конференция РусКрипто

КРИПТО ПРО

Облачная подпись и мобильные платформы

Смирнов Павел
Зам. начальника отдела разработок, к.т.н.
ООО «КРИПТО-ПРО»

План

- Необходимость облачной криптографии на мобильных устройствах
- Опыт Евросоюза
  - Эволюция законодательства
  - Практическое применение облачной электронной подписи: Испания, Норвегия, Австрия, Италия
- Европейские требования к реализации облачной подписи

Гранаты у него не той системы

- Подключить привычный носитель нельзя

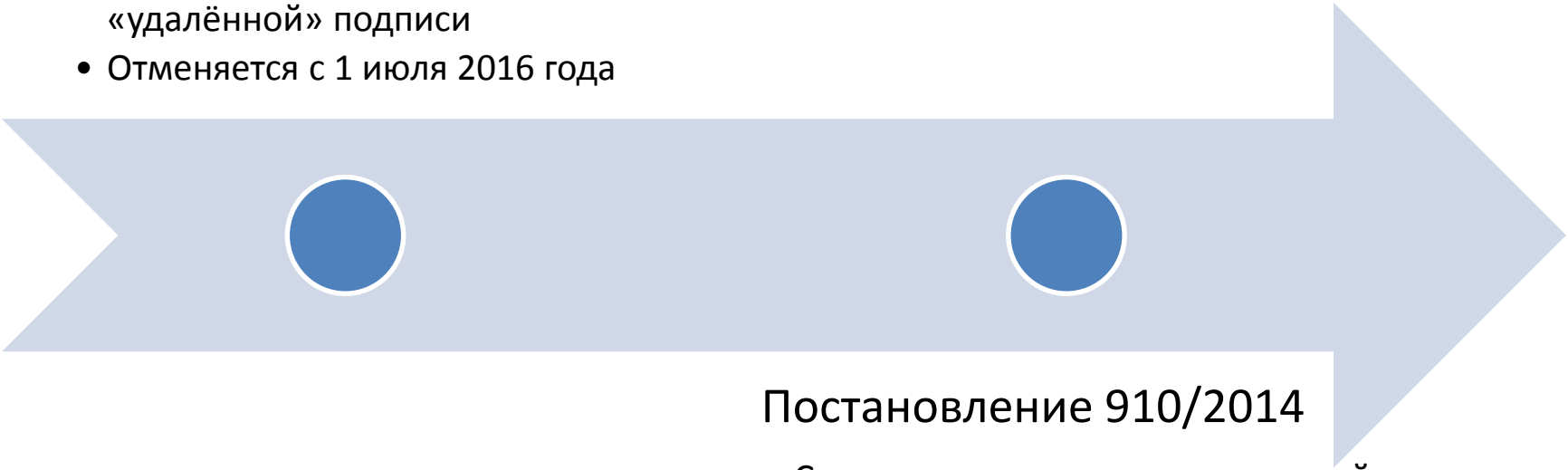
  или

- Сложно, дорого, неудобно

Европейское законодательство

Директива 1999/93/EC

- Не затрагивает вопросы «удалённой» подписи
- Отменяется с 1 июля 2016 года



Постановление 910/2014

- Создание и использование ключей квалифицированной подписи можно доверить третьей стороне
- Сервер квалифицированной подписи должен управляться аккредитованным поставщиком услуг

Испания: квалифицированная ЭП в облаке

- 350 000 квалифицированных сертификатов
- Из них 30 000 в облаке
- Создание усовершенствованных подписей (*AdES)
- Соответствует требованиям проекта стандарта CEN TS 419241
- Ключи хранятся в HSM

Норвегия: усиленная ЭП с квалифицированным сертификатом в облаке

С 2005 года

- 3 100 000 сертификатов
- Из них 2 930 000 в облаке
- Около 600 000 пользователей мобильного приложения
- Пиковое использование: ~1,3 млн операций в день
- Из них 20-25% - подписание
- Форматы подписываемых документов: текст, XML, PDF
- Ключи хранятся в HSM
- Система аттестована компетентными органами

Австрия: квалифицированная ЭП в облаке

С 2009 года

- Сервер подписи управляется аккредитованным УЦ
- Двухфакторная аутентификация: номер телефона + пароль, одноразовый пароль по SMS
- Поддерживает подпись документов PDF
- Ключи хранятся в HSM

Италия: квалифицированная ЭП в облаке

Греция признала итальянский сертификат SSCD

- Сервер подписи управляется аккредитованным УЦ под надзором уполномоченного госоргана
- Более 200 000 квалифицированных сертификатов
- Соответствует требованиям стандарта CEN TS 419241 по уровню 2 (квал. подпись) – подтверждено сертификатом
- Ключи хранятся в HSM

Техническая спецификация CEN TS 419241

“Security Requirements for Trustworthy Systems Supporting Server Signing”

CEN TS 419241 (14 октября 2013г)

Содержит требования и рекомендации к серверам электронной подписи

- Уровень 1: усиленная ЭП.
  Аутентификация пользователя в приложении, которое обращается к серверу для формирования подписи.
- Уровень 2: квалифицированная ЭП.

Требования к серверу квалифицированной ЭП

- Аутентификация пользователя напрямую на сервер подписи
- Многофакторная аутентификация (как минимум два)
- Ключ хранятся в специализированном защищённом устройстве (например, HSM)
- Остальные требования выполняются при использовании HSM, сертифицированного по КВ2

КриптоПро DSS соответствует!

Резюме

- Облачная подпись на мобильном устройстве не только полезна, но и удобна
- Европейский опыт подтверждает возможность использования квалифицированной облачной подписи
  - с законодательной точки зрения
  - из практики
  - с точки зрения технического регулирования

КРИПТО ПРО

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru

info@cryptopro.ru

spv@cryptopro.ru

Тел./факс:

+7 (495) 995-48-20