Перспективы развития российской криптографии для массового пользователя

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

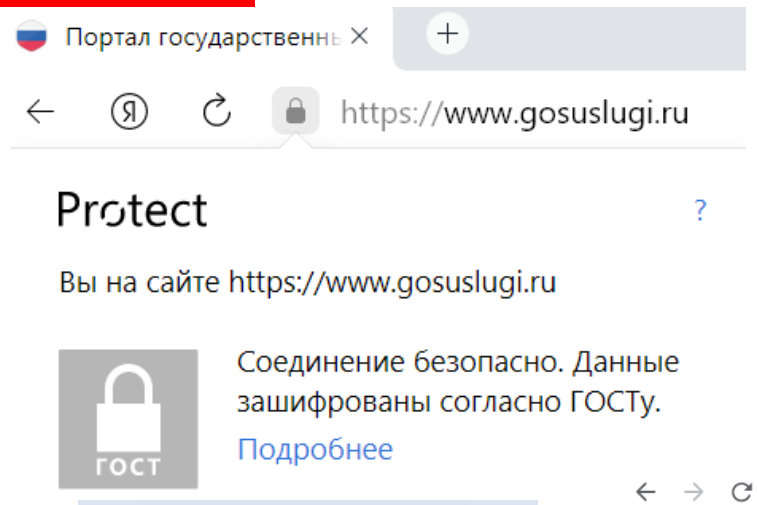
КРИПТОПРО

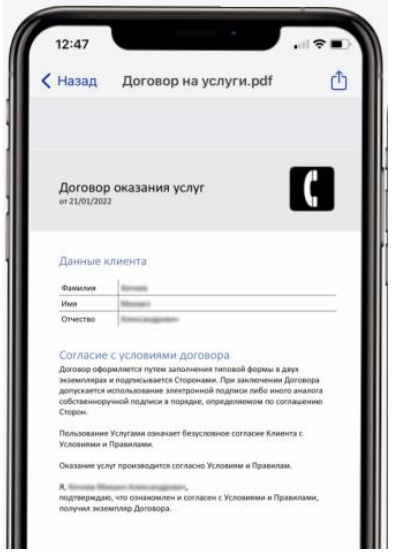
РусКрипто’2022

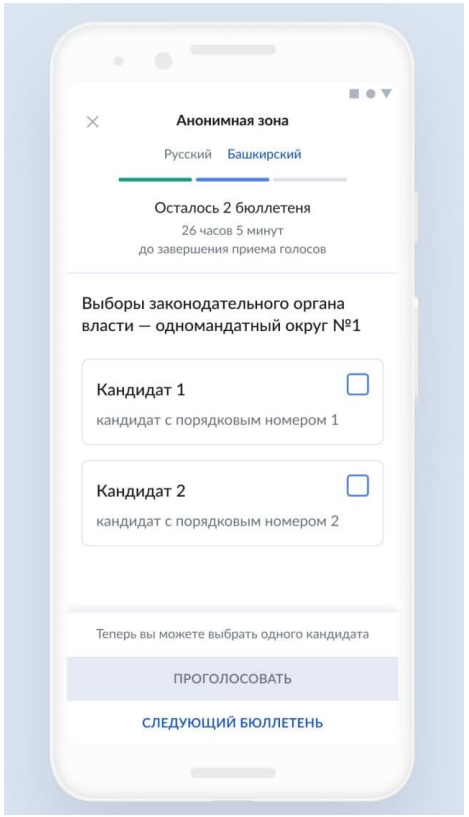
Опыт массового использования: 2021

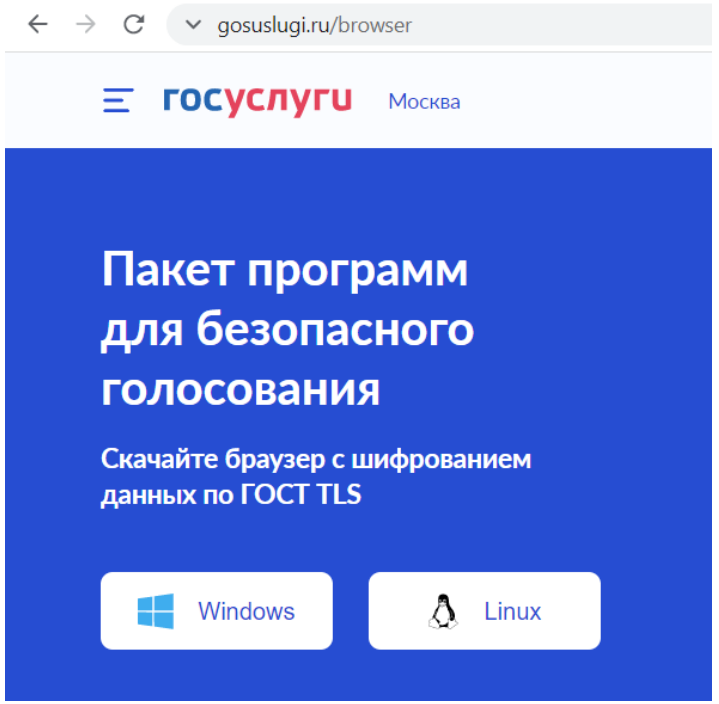
- Мобильные приложения с поддержкой функционала электронной подписи – локальной и гибридной (с защитой ключа на сервере).
- Системы дистанционного электронного голосования с применением мобильных приложений.
- Поддержка ГОСТ в браузере «из коробки».

– **массовые** СКЗИ/СЭП класса КС1.

