый тип закрытого ключа |
| 04 | Недопустимый тип ключа или ключ не соответствует правилам кодирования |
| 05 | Недопустимая длина ключа |
| 06 | Недопустимый идентификатор алгоритма подписи |
| 07 | Ошибка длины открытой экспоненты RSA |
| 08 | Недопустимое значение открытой экспоненты RSA |
| 10 | Нарушена четность исходного ключа |
| 11 | Нарушена четность целевого ключа или получен нулевой ключ |
| 12 | Содержимое пользовательского хранилища недоступно |
| 13 | Недопустимый идентификатор LMK |
| 14 | Недопустимый PIN, зашифрованный под LMK |
| 15 | Некорректные входные данные (некорректный формат, недопустимые символы или недостаточно данных) |
| 16 | Устройства вывода (консоль, принтер) не готовы или не подключены |
| 17 | Операция не авторизована или запрещена настройками безопасности |
| 18 | Формат документа не загружен |
| 20 | PIN-блок содержит недопустимые значения |
| 22 | Недопустимое значение PAN |
| 23 | Некорректный код формата PIN-блока (включая случаи применения настроек безопасности для реализации ограничений PCI HSM на использование PIN-блока в случае, когда команда пытается преобразовать PIN-блок в недопустимый формат) |
| 24 | Недопустимая длина PIN (меньше 4 или больше 12) |
| 25 | Ошибка таблицы децимализации |
| 26 | Некорректная ключевая схема |
| 27 | Несоответствующая длина ключа |
| 28 | Некорректный тип ключа |
| 29 | Недопустимая операция |
| 30 | Некорректный ссылочный номер (reference number) |
| 31 | Недостаточно записей запроса PIN для пакета |

| | |
|---|---|
| 33 | Хранилище смены ключей повреждено |
| 39 | Обнаружена PIN-атака |
| 41 | Внутренняя ошибка |
| 43 | Ошибка генерации ключа RSA |
| 48 | Ключ не может быть зашифрован под 3DES LMK |
| 49 | Ошибка закрытого ключа |
| 50 | Нулевой или слабый ключ |
| 68 | Команда недоступна |
| 69 | Формат PIN-блока недоступен |
| 74 | Недопустимый синтаксис digest info (только в режиме *Без хэширования*) |
| 75 | Попытка использования ключа DES как 2DES или 3DES |
| 76 | Некорректная длина открытого ключа RSA/зашифрованных данных или длина подписи/KEK не равна длине модуля открытого ключа |
| 77 | Ошибка расшифрованных данных |
| 78 | Ошибка длины закрытого ключа |
| 79 | Ошибка идентификатора объекта алгоритма хэширования |
| 80 | Ошибка длины данных (длина данных больше или меньше ожидаемого) |
| 81 | Недопустимый заголовок сертификата или длина подписи |
| 82 | Некорректная длина контрольной величины |
| 83 | Некорректный формат Key Block |
| 84 | Некорректное значение контрольной величины в Key Block |
| 85 | Недопустимое значение OAEP MGF |
| 86 | Недопустимая функция хэширования OAEP MGF |
| 87 | Ошибка OAEP Label |
| A1 | Несовместимые схемы LMK |
| A2 | Несовместимые идентификаторы LMK |
| A4 | Ошибка аутентификации Key Block |
| A5 | Несоответствующая длина ключа Key Block |
| A6 | Недопустимое использование ключа |
| A7 | Недопустимый алгоритм |
| A8 | Недопустимый режим использования |
| A9 | Недопустимый номер версии ключа |
| AA | Недопустимое значение экспортируемости |
| AB | Недопустимое количество опциональных блоков |
| B2 | Прочие ошибки Key Block |
| B5 | Несовместимые компоненты |
| B7 | Некорректное изменяемое поле |
| B8 | Некорректное старое значение |
| B9 | Некорректное новое значение |
| BA | Отсутствует блок статуса ключа |

| | |
|---|---|
| BB | Некорректный ключ шифрования ключа |
| BC | Повторяющийся опциональный блок |
| BD | Несовместимые типы ключей |
| BE | Недопустимый идентификатор заголовка Key Block |
| D3 | Сила ключа шифрования ключа меньше силы шифруемого ключа |
| | Специфические ошибки опциональных блоков заголовка |
| AC | Ошибка опционального блока |
| AD | Ошибка статуса ключа опционального блока |
| AE | Некорректная дата/время начала |
| AF | Некорректная дата/время окончания |
| B0 | Недопустимый режим шифрования |
| B1 | Недопустимый режим аутентификации |
| B3 | Некорректное количество опциональных блоков |
| B4 | Ошибка данных опционального блока |

# Приложение Б Настройки безопасности (security settings)

Как правило, по умолчанию значения настроек безопасности выставлены так, чтобы обеспечить максимально высокий уровень безопасности (за некоторыми исключениями, описанными ниже).

Для просмотра и изменения значений настроек безопасности используются следующие консольные команды:

• QS — Просмотр конфигурации безопасности
Команда выводит перечень доступных настроек безопасности и их текущие значения.

• CS — Настройка конфигурации безопасности
Команда устанавливает новые указанные значения для выбранных настроек и опционально сохраняет актуальные значения настроек на смарт-карту.

Таблица 2. Описание настроек безопасности

| **Название** | **Допустимые значения** | **Значение по умолчанию** |
|---|---|---|
| **ОБЩИЕ НАСТРОЙКИ** | | |
| **PIN length** | 4 .. 12 | 4 |
| Результат выполнения команд хоста, как правило, зависит от длины зашифрованного PIN (Encrypted PIN length). Длина зашифрованного PIN обозначается буквой "L" в поле **Формат** описаний команд хоста. Значение длины зашифрованного PIN: L = PIN length + 1. PIN в незашифрованном виде (передаваемый в команду хоста BA) должен иметь длину L; если длина PIN < L, он должен быть дополнен справа символами 0xF до длины L.<br>Например, если настройка `PIN length` имеет значение 6 (т.е., L = 7) и в команду BA необходимо передать 4-значный PIN = 1234, конечное отформатированное значение PIN, включаемое в команду — 1234FFF.<br>Все PIN, зашифрованные под DES LMK, имеют длину L.<br>При расшифровании PIN, зашифрованного под LMK, с использованием команды хоста NG, в полученном расшифрованном PIN дополнение символами 0xF необходимо удалить для получения значения PIN.<br>(!) Если значение настройки необходимо изменить (например, для возможности поддержки более длинных PIN), все существующие зашифрованные PIN должны быть транслированы.<br>Настройка безопасности влияет на выполнение следующих команд хоста: BA, BC, BE, BG, DE, DG, EE, JA, JC, JE, JG, NG, PE, PG, QC, QK. | | |
| **Atalla ZMK variant support** | On/Off | Off |
| Предназначена для взаимодействия с системами Atalla. Настройка позволяет включать дополнительные Atalla варианты в команды. При включенной настройке консольные команды управления ключами запросят Atalla вариант.<br>(!) Значение настройки не влияет на выполнение команд хоста, Atalla варианты могут передаваться в любой соответствующей команде независимо от значения настройки.<br>Настройка безопасности влияет на выполнение следующих консольных команд: IK, KE, KG.<br>Настройка безопасности влияет на выполнение следующих команд хоста: A6, FA (см. описание настройки `Enforce Atalla variant match to variant key type`). | | |

