Безопасная мобильная подпись для всех

Смышляев Станислав Витальевич
д.ф.-м.н., заместитель генерального директора КриптоПро

Смирнов Павел Владимирович
к.т.н., директор по развитию КриптоПро

КРИПТОПРО

PKI-Форум Россия 2023

Средства ЭП на мобильных устройствах

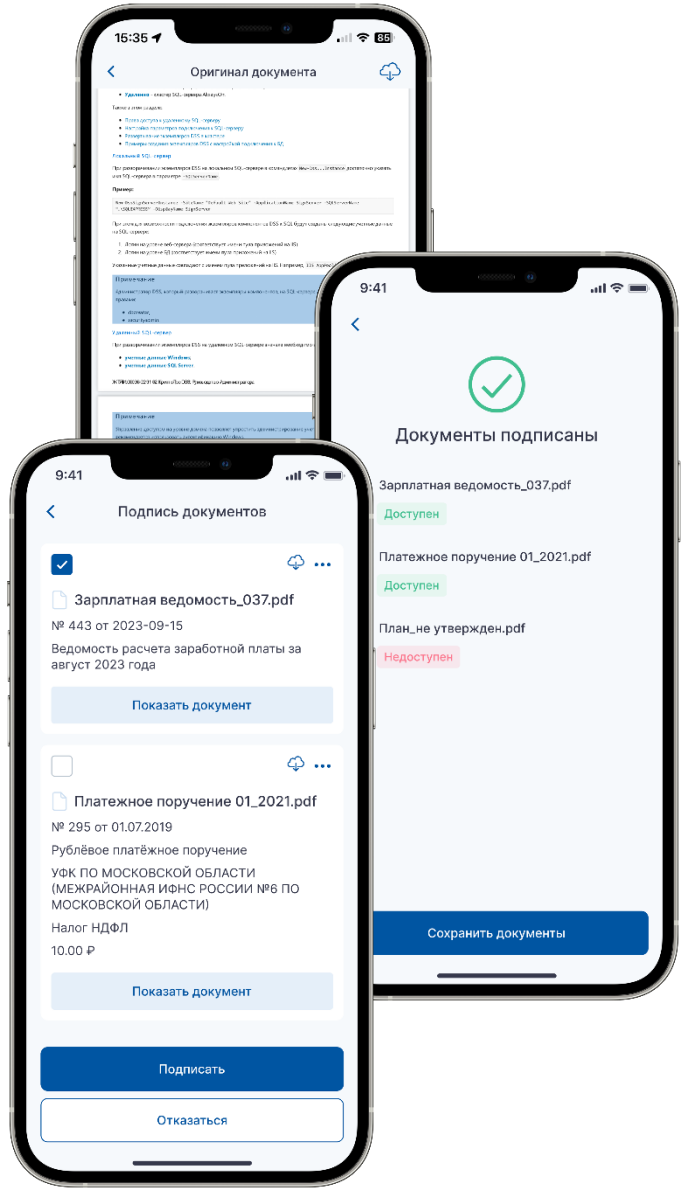
- Массовые СКЗИ/СЭП класса КС1.

- Общие проблемы СКЗИ на мобильных устройствах:
  - Удаление из магазинов приложений российских МП.
  - Уязвимости в импортируемых компонентах кода.
  - Уязвимости ОС (пример: iOS).
  - Риски блокировки магазинов приложений и удаленной блокировки устройств граждан.
  - Отзыв TLS-сертификатов, выданных международными УЦ.

– важнейшие вопросы, но за рамками данного доклада.

- Применение ЭП посредством мобильных устройств должно учитывать ряд важнейших особенностей эксплуатации и свойств модели нарушителя.

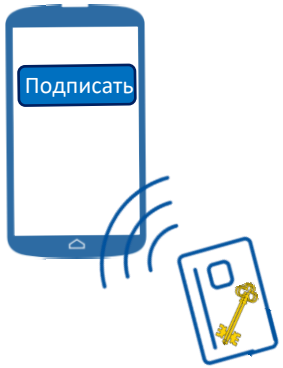
- Четыре подхода к «мобильной ЭП».



