Мобильная электронная подпись: российские реалии

Смышляев Станислав Витальевич, к.ф.-м.н.,
руководитель департамента информационной безопасности
Смирнов Павел Владимирович, к.т.н.,
руководитель департамента разработок

PKI-Форум Россия 2017

Мобильная подпись — задачи

Основные программные технологии мигрируют на мобильные устройства.
В первую очередь — как раз те, что, как и работа с электронной подписью, предполагают повседневное использование.

Основные вопросы

- Пожелания к порядку использования?
- Как обеспечить безопасность с учетом ограничений мобильных устройств?

Мобильная подпись — цели

Пожелания

Дать пользователю инструмент, позволяющий с помощью его мобильного телефона воспользоваться своим ключом ЭП.

- Произвольного телефона, не только на iOS или Android.
- Всюду, где есть связь, не обязательно мобильный Интернет.
- Работа с ключом ЭП без 40 минут (включая 25 минут на перезагрузку ОС с обновлениями) на начало работы с токеном (с пользователем, который может забыть воткнуть токен).

Цель

Путь — обеспечить работу с использованием ключевой информации на SIM-картах.

- Нет ограничений по телефону (работа через STK).
- Требуется только работа с сервисными сообщениями ($\approx$ SMS).
- Существенные ограничения по визуализации.

Подход «в лоб»

Ключ электронной подписи непосредственно на SIM-карте (аналогично мобильным приложениям для ЭП на iOS/Android).

Проблема

В ряде аспектов, важных для средств ЭП с учетом российских требований, SIM существенно отличается от привычных сред функционирования.

Причины

- Принципиальные отличия ГОСТ Р 34.10 от RSA.
- Необходимость доверенной реализации vs. Производительность.
- «Тяжеловесность» криптографии с открытым ключом при реализации с учетом российских требований (даже КС1) при работе на низкоресурсных вычислителях.
- Требования по визуализации: однозначное соответствие подписываемого документа визуализируемому.

Подход «в лоб»

Ключ электронной подписи непосредственно на SIM-карте (аналогично мобильным приложениям для ЭП на iOS/Android).

Проблема

В ряде аспектов, важных для средств ЭП с учетом российских требований, SIM существенно отличается от привычных сред функционирования.

Причины

- Принципиальные отличия ГОСТ Р 34.10 от RSA.
- Необходимость доверенной реализации vs. Производительность.
- «Тяжеловесность» криптографии с открытым ключом при реализации с учетом российских требований (даже КС1) при работе на низкоресурсных вычислителях.
- Требования по визуализации: однозначное соответствие подписываемого документа визуализируемому.

Безопасность подписи

Источник случайности

- В отличие от RSA для ГОСТ Р 34.10 требуется доверенный источник случайности.
- Его сбой влечет компрометацию ключа ЭП.
- Это событие крайне трудно детектировать автоматически (подпись останется корректной).

Безопасность подписи

Доверенные реализации криптографии на эл. кривых

- Реализация работы с эллиптическими кривыми на уровне апплета — 2-3 минуты.
- Реализация на SIM-карте с сопроцессором — не соответствует требованиям в случае зарубежной SIM, дорого в случае специальной российской.
- Необходимость противодействия атакам по побочным каналам (в т.ч. по времени) — дополнительное снижение производительности.

Безопасность подписи

Итого: безопасная реализация процедур вычисления электронной подписи непосредственно на SIM-карте существенно затруднена.

- Разумная цена за возможность пользоваться преимуществами асимметричных схем.
- Но действительно ли в случае мобильной подписи есть смысл платить эту цену?

Безопасность подписи

Дополнительная проблема: визуализация

- Российские требования строго обязывают в полной мере визуализировать документ.
- Требуется обеспечить эквивалентность визуализируемого документа подписываемому.
- Невозможно выполнить для сервисных ($\approx$ SMS) сообщений.
- Исключения: отдельные случаи коротких текстов/xml.

Следствие 1

Требуется отдельно обеспечить доверенную визуализацию документа дополнительными средствами.

Следствие 2

Требуются доверенные серверные компоненты, их взаимодействие с SIM и с компьютером пользователя.

Безопасность подписи

Дополнительная проблема: визуализация

- Российские требования строго обязывают в полной мере визуализировать документ.
- Требуется обеспечить эквивалентность визуализируемого документа подписываемому.
- Невозможно выполнить для сервисных ($\approx$ SMS) сообщений.
- Исключения: отдельные случаи коротких текстов/xml.

Следствие 1

Требуется отдельно обеспечить доверенную визуализацию документа дополнительными средствами.

Следствие 2

Требуются доверенные серверные компоненты, их взаимодействие с SIM и с компьютером пользователя.

К этим серверным компонентам не может не требоваться полное доверие: наличие злоумышленника, имеющего к ним доступ, немедленно приводит к угрозе подмены подписываемого сообщения.

- Требуется доверенная серверная часть.
- Отношения доверия пользователя с серверной частью устанавливаются явным образом.
- Аутентификация в рамках замкнутой системы.

$\Rightarrow$ потребности в «асимметричности» криптографии нет.