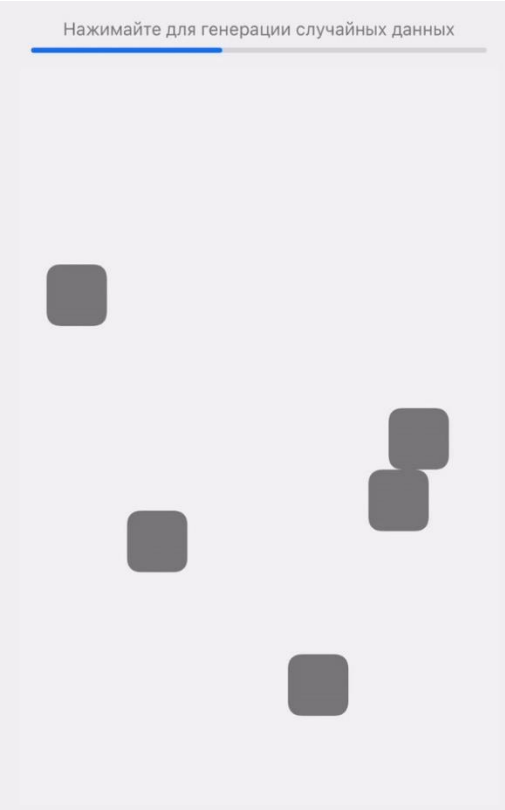




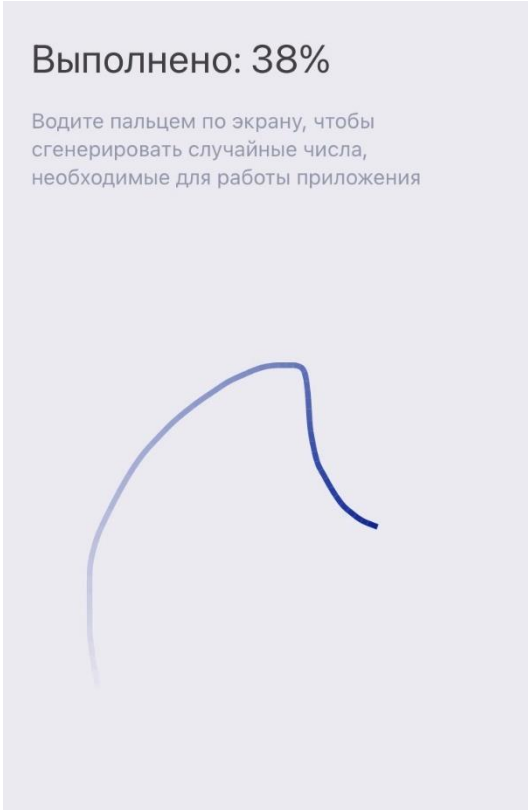




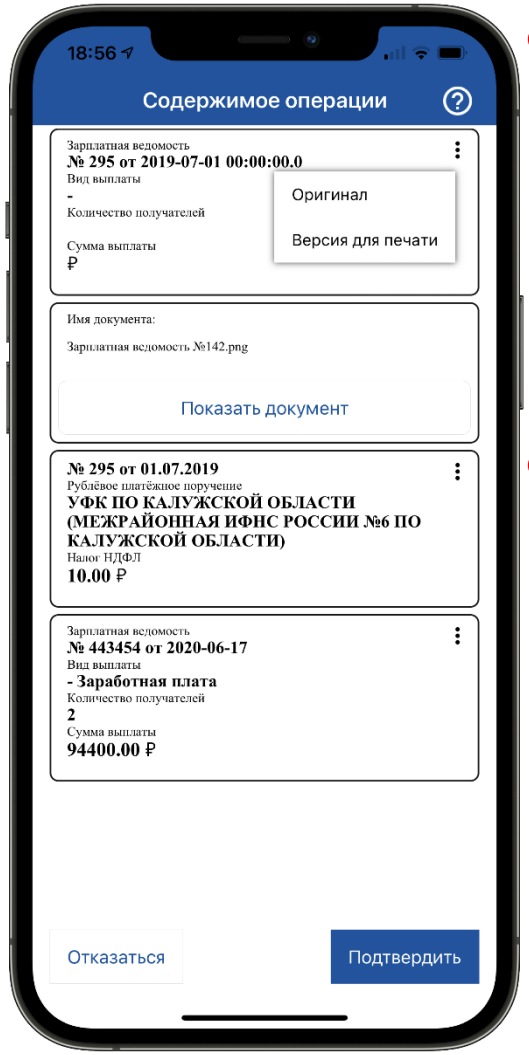
Трудности: удобство



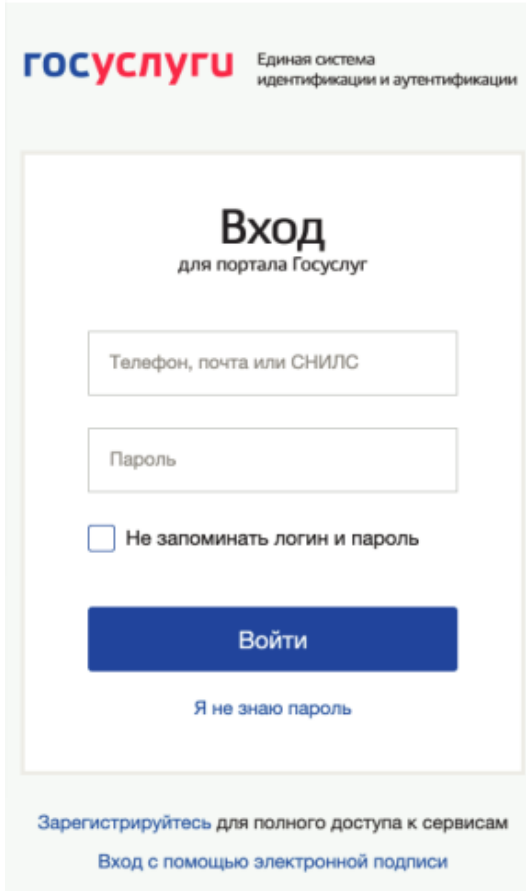
- Использование сертифицированной криптографии требует дополнительных действий от пользователя:
  - Инициализация ДСЧ.
  - Контроль целостности.
  - Локальная аутентификация.
- Проблема обновления версий мобильного приложения.
- Недопустимость работы на старых версиях ОС.
- Проблема лицензионного контроля и поэкземплярного учета.



