конференция
РусКрипто

Ежегодная международная научно-практическая конференция
«РусКрипто’2023»

Аппаратные модули безопасности для систем платёжных карт. Тенденции развития

Е.В.Мареева, А.В. Лаптев
ООО «Системы практической безопасности»

Участники Круглого Стола

Горелов Дмитрий Львович «Актив»

Качалин Алексей Игоревич Сбербанк

Мареева Елена Владимировна «СПБ»

Простов Владимир Михайлович «КриптоПро»

Шибина Ольга Михайловна «Штрих-М»

Ведущий круглого стола - Елистратов Андрей Алексеевич

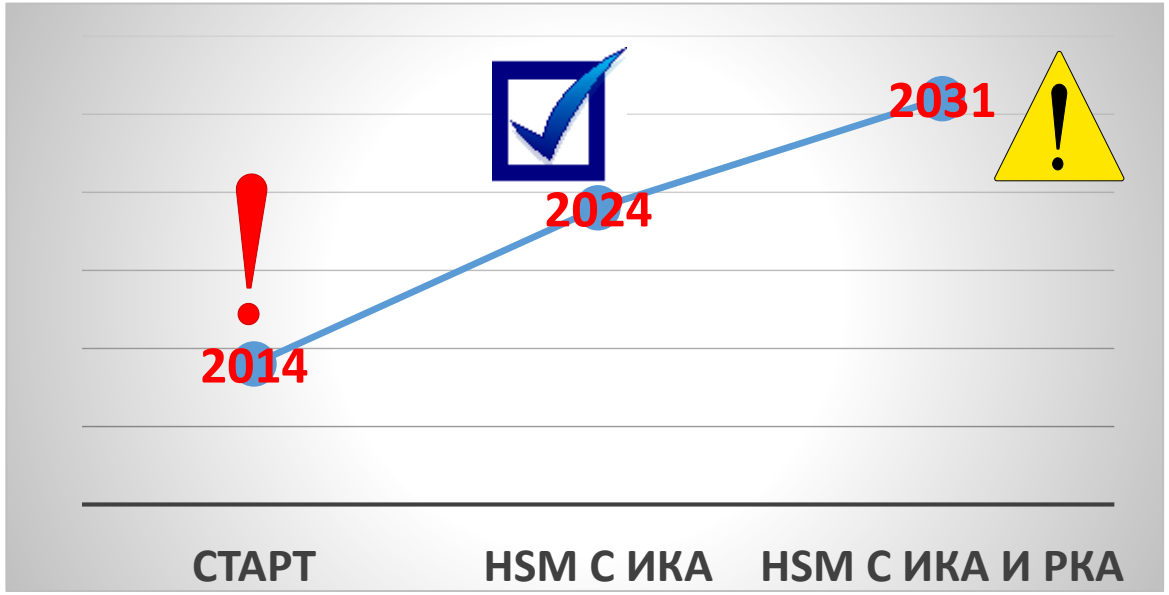
Две точки на прямой?

Положение БР 719-П предусматривает необходимость постепенного внедрения российских аналогов аппаратных модулей безопасности (HSM) в информационную инфраструктуру платежной системы:

- с 01.01.2024 года, реализующих иностранные криптографические,

- с 01.01.2031 года, реализующих иностранные криптографические алгоритмы и криптографические алгоритмы, определенные национальными стандартами Российской Федерации (российские).

Данные аппаратные модули безопасности должны иметь подтверждение соответствия требованиям, установленным к СКЗИ класса КВ.



