КРИПТО ПРО

VI-ая Международная конференция в сфере электронной торговли «Информационная безопасность и PKI»

г. Казань, 22–24 октября 2014 г.

Новинки и тенденции в развитии продуктов компании КРИПТО-ПРО

Маслов Юрий
Коммерческий директор
ООО «КРИПТО-ПРО»

Тренд № 1: Облачная технология реализации применения ЭП

КРИПТО ПРО

Что мы от неё хотим?

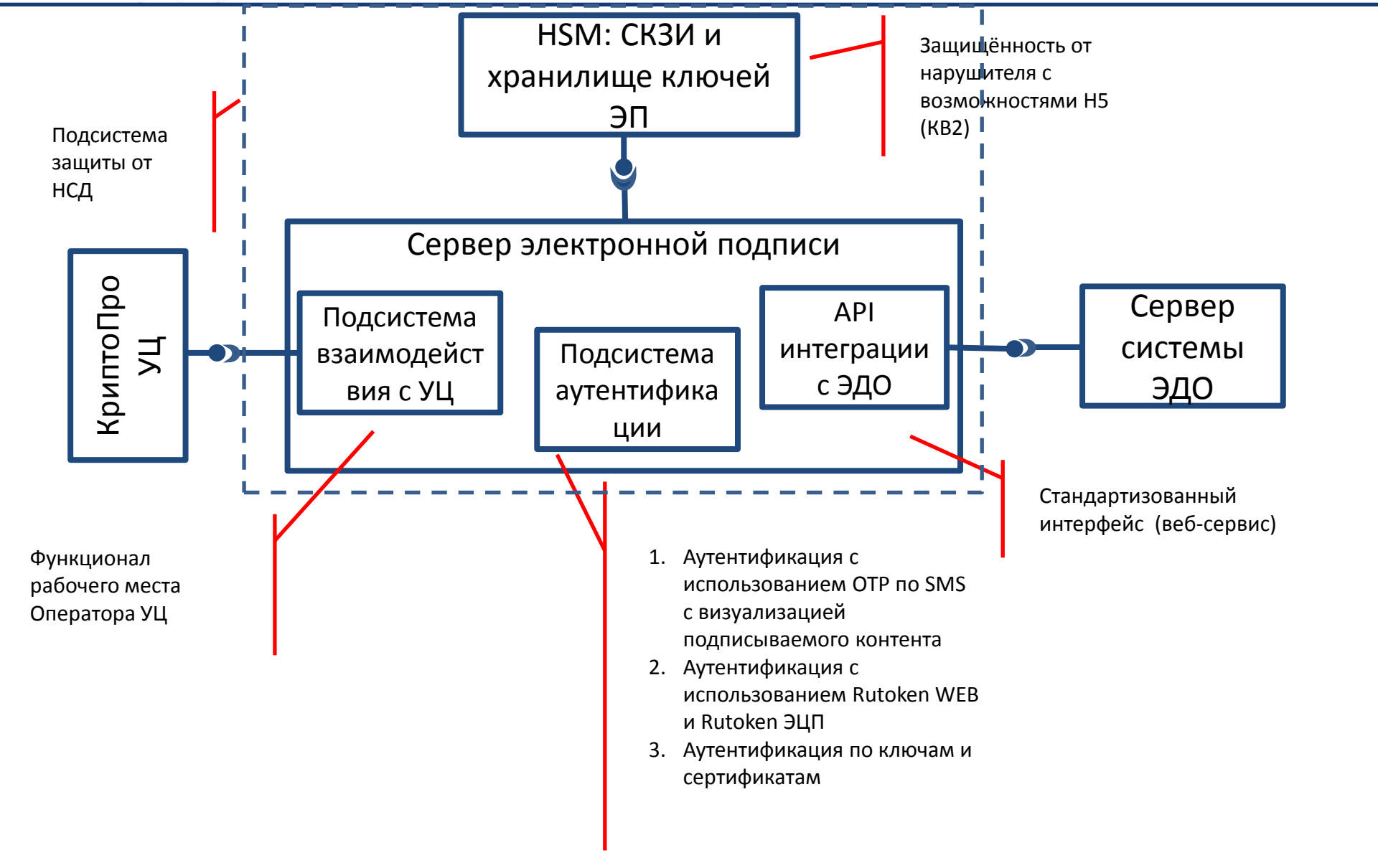
Исключить установку и использование средств ЭП на рабочем месте пользователя