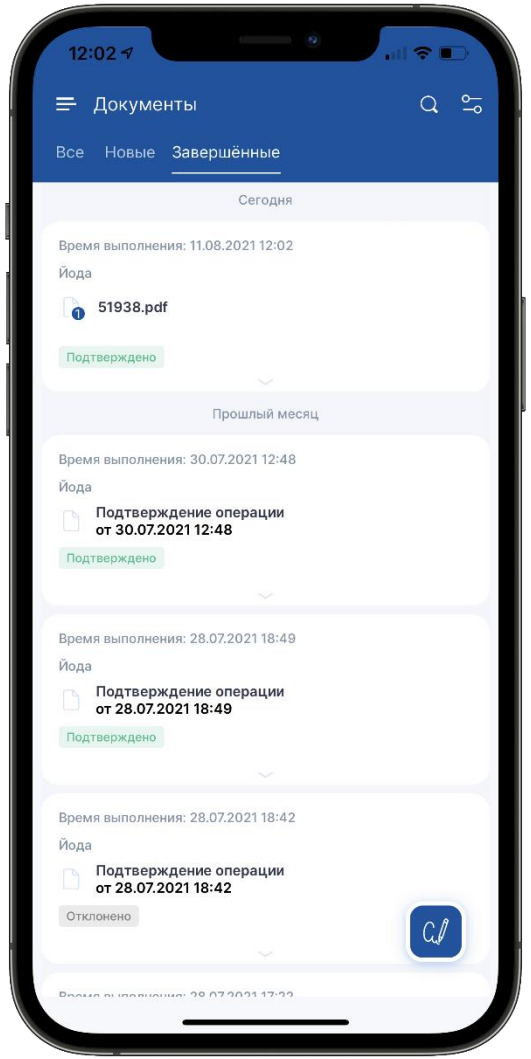
Трудности: безопасность



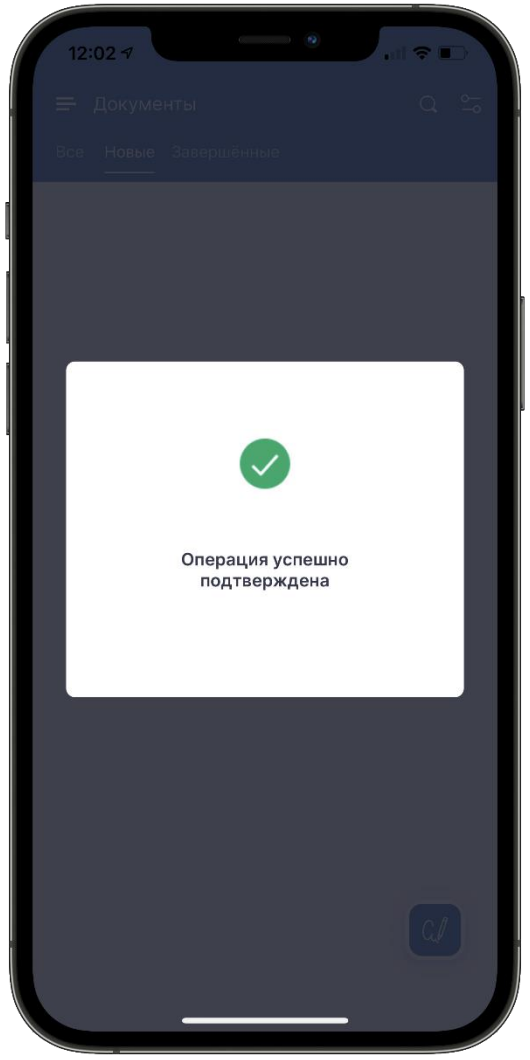
- В большинстве случаев документ требуется загружать с сервера.
  - Передача полного документа – большой объем данных.
  - Передача хэш-значения – требование доверия к платформе подписания.
- Новые проблемы.
  - Риск блокировки магазинов приложений.
  - Риск отзыва российских мобильных приложений.
  - Риск удаленной блокировки устройств граждан.
  - Отзыв TLS-сертификатов, выданных международными УЦ – в случае мобильных приложений решается переходом на TLS с ГОСТ и российские сертификаты.
- Априори более высокий риск потери или кражи устройства – новые требования к ключевой системе.