| | | |
|---|---|---|
| **Default LMK identifier** | 0 .. 9 | 0 |
| Определяет идентификатор LMK по умолчанию. Использование LMK по умолчанию позволяет не указывать каждый раз идентификатор LMK в командах хоста, даже если в HSM загружено несколько LMK. Максимальное значение (9) определяется количеством LMK, которые могут быть загружены в HSM одновременно. | | |
| **Enforce legacy RSA key format under Variant LMK** | Yes/No | No |
| Если настройка включена, закрытые ключи RSA, зашифрованные под Variant LMK, хранятся в legacy формате. | | |
| **Enforce legacy proprietary HMAC key format under Variant LMK/ZMK** | Yes/No | No |
| Если настройка включена, ключи HMAC, зашифрованные под Variant LMK или ZMK в формате '00' (проприетарный формат), хранятся в legacy формате. | | |
| **Enforce legacy PIN encryption algorithm A** | Yes/No | No |
| Настройка действительна, только если ранее была выставлена настройка `PIN encryption algorithm: A` (см. ниже).<br>Если настройка включена, PIN, зашифрованные эмитентом, хранятся в legacy формате.<br>Настройка безопасности влияет на выполнение следующих команд хоста: BA, BC, BE, BG, DE, DG, EE, JA, JC, JE, JG, NG, PE, PG, QC, QK. | | |
| **Enforce legacy AES PIN encryption algorithm** | Yes/No | No |
| Если настройка включена, PIN, зашифрованные эмитентом под AES LMK, хранятся в legacy формате, и вместо формата 'M' + 32 H используется 'J' + 32 H.<br>Настройка безопасности влияет на выполнение следующих команд хоста: BA, BC, BE, BG, DE, DG, EE, JA, JC, JE, JG, NG, PE, PG, QC, QK. | | |
| **Enforce Authorization** | Yes/No | No |
| Если настройка включена, то для выполнения некоторых команд требуется авторизация.<br>Если настройка выключена, то для выполнения команд авторизация не требуется. | | |
| **Enable multiple authorized activities** | Yes/No | No |
| Настройка действительна, только если ранее была выставлена настройка `Enforce Authorization: Yes`.<br>Если настройка включена, то доступна точечная настройка авторизованных действий (включая длительность действия авторизации).<br>Если настройка выключена, то HSM переходит в авторизованное состояние.<br>При смене значения настройки все текущие авторизации удаляются. | | |
| **НАЧАЛЬНЫЕ НАСТРОЙКИ** | | |
| **Enforce Atalla variant match to variant key type** | Yes/No | No |
| Настройка действительна, только если ранее была выставлена настройка `Atalla ZMK variant support: Yes`.<br>Если настройка включена, принудительно проверяется соответствие между Atalla вариантом и типом ключа Variant.<br>Настройка безопасности влияет на выполнение следующих консольных команд: IK.<br>Настройка безопасности влияет на выполнение следующих команд хоста: A6, FA. | | |

| **Select clear PINs** | Yes/No | No |
|---|---|---|
| Настройка позволяет включить поддержку расшифрования PIN.<br>ⓘ ИСПОЛЬЗОВАНИЕ КОМАНДЫ СОПРОВОЖДАЕТСЯ ЗНАЧИТЕЛЬНЫМИ РИСКАМИ ИБ, ЕСЛИ НЕ ПРЕДПРИНЯТЫ СООТВЕТСТВУЮЩИЕ МЕРЫ БЕЗОПАСНОСТИ НА ХОСТЕ.<br>Настройка безопасности влияет на выполнение следующих команд хоста: NG. | | |
| **Encrypt clear PINs** | Yes/No | No |
| Настройка позволяет включить поддержку зашифрования PIN.<br>ⓘ ИСПОЛЬЗОВАНИЕ КОМАНДЫ СОПРОВОЖДАЕТСЯ ЗНАЧИТЕЛЬНЫМИ РИСКАМИ ИБ, ЕСЛИ НЕ ПРЕДПРИНЯТЫ СООТВЕТСТВУЮЩИЕ МЕРЫ БЕЗОПАСНОСТИ НА ХОСТЕ.<br>Настройка безопасности влияет на выполнение следующих команд хоста: BA. | | |
| **Enable ZMK translate command** | Yes/No | No |
| Настройка позволяет включить поддержку трансляции ZMK, зашифрованного под другим ZMK.<br>ⓘ ИСПОЛЬЗОВАНИЕ КОМАНДЫ СОПРОВОЖДАЕТСЯ ЗНАЧИТЕЛЬНЫМИ РИСКАМИ ИБ.<br>Настройка безопасности влияет на выполнение следующих команд хоста: BY. | | |
| **Enable X9.17 for import** | Yes/No | No |
| Настройка позволяет включить поддержку импорта ключей в соответствии с ANSI X9.17. При импорте каждый ключ 2DES или 3DES зашифрован отдельно с использованием режима шифрования ECB.<br>ⓘ Опция снижает уровень безопасности, настоятельно рекомендуется использовать X9 TR-31 Key Block вместо X9.17.<br>Настройка безопасности влияет на выполнение следующих консольных команд: IK.<br>Настройка безопасности влияет на выполнение следующих команд хоста: A6, BY, FA. | | |
| **Enable X9.17 for export** | Yes/No | No |
| Аналогична предыдущей настройке применительно к экспорту ключей.<br>Настройка безопасности влияет на выполнение следующих консольных команд: KE, KG.<br>Настройка безопасности влияет на выполнение следующих команд хоста: A0, A8, HA, AE, AG, FE. | | |
| **Solicitation batch size** | 1 .. 1024 | 1024 |
| Определяет минимальное количество запросов (ссылочный номер и выбранный PIN), включаемых в один пакет. Следует избегать использования маленьких размеров пакета, чтобы не допустить соответствия ссылочного номера и номера карты (PAN).<br>Настройка безопасности влияет на выполнение следующих команд хоста: QC. | | |
| **Decimalization tables** | Encrypted/Plaintext | Encrypted |
| Настройка определяет формат таблицы децимализации — зашифрованная или незашифрованная. Рекомендуется использовать зашифрованные таблицы децимализации.<br>Настройка безопасности влияет на выполнение следующих команд хоста: BK, DA, DE, DU, EA, EE, GO. | | |

| | | |
|---|---|---|
| **Enable decimalization table checks** | Yes/No | Yes |
| Настройка предназначена для управления проверкой таблиц децимализации. Как правило, на значения в таблице децимализации накладываются ограничения с целью исключения потенциально небезопасных значений для обеспечения дополнительной безопасности.<br>Настройка безопасности влияет на выполнение следующих консольных команд: ED, TD.<br>Настройка безопасности влияет на выполнение следующих команд хоста: BK, DA, DE, DU, EA, EE, GO, LO. | | |
| **PIN encryption algorithm** | A/B | A |
| Определяет алгоритм зашифрования PIN, используемый в случае хранения зашифрованных PIN эмитентом.<br>В случае схемы B результат шифрования представлен в шестнадцатеричном виде, в случае схемы A — в десятичном.<br>Команды, взаимодействующие с зашифрованными PIN, обозначают их как "L N или L H".<br>Настройка безопасности влияет на выполнение следующих команд хоста: BA, BC, BE, BG, DE, DG, EE, JA, JC, JE, JG, NG, PE, PG, QC, QK. | | |
| **Minimum HMAC length in bytes** | 5..64 | 10 |
| Определяет минимальную длину HMAC, который может генерировать или проверять HSM.<br>Настройка безопасности влияет на выполнение следующих команд хоста: LQ, LS. | | |
| **Enable PKCS#11 import and export for HMAC keys** | Yes/No | No |
| Настройка определяет возможность импорта и экспорта ключей HMAC из/в формат PKCS#11.<br>Настройка безопасности влияет на выполнение следующих команд хоста: LU, LW. | | |
| **Enable ANSI X9.17 import and export for HMAC keys** | Yes/No | No |
| Настройка определяет возможность импорта и экспорта ключей HMAC из/в формат ANSI X9.17.<br>Настройка безопасности влияет на выполнение следующих команд хоста: LU, LW. | | |
| **Enable ZEK/TEK encryption of ASCII data or Binary data or None** | ASCII/Binary/None | None |
| Определяет тип данных, которые могут быть зашифрованы/расшифрованы/транслированы (с использованием ZEK или TEK) с помощью команд шифрования сообщений:<br>• ASCII: незашифрованное сообщение должно содержать только ASCII-символы (0x20-0x7F);<br>• Binary: ограничения на формат сообщения не накладываются;<br>• None: зашифрование с использованием ZEK или TEK не допускается.<br>Настройка безопасности влияет на выполнение следующих команд хоста: M0, M2, M4. | | |
| **Restrict Key Check Values to 6 hex chars** | Yes/No | Yes |
| Настройка позволяет ограничить значение KCV шестью шестнадцатеричными символами. Общая длина поля KCV не зависит от значения настройки. В случае значения "Yes" только первые 6 символов параметра KCV содержат проверочное значение ключа, остальные символы игнорируются (если KCV является входным параметром) или устанавливаются в '0' (если KCV является выходным параметром).<br>Настройка влияет на KCV только при использовании Variant LMK. В случае Key Block LMK KCV всегда содержит 6 символов.<br>Настройка безопасности влияет на выполнение следующих консольных команд: CK.<br>Настройка безопасности влияет на выполнение следующих команд хоста: BU, GI, GK, KI, FE, FA, KA. | | |

