



конференция  
РусКрипто'2013

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

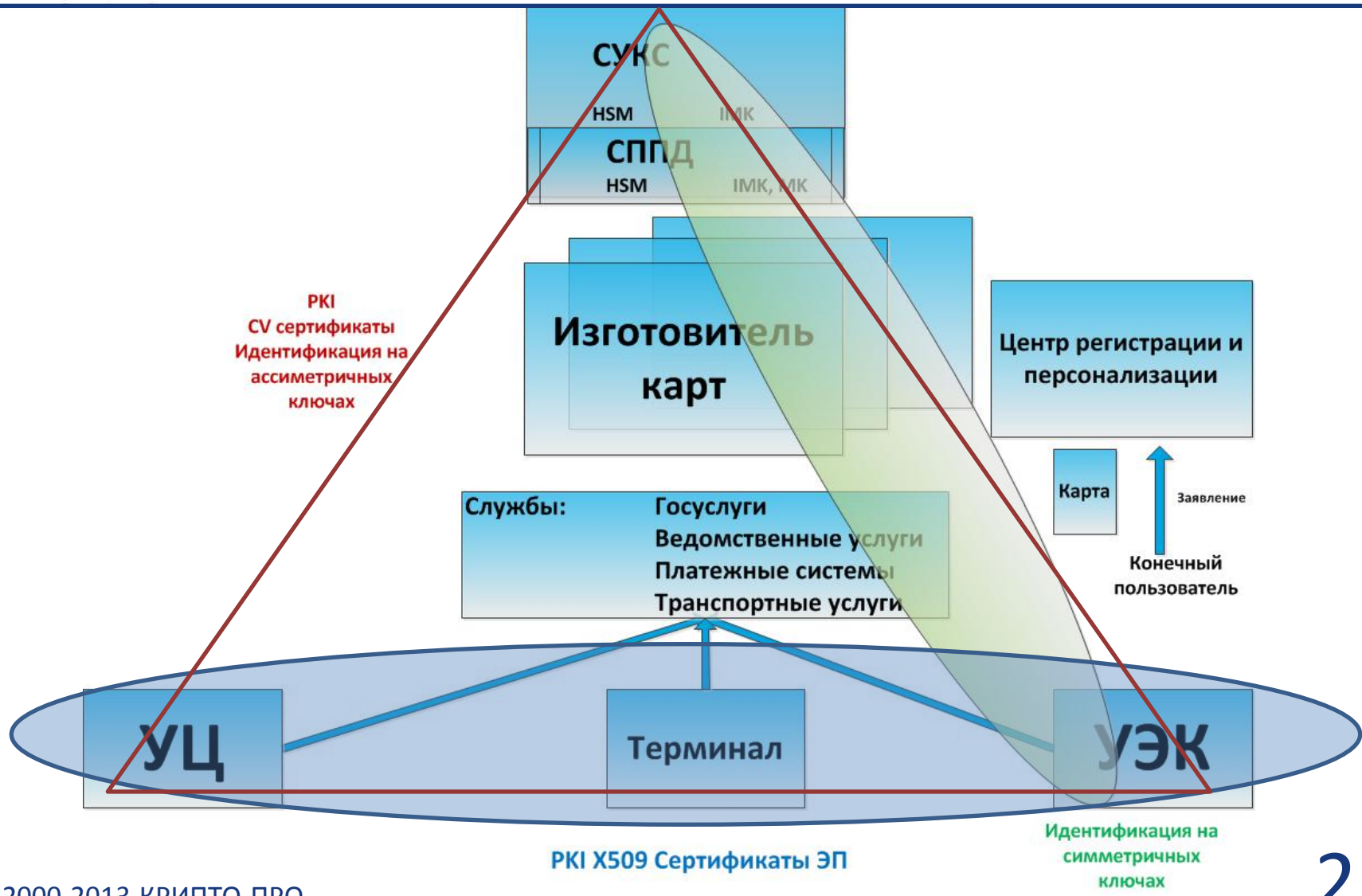


# Ключевые системы и криптографическая защита данных в системе Универсальной Электронной Карты

Павлов Михаил Вадимович  
