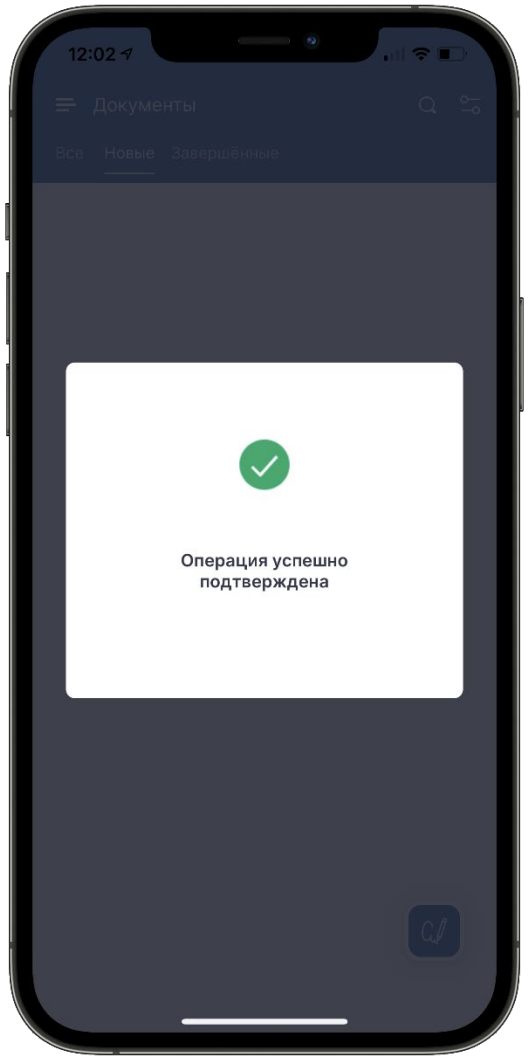
Мобильная электронная подпись: актуальные задачи и пути их решения

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

PKI-Форум Россия 2022

Трудности «мобильной ЭП»: техника

- Ограниченное доверие к среде функционирования: уязвимости ОС, условия применения, ДСЧ.
- Трудности реализации всех аспектов работы с ЭП на стороне мобильного устройства.
- Защищенные соединения с web-страницами по ГОСТ – трудности с WebView.
- Малоприменимость контактных считывателей и физически подключаемых токенов.
- И т.д.



- Специализированные технические и математические решения для работы в слабодоверенном окружении, ТК 26.
- Перенос части операций на серверную сторону: формирование документов, проверка корректности средства.
- Разработка альтернативного http-стека для работы WebView через TLS с ГОСТ.
- Защищенный канал с бесконтактными считывателями (NFC, Bluetooth): Secure Messaging и протокол SESPAKE.
- И т.п.

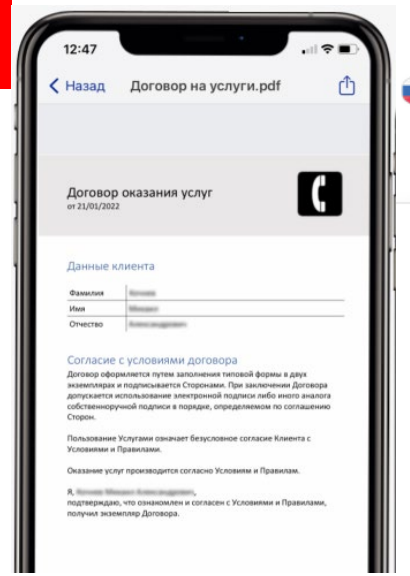
Опыт массового использования: 2021

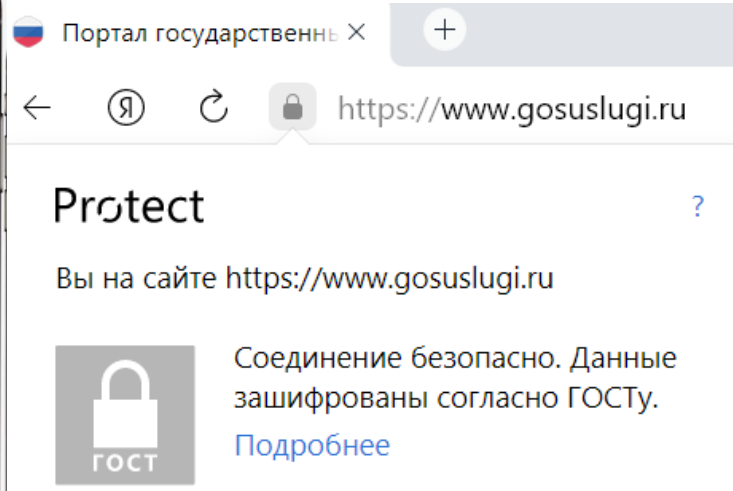
- Мобильные приложения с поддержкой функционала электронной подписи (УНЭП/УКЭП) – с «локальным», «облачным» и «гибридным» (с защитой ключа на сервере) хранением ключа.

