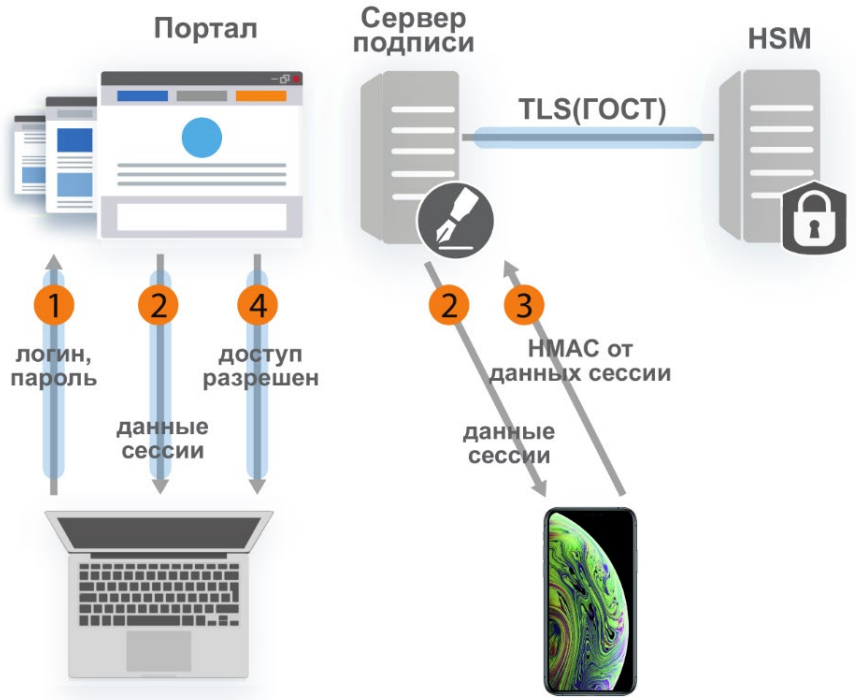
Дистанционное создание электронной подписи и стандартизация

Аристархов Иван Владимирович
Дробаденко Константин Валерьевич
Смышляев Станислав Витальевич

25 марта 2021 года

Идея «дистанционной подписи»

- Хранение ключей пользователей на серверной стороне, выполнение операций электронной подписи по аутентифицированным запросам владельцев.
- Потенциальные преимущества в части удобства:
  - Возможность доступа к своим ключам с нескольких устройств.
  - Высокая скорость подписания пакетов документов.
  - Возможность ограничить допустимое множество документов для подписи.
  - Возможность упростить порядок установки и распространения.
  - Повреждение/утеря устройства аутентификации не приводит к утере ключей.
  - В случае утери устройства доступ к ключам может блокироваться мгновенно.



Проблемы (до 2020 года)

- Только общие «Требования к средствам электронной подписи» – **отсутствие уточненных требований, в полной мере учитывающих особенности системы**.
- Отсутствие явных требований приводило к попыткам некоторых организаций строить «облачную» подпись без учета актуальных угроз.
  - Попытки строить средства «облачной» подписи без HSM на сервере.
  - Попытки строить средства «облачной» подписи с аутентификацией по паролю.
  - Попытки строить средства «облачной» подписи без TLS с ГОСТ.
- Как следствие, средства с HSM КВ2, полноценной ключевой аутентификацией, защитой канала, защитой от злонамеренных действий оператора **создавались и сертифицировались только с опорой на требования, определенные в отдельных ТЗ**.
- Невозможность строить единую инфраструктуру для работы с дистанционной подписью (работа разных систем ЭД с различными серверами дистанционной ЭП):
  - **Отсутствие единых требований по безопасности**, гарантирующих «равнопрочность» системы.
  - **Отсутствие системного подхода к инфраструктуре,** в том числе **стандартизированных протоколов взаимодействия решений различных производителей**.

Задачи

- Разработать единую модель инфраструктуры систем дистанционной подписи.
- Составить перечень функциональных требований к компонентам инфраструктуры.
- Оценить реальные угрозы для компонент инфраструктуры.
- Выработать требования по безопасности для каждой из компонент инфраструктуры.
- Определить актуальные задачи для стандартизации:
  - какие взаимодействия необходимо стандартизировать?
  - к каким взаимодействиям необходимо и достаточно выработать требования по безопасности?

476-ФЗ и дистанционная подпись

- Существенные изменения в 63-ФЗ «Об электронной подписи» :
  - **Статья 15, часть 2.2**: аккредитованным УЦ разрешается хранение и использование ключей ЭП для «дистанционной подписи» по поручению их владельцев (с 01.01.2021г.):
    - усиленные требования к аккредитации;
    - уточненные требования по безопасности.
  - Смежный вопрос: вводится возможность дистанционной идентификации (по действующему сертификату, через ЕСИА и ЕБС, по загранпаспорту нового поколения).

