Создание национальной системы платежных карт с использованием отечественных HSM

Дорожная карта

Цель

Создание национальной системы платежных карт (НСПК) с использованием отечественных HSM, обеспечивающих технологическую независимость и устойчивое функционирование НСПК как в автономном режиме, так и во взаимодействии с МПС

Основные задачи дорожной карты

Выявление угроз, связанных с применением импортных HSM

Определение принципов построения НСПК с использованием отечественных HSM, исключающих выявленные угрозы

Определение этапов создания НСПК с использованием отечественных HSM

Угрозы ИБ, связанные с применением импортных HSM

Угрозы	Последствия
Управление ключевой информацией по зарубежным технологиям и стандартам, в том числе , из-за пределов РФ	Возможность несанкционированного управления ключами, отзыв сертификатов, работа на договорных ключах
Риск введения санкций против российской платежной системы, например, прекращение поставок оборудования	Нарушение функционирования российской платежной системы даже внутри РФ
Наличие скрытых функциональных возможностей (программные и/или аппаратные закладки) в импортном оборудовании	Несанкционированный доступ к информационным активам НПС (ПД, PIN-кодам, информации о состоянии денежных счетов и т.д.), отказ в предоставлении услуг
Технологическая зависимость от импортного оборудования	Развитие НПС и применяемого оборудования по планам, навязанным иностранными технологиями и темпами развития
Скрытые функциональные возможности и известные уязвимости зарубежной криптографии	Несанкционированный доступ к информационным активам НПС, нарушение работоспособности системы
Замкнутость системы, невозможность парирования угроз, актуальных для НПС	Несанкционированный доступ к информационным активам НПС, нарушение работоспособности системы
Несоответствие требованиям надзорных и регулирующих органов, действующему законодательству РФ в области ИБ	Возникновение юридических препятствий для применения импортного оборудования, невозможность проведения сертификации на соответствие требованиям и нормам ИБ РФ

Принципы построения НСПК с использованием отечественных HSM

- Создание отечественного оборудования с учетом угроз, актуальных для НПС
- Управление ключевой информацией с помощью центров управления ключами (и сертификатами), расположенных на территории РФ
- Реализация криптографических алгоритмов и механизмов управления ключами, используемых в импортном оборудовании, для поддержки выполнения платежных операций в МПС
- Использование отечественной криптографии для защиты платежных операций в рамках НПС
- Сертификация всех разрабатываемых устройств в отечественной (для применения в НПС) и зарубежной (для применения в МПС) системах сертификации
- Поэтапная замена импортного оборудования на отечественные аналоги в соответствии с этапами развития НСПК

Этапы создания НСПК с использованием отечественного оборудования

1 этап

- Реализация отечественного HSM, повторяющего функционал импортных аналогов с использованием отечественных криптоалгоритмов только в автономных режимах

2 этап

- Реализация в отечественном HSM набора дополнительных команд с использованием отечественных криптоалгоритмов.
- Реализация с использованием отечественного HSM трёхуровневой PKI инфраструктуры с использованием импортных и отечественных криптографических алгоритмов. Реализация корневого УЦ НПС (аналога УЦ МПС Visa или MasterCard)

3 этап

- Разработка отечественной чиповой карты
- Разработка спецификаций и приложений с поддержкой отечественных криптоалгоритмов для всех устройств, участвующих в поддержке платежных транзакций.
- Разработка программы подготовки к эмиссии карт НПС и поэтапного перевода всех устройств на работу с двумя криптографическими алгоритмами

1 этап

ЦЕЛИ

Создание оборудования, способного заменить импортный аналог и обеспечивающего встречную работу с ним

Плавный переход на отечественный HSM без потери зашифрованных хранимых информационных активов

2 этап

ЦЕЛИ

Замкнуть управление ключами, участвующими в поддержке платежных транзакций в НПС, а также при эмиссии карт в российском сегменте, на территории РФ

Подготовка отечественного HSM к взаимодействию со всеми элементами НПС с использованием отечественных КА

3 этап

ЦЕЛИ

Создание чиповой платежной карты, обеспечивающей применение как в НПС, так и в МПС

Поддержка всеми устройствами платежных транзакций с использованием отечественных КА

3 этап Промежуточный итог. Что дальше?

