Сравнение подходов к электронной подписи с использованием мобильных приложений в свете развития Единой биометрической системы

Смышляев Станислав Витальевич, к.ф.-м.н.,
заместитель генерального директора

Смирнов Павел Владимирович, к.т.н.,
руководитель департамента разработки

PKI-Форум Россия 2019

Переход на мобильные устройства для работы с ЭП

Перенос средств работы с электронной подписью в условия мобильного использования

- Актуальность задачи в комментариях не нуждается.
- Другие практически важные модели нарушителя.
- Изменение порядка работы с ключами.
- Ограничения мобильных устройств (МУ).
- Мобильное приложение на МУ: самодостаточное СЭП или часть клиент-серверного решения.
- Хранение ключей на МУ, сопрягаемых с ним носителях или централизованным образом в HSM (“облачная” подпись).

Получение сертификатов без личной явки

Перспективы удаленной идентификации и аутентификации при получении (квалифицированного?) сертификата

- посредством ЕБС (с помощью мобильного приложения)
- посредством использования удостоверения личности гражданина (через NFC на МУ?)

— обсуждение использования криптографии на мобильных устройствах необходимо вести с учетом возможности поддержки схем получения сертификатов без личной явки.

Существующие подходы

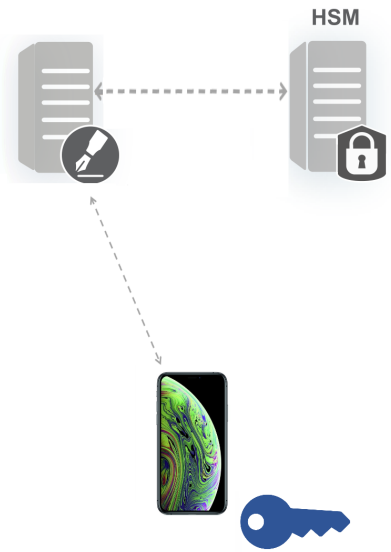
Три технологии

- Локальная подпись на МУ (напр., КриптоПро CSP 5.0 и КриптоАРМ).
- Локальная подпись на МУ с „облачной“ защитой ключей (IDpoint, КриптоПро CSP 5.0 при использовании шифрованных ключевых контейнеров).
- Удаленное формирование подписи („облачная“ подпись): аутентифицированное волеизъявление хранимым на устройстве ключом аутентификации (КриптоПро DSS + myDSS).

Локальная подпись на МУ

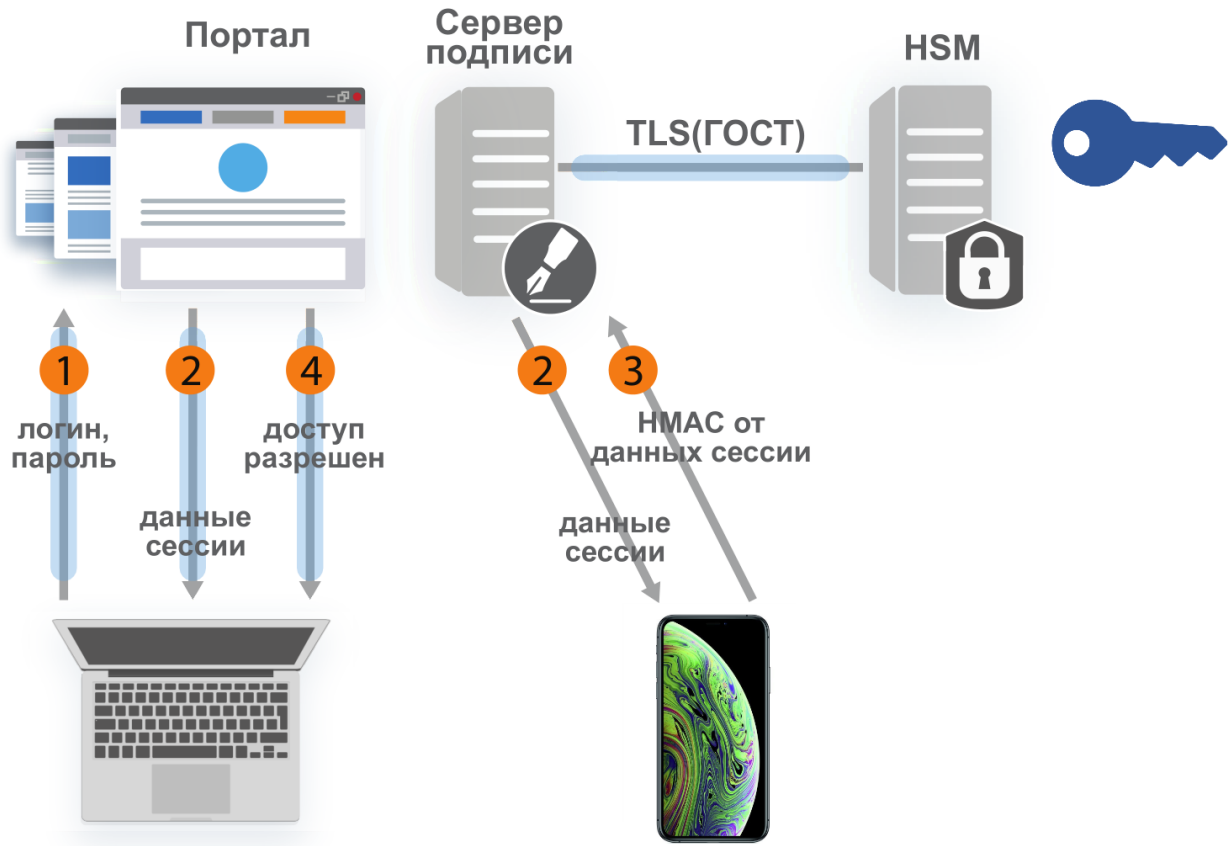
- Хранение ключа в памяти устройства или на совместимом с МУ ключевом носителе.

