Реализация «облачной подписи» с учетом выполнения требований Постановления Правительства РФ №1104 от 29 октября 2016 года

Смышляев Станислав Витальевич, к.ф.-м.н.,
начальник отдела защиты информации

Смирнов Павел Владимирович, к.т.н.,
зам. начальника отдела разработок

Постановление Правительства РФ №1104 от 29 октября 2016 г.

О проведении в 2016–2018 годах эксперимента в целях обеспечения направления электронных документов для государственной регистрации юридических лиц и индивидуальных предпринимателей и открытия им счетов в кредитных организациях с использованием специализированной защищенной автоматизированной системы, предназначенной для централизованного создания и хранения ключей усиленной квалифицированной электронной подписи, а также их дистанционного применения владельцами квалифицированных сертификатов ключа проверки электронной подписи.

Требования к дистанционному использованию ключей УКЭП

Требования предъявляются к:

1. хранению ключей;
2. порядку аутентификации субъектов;
3. порядку защиты информации при передаче по каналу;
4. к подтверждению волеизъявления владельца ключа;
5. к средствам и порядку автоматизированного создания подписи.

Вопросы

Соответствие требованиям ФСБ ⇒ криптография по ГОСТ.

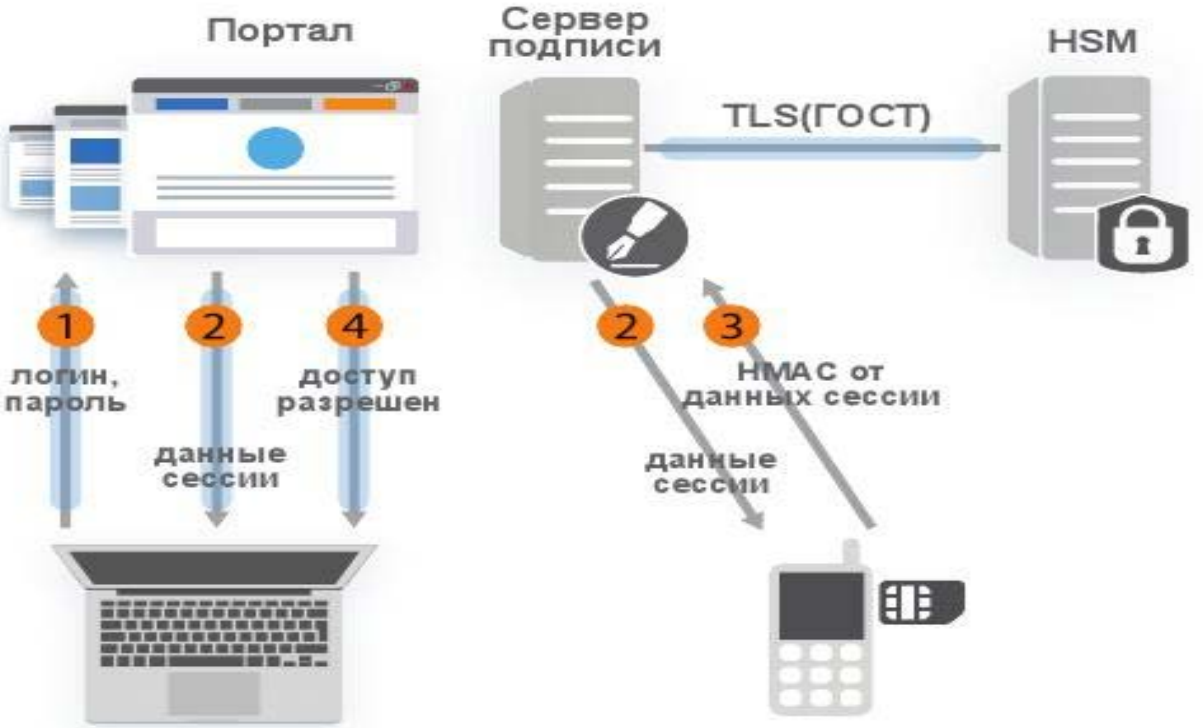
Работа с любого места — как аутентифицироваться?