В прошлых сериях…

Подходы к реализации «мобильной» подписи:

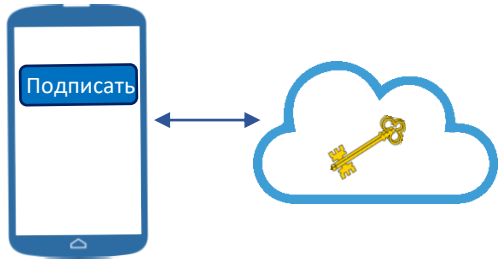
- «Локальная» подпись: полный контроль пользователя над ключом, низкая стоимость, отсутствие серверной стороны, полное доверие к среде функционирования (мобильной ОС), необходимость полного контроля над устройством, уязвимость к ВПО.



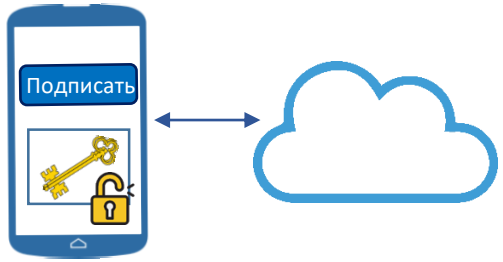
- Применение токенов по NFC: полный контроль пользователя над ключом, отсутствие серверной стороны, защита от извлечения ключа, риски компрометации разового доступа к ключу, высокая стоимость, поломки токенов, встраивание СКЗИ в приложения для защиты NFC-взаимодействий.

В прошлых сериях…

Подходы к реализации «мобильной» подписи:



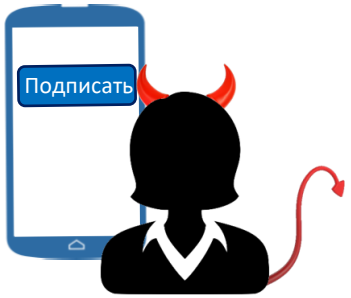
- «Облачная»/«дистанционная» подпись: производительность, снижение рисков при утере устройства, аудит, доступ к ключам с нескольких устройств, полное доверие серверу и администраторам, отдельные требования к средствам ЭП (п. 2.1 части 5 статьи 8 ФЗ-63), дополнительная аккредитация.



- Комбинированные клиент-серверные решения: полный контроль пользователя над ключом, аудит, снижение рисков при утере устройства, защита от компрометации сервера,
  [ранее:] компрометация ключа ЭП в случае ВПО на устройстве с доступом к памяти на чтение.
  - [Ранее:] ключ ЭП непосредственно перед совершением операции расшифровывался и временно присутствовал в памяти устройства в незащищенном виде.

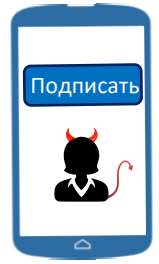
Семейство протоколов DKSSP

- Цель: защита ключей в условиях отсутствия доверия клиенту и серверу (но без сговора).
- Ключ ЭП ни в один момент времени не известен ни клиенту, ни серверу.
  - Все операции с ключом – распределенным образом.
- Пароли – исключительно в распределенных вычислениях высокоэнтропийных данных.
  - Аутентификация и работа с паролями – только через протоколы OPRF. Защита от перебора пароля.
- Защита от компрометации ключа ЭП
  - в случае утери мобильного устройства;



