Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Настоящее и будущее криптопротоколов в сети Интернет

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

Защита каналов по ГОСТ 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» [...]

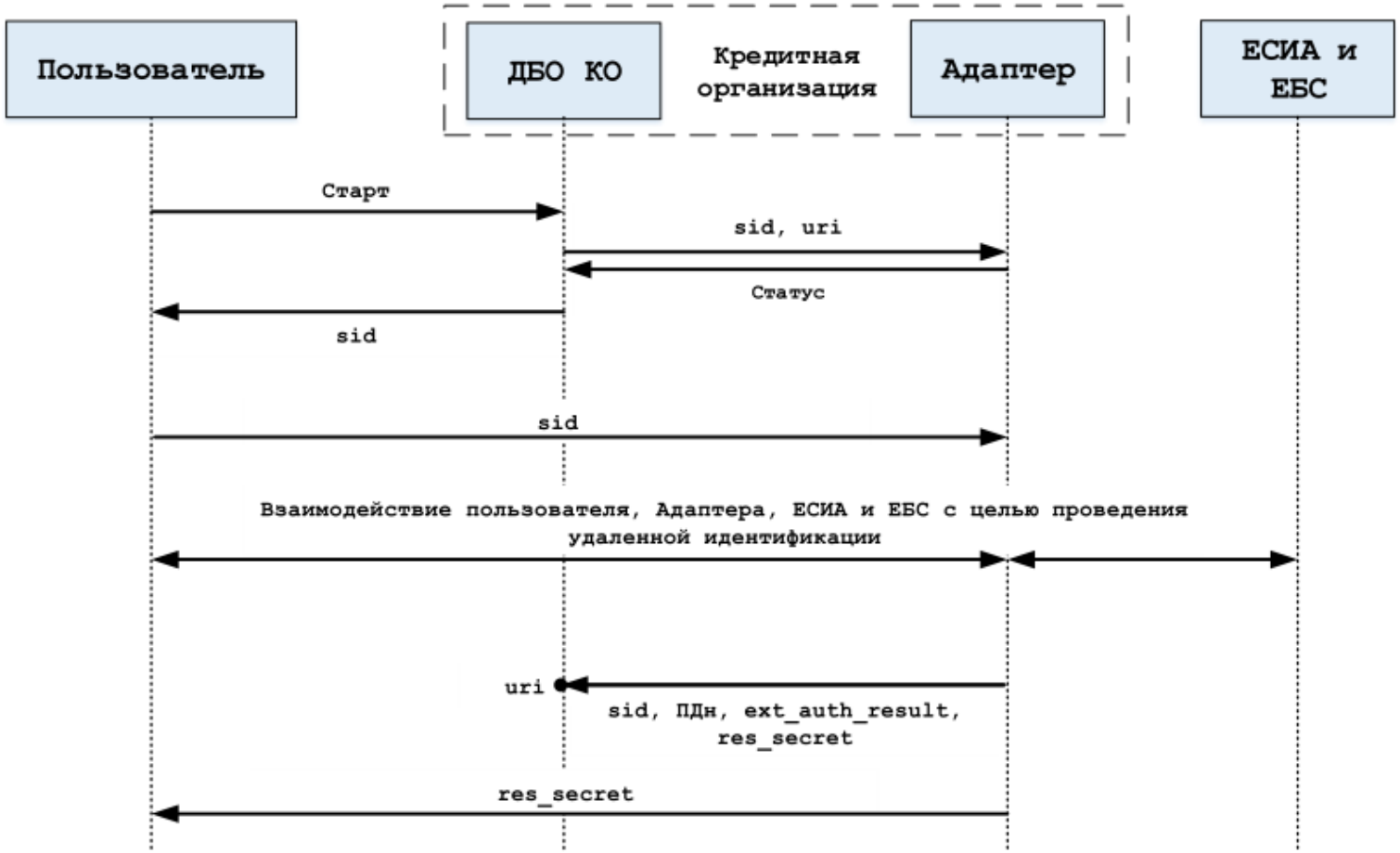
Что требуется для решения задач

- OpenID Connect: аутентификация, авторизация и согласие на передачу данных.
  - Единая биометрическая система (ЕБС)
  - Удаленное получение сертификатов пользователей
  - «Открытые API» для финансовых технологий
- TLS: защита клиент-серверных соединений.
  - Необходимая база для всех протоколов безопасности при использовании массовых устройств, в частности, OpenID Connect.
  - Защита соединений пользователей с поставщиками услуг.
- IPsec: защита site-to-site.
  - Выполнение законодательства поставщиками услуг.

