Применение квалифицированной электронной подписи: теория, практические проблемы и пути их решения

Смышляев Станислав Витальевич,
заместитель генерального директора КриптоПро

КРИПТОПРО

Развитие электронного документооборота.
Тренды. Регулирование. Практика.
Форум ЭДО – 2021

ЭП: дьявол в деталях

- Взгляд со стороны лаборатории, проводящей оценки влияния («контроль встраивания») для средств электронной подписи при встраивании в ИС и ППО.
  - Как встраивать средства ЭП, знают все.
  - Как встраивать средства ЭП правильно, не знает почти никто.

- Если применимы формулировки из ПКЗ-2005/п. 1.5 Формуляра («Если информация конфиденциального характера подлежит защите в соответствии с законодательством …»), требуется оценка влияния («контроль встраивания»).

- Даже если не применимы, основные принципы при встраивании полезно соблюдать, а расхождения между формулировками и техникой понимать.

ЭП: дьявол в деталях

- В случаях, «определяемых п. 1.5 Формуляра» (определенных в ПКЗ-2005) требуется оценка влияния на СКЗИ.

- Встраивание допустимо только по «белому списку» функций (их использование не требует полных тематических исследований нового СКЗИ).

- В него входят, в частности, операции:
  - Сформировать/проверить ЭП (любого формата) под документом (**не по хэшу**!) после отображения документа.
  - Вычислить зашифрованное CMS-сообщение в адрес сертификата получателя.
- Не входят, в частности, операции:
  - Проверить ЭП по открытому ключу (ключу проверки ЭП), без сертификата.
  - Вручную вызвать функции симметричного шифрования/расшифрования.
  - Подписать хэш документа (т.е. **нужно пересылать документ целиком, отображать**).

Автоматическое формирование ЭП

- В соответствии с требованиями ФСБ России и требованиями эксплуатационной документации необходимо обеспечивать доверенную визуализацию каждого документа перед подписанием.
- Проблема: большие пакеты документов.
- Различная трактовка понятия «работа средства ЭП в автоматическом режиме»:
  - «Может подписывать всё, что ему поступает на вход».
  - «Переподписывает те документы, что раньше были подписаны другой ЭП».

Пути решения:

- В рамках исследований системы в целом – обеспечение единого процесса работы с документами, так чтобы поступление документов на подписание могло происходить в системе исключительно от аутентифицированных сотрудников по защищенным каналам, ранее подтвердившим операцию.
- Доверенная визуализация документов по выбору пользователей, а не «принудительно».

Прикладное ПО и средства ЭП

- В случаях, «определяемых п. 1.5 Формуляра» (определенных в ПКЗ-2005) требуется оценка влияния на СКЗИ.

- По итогам оценки влияния прикладное ПО/ИС фиксируется – дальнейшие эволюционные изменения и улучшения системы существенно усложнены.

– требуется проработка вопроса об упрощенном порядке внесения изменений в системы, для которых проведена оценка влияния на СКЗИ.

Пути решения:

- Дальнейшее повышение логического уровня интерфейсов СКЗИ под конкретные задачи.

- Совмещение процедур оценки влияния измененного ПО с DevOps.

Терминальный доступ, NFC

- Проблема: доступ к ключу по незащищенному каналу (NFC, удаленный терминальный доступ).
- Аутентификация к ключу по ключу – спорное решение.
- Голый/неаутентифицированный канал – и формальное нарушение, и практическая угроза, даже по КС1.

Путь решения:

- Применение средств, поддерживающих Р 50.1.115–2016. Применение в современных токенах, электронных паспортах (УЛГ/ПЭН).

СЭП класса «выше КС1»

- Средства ЭП класс КС2 требуют использования электронных замков, а класса КС3 – специальных ОС либо пакетов безопасности для ОС.
- Виртуальные машины, мобильные устройства – в общем случае, **только КС1**.
- Следствие: в существующую ИС встроить средство ЭП класса КС2 и выше сложнее.

Путь решения:

- Выделение самодостаточных компонент, предоставляющих высокоуровневые интерфейсы (не «вычислить ЭП», а «полностью провести весь протокол взаимодействия»), построение на необходимых аппаратных и программных компонентах.

Распространение программных СЭП

- Требования поэкземплярного учета и доверенного распространения СЭП входят в противоречие с практикой загрузки ПО через Интернет – актуально для КС1.

Пути решения:

- сервера регистрации и учета экземпляров СКЗИ.
- специальные методы контроля целостности при скачивании на базе ЭП.
- доверенное распространение по каналам связи в случае поддержки TLS с ГОСТ.