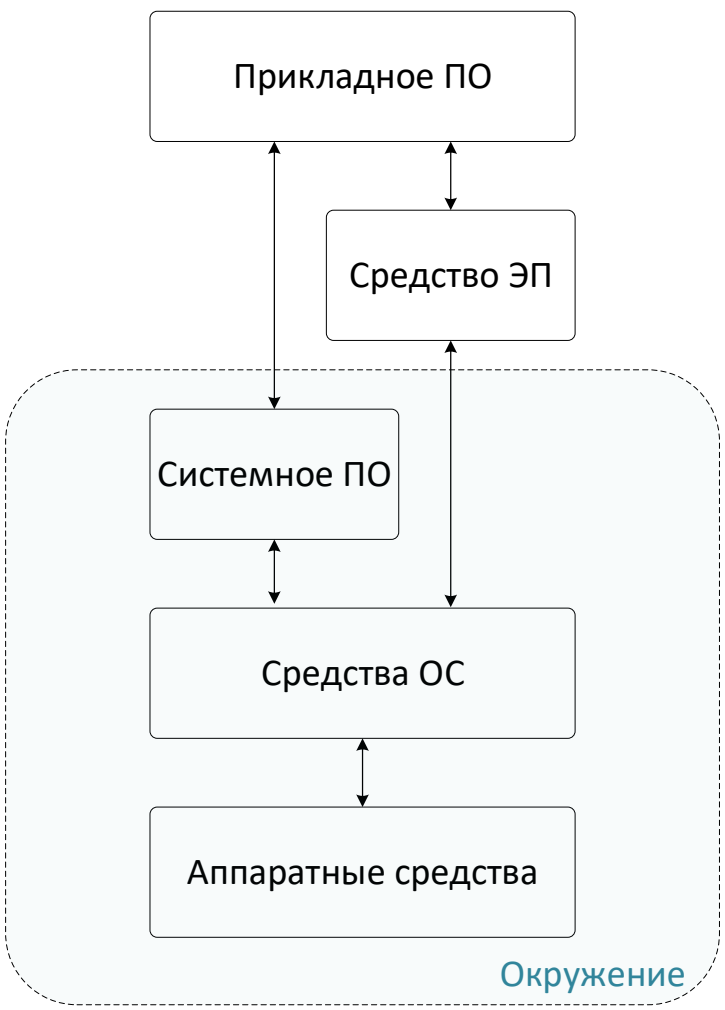
Трудности: разработка



- Защищенные соединения с web-страницами по TLS с 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.



Причины трудностей



- «Зашитая» в код операционной системы криптография в ряде случаев не позволяет её заменять сторонними реализациями.

⇒ Усложнение разработки и встраивания.

- Критичность последствий инцидентов безопасности в случае криптографических модулей существенно превышают типичную для мобильных приложений

⇒ Необходимость применять дополнительные механизмы обеспечения безопасности.

- Отсутствие возможности использования специализированных доверенных компонент.

⇒ Необходимость ограничивать класс защиты и дублировать в средстве ЭП часть функционала окружения.

КРИПТОПРО

Проблема доверия к источникам случайности

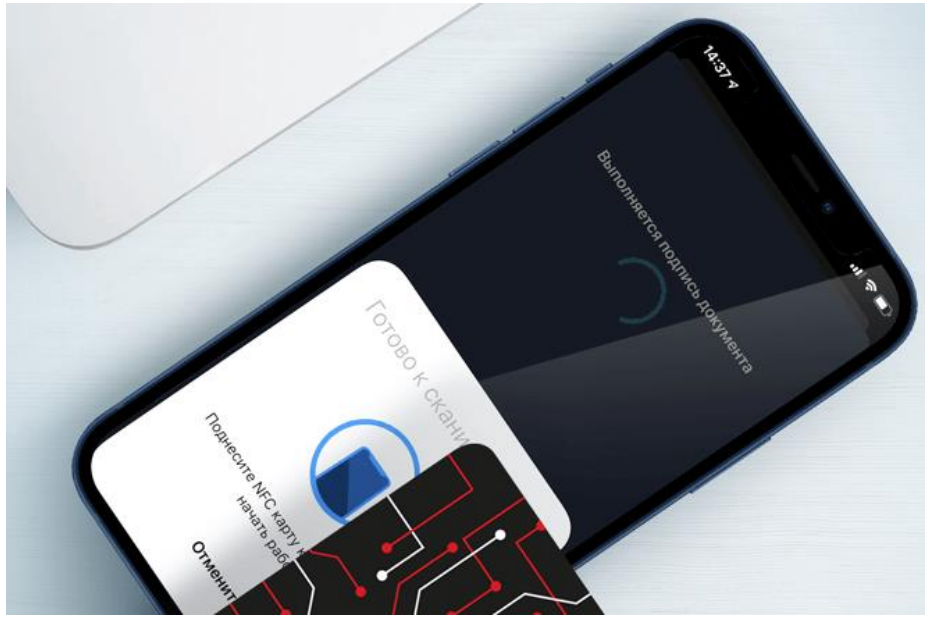
- Сбои устройств или намеренно внесенные уязвимости – даже в случае малой вероятности сбоя в случае массово используемых устройств последствия могут быть критическими.
  - Пример: смарт-карты граждан в Эстонии.
  - Путь решения: протоколы вычисления ЭП в усиленной модели нарушителя, внедрение элементов доказательств с нулевым разглашением – криптографические задачи по синтезу и анализу протоколов (есть законченные положительные результаты, есть новые задачи).
- Сбои СПО устройств, приводящие к вырождению/клонированию состояния ПДСЧ.
  - Риски: компрометация долговременных ключей с атакой по публично доступным значениям ЭП.
  - Гибридные реализации схемы ЭП с совмещением детерминированных и рандомизированных значений – криптографические задачи по синтезу и анализу протоколов (есть законченные положительные результаты, есть новые задачи).

Проблема хранения ключей

- Память устройства
- Специализированное устройство с доступом через сервер
  - SIM-карта
  - Паспорт с электронным носителем (ПЭН)
- Память устройства, под защитой серверного ключа – криптографические задачи по синтезу и анализу протоколов.
- «Облако». Задачи по маршрутизации документов между ИС и серверами дистанционной подписи.
- Токен или смарт-карта, доступ по бесконтактным интерфейсам – криптографические задачи по синтезу и анализу протоколов (есть законченные положительные результаты, есть новые задачи).

Защита взаимодействия с ключевыми носителями

- Условия использования ключевых носителей:
  - Бесконтактное взаимодействие (Bluetooth, NFC) – по незащищенному каналу.
  - Отсутствие практической возможности аутентифицировать взаимодействие чем-либо, кроме пароля.



- Защищенный канал с бесконтактными считывателями (NFC, Bluetooth) с взаимной аутентификацией по низкоэнтропийным данным: протокол SESPAKE.
  - RFC 8133.
  - Р 50.1.115–2016 "Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля“
- Поддержан в основных массовых СКЗИ и носителях:
  - Рутокен ЭЦП
  - JaCarta
  - Токен++
  - Паспорт с электронным носителем

Проблема утечки данных в оперативной памяти

- Компрометация сессионных ключей в некоторый момент времени
  - Утечка памяти из-за уязвимостей среды (пример: Heartbleed).
  - Выгрузка данных при небезопасном резервном копировании/сохранении состояния виртуальной машины.
  - Атаки по побочным каналам.

