КриптоПро DSS/myDSS. Реализация "облачной" электронной подписи на ПК и мобильных устройствах

Павел Луцик,
директор по продажам и развитию бизнеса
ООО «КРИПТО-ПРО»

О компании

КРИПТОПРО

- Почти 20 лет на рынке
- Лидеры разработки СКЗИ
- Реализовано множество PKI-проектов
- Продукты интегрированы во многие ИС
- Участвуем в разработке стандартов RFC
- Первое в России сертифицированное «облачное» решение (КриптоПро DSS)

SafeTech

- Компания-разработчик инновационных решений для защиты систем дистанционного банкинга и электронного документооборота.
- Широкий спектр предлагаемых средств аутентификации и подтверждения транзакций
- Совместная разработка с компанией КРИПТО-ПРО на базе программно-аппаратного комплекса «облачной» электронной подписи (ЭП) КриптоПро DSS и системы подтверждения электронных транзакций PayControl.

Тренды

- Все хотят в облака..
- Централизация администрирования
- Расширение перечня устройств для работы с ЭП
- Упрощение бизнес-процессов (учет СКЗИ, изменение требований к СКЗИ, переход на новые ГОСТы…)

Законодательство

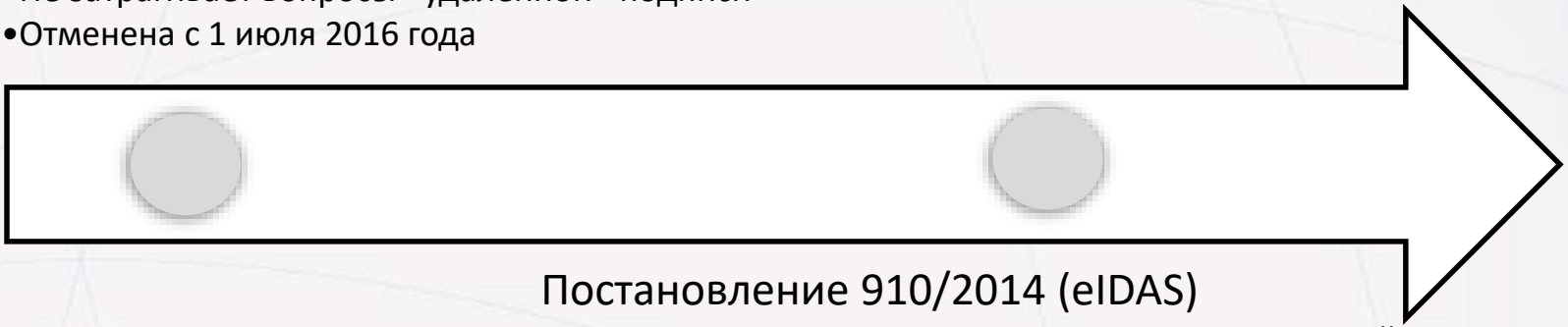
Нормативное регулирование «облачной» подписи

- В Европе
- В России

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

Технические стандарты:

- EN 419 241-1
- EN 419 241-2
- EN 419 241-5

- TS 119 431 (protocol)
- TS 119 432 (policy requirements)

Российское законодательство

КРИПТОПРО

- 63-ФЗ "Об электронной подписи"
- 683-П "Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента"
- 684-П "Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций"

Классическая и «облачная» ЭП. Особенности

КРИПТОПРО

Классическая ЭП

- Носитель закрытого ключа персональный (токен, смарт карта, реестр)
- Криптопровайдер – на рабочем месте пользователя
- Средство ЭП – на рабочем месте пользователя

«Облачная» ЭП

- Носитель закрытого ключа – централизованное защищенное хранилище + двухфакторная аутентификация
- Криптопровайдер – централизованный (HSM)
- Средство ЭП – централизованное (поддержка основных форматов подписи, возможность интеграции)

