Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

# Криптографические протоколы нового десятилетия с поддержкой российских алгоритмов

Станислав Смышляев, к.ф.-м.н.,
Заместитель генерального директора, КриптоПро

# 2011 год:

- ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ 28147-89
- Проприетарные реализации TLS, IPsec, CMS.
- Нет документов по стандартизации для криптографических протоколов.
- RFC и драфты IETF для части механизмов.
- Нет идентификаторов IANA – в России используются идентификаторы из приватной области.

# 2021 год:

- ГОСТ 34.10-2018, ГОСТ 34.11-2018, ГОСТ 34.12-2018, ГОСТ 34.13-2018
- Р 1323565.1.025–2019: Форматы сообщений, защищенных криптографическими методами – CMS
- Р 1323565.1.020-2020: Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)
- Р 1323565.1.030-2020: Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3) – внедрение одновременно со всем миром
- Р 1323565.1.035–2020: Использование российских криптографических алгоритмов в протоколе защиты информации ESP; ТС по IKEv1, работа по IKEv2 – 2021 год
- Р 1323565.1.034–2020: Протокол безопасности сетевого уровня, Iplir
- Р 1323565.1.033–2020: Использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML
- Стенды встречного тестирования по TLS 1.2, TLS 1.3, IPsec.
- Идентификаторы IANA по TLS 1.2, по TLS 1.3, по ESP и IKEv2

**Для всех основных протоколов массовой криптографии решены задачи по определению порядка использования российских алгоритмов.**