Проблема смены долговременных ключей

- Проблема: вручную не всегда возможно, автоматически при шифровании «нового на старом» неизбежна угроза неявной компрометации.
- Принцип для PKI: подпись нового запроса на сертификат на старом ключе.
  - В случае компрометации старого ключа защита от «пассивного нарушителя» есть.
  - Но может на компрометированном старом ключе успеть подписать запрос на новый сертификат, порождая параллельно работающую легитимную цепочку ключей.

Пути решения:

- IETF, РГ LAMPS: фиксировать хэш от будущего открытого ключа в сертификате «старого».
- На серверной стороне контролировать появление новых ключей, после подписи нового запроса на старом ключе «блокировать» подпись запросов на нем в будущем.

Дистанционное получение сертификатов

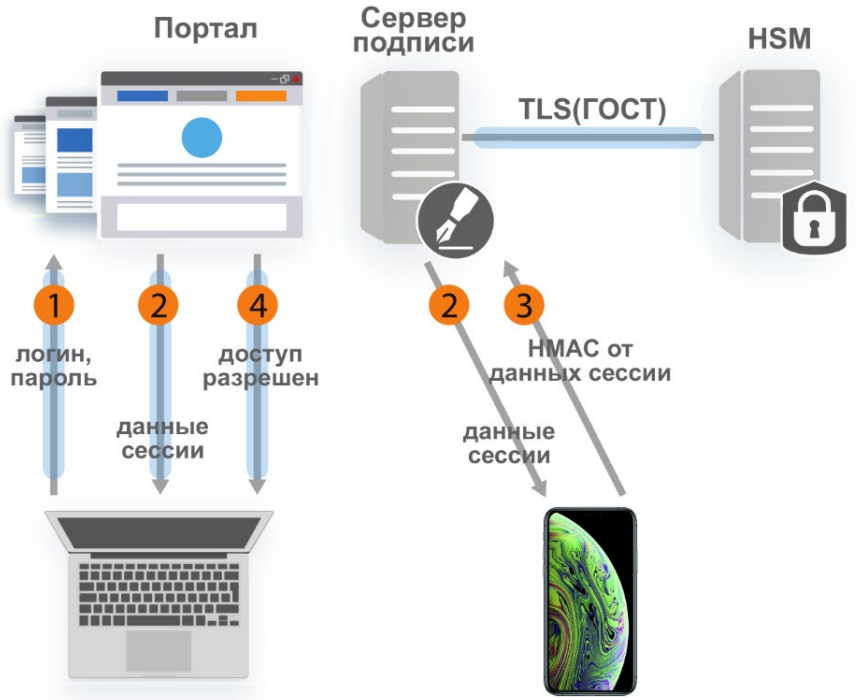
- В соответствии с положениями 476-ФЗ: 4 способа идентификации.
- Фактически полностью готов к применению: 2 способа идентификации (личная явка и действующие ключи УКЭП).

Пути решения:

- Для загранпаспортов: предоставление удостоверяющим центрам сервиса проверки ПВДНП.
- Для ЕСИА+ЕБС: переиспользование типовых решений для ЕБС, созданных для банков.

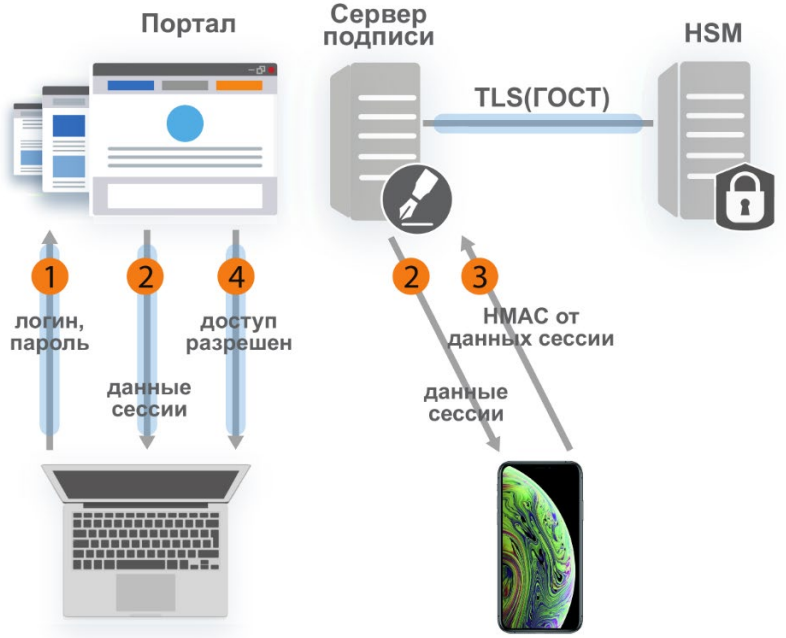
Идея «дистанционной подписи»

- 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.