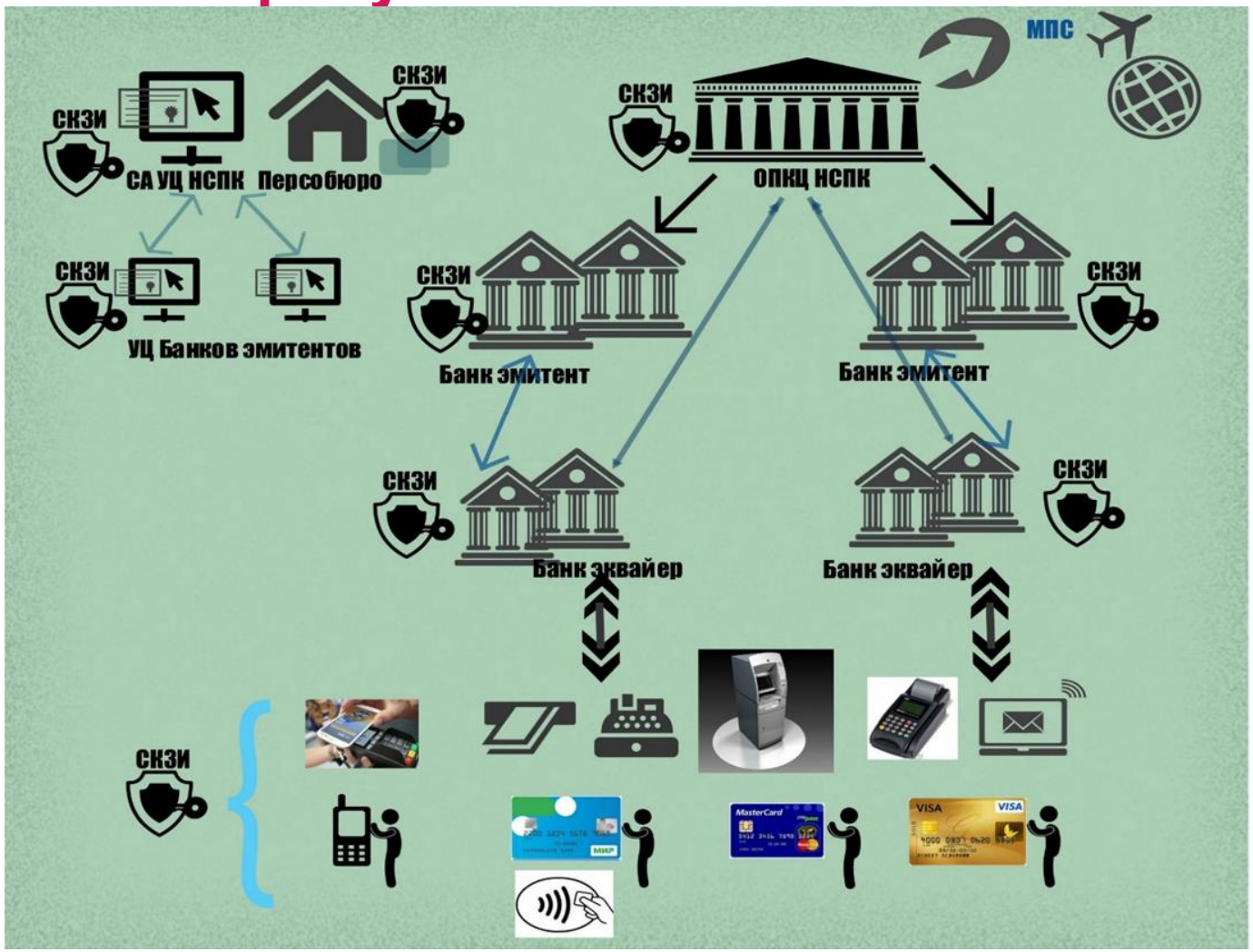
Внедрение РКА потребует …..

- ✓ **Утверждение МР Росстандарта**
- ✓ **Внедрения РКА (СКЗИ) в платёжные приложения SC МИР, мобильных абонентских терминалов, …**
- ✓ **Внедрения РКА (СКЗИ) в POS, ATM**
- ✓ **Внедрения РКА в HSM PS не только в контуре хранения и управления, но и в составе основных криптомеханизмов**

2031 год ?

