УЭК

Протокол защищенного обмена сообщениями SCP-F2

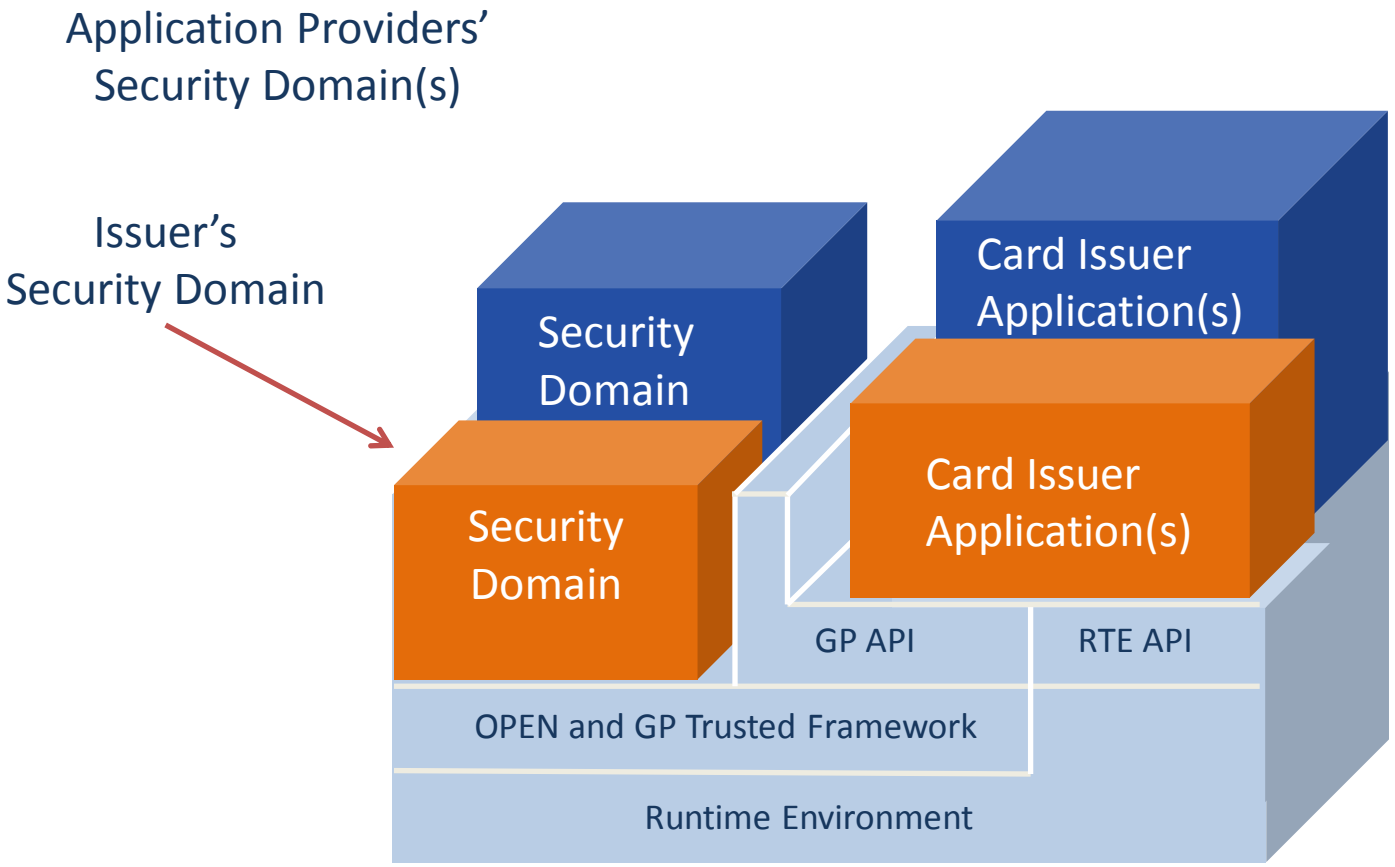
конференция
РусКрипто'2013

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