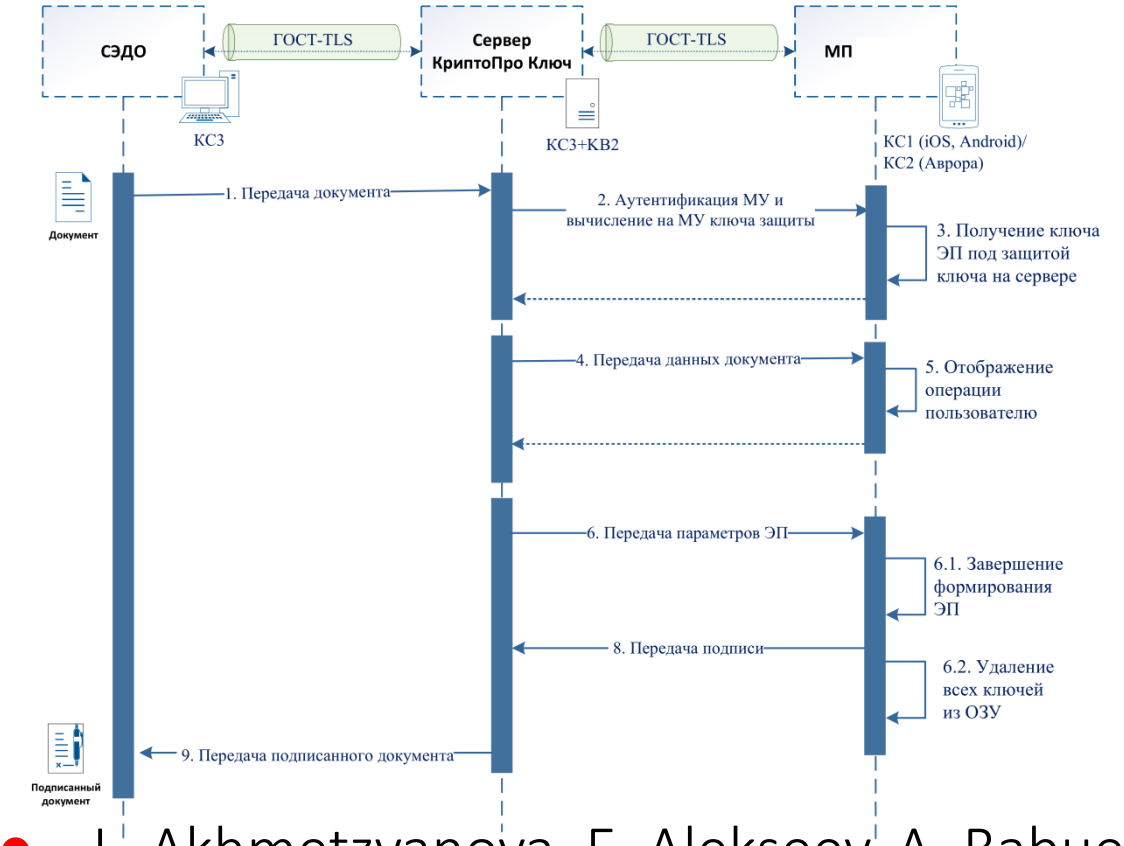
  - в случае полной компрометации серверных компонент;

  - в случае компрометации памяти устройства в любой момент времени.



