Легенды и мифы о средствах электронной подписи

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

PKI-Форум Россия 2015

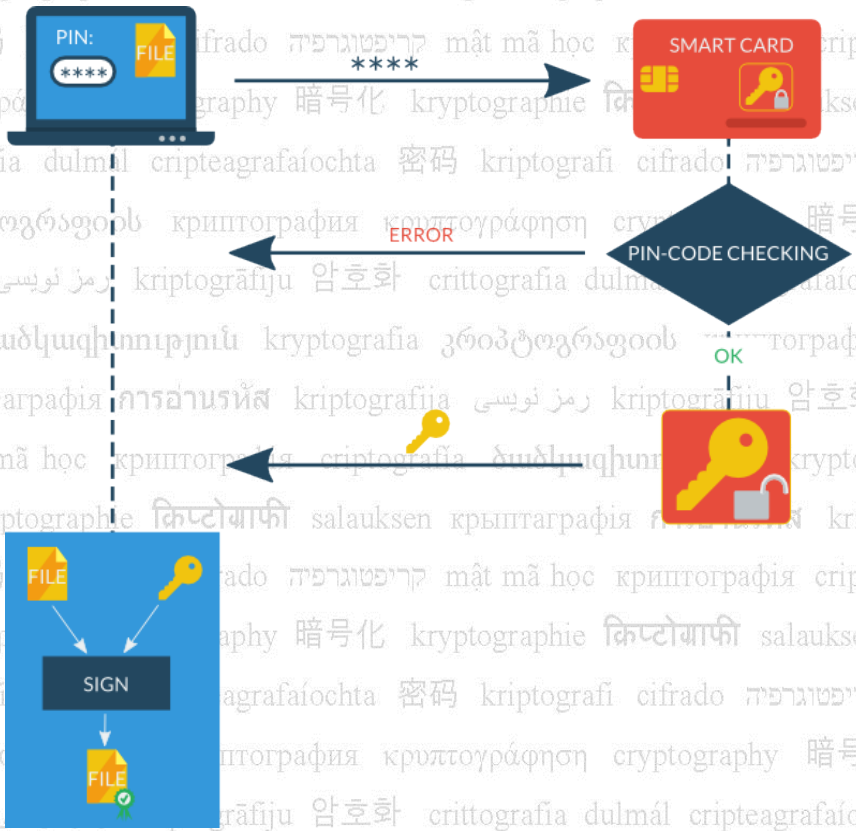
1. Отчуждаемые ключевые носители и работа с ними
2. Безопасная парольная аутентификация при малом объеме словаря паролей
3. Использование контактных и бесконтактных считывателей
4. Хранение ключей в облаке
5. Формирование ЭП с использованием SIM-карты

Миф 1: «Есть существенная разница в безопасности между пассивными носителями и автономными вычислителями».

КРИПТО ПРО

Пассивный носитель

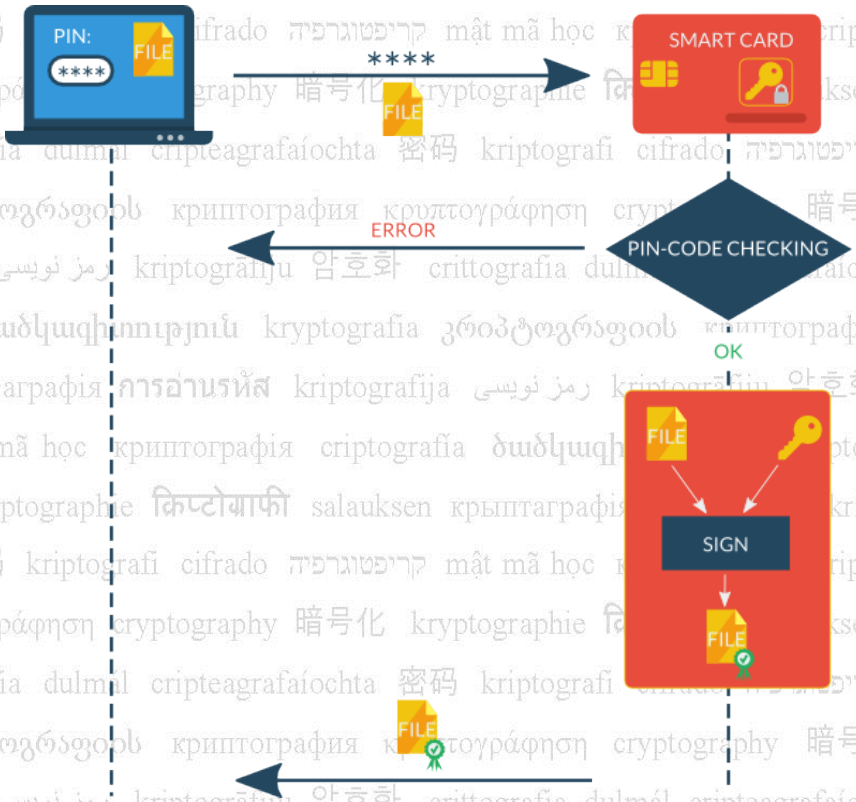
- Использование ключа основным криптосредством: вычисления в оперативной памяти системы.