| **Enable variable length PIN offset** | Yes/No | No |
|---|---|---|
| Позволяет настроить длину PIN Offset. Если настройка включена, длина генерируемого IBM 3624 PIN Offset соответствует длине входного PIN. В противном случае длина Offset определяется значением параметра *Проверочная длина*.<br>Настройка безопасности влияет на выполнение следующих команд хоста: BK, DE, DU. | | |
| **Enable weak PIN checking** | Yes/No | No |
| Позволяет настроить проверку слабых PIN. Если настройка включена, в командах генерации/выработки PIN будет выполняться проверка нового PIN на наличие в списках «слабых» PIN и на соответствие правилам.<br>Метод проверки силы PIN выбирается в соответствии с настройками ниже.<br>Настройка безопасности влияет на выполнение следующих команд хоста: BK, CU, DU, EE, FW, JA. | | |
| Если выставлена настройка `Enable weak PIN checking: Yes`, следующие 3 настройки определяют порядок проверки PIN: | | |
| **Check new PINs using global list of weak PINs** | Yes/No | No |
| Если настройка включена, команды генерации/выработки PIN проверяют наличие нового PIN в глобальном списке «слабых» PIN (загруженного в HSM с помощью команды BM). Если PIN присутствует в списке, возвращается код ошибки '86'.<br>Если настройка выключена, при генерации/выработке PIN наличие PIN в глобальном списке «слабых» PIN не проверяется. | | |
| **Check new PINs using local list of weak PINs** | Yes/No | No |
| Если настройка включена, команды генерации/выработки PIN проверяют наличие нового PIN в локальном списке «слабых» PIN (передаваемого в команде). Если PIN присутствует в списке, возвращается код ошибки '86'.<br>Если настройка выключена, при генерации/выработке PIN наличие PIN в локальном списке «слабых» PIN не проверяется. | | |
| **Check new PINs using rules** | Yes/No | No |
| Если настройка включена, команды генерации/выработки PIN проверяют PIN по правилам ниже.<br>PIN считается слабым, если выполняется хотя бы одно из следующих условий:<br>• больше 50% символов PIN имеют одинаковое значение (например, 1111, 0111, 1101);<br>• PIN целиком состоит из последовательно идущих десятичных цифр (например, 1234, 5432). | | |
| **Enable PIN Block Format 34 as output format for PIN translations to ZPK** | Yes/No | No |
| Если настройка включена, допускается использование формата PIN-блока 34 в качестве возвращаемого в командах трансляции PIN.<br>Настройка безопасности влияет на выполнение следующих команд хоста: CA, CC, JG, G0. | | |
| **Enable translation of account number for LMK encrypted PINs** | Yes/No | No |
| Если настройка включена, допускается трансляция номера карты (PAN) для PIN, зашифрованного под LMK, без изменения самого PIN.<br>Настройка безопасности влияет на выполнение следующих команд хоста: QK. | | |

| **Use HSM clock for date/time validation** | Yes/No | Yes |
|---|---|---|
| Если настройка включена, HSM использует встроенные часы для проверки даты/времени в опциональных блоках заголовка Key Block (если указаны). | | |
| **Additional padding to disguise key length** | Yes/No | No |
| Если настройка включена, HSM маскирует длину ключей 2DES в формате Key Block, добавляя 8 байтов дополнения, таким образом, все ключи 2DES неотличимы от ключей 3DES. | | |
| **Key export and import in trusted format only** | Yes/No | Yes |
| Если настройка включена, допускается импорт/экспорт ключей только из/в формат Key Block. В этом случае импорт/экспорт ключей из/в формат Variant (включая X9.17) запрещен.<br>Настройка безопасности влияет на выполнение следующих консольных команд: IK, KE, KG.<br>Настройка безопасности влияет на выполнение следующих команд хоста: A0, A6, A8, BY, L6, L8, HA, AE, AG, FE, FA. | | |
| **Enable use of Tokens in PIN Translation** | Yes/No | No |
| Позволяет настроить поддержку в командах трансляции PIN трансляции PIN-блока, сформированного с использованием токена (указывается в поле *Исходный PAN*), путем использования дополнительного поля *Целевой PAN* для возвращаемого PIN-блока.<br>Настройка безопасности влияет на выполнение следующих команд хоста: AQ, CA, CC, G0. | | |
| **Enable use of Tokens in PIN Verification** | Yes/No | No |
| Позволяет настроить поддержку в командах проверки PIN проверки PIN-блока, сформированного с использованием токена вместо настоящего номера карты (PAN), путем использования дополнительного поля *Номер карты (PAN)*.<br>Настройка безопасности влияет на выполнение следующих команд хоста: EC, GQ. | | |
| **Ignore LMK ID in Key Block Header** | Yes/No | No |
| Если настройка включена, идентификатор LMK в заголовке Проприетарного Key Block (байты 14-15) игнорируется. Вместо этого HSM использует тот же механизм получения идентификатора LMK, что и в случае использования Variant LMK — путем указания идентификатора LMK в команде.<br>Если настройка выключена (значение по умолчанию), для определения LMK, который необходимо использовать в команде, будет использоваться идентификатор LMK в заголовке Проприетарного Key Block. | | |
| **Enable import and export of RSA Private keys** | Yes/No | No |
| Если настройка включена, импорт и экспорт закрытых ключей RSA разрешен. В противном случае, соответствующие команды хоста сразу возвращают код ошибки '03'.<br>Настройка безопасности влияет на выполнение следующих команд хоста: L6, L8. | | |
| **Enable import of a ZMK** | Yes/No | No |
| Если настройка включена, команды импорта симметричных ключей поддерживают импорт ZMK.<br>Если настройка выключена, команды импорта поддерживают импорт ключей ZMK только из форматов Key Block.<br>Настройка безопасности влияет на выполнение следующих консольных команд: IK.<br>Настройка безопасности влияет на выполнение следующих команд хоста: A6, BY, GI. | | |

| | | |
|---|---|---|
| **Enable export of a ZMK** | Yes/No | No |

Если настройка включена, команды экспорта симметричных ключей поддерживают экспорт ZMK.

Настройка безопасности влияет на выполнение следующих консольных команд: KE, KG.

Настройка безопасности влияет на выполнение следующих команд хоста: A0, A8, B8, GK.

**НАСТРОЙКИ, ВЛИЯЮЩИЕ НА СООТВЕТСТВИЕ PCI HSM**

Следующие настройки безопасности влияют на соответствие PCI HSM.

Если все настройки ниже имеют значения, соответствующие PCI HSM, изменение значения любой из этих настроек недоступно без очистки содержимого HSM и сброса к заводским настройкам.

| | | |
|---|---|---|
| **Prevent single-DES keys masquerading as double or triple-length keys** | Yes/No | Yes |

Если настройка включена, HSM отслеживает и не допускает применение ключей DES, используемых как 2DES или 3DES.

Для работы в режиме совместимости с PCI HSM настройка должна иметь значение "Yes".

| | | |
|---|---|---|
| **Restrict PIN block usage for PCI HSM Compliance** | Yes/No | No |

Если настройка включена, HSM ограничивает доступные форматы PIN-блоков при трансляции PIN (подробнее см. раздел «Трансляция PIN-блоков» в «КриптоПро HSM. Руководство программиста».)