Дистанционная электронная подпись

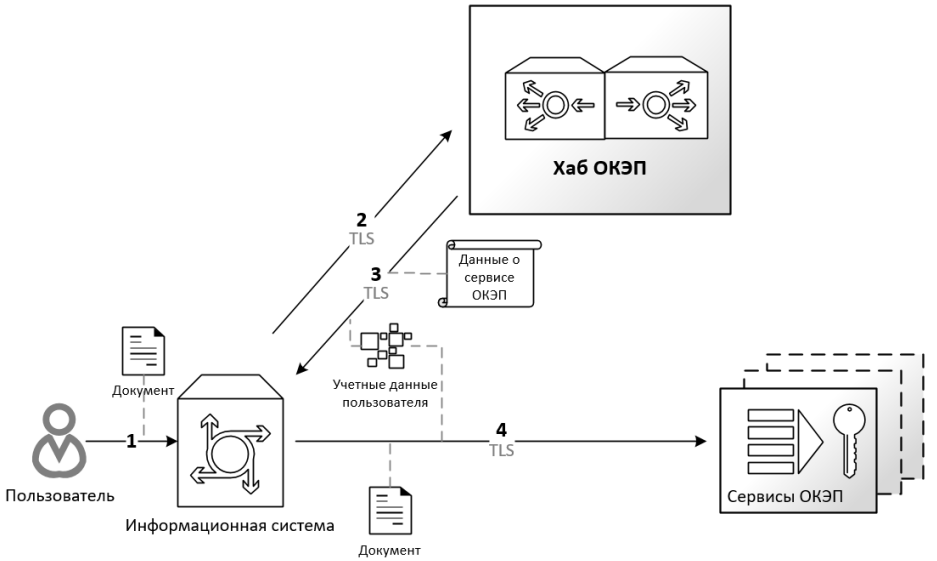
- Изменения в 63-ФЗ «Об электронной подписи» :
  - Статья 15, часть 2.2: аккредитованным УЦ разрешается хранение и использование ключей ЭП для «дистанционной подписи» по поручению их владельцев.



- Пока не опубликованы Требования ФСБ России, предусмотренные пунктом 2.1 части 5 статьи 8 Федерального закона "Об электронной подписи».
- Реализация функций, явно предусмотренных частью 2.2 статьи 15 Федерального закона "Об электронной подписи», должна осуществляться средствами после подтверждения соответствия этим требованиям.
- Сейчас: средства, сертифицированные по общим требованиям к средствам ЭП.

Работа с дистанционной ЭП в случае множественных СЭД и серверов ЭП

- 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.
- Путь решения: 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.



Нормативная база и технические реализации

- Взгляд со стороны разработчика средств ЭП и средств УЦ: изменения нормативной базы не всегда возможно отразить в технических решениях.
  - Перенос запрета на формирование ЭП по ГОСТ Р 34.10-2001 с 31.12.2018 г. на 31.12.2019 г. – необходимость экстренно пересертифицировать и массово обновлять СЭП на местах.
  - Оформить запрет на использование после той или иной даты можно отзывом сертификатов (приведет к прекращению и проверки тоже) или техническими ограничениями.
  - «Продление» действия ключей УКЭП на 3 месяца летом 2020 – конфликт со строгими ограничениями на срок действия ключей и на выпуск двух сертификатов на один ключ проверки ЭП.
  - «Квалифицированные сертификаты, выданные аккредитованными до дня вступления в силу настоящего ФЗ закона УЦ, действуют […] не более чем до 1 января 2022 года» – нет исключений для сертификатов TSP и долговременного хранения документов.

Нормативная база и технические реализации

- Взгляд со стороны разработчика средств ЭП и средств УЦ: изменения нормативной базы не всегда возможно отразить в технических решениях.
  - Требования RFC могут противоречить нормативной базе. Пример с сертификатами OCSP- и TSP-серверов: кто по 476-ФЗ выдает сертификат для OCSP-/TSP-сервера?
  - МЧД: описания вида МЧД не будет достаточно для переработки логики всех прикладных систем с целью при проверке ЭП дополнительно проверять МЧД.
    - Жизненный цикл МЧД: технически и технологически вопрос никак пока не решен, нет спецификаций. Пример: действия при смене ключа юр. лица.
    - Логика и реализация логики проверки МЧД: допроектирование, доработка + досертификация систем.

Спасибо за внимание!