Преимущества «облачной» ЭП

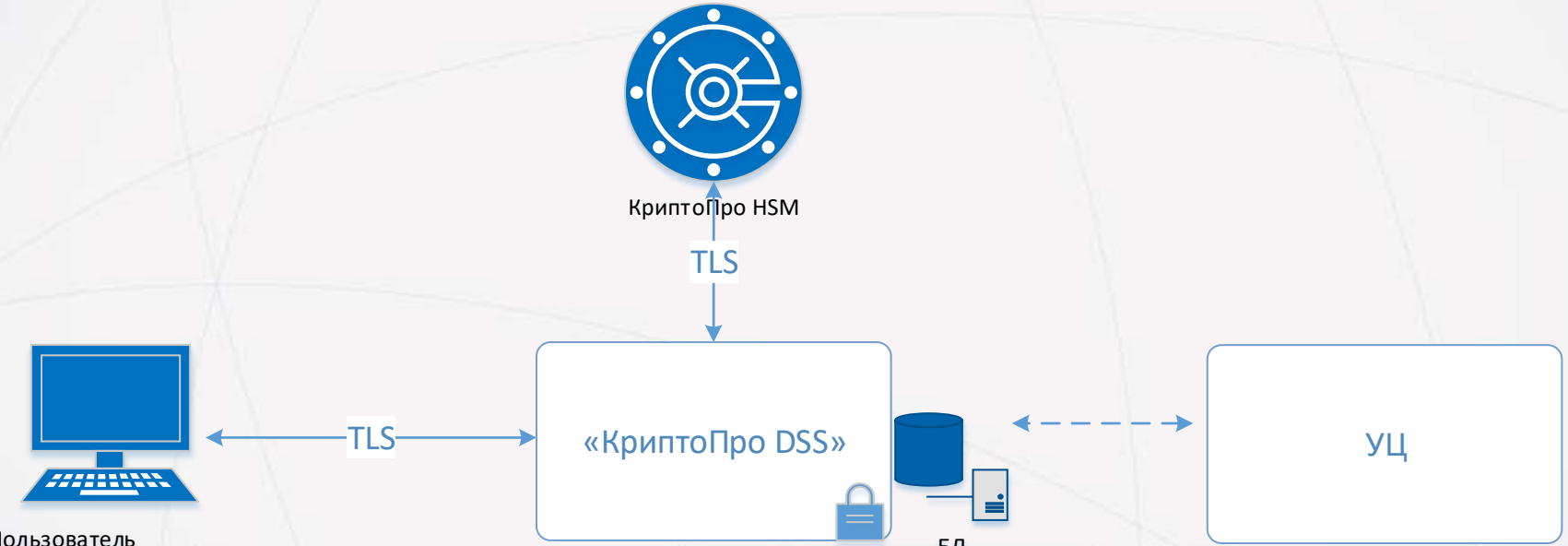
КРИПТОПРО

- Возможно использовать на любых мобильных телефонах, планшетах и др. устройствах, имеющих доступ в Интернет
- Снижение стоимости владения и развертывания инфраструктуры ЭП (экономия в разы)
- Доступность, как стоимостная, так и технологическая, т.к. не требует обучения для использования
- Простое встраивание функционала подписания и шифрования в существующие информационные системы
- Снижение риска компрометации ключей пользователей за счёт их централизованного защищённого хранения

Сервис «облачной» подписи ПАК «КриптоПро DSS»

- Централизованное защищенное хранение ключей
- Создание ЭП с использованием ПАКМ КриптоПро HSM

Схема взаимодействия с КриптоПро DSS



- Пользователь
- Оператор
- Информационная система

Безопасность ключей в облаке

Хранение ключей в КриптоПро HSM

- Неизвлекаемые ключи: доверенная генерация, хранение, использование и уничтожение.
- Датчики вскрытия, защита портов, доверенная замкнутая ОС.
- Защита от нарушителя среди администраторов: разделение ключа между администраторами, безопасные механизмы аудита.

Соответствие уровням защищенности

Российская система требований к СКЗИ/СЭП

- Работа с ключами пользователей – уровень КВ/КВ2.
- Управление пользователями и их аутентификацией – уровень КС3.
- Средства аутентификации – уровни КС1, КС2, КС3.

Требования Европейского комитета по стандартизации (CEN) к серверной подписи

- CEN/TS 419241, выполнены все требования высшего уровня (QES, уровень 2).

