конференция
РусКрипто'2013

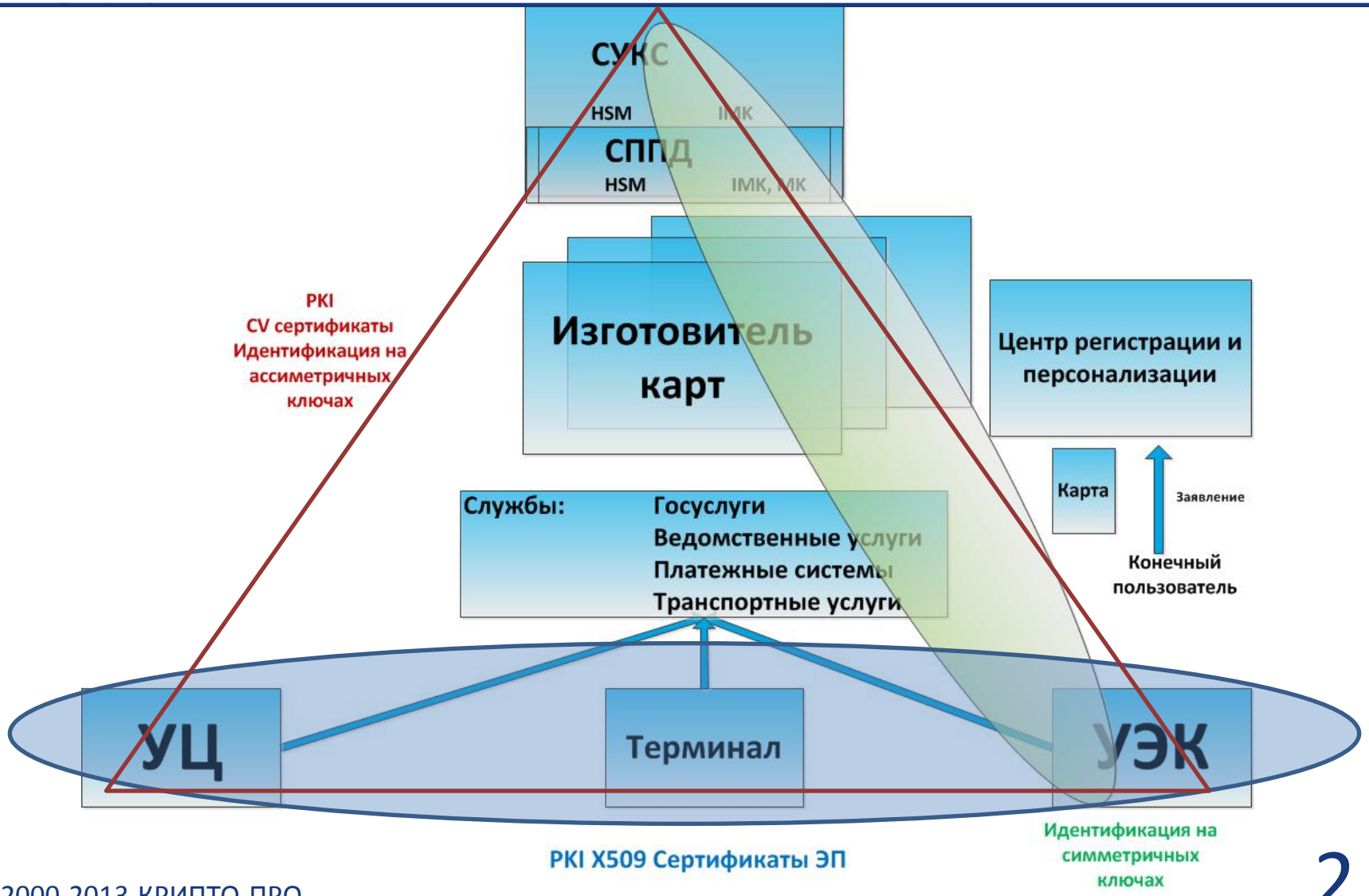
http://www.ruscrypto.ru/conference/

КРИПТО ПРО

Ключевые системы и криптографическая защита данных в системе Универсальной Электронной Карты

Павлов Михаил Вадимович
Попов Владимир Олегович

Информационные и ключевые потоки при производстве, персонализации и использовании УЭК.



Механизмы криптографической защиты информации системы УЭК.

