Платёжный HSM

Защита информации в платёжной системе и безопасное хранение криптографических ключей

КРИПТОПРО

Платёжный HSM — это средство криптографической защиты информации, предназначенное для обеспечения защиты чувствительной информации, обрабатываемой в платёжной системе, и безопасного хранения криптографических ключей, в соответствии с российскими и зарубежными стандартами.

Программно-аппаратный комплекс **КриптоПро HSM 2.0 R3 с платёжным модулем** разработан в соответствии с Положением Банка России от 4 июня 2020 г. N 719-П и PCI PTS HSM Modular Security Requirements, имеет сертификаты соответствия требованиям ФСБ России, является альтернативой для иностранных модулей **Thales payShield 9000** и **Thales payShield 10K** и может применяться вкачестве платёжного HSM для криптографической защиты информации, обрабатываемой в платёжных системах.

КриптоПро HSM 2.0 R3 позволяет полноценно заменить (как по функционалу, так и по производительности) соответствующие HSM-модули иностранного производства в действующих схемах подключения в рамках функционирования информационных систем участников финансового рынка:

- Банков-эмитентов платёжных карт
- Банков, осуществляющих эквайринг платёжных карт
- Процессинговых центров операторов платёжных систем

Платёжный HSM реализует интерфейс поддержки операций системы платёжных карт, позволяя решать следующие задачи:

- **Инициализация и эмиссия платёжных карт** с магнитной полосой, бесконтактных и смарт-карт, включая генерацию PIN/CVC/CVP и печать PIN-конвертов, смену и проверку PIN и прочее
- **Управление ключами** (и обеспечение безопасности ключей) на всех этапах жизненного цикла (включая генерацию, печать ключевых компонент, формирование ключей из компонент, диверсификацию ключей, импорт/экспорт и трансляцию)
- **Обработка платёжных транзакций**, банковских транзакций от платёжных устройств

ПОДДЕРЖИВАЕМЫЕ ТЕХНОЛОГИИ

- МИР
- Visa VIS, Visa VCP, Mastercard M/Chip, Mastercard MCBP, American Express AEIPS, JCB, Union Pay
- 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
- Global Platform Secure Channel Protocol 2 (SCP02), Secure Channel Protocol 3 (SCP03); EMV Common Personalization Specification (EMV CPS)
- DUKPT (X9.24)

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
Согласование ключей	ECDH

ФОРМАТЫ PIN-БЛОКОВ

Формат PIN-блока	ISO Format	Алгоритм
ISO 9564-1 & ANSI X9.8 Format 0	0	2DES, 3DES
ISO 9564-1 Format 1	1	2DES, 3DES
Standard EMV 1996	2	2DES, 3DES
Mastercard Pay Now & Pay Later	—	2DES, 3DES
Visa/Amex new PIN only	—	2DES, 3DES
Visa/Amex new & old PIN	—	2DES, 3DES
ISO 9564-1 & ANSI X9.8 Format 3	3	2DES, 3DES
ISO 9564-1 Format 4	4	AES

ФОРМАТЫ КЛЮЧЕЙ

- Key Block (в том числе ANSI X9 TR-31)
- ANSI X9.17
- Variant

ПРОИЗВОДИТЕЛЬНОСТЬ

На примере операции трансляции PIN-блоков:

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

КОНТАКТЫ

@CryptoProAssistantBot info@cryptopro.ru +7 (495) 995-48-20 https://cryptopro.ru