КРИПТО ПРО

Активный токен

- Все вычисления на самом устройстве, ключ в память не попадает.



Три точки перехвата информации, циркулирующей между токеном и пользовательской системой.

1. Терминал пользователя
   - RCS, Remote Control System: перехват параметров вызовов функций, данных приложений, парольных данных.
2. Токен
   - Возможность загрузки ВПО в сам ключевой носитель.

Таким образом, единственным типом нарушителей, за противодействие которому имеет смысл бороться при проектировании архитектуры решений с токенами, является нарушитель в канале.

Три точки перехвата информации, циркулирующей между токеном и пользовательской системой.

1. Терминал пользователя
   - RCS, Remote Control System: перехват параметров вызовов функций, данных приложений, парольных данных.
2. Токен
   - Возможность загрузки ВПО в сам ключевой носитель.

Таким образом, единственным типом нарушителей, за противодействие которому имеет смысл бороться при проектировании архитектуры решений с токенами, является нарушитель в канале.

КРИПТО ПРО

3. Канал передачи данных

- Как в случае пассивных токенов, так и активных.
- Пассивный токен: компрометируется и пароль и ключ ⇒ раскрытие ключа.
- Активный токен: компрометируется пароль и доступ к ключу ⇒ селективная подделка подписи.

Обязательное требование по эксплуатации: подключение к доверенному порту, т. е. отсутствие канала, в котором может присутствовать злоумышленник.

Пассивные хранилища и автономные вычислители

- Доступ нарушителя к пользовательскому процессу в системе означает компрометацию доступа к ключу.
- Доступ нарушителя к каналу от системы к носителю означает компрометацию доступа к ключу.
- В случае пассивного носителя нарушитель потенциально извлекает из памяти ключ.
- В случае автономного вычислителя нарушитель потенциально перехватывает пароль и возможность подписи произвольных данных.
- В случае автономного вычислителя опаснее атаки по побочным каналам (потребление, время).

Безопасная парольная аутентификация при малом объеме словаря паролей

Миф 2: «Парольная аутентификация заведомо не может быть стойкой, если нарушитель может присутствовать в канале, а словарь паролей невелик».

... и в случае возможности присутствия нарушителя в канале необходимо использовать схемы аутентификации на основе секретов с энтропией на уровне закрытых ключей (пароли из словаря объема 10^{18} и выше, CV-сертификаты, ...).

Безопасная парольная аутентификация при малом объеме словаря паролей

Миф 2: «Парольная аутентификация заведомо не может быть стойкой, если нарушитель может присутствовать в канале, а словарь паролей невелик».

... и в случае возможности присутствия нарушителя в канале необходимо использовать схемы аутентификации на основе секретов с энтропией на уровне закрытых ключей (пароли из словаря объема 10^{18} и выше, CV-сертификаты, ...).

КРИПТО ПРО

Основная цель

Ключевой носитель должен быть стойким по отношению к активному противнику в канале связи токен–система.