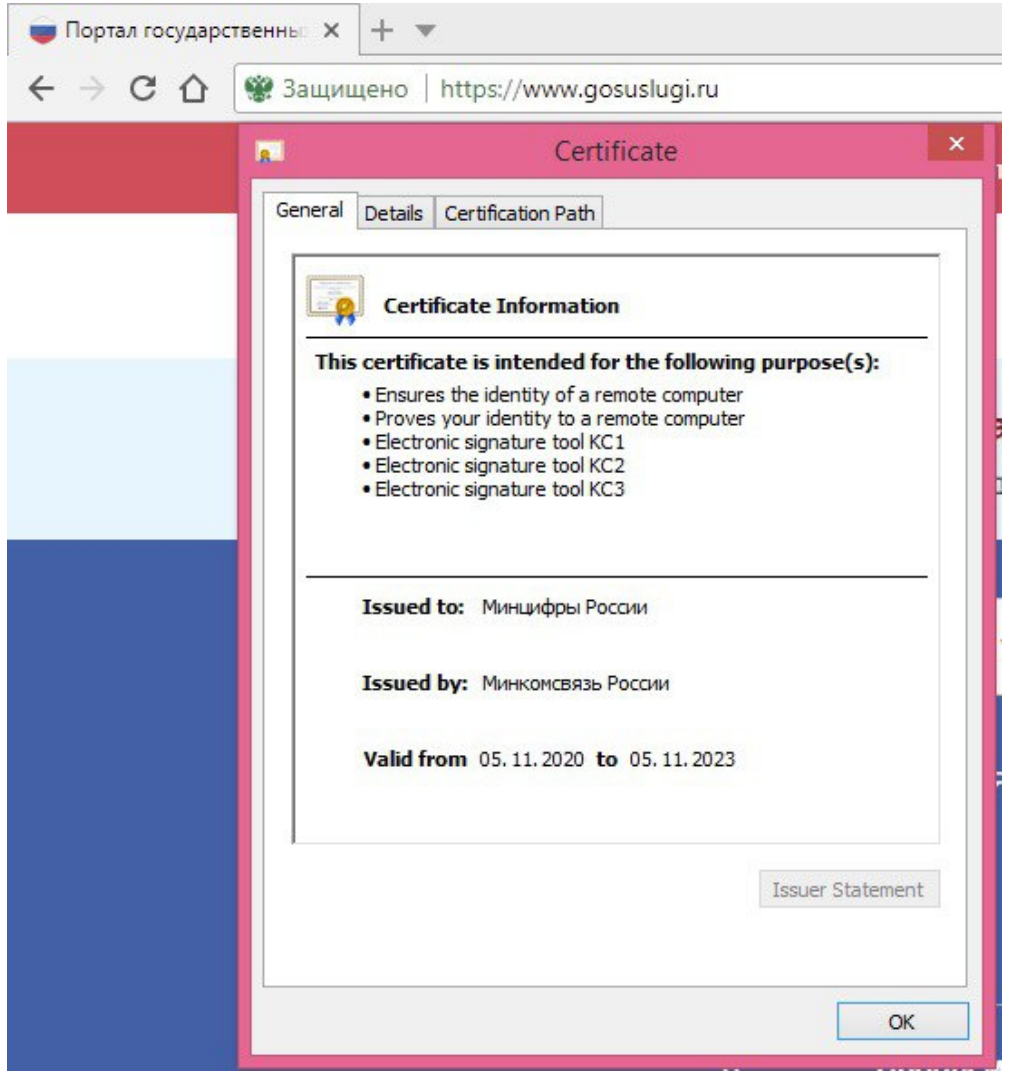
# TLS с ГОСТ: поддержка на сайтах

Защищено

- https://lkul.nalog.ru – личный кабинет налогоплательщика (юридического лица).
- https://eruz.zakupki.gov.ru/auth/ – единая информационная система в сфере закупок
- https://agregatoreat.ru – единый агрегатор торговли (по 44-ФЗ)
- https://cryptopro.ru – сайт КриптоПро

Февраль 2021:

- https://gosuslugi.ru
  – Единый Портал Государственных Услуг



# Получение серверных TLS-сертификатов

- Вводится в действие Национальный Удостоверяющий Центр
- Для защиты от угрозы отзыва зарубежных сертификатов важно выполнить два требования:
  - Основные веб-сайты оснащены вторым (отечественным) TLS-сертификатом
  - Большинство пользователей применяют ПО, поддерживающее отечественные TLS-сертификаты.
- Условия для выполнения первого требования создаются (все средства есть).
- Требуется также массовое внедрение отечественных TLS-сертификатов не только на веб-сайты органов государственной власти: 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.

# Получение серверных TLS-сертификатов

- Максимально безопасное получение сертификатов для веб-сайтов органов государственной власти.
- Обеспечить условия для получения отечественных сертификатов безопасности одновременно с приобретением доменного имени
- Обеспечить возможность владельцам сайтов быстро и просто получать отечественные сертификаты безопасности 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.

# Развитие на созданном фундаменте

- Дистанционное получение сертификатов электронной подписи
- Дистанционное предоставление услуг ФЛ и ЮЛ, требующих конфиденциального канала взаимодействия
- Системы дистанционного формирования электронной подписи
- Протоколы дистанционного электронного голосования
- Общие задачи дистанционной идентификации личности

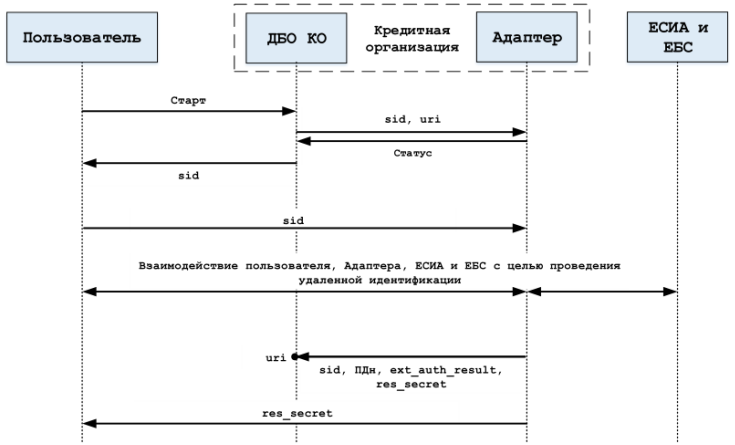
# Протоколы дистанционной регистрации

Требуют делегированной аутентификации и авторизации, строятся поверх TLS:

- Дистанционное получение сертификатов электронной подписи
- Удаленная идентификация новых клиентов банков
- Дистанционная регистрация в системах дистанционной («облачной») подписи
- Финансовые сервисы с дистанционным использованием

OpenID Connect – существуют сертифицированные решения, стандартизация в активной фазе.

OpenID Connect



# Протоколы для дистанционного электронного голосования

- Протокол подписи вслепую (разработка в ТК 26)
- Протоколы разделения секрета
- Протоколы распределенной выработки ключа
- Доказательства с нулевым разглашением

Требуется разработка и анализ порядка применения с ГОСТ (обсуждение на круглом столе «Технологии дистанционного электронного голосования. Задачи и перспективы», завтра в 15:30).

