СОГЛАСОВАНО
Первый заместитель
руководителя Научно-
технической службы
ФСБ России

_____ А.М. Ивашко
«24» 01 2020 г.

УТВЕРЖДАЮ
Заместитель Председателя
Банка России

_____ Д.Г. Скобелкин
«28» 02 2020 г.

ФУНКЦИОНАЛЬНО-ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К АППАРАТНОМУ МОДУЛЮ БЕЗОПАСНОСТИ (HSM-МОДУЛЬ)

№ ФТ-56-3/35
28.02.2020

Оглавление

ТЕРМИНЫ, определения и сокращения

В настоящих требованиях применяются следующие термины с соответствующими определениями.

Термин/Сокращение	Определение
Авторизованное состояние	Состояние, обеспечивающее доступ к критичным операциям HSM
ГСЧ	Генератор случайных чисел
Ключ шифрования ПИН-блока (ZPK – Zone PIN Key)	Криптографический ключ, предназначенный для безопасной передачи ПИН-блоков
Криптограмма	Зашифрованные с помощью криптографического преобразования данные
Криптографический ключ	Уникальная последовательность символов, предназначенная для преобразования данных при помощи криптографического алгоритма
Администратор HSM или Пользователь HSM	Администратор или Пользователь, сотрудник, назначенный приказом и уполномоченный производить следующие действия: — внедрение и сопровождение системы создания криптографических ключей для HSM (далее по тексту «Система HSM»); — контроль и обнаружение различных угроз, которым подвергается Система HSM и ее информационные ресурсы, а также реагирование на эти угрозы в режиме реального времени; выполнение административных мероприятий по установке, настройке и поддержке в работоспособном состоянии средств криптографической защиты информации, эксплуатируемых в Системе HSM, включая работу с криптографическими ключами
ПИН-блок	Набор двоичных данных определенного формата. Поддерживаемые форматы ПИН-блока: формат 0 ISO 9564, формат 1 ISO 9564, формат 3 ISO 9564, формат 4 ISO 9564
СКЗИ	Средство криптографической защиты информации
Слабый ключ	Криптографический ключ, использование которого приводит к уязвимости применяемого алгоритма шифрования
Транспортный ключ (ZMK – Zone Master Key, TMK – Terminal Master Key)	Криптографический ключ, предназначенный для безопасной передачи других ключей
УЦ	Удостоверяющий центр
3DES	Криптографический алгоритм для симметричного шифрования на основе алгоритма DES (Data Encryption Standard)
AES	Advanced Encryption Standard, криптографический алгоритм для симметричного шифрования
ARQC	Authorization Request Cryptogram, авторизационная криптограмма
audit log	Общий лог событий

CV (KCV)	Checksum value (key checksum value), контрольная сумма криптографического ключа
Error log	Лог с ошибками
HSM	Аппаратный криптографический модуль (Hardware Security Module), криптографическое средство шифрования информации и управления ключами
LMK	Local Master Key, главный локальный криптографический ключ HSM, с помощью которого происходит шифрование других криптографических ключей и данных
LMKs	Массив LMK или набор локальных мастер-ключей для одного типа криптографического алгоритма, имеющий один идентификатор
PAN	Primary account number, номер карты

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие требования разработаны и утверждены в рамках мероприятий федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»: 05.02.002.017.003 – «Определение порядка разработки, ответственных за поддержание в актуальном состоянии, а также разработка и опубликование функционально-технических требований к техническим средствам и программному обеспечению, реализующим СКЗИ (включая функциональные и эксплуатационные требования): аппаратный модуль безопасности (HSM-модули); платежные устройства с терминальным ядром; платежные карты (криптомодуль, приложение); интернет-браузеры и стандартные операционные системы и т.д.».

Настоящий документ определяет функционально-технические требования к техническим средствам и программного обеспечению, реализующим СКЗИ к аппаратному модулю безопасности (HSM-модуль).

Проведение тестирования технических средств на соответствие требованиям, представленным в настоящем документе, осуществляется с привлечением Центра тестирования технических средств и программного обеспечения в соответствии с регламентом и методиками проведения тестирования[1].

[1] Регламент и методики проведения тестирования разрабатываются в рамках выполнения мероприятия 05.02.002.017.008 «Создание и обеспечение функционирования центра тестирования технических средств и программного обеспечения на соответствие функционально-техническим требованиям, включая разработку регламента и методики тестирования» паспорта федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации», утвержденного президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для

Подтверждение соответствия требованиям настоящего документа не исключает подтверждение соответствия требованиям, устанавливаемым платежными системами, а также требованиям по информационной безопасности ФСБ России.

2. НЕФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

2.1. Требования к управлению LMKs

2.1.1. LMKs при необходимости их хранения в долговременной памяти HSM должны храниться в защищенном виде.

2.1.2. Должно обеспечиваться защищенное хранение LMKs-ключа на съемных носителях в виде шифрограммы или в виде не менее двух компонент. В случае сохранения LMKs в виде шифрограммы ключ, обеспечивающий доступ к LMKs, должен храниться на съемных носителях в виде не менее двух компонент.

2.1.3. Должна обеспечиваться возможность периодической смены LMKs и оповещение об истечении срока их действия.

2.1.4. При смене LMKs должна быть обеспечена возможность перешифрования информации, хранящейся на хосте в зашифрованном под LMKs виде.

2.1.5. Необходима поддержка работы с двумя и более LMKs (главными локальными криптографическими ключами HSM) одного или разных типов. *Например, 3DES LMK с идентификатором 00 и AES LMK с идентификатором 01 загружены на один HSM.* На усмотрение вендора или заказчика допустима реализации работы не с массивом LMKs, а с одним LMK.

2.1.6. На усмотрение вендора или заказчика допустима реализация работы с LMKs по алгоритму ГОСТ Р 34.12-2015.

2.2. Требования к операциям с ключами

2.2.1. Генерация всех ключей в HSM должна производиться с использованием ГСЧ.

2.2.2. Должна быть исключена возможность создания ключей, являющихся слабыми для данного алгоритма создания криптографических ключей.

улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 27 декабря 2018 № 6) / задача 1.22 «Обеспечение информационной безопасности, в том числе с использованием российских криптографических средств, в значимых платежных системах» паспорта федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации», утвержденного президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28 мая 2019 № 9, приложение 5 и приложение 8).

2.2.3. Вывод формируемых HSM-ключей в открытом виде на внешние носители или средства отображения должен быть невозможен.

2.2.4. Для защиты ключей разных типов, хранящихся на хосте, должна быть возможность использования различных LMK и/или различных диверсификаций LMK.

2.2.5. Должна обеспечиваться возможность загрузки заранее известных ключей, используемых в тестовых целях. Цели использования HSM регулируются организационными мерами.

2.3. Требования к ролевой модели

2.3.1. В HSM должны минимально поддерживаться следующие роли:

— администратор информационной безопасности, создающий учетные записи остальных администраторов (пользователей) со следующими полномочиями:

- создание резервной копии,
- проведение аудита журналов HSM;

— не менее двух администраторов управления, совместные действия которых позволяют проводить управление ключевой системой и платежными функциями.

2.3.2. Не допускается совмещение ролей администраторов информационной безопасности и администраторов управления HSM.

2.4. Требования к разграничению доступа

2.4.1. Доступ Администратора к функциям HSM должен осуществляться только после его двухфакторной аутентификации.

2.4.2. Доступ к управлению учетными записями пользователей HSM должен иметь только Администратор и только после его двухфакторной аутентификации.

2.4.3. Доступ к функциям управления платежными функциями HSM должен осуществляться только после аутентификации двух Администраторов, отвечающих за управление платежными функциями HSM.

2.4.4. Доступ к созданию резервных копий LMKs должны иметь только Администраторы с соответствующими полномочиями (см. требование 2.3.1).

2.4.5. Доступ к изменению (очистка, выгрузка) журналов регистрации событий HSM должны иметь только Администраторы с соответствующими полномочиями (см. требование 2.3.1).

