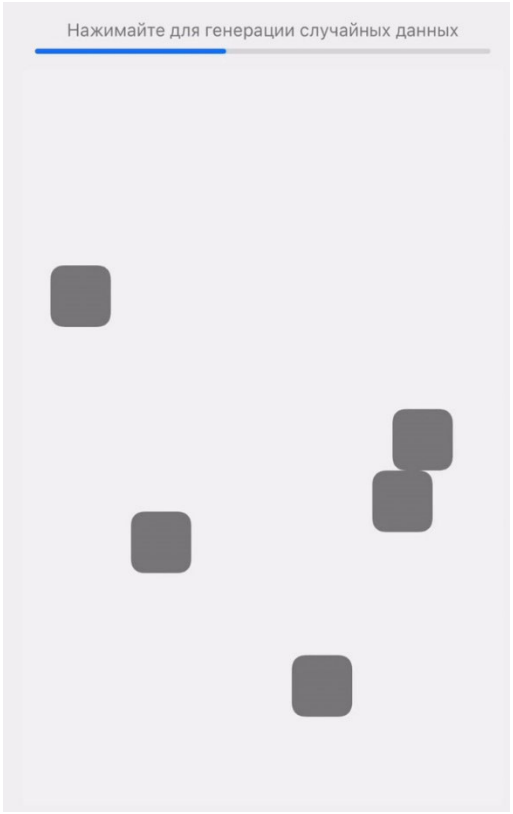
Мобильная подпись: проблемы и решения

Смышляев Станислав Витальевич,
заместитель генерального директора КриптоПро

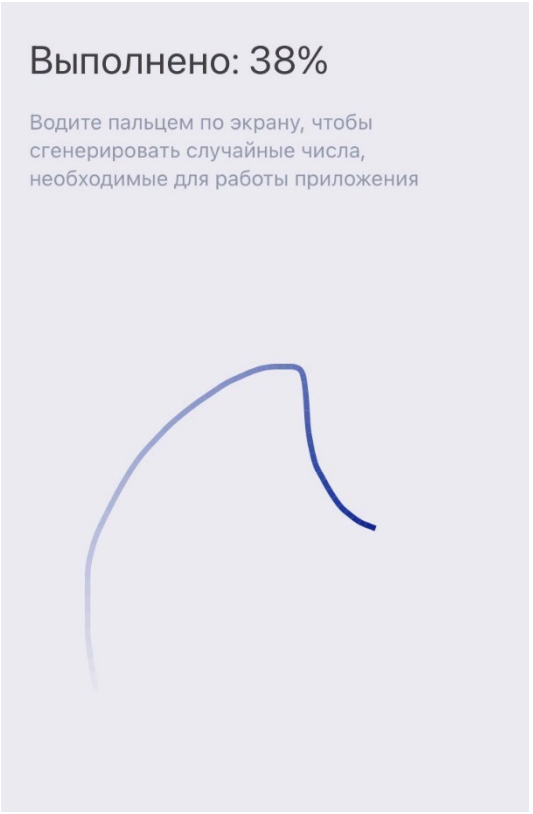
КРИПТОПРО

PKI-Форум Россия 2021

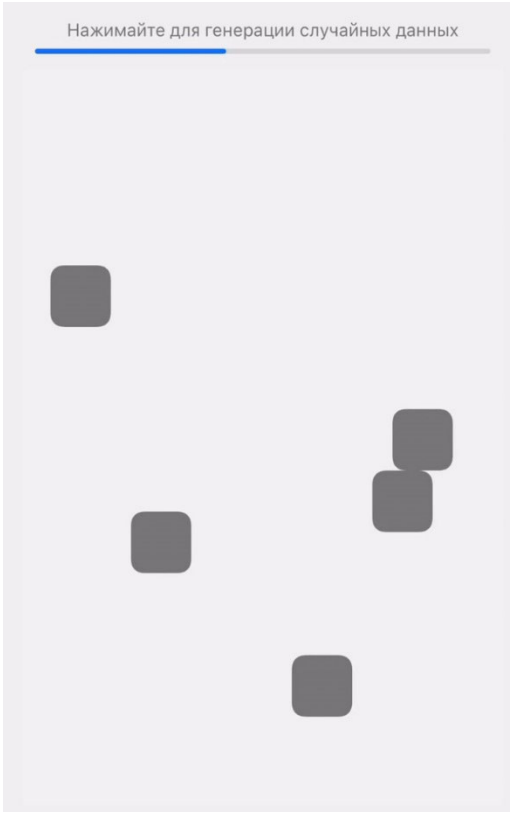
Проблемы: практика



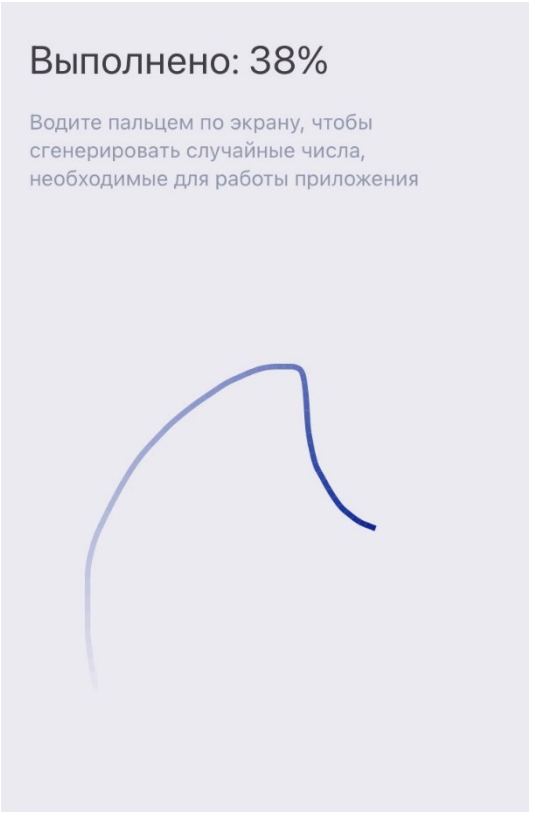
- Использование сертифицированной криптографии может требовать дополнительных действий от пользователя:
  - Контроль целостности.
  - Инициализация ДСЧ.
  - Локальная аутентификация.
