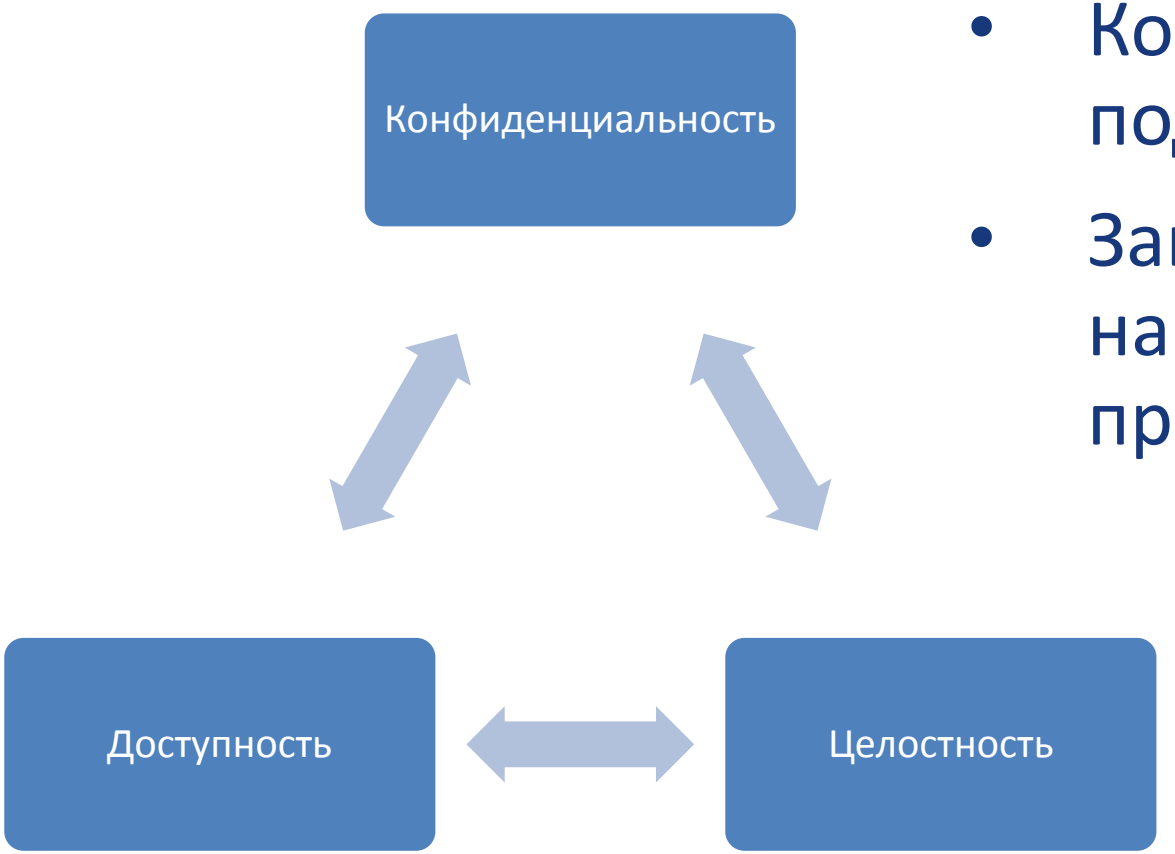
ИБ и ЭДО

Смирнов Павел

Зам. начальника отдела разработок, к.т.н.

ООО «КРИПТО-ПРО»

Краеугольные камни ИБ



- Комплексный подход
- Защита начинается на этапе проектирования

Характерные для ЭДО аспекты защиты

Защищаемый элемент - документ

Конфиденциальность

- Угрозы: кража, перехват, перенаправление …
- Ответ: защита от НСД, шифрование

Целостность

- Угрозы: искажение, уничтожение, отказ от авторства, юридическая ничтожность …
- Ответ: защита от НСД, электронная подпись

Применение криптографии в ЭДО

- Шифрование каналов связи
- Шифрование документов
  - При передаче
  - При хранении
- Электронная подпись документов

КриптоПро CSP

Популярность	• Наиболее распространённое в России сертифицированное средство ЭП
Платформы	• Windows, LSB Linux, ALT Linux, AIX, Solaris, Mac OS X, iOS, …
Ключевые носители	• Флеш-диск, Rutoken, eToken, Jacarta, Магистра, другие смарт-карты, HDD, Touch-Memory, …
Постоянное развитие	• С 2001 года, выпущено десять версий, получено более сорока сертификатов ФСБ
Экосистема продуктов и решений	• Более 20 продуктов нашей разработки, сотни продуктов партнёров

КриптоПро CSP
Примеры интеграции

Недостатки традиционного подхода

“Каждая система безопасна настолько, насколько безопасно ее самое слабое звено.”