2.4.6. Доступ к просмотру (без прав на изменение) журналов регистрации событий HSM должны иметь все Администраторы HSM и все Пользователи HSM.

2.4.7. Доступ к функциям по управлению ключевой системой HSM (авторизованный режим) должен осуществляться только после аутентификации двух Администраторов управления.

2.4.7.1. Список критичных платежных функций, требующих выполнения в авторизованном режиме, может быть расширен Администратором управления за счет установки соответствующих настроек.

2.5. Требования к управлению HSM

2.5.1. Управление (настройка) функциями HSM должно осуществляться посредством локальной и/или удаленной консоли управления с выводом результатов выполнения функций управления на экран.

2.5.2. В случае использования удаленной консоли управления канал управления должен быть защищен.

2.5.3. Возможность перевода HSM в авторизованное состояние и обратно с локальной или удаленной консоли управления.

2.5.4. Рекомендованные функции управления и настройки, доступные для параметризации в авторизованном режиме:

2.5.4.1. Постоянное разрешение активности в авторизованном режиме.

2.5.4.2. Включение принудительного ограничения времени авторизации.

2.5.4.3 Задание длины PIN.

2.5.4.4. Задание запрета вывода «чистого» PIN.

2.5.4.5. Задание проверки «слабых» PIN.

2.5.4.6. Задание запрета «уязвимых» PIN-блоков.

2.5.4.7. Добавление поддержки PIN-offset различной длины.

2.5.4.8. Включение нескольких авторизованных активностей.

2.5.4.9. Задание проверки слабых ключей в режимах генерации и импорта DES-ключей.

2.5.4.10. Импорт ключей.

2.5.4.11. Экспорт ключей.

2.5.4.12. Таблица децимализации Зашифрованная/Незашифрованная.

2.5.4.13. Добавление проверки таблицы децимализации.

2.5.5. Настройки, возможные к параметризации как на уровне отдельных настроек в авторизованном режиме, так и на уровне команд:

2.5.5. 1. Включить команду «Echo».

2.5.5. 2. Задать идентификатор LMK по умолчанию.

2.5.5. 3. Включить трансляцию ZMK.

2.5.5. 4. Включить поддержку X9.17 для импорта ключей.

2.5.5. 5. Включить поддержку X9.17 для экспорта ключей.

2.5.5. 6. Включить необходимость авторизованного состояния для импорта DES- ключей с использованием RSA-ключей.

2.5.5. 7. Выбор минимальной длины ключа для HMAC.

2.5.5. 8. Включить PKCS#11 для импорта и экспорта ключей HMAC.

2.5.5. 9. Включить ANSI X9.17 для экспорта и импорта ключей HMAC.

2.5.5. 10. Включить ZEK/TEK-шифрование для данных в ASCII или двоичных данных.

2.5.5. 11. Ограничить CV шестью знаками в hex.

2.5.5.12. Включить поддержку замены (трансляции) номера карты в PIN-блоке, зашифрованном с использованием LMK. При этом сам PIN не меняется.

2.5.5. 13. Использовать внутренние часы HSM для проверки времени.

2.5.5. 14. Включить импорт и экспорт ключей только в доверенном формате.

2.5.5. 15. Включить использование токенов при трансляции PIN.

2.5.5. 16. Включить использование токенов при проверке PIN.

2.5.5. 17. Управление идентификаторами LMK.

2.5.5. 18. Дополнительный паддинг для маскировки длины ключа.

2.6. Требования к резервированию и восстановлению

2.6.1. HSM должен обеспечивать возможность резервного копирования в защищенном виде LMKs, сертификатов (при наличии) и настроек на внешний носитель.

2.6.2. HSM должен обеспечивать возможность восстановления (загрузки) LMKs, сертификатов (при наличии) и настроек с внешних носителей в HSM.

2.7. Требования к тестированию

2.7.1. HSM должен обеспечивать возможность использования заранее известных LMKs в тестовых целях (тестовых LMKs). Данные LMKs должны быть опубликованы вендором. Цели использования тестовых LMKs в HSM регулируются организационными мерами.

2.7.2. HSM должен обеспечивать периодическую проверку работоспособности в автоматическом режиме и/или по команде Администратора.

2.8. Требования к регистрации

2.8.1. В HSM должна вестись регистрация действий Администраторов и Пользователей и выполняемых платежных функций.

2.8.2. В HSM должна вестись регистрация сообщений о системных ошибках (Error_log).

2.8.3. HSM должен обеспечивать возможность аудита журналов регистрации.

2.9. Требования к отказоустойчивости

2.9.1. HSM должен иметь два блока питания либо блок питания с резервированием.

2.9.2. HSM должен обеспечивать непрерывный режим работы 24/7 365 дней в году в течение всего срока эксплуатации.

2.10. Требования к быстродействию

2.10.1. HSM должен обеспечивать обработку 1 (одной) DES-операции за время не более чем 0,5 мс (миллисекунды).

2.10.2. HSM должен обеспечивать обработку 1 (одной) AES-операции за время не более чем 0,5 мс (миллисекунды) при длине ключа 128 бит.

2.10.3. HSM должен обеспечивать следующее время обработки операций:

Используемые команды	Максимальное время обработки для вариантного метода, мс	Максимальное время обработки для keyblock, мс
трансляция PIN-блока (трансляция PIN-блока с одного ZPK на другой ZPK)	2	3
проверка криптовеличины CVP (проверка CVC/ CVV)	1,5	2,3
проверка PIN с использованием метода VISA PVV	1,5	2,3
перешифрование PIN-блока с ZPK на LMK	1,5	2,3
перешифрование PIN-блока с LMK на ZPK	1,5	2,3
проверка криптограммы ARQC и генерация ARPC ((EMV 4.x))	4	5
шифрование блока данных 16 байт	1,5	2,3
расшифрование блока данных 16 байт	1,5	2,3
трансляция PAN без смены PIN, при этом PIN зашифрован на LMK	1,5	2,3

2.10.4. HSM должен обеспечивать возможность не менее 128 одновременных логических соединений.

2.11. Требования к физическим интерфейсам

2.11.1. HSM должен иметь не менее двух активных портов Ethernet (интерфейсов) для подключения к хост-системе и один порт управления Ethernet (management-интерфейс).

2.11.2. HSM должен иметь минимум два USB-порта (интерфейса), в том числе для подключения принтера для печати PIN-конвертов.

2.12. Требования к совместимости с хостовым ПО и выполнению команд

2.12.1. HSM должен обеспечивать обработку консольных и хостовых команд.

2.12.2. HSM должен обеспечивать подключение к хост-системе по интерфейсу Ethernet.

2.12.3. HSM должен обеспечивать взаимодействие с хостовым ПО по протоколам TCP или UDP:

2.12.3.1.HSM при работе по протоколу TCP должен выступать в качестве TCP-сервера и обрабатывать команды, посылаемые хостовым ПО, после установления TCP-сессии.

2.12.3.2.HSM при работе по протоколу UDP должен выступать в качестве UDP-сервера и обрабатывать команды, посылаемые хостовым ПО, без установления сессии.

2.12.4. HSM должен корректно обрабатывать прикладные команды, посылаемые хостовым ПО:

2.12.4.1.HSM не должен обрабатывать команду, если она сформирована некорректно.

2.12.4.2.Если команда сформирована некорректно, то HSM должен выдавать определенный код ошибки. Код ошибки должен быть описан в документации для идентификации проблемы.

2.12.4.3.HSM по результатам выполнения команды должен обеспечивать формирование ответного сообщения, содержащего в обязательном порядке код выполнения команды (норма или код ошибки) и выходные и/или диагностические данные (опционально).

2.12.4.4.HSM, находящийся в неавторизованном состоянии, не должен обрабатывать команды, требующие состояния авторизации.

