Модули безопасности для систем платежных карт

SPB HSM ₽S high,

SPB HSM ₽S base

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

2022

Содержание

1 Назначение изделия 3
2 Описание структуры и режимов работы изделия 4
2.1 Структура изделия 4
2.2 Режимы работы изделия 5
2.2.1 Режим Хост-команд 5
2.2.2 Режим Управления 5
3 Описание конструкции изделия 8
4 Технические характеристики 9
5 Функции ПО SPB HSM PS 11

1 Назначение изделия

Модуль безопасности для систем платёжных карт (МБ СПК) относится к классу платёжных HSM и предназначен для применения в банковских и платёжных системах и обеспечивает защиту данных держателей карт, а также транзакционную безопасность в следующих процессах:

- Инициализация платёжных карт при их производстве;
- Эмиссия платёжных карт, включая генерацию секретных величин, электрическую персонализацию и печать пин-конвертов;
- Авторизация платёжных транзакций;
- Эквайринг, обработка транзакций от платёжных устройств;
- 3D-Secure;
- Поддержка режима работы операционно-платёжного клирингового центра системы платёжных карт;
- Управление ключами, а именно – генерация, смена, резервирование, экспорт локальных, зональных, терминальных, транспортных мастер ключей, которые используются в вышеперечисленных процессах.

МБ СПК выполнен в виде аппаратно-программного комплекса в единой конструкции, обеспечивающей уровень физической и логической защиты в соответствии с национальными «Требованиями к СКЗИ в платёжных устройствах с терминальным ядром, серверных компонентах платёжных систем (HSM модулях), платёжных картах и иных технических средствах информационной инфраструктуры платёжной системы, используемых при осуществлении переводов денежных средств, указанных в пункте 2.20 положения Банка России от 09.06.12 г. № 382-П» и с учетом требований «PCI PTS HSM Modular Security Requirements 3.0.»

2 Описание структуры и режимов работы изделия

2.1 Структура изделия

Структурно, в состав единой конструкции МБ СПК входят два блока: блок управления и криптоблок, соединённые внутренним защищённым интерфейсом.

Блок управления обеспечивает ввод-вывод и разбор формата команд, поступающих от прикладной HOST системы, взаимодействие с криптоблоком для выполнения критичных криптографических преобразований, а также предоставляет функции для удалённого управления устройством через защищённый TLS канал.

К блоку управления подключаются внешние интерфейсы с HOST системой, а также интерфейс удалённого и локального управления.

Криптоблок обеспечивает все операции по генерации, защищённому хранению, экспорту, созданию резервных локальных мастер ключей, а также расшифрование и зашифрование персональных данных владельцев карт (ключей, PIN, PIN блоков) на локальных мастер ключах.

Непосредственно к криптоблоку подключается интерфейс взаимодействия с считывателем смарт-карт, поэтому все операции по экспорту/импорту локальных мастер ключей на смарт-карты осуществляются из криптоблока, минуя блок управления, имеющий подключённые внешние интерфейсы.

Также в состав МБ СПК входит программное обеспечение SPB HSM PS, обеспечивающее выполнение функций представленных в разделе 5.

2.2 Режимы работы изделия

Работа изделия заключается в выполнении двух основных режимов:

– обработка команд, поступающих от HOST системы – режим Хост-команд;
– управление устройством и его параметрами – режим Управления, аналогом которого является режим консольных команд.

2.2.1 Режим Хост-команд

Изделие в режиме Хост-команд с помощью программного обеспечения SPB HSM PS, выполняет основные функции, обеспечивающие поддержку необходимых криптографических операций в инфраструктуре платёжных систем, таких как:

– поддержка EMV,
– расчёт карточных величин (CVV/CVC/CVP, PVV),
– работа с PIN-блоками,
– поддержка экспорта/импорта ключей с использованием различных контейнеров: «ACS X9 TR-31 2018», PKCS#1 v1.5, ANSI X9.17 и других.