Или это только импортозамещение POS, ATM и SC , но с ИКА

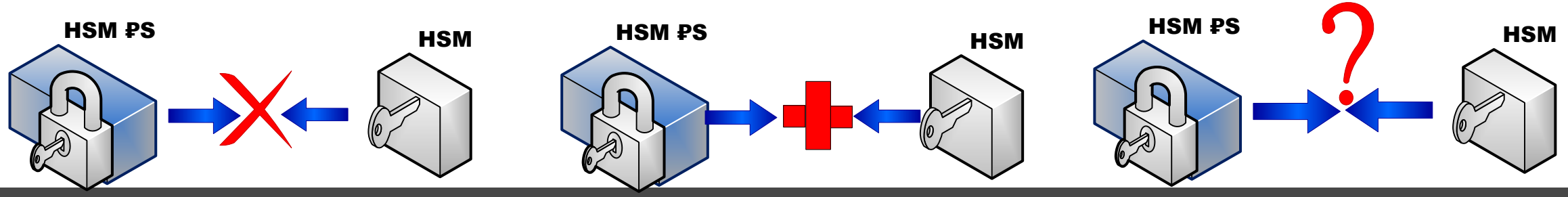
Нужна новая Дорожная карта



Универсальный или платёжный HSM. Вместе или врозь?

Платёжный HSM	HSM общего назначения (HSM CA, ЕБС, СБП….)
Реализация платёжных механизмов безопасности (вычисление PVV, CVV, ARQS/ARPC, SM, EMV сертификатов, TR-31, DUKPT..), которые используют различные криптопримитивы соответствующих КА	Реализация непосредственно в HSM только криптопримитивов соответствующих КА (TDES, AES, RSA, MAC…)
Промежуточные результаты криптопреобразований модуль не покидают, что обеспечивает максимальную степень защиты ДДК	Промежуточные результаты криптопреобразований модуль покидают, обрабатываются в ПАК системы платёжных карт. Вся логика, реализующая механизмы безопасности ДДК должна быть выполнена в платёжном приложении и должна быть обеспечена безопасность данного приложения от компьютерных атак на него
API к модулю – это запись в сокет UDP или TCP датаграмм, называемых командами и чтение с анализом ответов. API не стандартизировано	API к модулю – это стандартные крипто-API, такие как PKCS#11, Java, JCPROV, CSP и KSP.

Применение платёжных HSM и реализация защиты ДДК на уровне механизмов безопасности является предпочтительной с позиции уровня обеспечения защиты, а применение HSM общего назначения является хорошим решением для новых, ещё не специфицированных механизмов безопасности, и такие HSM могут быть за счёт стандартных крипто-API достаточно быстро интегрированы в платёжную индустрию



Поиск золотого сечения – что аппаратно, что программно

С 2020 года начался прием заявок на сертификацию приложений по требованиям PCI Software Security Framework (PCI SSF). В июне 2021 года завершилась сертификация по стандарту PA-DSS. PCI SSF состоит из двух связанных между собой стандартов — Secure Software Standard (SSS) и Secure Software Lifecycle (Secure SLC) Standard.

Требования в PCI SSS в части криптографической защиты:

- КА и методы, признанные отраслевыми стандартами (ОТС)
- Процедуры управления ключами, признанные ОТС
- ГСЧ, признанные ОТС и случайные числа с энтропией, удовлетворяющей минимальным требованиям ОТС

Подлежат оценке SSS	Не подлежат оценке SSS
ПО, которое обрабатывает, передает или хранит данные платежных карт или влияет на безопасность платежных операций, при соблюдении хотя бы одного из следующих условий: 1. Платежное ПО разработано для его продажи и коммерческого использования множеством других организаций. 2. Платежное ПО предназначено для использования на PTS POI устройствах, одобренных Советом PCI SSC.	• Платежное ПО собственной разработки, которое используется только компанией-разработчиком. • Платежное ПО, которое работает на любом мобильном устройстве, не предназначенном для приема платежей или обработки транзакций. • Операционные системы, на которые может быть установлено платежное ПО, при условии, что ОС не является интегрированным компонентом самого платежного ПО. • СУБД, которые платежное ПО может использовать для хранения данных о транзакциях, при условии, что СУБД не является интегрированным компонентом самого платежного ПО. • Другие виды коммерческого ПО, разработанного для целей, не связанных с обработкой транзакций или обеспечением безопасности, при условии, что они не являются интегрированными компонентами платежного ПО.