Если настройка включена, HSM не допустит трансляцию PIN-блока из формата ISO 0, 1, 3 и 4 (соответствующие кодам форматов 01, 05, 47 и 48) в любой формат, отличный от ISO. Также недоступна трансляция PIN-блоков из форматов, включающих PAN, в форматы, не включающие PAN. При трансляции PIN-блоков из одного формата в другой, оба из которых включают PAN, не допускается изменение значения PAN.

Кроме того, вычисление значений, вырабатываемых из значений PIN и PAN (например, PIN Offset и PVV), доступно только для форматов PIN-блока, включающих PAN.

Для работы в режиме совместимости с PCI HSM настройка должна иметь значение "Yes".

Настройка безопасности влияет на выполнение следующих команд хоста: AQ, BK, CA, CC, CU, DU, FW, G0, JC, JE, JG.

| | | |
|---|---|---|
| **Enforce key type 002 separation for PCI HSM compliance** | Yes/No | No |

Если настройка включена, HSM разделяет ключи, зашифрованные под LMK 14-15 (тип ключа 002).

Для работы в режиме совместимости с PCI HSM настройка должна иметь значение "Yes".

Если настройка включена, следующие команды недоступны: AE, FE, KA, OE.

| | | |
|---|---|---|
| **Enforce Multiple Key Components** | Yes/No | Yes |

Если настройка включена, все LMK и ключи, формируемые в HSM, могут быть сформированы только из 2 и более ключевых компонент.

Для работы в режиме совместимости с PCI HSM настройка должна иметь значение "Yes".

Настройка безопасности влияет на выполнение следующих консольных команд: FK, LK, LN, LO.

| | | |
|---|---|---|
| **Enforce PCI HSMv3 Key Equivalence for Key Wrapping** | Yes/No | Yes |

Если настройка включена, не допускается использовать ключ RSA с меньшей силой для зашифрования симметричного ключа с большей силой, а также симметричный ключ с меньшей силой (LMK или ZMK) для зашифрования или расшифрования ключа RSA с большей силой (подробнее о силе ключа см. NIST SP800-57).

Если настройка включена, не допускается использовать симметричный ключ с меньшей силой для зашифрования ключа ECC с большей силой, а также вырабатывать симметричный ключ с силой большей, чем у исходных ключей ECC.

Для работы в режиме совместимости с PCI HSM настройка должна иметь значение "Yes".

| | | |
|---|---|---|
| **Enforce minimum key strength of 1024-bits for RSA signature verification** | Yes/No | Yes |

Если настройка включена, не допускается проверка подписи RSA с использованием ключа длиной меньше 1024 бит.

Для работы в режиме совместимости с PCI HSM настройка должна иметь значение "Yes".

Настройка безопасности влияет на выполнение следующих команд хоста: EY, ES, GI, JY, KG.

| | | |
|---|---|---|
| **Enforce minimum key strength of 2048-bits for RSA** | Yes/No | Yes |

Если настройка включена, операции RSA (генерация и проверка подписи, зашифрование и расшифрование) с использованием ключа длиной меньше 2048 бит недоступны.

Настройка не влияет на минимальный размер ключей в командах выпуска карт.

Для работы в режиме совместимости с PCI HSM настройка должна иметь значение "Yes".

Настройка безопасности влияет на выполнение следующих команд хоста: AQ, B8, ES, EW, EY, GI, GK, JW, JY, QE.

# Приложение B Форматы сертификатов

Данные в сертификатах должны быть представлены в виде байтов, каждый байт содержит 2 шестнадцатеричные цифры '0'-'F'.

Данные могут быть представлены двумя способами:

1. с выравниванием по правому краю, при необходимости дополнены слева символами '0'
2. с выравниванием по левому краю, при необходимости дополнены справа символами 'F'

## Принятые обозначения

e — экспонента открытого ключа

N — модуль открытого ключа

Для обозначения принадлежности открытого ключа используются индексы (ниже приведены примеры для модуля (N), для экспоненты (e) аналогично):

| Обозначение | Длина | Описание |
|---|---|---|
| $N_{CA}$ | $LN_{CA}$ | модуль открытого ключа Удостоверяющего центра |
| $N_I$ | $LN_I$ | модуль открытого ключа эмитента |
| $N_I^R$ | $LN_I^R$ | остаток (Remainder) модуля открытого ключа эмитента |
| $N_{IC}$ | $LN_{IC}$ | модуль открытого ключа карты (ICC) |
| $N_{PE}$ | $LN_{PE}$ | модуль открытого ключа карты (ICC) для шифрования PIN |

## Формат запроса сертификата эмитента (Visa)

### Формат данных, неподписываемых закрытым ключом эмитента

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '22' |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов |
| Модуль открытого ключа эмитента ($N_I$) | n B | Модуль открытого ключа эмитента |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) |
| Tracking Number | 3 B | Значение из регистрационной формы Visa Financial Institution, выровненное по правому краю и при необходимости дополненное слева нулями |

**Формат данных, подписываемых закрытым ключом эмитента**

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '23' | да |
| Идентификатор сервиса | 4 B | Идентификатор сервиса Visa (Proprietary Application Identifier Extension (PIX)), выровненный по левому краю и дополненный справа '0000' | да |
| Формат сертификата | 1 B | Значение '02' | да |
| Идентификатор эмитента | 4 B | Крайние левые 3-8 цифр PAN, выровненные по левому краю и дополненные справа символами 'F' | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Tracking Number | 3 B | Значение из регистрационной формы Visa Financial Institution, выровненное по правому краю и при необходимости дополненное слева нулями | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа эмитента | да |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) | да |
| Крайние левые байты модуля открытого ключа эмитента ($N_I$) | n B | $LN_I$ - (39 + $Le_I$) наиболее значимых байтов модуля открытого ключа эмитента | да |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа эмитента и связанной с ним информации | нет |

## Формат запроса сертификата эмитента (Mastercard)

### Формат данных, неподписываемых закрытым ключом эмитента

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Идентификатор эмитента | 4 B | Крайние левые 3-8 цифр PAN, выровненные по левому краю и дополненные справа символами 'F' | нет |
| Индекс открытого ключа эмитента | 3 B | Номер, выбранный эмитентом, однозначно идентифицирующий открытый ключ, выровненный по правому краю и дополненный слева нулями | нет |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа эмитента | нет |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов | нет |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) | нет |
| Крайние левые байты модуля открытого ключа эмитента ($N_I$) | n B | $LN_I$ - 36 наиболее значимых байтов модуля открытого ключа эмитента | нет |
| Остаток модуля открытого ключа эмитента ($N_I^R$) | 36 B | 36 наименее значимых байтов модуля открытого ключа эмитента | да |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) | да |

**Формат данных, подписываемых закрытым ключом эмитента**

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '6A' | нет |
| Формат сертификата | 1 B | Значение '11' | да |
| Идентификатор эмитента | 4 B | Крайние левые 3-8 цифр PAN, выровненные по левому краю и дополненные справа символами 'F' | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Серийный номер сертификата | 3 B | Выбирается эмитентом, выровнен по правому краю и дополнен слева нулями | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа эмитента | да |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) | да |
| Крайние левые байты модуля открытого ключа эмитента ($N_I$) | n B | $LN_I$ - 36 наиболее значимых байтов модуля открытого ключа эмитента | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа эмитента и связанной с ним информации | нет |
| Трейлер | 1 B | Значение 'BC' | нет |

## Формат запроса сертификата эмитента (American Express)

### Формат данных, неподписываемых закрытым ключом эмитента

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '22' |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов |
| Модуль открытого ключа эмитента ($N_I$) | n B | Модуль открытого ключа эмитента |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) |
| Tracking Number | 3 B | Номер для отслеживания, выровненный по правому краю и при необходимости дополненный слева нулями |

**Формат данных, подписываемых закрытым ключом эмитента**

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '23' | да |
| Идентификатор сервиса | 4 B | American Express Product Identifier | да |
| Формат сертификата | 1 B | Значение '02' | да |
| Идентификатор эмитента (BIN) | 4 B | Идентификационный номер эмитента, выровненный по левому краю и дополненный справа символами 'F' | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Tracking Number | 3 B | Номер для отслеживания, выровненный по правому краю и при необходимости дополненный слева нулями | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа эмитента | да |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) | да |
| Крайние левые байты модуля открытого ключа эмитента ($N_I$) | n B | $LN_I$ - (39 + $Le_I$) наиболее значимых байтов модуля открытого ключа эмитента | да |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) | да |
| Хэш-значение | 20 B | Значение хэш-функции от указанных полей | нет |