Попов Владимир Олегович

© 2000-2013 КРИПТО-ПРО

# 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.

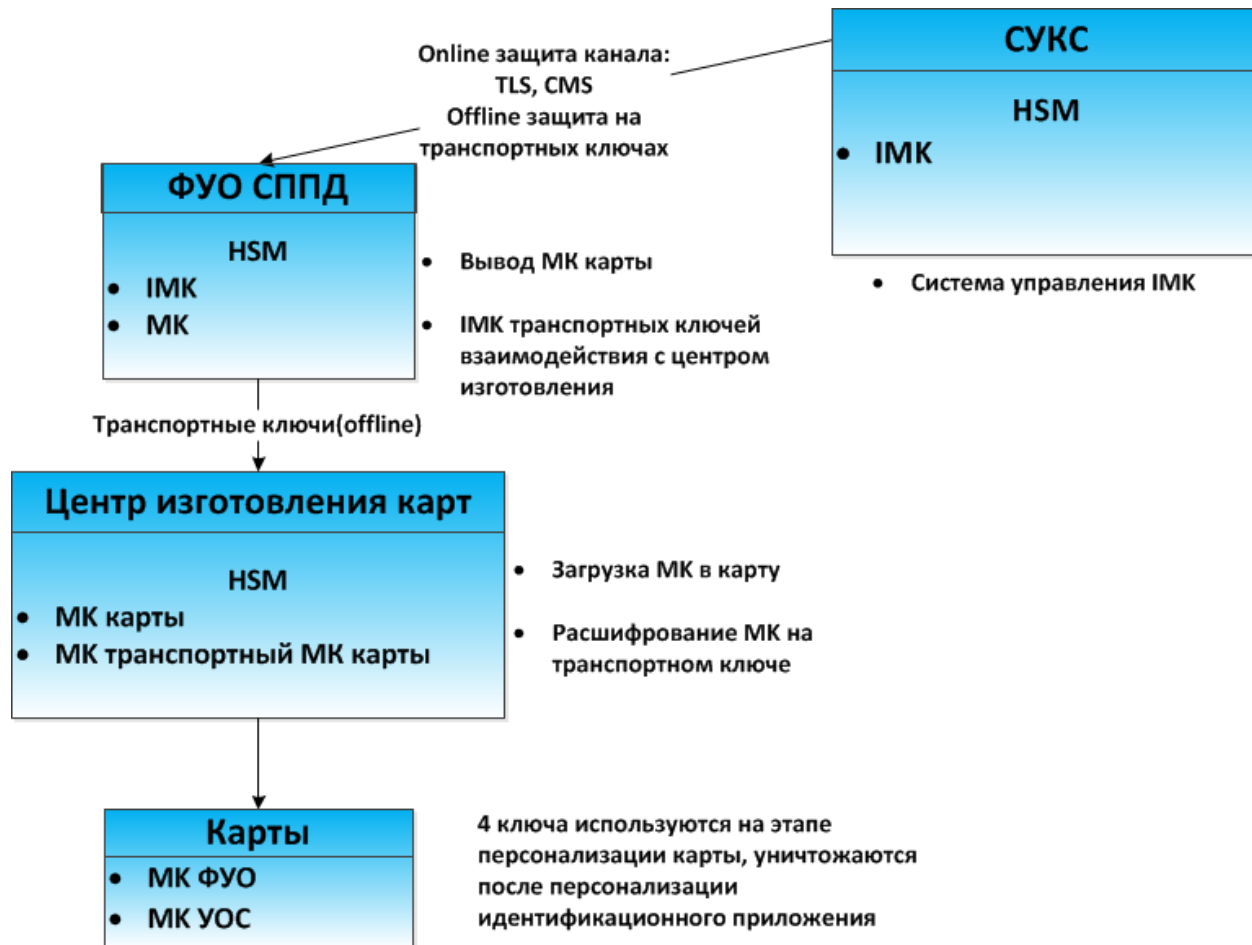
# Типы ключей системы УЭК