Локальная подпись на МУ с „облачной“ защитой ключей

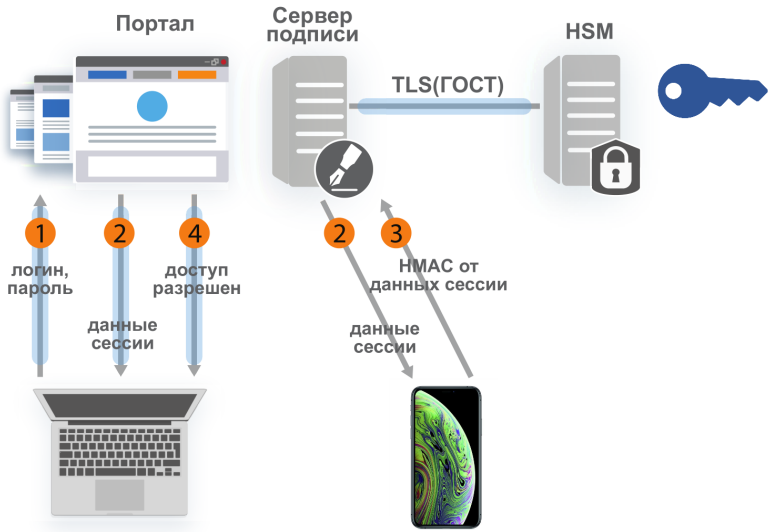


- Хранение ключа в памяти устройства в зашифрованном виде, хранение ключа шифрования ключа — на сервере.
- Для выполнения операций требуется доступ к серверу.

Удаленное формирование подписи



Удаленное формирование подписи



- Единое решение: серверная и клиентская компоненты.
- Серверная компонента — защищенное хранение ключей в неизвлекаемом виде, реализация операций по аутентифицированным запросам от клиентских компонент.
- Клиентская компонента — визуализация, аутентификация и подтверждение операций, защищенный канал.

По каким свойствам следует сравнивать?

Безопасность

- обеспечение безопасности работы с ключами:
  - создание
  - хранение и использование
  - плановая/внеплановая смена
  - блокировка доступа в случае утери устройства
- криптографическая стойкость итоговых систем в случае личного/удаленного получения сертификатов
- доверенный аудит

Общие свойства

- удобство
- производительность
- масштабируемость
- возможность бесшовного перехода

Сравнение подходов

Сценарии удаленной выдачи сертификатов с помощью ЕБС

- Локальная подпись на МУ: TLS-соединение, идентификация и аутентификация посредством ЕБС.
- Локальная подпись на МУ с „облачной“ защитой ключей: аналогично, с дополнительным обращением к серверной стороне при формировании запроса на сертификат.
- Удаленное формирование подписи: аналогично с более широкими возможностями по противодействию мошенническим действиям благодаря аудиту всех операций в HSM класса КВ.

Доклад с PKI-форума 2018

Удаленное получение сертификатов может быть поддержано в схеме удаленного формирования подписи с сохранением уровня стойкости при совершении операций — без понижения безопасности.

Блокировка ключей при утере устройства

- Локальная подпись на МУ: только с помощью отзыва сертификата.
- Локальная подпись на МУ с „облачной“ защитой ключей: мгновенная блокировка доступа к ключу на серверной стороне.
- Удаленное формирование подписи: мгновенная блокировка доступа к ключу на серверной стороне.

