Криптографические алгоритмы и протоколы: стандартизация и применение в Российской Федерации

Смышляев Станислав Витальевич,
заместитель генерального директора КриптоПро

КРИПТОПРО

Национальные интересы и международное сотрудничество в развитии ИКТ-инфраструктуры

Целесообразность международной стандартизации в области криптографии

- Статус у криптографического механизма «международного стандарта» или включение в RFC:
  - Необходим для использования в отраслевых протоколах: стандарты и спецификации ссылаются на документы своего же уровня.
  - Необходим для массового распространения ПО с криптографией: например, затруднена публикация приложений в AppStore/Google Play с использованием криптографических механизмов, не представленных в документах IETF/ISO.
- Получение международных идентификаторов:
  - Устраняет вероятность блокировки российских механизмов зарубежными.
  - Обеспечивает гарантию поддержки наших механизмов в свободном ПО.
  - Снижает вероятность конфликтов при эволюционном развитии технологий.
  - Позволяет достичь согласованности при работе со сторонним ПО.

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 TLS.
- 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.

Зарубежные криптографические механизмы и стандартизация в РФ

- В регулируемых областях: должны использоваться только криптографические механизмы, определяемые документами национальной системы стандартизации или имеющие положительное заключение регулятора.
- Базовые алгоритмы (напр., блочный шифр, хэш-функция, эллиптическая кривая): синтез с нуля – для всеобъемлющего анализа необходимо знание всех принципов, заложенных в алгоритм.
- Криптографические протоколы и сопутствующие алгоритмы (напр., TLS, HMAC): синтез с опорой на безопасность базовых алгоритмов, анализ с построением теоретико-сложностных сведений, анализ по известным методам – анализ сопровождается корректировками протокола для обеспечения стойкости.
- Учитывать зарубежный опыт при синтезе и анализе необходимо.
- Для обеспечения возможности интеграции российских реализаций в прикладные системы по возможности не менять общий технический каркас протоколов.

ГОСТы в документах ISO/IEC JTC1 SC27 WG2

- ГОСТ Р 34.10-2012 в ISO/IEC 14888-3.
- ГОСТ Р 34.11-2012 в ISO/IEC 10118-3.
- Работы по продвижению ГОСТ Р 34.12-2015. Дискуссии и политика.
- Российские режимы шифрования со сменой ключа АСРКМ в проекте дополнения к ISO/IEC 10116:2017.

Текущие и перспективные направления работ в IETF

- Документы IETF с российской криптографией:
  - Действующие ГОСТ Р:
    - RFC 6986 – ГОСТ Р 34.11-2012
    - RFC 7091 – ГОСТ Р 34.10-2012
    - RFC 7801 – ГОСТ Р 34.12-2015
    - …
- Действующие Рекомендации ТК26:
  - RFC 7836 – алгоритмы, сопутствующие применению ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012
  - RFC 8133 – протокол SESPAKE
  - RFC 8645 – плановый документ CFRG, механизмы смены ключей.
  - Драфты IETF по MGM, TLS 1.2 и TLS 1.3

Необходимость фундамента с TLS для практических задач

- 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

- все требуют применения защиты клиент-серверных взаимодействий в соответствии с требованиями ФСБ России. Фактически, единственное решение: TLS с ГОСТ

TLS

NETSCAPE

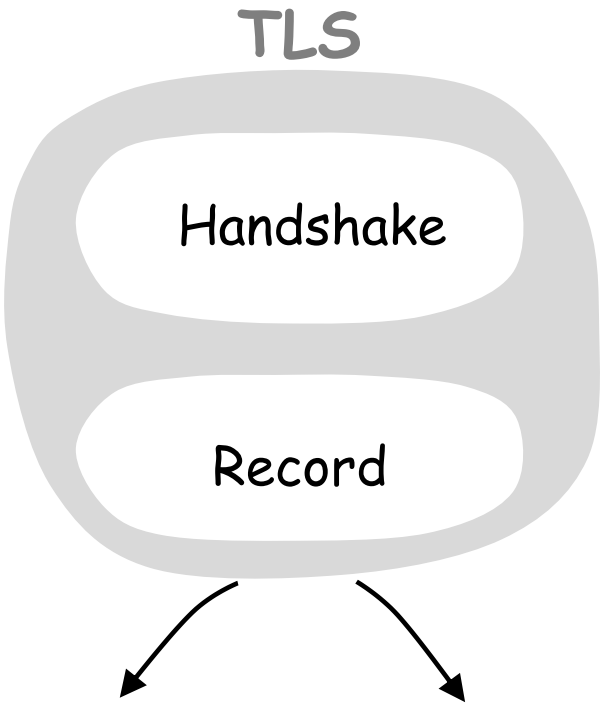
SSL 2.0 (1995) → SSL 3.0 (1996)

IETF

TLS 1.0 (1999) → TLS 1.1 (2006) → TLS 1.2 (2008)

TLS 1.3 (2018)

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
- ✓ Номера IANA

TLS 1.3

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

КРИПТОПРО

TLS с ГОСТ: существующие решения

- 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.
- TLS-сервера с одновременной поддержкой ГОСТ и зарубежных криптонаборов.
- SDK для создания мобильных приложений с поддержкой TLS с ГОСТ для ОС iOS, Android.
- Средства УЦ для выдачи TLS-сертификатов (ГОСТ).
- Клиентские и серверные решения для OCSP.
- Нет SDK для мобильных приложений без требования оценки влияния.
- Нет средств Certificate Transparency.
- Нет средств ACME.