OpenID Connect

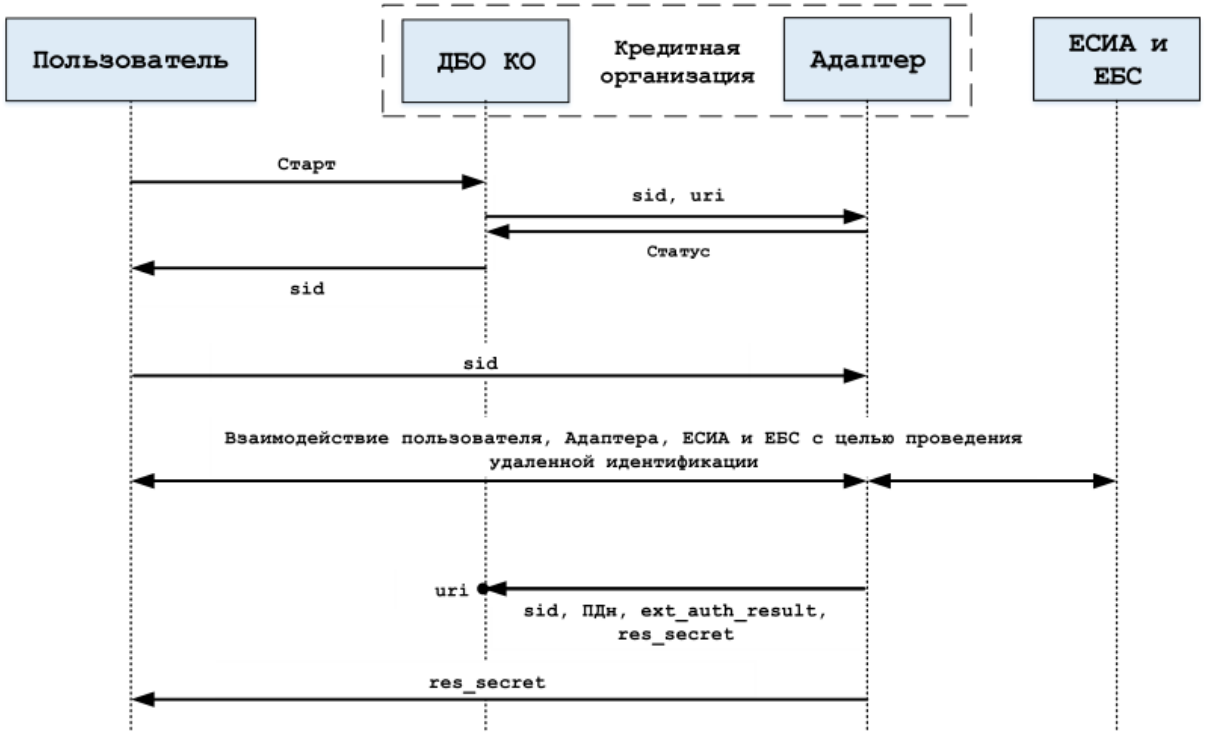
- Протокольное семейство, обеспечивающее функционирование децентрализованной системы аутентификации и авторизации.
- Де-факто стандарт в задачах установления взаимного доверия нескольких организаций и пользователей.
- Используется в ЕБС.
- Документ «Использование российских криптографических алгоритмов в протоколах OpenID Connect» включен в план работ рабочей группы ТК 26 на 2020 год.
- Проведены исследования представителя протокольного семейства с ГОСТ.