Доступ к изделию в режиме Хост-команд реализован через специальное API, формализующее обмен данными с HOST системой по протоколам TCP/UDP. При этом HOST система никогда не получает доступ к ключам или иным чувствительным данным в чистом виде – только в виде шифрограмм, защищённых на локальных мастер-ключах (LMK) или других ключах (ZMK, PVK и т.п.).

Алгоритм обмена заключается в следующем: HOST система подготавливает данные, форматирует (упаковывает) их в соответствующую конкретной команде структуру, содержащую в виде набора аргументов необходимые данные, например, для расчёта CVV, отправляет запрос в МБ СПК и получает в ответ рассчитанную величину.

2.2.2 Режим Управления

Доступ к изделию в режиме Управления осуществляется двумя способами:

– локально, по выделенному ETH-интерфейсу, доступ к которому возможен только из локальной подсети;
– удаленно, по выделенному HOST-интерфейсу, доступ к которому возможен из других подсетей, при этом в качестве IP-адреса шлюза по умолчанию используется заданный в строке «адрес шлюза (WEB консоль)».

Изделие в режиме Управления поддерживает следующие режимы доступа:

- аутентифицированный, требующий аутентификации одного администратора управления или администратора безопасности;
- авторизованный, требующий аутентификации двух администраторов управления;
- привилегированный, требующий аутентификации двух администраторов управления и одного администратора безопасности (критичный с точки зрения безопасности).

Администратор безопасности после аутентификации может выполнять следующие действия:

- проведение инициализации изделия;
- управление учётными записями администраторов безопасности и администраторов управления (создание/удаление/запись токенов);
- форматирование и подготовку смарт-карт для последующих операций с ключами LMK;
- формирование/смену ключей ЭП изделия;
- аудит криптографических событий (просмотр журнала безопасности).

Администратор управления после аутентификации может выполнять следующие действия:

- инициировать генерацию массива ключей LMK совместно со вторым администратором управления;
- инициировать резервирование и восстановление (экспорт/импорт) массива ключей LMK с использованием смарт-карт совместно со вторым администратором управления и администратором безопасности;
- настройку сетевых параметров и параметров хост команд;
- управление ключами с использованием ТУУ, а именно:
    1) импорт/экспорт ключей;
    2) зашифрование компонент ключей;
    3) формирование ключей из компонент;
    4) зашифрование таблицы децимализации и т.д.;
- сохранение на внешний носитель (токен) конфигурации безопасности;
- просмотр статистики обработки хост команд;
- аудит административных событий (просмотр журнала событий);
- управление доступом к выполнению хост команд:

1) разрешение/запрет использования;
2) разрешение/запрет использования в авторизованном состоянии.

3 Описание конструкции изделия

Конструктивно МБ СПК выполнен в виде моноблока, соответствующего 19″ стандарту МЭК 297-3-100-2008, и имеет в высоту 2U (88 мм).

МБ СПК, торговая марка SPB HSM ₽S, как аппаратная платформа выпускается в двух исполнениях high (см. Рисунок 1) и base (см. Рисунок 2).

Рисунок 1 – SPB HSM ₽S high

Рисунок 2 – SPB HSM ₽S base

4 Технические характеристики

Основные технические характеристики SPB HSM ₽S с учётом исполнений приведены в таблице:

Характеристики	Параметры	
	SPB HSM ₽S high	SPB HSM ₽S base
Интерфейс подключения к HOST системе	2 интерфейса × 1 GbE	
Протокол взаимодействия с HOST системой	UDP, TCP/IP	
Производительность, tps	40 000	1 000/250
API с ПО HOST системы	UDP/ TCP сокеты, режим команда-ответ в соответствии с определённым форматом	
Интерфейс подключения удалённого управления	1 интерфейс × 1 GbE	
Протокол взаимодействия удалённого управления	ГОСТ Р 1323565.1.030-2018 «Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня TLS»	
Лицензии ПО SPB HSM PS	– основная или Core, – обеспечивающая совместимость или Legacy, – обеспечивающая дополнительную совместимость или Legacy P3	
Международные криптографические алгоритмы и механизмы	Криптографические алгоритмы: DES/3DES – NIST FIPS 46-3 SP 800-67 и ISO 10116, AES – NIST FIPS 197, RSA – RFC 3447 NIST FIPS 186-4, SHA-1 – RFC 3174 и NIST FIPS 180-4, SHA-224, SHA-384, SHA-256, SHA-512 – ISO/IEC 10118-2 и NIST 180-4, MAC – ISO 9797 и NIST FIPS 198-1, HMAC – ISO/IEC 9797-2, Поддерживаемые механизмы: Global Platform v.2.2.1, EMV CPS 1.1, EMV3.1.1, EMV 4.1, EMV 4.3 (ARQC/ARPC/AAC), IDN, Union Pay (ARQC/ARPC), CVP/iCVP/CVP2, CVC/CVV/CVC3, PVV, MasterCard CAP, CAVV, PIN Block (ISO 9564-1) – в том числе ISO-0, ISO-3, ISO-4, IBM 3624, ANSI X9-24 (DUKPT)	
Российские криптографические алгоритмы (РКА)	Блочный шифр «Кузнечик» ГОСТ Р 34.12-2015 в режимах ГОСТ Р 34.13-2015, хэш функция ГОСТ Р 34.11-2012	

Характеристики	Параметры	
	SPB HSM ₽S high	SPB HSM ₽S base
Форм-фактор	19″ моноблок 2U (+1U воздухозабор)	
Электропитание (с резервированием)	220 В, 50 Гц	
Габариты, В×Ш×Д, мм, не более	88×482,6×710	
Масса, кг, не более	20	
Срок службы	10 лет	
Условия монтажа	19″ телекоммуникационный шкаф/стойка глубиной 800-1200 мм	
Условия эксплуатации	ГОСТ 15150 4 группа климатического исполнения УХЛ с уточнениями: – температура окружающего воздуха от + 5 до + 30°С; – относительная влажность воздуха до 80% при температуре + 25°С; – атмосферное давление от 84 до 106,7 кПа (от 630 до 800 мм рт. ст.).	
Физическая безопасность	Конструкция, обеспечивающая защиту от НСД, использование различных систем обнаружения НСД и датчиков вскрытия – механические микропереключатели, датчик объема	
Методы генерации, защиты и использования локальных мастер ключей	Совместное использование ФДСЧ и ПДСЧ для генерации, хранение в зашифрованном виде на РКА во внутренней памяти криптоблока, гарантированное стирание при обнаружении попытки НСД. Поддерживается два способа использования LMK: – вариантные LMK; – keyblock LMK.	
Поддерживаемые форматы ключевых контейнеров для экспорта	«ASC X9 TR-31-2018» (в том числе TR-31-TK26 MAGMA/KUZNECHIK), Variant Scheme (ANSI X9.17), PKCS #1 v1.5, PKCS#1 v2.2	
Резервирование локальных мастер-ключей	В виде компонент на смарт-картах непосредственно из криптоблока с применением алгоритмических мер защиты от ПЭМИН	

5 Функции ПО SPB HSM PS

Программное обеспечение SPB HSM PS, входящее в состав МБ СПК обеспечивает выполнение следующих основных функций:

1) Создание защищённого удалённого подключения к изделию, аутентификацию администраторов безопасности и администраторов управления с использованием их идентификаторов (USB-токенов), которые записываются при инициализации изделия.
2) Инициализацию, управление и настройку изделия в процессе его эксплуатации.
3) Журналирование действий пользователей и работы системных сервисов.
4) Реализацию основных криптографических механизмов:

– Выполнение криптографических операций с DES/3DES в соответствии с «NIST FIPS 46-3/NIST Special Publication 800-67» и «ISO/IEC 10116» (ECB, CBC).

– Выполнение криптографических операций с AES в соответствии с «NIST FIPS 197».