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

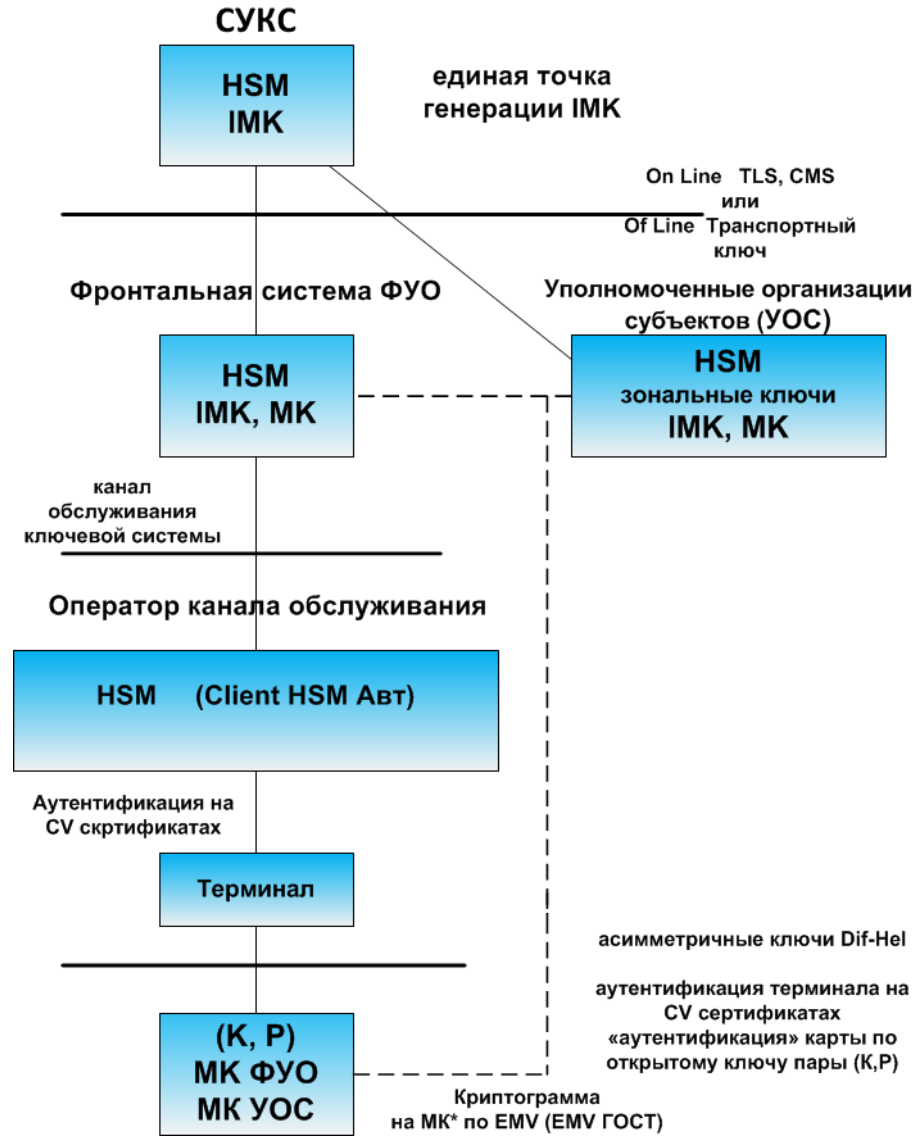


# Симметричные ключи. Процесс выпуска карт



Сессионные ключи. Выводятся из ключей согласования, полученных при помощи алгоритма Диффи-Хеллмана