# Направления развития протоколов Интернета

- Оптимизация работы высоконагруженных TLS-серверов: в частности, за счет механизмов «пакетного подписания» Handshake.
- DTLS 1.3 – разработка порядка использования ГОСТ не начата.
- Механизмы повышения безопасности использования источников энтропии на серверной стороне: RFC 8937.
- ESNI (Encrypted Server Name Indication). Законопроект о запрете в РФ.
- Общее направление по защите от отслеживания пользователей, анонимизация + авторизация: “Privacy Pass” и VOPRF – отсутствуют аналоги с ГОСТ.
- Использование дополнительного ключевого материала, полученного с помощью «квантовых» и «постквантовых» механизмов (пример: RFC 8773).

# Использование постквантовых механизмов

- Постквантовые механизмы и порядок их использования их в протоколах
- Изогении на эллиптических кривых
- Подписи, основанные на деревьях Меркля и хэш-функциях – постквантовая криптография с доказанной стойкостью. Дополнительные сложности реализации.
- Подписи на основе теории кодирования и теории решеток.
- Проблемы больших открытых ключей и значений подписи.
- Отдельная рабочая группа «Постквантовые криптографические механизмы» в ТК 26 для разработки механизмов. Порядок использования в протоколах далее можно определять в РГ по протоколам.
- Подробнее – на секции «Криптография и криптоанализ».

# Перспективные протоколы защиты соединений

- Wireguard
  - Сам протокол намеренно не предполагает вариабельности криптоалгоритмов (“crypto agility”) ради упрощения реализаций.
  - При этом сам протокол устроен весьма продуманно с точки зрения криптографии, за счет минималистичности обеспечивает высокую производительность в реальных приложениях.
  - Проект «Ru-WireGuard».
- QUIC – экспериментальный протокол от Google, поверх UDP.
  - Со встроенной криптографией.
  - Механизмы безопасности – на основе «встроенного» TLS 1.3.

# Стандартизация и частные решения

- HPKE – внутренние интерфейсы «правильной» работы для криптосистем с открытым ключом.
  - Требуется ли отдельная стандартизация внутренних интерфейсов, индивидуальных в каждом протоколе?
- Криптография в мессенджерах, протоколы MLS.
  - Требуется ли стандартизировать протоколы, работающие априори внутри единого решения?
- Криптография в системах дистанционной подписи.
  - Стандартизация порядка взаимодействия компонент различных производителей важна: OpenID Connect, хабы электронной подписи.
  - Требуется ли стандартизировать протоколы, работающие априори внутри единого решения?

# Отраслевые протокольные решения

- Протоколы платежных систем (7 документов ТК 26 принято, работа продолжается).
- Протоколы сервисов электронной коммерции.
- Российские алгоритмы в GSMA, включая 5G.
- Протокол беспроводной передачи данных NB-Fi и LoRA
- Р 1323565.1.032-2020: Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS.
- Протоколы доверенной третьей стороны.

– на секциях «Российская и международная стандартизация», «Криптография и информационная безопасность в банковской сфере»

# Заключение

- Ряд активно развивающихся новых направлений массового использования российской криптографии:
  - Дистанционное электронное голосование, платежные системы, дистанционная электронная подпись, криптография в GSM, дистанционная идентификация, биометрические системы, электронная коммерция...
  - Готов и стандартизирован фундамент: алгоритмы (ГОСТ 34.1х-2018) и базовые протоколы (TLS, IPsec, CMS).
  - Развитию протоколов нужно время, но разрыв удалось сократить с 20 лет до 0.
  - Внимательно следим за перспективными протоколами на ранних этапах.
- Для новых прикладных протоколов:
  - Требуются реалистичные сроки: НИР (Академия Криптографии), основные технические решения (коммерческие компании, НТЦ ЦК), одновременно нормативная база.
  - Появился существенный задел на будущее. Подробнее – на секциях РусКрипто.

