КРИПТОПРО

Ключевое слово
в защите информации

Особенности криптографической защиты платежных систем в условиях санкций

Павел Луцик, Директор по развитию бизнеса, КриптоПро

Уход Thales из России

HSM Thales Payshield 9000/10k – самые популярные модели

80%

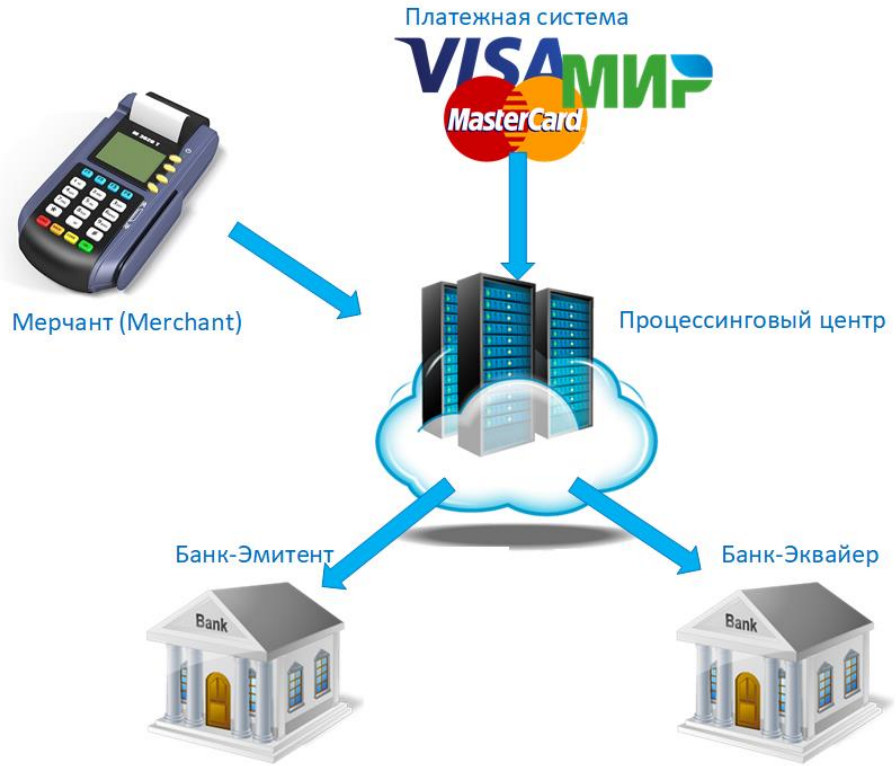
Important Dates for payShield 9000

30th June 2020 – last time buy on hardware

31st December 2022 – end-of-life for support

Кто использует HSM?

- Банки - эмитенты платёжных карт
- Банки - эквайеры платёжных терминалов и банкоматов
- Процессинговые центры операторов платёжных систем



Лидеры разработки платежного ПО в РФ

РЕГУЛИРОВАНИЕ

PCI Security Standards Council

Банк России

НСПК
НАЦИОНАЛЬНАЯ СИСТЕМА ПЛАТЕЖНЫХ КАРТ

Оператор значимой платежной системы с 01.01.2024 должен обеспечить использование:

- В аппаратных модулях безопасности информационной инфраструктуры платежной системы СКЗИ, реализующих иностранные криптоалгоритмы, криптоалгоритмы, определенные национальными стандартами РФ, имеющих подтверждение соответствия требованиям ФСБ

- В аппаратных модулях безопасности информационной инфраструктуры платежной системы СКЗИ, реализующих криптографические алгоритмы, не определенные национальными стандартами РФ, имеющих подтверждение соответствия требованиям ФСБ

ФСБ России + Банк России

Банк России

№ФТ-56-3/32 от 28.02.2020

Опубликованы на официальных сайтах ФСБ России и Банка России

Требования международных платежных систем

Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) **Modular Security** Requirements Version 3.0 June 2016.

Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) **Modular Derived Test** Requirements Version 3.0 June 2016.

Основные результаты работ по обеспечению выполнения требований PCI HSM

Проведено изучение открытой документации компании Thales.

Подготовлены технические решения по выполнению требований PCI HSM.

Технические решения направлены в сертификационную лабораторию PCI HSM.

НСПК + VISA (MASTER CARD)

НСПК +UNION PAY ?

THALES

Компания Thales **прекратила поставки и техническую поддержку** HSM модулей для кредитных и иных организаций на территории РФ

Риски ухода Thales из России

Взаимодействие с платежной системой UNION PAY

До решения вопроса о необходимости сертификации по PCI HSM для взаимодействия с UNION PAY **должны быть разделены потоки транзакций**.

Следует договориться о **возможности корректировки требований** для эксплуатации СКЗИ на территории РФ. Выполнить только **требования ФСБ**.

Привлечь лаборатории КНР для сертификации российских СКЗИ по требованиям PCI HSM. Не очевидна возможность получения сертификата PCI

НСПК является **национально значимой платежной системой** и при ее функционировании должны выполняться положения 161-ФЗ "О НПС".

Выполнение требований ЦБ и ФСБ должны являться достаточным условием для возможности эксплуатации HSM в национально значимых ПС, в том числе НСПК.

В текущих условиях **обязательное требование** по применению нормативных документов **PCI должно быть исключено**.

КриптоПро HSM 2.0 с программным платежным модулем (платежный HSM)

Поддерживаемые алгоритмы

Шифрование	2DES, 3DES, AES
Электронная подпись	RSA, ECDSA
Хэш-функции	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, MD5, ISO 10118-2
MAC	ISO 9797-1 MAC algorithm 1, ISO 9797-1 MAC algorithm 3, ANSI X9.19, CBC-MAC, CMAC

Форматы ключей

- ANSI X9 TR-31 Key Block
- Проприетарный Key Block
- ANSI X9.17
- Variant

Производительность

- 10 000 tps на AES
- 20 000 tps на 3DES

Поддерживаемые технологии

- Visa VIS, Visa VCP, Mastercard M/Chip, Mastercard MCBP, American Express AEIPS, JCB, Union Pay, МИР
- EMV CPS, EMV 3.1.1, EMV 4.1, EMV 4.3
- Visa CVV, iCVV, CAVV; Mastercard CVC, Chip CVC, AAV
- IBM 3624 (IBM Offset)
- ABA PVV
- Mastercard CAP, Visa DPA
- PIN Block (ISO 9564-1 & ANSI X9.8): Format 0, Format 1, Format 3, Format 4
- Global Platform Secure Channel Protocol 2 (SCP02), EMV Common Personalization Specification (EMV CPS)
- DUKPT (X9.24)

КРИПТОПРО

Ключевое слово
в защите информации

СПАСИБО ЗА ВНИМАНИЕ!

127018, г. Москва, ул. Сущевский Вал, д.18
Тел./факс: +7 (495) 995-48-20

https://cryptopro.ru

Простов Владимир Михайлович
prostov@cryptopro.ru

Основные результаты работ по согласованию технических решений с сертификационной лабораторией

Согласованы следующие технические решения:

1. Общая конструкция HSM модуля.
2. Физическая защита HSM модуля от возможных проникновений.
3. Механизмы защиты от утечки информации по побочным каналам.
4. Микропрограммное и программное обеспечение HSM модуля.
5. Процедура загрузки программного обеспечения.
6. Механизмы защиты от изменений условий окружающей среды и целенаправленных изменений условий эксплуатации.
7. Датчик случайных чисел.

Контроль целостности программно-аппаратных средств должен применяться с использованием российских криптографических алгоритмов

Удаленное обновление программного обеспечения должно осуществляться с использованием российских криптографических алгоритмов