- До издания ФСБ России требований, предусмотренных пунктом 2.1 части 5 статьи 8 Федерального закона "Об электронной подписи", и до осуществления подтверждения соответствия изданным требованиям **никакие средства не могут применяться для реализации функций, предусмотренных частью 2.2 статьи 15 Федерального закона "Об электронной подписи"**.

Комплекс научных работ

- Цель: разработка научно-обоснованных методологических подходов к созданию **защищенных протоколов** взаимодействия компонентов **инфраструктуры дистанционного создания/проверки квалифицированной электронной подписи** и обмена электронными документами для решения задач Цифровой экономики

- Обзор существующих решений, в т.ч. средств с функционалом дистанционной ЭП.
- Требования к протоколам удаленной идентификации при выдаче сертификатов и инициализации работы с дистанционной подписью.
- Основные функциональные требования, важные для конечных пользователей.
- Общие классы требований к элементам инфраструктуры: соответствующие актуальным угрозам и выполнимые существующими решениями.
- Концепция взаимодействия компонентов разнородной инфраструктуры.

Функциональные требования (1)

На основе проведенного обзора существующих решений и практики их применения выделены следующие важные для практического использования функциональные требования:

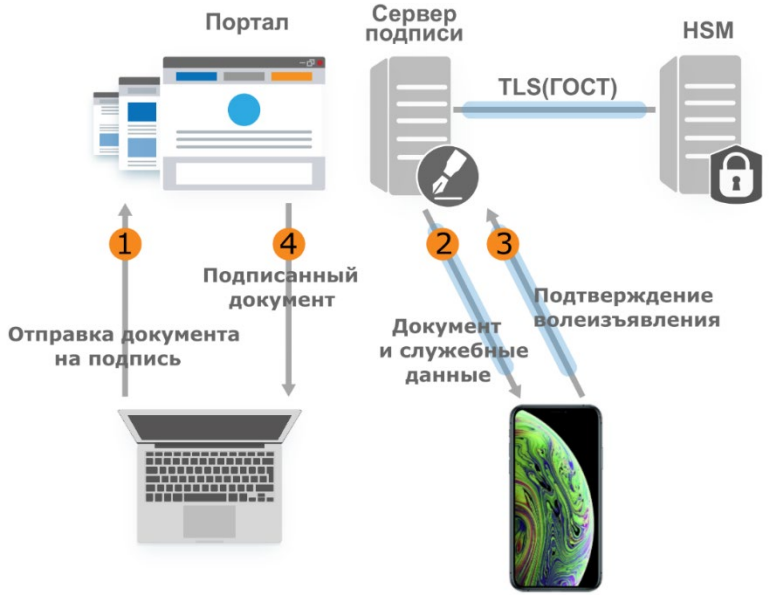
- Возможность работы с документами, обрабатываемыми системами электронного документооборота.
- Существование у оператора возможности мгновенной блокировки учетной записи в случае обращения ее владельца с заявлением об утере устройства с ключом аутентификации.
- Возможность организации контроля за использованием хранимых ключей ЭП.
- Возможность доступа к хранимым ключам подписи с нескольких устройств.

Функциональные требования (2)

- Возможность масштабирования (кластеризации) серверных компонент.
- Возможность по желанию владельца ключа ограничить на серверной стороне допустимое множество документов, поступающих ему на подпись.
- Отображение пользователю содержимого подписываемого документа.
- Возможность распространения пользовательских компонентов через сторонние магазины мобильных приложений
- Возможность дистанционной регистрации и учета экземпляров клиентских компонентов СКЗИ

Классы защиты: общие принципы

- У пользователя: мобильное приложение (КС1).
  - Угрозы использования опубликованных уязвимостей среды функционирования.
  - Использование уязвимостей в случае сбоев ДСЧ.
  - Угрозы на этапе доставки МП (распространение через магазины приложений).
- На сервере: ключи и ЭП в HSM КВ2, защита каналов с пользователем и с системами электронного документооборота по TLS с ГОСТ КС3.
  - Угрозы ключам пользователей в HSM (КВ/КВ2).
  - Возможен нарушитель среди администраторов (исключая сговор).
  - Угрозы искажения истории операций (нужен аудит с использованием HSM КВ2).
- Угрозы доступности сервисов мгновенной блокировки учетной записи.