Сертификация

- КриптоПро DSS с КриптоПро HSM 2.0: в августе 2018 получены сертификаты на 11 исполнений
- В том числе, с компонентами аутентификации в виде мобильных приложений (iOS, Android) и апплета на SIM-карте

Безопасные механизмы аутентификации в КриптоПро DSS

«Сертифицированные» ФСБ России методы аутентификации

1. SSL-ГОСТ с использованием сертификатов X.509
2. SSL-ГОСТ с использованием логина и пароля
3. Криптоапплет на SIM-карте
4. Приложение myDSS для смартфона

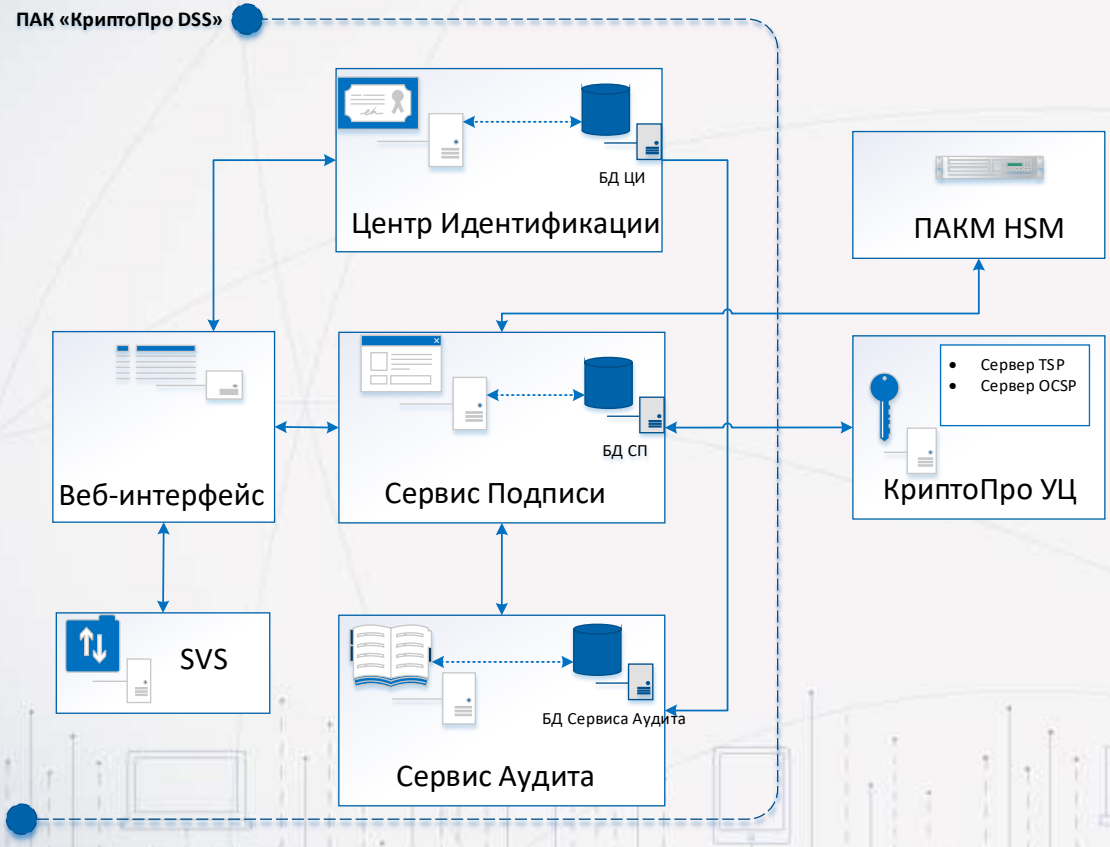
Квалифицированная ЭП

Иные методы аутентификации, реализованные в DSS

1. SSO
2. Генератор OTP (физический токен)
3. OTP-via-SMS
4. OTP-via-EMAIL

Неквалифицированная ЭП

Архитектура решения КриптоПро DSS



Состав КриптоПро DSS:

- ПАКМ «КриптоПро HSM»
- Сервис Подписи
- Центр Идентификации

- Веб-интерфейс Пользователя
- Сервис Аудита

Ключевые особенности DSS

- ✓ Реализует как функции создания/проверки электронной подписи так и шифрования/расшифрования электронных документов
- ✓ Поддерживает различные форматы электронной подписи
- ✓ Возможность дополнения ЭП до усовершенствованного формата
- ✓ Возможность создания нескольких экземпляров сервиса подписи и центров идентификации на одном сервере
- ✓ Возможность использования локальных закрытых ключей ЭП – режим DSS Lite

Ключевые особенности DSS

КРИПТОПРО

- ✓ API для интеграции (SOAP, REST и HTTP API)
- ✓ Отказоустойчивость и доступность
- ✓ Высокая производительность
- ✓ Применение NGate с DSS для повышения безопасности
- ✓ Мониторинг функционирования и доступности