- Не ключевой носитель — иначе сводится на нет ряд преимуществ дистанционной подписи.
- Пароля не хватит — по требованиям Постановления.
- Смартфон/планшет?
- SIM-карта на телефоне?

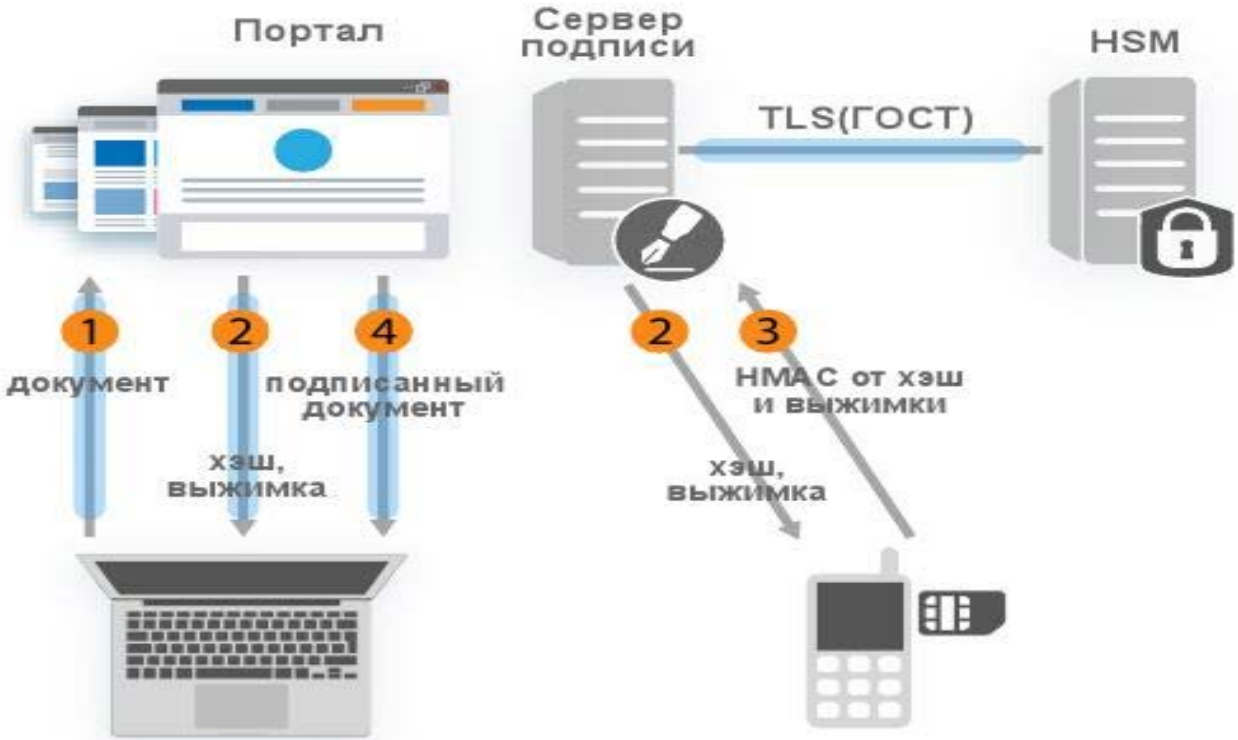
Задачи аутентификации владельца подписи и аутентификации запроса на формирование подписи

- выделяются независимым образом,
- требуют различных механизмов/ключей.

Аутентификация на сервере



Подтверждение волеизъявления операций



1. Требование к хранению ключей

Использование сертифицированного ПАКМ (HSM), обеспечивающего доверенную генерацию, хранение, использование и уничтожение ключей.

