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 ПЛАТЕЖНЫМ КАРТАМ (КРИПТОМОДУЛЬ, ПРИЛОЖЕНИЕ)

№ ФТ-56-3/34
28.02.2020

СОДЕРЖАНИЕ

ТЕРМИНЫ, определения и сокращения

В настоящих требованиях применяются следующие термины с соответствующими определениями.

Термин/Сокращение	Определение
ЗОС	Защищенный обмен сообщениями
СКЗИ	Средство криптографической защиты информации
HSM	Защищенное от несанкционированного внешнего воздействия аппаратное криптографическое устройство (Hardware Security Module), используемое для хранения ключа верхнего уровня (LMK – Local Master Key) и выполнения криптографических операций

1. Общие положения

1.1. Введение

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 программному обеспечению, реализующим СКЗИ в платежных картах (криптомодуль, приложение).

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].

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

---

[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 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).

1.2. Классификация карт по реализуемой технологии

1.2.1. Карта с поддержкой технологии Java – интероперабельная карта, соответствующая стандарту Global Platform.

1.2.2. Карта с поддержкой native технологии – карта, реализующая проприетарную технологию производителя.

1.2.3. Карта с поддержкой технологии MultOS – карта, реализующая технологию MultOS.

1.3. Классификация карт по интерфейсу взаимодействия с терминалами

1.3.1. Карта с поддержкой контактного интерфейса.

1.3.2. Карта с поддержкой бесконтактного интерфейса.

1.3.1. Карта с поддержкой дуального интерфейса.

1.4. Классификация карт по форм-фактору

1.4.1. ISO1 (классический формат).

1.4.2. Другие форматы (Sticker, Mini-tag, Micro-tag, Flexi-tag), поддерживающие платежный функционал.

2. Требования к чип-модулю

Требования к картам с поддержкой контактного интерфейса описаны в ISO 7816 / ГОСТ Р ИСО/МЭК 7816.

- Часть 1 описывает физические параметры карт (в том числе требования к стойкости карт к излучениям и механическим нагрузкам).
- Часть 2 описывает расположение и назначение контактов.
- Часть 3 описывает электрические параметры интерфейса и некоторые принципы установления связи для карт с асинхронным интерфейсом.
- Часть 4 описывает протокол обмена и механизм действия команд. По факту распространяется также на другие смарт-карты, совместимые с ISO 7816.
- Части 5–15 являются фактически пояснениями и дополнениями к ISO 7816-3 и ISO 7816-4.
    - Часть 5: Registration of application providers. Специфицирует процедуру регистрации в регулирующих органах идентификатора приложения (RID).

- Часть 6: Interindustry data elements for interchange. Специфицирует номера тэгов и формат записи для популярных типов данных: имен, дат, фотографий, биометрики и т. п.
- Часть 7: Interindustry commands for Structured Card Query Language (SCQL).
- Часть 8: Commands for security operations. Специфицирует формат команд для доступа к криптографическим процедурам и менеджменту криптоключей.
- Часть 9: Commands for card management. Специфицирует формат команд для доступа к файловой системе карты.
- Часть 10: Electronic signals and answer to reset for synchronous cards. Специфицирует назначение контактов и принципы установления связи для карт с синхронным интерфейсом.
- Часть 11: Personal verification through biometric methods.
- Часть 12: Cards with contacts – USB electrical interface and operating procedures. Специфицирует назначение контактов и принципы установления связи для карт с интерфейсом USB. В значительной степени пересекается со спецификацией USB CCID Device Class.
- Часть 13: Commands for application management in multi-application environment.
- Часть 15: Cryptographic information application.

Требования к картам с поддержкой бесконтактного интерфейса описаны в **ISO/IEC 14443 /** ГОСТ Р ИСО/МЭК 14443.

- Часть 1 определяет физические нормативы карт и условия нормальной работы;
- Часть 2 определяет радиочастотные параметры и методы модуляции;
- Часть 3 определяет протокол инициализации обмена (в основном это процедура антиколлизии – разделения нескольких карт в поле считывателя);
- Часть 4 определяет протокол обмена данными.