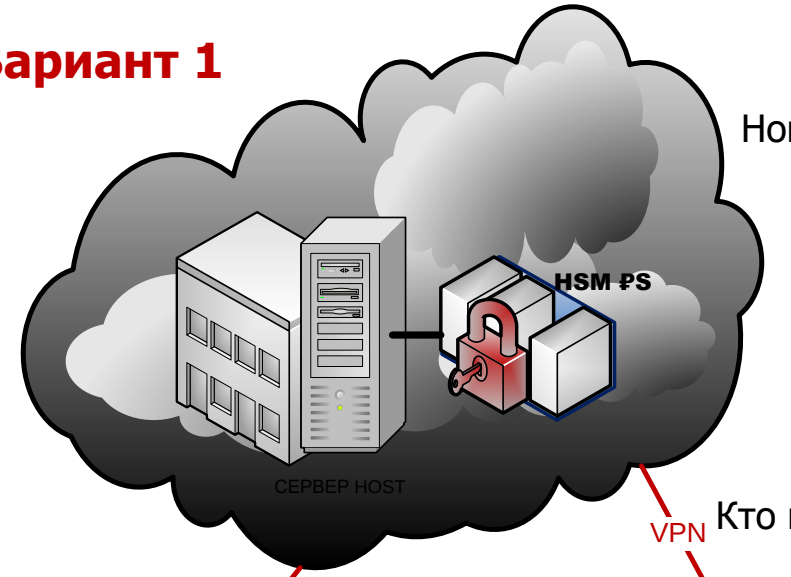
- ✓ **Логика реализации криптомеханизмов**
- ✓ **Реализация КА**

HSM

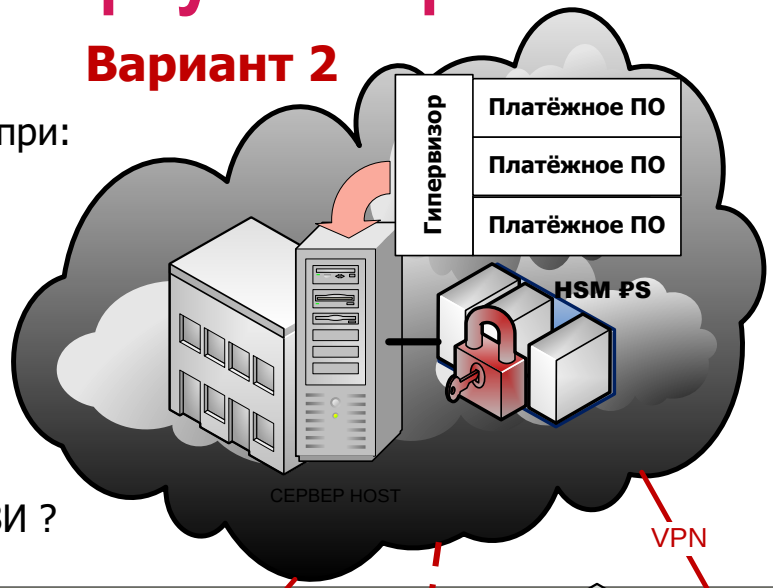
- ✓ **ГСЧ и генерация ключей**
- ✓ **Надёжное хранение мастер ключей**
- ✓ **Криптозащита ключей держателей карт**

Облачный HSM. Что имеет смысл виртуализировать?