Удаленная идентификация и OpenID Connect

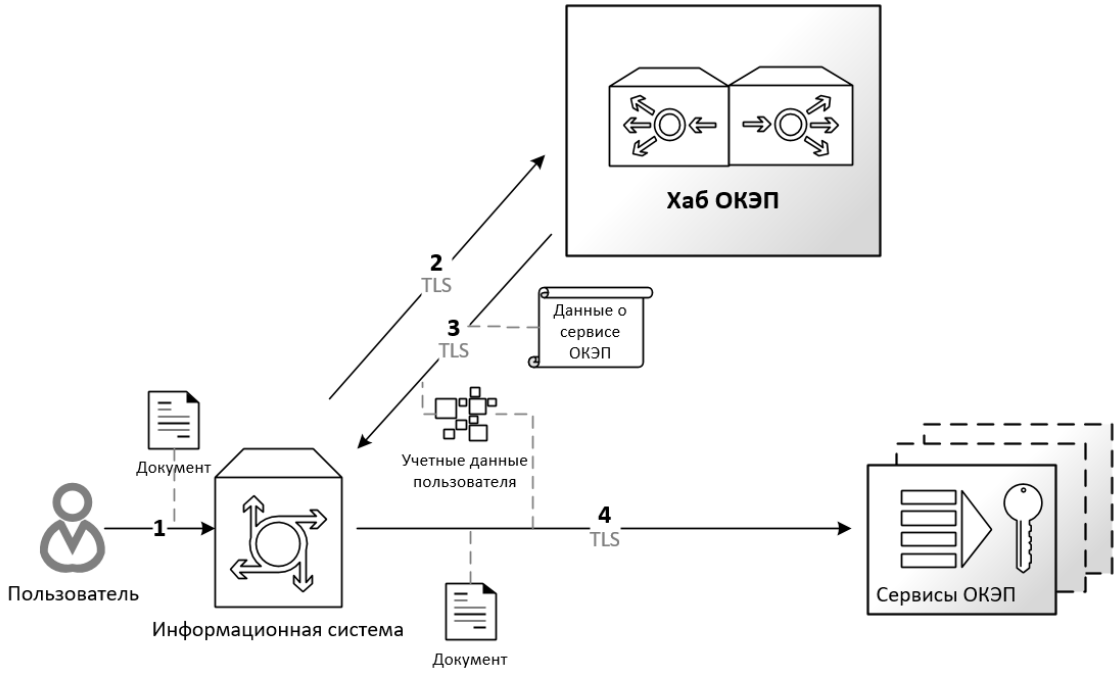
- Анализ протокольного семейства OpenID Connect, требования к его уточненной версии для использования совместно с удаленной идентификацией при выдаче сертификатов и инициализации работы с дистанционной подписью.
- Стандартизация в ТК 26 для части применений (с учетом использования в банковском секторе) – уже в процессе. В план работ ТК 26 включена разработка Технической спецификации «Использование российских криптографических алгоритмов в протоколах OpenID Connect».
- По итогам: задачи по расширению и уточнению множества представителей протокольного семейства OpenID Connect.

Инфраструктура в целом. Хабы.

- Исходные данные: пользователь – система электронного документооборота – сервис подписи (в АУЦ); много пользователей, много СЭД, много сервисов подписи.
- Задача: обеспечить в инфраструктуре дистанционной и мобильной подписи возможность работы нескольких сервисов подписи аккредитованных УЦ так, чтобы пользователь, инициировавший подписание документа из любой внешней системы электронного документооборота, мог безопасно совершить требуемую операцию при нахождении его ключа в любом сервисе.
- Предлагаемое решение: хаб электронной подписи – система, предоставляющая информацию о сервисе подписи, в котором находится ключ ЭП пользователя, с целью дальнейшего подключения к нужному сервису для создания ЭП документов с использованием прямой аутентификации пользователя.

Концепция «хабов»

- Поиск сведений о сервисе подписи, в котором находится ключ ЭП пользователя, по идентификатору пользователя.
- Запрос сведений о сервисе подписи, в котором находится ключ ЭП пользователя, от другого хаба при необходимости.
- Регистрация сервисов подписи в хабе.
- Регистрация ИС в хабе.
- Регистрация существующих и новых пользователей сервисов ОКЭП в хабе.



Задачи стандартизации

- Создание единой инфраструктуры дистанционной подписи, связывающей различные системы документооборота и различные средства дистанционной подписи (возможное решение: концепция хабов), стандартизация протоколов.
- Требования по информационной безопасности:
  - учитывающие актуальные угрозы;
  - позволяющие сохранить основные преимущества технологии;
  - допускающие эволюционное развитие решений различными путями для частных функциональных требований (взаимодействие клиентских и серверных компонент внутри каждого решения не обязательно стандартизировать).
- Две идеологии подписи с использованием мобильных устройств:
  - Ключ/компонента ключа на устройстве пользователя.
  - На устройстве только ключ аутентификации.

  – у каждой есть свои преимущества (и функциональные, и по безопасности). Целесообразно развивать обе.
- Требования к обеспечению безопасности в процессе дистанционной регистрации пользователей, учитывающие актуальные угрозы и одновременно позволяющие сохранить основные преимущества технологии, стандартизация протоколов.

Спасибо за внимание!