## Формат запроса сертификата эмитента (Мир)

### Формат данных, неподписываемых закрытым ключом эмитента

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '22' |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов |
| Модуль открытого ключа эмитента ($N_I$) | n B | Модуль открытого ключа эмитента |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) |
| Tracking Number | 3 B | Уникальный номер запроса сертификата в системе эмитента, выровненный по правому краю и при необходимости дополненный слева нулями |

**Формат данных, подписываемых закрытым ключом эмитента**

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '23' | да |
| Идентификатор сервиса | 4 B | Идентификатор приложения. Присваивается в соответствии с документом «ТРЕБОВАНИЯ К ПЛАТЕЖНОЙ КАРТЕ МИР» | да |
| Формат сертификата | 1 B | Значение '02' | да |
| Идентификатор эмитента | 4 B | Крайние левые 3-8 цифр PAN, выровненные по левому краю и дополненные справа символами 'F' | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Tracking Number | 3 B | Уникальный номер запроса сертификата в системе эмитента, выровненный по правому краю и при необходимости дополненный слева нулями | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа эмитента | да |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) | да |
| Крайние левые байты модуля открытого ключа эмитента ($N_I$) | n B | $LN_I$ - (39 + $Le_I$) наиболее значимых байтов модуля открытого ключа эмитента | да |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа эмитента и связанной с ним информации | нет |

## Формат сертификата эмитента (Visa)

### Формат данных, неподписываемых УЦ

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '24' | нет |
| Идентификатор сервиса | 4 B | Идентификатор сервиса Visa (Proprietary Application Identifier Extension (PIX)), выровненный по левому краю и дополненный справа '0000' | нет |
| Идентификатор эмитента | 4 B | Крайние левые 3-8 цифр PAN, выровненные по левому краю и дополненные справа символами 'F' | нет |
| Серийный номер сертификата | 3 B | Назначается УЦ Visa | нет |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | нет |
| Длина остатка модуля открытого ключа эмитента ($LN_I^R$) | 1 B | Количество байтов | нет |
| Остаток модуля открытого ключа эмитента ($N_I^R$) | n B | Присутствует, только если $LN_I > LN_{CA}$ - 36; $LN_I$ - $LN_{CA}$ + 36 наименее значимых байтов модуля открытого ключа эмитента<br>$N_{CA}$ — длина в байтах ключа УЦ VSDC, используемого для создания сертификата открытого ключа эмитента | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) | нет |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) | да |
| Индекс открытого ключа УЦ | 1 B | Индекс открытого ключа УЦ | нет |

**Формат данных, подписываемых УЦ**

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '6A' | нет |
| Формат сертификата | 1 B | Значение '02' | да |
| Идентификатор эмитента | 4 B | Крайние левые 3-8 цифр PAN, выровненные по левому краю и дополненные справа символами 'F' | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Серийный номер сертификата | 3 B | Уникальный номер, назначается УЦ | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа эмитента | да |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов | да |
| Модуль открытого ключа эмитента ($N_I$) или его крайние левые байты | n B | В случае $LN_I \leq LN_{CA}$ - 36 поле содержит модуль открытого ключа эмитента, выровненный по левому краю и дополненный справа $LN_{CA}$ - 36 - $LN_I$ байтами 'BB'<br>В случае $LN_I > LN_{CA}$ - 36 поле содержит $LN_{CA}$ - 36 наиболее значимых байтов модуля открытого ключа эмитента | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа эмитента и связанной с ним информации | нет |
| Трейлер | 1 B | Значение 'BC' | нет |

**Формат присоединенной подписи, генерируемой УЦ**

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '00' |
| Код формата блока | 1 B | Значение '01' |
| Символы дополнения | n B | Значение 'FF'. Длина дополнения = $LN_{CA}$ - 38 |
| Разделитель | 1 B | Значение '00' |
| Идентификатор алгоритма хэширования | 15 B | Идентификатор алгоритма хэширования, используемого УЦ |
| Хэш-значение | 20 B | Значение хэш-функции от конкатенации данных, неподписываемых УЦ, и данных открытого ключа эмитента, подписываемых УЦ |

## Формат сертификата эмитента (Mastercard)

### Формат данных, неподписываемых УЦ

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Идентификатор эмитента | 4 B | Крайние левые 3-8 цифр PAN, выровненные по левому краю и дополненные справа символами 'F' | нет |
| Индекс открытого ключа эмитента | 3 B | Номер, выбранный эмитентом, однозначно идентифицирующий открытый ключ | нет |
| Индекс открытого ключа УЦ | 1 B | Номер, однозначно идентифицирующий открытый ключ УЦ | нет |
| Остаток модуля открытого ключа эмитента ($N_I^R$) | n B | Присутствует, только если $LN_I > LN_{CA}$ - 36; $LN_I$ - $LN_{CA} + 36$ наименее значимых байтов модуля открытого ключа эмитента | да |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) | да |

**Формат данных, подписываемых УЦ**

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '6A' | нет |
| Формат сертификата | 1 B | Значение '02' | да |
| Идентификатор эмитента | 4 B | Крайние левые 3-8 цифр PAN, выровненные по левому краю и дополненные справа символами 'F' | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Серийный номер сертификата | 3 B | Уникальный номер, назначается УЦ | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа эмитента | да |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов | да |
| Модуль открытого ключа эмитента ($N_I$) или его крайние левые байты | n B | В случае $LN_I \leq LN_{CA}$ - 36 поле содержит модуль открытого ключа эмитента, выровненный по левому краю и дополненный справа $LN_{CA}$ - 36 - $LN_I$ байтами 'BB'<br>В случае $LN_I > LN_{CA}$ - 36 поле содержит $LN_{CA}$ - 36 наиболее значимых байтов модуля открытого ключа эмитента | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа эмитента и связанной с ним информации | нет |
| Трейлер | 1 B | Значение 'BC' | нет |

## Формат сертификата эмитента (American Express)

### Формат данных, неподписываемых УЦ

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '24' | нет |
| Идентификатор сервиса | 4 B | American Express Product Identifier | нет |
| Идентификатор эмитента | 4 B | Идентификационный номер эмитента, выровненный по левому краю и дополненный справа символами 'F' | нет |
| Серийный номер сертификата | 3 B | В формате '01nnnn', где nnnn — Tracking Number из запроса на сертификат | нет |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | нет |
| Длина остатка модуля открытого ключа эмитента ($LN_I^R$) | 1 B | Количество байтов | нет |
| Остаток модуля открытого ключа эмитента ($N_I^R$) | n B | Присутствует, только если $LN_I > LN_{CA}$ - 36; $LN_I - LN_{CA} + 36$ наименее значимых байтов модуля открытого ключа эмитента | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) | нет |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) | да |
| Индекс открытого ключа УЦ | 1 B | Индекс открытого ключа УЦ | нет |

**Формат данных, подписываемых УЦ**

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '6A' | нет |
| Формат сертификата | 1 B | Значение '02' | да |
| Идентификатор эмитента | 4 B | Идентификационный номер эмитента, выровненный по левому краю и дополненный справа символами 'F' | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Серийный номер сертификата | 3 B | В формате '01nnnn', где nnnn — Tracking Number из запроса на сертификат | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа эмитента | да |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов | да |
| Модуль открытого ключа эмитента (его крайние левые байты) ($N_I$) | n B | В случае $LN_I > LN_{CA}$ - 36 поле содержит $LN_{CA}$ - 36 наиболее значимых байтов модуля открытого ключа эмитента<br>В случае $LN_I \leq LN_{CA}$ - 36 поле содержит модуль открытого ключа эмитента, выровненный по левому краю и дополненный справа $LN_{CA}$ - 36 - $LN_I$ байтами 'BB' | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа эмитента и связанной с ним информации | нет |
| Трейлер | 1 B | Значение 'BC' | нет |