Аудит

- Локальная подпись на МУ: на практике — невозможен.
- Локальная подпись на МУ с „облачной“ защитой ключей: журналы на серверной стороне позволяют определить время операций.
- Удаленное формирование подписи: максимально подробный аудит на серверной стороне с защитой журналов в HSM класса КВ с помощью цепной записи данных.

Последствия повреждения устройства

- Локальная подпись на МУ: потеря ключей.
- Локальная подпись на МУ с „облачной“ защитой ключей: потеря ключей.
- Удаленное формирование подписи: потеря доступа к ключам, восстанавливается при личной явке.

Производительность при пакетном подписании данных

- Локальная подпись на МУ: ограничена ресурсами МУ.
- Локальная подпись на МУ с „облачной“ защитой ключей: ограничена ресурсами МУ (плюс однократная задержка до начала операций).
- Удаленное формирование подписи: высокопроизводительные кластеризуемые аппаратные решения на стороне сервера — более высокая скорость подписания пакетов документов.

Работа с внешними порталами при плохом соединении

- Локальная подпись на МУ: трудности обработки больших документов и пакетов документов.
- Локальная подпись на МУ с „облачной“ защитой ключей: трудности обработки больших документов и пакетов документов.
- Удаленное формирование подписи: возможность для конкретных видов данных определять оптимизированные сценарии просмотра и подтверждения операций.

Общие последствия однократного сбоя ДСЧ

- По зашифрованному https/TLS/IPsec-трафику можно восстановить открытый текст.
- По значению ЭП можно восстановить ключ подписи.

Последствия сбоя ДСЧ

- Локальная подпись на МУ: риск компрометации ключа ЭП.
- Локальная подпись на МУ с „облачной“ защитой ключей: риск компрометации ключа ЭП (эквивалентный).
- Удаленное формирование подписи: риски компрометации ключа ЭП отсутствуют, но может быть нарушена конфиденциальность самих данных.

Перевод существующих прикладных систем

- Локальная подпись на МУ: переход требует разработки дополнительных модулей.
- Локальная подпись на МУ с „облачной“ защитой ключей: переход требует разработки дополнительных модулей.
- Удаленное формирование подписи: благодаря функционалу Cloud CSP в сертифицированном КриптоПро CSP 5.0 возможен бесшовный переход любых ранее написанных прикладных систем.

Задача

Возможно ли бесшовно перевести существующие системы на работу через МУ с ключами на бесконтактных токенах, УЛГ, социальных картах?

Перевод существующих прикладных систем

- Локальная подпись на МУ: переход требует разработки дополнительных модулей.
- Локальная подпись на МУ с „облачной“ защитой ключей: переход требует разработки дополнительных модулей.
- Удаленное формирование подписи: благодаря функционалу Cloud CSP в сертифицированном КриптоПро CSP 5.0 возможен бесшовный переход любых ранее написанных прикладных систем.

Задача

Возможно ли бесшовно перевести существующие системы на работу через МУ с ключами на бесконтактных токенах, УЛГ, социальных картах?

CRYPTOPRO

1. Существующие подходы
2. Сравнение подходов
3. Синтез четвертого решения
4. Заключение

Синтез четвертого решения

Предпосылки

- Удобные и безопасные сценарии для использования токенов, работающих по NFC или Bluetooth (“бесконтактных”), с МУ?
- Формирование подписываемых документов непосредственно на телефоне в ряде случаев неудобно — уместнее использовать телефон для аутентифицированного подтверждения.
- Существующие процессы работы с ЭП: системы документооборота и прикладное ПО, в которые 19 лет встраивается CSP; новые системы, интегрированные с DSS.
- Полезно требовать второй фактор, чтобы нивелировать сопутствующие бесконтактной работе опасности.

