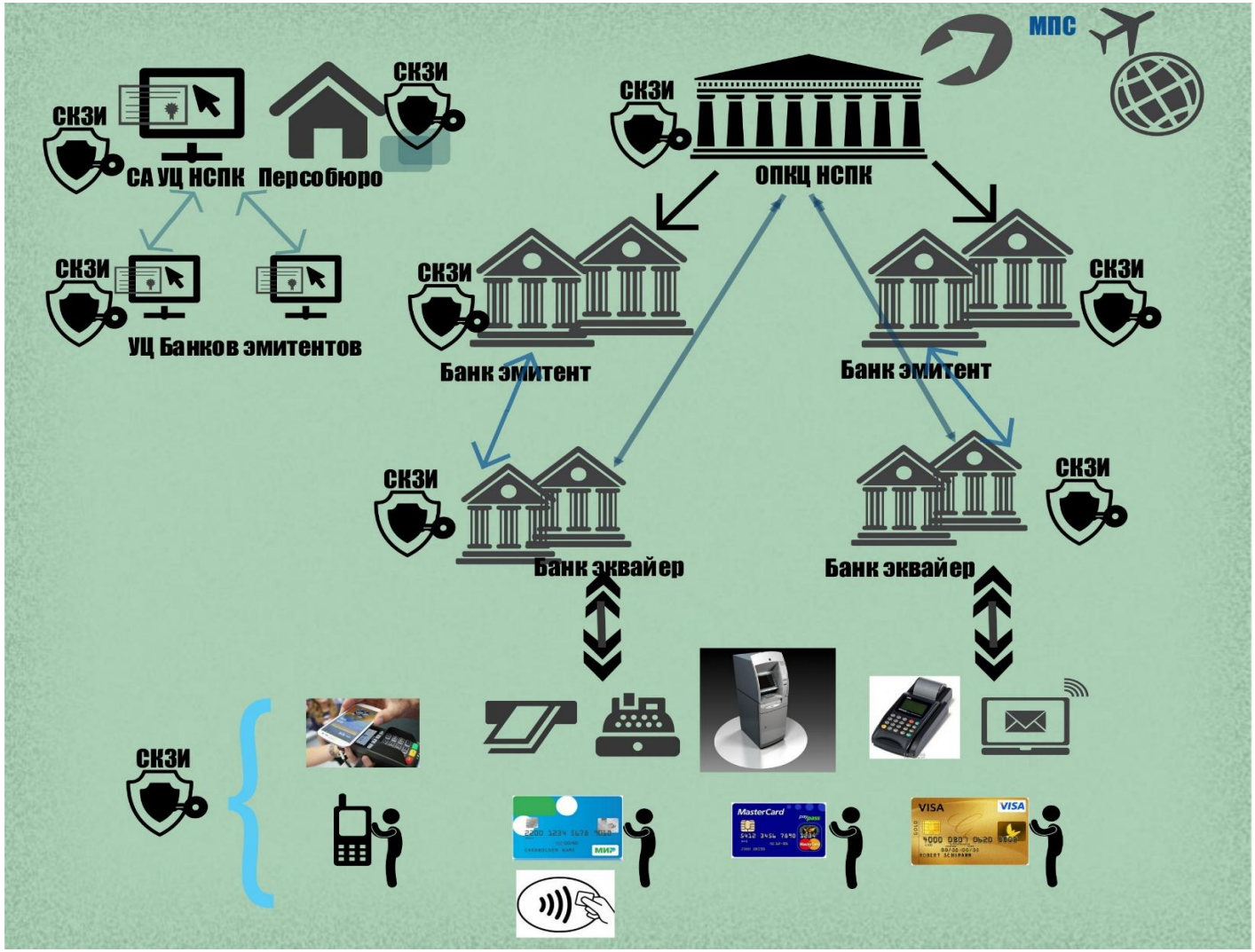
НЕКОТОРЫЕ УГРОЗЫ ПРИМЕНЕНИЯ ИМПОРТНЫХ HOST SECURITY MODULE (HSM) В НАЦИОНАЛЬНОЙ СИСТЕМЕ ПЛАТЁЖНЫХ КАРТ

Новое время – новые угрозы информационной безопасности системы платёжных карт

Атаки на систему платёжных карт – это целевые атаки на элементы инфраструктуры платёжных карт



Запрет использования технологии или прекращение поставок

Запрет экспорта. Основные поставщики

THALES
Thales e-Security

Thales e-Security из состава международной промышленной группы ThalesGroup

gemalto
security to be free
SafeNet

SafeNet, Inc. (now Gemalto)

Запрет использования технологии (распоряжения по Крыму – конец декабря 2014)

«прекратить выпуск карт, оказание услуг эквайринга или любых иных операций в Крыму с использованием продуктов и услуг Visa». Аналогично MasterCard

VISA
MasterCard

Платёжные системы не могут «оказывать услуги (поддерживать эмиссию и прием карт в Крыму, а также их обслуживание в банкоматах) и предлагать свои продукты в Крыму».