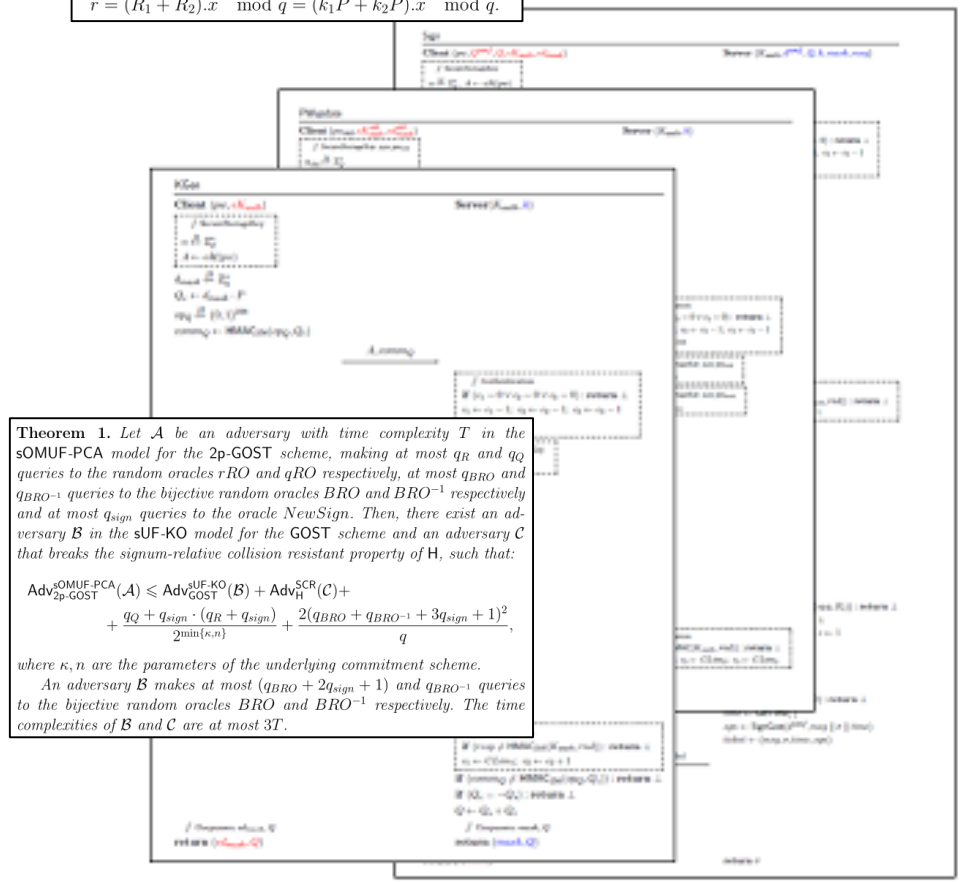
КРИПТОПРО

Синтез и анализ стойкости ядра протокола



$$s = (k_1 + k_2)e + (d_1 + d_2)r = (k_1 e + d_1 r) + (k_2 e + d_2 r),$$

$$r = (R_1 + R_2).x \mod q = (k_1 P + k_2 P).x \mod q.$$



Theorem 1. *Let $\mathcal{A}$ be an adversary with time complexity T in the* sOMUF-PCA *model for the* 2p-GOST *scheme, making at most q_R and q_Q queries to the random oracles rRO and qRO respectively, at most q_{BRO} and $q_{BRO^{-1}}$ queries to the bijective random oracles BRO and BRO^{-1} respectively and at most q_{sign} queries to the oracle $NewSign$. Then, there exist an adversary $\mathcal{B}$ in the* sUF-KO *model for the* GOST *scheme and an adversary $\mathcal{C}$ that breaks the signum-relative collision resistant property of* H*, such that:*

$$\mathsf{Adv}^{\mathsf{sOMUF\text{-}PCA}}_{\mathsf{2p\text{-}GOST}}(\mathcal{A}) \leqslant \mathsf{Adv}^{\mathsf{sUF\text{-}KO}}_{\mathsf{GOST}}(\mathcal{B}) + \mathsf{Adv}^{\mathsf{SCR}}_{\mathsf{H}}(\mathcal{C}) + \\ + \frac{q_Q + q_{sign} \cdot (q_R + q_{sign})}{2^{\min\{\kappa,n\}}} + \frac{2(q_{BRO} + q_{BRO^{-1}} + 3q_{sign} + 1)^2}{q},$$

where κ, n are the parameters of the underlying commitment scheme.

An adversary $\mathcal{B}$ makes at most $(q_{BRO} + 2q_{sign} + 1)$ and $q_{BRO^{-1}}$ queries to the bijective random oracles BRO and BRO^{-1} respectively. The time complexities of $\mathcal{B}$ and $\mathcal{C}$ are at most $3T$.

- L. Akhmetzyanova, E. Alekseev, A. Babueva, L. Nikiforova, S. Smyshlyaev, “**Two-party GOST in two parts: fruitless search and fruitful synthesis**”, Proceedings of the 12th Workshop on Current Trends in Cryptology (CTCrypt 2023), 2023, 29–66.

КРИПТОПРО

Ключевые свойства безопасности

- Компрометация устройства клиента не приводит к компрометации ключа ЭП.
  - Для создания подписи/регистрации нового ключа нарушителем необходима компрометация аутентификации в ходе взаимодействия с сервером (аутентификация с применением протокола OPRF).
- Компрометация сервера не приводит к компрометации ключа пользователя или возможности создания подписи нарушителем.
- Одновременная компрометация устройства клиента и его пароля не приводит к компрометации ключа подписи или возможности создания подписи нарушителем без штатного взаимодействия с сервером (аудит).

Реализация: КриптоПро Ключ

- Техническое задание согласовано ФСБ России 24 мая 2023 года.
- Основное исполнение – на основе протокола DKSSP.
  - Не «облачная»/«дистанционная» подпись.
  - Криптография на серверной стороне – в HSM (класс КВ/КВ2).
- Самостоятельные мобильные приложения и встраивание в существующие приложения.
- Преемственность интерфейсов взаимодействия (бесшовная миграция с DSS).
- Реализация криптопротоколов программных компонент – в новом КриптоПро CSP 5.0 R3 (получено заключение ФСБ России).
- Реализация механизмов безопасности в HSM – в новом КриптоПро HSM 2.0 R3 (получено заключение ФСБ России).

Спасибо за внимание!