2. Требование к порядку аутентификации субъекта

В случае использования с подключением к общедоступным сетям:

- Первичная идентификация.
- Ключ аутентификации на мобильном устройстве/SIM-карте.

3. Требование к защите информации в канале

Использование стандартизированного TLS с алгоритмами ГОСТ в сертифицированном СКЗИ.

4. Требование к подтверждению волеизъявления владельца

Подтверждение волеизъявления на основе вычисления кода аутентификации операции с использованием ключа HMAC на мобильном устройстве/SIM-карте.

5. Требование к средствам и порядку автоматизированного создания подписи

Использование соответствующих требованиям ФСБ России средств автоматизированного создания электронной подписи на стороне сервера.

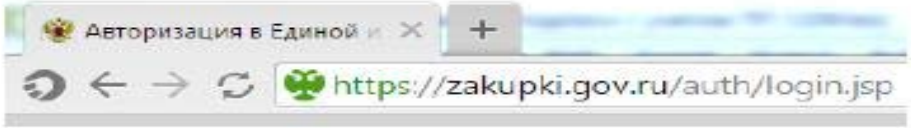
Обеспечить удобный для пользователей софт для TLS с ГОСТ

Поручение Президента РФ Пр 1380 (п.1) от 16 июля 2016 года

«...разработку и реализацию комплекса мероприятий, необходимых для поэтапного перехода федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, государственных внебюджетных фондов, органов местного самоуправления на использование российских криптографических алгоритмов и средств шифрования в рамках исполнения полномочий при электронном взаимодействии между собой, с гражданами и организациями.»

TLS: клиентская часть

- CSP для поддержки TLS в Internet Explorer.
- Браузер «Спутник» — поддержка TLS с ГОСТ.



- Встраивание CSP в приложения банков.

TLS: серверная часть

- Требуется высокопроизводительный TLS-шлюз с ГОСТ (КриптоПро NGate).

Хранение ключей, формирование подписи и аутентификация

- КриптоПро HSM для хранения ключей.
- КриптоПро DSS для предоставления интерфейсов.
- КриптоПро DSS — поддержка аутентификации (первичной и волеизъявления) с использованием ключей HMAC на мобильном устройстве/SIM-карте.

Если использовать SIM, почему не хранить на ней сам ключ и не отказаться от дистанционной подписи?

Хранимые на SIM ключи	Ключ электронной подписи	Ключи аутентификации для облачной подписи
Время операции (без сопроцессора)	2-3 мин.	2 сек.
Необходимость сервера ЭП	Требуется (визуализация)	Требуется
Рабочее место с TLS по ГОСТ	Требуется	Требуется
Создание и смена ключей УКЭП	При личном присутствии, запись на SIM контактно с сертифицированного АРМ	Дистанционно пользователем с использованием ключей аутентификации
Распространение SIM-карт с ключами	Отдельное СКЗИ требуется лицензия ФСБ	Компонента, не отдельное СКЗИ
Дополнительные мероприятия по контролю за SIM-картами	Поэкземплярный учет SIM-карт как СКЗИ	Компонента, не отдельное СКЗИ
При сбое ДСЧ SIM	Компрометация ключей	Без последствий
Возможность утери ключа ЭП	Присутствует	Отсутствует
Степень уязвимости к атакам по побочным каналам	Повышенная	Низкая
Ориентировочное число операций с одной SIM-карты	25	100000
Ориентировочный срок действия ключей на SIM-карте	1 год и 3 месяца	10 лет
Критичные компоненты системы, кроме серверных	АРМ инициализации SIM в каждой точке выдачи	Отсутствуют

myDSS

Что добавит использование мобильного приложения?

- Удобство интерфейсов для пользователя.
- Полноценная визуализация.

Выводы

Требования Постановления Правительства РФ №1104 можно реализовать:

- удобным для пользователя образом;
- в соответствии с требованиями ФСБ России;
- на основе существующих решений;
- с использованием SIM-карт или мобильного приложения.

Спасибо за внимание!

Вопросы?

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