- ГОСТ 28147-89, шифрование (на карте в режиме CBC), имитозащита.
- ГОСТ Р 34.10 – 2001, ЭЦП и ключи протокола Диффи-Хеллмана.
- ГОСТ Р 34.11 – 94, функция хэширования.
- RFC4357, алгоритмы ключевых систем.
- Сертификаты X.509, CV сертификаты.
- ЕПСС УЭК – Спецификация идентификационного приложения. Часть 3. Обеспечение безопасности и управление ключами.

Типы ключей системы УЭК

- Симметричные ключи
  - IMK – ключи Эмитента. Хранятся в HSM СУКС.
  - MK - Мастер ключи, выводятся из IMK и пересылаются в низовые звенья
  - K - Сессионные ключи, выводятся из MK, шифрование, MAC
- Ассиметричные ключи в системе PKI CV сертификатов
  - S,P - ключевая пара аутентификации субъектов обмена и идентификации ID-приложения карты
  - K - согласованный сессионный ключ, полученный по алгоритму Диффи-Хеллмана (VKO RFC 4357) On Line защиты ключей и обмена Терминал - карта
- Ассиметричные ключи в системе PKI X.509 сертификатов
  - S,P - ключевая пара ЭП владельца карты в системе PKI службы;
    - ключевая пара аутентификации субъектов обмена
  - K - согласованный сессионный ключ, полученный по алгоритму Диффи-Хеллмана (VKO RFC 4357) On Line защиты ключей
- Транспортные ключи
  - Разделённые ключи, Off Line защита ключевой информации

Алгоритмы EMV. Алгоритмы ОАО «УЭК»

EMV определяет основные криптографические протоколы жизненного цикла интеллектуальной карты и её окружения в платёжной системе на базе стандартов DES, RSA, SHA-1

Криптографические протоколы (аутентификация на ключах карты, парольная аутентификация)

Криптографические алгоритмы (шифрование и коды аутентификации, диверсификация ключей).

ООО УЕК определяет аналоги криптографических алгоритмов и протоколов на базе российских стандартов ГОСТ 28147-89, ГОСТ Р3410-2001, ГОСТ 3411-94.

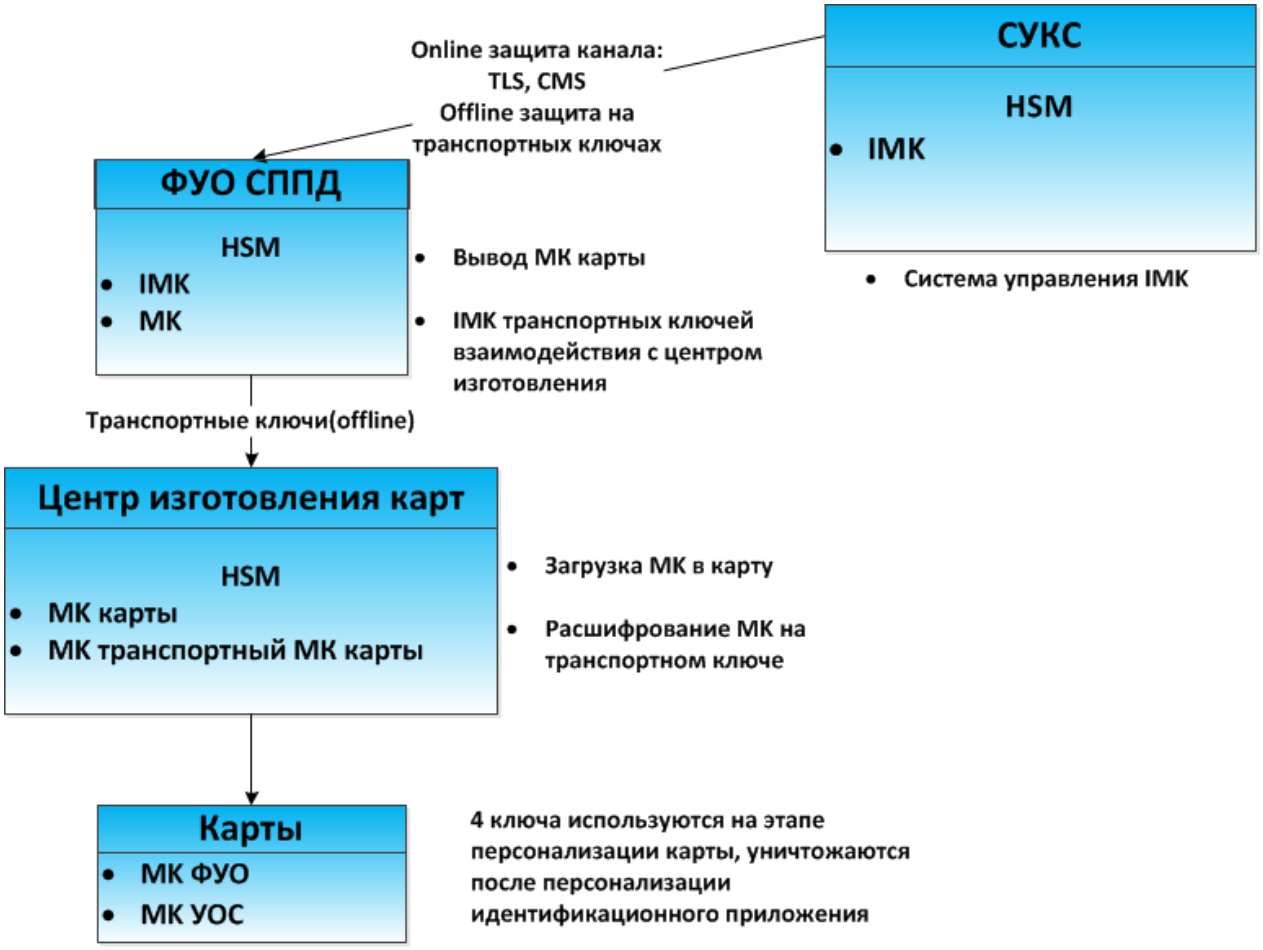
Наиболее интересны функции вывода мастер ключа из ключа эмитента и сессионного ключа из мастер ключа:

MK := **ENC**[**IMK**](**Hash**(**DD**)). CBC – шифрование.

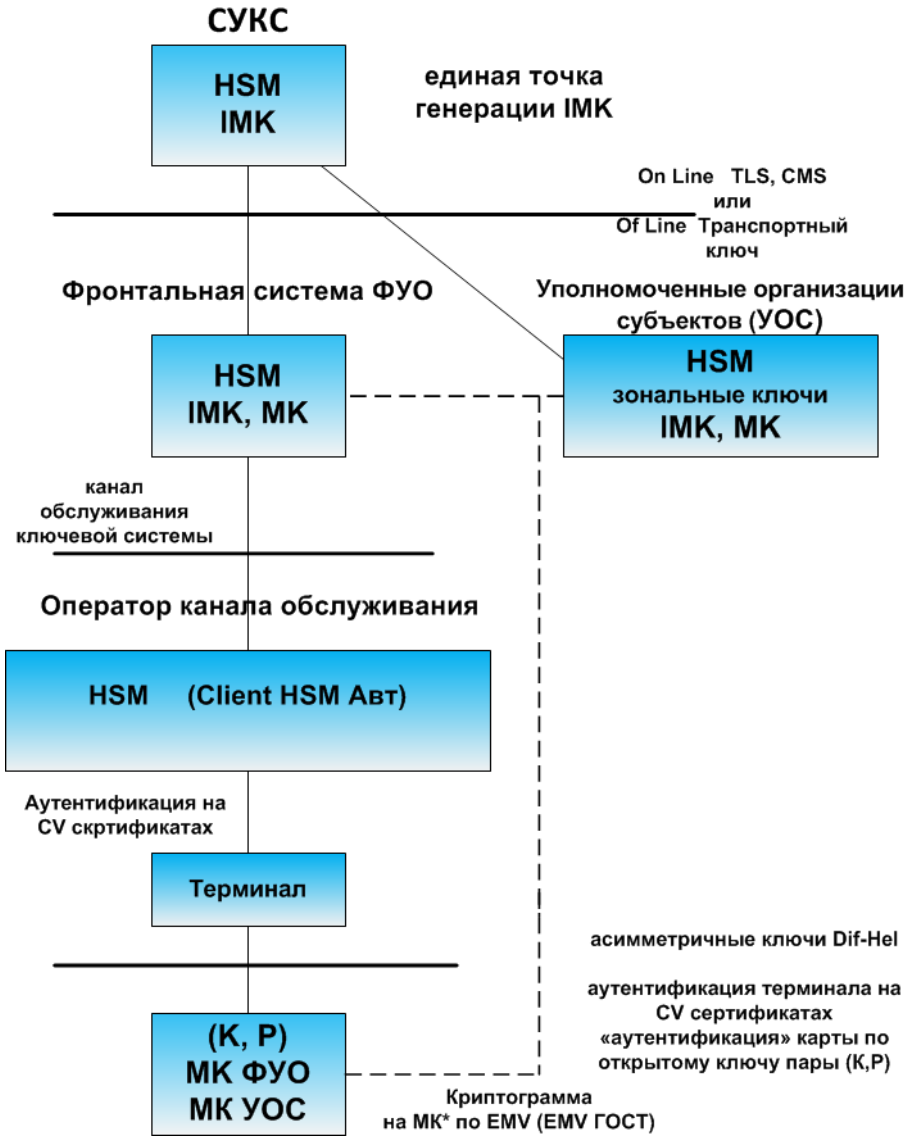
SK := **HASH**(**MK**||**DD**)

