Использование отечественной криптографии в российском сегменте сети Интернет

Смышляев Станислав Витальевич,
заместитель генерального директора КриптоПро

КРИПТОПРО

Состояние и перспективы развития ИКТ-инфраструктуры при обеспечении доверия и безопасности

Российская криптография для массового пользователя

- Поручение Президента от 16 июля 2016 года № Пр-1380
- Единая биометрическая система (ЕБС): 482-ФЗ от 31.12.2017 и 4-МР ЦБ от 14.02.2019.
- «Открытые API» для финансового рынка: прикладные программные интерфейсы обеспечения безопасности финансовых сервисов.
- Перспективы развития требований к собственным биометрическим подсистемам банков.
- Федеральный закон от 27.12.2019 N 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи» [...]
- Для всех задач: требуется обеспечить защиту клиент-серверных соединений по ГОСТ.

TLS

NETSCAPE

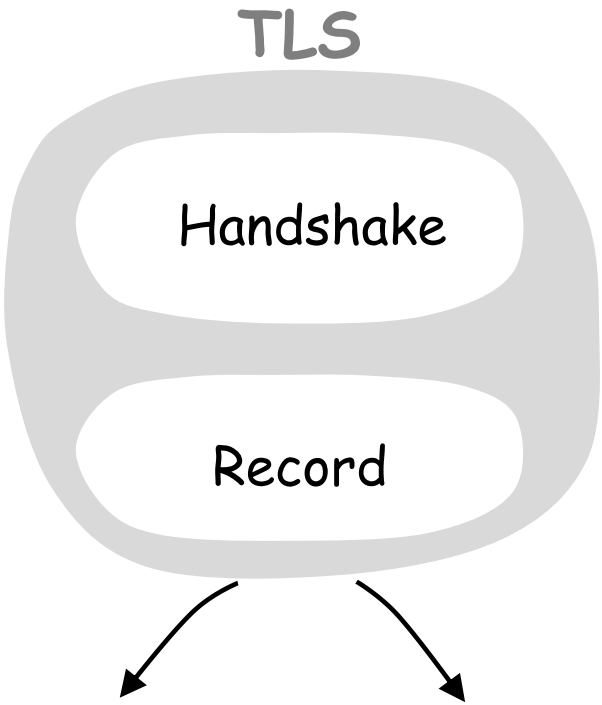
SSL 2.0 (1995) → SSL 3.0 (1996)

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, на рецензировании
- ✓ Номера IANA

TLS 1.3

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

КРИПТОПРО

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]

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

TLS с ГОСТ: требуемые компоненты

- Браузеры с поддержкой TLS с ГОСТ.
- TLS-сервера требуемого класса защиты с одновременной поддержкой ГОСТ и зарубежных криптонаборов.
- Почтовые клиенты со встроенной поддержкой S/MIME с CMS по ГОСТ.
- SDK для создания мобильных приложений с поддержкой TLS с ГОСТ.
- Средства УЦ для выдачи TLS-сертификатов (ГОСТ).
- Вспомогательные средства PKI для TLS-сертификатов (ГОСТ).

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 средств Certificate Transparency.
- Нет средств ACME.

TLS с ГОСТ: примеры поддержки

- 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

Спасибо за внимание!

svs@cryptopro.ru