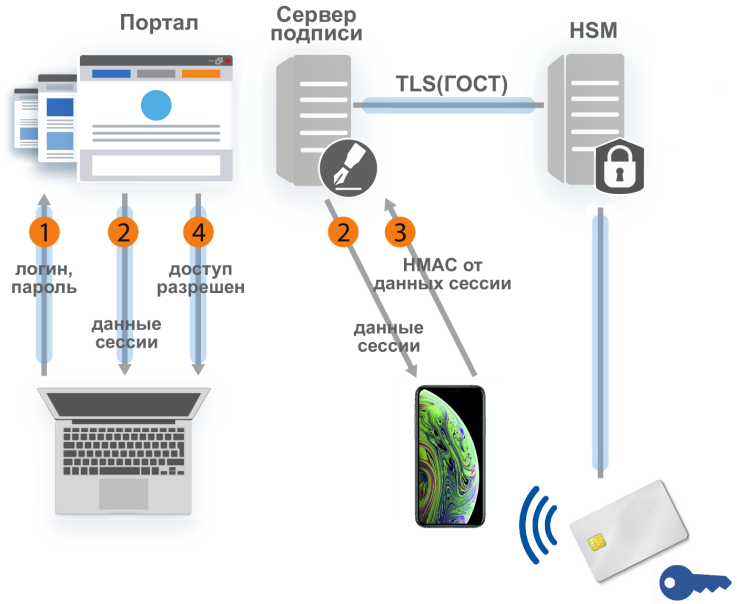
Описание схемы

Идея

- Переиспользовать всё уже сделанное в DSS для безопасной работы с документами: интеграция, доверенная визуализация, управление ключами, аудит.
- Поддержать безопасную работу с ключами, хранимыми не на HSM самого DSS, а на токене пользователя, насквозь пробрасывая к нему защищенный канал через аутентифицированное МУ и используя МУ как считыватель.

Перспективная схема: бесшовный переход на использование бесконтактных ключевых носителей

Перспективная схема: бесшовный переход на использование бесконтактных ключевых носителей



- Работа по схеме DSS, но для работы с ключами обращение идет не в HSM, а по защищенному каналу на бесконтактный токен.

Решение (общая схема взаимодействия):

- Пользователь первично аутентифицируется на DSS.
- Засылает любым поддерживаемым образом (в том числе, через CryptoAPI/Cloud CSP) документ на подпись.
- Ему на МУ (ранее инициализированное) прилетает уведомление о новом документе.
  - Устанавливается односторонний TLS между телефоном и DSS.
  - Аутентификация телефона внутри этого TLS перед сервером с помощью HMAC-ключа (как в myDSS).
  - Сервер внутри установленного TLS направляет пользователю документ, тот его подтверждает ключом HMAC, чем подтверждает серверу, что «готов подписывать».
- Предложение приложить бесконтактный токен к МУ.
- Токен с DSS устанавливают защищенное соединение, SESPAKE.
- Внутри защищенного соединения и TLS DSS направляет на токен хэш, формирование подписи ключом на токене.
- DSS возвращает подпись в исходное приложение.

Преимущества

- Полностью бесшовно поддерживаем всё уже работающее с CSP (в режиме Cloud CSP), без переработок прикладного ПО.
- Полноценное безопасное использование ключей на токенах.
- Полный аудит всего благодаря DSS и HSM.
- Возможность мгновенной блокировки в случае утери МУ/токена.
- Три фактора: сам токен, HMAC-ключ на телефоне, логин-пароль для самого начала взаимодействия, плюс еще и пин-код/отпечаток пальца для входа в myDSS.
- Не надо трогать чип/карту.
- Сохраняется возможность накладывать ограничения по подписываемым файлам (могут контролироваться на сервере).

Серверная компонента служит:

- для связи системы/компьютера с Cloud CSP с МУ;
- для обеспечения аутентификации сторон взаимодействия;
- для оперативной блокировки в случае утери МУ/токена;
- для доверенного аудита.

Использование HSM KB/KB2

- Хранение в неизвлекаемом виде мастер-ключей и порождения пользовательских ключей аутентификации.
- Хранение ключей серверных компонент при построении защищенных каналов связи.
- Хранение ключей доверенного аудита, предназначенных только для построения подписанных журналов аудита, построенных по принципу цепной записи данных.

Требуемые компоненты

Все “кирпичи” готовы

- CSP 5.0 (с поддержкой iOS и Android)
- Модули SESPAKE в CSP 5.0
- Модуль Cloud CSP
- КриптоПро HSM 2.0 и КриптоПро DSS
- Бесконтактные токены, в том числе Рутокен ЭЦП 2.0 (Bluetooth, NFC), УЛГ (NFC), социальные карты

— можно строить все варианты из рассмотренных.

Требуемые компоненты

... и по отдельности сертифицированы

- CSP 5.0 (с поддержкой iOS и Android) — сертификаты СФ/114-3726, СФ/124-3727, СФ/124-3728
- КриптоПро HSM 2.0 и КриптоПро DSS — сертификаты СФ/124-3475, СФ/124-3481
- Рутокен ЭЦП 2.0 — сертификаты СФ/124-3499, СФ/124-3475, СФ/124-3673
- УЛГ — следим за новостями

Выводы

- Рассмотрены четыре схемы работы с ЭП на МУ.
- Для каждой из схем возможно совмещение с удаленным получением сертификатов с использованием ЕБС.
- Схемы, предполагающие локальное хранение ключа, имеют ряд недостатков, мешающих широкому внедрению.
- Сертифицированные КриптоПро DSS и CSP 5.0 позволяют бесшовно перейти на использование МУ в существующих системах по схеме удаленного формирования подписи.
- Описан четвертый подход, позволяющий удобно использовать бесконтактные токены, УЛГ и социальные карты, с бесшовным переходом на них.