КриптоПро CSP 5.0: Облачный провайдер

- Подписано заключение ФСБ России
- Добавлена поддержка платформы Android
- Работа с неизвлекаемыми ключами (ФКН)
- «Облачный» токен – технология Cloud CSP

ООО "КРИПТО-ПРО"

https://cryptopro.ru/products/csp_5_0

Бесшовный переход на «облачную» ЭП

Система электронного документооборота

Стандартизованный криптографический программный интерфейс (CryptoAPI)

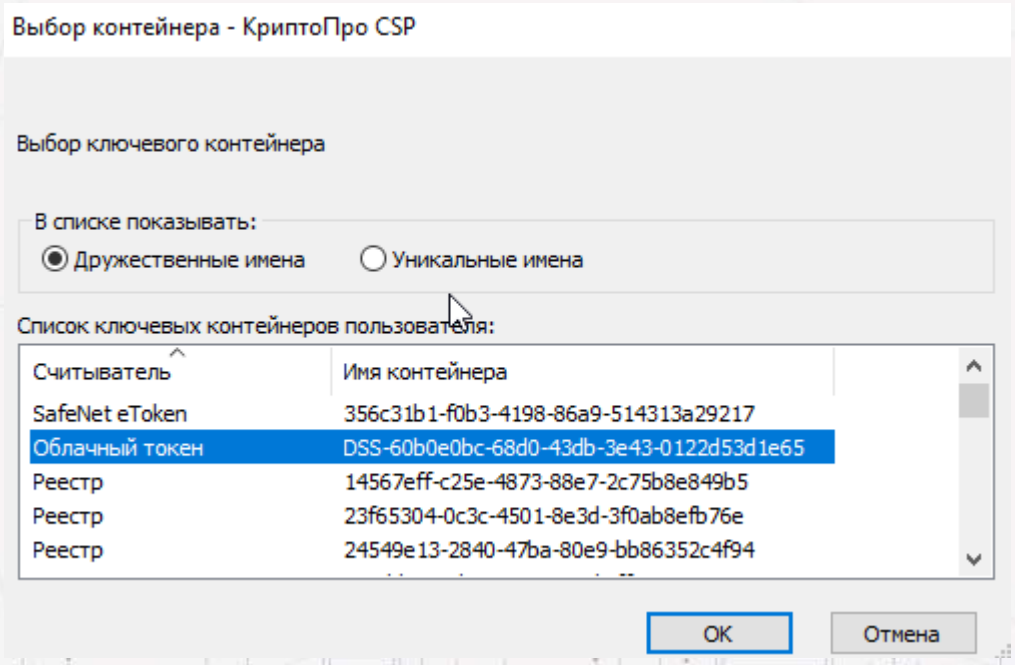
Уровень криптопровайдеров

«КриптоПро CSP»

