PKI-FORUM
РОССИЯ

Квалифицированная облачная подпись как услуга Удостоверяющего центра

Павел Смирнов
Станислав Смышляев
Сергей Ковтунов
Компания КриптоПро

КРИПТОПРО

О чем пойдёт речь

- Нормативное регулирование «облачной» подписи
  - В Европе
  - В России
- Проблемы распространения технологии
- Новые возможности использования «облачной» подписи
  - Для УЦ
  - Для пользователей

Европейское законодательство

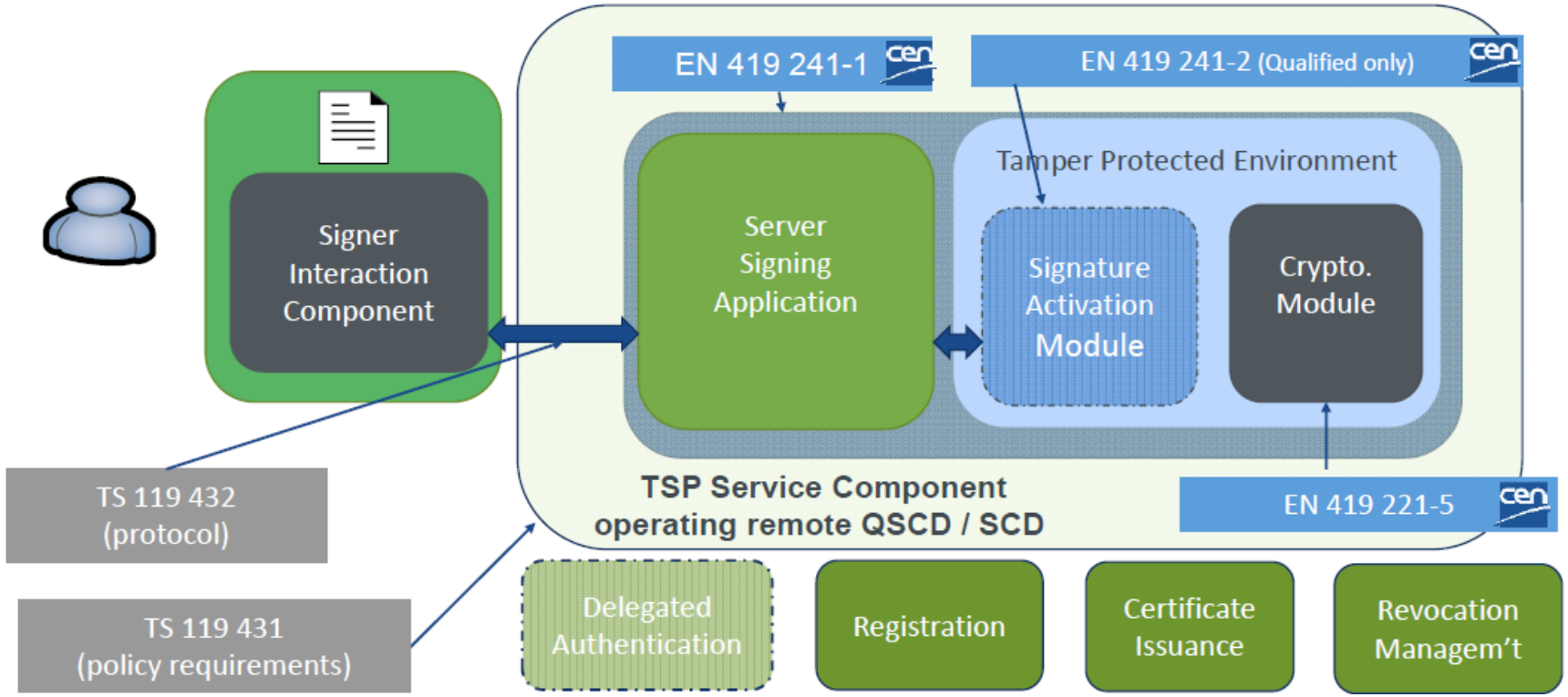
Директива 1999/93/EC

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

Постановление 910/2014 (eIDAS)

- Создание и использование ключей квалифицированной подписи можно доверить третьей стороне
- Сервер квалифицированной подписи должен управляться аккредитованным поставщиком услуг
- Нет отдельного вида поставщика услуг для «удалённой» подписи