# Контактная информация

Электронная почта:

svs@cryptopro.ru

Телефон:

+7-916-332-3329

Сайт:

cryptopro.ru

# TLS 1.2 с ГОСТ: стандартизация

- Подзадачи:
  - Определение в ISO и IETF алгоритмов и эл. кривых: **ISO/IEC 14888-3**, **ISO/IEC 10118-3:2018**, **RFC 6986**, **RFC 7091**, **RFC 7801**, **RFC 7836**
  - Стандартизация CTR-ACPKM в России: **Р 1323565.1.017-2018**
  - Стандартизация CTR-ACPKM в IETF: **RFC 8645**
  - Стандартизация CTR-ACPKM в ISO: *проект ISO/IEC 10116 AMD 1*
- Стандартизация в России TLS 1.2 с ГОСТ: **Р 1323565.1.020-2018**
- Идентификаторы IANA российских криптонаборов TLS 1.2 в IETF:

| | | |
|---|---|---|
| 0xC1,0x00 | TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC | [draft-smyshlyaev-tls12-gost-suites] |
| 0xC1,0x01 | TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC | [draft-smyshlyaev-tls12-gost-suites] |
| 0xC1,0x02 | TLS_GOSTR341112_256_WITH_28147_CNT_IMIT | [draft-smyshlyaev-tls12-gost-suites] |

- Описание российских криптонаборов TLS 1.2 в IETF: *draft-smyshlyaev-tls12-gost-suites*

# TLS 1.3 с ГОСТ: стандартизация

- Подзадачи:
  - Определение в ISO и IETF алгоритмов и эл. кривых: **ISO/IEC 14888-3**, **ISO/IEC 10118-3:2018, RFC 6986**, **RFC 7091**, **RFC 7801**, **RFC 7836**
  - Стандартизация режима MGM в России: **Р 1323565.1.026–2019**
  - Определение режима MGM в IETF: *draft-smyshlyaev-mgm*

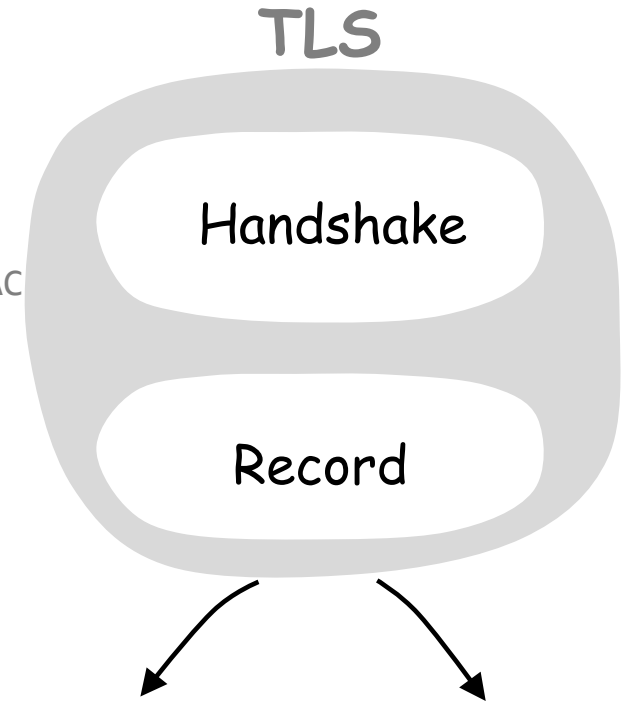
- Стандартизация в России TLS 1.3 с ГОСТ: **Р 1323565.1.030-2020**

- Идентификаторы IANA российских криптонаборов TLS 1.3 в IETF:

| | | |
|---|---|---|
| 0xC1,0x03 | TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L | [draft-smyshlyaev-tls13-gost-suites] |
| 0xC1,0x04 | TLS_GOSTR341112_256_WITH_MAGMA_MGM_L | [draft-smyshlyaev-tls13-gost-suites] |
| 0xC1,0x05 | TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S | [draft-smyshlyaev-tls13-gost-suites] |
| 0xC1,0x06 | TLS_GOSTR341112_256_WITH_MAGMA_MGM_S | [draft-smyshlyaev-tls13-gost-suites] |

- Описание российских криптонаборов TLS 1.3 в IETF: *draft-smyshlyaev-tls13-gost-suites*

# TLS с ГОСТ




TLS_GOSTR341112_256_WITH_28147_CNT_IMIT
TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC
TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC

TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
TLS_GOSTR341112_256_WITH_MAGMA_MGM_S

## TLS 1.2

- ✓ Р 1323565.1.020-2018
- ✓ Драфт RFC, на рецензировании
- ✓ Номера IANA

## TLS 1.3

- ✓ Р 1323565.1.030-2020
- ✓ Драфт RFC
- ✓ Номера IANA