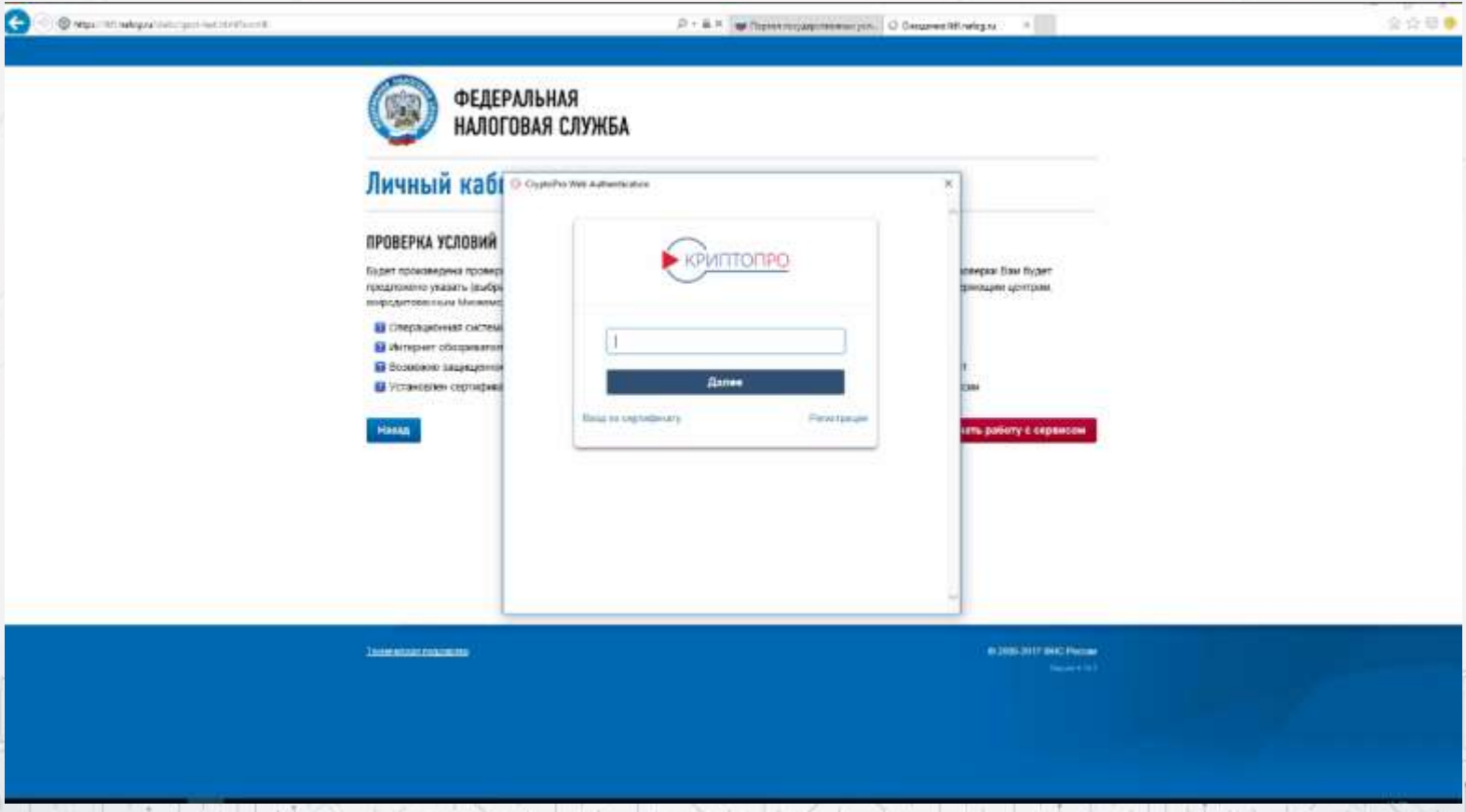
«КриптоПро Cloud CSP»

«КриптоПро DSS»