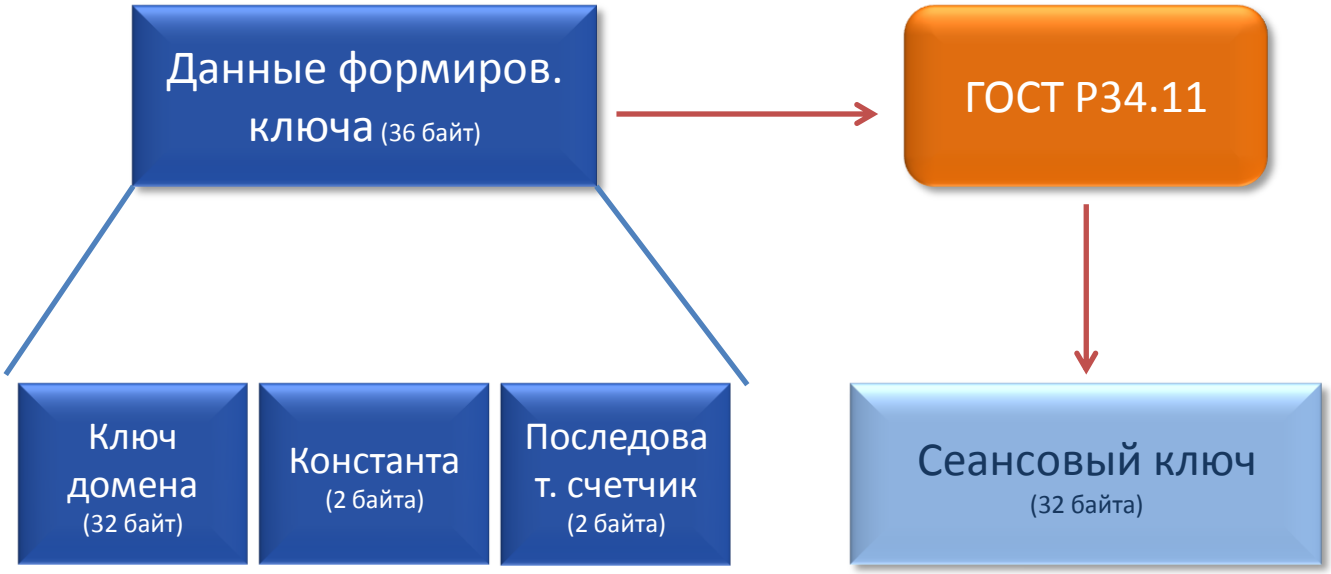
29 марта 2013 года

Применение Global Platform

Архитектура GlobalPlatform



Создание сеансового ключа на основе ключа домена