- Проблема обновления версии мобильного приложения.
- Проблема лицензионного контроля и поэкземплярного учета.



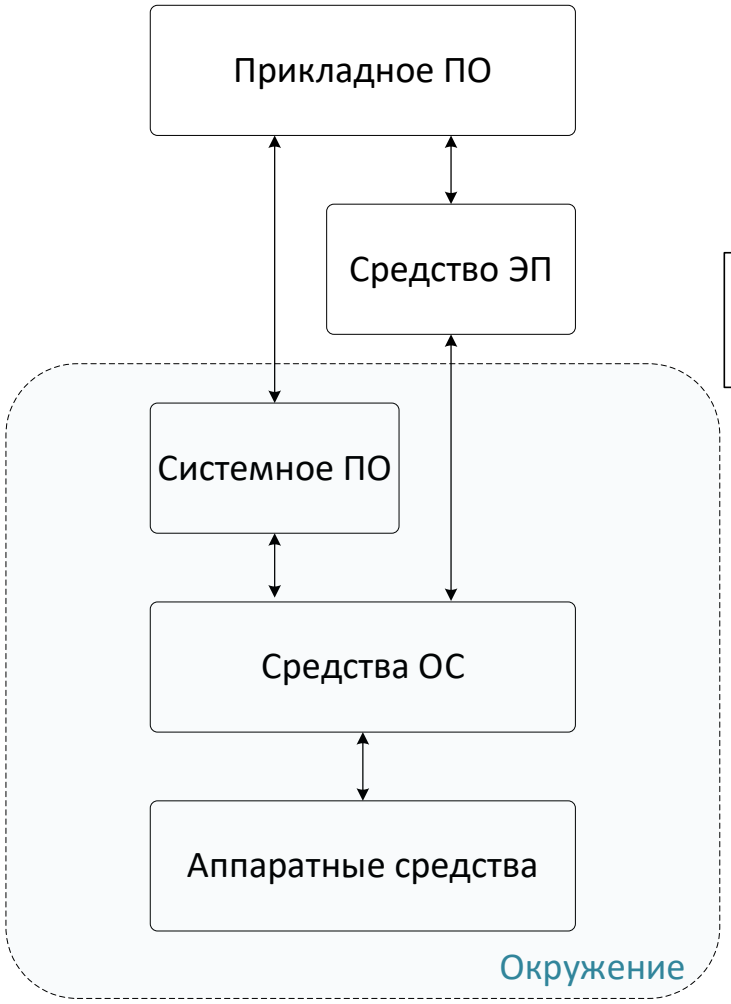
Проблемы: практика



- Недопустимость работы на старых версиях ОС.
- Защищенные соединения с web-страницами по ГОСТ – нетривиальная работа с WebView.
- Специфика импорта/экспорта ключей.
- Малоприменимость контактных считывателей и физически подключаемых токенов.
- Принципиальная невозможность повышения класса программной части средства выше КС1.