2.12.5. HSM может обеспечивать выполнение команд управления по web-интерфейсу.

2.13. Требования к документации

2.13.1. Эксплуатационная документация HSM должна включать следующие сведения:

2.13.1.1.сведения о комплектации HSM;

2.13.1.2.сведения о назначении HSM и основных функциях;

2.13.1.3.сведения о физических интерфейсах;

2.13.1.4.информацию о средствах управления HSM;

2.13.1.5.информацию о поддерживаемых ролях HSM;

2.13.1.6.описание конфигурации и настроек функционирования HSM;

2.13.1.7.описание порядка ввода в эксплуатацию HSM;

2.13.1.8.описание порядка регистрации Администраторов и Пользователей, а также записи носителей аутентификации;

2.13.1.9.описание порядка аутентификации Администратора и Пользователя;

2.13.1.10. описание начала работы HSM;

2.13.1.11. описание режимов эксплуатации HSM;

2.13.1.12. описание порядка действий Администратора и Пользователя при работе с локальной и/или удаленной консолью управления HSM;

2.13.1.13. описание порядка генерации и смены LMK;

2.13.1.14. описание консольных и хостовых команд;

2.13.1.15. описание кодов ошибок.

2.13.2. Программная документация HSM должна включать следующие сведения:

2.13.2.1.описание программы;

2.13.2.2.описание протоколов (как сетевого, так и прикладного уровней) и форматов взаимодействия с ПО хост-системы;

2.13.2.3.описание всех выполняемых функций HSM, включая описание входных и выходных параметров;

2.13.3. Должны быть разработаны правила пользования HSM, включающие следующие сведения:

2.13.3.1. общие сведения (класс СКЗИ и реализуемые им криптографические функции, вид и формат защищаемой и защищенной информации, условия эксплуатации СКЗИ и ограничения на использование СКЗИ);

2.13.3.2. инструкция по вводу СКЗИ в эксплуатацию;

2.13.3.3. порядок формирования (изготовления) и работы с ключевой информацией, а также меры защиты ключевой информации от несанкционированного доступа;

2.13.3.4. меры по обеспечению целостности СКЗИ и документации на СКЗИ после завершения производства, хранения, транспортировки и ввода в эксплуатацию (пусконаладочных работ) СКЗИ и на этапе его эксплуатации;

2.13.3.5. меры по защите от несанкционированного доступа к информации в системах, в которых используются СКЗИ, в том числе административный регламент и порядок проверки выполнения требований по защите от несанкционированного доступа к информации, СКЗИ;

2.13.3.6. порядок действий в нештатных ситуациях, связанных с использованием СКЗИ, инструкция по контролю технических характеристик СКЗИ при эксплуатации и хранении СКЗИ;

2.13.3.7.перечень ситуаций, в которых должно производиться аварийное (экстренное) уничтожение ключевой и криптографически опасной информации;

2.13.3.8. порядок выполнения технического обслуживания, регламентных работ, ремонта, вывода из эксплуатации и утилизации СКЗИ;

2.13.3.9. организационные меры по обеспечению безопасности СКЗИ.

2.13.4. Должны быть разработаны правила встраивания HSM в банковское ПО, включающие следующие сведения:

2.13.4.1.требования к установке общесистемного и специального ПО, включая требование по отсутствию средств разработки и отладки ПО;

2.13.4.2. меры контроля целостности аппаратного и программного обеспечения;

2.13.4.3.требования по конфигурации СКЗИ и общесистемного ПО, а также СЗИ, используемых совместно с СКЗИ;

2.13.4.4. требования по хранению ключевой и аутентификационной информации используемого при эксплуатации СКЗИ.

2.13.4.5.конкретные требования по встраиванию, содержащие перечень аргументов и возвращаемых значений криптографических функций, обеспечивающих возможность использования СКЗИ, с указанием допустимых значений этих параметров.

2.14. Требования к мониторингу состояния

2.14.1. Необходим полный вывод информации о работе HSM, в частности:

2.14.1.1.вывод информации о доступности Host port;

2.14.1.2.вывод информации о доступности Management port;

2.14.1.3.вывод информации о текущих командах, которые обрабатывает HSM;

2.14.1.4.вывод информации о загрузке в процентах;

2.14.1.5.вывод информации о времени ответа на различные команды (с разбивкой по каждой команде отдельно);

2.14.1.6.вывод информации о количестве обрабатываемых команд;

2.14.1.7.вывод информации о количестве сообщений в Error log;

2.14.1.8.вывод информации о количестве сообщений в audit log;

2.14.1.9.вывод информации о количестве перезагрузок с момента инициализации;

2.14.1.10. вывод информации о версии прошивки;

2.14.1.11. вывод информации серийного номера;

2.14.1.12. вывод информации о времени работы HSM с момента последней перезагрузки;

2.14.1.13. вывод информации о состоянии HSM;

2.14.2. Передача информации о контролируемых параметрах состояния и функционирования HSM осуществляется по настраиваемым значениям за указанный интервал (раз в минуту/10 сек./1 час).

3. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

3.1. Перечень необходимых криптографических алгоритмов и стандартов

3.1.1. DES/3DES в соответствии с NIST FIPS 46-3/NIST Special Publication 800-67 и ISO/IEC 10116 (ECB, CBC).

3.1.1.1. Генерация симметричных ключей (DES/3DES) различной длины (64, 128 и 192 бита с учетом битов четности) с использованием встроенного ГСЧ.

3.1.1.2. Сформированный DES-ключ проверяется HSM по таблицам «слабых» DES-ключей.

3.1.1.3. Двойной (тройной) 3DES-ключ не должен быть сформирован с использованием одинаковых одиночных ключей.

3.1.1.4. Сгенерированный ключ выводится в зашифрованном виде с использованием LMK или с использованием ZMK.

3.1.1.5. Вместе со сгенерированным ключом должна выводиться контрольная величина ключа: не менее трех левых байтов результата зашифрования с использованием сгенерированного ключа 64 бинарных ‘0’.

3.1.1.6. Примечание – для выполнения функции генерации ключей требуется авторизованное состояние HSM (если задана соответствующая настройка в консольном режиме).

3.1.2. AES в соответствии с NIST FIPS 197

3.1.2.1. Генерация симметричных ключей (AES) различной длины (128, 192 или 256 битов) с использованием встроенного ГСЧ HSM.

3.1.2.2. Сформированный ключ выводится в зашифрованном виде с использованием LMK или с использованием ZMK в формате key block.

3.1.2.3. Вместе со сгенерированным ключом должна выводиться контрольная величина ключа. Алгоритм определяется вендором.

3.1.2.4. Примечание – для выполнения функции генерации ключей требуется авторизованное состояние HSM (если задана соответствующая настройка в консольном режиме).

3.1.3. RSA в соответствии RFC 3447 и NIST FIPS 186-4

3.1.3.1. Генерация пары ключей RSA: закрытый ключ (длиной от 400 до 4096 битов) и открытый ключ (DER-кодирование для ASN.1 Public Key: unsigned representation и 2's complement representation) с использованием встроенного ГСЧ HSM.

3.1.3.2. Сформированный ключ требует проверки на слабые ключи.

3.1.4. SHA-1 в соответствии с RFC 3174 и NIST FIPS 180-4, SHA-224, SHA-384, SHA-256, SHA-512 в соответствии с ISO/IEC 10118-2 и NIST FIPS 180-4

3.1.4.1. Вычисление значения хэш-функции блока данных.

3.1.4.2. HSM вычисляет значение хэш-функции блока данных и возвращает в хост-систему.

3.1.5. MAC с использованием DES, 3DES, AES.

3.1.5.1. Генерация MAC за данные в соответствии с:

– ISO 9797-1 MAC algorithm 1 или algorithm 3 (DES, 3DES);
– CBC_MAC (AES);
– CMAC (AES).

3.1.5.2. HSM вычисляет MAC за сообщение, подаваемое на вход функции, и возвращает вычисленный MAC хост-системе.

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

3.1.6.1. Вычисление значения HMAC в соответствии с ISO/IEC 9797-2 (MAC Algorithm 2) и NIST FIPS 198-1 блока данных.

3.1.6.2. HSM должен обеспечивать возможность вычисления HMAC с использованием алгоритмов хэш-функции: SHA-224, SHA-384, SHA-256, SHA-512.