OpenID Connect в ЕБС



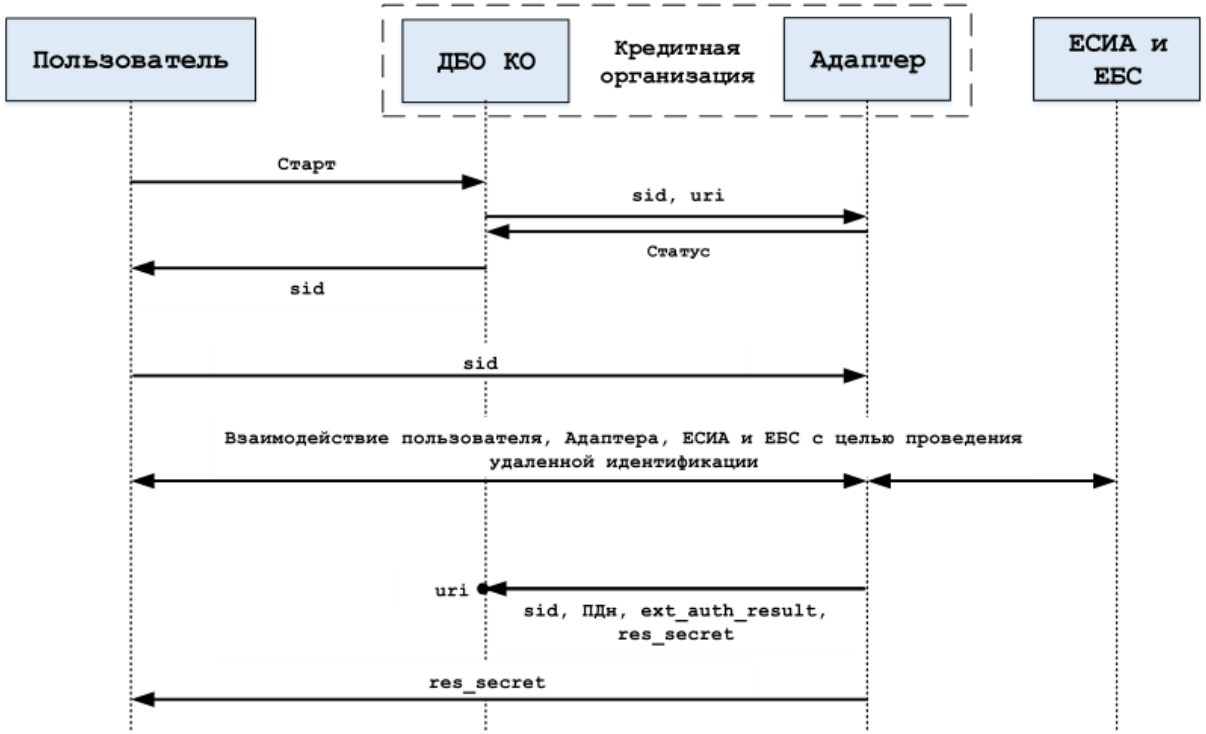
OpenID Connect в ЕБС

- Требует защиты клиент-серверных соединений между пользователем и ДБО.
- Требует защиты соединений между серверами между ДБО и ЕСИА/ЕБС.



OpenID Connect

- На мобильных устройствах пользователей необходим TLS с ГОСТ.
- Защита каналов связи между серверами: IPsec (или альтернативы).



IPsec

- В 2019 году возникло сразу несколько площадок, для которых требуется совместимая работа шлюзов сетевого уровня.
- IPsec с ГОСТ: создан в 2013 году для совместимой работы, но цель выполнена не была – существует два параллельно живущих протокола.
- 2020 год: в план работы ТК 26 включены документы «Использование российских криптографических алгоритмов в протоколе обмена ключами в Интернете версии 2 (IKEv2)» и «Использование российских криптографических алгоритмов в протоколе защиты информации ESP».

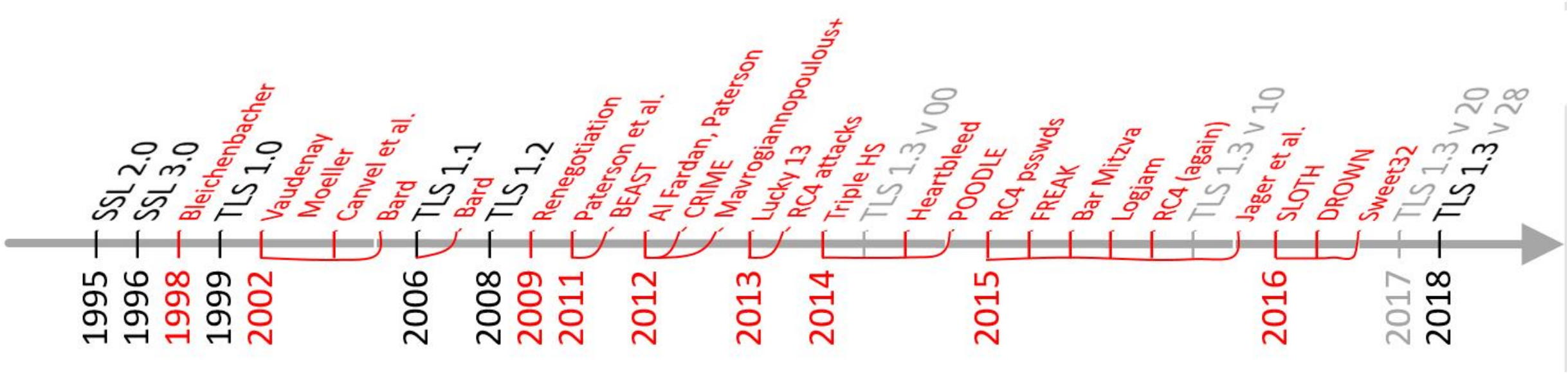
TLS

SSL 2.0 (1995) → SSL 3.0 (1996)

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

TLS 1.3 (2018)

TLS: история уязвимостей



TLS 1.2

- 2-RTT/1-RTT
- обычно нет PFS
- Handshake в открытом виде
- багаж уязвимых криптонаборов для защиты Record
- возможно задание параметров групп ключевого обмена