Определяет систему выработки и распространения симметричных ключей с центром доверия СУКС.

Симметричные ключи. Процесс выпуска карт



Симметричные ключи. Процесс обслуживания карт



Асимметричные ключи. Иерархия PKI CV-сертификатов

CV сертификаты служат исключительно для аутентификации карт, создания защищенных каналов

Асимметричные ключи. PKI конечного пользователя, X.509 сертификаты.

- Реестр УЦ – список аккредитованных УЦ.
  Обеспечивают выпуск квалифицированных сертификатов.

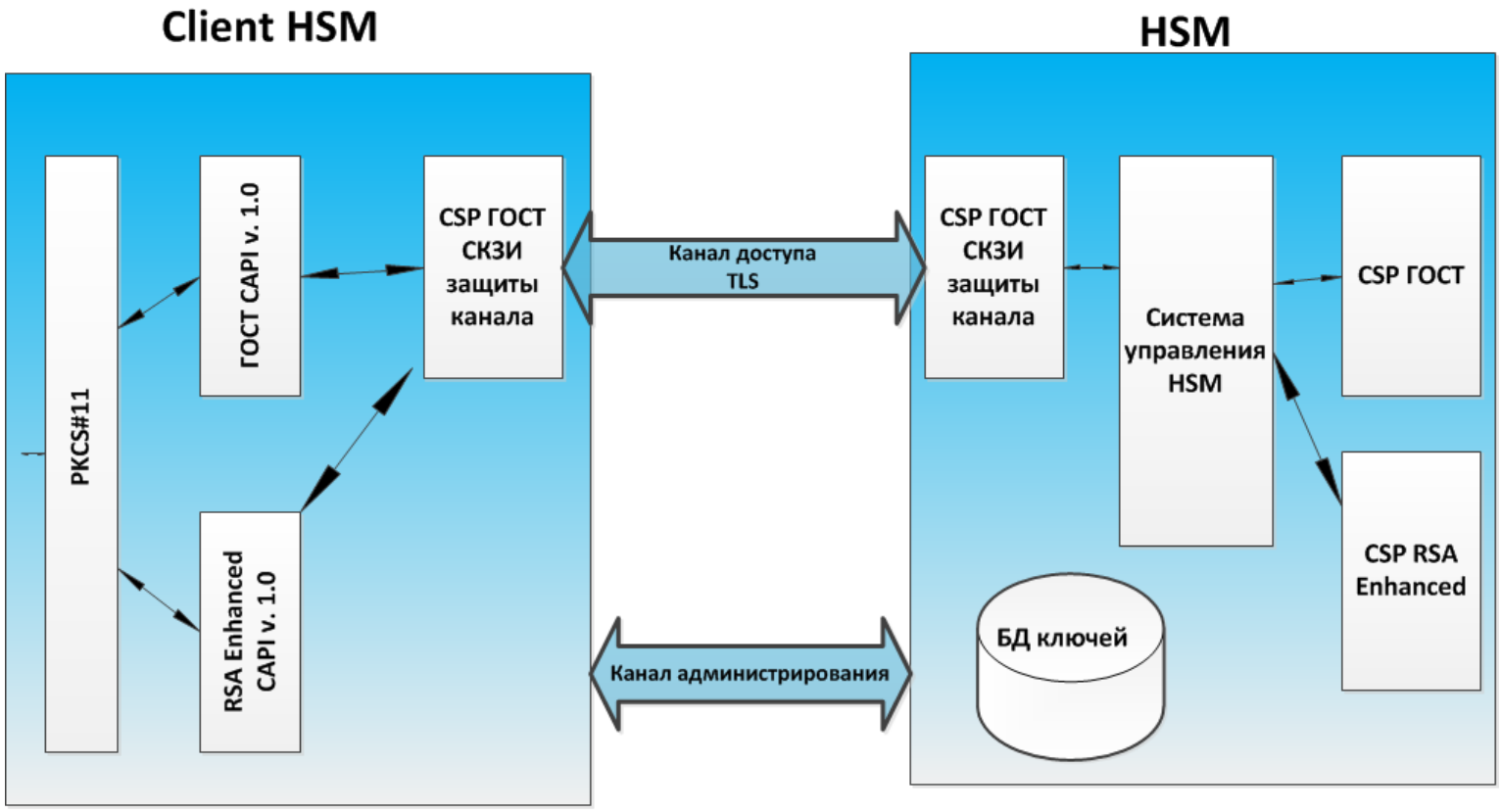
- Ключ подписи пользователя УЭК включается в одну из систем PKI УЦ.