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

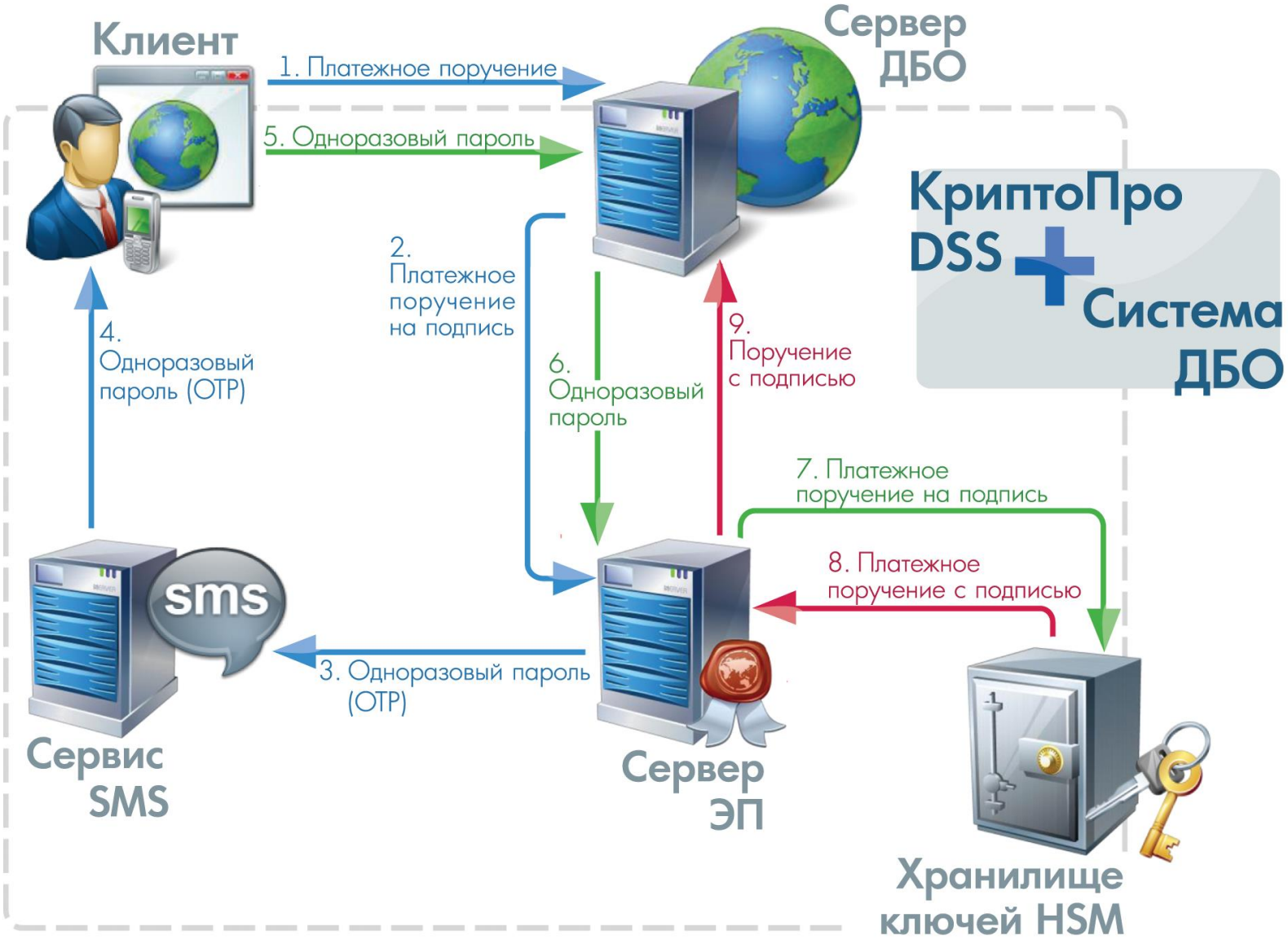
Исключить хранение ключа ЭП непосредственно у владельца

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

Структурная схема «КриптоПро DSS»



Пример подписания документа в ДБО с аутентификацией «OTP по SMS»



ПАКМ «КриптоПро HSM»

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-2344* от "*15*" *марта* 2014 г.