Б.Шнайер, Н.Фергюсон “Практическая криптография” (2003)

Основные слабости:

- Утрата и кража ключевых носителей
- Невозможность контроля среды функционирования криптосредства на рабочем месте клиента

«Облачная» ЭП – что хочется

Исключить установку и использование средств ЭП на рабочем месте пользователя

- Любой компьютер, в любой точке мира, на любой платформе
- Массовый, неквалифицированный пользователь
- Не требуется контроль среды функционирования криптосредства на рабочем месте клиента

Исключить хранение ключа ЭП непосредственно у владельца

- Не имею и не теряю
- Невозможность компрометации ключа ЭП владельцем

«Облачная» ЭП. Требования к защите ключа

КРИПТО ПРО

Должна обеспечивать доверенное хранение и использование ключей электронных подписей

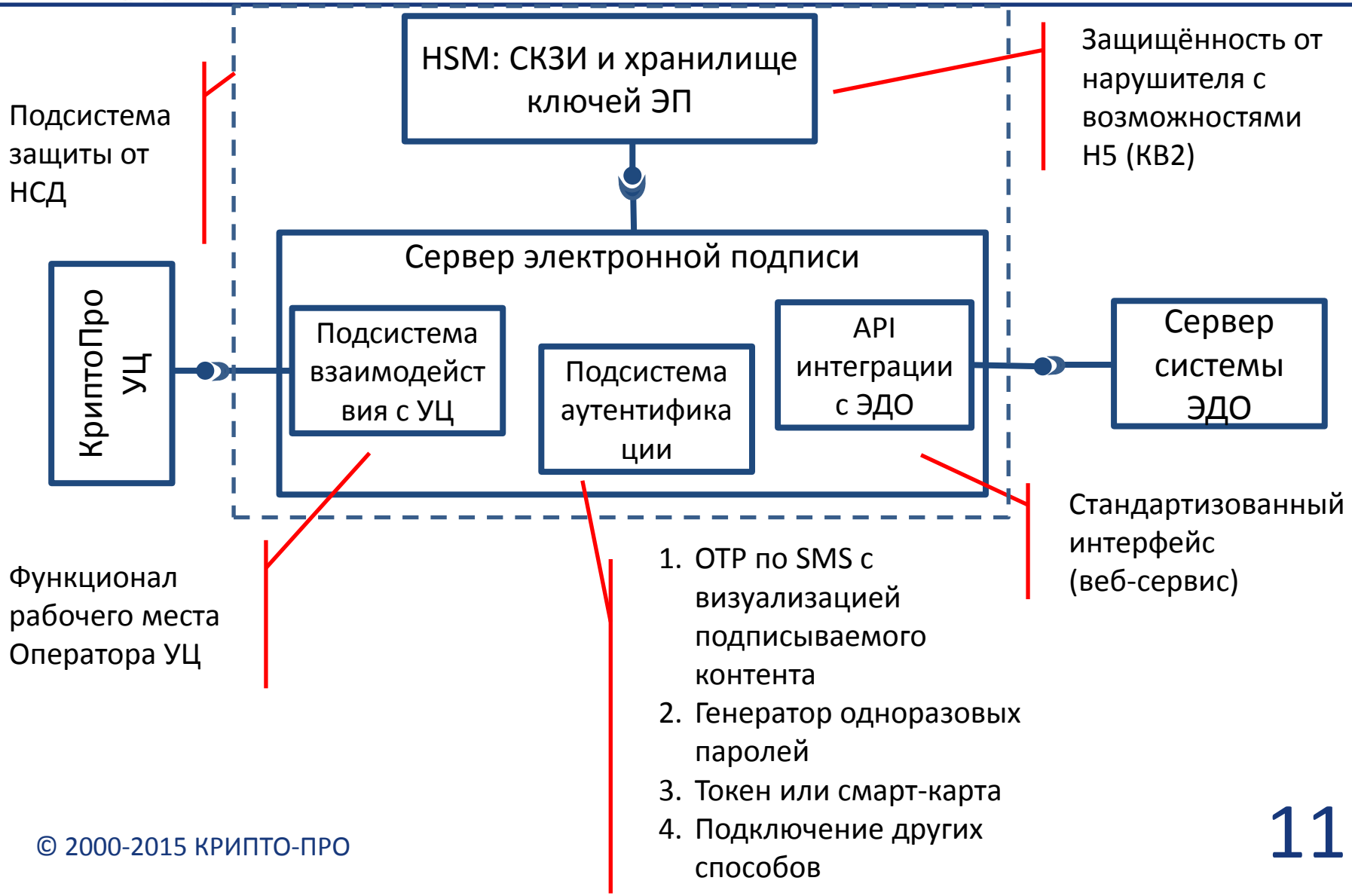
- Доказываемое исключение из числа нарушителей любого сотрудника оператора «облачной» технологии, включая администраторов системы
- Гарантированная защита от компрометации ключей по любым каналам атак
- Доверенная среда функционирования средства ЭП, использующего ключи ЭП пользователей