Техническое регулирование



- 6 технических стандартов,
  все будут приняты в 2018 году

Российское законодательство

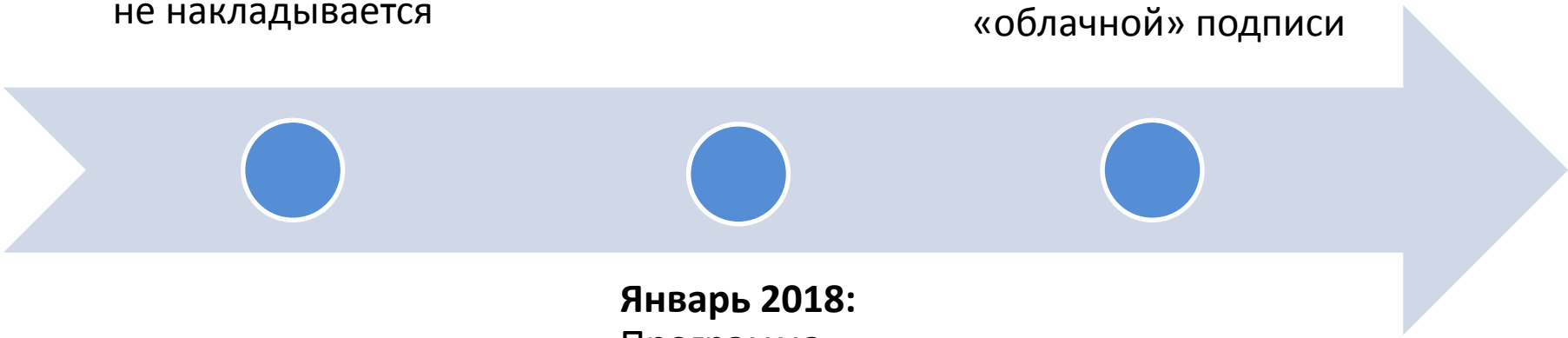
63-ФЗ «Об электронной подписи»

- ч.1 ст.10 разрешает использование ключа подписи с согласия владельца
- Финансовая ответственность не накладывается

Январь 2018:
Программа «Цифровая экономика», внесение изменений в 63-ФЗ

Сентябрь 2018:
Поправки АНО «Цифровая экономика»

- Повышенная финансовая ответственность для оператора средств квалифицированной «облачной» подписи



Дополнительные требования к средствам облачной ЭП в законопроекте

- Хранение ключей ЭП и автоматизированное создание такой подписи с их использованием по поручению владельцев
- Аутентификация владельцев сертификатов
- Защита информации, передаваемой между владельцем сертификата и УЦ
- Доказательство неотказуемости владельца сертификата от поручения на создание ЭП

Преимущества «облачной» подписи

- Возможно использовать на любых мобильных телефонах, планшетах и др. устройствах
- Доступность, как стоимостная, так и технологическая
- Снижение стоимости владения и развертывания инфраструктуры ЭП

Что мешало «облачной» подписи

- Отсутствие удобных сертифицированных средств «облачной» подписи
- Необходимость доработки информационных систем
- Юридические риски использования несертифицированных решений

Что изменилось 10 августа

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3480* от "*10*" *августа* 2018 г.

Действителен до "*10*" *августа* 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)** (исполнения «DSS + SIM (QES)», «DSS + SIM (M2M)») в комплектации согласно формуляру ЖТЯИ.00096-02 30 01

