РУТОКЕН

XX международная научно-практическая конференция
«РусКрипто’2018»

Криптографические средства на рабочих местах клиентов ДБО

Кирилл Мещеряков,
компания «Актив»

Аутентификация и электронная подпись

- Коммерческий банк — сервисная организация, выполняющая действия (поручения) от лица своего клиента
- Поручения могут быть исполнены только если банк удостоверился что клиент — это действительно тот, за кого он себя выдает
- Как убедиться в этом?
- Личная встреча, аутентификация по документам, образец подписи
- Если удаленно — методами аутентификации

Методы удаленной аутентификации

- Аутентификация по многоразовым паролям
- Аутентификация по одноразовым паролям
- Двухфакторная аутентификация
- Строгая двухфакторная аутентификация
- Многофакторная аутентификация

Где действует нарушитель в ДБО

- Как и в оффлайне,
  в дистанционном банковском обслуживании
  применяются те же методы:
  - Подделка аутентификаторов
  - Выдача себя за другое лицо
  - Обман проводящей аутентификацию системы

Как банк защищается от нарушителя в ДБО

- Как и в оффлайне,
  в дистанционном банковском обслуживании
  применяются те же методы:
  - Усиление проверки аутентификаторов
    (увеличение количества проверок)
  - Использование аутентификаторов,
    которые сложнее подделать
  - Повышение доверия к проводящей
    аутентификацию системе

Разделяемый секрет клиента и банка

- В оффлайн мире обычно банк вместе с клиентом договариваются о наличии «секретного слова»
- В ДБО вместо «секретного слова» очень хорошо работает симметричная или ассиметричная криптография

Практика использования аутентификации

- Программный генератор одноразовых паролей
  - обычно мобильное приложение
- Аппаратный генератор одноразовых паролей
  - импортное устройство (отечественных аналогов нет)
- Инициализируется с помощью закрытого ключа
- Закрытый ключ передается клиенту
- Однако, ключ теоретически все-таки может быть скомпрометирован

Практика использования аутентификации

- Программный токен (ключи в PFX-файле)
- Ключи хранятся в файле и защищены паролем
- На клиентском месте криптографические операции производятся с помощью специального программного обеспечения — криптопровайдера или браузерного плагина
- Закрытый ключ хранится в файловой системе, а значит легко копируется, пароль от ключевого контейнера легко перебрать и скомпрометировать

Практика использования аутентификации

- Криптографический токен (иностранного происхождения)
- Ключи хранятся в устройстве и физически не извлекаются
- На клиентском месте криптографические операции производятся на самом аппаратном ключе
- Доступ к ключу и к криптографическим операциям происходит с помощью браузерного плагина
- Периодически приходят новости об успешных атаках на то или иное устройство (самый последний случай — эстонские ID карты)

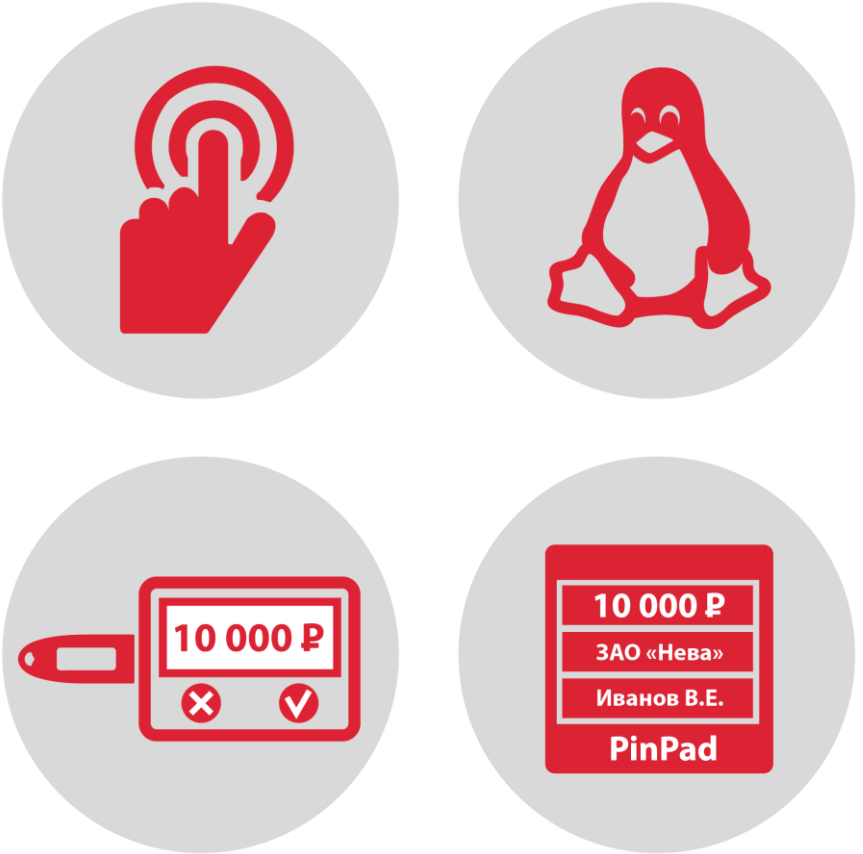
Практика использования аутентификации

- Криптографический токен — с поддержкой ГОСТ-криптографии
- Ключи хранятся в устройстве и физически не извлекаются
- На клиентском месте криптографические операции производятся на самом аппаратном ключе
- Доступ к ключу и к криптографическим операциям происходит с помощью браузерного плагина
- Именно криптографические токены с поддержкой ГОСТ-криптографии стали мейстримом

Практика использования аутентификации

Способы повышения доверия к среде:

- Криптографический токен с кнопкой — для защиты от удаленного управления
- Криптографический токен с доверенным ПО — для защиты от подмены программного обеспечения на месте клиента, либо с доверенной средой (linux)
- Криптографический токен с подключаемым средством просмотра
- Криптографический токен со встроенным средством просмотра



Практика использования аутентификации

- Криптографический токен с возможностью подключения к мобильным устройствам
- Большое количество разъемов для подключения внешних устройств, поэтому сложно создать устройство, которое смогло бы подключиться к любому
- Операционные системы iOS и Android содержат внушительное количество средств сбора телеметрии, а значит хранить внутри устройств криптографические ключи небезопасно

Итоги

По данным компании «Актив»

- 44 коммерческих банка
  из ТОП-50 используют для ДБО
  криптографические токены
  с неизвлекаемыми ключами
- Примерно половина из них
  использует токены с ГОСТ-криптографией
- Практика показывает, что использование для ДБО
  токенов с неизвлекаемыми ключами позволяет получить
  прогнозируемый уровень доверия при небольших затратах

Вопросы

Контактная информация

Кирилл Мещеряков

Электронная почта:

mk@rutoken.ru

hotline@rutoken.ru

Сайты:

www.rutoken.ru

www.aktiv-company.ru

Телефон:

+7 495 925-77-90

+7 905 509-70-24