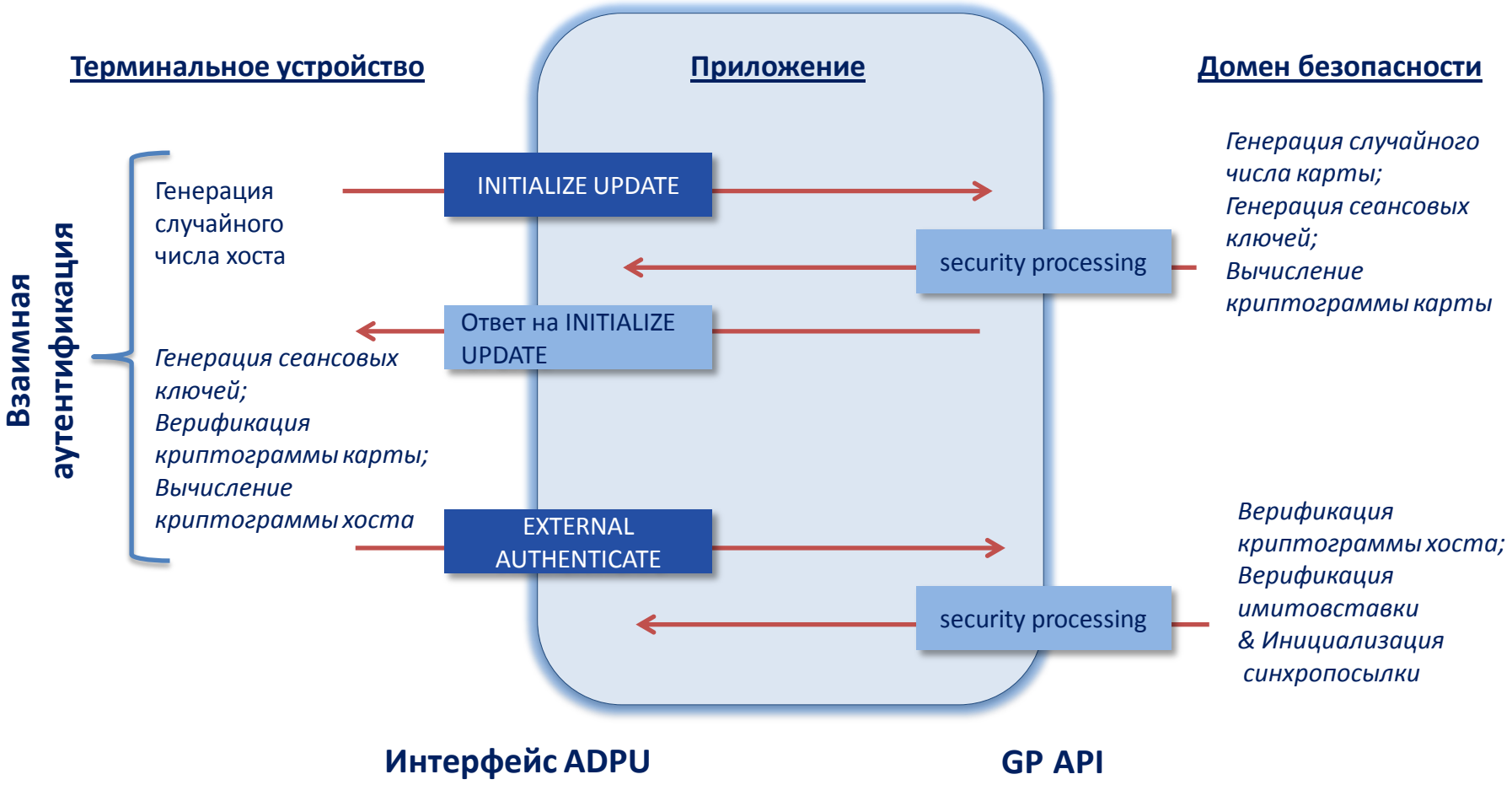


SCP-F2 – Ключи безопасного соединения домена безопасности

- Взаимная аутентификация
- Целостность и аутентификация источника данных
- Конфиденциальность