Действителен до "*15*" *марта* 2017 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» v. 1.0** в комплектации согласно формуляру ЖТЯИ.00046-01 30 01

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, требованиям ФСБ России к шифровальным (криптографическим) средствам класса КВ2 и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти, вычисление имитовставки для данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти, криптографическая аутентификация абонентов при установлении соединения, вычисление и проверка электронной подписи для данных, содержащихся в областях оперативной памяти) информации, не содержащей сведений, составляющих государственную тайну.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/121-2414* от "*17*" *июня* 2014 г.

Действителен до "*17*" *июня* 2017 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» v. 1.0** в комплектации согласно формуляру ЖТЯИ.00046-01 30 01

соответствует требованиям Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КВ2, и может использоваться для реализации функций электронной подписи (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Сервер ЭП «КриптоПро DSS»

Ключевые особенности

- Интеграция через API по HTTP и WS-Security с одной или несколькими СЭД
- Взаимодействие с одним или несколькими УЦ
- Электронная подпись и шифрование
- Форматы PKCS#7, XMLDSig, PDF, Office Signature
- Классический формат и усовершенствованный формат ЭП (CAdES)
- Возможность использования внешних Центров идентификации (SAML-токены)
- SDK для подключения способов аутентификации
- Возможность организации горячего резервирования
- Кластеризация на основе Windows Server
- Содержит подсистему проверки ЭП в документах (Сервер проверки ЭП)

Тренд № 2: Облачная технология сборки ЭП

КРИПТО ПРО

Производители браузеров отказываются от поддержки плагинов

- Google планирует в начале 2015 года убрать поддержку NPAPI из Chrome
- Internet Explorer в режиме планшета на Windows 8 и выше не поддерживает ActiveX
- в Firefox теперь необходимо сделать дополнительный щелчок мыши в окне с предупреждением, чтобы разрешить запуск плагина.
- набор API для вызова криптографических функций проходит стандартизацию в W3C (WebCrypto)
- Поддержка WebCrypto уже доступна в IE, Chrome и ведётся разработка в других браузерах
- в WebCrypto нет функций для создания форматов ЭП, только «голая» подпись

Тренд № 2: Облачная технология сборки ЭП

КРИПТО ПРО

Что мы от неё хотим?

Повысить функциональность средств применения ЭП

- Личное владение и использование ключа ЭП, но централизованное формирование ЭП
- Централизованная мультиформатность

Уменьшить количество устанавливаемого ПО на клиенте

- Массовый, неквалифицированный пользователь
- Уменьшение стоимость применения ЭП

Условное наименование: DSS Lite

предназначен для подписания документов электронной подписью в браузере с использованием средства ЭП, установленного на устройстве пользователя

позволяет отказаться от покупки и установки плагинов и дополнительных приложений для подписания различных форматов документов.

Форматы

Поддержка форматов подписи PKCS#7, Microsoft Office, PDF, XMLDSig, усовершенствованной подписи CAdES

Платформы

Поддержка разных платформ (Windows/Linux/Mac)

Веб-браузеры

Работает через любой веб-браузер

Интеграция с УЦ

Единая точка входа для подписания документов и управления своими сертификатами

Какие возможности дают облачные технологии применения ЭП?

Продавать ЭП как сервис

- Идентифицированные владельцы ЭП «привязаны» к оператору сервиса ЭП

Существенное уменьшение цены владения ЭП

- Исключается возможность компрометации ключей
- Не требуется установка и сопровождение средств применения ЭП на рабочих местах
- Не требуется лицензирование по ФСБ России

КРИПТО ПРО

СПАСИБО ЗА ВНИМАНИЕ!

Вопросы?

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru
info@cryptopro.ru

Тел./факс:
+7 (495) 995-48-20
+7 (495) 984-07-90