«Облачная» ЭП. Требования к аутентификации

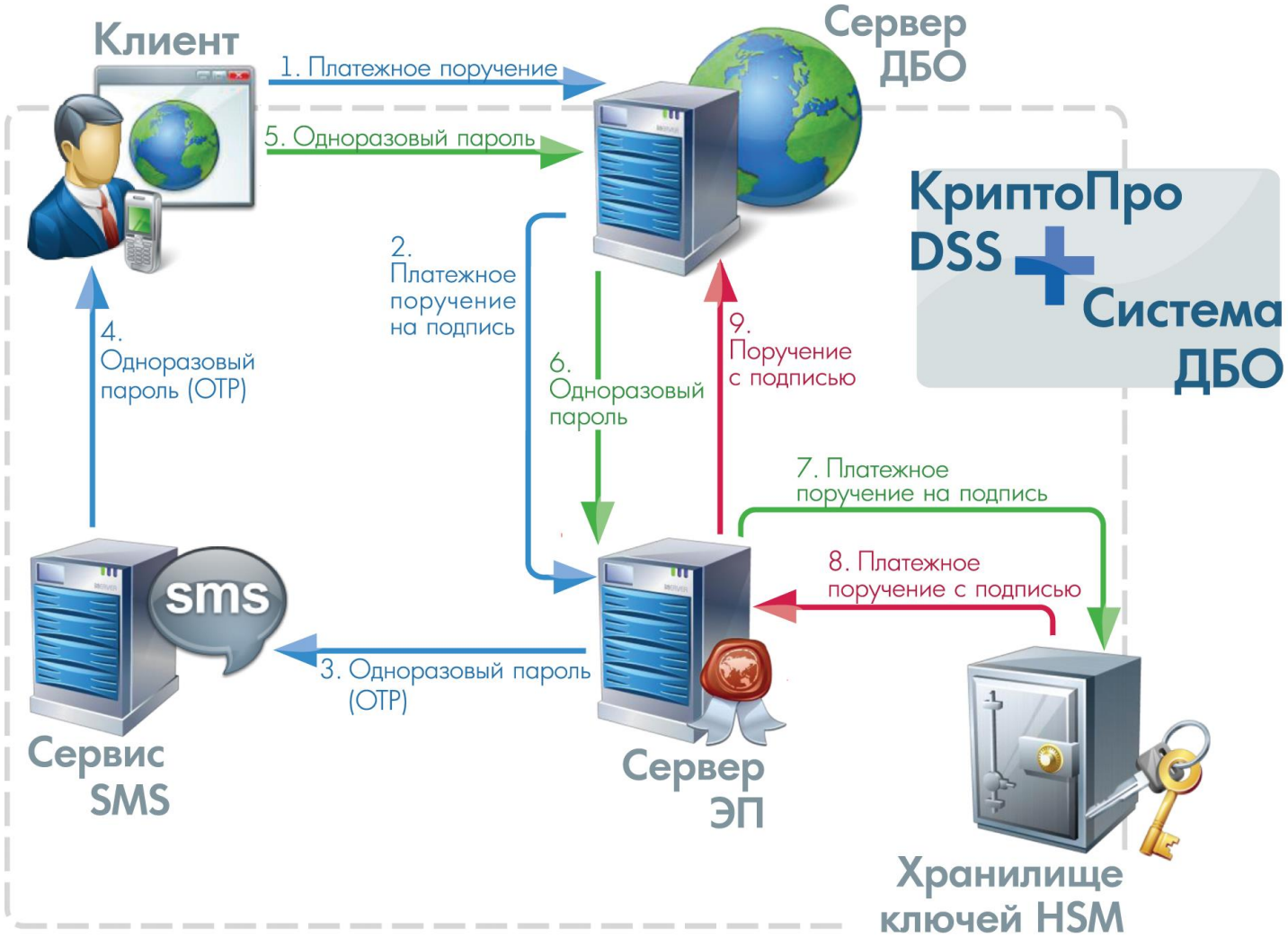
Должна реализовывать надежную и оцениваемую систему аутентификации владельца сертификата