3.1.6.3. HSM вычисляет значение HMAC блока данных и возвращает в хост-систему.

3.1.7. Представление ключей в формате key block в соответствии с «ANSI TR-31: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms».

3.1.7.1. Формирование ключевого контейнера в формате key block в соответствии с «ANSI TR-31».

3.1.7.2. HSM формирует на хосте ключевой контейнер в формате key block в соответствии с «ANSI TR-31».

3.2. Требования по функциям

3.2.1. Генерация симметричных и асимметричных ключей

3.2.1.1. Генерация DES-, 3DES-, AES-ключа. *На усмотрение вендора или заказчика допустима реализации работы с LMK по алгоритму ГОСТ Р 34.12-2015. Должно быть доступно и в хостовом, и в консольном режиме.*

3.2.1.2. Генерация и печать компоненты ключа (ZMK).

3.2.1.3. Генерация ключевой пары RSA (закрытого и открытого ключей). При этом:

- открытый ключ выдается в DER-кодировании для ASN.1 Public Key.
- закрытый ключ (в соответствии с pkcs #1 - rfc 3447), зашифрованный с использованием LMK.

3.2.1.4. Генерация чистых компонент двойной длины ключа ZMK. *Доступно и в хостовом, и в консольном режиме.*

3.2.1.5. Генерация компоненты ключа ZMK (чистой или зашифрованной). *Доступно и в хостовом, и в консольном режиме.*

3.2.1.6. Генерация компоненты ключа (чистой или зашифрованной). *Доступно и в хостовом, и в консольном режиме.*

3.2.1.7. Экспорт LMK. *Доступно только в консольном режиме.*

3.2.1.8. Генерация LMK. *Доступно только в консольном режиме.*

3.2.1.9. Импорт (восстановление) LMK. *Доступно только в консольном режиме.*

3.2.1.10.Генерация ключа и запись компонент на защищенный носитель. *Доступно и в хостовом, и в консольном режиме.*

3.2.1.11.Генерация ключа ZMK с записью на защищенный носитель. *Доступно и в хостовом, и в консольном режиме.*

3.2.1.12.Генерация ключа для HMAC.

3.2.1.13.Формирование 3DES и AES-ключей из компонент. *Доступно только в консольном режиме.*

3.2.2. Действия с симметричными ключами (за исключением генерации из раздела 3.2.1)

3.2.2.1. Формирование ключа (ZMK) из зашифрованных компонент (2–9 компонент). HSM расшифровывает компоненты и формирует ключ сложением компонент по mod 2. Если используется 3DES, то сформированный ключ проверяется по таблицам «слабых» DES-ключей. Сформированный ключ выводится в зашифрованном виде с использованием LMK. Вместе со сформированным ключом должна выводиться контрольная величина ключа. Формирование ключа (ZMK) из двух или трех зашифрованных компонент обязательно к реализации. Формирование ключа (ZMK) из более чем трех (4–9) зашифрованных компонент опционально. *Должно быть доступно и в хостовом, и в консольном режиме.*

3.2.2.2. Формирование ключа (ZMK) из чистых компонент (из двух или трех компонент). HSM формирует ключ сложением введенных компонент по mod 2. Если используется 3DES, то сформированный ключ проверяется по таблицам «слабых» DES-ключей. Сформированный ключ выводится в зашифрованном виде с использованием LMK. Вместе со сформированным ключом должна выводиться контрольная величина ключа. Формирование ключа (ZMK) из более чем трех (4–9) компонент опционально. *Должно быть доступно и в хостовом, и в консольном режиме.*

3.2.2.3. Формирование ключа из чистых или зашифрованных компонент (аналогично п.3.2.2.1 или 3.2.2.2).

3.2.2.4. Импорт ключа с проверкой CV. HSM перешифровывает импортируемый ключ из-под ключа импорта под ключ LMK. Расшифрованный ключ проверяется по таблицам «слабых» DES-ключей. Вместе со сформированным ключом должна выводиться контрольная величина ключа. *Должно быть доступно и в хостовом, и в консольном режиме.*

3.2.2.5. Трансляция (экспорт) ключа, зашифрованного с помощью LMK, в ключ, зашифрованный с помощью ZMK.

3.2.2.6. Трансляция (перешифрование) CVK-pair, зашифрованного с помощью старого LMK, в CVK-pair, зашифрованный с использованием нового LMK.

3.2.2.7. Генерация (проверка) CV для ключа (ZMK), зашифрованного с помощью LMK. HSM формирует CV в соответствии с документом Global Platform v.2.2.1 Appendix B.6.

3.2.2.8. Трансляция (перешифрование) ключа, зашифрованного с помощью старого LMK, в ключ, зашифрованный с использованием нового LMK, и миграция на новый тип ключа.

3.2.2.9. Трансляция (перешифрование) PIN-блока, зашифрованного с помощью одного ZPK, в PIN-блок, зашифрованный с использованием нового ZPK (TPK, BDK).

3.2.2.10. Трансляция (перешифрование) PIN-блока, зашифрованного с использованием ZPK, в PIN-блок, зашифрованный с использованием LMK. *Должно быть доступно и в хостовом, и в консольном режиме.*

3.2.2.11. Трансляция (перешифрование) PIN-блока, зашифрованного с использованием LMK, в PIN-блок, зашифрованный с использованием ZPK (TPK, BDK). *Должно быть доступно и в хостовом, и в консольном режиме.*

3.2.2.12. Вывод мастер-ключа карты из соответствующего мастер-ключа эмитента (MK-CL, MK-IDN). Ключи MK_{CL} и MK_{IDN} выводятся из соответствующих мастер-ключей эмитента IMK_{CL} и IMK_{IDN} в соответствии с алгоритмами документа «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.3 (случай 1 и случай 2). HSM производит в соответствии с заданными алгоритмами генерацию ключей MK_{AC} и MK_{IDN} и вывод их в хост-систему в защищенном (зашифрованном) виде с использованием транспортного ключа (Key Encryption Key – KEK).

3.2.2.13. Вывод мастер-ключей карты MK_{AC}, MK_{SMC}, MK_{SMI}, MK_{IDN}. Ключи MK_{AC}, MK_{SMC}, MK_{SMI}, MK_{IDN} выводятся из соответствующих мастер-ключей эмитента IMK_{AC}, IMK_{SMC}, IMK_{SMI}, IMK_{IDN} в соответствии с алгоритмами документа «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.3 (случай 1 и случай 2). HSM производит в соответствии с заданными алгоритмами генерацию ключей MK_{AC}, MK_{SMC}, MK_{SMI}, MK_{IDN} и вывод их в хост-систему в защищенном (зашифрованном) виде с использованием транспортного ключа (Key Encryption Key – KEK) для передачи в систему персонализации.

3.2.2.14. Зашифровать блок данных.

3.2.2.15. Расшифровать блок данных.

3.2.2.16.Зашифровать чистую компоненту. *Должно быть доступно и в хостовом, и в консольном режиме.*

3.2.2.17.Зашифровать чистую компоненту ключа ZMK. *Должно быть доступно и в хостовом, и в консольном режиме.*

3.2.2.18.Трансляция (перешифрование) ZPK. *Должно быть доступно только в консольном режиме.*

3.2.3. Защищенный обмен с картой при производстве по протоколу SCP-02.

3.2.3.1. Диверсификация ключей с использованием HSM для формирования ключей карты в соответствии с Global Platform v.2.2.1 (E.2.): ключа защиты ключей, ключа для поддержки конфиденциальности сообщений и формирования криптограмм, ключей для поддержки целостности сообщений. Вывод ключей в хост в виде key block под LMK или совмещение функции диверсификации ключей с функцией формирования сессионных ключей для защищенного обмена с картой (п.3.2.3.2), в этом случае шифрограммы ключей карты в хост не выдаются.

3.2.3.2. Формирование с использованием HSM сессионных ключей для защищенного обмена с картой в соответствии с Global Platform v.2.2.1 (E.4.1.): ключа защиты ключей, ключа для поддержки конфиденциальности сообщений и формирования криптограмм, ключа для поддержки целостности сообщений. Вывод ключей в хост в виде key block под LMK.