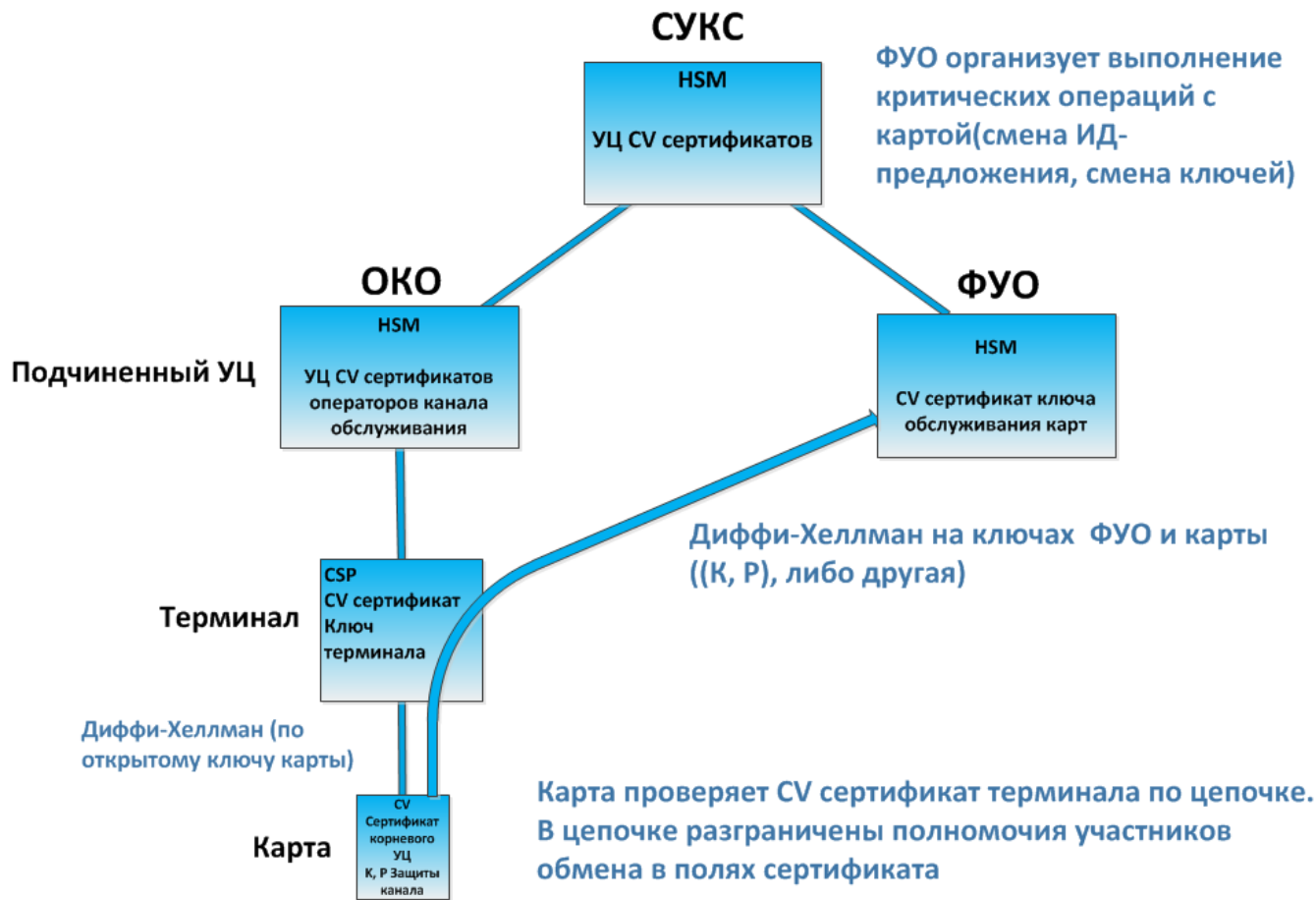
# Симметричные ключи. Процесс обслуживания карт



