О реализации систем удалённого хранения ключей и формирования ЭЦП

Меньшенин Александр
Демос

Смирнов Павел
ООО «КРИПТО-ПРО»
ведущий специалист, к.т.н.

Традиционные ключевые хранилища

	S/W т.е. хранимые на жестком диске	**H/W** т.е. хранимые на смарт картах
Ключи и подпись	**низкий уровень безопасности**	**высокий уровень безопасности**
Удобство пользования	**Низкий или отсутствующий уровень мобильности** **Простая установка**	**Низкая мобильность** **Требуются драйверы и доп аксессуары**
Управление	**Сложное**	**Сложное**

Виртуальная «чип-карта»: Сервер подписи

Предоставляет возможность выполнять цифровую подпись без всякого ПО, аппаратных средств и ключей, установленных на стороне клиента

- Доступ отовсюду через браузер
  - Полная мобильность
  - Отсутствие риска потери колючей, карты, PC, …
- Ключи порождаются, хранятся и управляются централизовано на сервере подписи, где обеспечено:
  - Безопасное окружение: аппаратные криптографические модули, физическая защита,...
  - Секретные ключи никогда не покидают защищенный периметр
- Доступ к ключам обеспечивается дополнительным сервером аутентификации, функционирующим через:
  -SMS, Fax, e-Mail, scracth-card и пр, ...
- Журнал аудита позволяет разрешать конфликтные ситуации

Пример: Мобильность в Е-банкинге

- Чего не хватает:
  - PKI-совместимое решение на EMV-картах, но прозрачное для пользователей существующего процессинга
    - Защита ключей с помощью PIN-кода
- Предлагаемое решение: «виртуальная чип-карта»
  - Закрытый ключ всегда на одном сервере
    - или на нескольких серверах с разделяемым секретом
    - подпись осуществляется под контролем пользователя
  - Первый шаг – установка защищенного канала
  - Второй – аутентификация на основе OTP (токен или SMS)

Двухфакторная аутентификация

Стержень безопасности – строгий контроль доступа к ключам подписи

Это накладывает требование к механизмам аутентификации через два независимых канала