Проблемы: теория



КРИПТОПРО

Пути решения

- Защищенный канал с бесконтактными считывателями (NFC, Bluetooth).
- Взаимная аутентификация с внешними устройствами по SESPAKE.
- Частичный перенос операций на серверную сторону:
  - Дистанционное формирование электронной подписи (напр., КриптоПро DSS).
  - Реализация интеграции с внешними ИС на серверной стороне (напр., КриптоПро CSP, Госключ).
- Применение протокольных решений, предназначенных для работы в слабодоверенном окружении (в т.ч. российские криптонаборы TLS).
- Специализированные технические и математические решения для защиты от сбоев используемых датчиков случайных чисел.

Вопросы

1. Практический опыт решения указанных проблем.
2. Есть ли что-то, что не укладывается в существующую практику и требования к СЭП?
3. «Локальная» и «дистанционная» подпись: взаимоисключающие или совместно работающие подходы?
4. Доверенные российские ОС и аппаратные средства – мнение о перспективах для использования с массовой мобильной ЭП.
5. Повышение классов защиты решений, использующих мобильную ЭП: подходы.
6. Ключевые носители для мобильных устройств: токены с NFC, SIM-карты, ПЭН (УЛГ).

Дополнительно: Примеры дистанционного получения услуг

- Дистанционное получение сертификатов электронной подписи
- Дистанционное предоставление услуг ФЛ и ЮЛ, требующих конфиденциального канала взаимодействия
- Системы дистанционного формирования электронной подписи
- Протоколы дистанционного электронного голосования
- Протоколы, предполагающие дистанционную идентификацию личности

– в части соответствия требованиям по безопасности требуют TLS с ГОСТ с использованием сертифицированных СКЗИ в качестве фундамента.

Дополнительно: TLS с ГОСТ

- Необходимым условием для безопасности любой дистанционной услуги через Интернет является защищенное TLS-соединение.
  - Порталы дистанционного банковского обслуживания.
  - Системы дистанционного электронного голосования.
  - Почтовые сервисы.
  - Системы государственных и муниципальных услуг.
  - Дистанционная выдача сертификатов ключей проверки ЭП.
  - ЕСИА, ЕБС, идентификация и аутентификация на сторонних ресурсах.
- Веб-сайты в России оснащены TLS-сертификатами, выданными зарубежными удостоверяющими центрами. Риск отзыва TLS-сертификата. Прецеденты были: отзыв TLS-сертификата Общественной Палаты РФ 4 июня 2018 года.
- На решение проблемы направлено поручение Президента от 16 июля 2016 года № Пр-1380, дорожные карты.

Дополнительно: Что есть для TLS

- В 2021 году планируется введение в действие НУЦ (Национального Удостоверяющего Центра), будут созданы условия для выдачи TLS-сертификатов безопасности государственным ресурсам.
- Разработаны и начинают внедряться серверные средства, поддерживающие как зарубежные, так и российские криптонаборы TLS (необходимо для плавного, бесшовного внедрения).
- Разработаны и начинают внедряться SDK для создания мобильных приложений с поддержкой TLS с ГОСТ для ОС iOS, Android.
- Браузеры с поддержкой TLS с ГОСТ: Яндекс.Браузер, «Спутник», браузеры в составе Astra Linux и ALT Linux (Chromium GOST, Firefox GOST), модули для Internet Explorer.
- Средства удостоверяющего центра, клиентские и серверные решения для OCSP.

Дополнительно: Что требуется для TLS

- Условия для выполнения первого требования создаются (все средства есть).
- Требуется также массовое внедрение отечественных TLS-сертификатов не только на веб-сайты ОГВ: веб-сайты коммерческих компаний, социальных сетей, блогов.
- Задача аналогична массовому переводу веб-сайтов с http на https в начале 2000-х (окончательный успех – после появления ACME и Let’s Encrypt).
- Максимально безопасное получение сертификатов для веб-сайтов ОГВ.
- Обеспечить условия для получения отечественных TLS-сертификатов одновременно с приобретением доменного имени
- Обеспечить возможность владельцам сайтов быстро получать отечественные TLS-сертификаты на свои сайты – с помощью механизмов автоматического получения сертификатов с пониженным, по сравнению с очным получением, уровнем доверия (зарубежный пример: Let’s Encrypt, получение сертификатов онлайн) – требуется разработка и стандартизация протоколов ACME с ГОСТ.