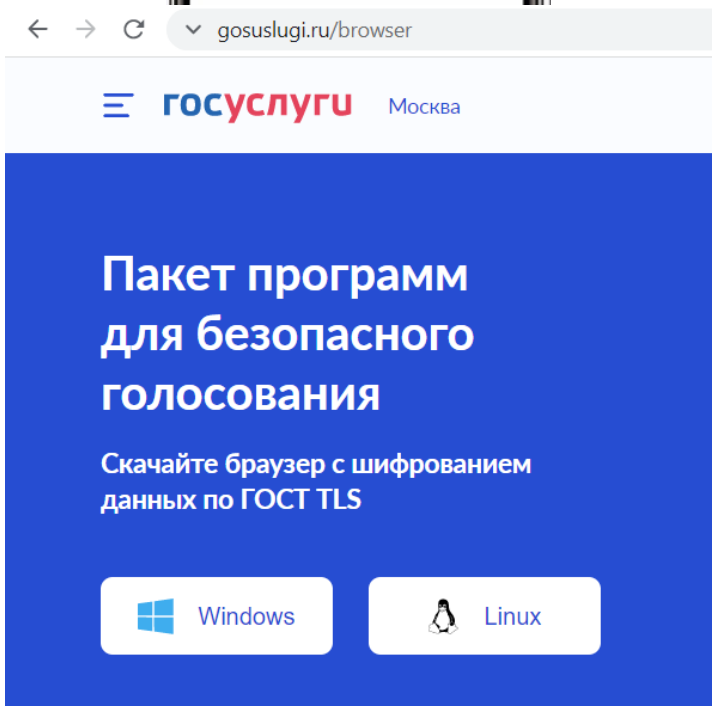
- Системы дистанционного электронного голосования с применением мобильных приложений.

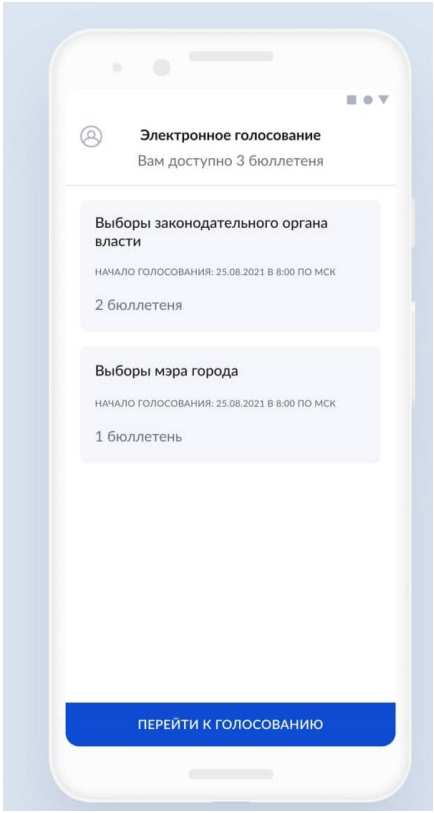
- Поддержка веб-сайтами и системами идентификации и аутентификации TLS с ГОСТ.

– **массовые** СКЗИ/СЭП класса КС1.