Аппаратно-программная платформа ключевой системы УЭК

- Крипто Про HSM (уровень защиты КВ2, на этапе тематических исследований)
- Крипто Про клиент HSM (уровни защиты КВ2, КС3… , на этапе тематических исследований)
- Крипто Про CSP-ФКН – криптосервиспровайдер для работы с картами подписи. Используется в терминалах и АРМ’ах пользователей для доступа к системе УЭК (уровни защиты КС1(сертифицирован) КС3,КС2 , на этапе согласования ТЗ)
- УЭК (уровни защиты КС3 – КС1 (сертифицирован))

КриптоПро HSM

Система доверенного хранения и обработки ключей (уровень защиты КВ2)



Принцип: ключи в HSM либо не экспортируются (как правило корневые ключи HSM), либо экспортируются в защищенном виде (шифр + имита).

Криптографические протоколы системы УЭК.

- Аутентификация терминала
  - Процедура проверки сертификатов терминала и ОКО ИД-приложением
  - Динамическая аутентификация терминала (ГОСТ Р 34.10-2001)
    - *Механизмы: DH + проверка подписи терминала ИД-приложением*

- Защищённый обмен сообщениями
  - *Механизмы шифрования, MAC, счётчиков ЗОС*
- Контрольное приветствие
  - *Механизм контроля терминала через контрольную фразу (опционально).*
- Верификация держателя карты по PIN коду держателя карты

- Аутентификация ИД-приложения.
  - *Механизм контроля ОКО, ФУО достоверности УЭК*
  - Запрос аутентификации ИД-приложения в режиме online
  - *вычисление картой и проверка ФУО кода аутентификации на ключе МК ФУО*
  - Запрос аутентификации ИД-приложения в режиме offline
  - *вычисление картой и проверка ФУО подписи на ключе аутентификации на CV-сертификатах*
  - Обработка результатов аутентификации ИД-приложения
  - *ОКО и ФУО аутентифицируются по подписи на CV-сертификатах*

Криптографические протоколы системы УЭК. (продлжение)

•Электронная подпись держателя карты УЭК

Формирование электронной подписи держателя карты УЭК

Проверка электронной подписи держателя карты УЭК

• Аутентификация эмитента ИД-приложения

-Механизм: на производном ключе от МК эмитента

• Защищённый канал терминала с Поставщиком услуг

-Механизм: DH на статических ключах

Настройка защищённого канала

Защищённая передача запроса на оказание услуги

Защищённая передача ответа на запрос оказания услуги

• Аутентификация терминалом поставщика услуги

-Механизм: подпись на ключе поставщика услуг

Архитектура GlobalPlatform и криптографические алгоритмы и протоколы

Защита APDU команд в канале терминал – карта на ключах, полученных по протоколу “Аутентификация терминала”

КРИПТО ПРО

Выводы

Вопросы

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru
pav@cryptopro.ru
vpopov@cryptopro.ru

Тел./факс:
+7 (495) 780-48-20
+7 (495) 660-23-30