# 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

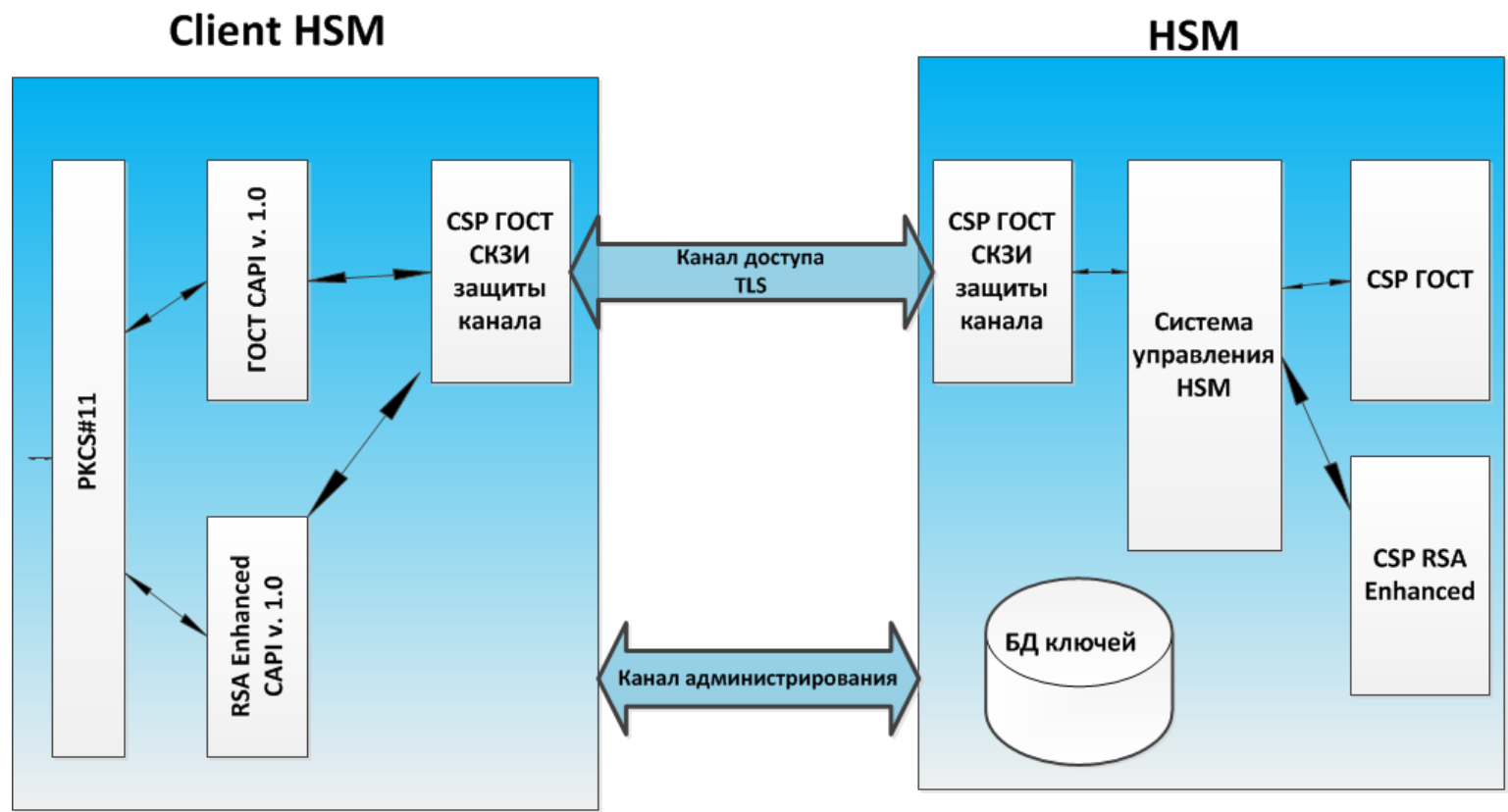


- Крипто Про HSM (уровень защиты KB2, на этапе тематических исследований)
- Крипто Про клиент HSM (уровни защиты KB2, KC3... , на этапе тематических исследований)
- Крипто Про CSP-ФКН – криптосервиспровайдер для работы с картами подписи. Используется в терминалах и АРМ'ах пользователей для доступа к системе УЭК (уровни защиты KC1(сертифицирован) KC3, KC2 , на этапе согласования ТЗ)
- УЭК (уровни защиты KC3 – KC1 (сертифицирован) )



# КриптоПро HSM

## Система доверенного хранения и обработки ключей (уровень защиты KB2)



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.

(продление)



- 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”



**Выводы**

**Вопросы**

**СПАСИБО ЗА ВНИМАНИЕ!**

**КРИПТО-ПРО – ключевое слово в защите информации**

<http://www.cryptopro.ru>

[pav@cryptopro.ru](mailto:pav@cryptopro.ru)

[vporov@cryptopro.ru](mailto:vporov@cryptopro.ru)

Тел./факс:

+7 (495) 780-48-20

+7 (495) 660-23-30