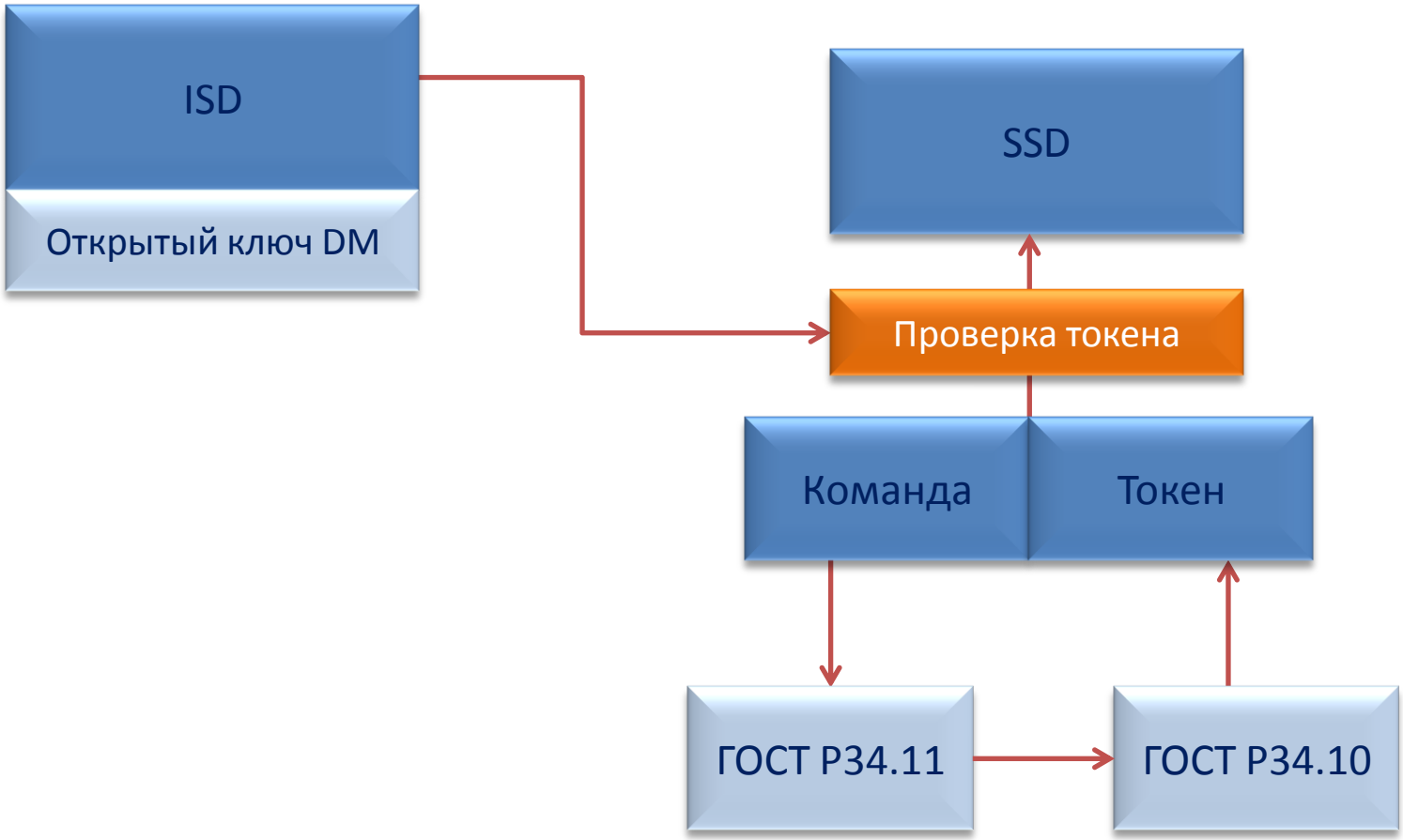
Ключ	Применение
Ключ шифрования	Аутентификация и шифрование(ГОСТ 28147-89)
Ключ для расчета имитовставки (S-MAC)	Генерация и проверка имитовставки (ГОСТ 28147-89)
Ключ для шифрования критических данных (DEK)	Шифрование и расшифрование критических данных (ГОСТ 28147-89)

Установление сессии защищенного обмена сообщениями



Delegated Managment

Для вычисления токенов используется алгоритм вычисления ЭП ГОСТ Р34.10-2001 вместе с алгоритмом хеширования ГОСТ Р34.11-94



Спасибо за внимание!

Безнос Александр Владимирович
Начальник отдела развития микропроцессорных платформ
Beznos-AV@uecard.ru

Федеральная уполномоченная организация - открытое акционерное общество «Универсальная электронная карта»

119021, Москва, улица Тимура Фрунзе дом 11, стр. 15
Тел./Факс: +7 495 777 13 27
E-mail: info@uecard.ru
www.uecard.ru