Вариант 1

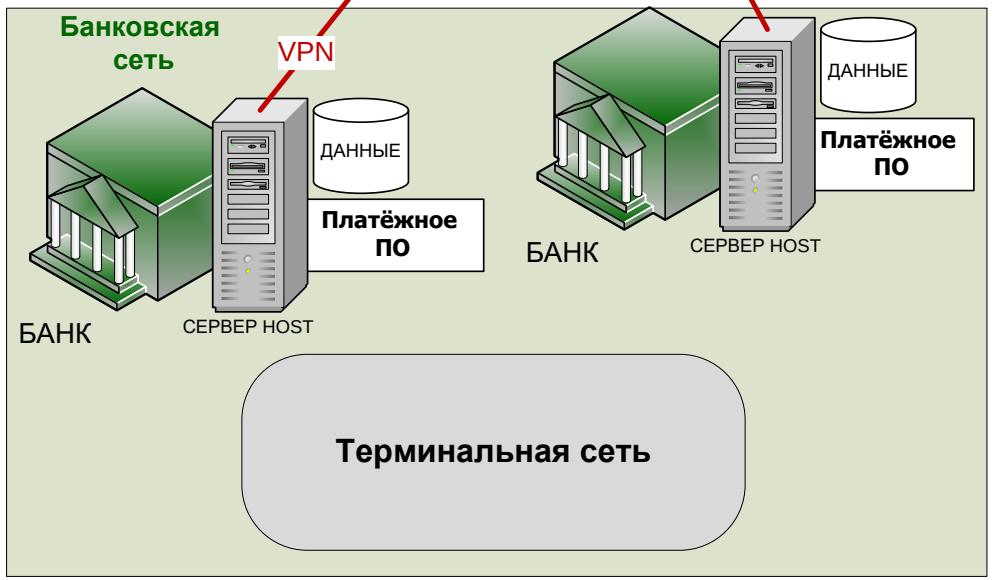


Вариант 2



Новые требования по безопасности при:
- Изоляции vHSM в составе HSM
- Передаче ДДК в облако
- Удалённом управлении параметрами
- Удалённом управлении
- ключами

Кто может эксплуатировать такое СКЗИ ?



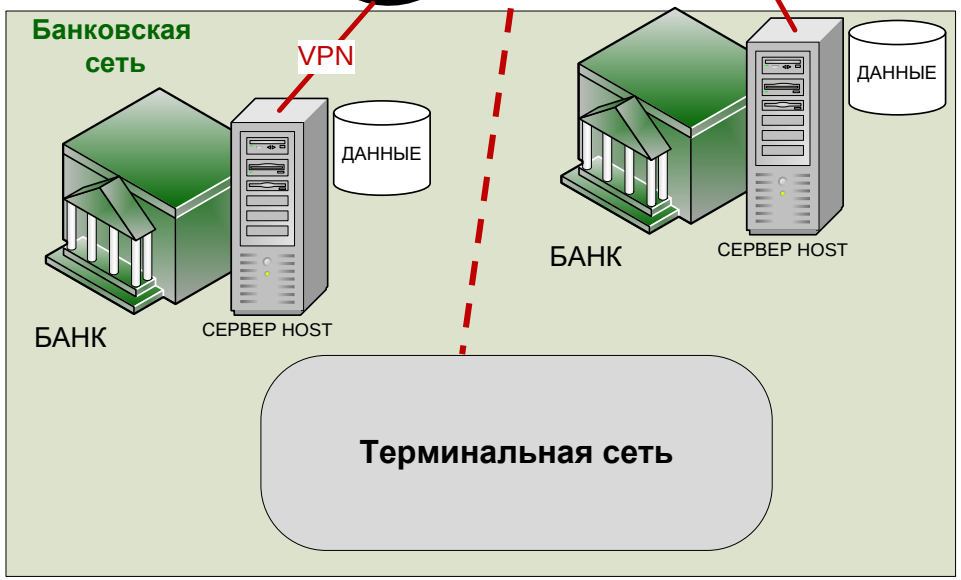
Балансировка ресурсов ?

Время отклика ?

Резервирование ?

Компрометация ?

Биллинг ?



Каким требованиям по безопасности должен соответствовать платёжный HSM?

PCI DSS

PCI PTS HSM 3.0 (4.0)

PCI SSF в составе Secure Software Standard (SSS)
и Secure Software Lifecycle (Secure SLC) Standard

НТС ФСБ

Требования к СКЗИ

Требования к СКЗИ в HSM модулях платёжных систем (ФТ-32)

Разработка и эксплуатация СКЗИ должны проводиться в соответствии с Положением ПКЗ-2005

Контактная информация

Электронная почта:

mareeva@systempb.ru

Телефон:

+7 812 468-15-61

Сайт:

www.systempb.ru

skzi.ru