**Формат присоединенной подписи, генерируемой УЦ**

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '00' |
| Код формата блока | 1 B | Значение '01' |
| Символы дополнения | n B | Значение 'FF'. Длина дополнения = $LN_{CA}$ - 38 |
| Разделитель | 1 B | Значение '00' |
| Идентификатор алгоритма хэширования | 15 B | Идентификатор алгоритма хэширования, используемого УЦ |
| Хэш-значение | 20 B | Значение хэш-функции от конкатенации данных, неподписываемых УЦ, и данных открытого ключа эмитента, подписываемых УЦ |

## Формат сертификата эмитента (Мир)

### Формат данных, неподписываемых УЦ

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '24' | нет |
| Идентификатор сервиса | 4 B | Идентификатор приложения. Присваивается в соответствии с документом «ТРЕБОВАНИЯ К ПЛАТЕЖНОЙ КАРТЕ МИР» | нет |
| Идентификатор эмитента | 4 B | Крайние левые 3-8 цифр PAN, выровненные по левому краю и дополненные справа символами 'F' | нет |
| Серийный номер сертификата | 3 B | Уникальный номер сертификата ключа эмитента | нет |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | нет |
| Длина остатка модуля открытого ключа эмитента ($LN_I^R$) | 1 B | Количество байтов | нет |
| Остаток модуля открытого ключа эмитента ($N_I^R$) | n B | Присутствует, только если $LN_I > LN_{CA}$ - 36; $LN_I - LN_{CA} + 36$ наименее значимых байтов модуля открытого ключа эмитента | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) | нет |
| Экспонента открытого ключа эмитента ($e_I$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) | да |
| Индекс открытого ключа УЦ | 1 B | Номер ключа УЦ, с использованием которого подписан сертификат | нет |

**Формат данных, подписываемых УЦ**

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '6A' | нет |
| Формат сертификата | 1 B | Значение '02' | да |
| Идентификатор эмитента | 4 B | Крайние левые 3-8 цифр PAN, выровненные по левому краю и дополненные справа символами 'F' | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Серийный номер сертификата | 3 B | Уникальный номер, назначается УЦ | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа эмитента | да |
| Длина модуля открытого ключа эмитента ($LN_I$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа эмитента ($Le_I$) | 1 B | Количество байтов | да |
| Модуль открытого ключа эмитента ($N_I$) или его крайние левые байты | n B | В случае $LN_I \leq LN_{CA}$ - 36 поле содержит модуль открытого ключа эмитента, выровненный по левому краю и дополненный справа $LN_{CA}$ - 36 - $LN_I$ байтами 'BB'<br>В случае $LN_I > LN_{CA}$ - 36 поле содержит $LN_{CA}$ - 36 наиболее значимых байтов модуля открытого ключа эмитента | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа эмитента и связанной с ним информации | нет |
| Трейлер | 1 B | Значение 'BC' | нет |

**Формат присоединенной подписи, генерируемой УЦ**

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '00' |
| Код формата блока | 1 B | Значение '01' |
| Символы дополнения | n B | Значение 'FF'. Длина дополнения = $LN_{CA}$ - 38 |
| Разделитель | 1 B | Значение '00' |
| Идентификатор алгоритма хэширования | 15 B | Идентификатор алгоритма хэширования, используемого УЦ |
| Хэш-значение | 20 B | Значение хэш-функции от конкатенации данных, неподписываемых УЦ, и данных открытого ключа эмитента, подписываемых УЦ |

## Формат сертификата карты

### Формат данных, подписываемых эмитентом

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Формат сертификата | 1 B | Значение '04' | да |
| PAN | 10 B | PAN, выровненный по левому краю и дополненный справа символами 'F' | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Серийный номер сертификата | 3 B | Уникальный номер, назначается эмитентом | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа карты | да |
| Длина модуля открытого ключа карты ($LN_{IC}$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа карты ($Le_{IC}$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) | да |
| Крайние левые байты модуля открытого ключа карты ($N_{IC}$) | n B | В случае $LN_{IC} \leq LN_I$ - 42 поле содержит модуль открытого ключа карты, выровненный по левому краю и дополненный справа $LN_I$ - 42 - $LN_{IC}$ байтами 'BB'<br>В случае $LN_{IC} > LN_I$ - 42 поле содержит $LN_I$ - 42 наиболее значимых байтов модуля открытого ключа карты | да |
| Остаток модуля открытого ключа карты ($N_{IC}^R$) | n B | Присутствует, только если $LN_{IC} > LN_I$ - 42; $LN_{IC}$ - $LN_I$ + 42 наименее значимых байтов модуля открытого ключа карты | да |
| Экспонента открытого ключа карты ($e_{IC}$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) | да |
| Статические данные | n B | Статические данные для аутентификации | да |

**Формат данных сертификата открытого ключа карты**

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '6A' |
| Формат сертификата | 1 B | Значение '04' |
| PAN | 10 B | PAN, выровненный по левому краю и дополненный справа символами 'F' |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ |
| Серийный номер сертификата | 3 B | Уникальный номер, назначается эмитентом |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа карты |
| Длина модуля открытого ключа карты ($LN_{IC}$) | 1 B | Количество байтов |
| Длина экспоненты открытого ключа карты ($Le_{IC}$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) |
| Модуль открытого ключа карты ($N_{IC}$) или его крайние левые байты | n B | В случае $LN_{IC} \leq LN_I$ - 42 поле содержит модуль открытого ключа карты, выровненный по левому краю и дополненный справа $LN_I$ - 42 - $LN_{IC}$ байтами 'BB'<br>В случае $LN_{IC} > LN_I$ - 42 поле содержит $LN_I$ - 42 наиболее значимых байтов модуля открытого ключа карты |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа карты и связанной с ним информации |
| Трейлер | 1 B | Значение 'BC' |

## Формат сертификата карты для шифрования PIN (Мир)

### Формат данных, подписываемых эмитентом

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Формат сертификата | 1 B | Значение '04' | да |
| PAN | 10 B | PAN, выровненный по левому краю и дополненный справа символами 'F' | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Серийный номер сертификата | 3 B | Уникальный номер, назначается эмитентом | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа карты для шифрования PIN | да |
| Длина модуля открытого ключа карты для шифрования PIN ($LN_{PE}$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа карты для шифрования PIN ($Le_{PE}$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) | да |
| Крайние левые байты модуля открытого ключа карты для шифрования PIN ($N_{PE}$) | n B | В случае $LN_{PE} \leq LN_I$ - 42 поле содержит модуль открытого ключа карты для шифрования PIN, выровненный по левому краю и дополненный справа $LN_I$ - 42 - $LN_{PE}$ байтами 'BB'<br>В случае $LN_{PE} > LN_I$ - 42 поле содержит $LN_I$ - 42 наиболее значимых байтов модуля открытого ключа карты для шифрования PIN | да |
| Остаток модуля открытого ключа карты для шифрования PIN ($N^R_{PE}$) | n B | Присутствует, только если $LN_{PE} > LN_I$ - 42; $LN_{PE}$ - $LN_I$ + 42 наименее значимых байтов модуля открытого ключа карты для шифрования PIN | да |
| Экспонента открытого ключа карты для шифрования PIN ($e_{PE}$) | 1 или 3 B | Допустимые значения: '03' (для экспоненты 3) или '010001' (для экспоненты 65537) | да |

**Формат данных сертификата открытого ключа карты для шифрования PIN**

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '6A' |
| Формат сертификата | 1 B | Значение '04' |
| PAN | 10 B | PAN, выровненный по левому краю и дополненный справа символами 'F' |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ |
| Серийный номер сертификата | 3 B | Уникальный номер, назначается эмитентом |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа карты для шифрования PIN |
| Длина модуля открытого ключа карты для шифрования PIN ($LN_{PE}$) | 1 B | Количество байтов |
| Длина экспоненты открытого ключа карты для шифрования PIN ($Le_{PE}$) | 1 B | Количество байтов. Допустимые значения: '01' (для экспоненты 3) или '03' (для экспоненты 65537) |
| Модуль открытого ключа карты для шифрования PIN ($N_{PE}$) или его крайние левые байты | n B | В случае $LN_{PE} \leq LN_I$ - 42 поле содержит модуль открытого ключа карты для шифрования PIN, выровненный по левому краю и дополненный справа $LN_I$ - 42 - $LN_{PE}$ байтами 'BB'<br>В случае $LN_{PE} > LN_I$ - 42 поле содержит $LN_I$ - 42 наиболее значимых байтов модуля открытого ключа карты для шифрования PIN |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа карты для шифрования PIN и связанной с ним информации |
| Трейлер | 1 B | Значение 'BC' |