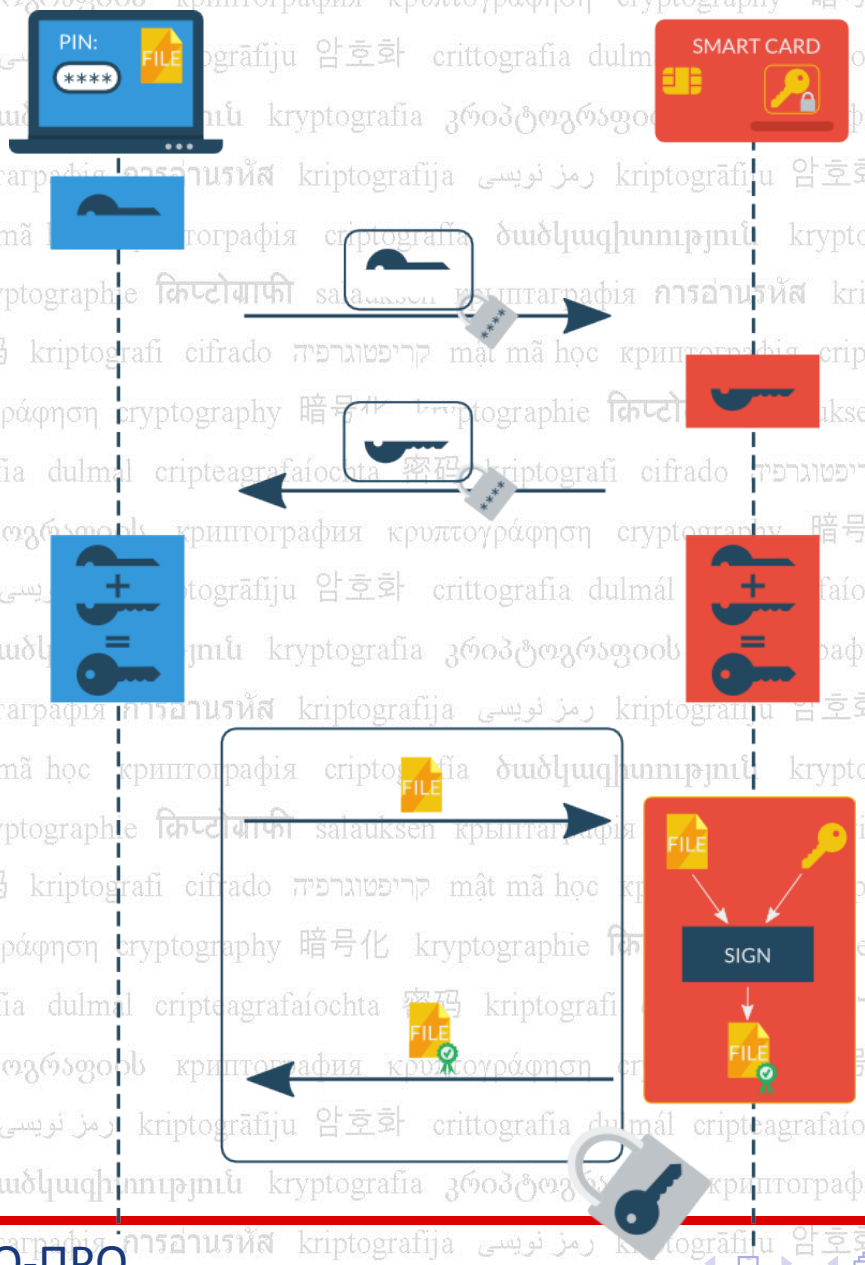
Основная идея

Данные, передаваемые для формирования защищенного канала, защищаются с помощью пароля на токен.

Ключевое дополнительное требование

Активный противник в канале не должен иметь возможность получить критерий для бесконтрольного угадывания пароля (так называемого ”offline-перебора”).

Функциональный ключевой носитель



КРИПТО ПРО

Функциональный ключевой носитель

- На аутентифицированном на пароле ключе согласования устанавливается защищенный канал связи между системой и носителем.
- Все дальнейшие пересылки между носителем производятся посредством защищенного канала.
- За счет распределения вычислений возможно уменьшение опасности атак по побочным каналам.
- Сам пароль также защищен от оффлайного перебора пароля с опробованием по полученным в канале данным (после действий нарушителя в канале).

Использование контактных и бесконтактных считывателей

Миф 3: «Можно на основе отчуждаемого носителя сделать «бесконтактное» решение и спокойно с ним работать».