Альтернатива

- Аутентификацию сообщений между мобильным устройством и серверной стороной можно осуществлять с использованием симметричных алгоритмов.
- HMAC_GOSTR3411_2012_256, стандартизированный в Р 50.1.113–2016 Росстандарта.

Задача безопасной реализации данного алгоритма на SIM-карте является беспроблемно выполнимой.

- Производительности базовой (без криптосопроцессора) архитектуры достаточно.
- Учесть необходимость противодействия атакам по побочным каналам можно без вреда для эффективности вычислений.
- Нет требований по доверенным ДСЧ на клиентской стороне.

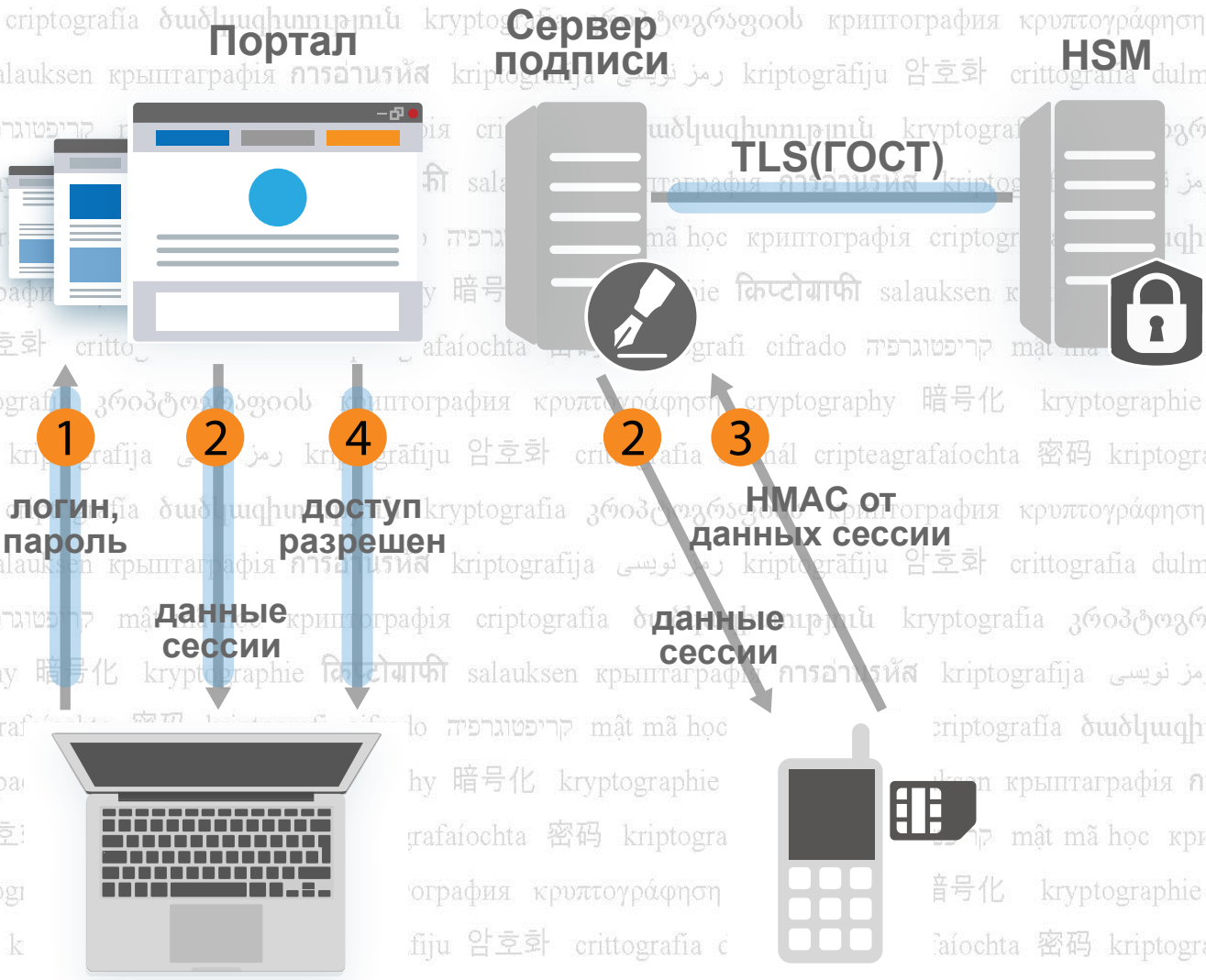
Альтернатива

- Аутентификацию сообщений между мобильным устройством и серверной стороной можно осуществлять с использованием симметричных алгоритмов.
- HMAC_GOSTR3411_2012_256, стандартизированный в Р 50.1.113–2016 Росстандарта.

Задача безопасной реализации данного алгоритма на SIM-карте является беспроблемно выполнимой.

- Производительности базовой (без криптосопроцессора) архитектуры достаточно.
- Учесть необходимость противодействия атакам по побочным каналам можно без вреда для эффективности вычислений.
- Нет требований по доверенным ДСЧ на клиентской стороне.