Управляемые результаты работы криптоалгоритмов или где лучше всего делать закладки?

- Dual_EC_DRBG — криптографически стойкий генератор псевдослучайных чисел, разработанный АНБ США, один из четырёх криптографически стойких генераторов, стандартизованных NIST . Предполагалось его применение в том числе в криптографических системах для генерации ключей. Алгоритм основан на использовании эллиптических кривых.
- Вскоре после публикации NIST, в 2007 году, было высказано предположение, что данный ГПСЧ содержит бэкдор. Учитывая широкое применение ГПСЧ в криптографии, уязвимость алгоритма позволяет взломать практически любую основанную на нём криптосистему.
- 20 декабря 2013 года стало известно о факте взятки, выданной АНБ США известной компании RSA Security. В обмен на крупную сумму денег, компания RSA обязывалась использовать генератор Dual_EC_DRBG как предпочтительный и по умолчанию в своих криптографических библиотеках семейства RSA BSAFE.
- Стандарт NIST SP 800-90 полностью одобрен по FIPS 140-2.
- Некоторые продукты компании RSA Security используют Dual EC DRBG по умолчанию с 2004 года. Лишь осенью 2013 года компания призвала не пользоваться алгоритмом.
- В декабре 2013 года Рейтер сообщило, что АНБ тайно заплатила компании RSA 10 миллионов долларов, чтобы та использовала Dual EC DRBG по умолчанию.
- Основные используемые в настоящее время в импортных HSM криптоалгоритмы: DES, 3DES, AES, RSA, SHA, MD-5, HMAC

Отказ в обслуживании или получение несанкционированного доступа к данным

Управляемый отказ в обслуживании может возникнуть в результате целевой атаки, поданной в HSM из внешнего ПО недекларированной команды или недекларированного параметра в штатной команде

- обнаружили достаточно большое количество недокументированных команд и параметров у команд в импортных HSM

Изменения касаются команд управления ключами – диверсификация ключей карты из мастер ключа, формирование криптограмм при проведении процессинга.

- Команды ZY, PM, KQ, HC

В банке эмитенте наиболее уязвим участок подготовки секретных величин карт

Используется прошивка HSM, которая имеет наименование Card Issuance Firmware (1119-0902) - Card Issuing Processing и не имеет сертификата PCI HSM

На участке выполняются режимы управления EMV-сертификатами эмитента и карточки, загрузки корневых сертификатов, генерации производных симметричных ключей и несимметричной пары для карточки, генерятся PINы

Особенности эксплуатации. Смена ключей – это сложно

Попытки сэкономить на количестве используемых устройств, за счёт «выравнивания» локальных мастер-ключей в большом количестве используемых в банке устройств

Процедура смены локальных мастер ключей становится критичной, как с точки зрения времени выполнения, так и возможности её безотказного выполнения. Данная процедура ещё и плохо автоматизирована

Попытки автоматизации работы с HSM иногда противоречат требованиям безопасности

Безопасность за Ваши деньги на заказ. А может это НДВ? Как правильно встраивать HSM в банковское ПО и кто это контролирует.

Существует практика, в соответствии с которой, любая фирма может заказать разработку своей специфической криптографической функциональности

- дополнительные команды порождают специфическую прошивку, которая сертификацию не проходит и за безопасность которой никто ответственности не несёт.

Используемые HSM работают под управлением различных модулей банковского ПО. Встраивание HSM в банковское ПО лишь косвенно регулируется PSI DSS и выполняется разработчиками банковского ПО

- Отсутствие чётко сформулированных требований по встраиванию базовой функциональности HSM (и тем более по дополнительным функциям) может приводить к ошибочным и небезопасным последствия

Выводы


1. Требуется парирование новых угроз применения импортных HSM в составе национальной системы платёжных карт
2. Парирование угроз возможно поэтапной заменой импортных HSM на отечественные HSM
3. Первоочередной задачей является замена импортных HSM на отечественные, функционирующие в режиме совместимости, на участке генерации секретных величин.
4. Задачей второго этапа является разработка процедур управления ключами и платёжными транзакциями по карте «МИР», при этом должны быть использованы отечественные криптоалгоритмы
5. Необходимо провести разработку отечественных стандартов, являющихся аналогом PCI HSM, правил встраивания HSM в банковское ПО и аудита выполнения данных требований