Типично

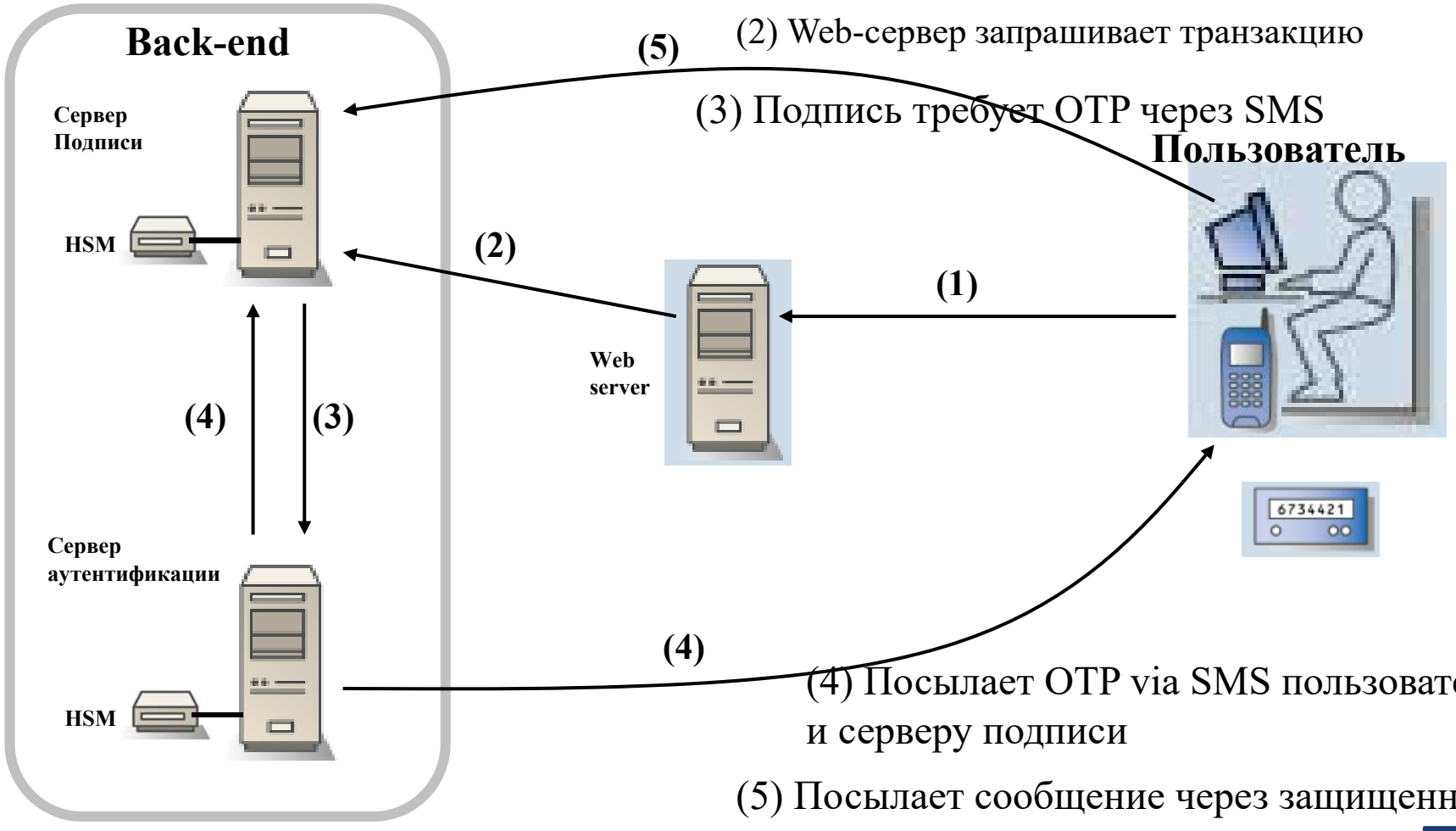
- Что-то, что вы имеете и
- Что-то, что вы знаете

Для предотвращения фишинга

Безопасность аутентификации и авторизации

- Варианты аутентификации
  - Пользователь получает одноразовый пароль от сервера аутентификации через отдельный канал, например SMS
  - Пользователь имеет интеллектуальный токен с разделением секрета с сервером аутентификации
- Авторизация пользователей
  - Защищенный канал/туннель
    - Между веб-сервером и сервером подписи
    - Пользователь посылает одноразовый пароль на сервер подписи
    - Сервер аутентификации посылает хэш-значение на сервер подписи
    - Сервер подписи осуществляет проверку

Как работает сервер подписи



(1) Пользователь заходит на Web-сервер

(2) Web-сервер запрашивает транзакцию

(3) Подпись требует OTP через SMS

(4) Посылает OTP via SMS пользователю и серверу подписи

(5) Посылает сообщение через защищенный канал серверу подписи

Применение HSM на сервере подписи

- Аппаратные модули (HSM) обеспечивают
  - Безопасность критических параметров аутентификации
  - Защиту использования ключей в критичных операциях
  - Генерацию ключевого материала и паролей
  - Аудит использования закрытых ключей
- Механизмы аутентификации внутри HSM
  - Системный администратор не может компрометировать ключевой материал
  - Системный администратор не может фальсифицировать ответ сервера аутентификации

Выводы

- Комбинирование традиционных PKI-систем с сервером подписи на основе HSM существенно расширяет область применения PKI
- Примеры
  - E/M-банкинг
  - E/M-голосование
  - Универсальная электронная карта

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru
info@cryptopro.ru
spv@cryptopro.ru

Тел./факс:
+7 (495) 780-48-20
+7 (495) 660-23-30