## Формат самоподписанного сертификата УЦ (Visa)

### Формат данных, неподписываемых УЦ

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '20' | нет |
| Идентификатор сервиса | 4 B | Идентификатор сервиса Visa (Proprietary Application Identifier Extension (PIX)), выровненный по левому краю и дополненный справа '0000' | нет |
| Длина модуля открытого ключа УЦ ($LN_{CA}$) | 2 B | Количество байтов | нет |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа УЦ | нет |
| Длина экспоненты открытого ключа УЦ ($Le_{CA}$) | 1 B | Количество байтов | нет |
| Идентификатор RID | 5 B | Идентификатор RID | да |
| Индекс открытого ключа УЦ | 1 B | Уникальный номер открытого ключа УЦ | да |
| Модуль открытого ключа УЦ ($N_{CA}$) | n B | Модуль открытого ключа УЦ | да |
| Экспонента открытого ключа УЦ ($e_{CA}$) | n B | Экспонента открытого ключа УЦ | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа УЦ и связанной с ним информации | нет |

**Формат данных, подписываемых УЦ**

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '21' |
| Идентификатор сервиса | 4 B | Идентификатор сервиса Visa (Proprietary Application Identifier Extension (PIX)), выровненный по левому краю и дополненный справа '0000' |
| Идентификатор RID | 5 B | Идентификатор RID |
| Индекс открытого ключа УЦ | 1 B | Уникальный номер открытого ключа УЦ |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа УЦ |
| Крайние левые байты модуля открытого ключа УЦ ($N_{CA}$) | n B | $LN_{CA}$ - (36 + $Le_{CA}$) наиболее значимых байтов модуля открытого ключа УЦ |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* |
| Длина экспоненты открытого ключа УЦ ($Le_{CA}$) | 1 B | Количество байтов |
| Экспонента открытого ключа УЦ ($e_{CA}$) | n B | Экспонента открытого ключа УЦ |
| Хэш-значение | 20 B | Хэш-значение из данных, не подписываемых УЦ |

## Формат самоподписанного сертификата УЦ (Mastercard)

### Формат данных, неподписываемых УЦ

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Идентификатор RID | 5 B | Идентификатор RID | нет |
| Индекс открытого ключа УЦ | 1 B | Уникальный номер открытого ключа УЦ | нет |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа УЦ | нет |
| Длина модуля открытого ключа УЦ ($LN_{CA}$) | 1 B | Количество байтов | нет |
| Длина экспоненты открытого ключа УЦ ($Le_{CA}$) | 1 B | Количество байтов | нет |
| Крайние левые байты модуля открытого ключа УЦ ($N_{CA}$) | n B | $N_{CA}$ - 37 наиболее значимых байтов модуля открытого ключа УЦ | нет |
| Остаток модуля открытого ключа карты ($N^{R}_{CA}$) | 37 B | 37 наименее значимых байтов модуля открытого ключа УЦ | да |
| Экспонента открытого ключа УЦ ($e_{CA}$) | n B | Экспонента открытого ключа УЦ | да |

**Формат данных, подписываемых УЦ**

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '6A' | нет |
| Формат сертификата | 1 B | Значение '10' | да |
| Идентификатор RID | 5 B | Идентификатор RID | да |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ | да |
| Серийный номер сертификата | 3 B | Уникальный номер сертификата | да |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* | да |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа УЦ | да |
| Длина модуля открытого ключа УЦ ($LN_{CA}$) | 1 B | Количество байтов | да |
| Длина экспоненты открытого ключа УЦ ($Le_{CA}$) | 1 B | Количество байтов | да |
| Крайние левые байты модуля открытого ключа УЦ ($N_{CA}$) | n B | $N_{CA}$ - 37 наиболее значимых байтов модуля открытого ключа УЦ | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа УЦ и связанной с ним информации | нет |
| Трейлер | 1 B | Значение 'BC' | нет |

## Формат самоподписанного сертификата УЦ (American Express)

### Формат данных, неподписываемых УЦ

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '20' | нет |
| Идентификатор сервиса | 4 B | American Express Product Identifier | нет |
| Длина модуля открытого ключа УЦ ($LN_{CA}$) | 2 B | Количество байтов | нет |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа УЦ | нет |
| Длина экспоненты открытого ключа УЦ ($Le_{CA}$) | 1 B | Количество байтов | нет |
| Идентификатор RID | 5 B | Идентификатор RID | да |
| Индекс открытого ключа УЦ | 1 B | Уникальный номер открытого ключа УЦ | да |
| Модуль открытого ключа УЦ ($N_{CA}$) | n B | Модуль открытого ключа УЦ | да |
| Экспонента открытого ключа УЦ ($e_{CA}$) | n B | Экспонента открытого ключа УЦ | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа УЦ и связанной с ним информации | нет |

**Формат данных, подписываемых УЦ**

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '21' |
| Идентификатор сервиса | 4 B | American Express Product Identifier |
| Идентификатор RID | 5 B | Идентификатор RID |
| Индекс открытого ключа УЦ | 1 B | Уникальный номер открытого ключа УЦ |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа УЦ |
| Крайние левые байты модуля открытого ключа УЦ ($N_{CA}$) | n B | $LN_{CA}$ - (36 + $Le_{CA}$) наиболее значимых байтов модуля открытого ключа УЦ |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* |
| Длина экспоненты открытого ключа УЦ ($Le_{CA}$) | 1 B | Количество байтов |
| Экспонента открытого ключа УЦ ($e_{CA}$) | n B | Экспонента открытого ключа УЦ |
| Хэш-значение | 20 B | Хэш-значение из данных, не подписываемых УЦ |

## Формат самоподписанного сертификата УЦ (Мир)

### Формат данных, неподписываемых УЦ

| Поле | Длина, формат | Описание | Входные данные хэш-функции |
|---|---|---|---|
| Заголовок | 1 B | Значение '20' | нет |
| Идентификатор сервиса | 4 B | Идентификатор приложения | нет |
| Длина модуля открытого ключа УЦ ($LN_{CA}$) | 2 B | Количество байтов | нет |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа УЦ | нет |
| Длина экспоненты открытого ключа УЦ ($Le_{CA}$) | 1 B | Количество байтов | нет |
| Идентификатор RID | 5 B | Идентификатор RID | да |
| Индекс открытого ключа УЦ | 1 B | Уникальный номер открытого ключа УЦ | да |
| Модуль открытого ключа УЦ ($N_{CA}$) | n B | Модуль открытого ключа УЦ | да |
| Экспонента открытого ключа УЦ ($e_{CA}$) | n B | Экспонента открытого ключа УЦ | да |
| Хэш-значение | 20 B | Значение хэш-функции от открытого ключа УЦ и связанной с ним информации | нет |

**Формат данных, подписываемых УЦ**

| Поле | Длина, формат | Описание |
|---|---|---|
| Заголовок | 1 B | Значение '21' |
| Идентификатор сервиса | 4 B | Идентификатор приложения |
| Идентификатор RID | 5 B | Идентификатор RID |
| Индекс открытого ключа УЦ | 1 B | Уникальный номер открытого ключа УЦ |
| Дата окончания срока действия сертификата | 2 B | В формате ММГГ |
| Идентификатор алгоритма подписи | 1 B | Идентификатор алгоритма подписи открытого ключа УЦ |
| Крайние левые байты модуля открытого ключа УЦ ($N_{CA}$) | n B | $LN_{CA}$ - (36 + $Le_{CA}$) наиболее значимых байтов модуля открытого ключа УЦ |
| Идентификатор алгоритма хэширования | 1 B | Идентификатор алгоритма, используемого для получения *Хэш-значения* |
| Длина экспоненты открытого ключа УЦ ($Le_{CA}$) | 1 B | Количество байтов |
| Экспонента открытого ключа УЦ ($e_{CA}$) | n B | Экспонента открытого ключа УЦ |
| Хэш-значение | 20 B | Хэш-значение из данных, не подписываемых УЦ |

# Приложение Г  Форматы закрытого ключа

## ASN.1

Закрытый ключ RSA имеет следующий формат (ASN.1):

```
RSAPrivateKey::= SEQUENCE{
  p             BIT STRING,
  q             BIT STRING,
  dp            BIT STRING,
  dq            BIT STRING,
  q^-1 mod p     BIT STRING}
```

В нотации ASN.1 для обозначения типа SEQUENCE применяется тег **0x30**, для типа BIT STRING — **0x03**.