1. Attacking at a distance of up to 1 *m* (30 *cm* in realistic conditions; "TEMPEST"),
2. Using minimal equipment (fits in a jacket pocket, costs less than €200) and
3. Needing only a few minutes (5 minutes for 1 *m* and 50 seconds for 30 *cm*).

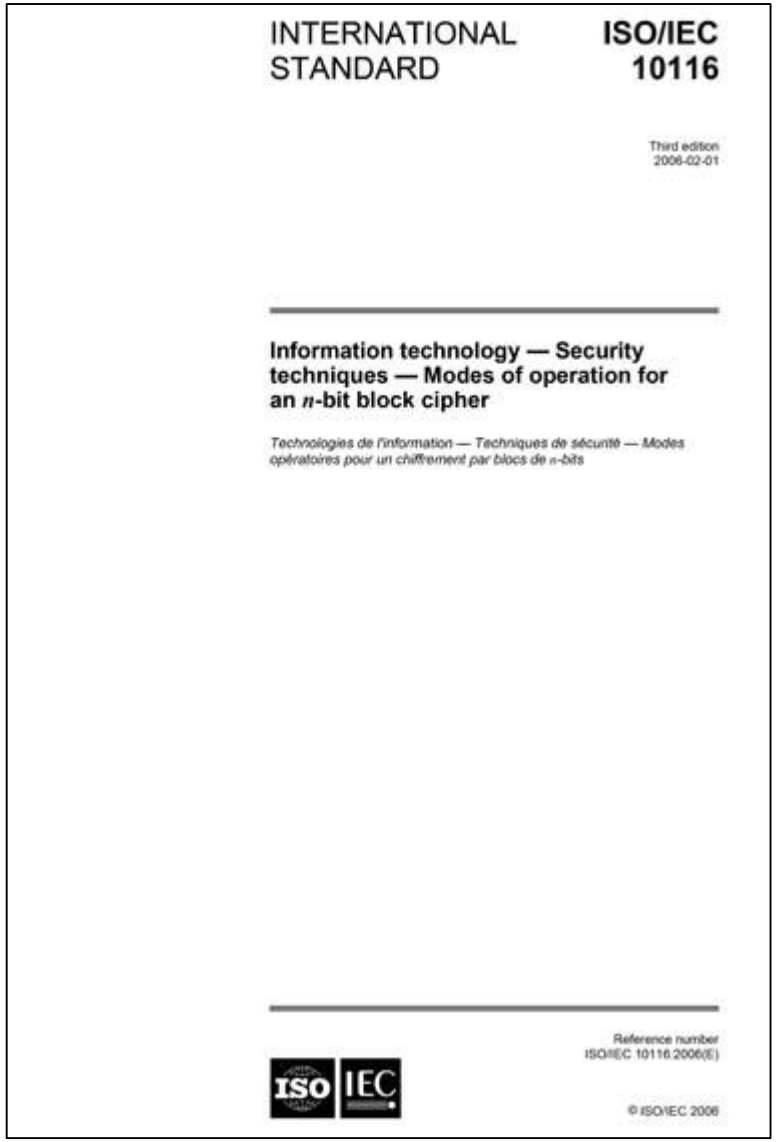
- Путь решения: механизмы регулярной смены ключей – криптографические задачи по синтезу и анализу протоколов (есть законченные положительные результаты, есть новые задачи).

- Стандартизация.

ISO/IEC 10116:2017/AMD 1:2021

- «Information technology — Security techniques — Modes of operation for an n-bit block cipher»
- Дополнение к международному стандарту ISO/IEC 10116:2017, содержащее описание режима шифрования CTR-ACPKM.

- Ранее был утвержден в:
  - Рекомендациях по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования».
  - RFC 8645 (CFRG): Re-keying Mechanisms for Symmetric Keys.


INTERNATIONAL STANDARD

ISO/IEC 10116

Third edition
2006-02-01

Information technology — Security techniques — Modes of operation for an *n*-bit block cipher

Technologies de l'information — Techniques de sécurité — Modes opératoires pour un chiffrement par blocs de n-bits

Reference number
ISO/IEC 10116:2006(E)