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

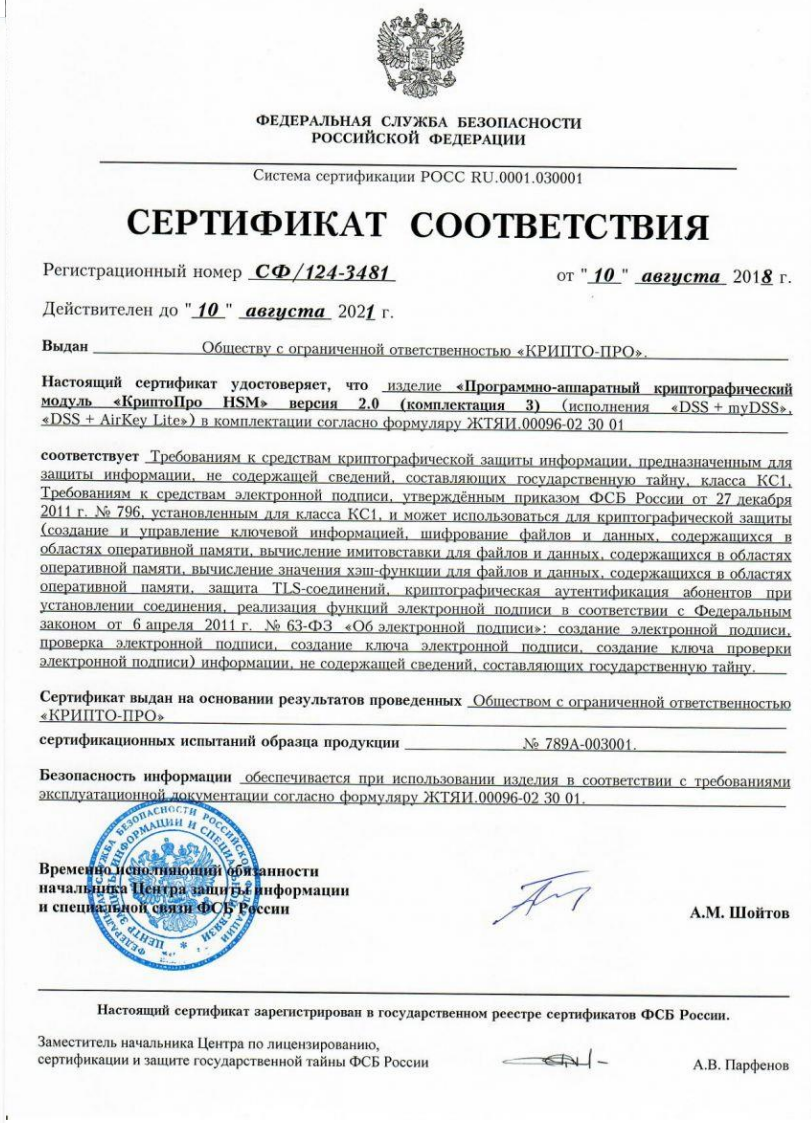
сертификационных испытаний образца продукции № 789А-003001.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЯИ.00096-02 30 01.

Временно исполняющий обязанности начальника Центра защиты информации и специальной связи ФСБ России А.М. Шойтов

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3481* от "*10*" *августа* 2018 г.

Действителен до "*10*" *августа* 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)** (исполнения «DSS + myDSS», «DSS + AirKey Lite») в комплектации согласно формуляру ЖТЯИ.00096-02 30 01

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-003001.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЯИ.00096-02 30 01.

Временно исполняющий обязанности начальника Центра защиты информации и специальной связи ФСБ России А.М. Шойтов

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

Что именно сертифицировано

КриптоПро DSS – программно-аппаратный комплекс, предназначенный для централизованного, защищенного хранения закрытых ключей пользователей, а также для удаленного выполнения операций по созданию электронной подписи (ЭП) с использованием ПАКМ «КриптоПро HSM».

КриптоПро myDSS – приложение для смартфона, которое обеспечивает строгую криптографическую аутентификацию пользователей, безопасное online-взаимодействие, отображение документа и подтверждение операций в порталах госуслуг, системах ЭДО, электронных торговых площадках и т.д.

КриптоПро Cloud CSP – криптопровайдер, обеспечивающий возможность использования ключей, хранящихся в КриптоПро DSS, через Microsoft CryptoAPI. Теперь ключи, хранимые в облаке, могут быть легко использованы классическими пользовательскими приложениями.

Почему это может быть интересно клиентам УЦ?

- Возможность подписывать документы **квалифицированной** электронной подписью даже на мобильном телефоне.
- В базовом варианте использования - нет необходимости настраивать рабочий компьютер и устанавливать на нем дополнительное ПО. Используйте электронную подпись отовсюду.
- При использовании КриптоПро Cloud CSP можно подписывать «облачной» подписью даже в информационных системах, которые не интегрированы с КриптоПро DSS.
- Число информационных систем и продуктов, которые умеют работать с «облачной» подписью напрямую, постоянно расширяется.

Почему это может быть интересно УЦ?

- Предоставление услуги подписания «облачной» подписью документов для клиентов.
  Доступный везде сервис - это конкурентное преимущество.
- Расширение аудитории клиентов за счет более низкой суммарной стоимости владения «облачной» ЭП по сравнению с обычной ЭП.
  Более низкая цена – конкурентное преимущество.
- Расширение аудитории клиентов за счет снижения образовательного «порога» клиентов.
  Простота использования – конкурентное преимущество.
- Дополнительные доходы от продажи ПО клиентам (КриптоПро myDSS и при необходимости – КриптоПро Cloud CSP) при снижении стоимости выпуска самой ЭП.

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru

spv@cryptopro.ru

svs@cryptopro.ru

kovtunov@cryptopro.ru

Тел./факс:

+7 (495) 995-48-20