«Облачный» токен



Пример бесшовного перехода

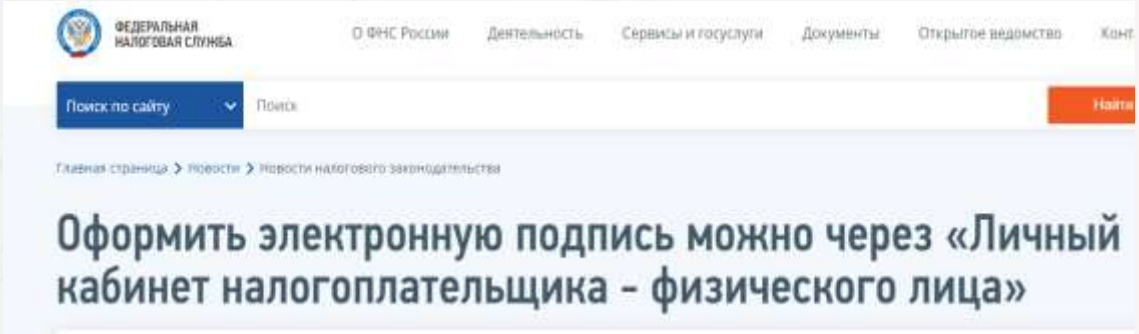


Примеры интеграции

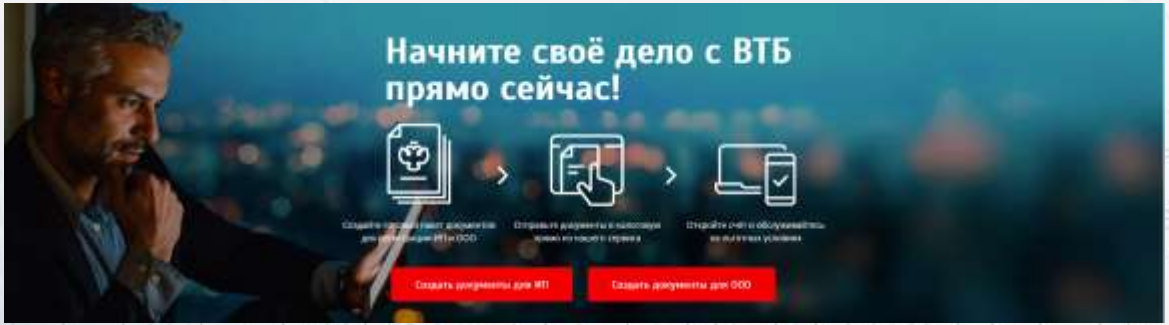
- ✓ Интеграция по протоколам SOAP, REST и HTTP API
- ✓ Подключение сторонних центров аутентификации по протоколам OAuth 2.0 и WS-Federation с поддержкой SAML 1.1/2.0.
- ✓ По стандартному CryptoAPI посредством дополнительного модуля CSP 5.0 (технология Cloud CSP)
- ✓ Создание и проверка электронной подписи в веб-интерфейсе DSS (альтернатива КриптоАРМ)

Опыт реализации интеграционных проектов

ФНС России



ВТБ



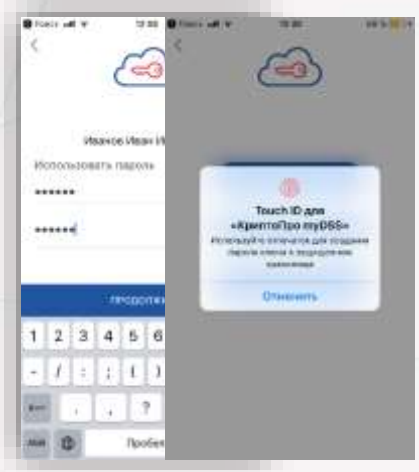
КриптоПро myDSS

Загрузите в App Store

ДОСТУПНО В Google Play

- ✓ Совместная разработка компаний КРИПТО-ПРО и SafeTech
- ✓ Технология PayControl
- ✓ Строгая аутентификация пользователей
- ✓ Безопасное online-взаимодействие
- ✓ Отображение документа
- ✓ Подтверждение операций с помощью функции HMAC_GOSTR3411_2012_256

КриптоПро myDSS. Инициализация



Интерфейс и шаги клиента:

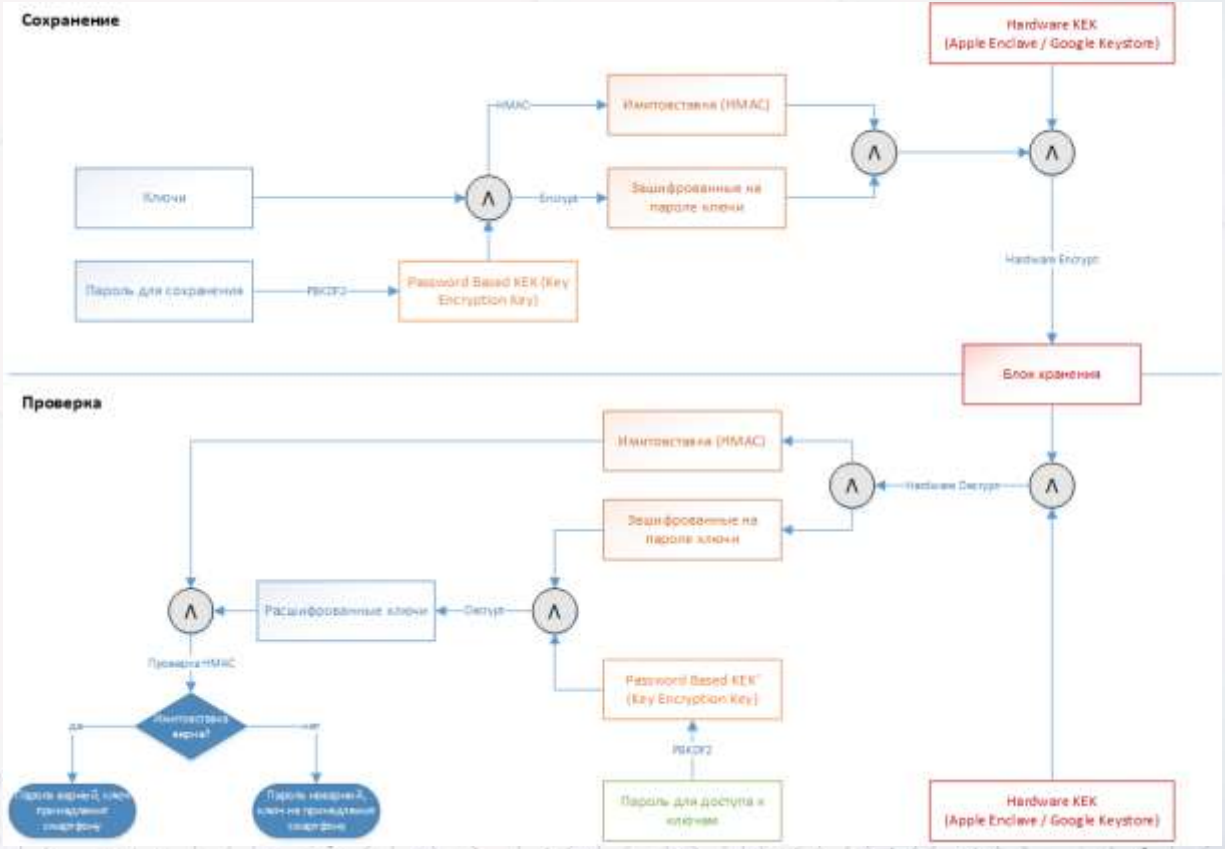
- Отсканировать QR-Код
- Получить SMS для активации
- Задать пароль/TouhID/FaceID для доступа к ключу
- Приложение инициализировано