Закрытый ключ в формате ASN.1 имеет вид:

30 | Общая длина SEQUENCE | 03 | Длина BIT STRING (p) | p | 03 | Длина BIT STRING (q) | q | 03 | Длина BIT STRING (dp) | dp | 03 | Длина BIT STRING (dq) | dq | 03 | Длина BIT STRING ($q^{-1}$ mod p) | $q^{-1}$ mod p

При определении длины битовой строки (BIT STRING) сначала указывается длина строки в байтах, а затем количество неиспользуемых (игнорируемых) битов в последнем байте.

Например, битовая строка '101010' кодируется как 03 02 02 A8, где 03 — тег битовой строки, 02 — длина строки в байтах, 02 — количество игнорируемых битов в конце, A8 (**10101000**) — данные строки, дополненные в конце нулями (значение дополнения может быть любым).

**Пример представления ключа в формате ASN.1:**

p:

```
FADD62A62492706C 5784790CDC40D76C
5CA0736FA0E07CAA EB1729C1C7FF18E1
70EFC25B7711C907 B515542ACFD80823
```

q:

```
EC43DD6A0F955408 09579E9A8D0DECC3
B4050712A28C97F0 6521505342D6E102
58F3BBBB845CBAB0 3B136EC6A7E1F6E9
```

dp:

```
A73E41C41861A048 3A5850B33D808F9D
9315A24A6B40531C 9CBA1BD68554BB40
F5F52C3CFA0BDB5A 78B8E2C7353AB017
```

dq:

```
9D82939C0A638D5A B0E5146708B3F32D
22AE04B71708654A EE16358CD739EB56
E5F7D27D02E87C75 7CB79F2F1A96A49B
```

u ($q^{-1}$ mod p):

```
CEB3DA4206C267C1 1EF3DCCB77268707
09E735BED60E68D5 3C0E573FB64A634F
376B15CCC0219C5A 02F09B834048ECB9
```

Закрытый ключ (ASN.1):

```
30 81 FF 03 31 00 FA DD 62 A6 24 92 70 6C 57 84
79 0C DC 40 D7 6C 5C A0 73 6F A0 E0 7C AA EB 17
29 C1 C7 FF 18 E1 70 EF C2 5B 77 11 C9 07 B5 15
54 2A CF D8 08 23 03 31 00 EC 43 DD 6A 0F 95 54
08 09 57 9E 9A 8D 0D EC C3 B4 05 07 12 A2 8C 97
F0 65 21 50 53 42 D6 E1 02 58 F3 BB BB 84 5C BA
B0 3B 13 6E C6 A7 E1 F6 E9 03 31 00 A7 3E 41 C4
18 61 A0 48 3A 58 50 B3 3D 80 8F 9D 93 15 A2 4A
6B 40 53 1C 9C BA 1B D6 85 54 BB 40 F5 F5 2C 3C
FA 0B DB 5A 78 B8 E2 C7 35 3A B0 17 03 31 00 9D
82 93 9C 0A 63 8D 5A B0 E5 14 67 08 B3 F3 2D 22
AE 04 B7 17 08 65 4A EE 16 35 8C D7 39 EB 56 E5
F7 D2 7D 02 E8 7C 75 7C B7 9F 2F 1A 96 A4 9B 03
31 00 CE B3 DA 42 06 C2 67 C1 1E F3 DC CB 77 26
87 07 09 E7 35 BE D6 0E 68 D5 3C 0E 57 3F B6 4A
63 4F 37 6B 15 CC C0 21 9C 5A 02 F0 9B 83 40 48
EC B9
```

## Компоненты CRT

Длина в битах каждой компоненты CRT (Китайская теорема об остатках) равна половине длины модуля с округлением к большему ($\lceil L_n/2 \rceil$). Например, если длина модуля $L_n = 1007$ бит, то длина компоненты CRT = 504 бит.

Размер каждой компоненты определяется значением $\lceil x/24 \rceil * 3$, где x — длина компоненты в битах. Например, для значения длины выше, $\lceil 504/24 \rceil * 3 = 63$. Полученное значение определяет исходный размер компоненты CRT перед применением форматирования или дополнения (которое требуется для достижения кратности 8 байтам).

Незашифрованное значение компоненты формируется следующим образом:

| Длина | Компонента CRT | Дополнение |
|---|---|---|
| (1 байт) опционально | переменная длина | В зависимости от указанного режима выравнивания в команде:<br>1) байты '00' до кратности 8 байтам (DES KEK) или 16 байтам (AES KEK)<br>2) 4 байта '8000 0000' или 8 байтов '8000 0000 0000 0000' до кратности 8 байтам (DES KEK)<br>или<br>4 байта '8000 0000', 8 байтов '8000 0000 0000 0000', 12 байтов '8000 0000 0000 0000 0000 0000' или 16 байтов '8000 0000 0000 0000 0000 0000 0000 0000' до кратности 16 байтам (AES KEK)<br>3) *(режим по умолчанию)* 1 байт '80' и несколько байтов '00' до кратности 8 байтам (DES KEK) или 16 байтам (AES KEK) |

## Альтернативный формат компонент CRT

При формировании закрытого ключа в формате 5 компонент CRT возможно также указать одно из условий для компонент q и p: $q > p$ или $p > q$.

Некоторые приложения требуют представления 5-го компонента ($q^{-1} \bmod p$) в другой форме — $p^{-1} \bmod q$. Это достигается следующим образом:

1. если требуется q > p

- установить условие p > q (противоположное тому, что требуется)
- переупорядочить полученные 5 компонент (p, q, dp, dq, $q^{-1}$ mod p) в соответствии со следующим правилом:

| Для новой компоненты | Использовать полученную компоненту |
|---|---|
| p | q |
| q | p |
| dp | dq |
| dq | dp |
| $p^{-1}$ mod q | $q^{-1}$ mod p |

2. если требуется p > q

- установить условие q > p (противоположное тому, что требуется)
- переупорядочить полученные 5 компонент (p, q, dp, dq, $q^{-1}$ mod p) в соответствии с таблицей выше

## Модуль и экспонента

Закрытый ключ может быть представлен в формате закрытой экспоненты (d) и модуля (n), которые имеют следующий вид:

| Длина | Закрытая экспонента (d) или модуль (n) | Дополнение |
|---|---|---|
| (1 байт)<br>HEX<br>опционально | переменная длина | В зависимости от указанного режима выравнивания в команде:<br>1) *(режим по умолчанию)* байты '00' до кратности 8 байтам (DES KEK) или 16 байтам (AES KEK)<br>2) 4 байта '8000 0000' или 8 байтов '8000 0000 0000 0000' до кратности 8 байтам (DES KEK)<br>или<br>4 байта '8000 0000', 8 байтов '8000 0000 0000 0000', 12 байтов '8000 0000 0000 0000 0000 0000' или 16 байтов '8000 0000 0000 0000 0000 0000 0000 0000' до кратности 16 байтам (AES KEK)<br>3) 1 байт '80' и несколько байтов '00' до кратности 8 байтам (DES KEK) или 16 байтам (AES KEK) |

# Перечень команд (по алфавиту)