Общая схема


Портал
Сервер подписи
HSM
TLS(ГОСТ)
1
2
4
2
3
логин, пароль
доступ разрешен
данные сессии
HMAC от данных сессии
данные сессии

Централизованное хранение ключей ЭП пользователей на серверной стороне решает и ряд других задач:

- Повреждение/утеря телефона не приводит к утере ключей ЭП, в случае утери доступ к ключам блокируется мгновенно на серверной стороне (а не через CRL с задержкой).
- Наличие журналов аудита на сервере при любой нештатной ситуации позволяет гарантированно установить, был ли осуществлен несанкционированный доступ к ключу подписи.
- Пользователь имеет возможность доступа к своим ключам подписи сразу с нескольких устройств, что удобно для «мобильных» сотрудников и для руководителей высшего звена.

Централизованное хранение ключей ЭП пользователей на серверной стороне решает и ряд других задач:

- Преимущества симметричных алгоритмов в части сроков действия ключей — нет априорно известного нарушителю открытого ключа, не начать атаку до использования ключа.
- На телефоне — только средство аутентификации, компонента, не являющаяся самостоятельным СКЗИ. Важно для массовой криптографии с пониженным регулированием.

- КриптоПро DSS (первые 11 исполнений) сертифицирован (СКЗИ, СЭП) в августе 2017.
- Работа КриптоПро DSS в составе КриптоПро УЦ 2.0 — согласование новых (включающих в свой состав DSS) исполнений КриптоПро УЦ 2.0 в процессе, по доп. ТЗ.
- КриптоПро DSS с поддержкой SIM с ключом аутентификации (HMAC) — отчет на экспертизе с июня 2017.

Централизованное хранение ключей ЭП пользователей на серверной стороне решает и ряд других задач:

- Преимущества симметричных алгоритмов в части сроков действия ключей — нет априорно известного нарушителю открытого ключа, не начать атаку до использования ключа.
- На телефоне — только средство аутентификации, компонента, не являющаяся самостоятельным СКЗИ. Важно для массовой криптографии с пониженным регулированием.

- КриптоПро DSS (первые 11 исполнений) сертифицирован (СКЗИ, СЭП) в августе 2017.
- Работа КриптоПро DSS в составе КриптоПро УЦ 2.0 — согласование новых (включающих в свой состав DSS) исполнений КриптоПро УЦ 2.0 в процессе, по доп. ТЗ.
- КриптоПро DSS с поддержкой SIM с ключом аутентификации (HMAC) — отчет на экспертизе с июня 2017.

CRYPTOPRO

Спасибо за внимание!

Вопросы?

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

CRYPTOPRO

Спасибо за внимание!

Вопросы?

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

Эксперимент в июле

- Цель: скачать и поставить КриптоПро CSP и без документации начать использовать имеющийся токен с ключом для аутентификации в рамках двустороннего TLS.
- Итоги: ≈ 40 минут, 2 подсказки.
- ≈ 25 минут — пока Windows ставила свои обновления при первой за долгое время перезагрузке.
- Проблема 1: попытки при регистрации для скачивания вводить бессмысленные данные отвергались фильтрами, пришлось вводить настоящие данные.
- Проблема 2: для использования ключа на токене было необходимо вставить сам токен.
- Сертификаты ГУЦ в новых версиях CSP ставятся при установке провайдера.
- На сайте уточнены подсказки при регистрации.
- При перезагрузке для установки CSP теперь по умолчанию подавляется установка обновлений ОС.

Эксперимент в июле

- Цель: скачать и поставить КриптоПро CSP и без документации начать использовать имеющийся токен с ключом для аутентификации в рамках двустороннего TLS.
- Итоги: ≈ 40 минут, 2 подсказки.
- ≈ 25 минут — пока Windows ставила свои обновления при первой за долгое время перезагрузке.
- Проблема 1: попытки при регистрации для скачивания вводить бессмысленные данные отвергались фильтрами, пришлось вводить настоящие данные.
- Проблема 2: для использования ключа на токене было необходимо вставить сам токен.
- Сертификаты ГУЦ в новых версиях CSP ставятся при установке провайдера.
- На сайте уточнены подсказки при регистрации.
- При перезагрузке для установки CSP теперь по умолчанию подавляется установка обновлений ОС.

Эксперимент в июле

- Цель: скачать и поставить КриптоПро CSP и без документации начать использовать имеющийся токен с ключом для аутентификации в рамках двустороннего TLS.
- Итоги: ≈ 40 минут, 2 подсказки.
- ≈ 25 минут — пока Windows ставила свои обновления при первой за долгое время перезагрузке.
- Проблема 1: попытки при регистрации для скачивания вводить бессмысленные данные отвергались фильтрами, пришлось вводить настоящие данные.
- Проблема 2: для использования ключа на токене было необходимо вставить сам токен.
- Сертификаты ГУЦ в новых версиях CSP ставятся при установке провайдера.
- На сайте уточнены подсказки при регистрации.
- При перезагрузке для установки CSP теперь по умолчанию подавляется установка обновлений ОС.

CRYPTOPRO

Спасибо за внимание!

Вопросы?

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