Загрузите в App Store

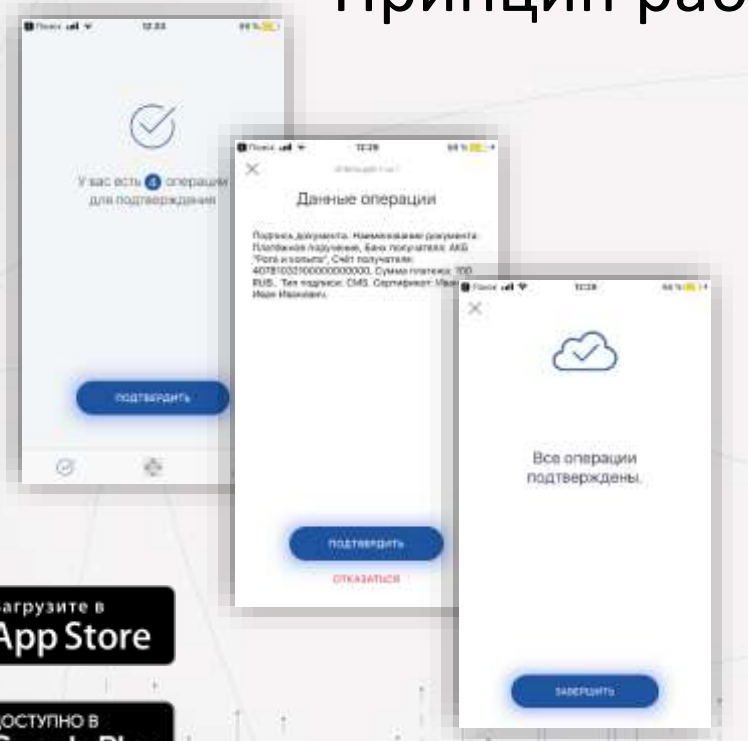
ДОСТУПНО В Google Play

myDSS. Хранение ключей

- Ключи хранятся в библиотеках SDK в зашифрованном виде
- Ключей шифрования ключей – два: производная от пароля и аппаратный ключ смартфона
- Вместо (или вместе) с паролем может использоваться Apple TouchID / Apple FaceID / Google Imprint



КриптоПро myDSS. Принцип работы



- Информация об операции приходит в Мобильное приложение myDSS
- Клиент нажимает «Подтвердить»
- Документ подтверждается ЭП

Загрузите в App Store

ДОСТУПНО В Google Play

myDSS. Проверки окружения

Привязка ключа к экземпляру аппарата

при персонализации приложения выполняется формирование «отпечатка» устройства, который в последующем используется при выработке HMAC.
в комбинации с привязкой ключей к аппаратному хранилищу (см. предыдущий слайд) делает невозможным использование ключей вне конкретного устройства