CRYPTOPRO

Спасибо за внимание!

Вопросы?

- Материалы, вопросы, комментарии:
  svs@cryptopro.ru
  spv@cryptopro.ru

Удаленное формирование подписи

Преимущества: удобство

- Повреждение устройства аутентификации (телефона с SIM-картой со специальным апплетом, смартфона с мобильным приложением, токена доступа) не приводит к утере ключей — только к временной утере доступа к ним.
- Средство аутентификации налагает существенно меньшее количество требований к окружению, чем средство ЭП, что позволяет упростить порядок установки и распространения, расширить перечень устройств.
- Пользователь имеет возможность доступа к своим ключам ЭП с нескольких устройств, что удобно для «мобильных» сотрудников и для руководителей высшего звена.
- Высокопроизводительные кластеризуемые аппаратные решения на стороне сервера — высокая скорость подписания пакетов документов.

Удаленное формирование подписи

Преимущества: безопасность

- Повреждение/утеря устройства аутентификации не приводит к утере ключей ЭП, в случае утери доступ к ключам блокируется мгновенно на серверной стороне.
- Журнал аудита на сервере при нештатной ситуации позволяет установить, был ли несанкционированный доступ к ключу подписи.
- Возможность прямого взаимодействия серверных компонент средства подписи с ИС позволяет по желанию владельца ключа ограничить допустимое множество документов, поступающих ему на подпись.

Преимущества „облачной“ подписи в части безопасности

- Возможность мгновенной блокировки ключа.
- Максимально доверенный аудит.
- Возможность ограничить сферу применения ключа.

$\Rightarrow$ защищенность пользователя повышается, что особенно важно в случае легитимного способа получения сертификата с помощью биометрической идентификации.

Дополнительно усилить безопасность

- Выдачу новых аутентификаторов на ключ — только с использованием уже существующих аутентификаторов.
- При выдаче нового аутентификатора на существующий ключ извещать владельца с помощью доступных каналов взаимодействия.

СКПЭП, выданные без личной явки, снабжать соответствующими идентификаторами, а в ИС принимать с учетом моделей угроз.

OpenID Connect в версии ЕСИА/ЕБС позволяет передавать степень схожести — в случае получения СКПЭП повысить требования к ней.

При дистанционном получении сертификата уведомить владельца с использованием доступных (по информации в ЕСИА) каналов связи, а сертификат выдавать с задержкой.

Удаленное получение сертификата при локальном хранении (обычном и с „облачной“ защитой ключей)

1. Пользователь с помощью сертифицированного средства ЭП создает ключ ЭП на своем носителе и запрос на сертификат.
2. Пользователь обращается в УЦ, аутентифицируется и авторизуется через ЕСИА/ЕБС, после чего пересылает по созданному защищенному каналу запрос на сертификат в УЦ.
3. УЦ выпускает квалифицированный сертификат на данного пользователя, передает его пользователю.
4. Пользователь использует свое средство ЭП и сертификат обычным образом.

Удаленное получение сертификата в случае удаленной работы с ЭП

1. Пользователь по защищенному каналу с односторонней аутентификацией обращается к серверу „облачной“ подписи, запрашивает генерацию нового ключа с получением аутентификатора к нему, а также запроса на сертификат.
2. Пользователь обращается в УЦ, аутентифицируется и авторизуется через ЕСИА/ЕБС, после чего пересылает по созданному защищенному каналу запрос на сертификат в УЦ.
3. УЦ выпускает квалифицированный сертификат на данного пользователя, передает его пользователю.
4. Пользователь пересылает полученный сертификат на сервер.
5. Пользователь использует свой ключ в средстве ЭП обычным образом с помощью своего аутентификатора.

Использование HSM КВ/КВ2

Общий подход к защите серверной стороны

В системах, в которых возникает “централизация” доверия с доступностью систем из Интернета, требуется обеспечивать повышенную защиту серверных ключей. Примеры: OCSP/TSP-сервера (см. условия подключения ПАК “Службы УЦ” 2.0 к Интернет), ГУЦ, компоненты ЕБС — всюду HSM КВ/КВ2.