- Всякий бесконтактный способ взаимодействия с токеном ⇒ необходимость рассматривать возможность присутствия противника в канале.
- Использование пассивных хранилищ или активных токенов в помещениях, отличных от специально оборудованных для подобного использования, недопустимо.
- С Bluetooth или NFC-считывателями необходимо использовать независимые средства для конкретного беспроводного канала либо протоколы EKE для совмещения решения задач парольной аутентификации и защиты канала «система-карта».

Хранение ключей в облаке

Миф 4: «Хранение ключей в облаке неминуемо приводит к ослаблению доверия к ключам — однозначно лучше держать ключи при себе».

Без облака

Информация не покидает некоторого защищённого периметра

В облаке

- Само понятие периметра отсутствует.
- Ответственность между владельцем информации и поставщиком облачных услуг.

Хранение ключей в облаке

Миф 4: «Хранение ключей в облаке неминуемо приводит к ослаблению доверия к ключам — однозначно лучше держать ключи при себе».

Без облака

Информация не покидает некоторого защищённого периметра

В облаке

- Само понятие периметра отсутствует.
- Ответственность между владельцем информации и поставщиком облачных услуг.

КРИПТО ПРО

Доверие к облачной подписи

- Аутентификация пользователя на ключи.
- Безопасность хранения и использования ключа на сервере и надежностью механизмов аутентификации.

Хранение ключей в облаке

Security Requirements for Trustworthy Systems Supporting Server Signing Европейского Комитета по Стандартизации (CEN)

Требования и рекомендации к построению серверов электронной подписи, позволяющих формировать ЭП, эквивалентную полученной на персональном доверенном защищенном специализированном устройстве (например, криптографическом токене), и, соответственно, эквивалентную собственноручной.

- Уровень 1: аутентификация производится на приложение на пользовательской системе, которое далее само связывается с сервером подписи для формирования автоматизированной подписи.
- Уровень 2, Квалифицированная электронная подпись (QES).

Уровень 2

- Поддержка строгих вариантов аутентификации на сервере подписи, при которых процесс аутентификации пользователя происходит напрямую на сервер подписи.
- Пользовательские ключи подписи для формирования квалифицированной ЭП должны храниться строго в памяти специализированного защищенного устройства (криптографический токен, HSM).
- Аутентификация пользователя на сервере электронной подписи обязана быть как минимум двухфакторной.

Допускается использование сервера электронной подписи для формирования подписей для кластера сообщений разом, что оказывается весьма полезным при подписании большого массива однородных документов, отличающихся лишь данными в нескольких полях. При этом аутентификация пользователя производится не на операцию (формирования подписи), а на сессию.

Требования к формированию, обработке, использованию и удалению пользовательского ключевого материала, а к свойствам внутренней ключевой системы сервера электронной подписи и к аудиту. Представленные требования не сильнее (в основном — существенно слабее) требований, предъявляемых к СЭП класса КВ2.

Формирование ЭП с использованием SIM-карты

Миф 5: «Средства подписи на основе SIM-карты разумно делать только аналогично токенам».

Ключ ЭП на SIM-карте

- Вопросы надежности хранения ключа ЭП.
- Безопасные реализации криптографии.
- Качество ДСЧ/ПДСЧ.

КРИПТО ПРО

Ключ ЭП на SIM-карте

- Узкий канал связи.
- Ограниченность ресурсов по визуализации.
- Пересылка выжимки полей сообщения ⇒ строгая привязка выжимки к сообщению.

Иначе: возможность проведения атак с подменой подписываемых сообщений противоречит принципу персональной ответственности пользователя за подписываемые данные.

Аутентификация на ключ по SIM-карте

Альтернатива — сервер подписи, хранящий пользовательские ключи и предоставляющий доступ к операциям формирования ЭП с аутентификацией по SIM.

- Основной вопрос: ответственность за ключи.
- При обеспечении привязки происходит аутентификация сообщения посредством некоторого ключевого материала. Компрометация либо неаутентифицированное использование данного ключевого материала по возможным последствиям совершенно эквивалентны компрометации ключа подписи. А значит, фактическое заверение документа происходит исходно с использованием внешнего сервера – автоматизированного средства, к которому при этом не может не требоваться полное доверие.
- Вопросы аудита в случае серверной подписи.

КРИПТО ПРО

Спасибо за внимание!

Вопросы?

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