3.2.3.3. Формирование с использованием HSM криптограммы хоста в соответствии с Global Platform v.2.2.1 (E.4.2.). Вывод криптограммы в хост.

3.2.3.4. Формирование с использованием HSM криптограммы карты в соответствии с Global Platform v.2.2.1 (E.4.2.) и сравнение с принятой. Вывод результата сравнения в хост.

3.2.3.5. Шифрование с использованием HSM ключей для загрузки на карту в соответствии с Global Platform v.2.2.1 (E.4.7.). HSM перешифровывает ключи для загрузки на карту из-под транспортных ключей под сессионный ключ защиты ключей и выдает результат зашифрования в хост. Данная функция может быть совмещена с функцией формирования сообщений (п. 3.2.4), в этом случае шифрограмма ключей в хост не выдается.

3.2.3.6. Формирование с использованием HSM сообщений с поддержкой конфиденциальности и целостности в соответствии с Global Platform v.2.2.1 (Appendix E). HSM, в зависимости от настроек безопасности установления сеанса защищенного обмена сообщениями, на основе входных данных

формирует сообщение-запрос с поддержкой конфиденциальности и/или целостности и выдает сформированное сообщение в хост.

3.2.3.7. Проверка с использованием HSM целостности сообщений (и расшифровка данных, при необходимости) в соответствии с Global Platform v.2.2.1 (Appendix E). HSM выполняет проверку целостности полученного от карты сообщения-ответа и выдает результат проверки в хост.

3.2.4. Защищенный обмен с картой при эмиссии по протоколу SCP-02

3.2.4.1. Диверсификация ключей с использованием HSM для формирования мастер-ключей карты для персонализации: K_{ENC}, K_{DEC}, K_{MAC}. Ключи K_{ENC}, K_{DEC}, K_{MAC} могут выводиться из KMC (Initial Issuer Master Key – первоначальный мастер-ключ Эмитента) двумя способами:

– с использованием алгоритма EMV CPS 1.1 в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.8.1;

– с использованием алгоритма Visa2 в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.8.2.

Вывод ключей в хост в виде key block под LMK или совмещение функции диверсификации ключей с функцией формирования сессионных ключей для защищенного обмена с картой (п.3.2.4.2), в этом случае шифрограммы ключей карты в хост не выдаются.

3.2.4.2. Формирование с использованием HSM сессионных ключей для защищенного обмена с картой в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.9: SKU_{ENC}, SKU_{DEC}, SKU_{MAC}. Вывод ключей в хост в виде key block под LMK.

3.2.4.3. Формирование с использованием HSM криптограммы карты в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.9, Global Platform v.2.2.1 (Appendix E) и EMV CPS v.1.1, п.3.2.5 и сравнение с принятой. Вывод результата сравнения в хост.

3.2.4.4. Шифрование с использованием HSM конфиденциальных данных для загрузки на карту в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.9, Global Platform v.2.2.1 (Appendix E) и EMV CPS v.1.1., пп.5.5, 5.6, 5.7. HSM перешифровывает конфиденциальные данные

для загрузки на карту из-под транспортных ключей под сессионный ключ SKU_{DEC} и выдает результат зашифрования в хост. Данная функция может быть совмещена с функцией формирования сообщений (п.3.2.4.5), в этом случае шифрограмма ключей в хост не выдается.

3.2.4.5. Формирование с использованием HSM сообщений с поддержкой конфиденциальности и целостности в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», Global Platform v.2.2.1 (Appendix E) и EMV CPS v.1.1., п.5.4. HSM, в зависимости от настроек безопасности установления сеанса защищенного обмена сообщениями, на основе входных данных формирует сообщение-запрос с поддержкой конфиденциальности и/или целостности и выдает сформированное сообщение в хост.

3.2.4.6. Проверка с использованием HSM целостности сообщений (и расшифровка данных, при необходимости) в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», Global Platform v.2.2.1 (Appendix E) и EMV CPS v.1.1., п.5.4. HSM выполняет проверку целостности полученного от карты сообщения-ответа и выдает результат проверки в хост.

3.2.5. Генерация и проверка криптограмм, обработка сообщений

3.2.5.1. Генерация CVP (CVC/CVV)/ППК. CVP/ППК (Card Verification Parameter/Проверочный параметр карты) – трехзначный код проверки подлинности карты «Мир». CVP/iCVP/CVP2 формируется в соответствии с документом «Требования к данным на магнитной полосе и EMV-эквиваленте карты платежной системы «Мир», п.2.6. HSM производит генерацию CVP (CVC/CVV)/ППК и выводит сформированное значение в хост-систему. В процессе проверки вычисляется значение CVP/iCVP/CVP2, которое сравнивается с полученным в ходе транзакции по магнитной полосе, транзакции чиповой карты в моде магнитной полосы или транзакции электронной коммерции значением CVP/iCVP/CVP2 карты «Мир». Если вычисленное и присутствующее на карте «Мир» значения CVP/iCVP/CVP2 совпадают, то проверка выполнена успешно. *Должно быть доступно и в хостовом, и в консольном режиме.*

3.2.5.2. Проверка криптовеличины CVP (CVC/CVV). HSM производит проверку CVP/iCVP/CVP2 (CVC1/CVC2/Chip CVC) и передает результат проверки хост-системе.

3.2.5.3. Проверка a Dynamic Card Verification Value (dCVV) или Card Verification Code (CVC3). HSM производит проверку dCVV или CVC3 (в

зависимости от типа платежной системы: «Мир», Visa, MasterCard, American Express, UnionPay, JCB – и заданного метода расчета) и передает результат проверки хост-системе.

3.2.5.4. Генерация и проверка криптовеличины PVV по алгоритму VISA PVV. PVV – эталонная величина для проверки PIN. Проверка PVV осуществляется в соответствии с документом «Требования к данным на магнитной полосе и EMV-эквиваленте карты платежной системы «Мир», п.2.5. HSM производит проверку PIN по зашифрованному PIN-блоку и PVV, результат проверки передает в хост-систему. В процессе проверки по расшифрованному PIN-блоку вычисляется значение PVV, которое сравнивается с полученным в аутентификационном сообщении PVV карты «Мир». Если вычисленное и присутствующее на карте «Мир» значения PVV совпадают, то PIN считается верным, если нет, то неверным.

3.2.5.5. Проверка криптограммы ARQC и/или генерация ARPC (EMV 3.1.1).

3.2.5.6. Проверка криптограммы ARQC и/или генерация ARPC (EMV 4.x).

— Криптограмма приложения (ARQC, TC, AAC) вычисляется с использованием алгоритма MAC (алгоритм 3 ISO/IEC 9797-1) в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», п.3.2. MAC формируется с использованием сессионного ключа SK_{AC}. Сессионный ключ SK_{AC} формируется из мастер-ключа карты MK_{AC} в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.4. Ключ MK_{AC} выводится из мастер-ключа эмитента IMK_{AC} в соответствии с алгоритмами документа «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.3 (случай 1 и случай 2).

— Криптограмма ARPC вычисляется в случае положительной проверки прикладной криптограммы Authorization Request Cryptogram (ARQC), сформированной платежным приложением карты. Криптограмма ARPC вычисляется с помощью алгоритма вычисления величины MAC с использованием сессионного ключа SK_{AC}, значения ARQC, 4-байтного элемента данных Card Status Update (CSU) и элемента Proprietary Authentication Data нулевой длины в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», п.3.5.

3.2.5.7. Вычисление и проверка American Express Card Security Codes (CSC): CSC3, CSC4 и CSC5.

3.2.5.8. Проверка криптограммы ARQC и/или генерация ARPC в соответствии с документацией Union Pay.