Реализация во всех элементах платёжной системы двух систем криптографии с выбором соответствующей в зависимости от платёжного приложения

Национальное платёжное приложение – система команд с отечественной криптографией, международное платёжное приложение (VSDC или MChip) – система команд с импортной криптографией

Создание гибкой платежной системы, устойчиво функционирующей как в виде российского сегмента международной платежной системы, так и в виде автономной (изолированной) национальной платежной системы на территории РФ

Сертификация элементов системы

Разработка организационно - распорядительной документации

Разработка программы поэтапного перевода всех устройств на работу с двумя КА с учетом переходного периода

Схема взаимодействия НСПК и МПС через HSM

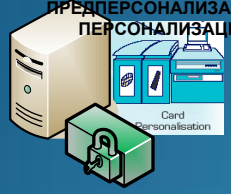
НСПК

УЦ НСПК (аналог УЦ МПС)

Система мониторинга, анализа и контроля ИБ НСПК в части HSM

Сеть НСПК

СРЕДСТВА ПРЕДПЕРСОНАЛИЗАЦИИ и ПЕРСОНАЛИЗАЦИИ



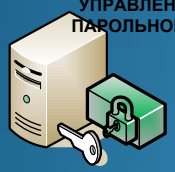
Банк Эмитент

Банк Эмитент

Банк Эмитент

Банковская сеть

СРЕДСТВА УПРАВЛЕНИЯ КЛЮЧЕВОЙ и ПАРОЛЬНОЙ ИНФОРМАЦИЕЙ



Банк Эквайер

Банк эквайер

Банк Эквайер

Сеть доступа

Импортный HSM

VSDC Или MChip

Международное Платёжное Приложение

НПП

Национальное Платёжное Приложение

Отечественный HSM

VSDC Или MChip

НПП

Криптография

- Схема замены импортных криптографических алгоритмов отечественными

Криптографическая операция	Импортный алгоритм	Отечественный алгоритм
Симметричное шифрование	DES, TripleDES, AES	ГОСТ 28147-89
Ассиметричное шифрование	RSA	Аналогов нет Возможно использование VKO GOST R 34.10-2012 для обмена ключами для симметричного шифрования
Имитозащита (MAC)	X9.19	ГОСТ 28147-89
Хэширование	SHA-1	ГОСТ Р 34.11-2012
Электронная цифровая подпись	RSA	ГОСТ Р 34.10-2012
Обмен ключами	Диффи-Хеллман	VKO GOST R 34.10-2012

Примеры команд HSM

Импортный HSM		Отечественный HSM	
Код	Описание	Код	Описание
A0 (A1)	Генерация ключа (DES/TripleDES)	T0 (T1)	Генерация ключа (ГОСТ 28147-89)
A2 (A3)	Генерация и печать компонент ключа в PIN-конверты (DES/TripleDES)	T2 (T3)	Генерация и печать компонент ключа в PIN-конверты (ГОСТ 28147-89)
A4 (A5)	Генерация ключа из зашифрованных компонент (DES/TripleDES)	T4 (T5)	Генерация ключа из зашифрованных компонент (ГОСТ 28147-89)
MA (MB)	Вычисление MAC-кода сообщения (X9.19)	TC (TD)	Вычисление имитовставки на сообщение (ГОСТ 28147-89)
JQ (JR)	Проверка сертификата открытого ключа эмитента (RSA, Mchip)	TQ (TR)	Проверка сертификата открытого ключа УЦ (ГОСТ Р 34.10-2012)

Сертификация

Все разрабатываемое оборудование и ПО должно пройти сертификацию в двух системах сертификации:

- **для применения в НПС – в соответствии с требованиями ЦБ и ФСБ в части СКЗИ**
- **для применения в МПС – в соответствии с требованиями PCI DSS, PCI PA-DSS(в части платёжных приложений), требованиям FIPS 140-2 Level 3, PCI HSM v1.0 в части HSM**

Стратегия развития НСПК

1 этап	• Разработка концепции обеспечения защиты информации при проведении транзакций в НСПК
2 этап	• Разработка регламентов функционирования НСПК в обеспечение защищенных транзакций.
3 этап	• Разработка программы подготовки к эмиссии карт НПС и поэтапного перевода всех устройств на работу с двумя криптографическими алгоритмами

Выводы

Использование отечественных технологий, включая криптографические алгоритмы, в разрабатываемых платежных приложениях и оборудовании, позволит создать надежную и безопасную национальную систему платежных карт

Спасибо за внимание!