ISO IEC

© ISO/IEC 2006

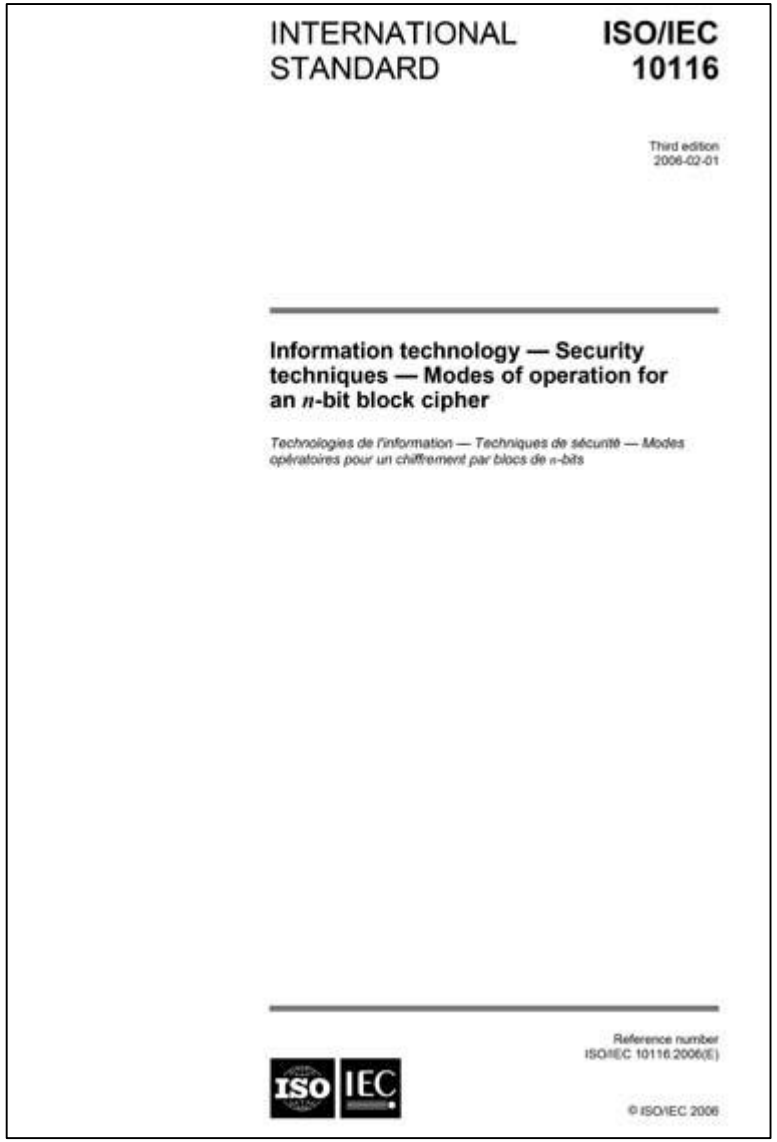
ISO/IEC 10116:2017/AMD 1:2021

- CTR-ACPKM стал в международном стандарте ISO наряду с разработанными более 30 лет назад классическими режимами
  - ECB (простой замены),
  - CTR (гаммирования),
  - CFB (гаммирования с обратной связью по шифртексту),
  - CBC (простой замены с зацеплением),
  - OFB (гаммирования с обратной связью по выходу),

шестым режимом работы блочных симметричных алгоритмов

  - **CTR-ACPKM** (гаммирования с преобразованием ключей).

- Применяется в:
  - CMS: Р 1323565.1.025–2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами»
  - TLS 1.2: Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»


INTERNATIONAL STANDARD

ISO/IEC 10116

Third edition
2006-02-01

Information technology — Security techniques — Modes of operation for an *n*-bit block cipher

Technologies de l'information — Techniques de sécurité — Modes opératoires pour un chiffrement par blocs de n-bits

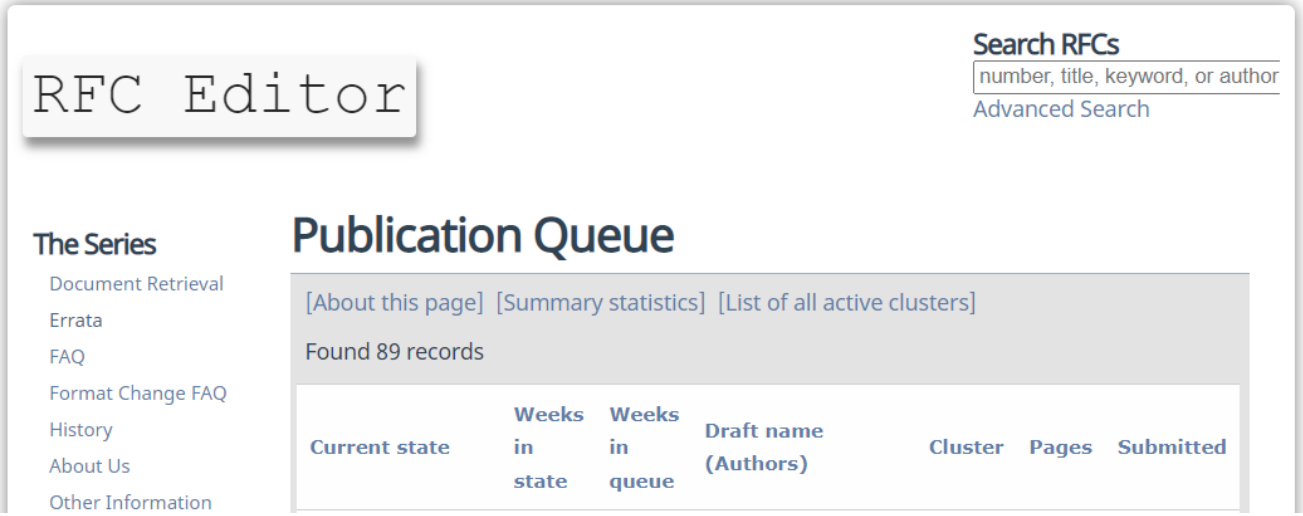
Reference number
ISO/IEC 10116:2006(E)

© ISO/IEC 2006

Стандартизация: IETF

- **RFC 9189**, «GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.2», **March 2022**. Stanislav Smyshlyaev, Dmitry Belyavskiy, Evgeny Alekseev.
- **RFC 9215**, «Using GOST R 34.10-2012 and GOST R 34.11-2012 algorithms with the Internet X.509 Public Key Infrastructure», **March 2022.** Dmitry Baryshkov, Vasily Nikolaev, Aleksandr Chelpanov.

- RFC 9058, «Multilinear Galois Mode (MGM)», June 2021. Stanislav Smyshlyaev, Vladislav Nozdrunov, Vasily Shishkin, Ekaterina Griboedova.