3.2.5.9. Проверка и/или генерация криптограммы MST. Криптограмма MST вычисляется с использованием алгоритма MAC (алгоритм 3 ISO/IEC 9797-1 padding 2) с последующей децимализацией. MAC формируется с использованием сессионного ключа SK_{AC}. Сессионный ключ SK_{AC} формируется из мастер-ключа карты MK_{AC} в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.4. Ключ MK_{AC} выводится из мастер-ключа эмитента IMK_{AC} в соответствии с алгоритмами документа «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир», приложение 1.3 (случай 1 и случай 2). HSM производит:

— вывод ключа MK_{AC} из IMK_{AC};

— вывод ключа SK_{AC} из MK_{AC};

— генерацию в соответствии с заданными алгоритмами криптограммы MST и сравнение с принятой;

— вывод в хост-систему результата проверки криптограммы.

3.2.5.10.Генерация и проверка IDN (ICC Dynamic Number). HSM вычисляет IDN как функцию номера текущей транзакции ATC (Application Transaction Counter) с использованием мастер-ключа MK_{IDN} в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир» и сравнивает со значением во входных данных. Результат сравнения возвращается хост-системе.

3.2.5.11. Проверка Truncated Application Cryptogram (MasterCard CAP). HSM на основе данных транзакции формирует CAP и сравнивает с полученной во входных данных. Результат проверки возвращается хосту. Функция 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.

3.2.5.12.Расшифрование счетчиков карты. HSM производит расшифрование счетчиков, содержащихся в объекте Issuer Application Data, подготовленном приложением для эмитента при онлайновой аутентификации, в

соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир».

3.2.5.13.Генерация и проверка CAVV. HSM производит вычисление MAC в соответствии с ISO 9797-1 MAC (algorithm 2) за данные транзакции и сравнивает со значением, полученным от хост-системы. Результат сравнения возвращается в хост-систему.

3.2.5.14.Генерация сообщений скрипт-процессинга (Secure Message) с обеспечением целостности и конфиденциальности в соответствии с документом «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения ПС «Мир» и EMV 4.3, п.9. HSM с использованием сессионных ключей карты SK_{SMC} и SK_{SMI} выполняет зашифрование конфиденциальных данных (опционально) и расчет MAC за сообщение и возвращает зашифрованные данные и MAC хосту. Сессионные ключи SK_{SMC} и SK_{SMI} выводятся из мастер-ключей карты MK_{SMC} и MK_{SMI} соответственно согласно документу «Стандарт платежной системы «Мир». Механизмы безопасности платежного приложения платежной системы «Мир».

3.2.5.15.Генерация сообщений скрипт-процессинга с обеспечением целостности и конфиденциальности в соответствии с документацией Union Pay.

3.2.5.16.Создание и проверка криптограммы НСПК-CAV в соответствии с документом «Стандарт платежной системы «Мир». MirAccept 2.0. Руководство по внедрению для эмитента».

3.2.6. Действия с асимметричными ключами (за исключением генерации из раздела 3.2.1).

3.2.6.1. Трансляция (перешифрование) закрытого ключа, зашифрованного с помощью старого LMK в ключевом контейнере, в ключ, зашифрованный с использованием нового LMK.

3.2.6.2. Импорт открытого ключа RSA/ECDSA совместно с созданием MAC к нему с использованием LMK либо с созданием keyblock (преобразование в keyblock-формат).

3.2.6.3. Импорт закрытого ключа RSA/ECDSA под ZMK (AES или 3DES) в соответствии с ASC X9 TR 31-2018.

3.2.6.4. Экспорт закрытого ключа RSA/ECDSA из-под ZMK (AES или 3DES) в соответствии с ASC X9 TR 31-2018.

3.2.6.5. Экспорт открытого ключа RSA/ECDSA под ZMK (AES или 3DES).

3.2.6.6. Проверка открытого ключа.

3.2.6.7. Генерация RSA-подписи с использованием закрытого ключа.

3.2.6.8. Проверка RSA-подписи с использованием открытого ключа.

3.2.6.9. Импорт данных под открытым RSA-ключом (преобразование AES-, 3DES-, HMAC-ключа, зашифрованного открытым RSA-ключом, в HSM-формат с зашифрованием под LMK). Импортируемый DES-ключ проверяется по таблицам «слабых» DES-ключей.

3.2.6.10.Генерация (используется совместно с пунктом 3.2.4.4) или проверка (используется совместно с пунктом 3.2.4.5) RSA-подписи для длинных сообщений.

3.2.6.11.Экспорт AES-ключа (HMAC или 3DES) под открытым RSA-ключом (преобразование AES-ключа (или 3DES-ключа), зашифрованного с использованием LMK, в ключ, зашифрованный открытым RSA ключом). Экспортируемый DES-ключ проверяется по таблицам «слабых» DES-ключей.

3.2.6.12.Генерация ключевой пары RSA (закрытый и открытый ключ) эмитента и соответствующего самоподписанного сертификата по стандарту EMV.

Детали формата сертификата определяются документами соответствующей платежной системы («Мир», Visa, Master Card и т.д.).

3.2.6.13.Проверка EMV-сертификата RSA-ключа эмитента, подписанного корневым ключом УЦ, по стандарту EMV. Детали формата сертификата определяются документами соответствующей платежной системы («Мир», Visa, Master Card и т.д.). Для платежной системы «Мир» – в соответствии с документом «Описание форматов обмена данными с УЦ НСПК».

3.2.6.14.Импорт (с проверкой) EMV-сертификата корневого ключа УЦ. Детали формата сертификата определяются документами соответствующей платежной системы («Мир», Visa, Master Card и т.д.). Для платежной системы «Мир» – в соответствии с документом «Описание форматов обмена данными с УЦ НСПК».

3.2.6.15.Генерация ключевой пары RSA (закрытый и открытый ключ) карты. HSM выполняет генерацию ключевой пары RSA и возвращает открытый ключ в формате DER encoding in ASN.1 и закрытый ключ в виде шифрограммы под LMK или в формате из пяти компонент в соответствии с Китайской теоремой об остатках, зашифрованных под KEK.

3.2.6.16.Генерация ключевой пары RSA (закрытый и открытый ключ) и соответствующего сертификата x.509 v.3 (ITU-T X.509).

3.2.6.17.Генерация ключевой пары и выпуск неявных сертификатов в формате ECQV (Elliptic Curve Qu-Vanstone Implicit Certificate Sheme).

3.2.6.18.Преобразование открытой компоненты RSA ключа в формат key-block в соответствии с v1.5 method (EME-PKCS1-v1_5), PKCS#1 v2.2 2, OAEP method (EME-OAEP-ENCODE).

3.2.7. Функции для расчета MAC

3.2.7.1. Генерация ISO 9797-1 MAC (algorithm 1, 3). HSM вычисляет MAC за сообщение, подаваемое на вход функции, и возвращает вычисленный MAC хост-системе.

3.2.7.2. Проверка ISO 9797-1 MAC (algorithm 1, 3). HSM вычисляет MAC за сообщение, подаваемое на вход функции, сравнивает с MAC во входных данных и возвращает результат проверки MAC хост-системе.

3.2.8. Функции работы с HMAC

3.2.8.1. Генерация HMAC для блока данных. Вычисление значения HMAC в соответствии с ISO/IEC 9797-2 (MAC Algorithm 2) и NIST FIPS 198-1 за блок данных. HSM вычисление HMAC с использованием алгоритмов хэш-функции SHA-1, SHA-224, SHA-384, SHA-256, SHA-512.

3.2.8.2. Проверка HMAC для блока данных. HSM вычисляет значение HMAC за блок данных, сравнивает с HMAC во входных данных и возвращает результат сравнения в хост-систему.

3.2.8.3. Импорт ключа HMAC из-под ZMK.

3.2.8.4. Экспорт ключа HMAC под ZMK.

3.2.8.5. Трансляция (перешифрование) ключа для HMAC Key, зашифрованного с использованием старого LMK в ключевом контейнере, в ключ, зашифрованный с использованием нового LMK.

3.2.9. Функции работы с PIN (за исключением функций п.п.3.2.2 и 3.2.5).

3.2.9.1. Трансляция (смена) PAN для PIN-блока, зашифрованного с использованием LMK.

3.2.9.2. Генерация PIN с возможностью печати. HSM производит генерацию случайного PIN. Сформированный PIN в зашифрованном под LMK виде передается хост-системе или в открытом виде выводится на печать (в PIN-конверты). Примечание: для вывода PIN на печать требуется авторизованное состояние HSM.