Обнаружение root/jailbreak

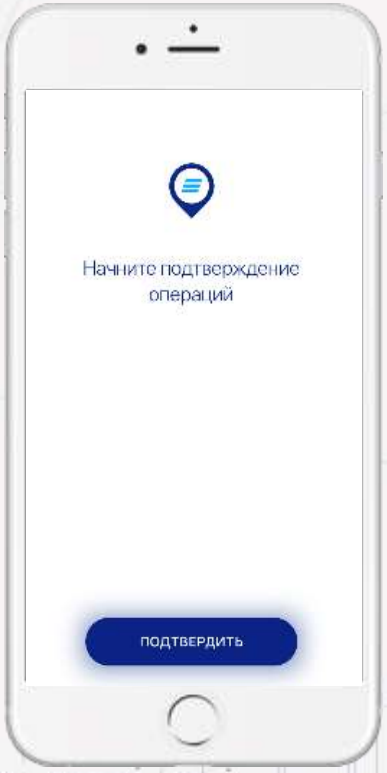
проверка на root 10-ю способами
проверка на jailbreak 3-мя способами

Обнаружение потенциально опасных приложений

обнаружение приложений, имеющих потенциально опасные разрешения – блокирует использование overlay-атак

Проверка, установлен ли антивирус

myDSS. Персонализация



myDSS в проме (видео 1)

myDSS в проме (видео 2)

ПАКМ «КриптоПро HSM»

Аппаратная платформа:

- ✓ Программно-аппаратный криптографический модуль "КриптоПро HSM" версии 2.0. Вариант исполнения 1

Сертификаты:

- ✓ Сертификат на модернизацию ПАКМ "КриптоПро HSM" до версии 2.0
- ✓ Сертификат технической (расширенной технической) поддержки ПО, входящего в состав ПАКМ "КриптоПро HSM" сроком на 1 (2, 3) года
- ✓ Сертификат сервисного (расширенного сервисного) обслуживания аппаратной платформы ПАКМ "КриптоПро HSM" сроком на 1 (2, 3) года

Лицензирование ПАК «КриптоПро DSS»

- ✓ Лицензия на право использования ПАК "КриптоПро DSS" версии 2.0 на одном сервере:
  - до 10 000 пользователей
  - до 20 000 пользователей
  - до 40 000 пользователей
  - до 50 000 пользователей
  - до 100 000 пользователей
  - > 100 000 пользователей по запросу info@cryptopro.ru

- ✓ Лицензия на расширение права использования ПАК "КриптоПро DSS" версии 2.0 на 10 000 пользователей

- ✓ Лицензия на право использования ПАК "КриптоПро DSS" версии 2.0 на одном дополнительном сервере

- ✓ Сертификат технической (расширенной технической) поддержки ПАК "КриптоПро DSS" на одном сервере сроком на 1 (2, 3) года

Лицензирование myDSS

От 100 пользователей

Бессрочные	Годовые

- Базовые
- На расширение

Планы на будущее

КРИПТОПРО

- myDSS SDK для Android/iOS, который можно встраивать в другие мобильные приложение в соответствии с «белым списком» функций API
- ГОСТ TLS
- Передача ключа в myDSS SDK по каналу связи с DSS

Материалы по DSS

- https://cryptopro.ru/products/dss/ - общее описание
- https://cryptopro.ru/products/mydss - КриптоПро myDSS
- https://cryptopro.ru/products/dss/downloads - загрузка ПАК «КриптоПро DSS»
- https://dss.cryptopro.ru/docs/articles/admin/quick_start.html - Быстрый старт
- https://dss.cryptopro.ru/textual.html - доступ к тестовому стенду
- https://dss.cryptopro.ru/docs/ - online-документация
- dss@cryptopro.ru - ящик для вопросов по DSS
- https://events.webinar.ru/13369733/2403347 - материалы вебинара
- https://cryptopro.ru/news/2019/06/statya-v-bloge-o-realizatsii-trebovanii-683-p-i-684-p-tsb-rf - статья в блоге о реализации требований 683-П и 684-П ЦБ РФ
- ИБ в Финсекторе, ИБ ЕБС:

https://t.me/FinSecurity , https://t.me/ibebs

https://www.facebook.com/groups/2384898694894659/, https://www.facebook.com/groups/1193170377507545

Спасибо за внимание !

Павел Луцик, КриптоПро
plutsik@cryptopro.ru
+7 (495) 995-48-20 (доб. 150)

Дарья Верестникова, SafeTech
D.verestnikova@safe-tech.ru