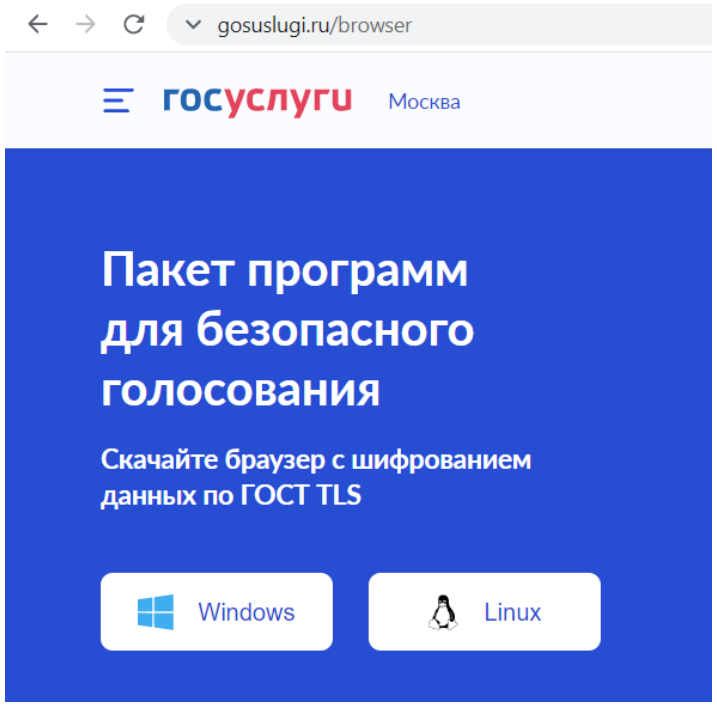


- draft-smyslov-esp-gost, «Using GOST ciphers in ESP and IKEv2», Valery Smyslov.

Заключение.
Продвижения в решении задач

- Первые массовые мобильные приложения и браузеры с российской криптографией.

- Протокольные решения, предназначенные для работы в слабодоверенном окружении, стандартизация.
  - CTR-ACPKM, TLS 1.2 с ГОСТ, режим MGM.
  - Защищенный канал с бесконтактными считывателями (NFC, Bluetooth): SESPAKE.
- Специализированные технические и математические решения для защиты от сбоев используемых ДСЧ.
- Поддержка TLS с ГОСТ на мобильных устройствах, в браузере и на серверной стороне.
  - Программные и программно-аппаратные решения различных производителей для TLS-серверов..
  - Поддержка в браузерах: Яндекс.Браузер с ГОСТ.



Заключение. Актуальные теоретические и практические задачи

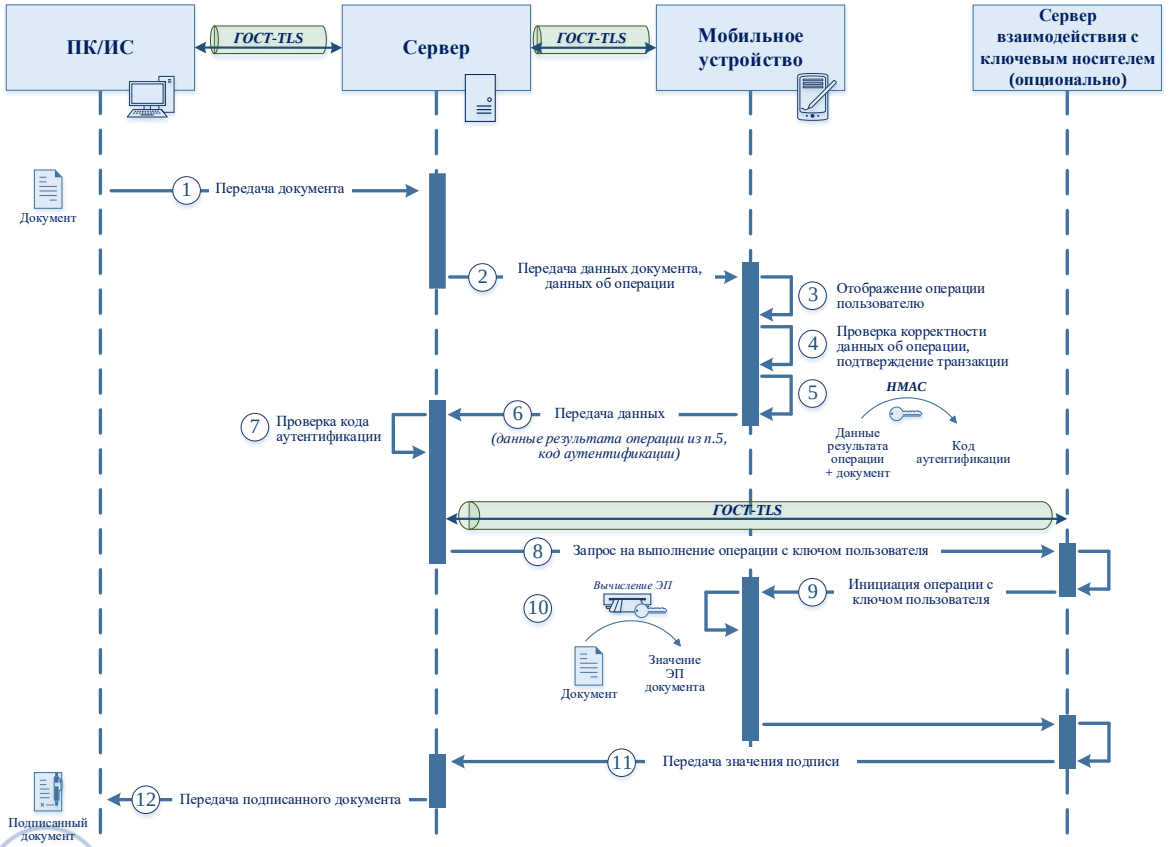
- Синтез и анализ криптографических протоколов формирования ЭП в рамках клиент-серверного взаимодействия в усиленных моделях нарушителя.
- Дальнейшее развитие криптографических механизмов для обеспечения защиты информации в условиях слабодоверенного окружения.
- Повышение надежности и защищенности способов доставки мобильных приложений, браузеров и корневых сертификатов.
- Создание законченных защищенных «коробочных» решений для поддержки ЭП с применением мобильных устройств для простой и безопасной интеграции с существующими ИС – в том числе, с поддержкой различных вариантов хранения ключей ЭП и получения сертификатов.
- **Разработка/развитие и сертификация высокоуровневых SDK для дальнейшего упрощения встраивания криптографии в мобильные приложения.**

Спасибо за внимание!