– Генерацию пары ключей RSA: закрытый ключ и открытый ключ в соответствии «RFC 3447» и «NIST FIPS 186-4».

– Вычисление хэш функций семейства SHA в соответствии с «RFC 3174», «NIST FIPS 180-4» и «ISO/IEC 10118-2».

– Вычисление функций MAC за данные в соответствии с «ISO 9797-1» MAC (DES, 3DES), CBC_MAC (AES), CMAC (AES).

– Вычисление функций HMAC в соответствии с «ISO/IEC 9797-2» (MAC Algorithm 2) и «NIST FIPS 198-1».

– Работу с ключами в формате key block в соответствии с «ASC X9 TR 31-2018».

– Трансляцию (перешифрование) PIN-блока, зашифрованного с помощью одного ключа, в PIN-блок, зашифрованный с использованием других ключей.

– Вывод мастер-ключа карты из соответствующего мастер-ключа эмитента (MK_{CL}, MK_{IDN}).

– Вывод мастер-ключей карты MK_{AC}, MK_{SMC}, MK_{SMI}, MK_{IDN} в соответствии с алгоритмами документа «Стандарт платежной системы «Мир».

– Зашифровывание чистой компоненты ключа.

– Трансляцию (перешифрование) ZPK.

- Реализацию функции для защищенного обмена с картой при производстве по протоколу «SCP-02», в том числе диверсификацию ключей, формирование сессионных ключей для защищенного обмена с картой, а также формирование криптограммы карты в соответствии с «Global Platform v.2.2.1» (E.4.2.).
- Реализацию функции для защищенного обмена с картой при эмиссии в том числе:
  1) с использованием алгоритма EMV CPS 1.1 в соответствии с документом «Стандарт платежной системы «Мир».
  2) с использованием алгоритма Visa 2 в соответствии с документом «Стандарт платежной системы «Мир».
- Генерацию CVP (CVC/CVV)/ППК (Card Verification Parameter/Проверочный параметр карты). CVP/ППК в соответствии с документом «Требования к данным на магнитной полосе и EMV-эквиваленте карты платежной системы «Мир».
- Проверку Dynamic Card Verification Value (dCVV) или Card Verification Code (CVC3), в зависимости от типа платежной системы: «Мир», Visa, MasterCard, American Express, UnionPay, JCB.
- Генерацию и проверку криптовеличины PVV по алгоритму VISA PVV в соответствии с документом «Требования к данным на магнитной полосе и EMV-эквиваленте карты платежной системы «Мир».
- Проверку криптограммы ARQC и/или генерацию ARPC (EMV 3.1.1).
- Проверку криптограммы ARQC и/или генерацию ARPC (EMV 4.x).
- Вычисление и проверку American Express Card Security Codes (CSC): CSC3, CSC4 и CSC5.
- Проверку криптограммы ARQC и/или генерацию ARPC в соответствии с документацией Union Pay.
- Генерацию и проверку IDN (ICC Dynamic Number).
- Проверку Truncated Application Cryptogram (MasterCard CAP).
- Генерацию и проверку CAVV.
- Генерацию ключевой пары RSA (закрытый и открытый ключи) эмитента и соответствующего самоподписанного сертификата в соответствии с требованиями платежных систем и по стандарту «EMV 4.3».
- Проверки EMV-сертификата RSA-ключа эмитента, подписанного корневым ключом УЦ по стандарту «EMV 4.3».
- Импорт (с проверкой) EMV-сертификата корневого ключа УЦ.

- Генерацию PIN с возможностью печати.
- Трансляцию PIN-блока из одного формата в другой с возможностью перешифрования из-под одного ключа под другой. Допустимые форматы трансляции («ISO 9564-1»): ISO-0 (Format 0), ISO-1(Format 1), ISO-3(Format 3), ISO-4(Format 4).
- Генерацию, проверку и смену PIN-offset с использованием метода «IBM 3624».
- Обеспечение функции управления ключами (DUKPT).