3.2.9.3. Трансляция PIN-блока из одного формата в другой с возможностью перешифрования из-под одного ключа под другой. HSM расшифровывает PIN-блок, производит переформирование PIN-блока в заданный формат, зашифровывает под указанный ключ и возвращает зашифрованный PIN-блок хосту.

Допустимые форматы трансляции (ISO 9564-1):

– из формата ISO-0 (Format 0) в формат ISO-3 (Format 3) или формат ISO-4 (Format 4);

– из формата ISO-3 (Format 3) или формата ISO-4 (Format 4) в формат ISO-0 (Format 0);

– из формата ISO-1 (Format 1) в формат ISO-0 (Format 0);

– из формата ISO-1 (Format 1) в формат ISO-3 (Format 3) или формат ISO-4 (Format 4).

3.2.9.4. Генерация PIN-offset. HSM выполняет генерацию PIN-offset для PIN, расшифрованного из-под LMK или полученного в результате выполнения транзакции, с использованием IBM 3624 метода и возвращает полученное значение хосту.

3.2.9.5. Проверка PIN-offset. HSM выполняет проверку PIN-offset для значения PIN с использованием IBM 3624 метода и возвращает результат проверки хосту.

3.2.9.6. Смена PIN-offset. HSM выполняет проверку PIN-offset для текущего значения PIN с использованием IBM 3624 метода, в случае положительного результата проверки вычисляет значение PIN-offset для нового значения PIN и возвращает полученное значение хосту.

3.2.10. Функции управления ключами (DUKPT)

3.2.10.1.Формирование IPEK в соответствии с ANSI X9.24 из BDK и KSN с последующим экспортом его под терминальным транспортным ключом (TMK). HSM, используя полученные от хоста KSN и в зашифрованном виде BDK, формирует ключ IPEK, шифрует его под TMK и возвращает обратно хосту.

3.2.10.2. Трансляция PIN-блока, зашифрованного под ключом, полученным из BDK с использованием схемы DUKPT, под ZPK или ключ, полученный из другого BDK. HSM получает от хоста зашифрованный PIN-блок, BDK и KSN, расшифровывает его по схеме DUKPT в соответствии с ANSI X9.24 и перешифровывает с использованием новых значений KSN и BDK или с использованием ключа ZPK, результат возвращает хосту.

3.2.10.3.Расчет MAC (и сравнение, опционально) за данные с использованием схемы DUKPT. HSM извлекает ключ транзакции из предоставленного BDK и формирует ключ MAC в соответствии с ANSI X9.24, затем вычисляет MAC и возвращает MAC или результат сравнения.

3.2.11. Реализация алгоритма ECDSA в соответствии с эллиптическими кривыми P-192, P-224, P-256, P384 и P-521 и с использованием встроенного ГСЧ HSM.

3.2.12. Разные функции

3.2.12.1.Генерация случайных данных заданного размера длиной до 256 байт.

3.2.12.2.Вычисление значения хэш-функции SHA-256 за блок данных.

3.2.12.3.Проверка значения хэш-функции SHA-256 за блок данных.

3.2.12.4.Команда Echo.

3.2.12.5.Проверки параметров HSM и связи с HSM. Возвращает CV обнаруженных LMK.

3.2.12.6.Отправка пакета команд на HSM.

3.2.12.7.Работа с TLS-сертификатами *(Доступно только в консольном режиме):*

— сертификата HSM;

— клиентского сертификата.

3.2.12.8.Расшифрование SDK Encrypted Data (JWE-объект) согласно JWE (RFC 7516).

3.2.12.9.Расшифрование SDK Encrypted Data (JWA-объект) по алгоритму Diffie-Hellman на эллиптических кривых согласно JWA (RFC 7518) в режиме Direct Key Agreement.

3.3. Требования по российским криптографическим алгоритмам

3.3.1. Функция хэширования в соответствии с ГОСТ Р 34.11-2012 (id-tc26-gost3411-2012-256).

3.3.1.1. Вычисление значения хэш-функции блока данных. HSM вычисляет значение хэш-функции ГОСТ Р 34.11-2012 блока данных и возвращает в хост-систему.

3.3.2. ГОСТ Р 34.10-2012.

3.3.2.1. Генерация пары ключей ГОСТ Р 34.10-2012: закрытый ключ (длиной от 256 битов) и открытый ключ с использованием встроенного ГСЧ HSM.

3.3.2.2. Формирование и проверка ЭП в соответствии с ГОСТ Р 34.10-2012. Набор параметров для формирования/проверки ЭП: id-GostR3410-2001-CryptoPro-A-ParamSet.

3.3.3. ГОСТ 28147-89

3.3.3.1. Генерация симметричных ключей длины 256 битов с использованием встроенного ГСЧ HSM для алгоритма ГОСТ 28147-89.

3.3.3.2. Сформированный ключ выводится в зашифрованном виде с использованием LMK или с использованием ZMK. При этом LMK и ZMK должны быть созданы в формате key block-gost.

3.3.3.3. Вместе со сгенерированным ключом должна выводиться контрольная величина ключа: имитовставка в соответствии с ГОСТ 28147-89 с узлом замены id-tc26-gost-28147-param-Z с использованием сгенерированного ключа за 128 бинарных '0'.

Примечания:

1. Алгоритм формирования контрольной величины ключа может быть определен в ходе разработки соответствующей рекомендации в рамках ТК26.

2. Возможность использования алгоритма ГОСТ 28147-89 определяется «Извещением о порядке использования алгоритма блочного шифрования ГОСТ 28147-89», опубликованным ФСБ России 1 июля 2019 года.

3.3.4. «Магма» ГОСТ Р 34.12-2015.

3.3.4.1. Генерация симметричных ключей длины 256 битов с использованием встроенного ГСЧ HSM для алгоритма «Магма» ГОСТ Р 34.12-2015.

3.3.4.2. Сформированный ключ выводится в зашифрованном виде с использованием LMK или с использованием ZMK. При этом LMK и ZMK должны быть созданы в формате key block-gost.

3.3.4.3. Вместе со сгенерированным ключом должна выводиться контрольная величина ключа: имитовставка в соответствии с ГОСТ Р 34.13-2015 с использованием сгенерированного ключа за 128 бинарных '0'.

Примечания:

1. Алгоритм формирования контрольной величины ключа может быть определен в ходе разработки соответствующей рекомендации в рамках ТК26.

2. В случае невозможности использования алгоритма ГОСТ 28147-89 в соответствии с «Извещением о порядке использования алгоритма блочного шифрования ГОСТ 28147-89», опубликованным ФСБ России 1 июля 2019 года, функции, приведенные в п.3.4., должны использовать алгоритм «Магма» (ГОСТ Р 34.12-2015) вместо алгоритма ГОСТ 28147-89. В рамках ТК26 в этом случае должна быть выполнена соответствующая работа по корректировке рекомендаций, представленных в п.3.4.

3.3.5. Представление ключей в формате key block-gost

3.3.5.1. Формирование ключевого контейнера в формате key block-gost (*требуется разработка рекомендации в рамках ТК26 по использованию ГОСТ Р 34.12-2015 и ГОСТ Р34.13-2015 в формате ключевого блока).*

3.3.5.2. HSM формирует ключевой контейнер в формате key block-gost в соответствии с рекомендацией из пункта 3.3.5.1.

3.4. Требования к функциям с использованием российских криптографических алгоритмов

3.4.1. Реализация протокола SCP-F2 защищенного обмена сообщениями в процессе эмиссии платежных карт в соответствии с рекомендацией по стандартизации Р 1323565.1.013-2017.

3.4.1.1. Выработка с использованием HSM сессионных ключей для защиты сообщений SCP-F2: ключа для вычисления имитовставки запроса, ключа для вычисления имитовставки ответа, ключа для формирования/проверки криптограммы аутентификации, ключа для зашифрования/расшифрования полей сообщения, ключа для зашифрования/расшифрования критичных данных.