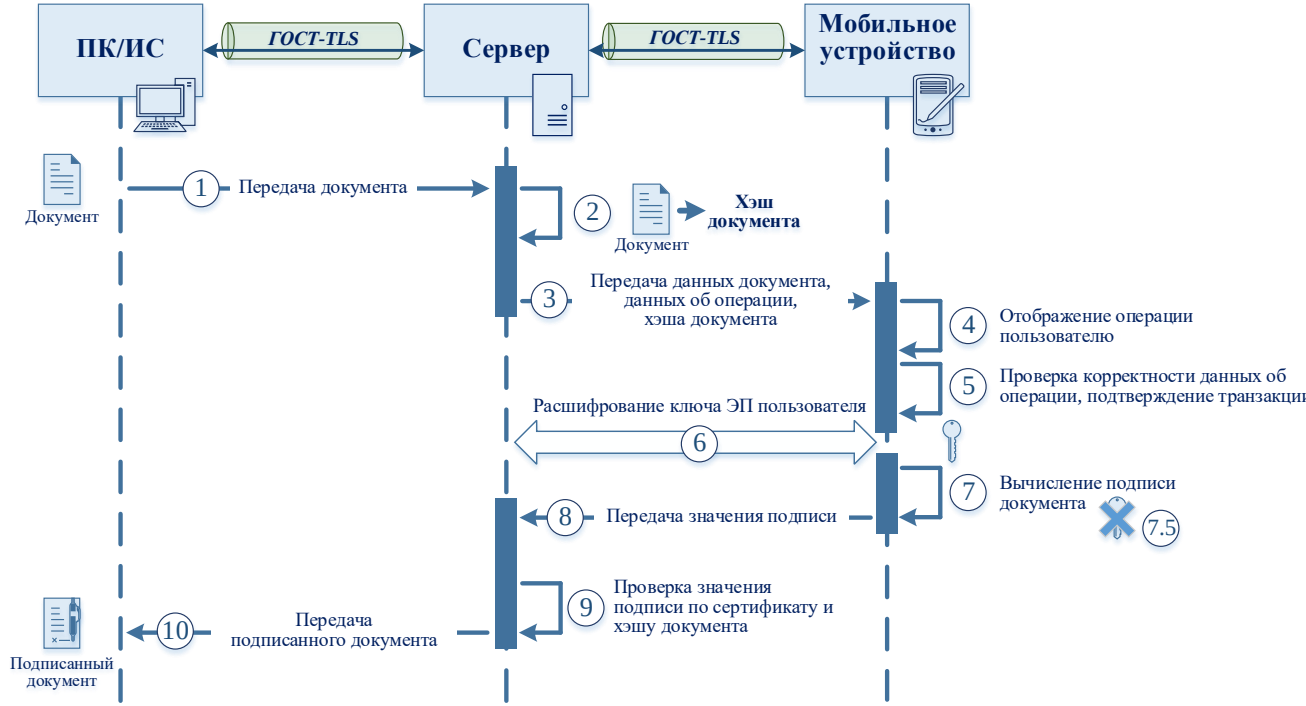
Дополнительные слайды

Проблема хранения ключей

- Специализированное устройство с доступом через сервер
  - SIM-карта
  - Паспорт с электронным носителем (ПЭН)

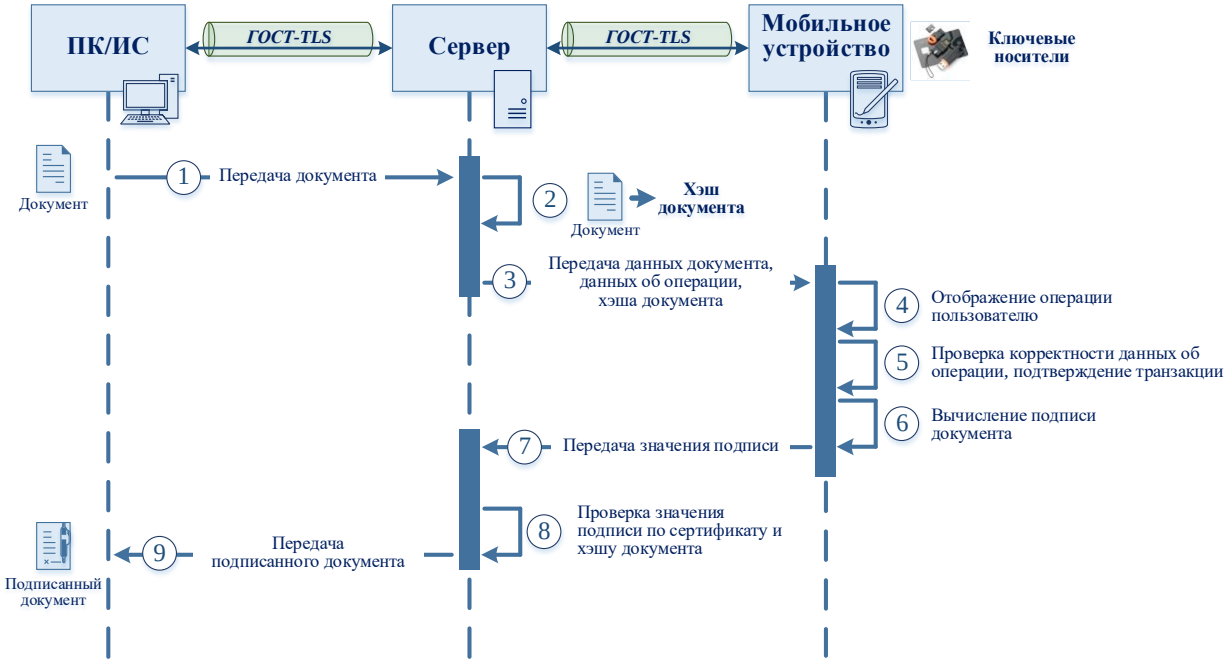


- Память устройства, под защитой серверного ключа – криптографические задачи по синтезу и анализу протоколов



Проблема хранения ключей

- Память устройства
- Токен или смарт-карта



- «Облако»