- Доказываемая аутентификация в рамках принятой модели нарушителя и модели угроз
- Несколько способов многофакторной аутентификации владельцев ключа электронной подписи
- Использование резервных методов аутентификации

Структурная схема «КриптоПро DSS»



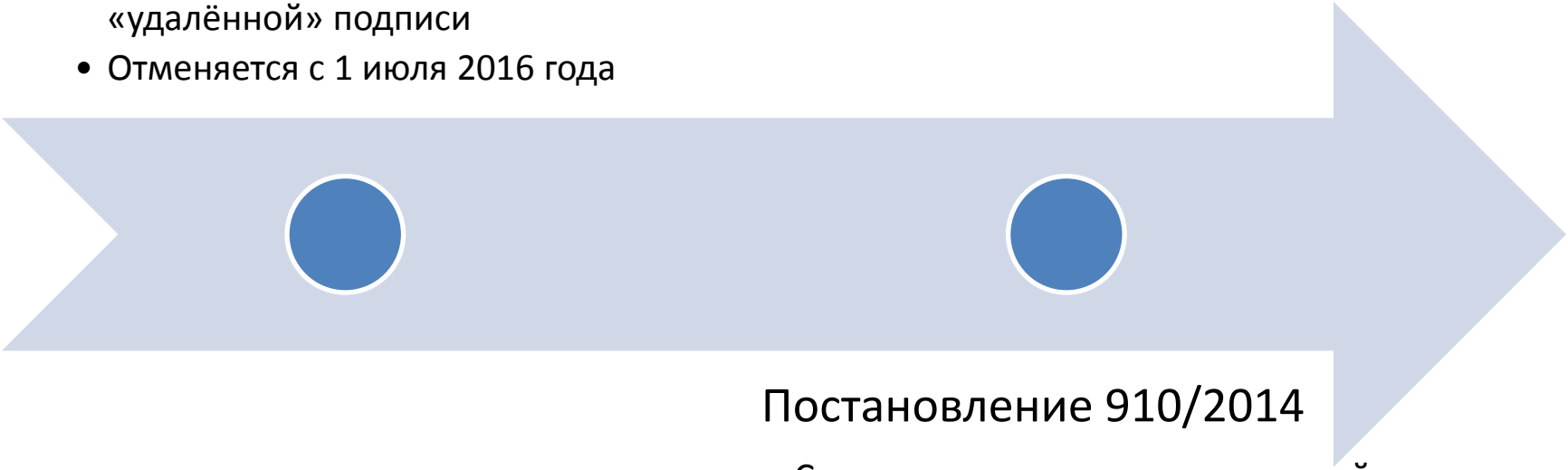
Пример подписания документа с аутентификацией «OTP по SMS»



Европейский опыт «облачной» ЭП: Законодательство

Директива 1999/93/ЕС

- 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

Европейский опыт «облачной» ЭП: Техническое регулирование

“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.
- Уровень 2: квалифицированная ЭП.

Европейский опыт «облачной» ЭП: Практическое применение

Испания

Норвегия

Австрия

Италия

Что нужно пользователю технологии ЭП? КриптоПро DSS!

Безопасность

Любые устройства

Любые платформы

Любые браузеры

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