3. Функциональные требования

3.1. Подготовка карт у производителя

Загрузка ключей домена безопасности Issuer Security Domain (ISD) для дальнейшего безопасного управления картой

- Global Platform Card specification v.2.2.1 (п.7 и приложение E (SCP-02))

- Р 1323565.1.013-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт»[2].

3.2. Установка платежного приложения

3.2.1 Аутентификация с использованием ранее установленных на карту ключей домена безопасности Issuer Security Domain (ISD) или Supplementary Security Domain (SSD) с выработкой сессионных ключей для обеспечения защищенного обмена сообщениями (ЗОС)

- Global Platform Card specification v.2.2.1 (п.10 и приложение E (SCP-02))
- Р 1323565.1.013-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт»2.

3.2.2 Поддержка защищенного обмена сообщениями (ЗОС). Обработка защищенных сообщений от терминала и формирование ответных сообщений для обеспечения confidentiality and integrity

- Global Platform Card specification v.2.2.1 (п.10 и приложение E (SCP-02))
- Р 1323565.1.013-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт»2.

3.2.3 Загрузка приложения на карту через канал ЗОС[3]

- Global Platform Card specification v.2.2.1 (п. 9.3)

3.2.4 Установка приложения через канал ЗОС

- Global Platform Card specification v.2.2.1 (п. 9.3)

---

[2] в данный момент не поддерживается ни одним из производителей. Сроки разработки продуктов с поддержкой данного функционала должны прорабатываться и определяться отдельно.

[3] Данная функциональность может отсутствовать в ОС или не использоваться в том случае, если приложение уже встроено в ОС чип-модуля. Это возможно в случае нативной реализации (см. 1.3.2) или в случае предзагруженного байт-кода приложений для технологий JavaCard и MultOS (см. 1.3.1, 1.3.3).

3.3. Преперсонализация платежного приложения

3.3.1 Аутентификация с использованием ранее установленных на карту ключей домена безопасности Issuer Security Domain (ISD) или Supplementary Security Domain (SSD) с выработкой сессионных ключей для обеспечения защищенного обмена сообщениями (ЗОС)

- Global Platform Card specification v.2.2.1 (п.10 и приложение E (SCP-02))
- Р 1323565.1.013-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт».

3.3.2 Поддержка защищенного обмена сообщениями (ЗОС). Обработка защищенных сообщений от терминала и формирование ответных сообщений для обеспечения confidentiality and integrity

- Global Platform Card specification v.2.2.1 (п.10 и приложение E (SCP-02))
- Р 1323565.1.013-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт».

3.3.3 Загрузка ключей персонализации приложения (K_{ENC}, K_{MAC}, K_{DEC}) через канал ЗОС

- EMV CPS 1.1, п. 4.2
- Спецификации платежных систем.

3.4. Персонализация платежного приложения

3.4.1 Аутентификация с использованием ранее загруженных в приложение ключей персонализации (K_{ENC}, K_{MAC}, K_{DEC}) с выработкой сессионных ключей для обеспечения защищенного обмена сообщениями (ЗОС)

- Global Platform Card specification v.2.2.1 (п.10 и приложение E (SCP-02))
- Р 1323565.1.013-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт»
- EMV CPS 1.1, п.5.

3.4.2 Поддержка защищенного обмена сообщениями (ЗОС). Обработка защищенных сообщений от терминала и формирование ответных сообщений для обеспечения confidentiality and integrity

- Global Platform Card specification v.2.2.1 (п.10 и приложение E (SCP-02))
- Р 1323565.1.013-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт»
- EMV CPS 1.1, п.5.

3.4.3 Персонализация платежного приложения

- EMV CPS 1.1, п. 6
- Спецификации платежных систем.

3.5. Эксплуатация платежного приложения

3.5.1. Обработка платежной транзакции

- Группа стандартов EMV Integrated Circuit Card Specifications for Payment Systems, version 4.3
- Спецификации платежных систем.

От ФСБ России

А.М. Шойтов

21/01/20

От Банка России

Директор Департамента
информационной безопасности

В.А. Уваров

22.01.2020г

Васильев С.Н.