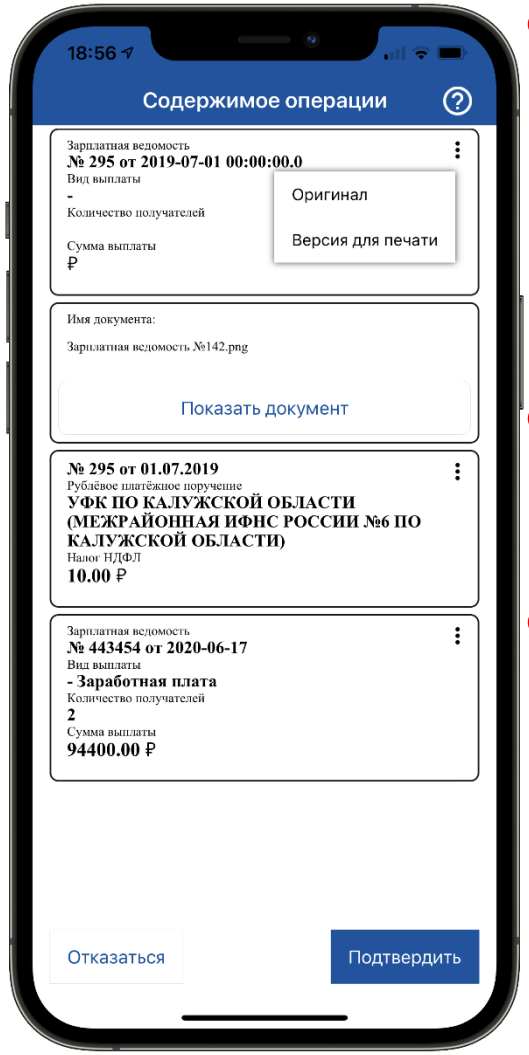




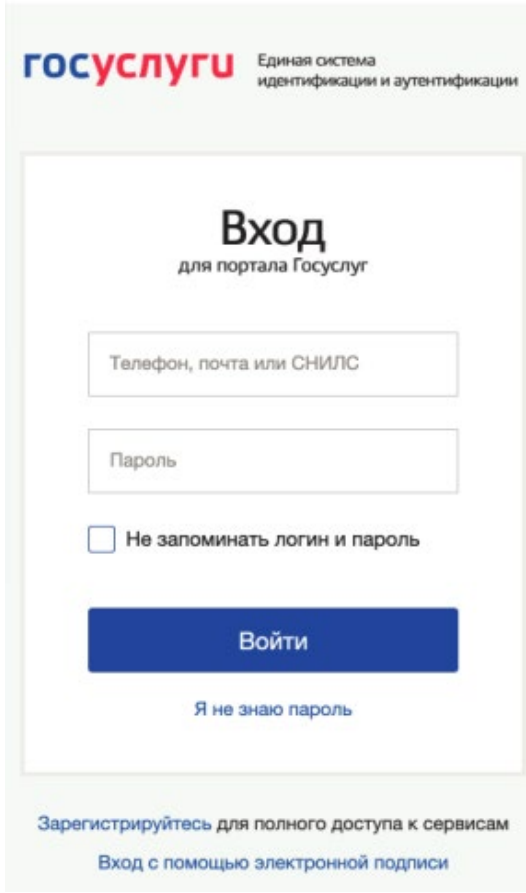


КРИПТОПРО

Мобильная подпись: задачи



- Априори более высокий риск потери или кражи устройства, подходы к хранению ключей
  - «Облачная»/«локальная» и «гибридная» подпись: преимущества и недостатки подходов.
  - Нормативная база в части «облачной» подписи.
  - Специализированные ключевые носители: ПЭН, SIM.
- Способы идентификации
  - Для УКЭП: ЕСИА/ЕБС, старый сертификат, загранпаспорт, **личная явка**.
- Новые трудности
  - Удаление из магазинов приложений российских МП.
  - Уязвимости в импортируемых компонентах кода
  - Риски блокировки магазинов приложений и удаленной блокировки устройств граждан.
  - Отзыв TLS-сертификатов, выданных международными УЦ – в случае мобильных приложений решается переходом на TLS с ГОСТ и российские сертификаты.



Мобильная подпись: общие вопросы

- ЭП как самостоятельный продукт – или только в составе сервиса?
- Можно ли (и нужно ли) сохранить единственность ключа ЭП одного владельца?
  - Использование со стационарного рабочего места ключа ЭП, привязанного к МП.
  - Использование с мобильного приложения ключа ЭП на отчуждаемом ключевом носителе.
  - Будущее ключевых носителей.
- Защита владельца ключа с учетом риска утери мобильного устройства.
- Возможность развития прикладного функционала МП без доп. заключения ФСБ.
  - Задача изменения прикладной составляющей МП со встроенным СКЗИ («SDK с супербелыми функциями»).
  - Пониженное доверие к среде функционирования и к вызывающим СКЗИ прикладным компонентам.

Вопросы к обсуждению

1. В каких случаях «мобильная подпись» имеет смысл как самостоятельный продукт? Или её ценность возникает только в качестве компонента сервиса, решающего прикладную задачу? И в этом случае требуется ли именно УКЭП?
2. Способы идентификации владельцев сертификатов: чего не хватает для счастья?
3. «Облачный», «локальный» и «гибридный» подходы к хранению ключей: преимущества и недостатки.
4. Будущее использования ключевых носителей: «классическая подпись» как альтернатива «мобильной подписи» или сосуществование в рамках разных сценариев работы?