синтез в ответ на уязвимости

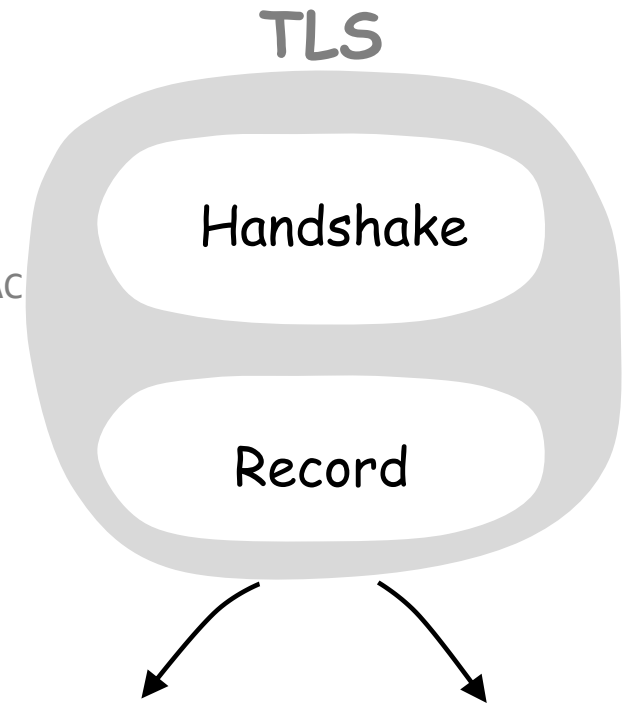
TLS 1.3

- 1-RTT/0-RTT
- PFS
- часть Handshake зашифрована
- удаление уязвимых криптонаборов, улучшение существующих
- только фиксированные группы для ключевого обмена

синтез с одновременным анализом стойкости и обоснованиями

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

ГОСТ в международных протоколах

- Валерий Смыслов – в составе Security Area Directorate в IETF.
- Станислав Смышляев в январе 2020 назначен соруководителем CFRG в IETF (взамен Кенни Патерсона).
- Российские режимы шифрования со сменой ключа ACPKM:
  - в проекте документа ISO/IEC JTC1 SC27: ISO/IEC 10116:2017;
  - в августе 2019 года в составе RFC 8645.
- Доклад Лео Перрена на IETF 105 в Монреале о необходимости запрета использования российских криптоалгоритмов в протоколах IETF – позиции России успешно защищены.

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: требуемые компоненты

- Браузеры с поддержкой TLS с ГОСТ.
- TLS-серверы 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-серверы требуемого класса защиты 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.
- Клиентские и серверные решения для «облачной» подписи.
- Нет средств Certificate Transparency.
- Нет средств ACME.
- Требует дальнейших шагов задача обеспечения удобного встраивания СКЗИ (КС1) в мобильные приложения с прикладным функционалом.

Контактная информация

Электронная почта:

svs@cryptopro.ru

Телефон:

+7-916-332-3329

Сайт:

cryptopro.ru

TLS с ГОСТ: поддержка на сайтах

- 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

Задачи для массовых СКЗИ

- Для приложений, аналогичных удаленной аутентификации через ЕБС, достаточен класс КС1
- Возможность размещения в магазинах приложений (AppStore, Google Play)
- Обеспечение поэкземплярного учета
- Механизмы контроля целостности
- Возможность использования безопасных модулей реализации ГОСТ в прикладных мобильных приложениях заказчиков – требуется высокоуровневый интерфейс для выполнения требований функциональной законченности

Кратчайшая история уязвимостей TLS

- **Bleichenbacher, DROWN, ROBOT, 9Lives**: проблемы использования механизмов дополнения при RSA-зашифровании приводили к побочному каналу информации.
- **Vaudenay, Lucky Thirteen, POODLE, LuckyMicroseconds**: невнимательное отношение к обработке при расшифровании дополнения открытого текста («padding») приводило к побочному каналу информации.
- **Renegotiation/Triple Handshake**: нетривиальная логика протокола при повторном согласовании – потенциальные уязвимости прикладных систем.
- **BEAST**: базовые свойства безопасности режима CBC не были учтены, существовали условия, при которых можно было осуществлять бесключевое чтение.
- **RC4**: существенные корреляции выходной гаммы шифра.

Направления развития TLS

- ESNI (Encrypted Server Name Indication).
- Использование дополнительного ключевого материала, полученного с помощью «постквантовых» механизмов.
- Механизмы повышения безопасности использования источников энтропии на серверной стороне.
- Exported authenticators.
- Оптимизация работы высоконагруженных TLS-серверов: в частности, за счет механизмов «пакетного подписания» HS.
- DTLS 1.3.
- Общее направление по защите от отслеживания пользователей (защита от «fingerprinting»).