3.4.1.2. Генерация с использованием HSM криптограммы аутентификации хоста.

3.4.1.3. Проверка с использованием HSM криптограммы аутентификации карты.

3.4.1.4. Формирование с использованием HSM защищенных сообщений хоста: зашифрование критичных данных (опционально), зашифрование полей сообщения (опционально), вычисление имитовставки запроса.

3.4.1.5. Верификация с использованием HSM защищенных сообщений карты: вычисление имитовставки ответа карты и сравнение с принятой.

3.4.2. Реализация функций в соответствии с рекомендацией по стандартизации Р 1323565.1.016-2018 «Использование режимов алгоритма блочного шифрования, алгоритмов электронной подписи и функции хэширования в процедуре офлайновой аутентификации платежного приложения».

3.4.2.1. Генерация и проверка IDN (ICC Dynamic Number). HSM вычисляет IDN как функцию номера текущей транзакции ATC (Application Transaction Counter) с использованием мастер-ключа MK_{IDN} в соответствии с рекомендацией по стандартизации Р 1323565.1.016-2018 (п.4.1) и сравнивает со значением во входных данных. Результат сравнения возвращается хост-системе.

3.4.3. Реализация функций в соответствии с рекомендацией по стандартизации Р 1323565.1.015-2018 «Задание параметров алгоритмов электронной подписи и функции хэширования в профиле EMV-сертификатов открытых ключей платежных систем».

3.4.3.1. Генерация ключевой пары ГОСТ Р 34.10-2012 (закрытый и открытый ключ) эмитента и соответствующего самоподписанного сертификата в соответствии с рекомендацией по стандартизации Р 1323565.1.015-2018.

3.4.3.2. Проверка EMV-сертификата ключа эмитента ГОСТ Р 34.10-2012, подписанного корневым ключом УЦ, в соответствии с рекомендацией по стандартизации Р 1323565.1.015-2018.

3.4.3.3. Импорт (с проверкой) EMV-сертификата корневого ключа УЦ в соответствии с рекомендацией по стандартизации Р 1323565.1.015-2018.

3.4.4. Реализация функций в соответствии с рекомендацией по стандартизации Р 1323565.1.010-2017 «Использование функции диверсификации для формирования производных ключей платежного приложения».

3.4.4.1. Вывод мастер-ключей карты MK_{AC}, MK_{SMC}, MK_{SMI}, MK_{IDN}. Ключи MK_{AC}, MKSMC, MK_{SMI}, MK_{IDN} выводятся из соответствующих мастер-ключей эмитента IMK_{AC}, IMKSMC, IMK_{SMI}, IMK_{IDN} в соответствии с рекомендацией по стандартизации Р 1323565.1.010-2017 (п.5.1). HSM производит в соответствии с заданными алгоритмами генерацию ключей MK_{AC}, MK_{SMC}, MK_{SMI}, MK_{IDN} и вывод их в хост-систему в защищенном (зашифрованном) виде с использованием транспортного ключа (Key Encryption Key – KEK) для передачи в систему персонализации.

3.4.5. Реализация функций в соответствии с рекомендацией по стандартизации Р 1323565.1.008-2017 «Использование режимов алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением».

3.4.5.1. Генерация сообщений скрипт-процессинга (Secure Message) с обеспечением целостности и конфиденциальности в соответствии с рекомендацией по стандартизации 1323565.1.008-2017 (п.5.1 и п.5.2). HSM с использованием сессионных ключей карты SK_{SMC} и SK_{SMI} выполняет зашифрование конфиденциальных данных (опционально) и расчет имитовставки за сообщение и возвращает зашифрованные данные и имитовставку хосту. Сессионные ключи SK_{SMC} и SK_{SMI} выводятся из мастер-ключей карты MK_{SMC} и MK_{SMI} соответственно согласно рекомендации Р 1323565.1.010-2017 (п.5.2).

3.4.5.2. Расшифрование счетчиков карты. HSM производит расшифрование счетчиков, содержащихся в объекте Issuer Application Data, подготовленном приложением для эмитента при онлайновой аутентификации, в соответствии с рекомендацией по стандартизации Р 1323565.1.008-2017 (п.5.3).

3.4.6. Реализация функций в соответствии с рекомендацией по стандартизации Р 1323565.1.009-2017 «Использование режимов алгоритма блочного шифрования при формировании прикладных криптограмм в платежных системах».

3.4.6.1. Проверка криптограммы ARQC и/или генерация ARPC (Р 1323565.1.009-2017).

— Криптограмма приложения (ARQC, TC, AAC) вычисляется с использованием алгоритма MAC (ГОСТ 28147-89[2] в режиме выработки имитовставки с узлом замены id-tc26-gost-28147-param-Z) в соответствии с рекомендацией Р 1323565.1.009-2017, п.5.1. MAC формируется с использованием сессионного ключа SK_{AC}. Сессионный ключ SK_{AC} формируется из мастер-ключа карты MK_{AC} в соответствии с рекомендацией Р 1323565.1.010-2017. Ключ MK_{AC} выводится из мастер-ключа эмитента IMK_{AC} в соответствии с рекомендацией Р 1323565.1.010-2017.

— Криптограмма ARPC вычисляется в случае положительной проверки прикладной криптограммы Authorization Request Cryptogram (ARQC), сформированной платежным приложением карты. Криптограмма ARPC вычисляется с помощью алгоритма вычисления величины MAC с использованием сессионного ключа SK_{AC}, значения ARQC, 4-байтного элемента данных Card Status Update (CSU) и элемента Proprietary Authentication Data нулевой длины в соответствии с Р 1323565.1.009-2017, п.5.2.

3.4.7. Реализация функций в соответствии с рекомендацией по стандартизации Р 1323565.1.007-2017 «Использование режимов алгоритма блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN».

3.4.7.1. Генерация CVP /ППК. CVP/ППК (Card Verification Parameter/Проверочный Параметр Карты) – трехзначный код проверки подлинности карты. CVP/iCVP/CVP2 формируется в соответствии с рекомендацией Р 1323565.1.007-2017, п.5.1. HSM производит генерацию CVP/ППК и выводит сформированное значение в хост-систему.

---

[2] См. примечание к п.3.3.4.

3.4.7.2. Проверка криптовеличины CVP (CVC/CVV). HSM производит проверку CVP/iCVP/CVP2 (CVC1/CVC2/Chip CVC) и передает результат проверки хост-системе. В процессе проверки вычисляется значение CVP/iCVP/CVP2 в соответствии с рекомендацией Р 1323565.1.007-2017, п.5.1, которое сравнивается с полученным в ходе транзакции по магнитной полосе, транзакции чиповой карты в моде магнитной полосы или транзакции электронной коммерции значением CVP/iCVP/CVP2 карты. Если вычисленное и присутствующее на карте значения CVP/iCVP/CVP2 совпадают, то проверка выполнена успешно.

3.4.7.3. Генерация криптовеличины PVV в соответствии с рекомендацией Р 1323565.1.007-2017, п.5.2. HSM производит генерацию PVV для значения PIN и выводит сформированное значение в хост-систему.

3.4.7.4. Проверка криптовеличины PVV. HSM производит проверку PIN по зашифрованному PIN-блоку и PVV, результат проверки передает в хост-систему. В процессе проверки по расшифрованному PIN-блоку вычисляется значение PVV в соответствии с рекомендацией Р 1323565.1.007-2017, п.5.2, которое сравнивается с полученным в аутентификационном сообщении PVV карты. Если вычисленное и присутствующее на карте значения PVV совпадают, то PIN считается верным, если нет, то неверным.

3.4.8. Реализация алгоритма ECDSA в соответствии с NIST FIPS 186-4 и «ANSI X9.62: Public Key Cryptography for the Financial Services ECDSA».

3.4.8.1. Генерация закрытых ключей ECDSA для кривых P-192, P-224, P-256 P-384 и P-521 с использованием встроенного ГСЧ HSM.

От ФСБ России

А.М. Шойтов

21/01/20

От Банка России

Директор Департамента
информационной безопасности

В.А. Уваров

22.01.2020г.