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.

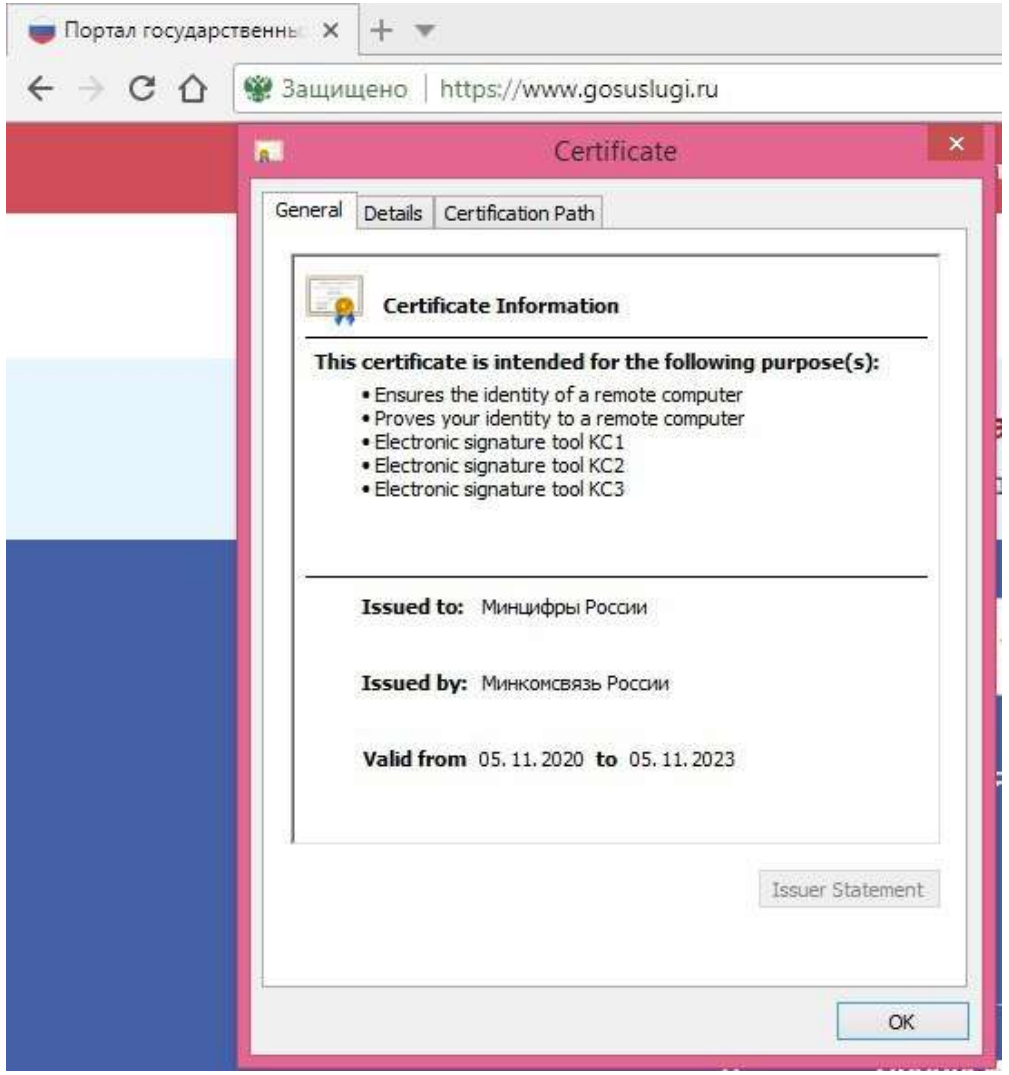
TLS с ГОСТ: поддержка на сайтах

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



Заключение

- Применяться в регулируемых законодательствам областях должны только стандартизированные (или получившие заключение) механизмы.
- При синтезе необходимо учитывать обеспечение совместной работы в конечных системах: общая архитектура протоколов, принципиальное соответствие моделей нарушителя для базовых механизмов, учет зарубежного опыта, международно признаваемые идентификаторы.
- Международная стандартизация важна, в частности, для работы внутри РФ.
- TLS с ГОСТ как пример решения с использованием стандартизированных в РФ решений: с учетом международного опыта, с соответствием российским требованиям, с международно признаваемыми идентификаторами и практическим внедрением на массовых ресурсах.

Спасибо за внимание!

svs@cryptopro.ru