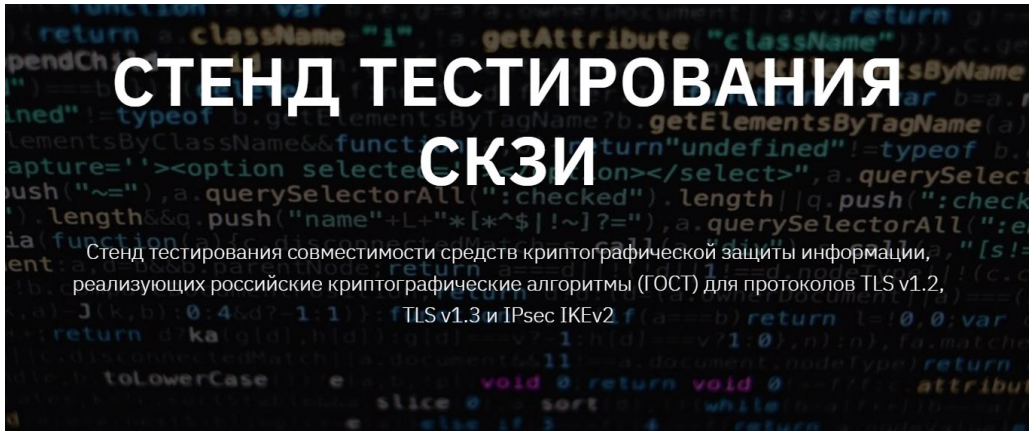
Перспективы развития СКЗИ для защиты каналов связи в свете работ ТК 26

Смышляев Станислав Витальевич,
заместитель генерального директора КриптоПро

КРИПТОПРО

IX симпозиум
«Современные тенденции в криптографии»
CTCrypt 2020

Проблема совместимости СКЗИ



Акционерное общество
«Научно-производственная компания «Криптонит»

«УТВЕРЖДАЮ»

Генеральный директор
АО «НПК «Криптонит»

В. М. Хачатуров

«____» _____ 2020 г.

Методика проведения тестовых испытаний совместимости средств криптографической защиты информации, реализующих российские криптографические алгоритмы для протоколов TLS v1.2, TLS v1.3 и IPsec IKEv2

Версия 1.2.2 от 23.07.2020

Подкомитет № 2

«Криптографические алгоритмы и протоколы для применения в поставляемых для федеральных государственных нужд шифровальных (криптографических) средствах защиты информации, содержащей сведения, относимые к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа»

Рабочая группа 2.1

по сопутствующим криптографическим алгоритмам и протоколам

Руководители: Смышляев С.В. (ООО КРИПТО-ПРО), Бондаренко А.И.

Проблема совместимости СКЗИ

- С начала существования ТК 26 функционирует РГ по сопутствующим криптографическим алгоритмам и протоколам – единая площадка для выработки совместимых решений, в том числе, по TLS и IPsec.
- Начиная с 2015 года, неотъемлемой частью разработки документов является создание контрольных примеров и методик встречного тестирования.
- В рамках тематических исследований лаборатории проверяют встречную работу.
- Единого стенда, направленного на как можно более широкий набор сценариев проверки встречной работы, не существовало.

Проблема совместимости СКЗИ

- TLS с ГОСТ: Пр-1380, НУЦ, ПП №963 от 30.06.20 «О реализации пилотного проекта по использованию российских криптографических алгоритмов и средств шифрования в государственных информационных системах».
- По TLS совместимость обеспечивается (отдельные случаи разработчиками отрабатываются в частном порядке), по IPsec на текущий момент далеко не все решения совместимы (с учетом специфики протокола, не всегда это проблема).

IPsec

- Для IPsec с ГОСТ 28147-89 существовал только набор технических спецификаций ТК 26, так как в 2013 году разработчики СКЗИ не смогли прийти к единому решению.
  - ТС 26.2.001-2015 «Использование ГОСТ 28147-89, ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 в протоколах обмена ключами IKE и ISAKMP»
  - ТС 26.2.002-2014 «Использование ГОСТ 28147-89 при шифровании вложений в протоколах IPSEC ESP»
- Реализация IPsec с ГОСТ 28147-89 осуществлялась у разных производителей СКЗИ двумя несовместимыми способами.

IPsec

- В соответствии с планом работы ТК 26 в 2020-2021 годах будут выпущены документы (рекомендации по стандартизации).
  - «Использование российских криптографических алгоритмов в протоколе обмена ключами в Интернете версии 2 (IKEv2)»
  - «Использование российских криптографических алгоритмов в протоколе защиты информации ESP».
- Для ESP и IKEv2 с ГОСТ выделены идентификаторы IANA.
- В 2019 году возникло сразу несколько областей в области применения СКЗИ, для которых требуется совместимая работа шлюзов сетевого уровня.
- 2020 год: https://gost.kryptonite.ru/, тестирование IPsec (IKEv2/ESP с ГОСТ Р 34.1x-2015).

Стандартизация протоколов защиты каналов в ТК 26 вне РГ по СКАиП

- 2019 год, стандартизация протокола CRISP: Р 1323565.1.029–2019 «Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем»
- Планы на 2020 год: принятие в ТК 26 документа «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня», определяющего протокол IPlir.
- Планы на 2021 год: дополнение рекомендаций по CRISP криптонаборами с длинными (8-байтными) имитовставками.

TLS

NETSCAPE

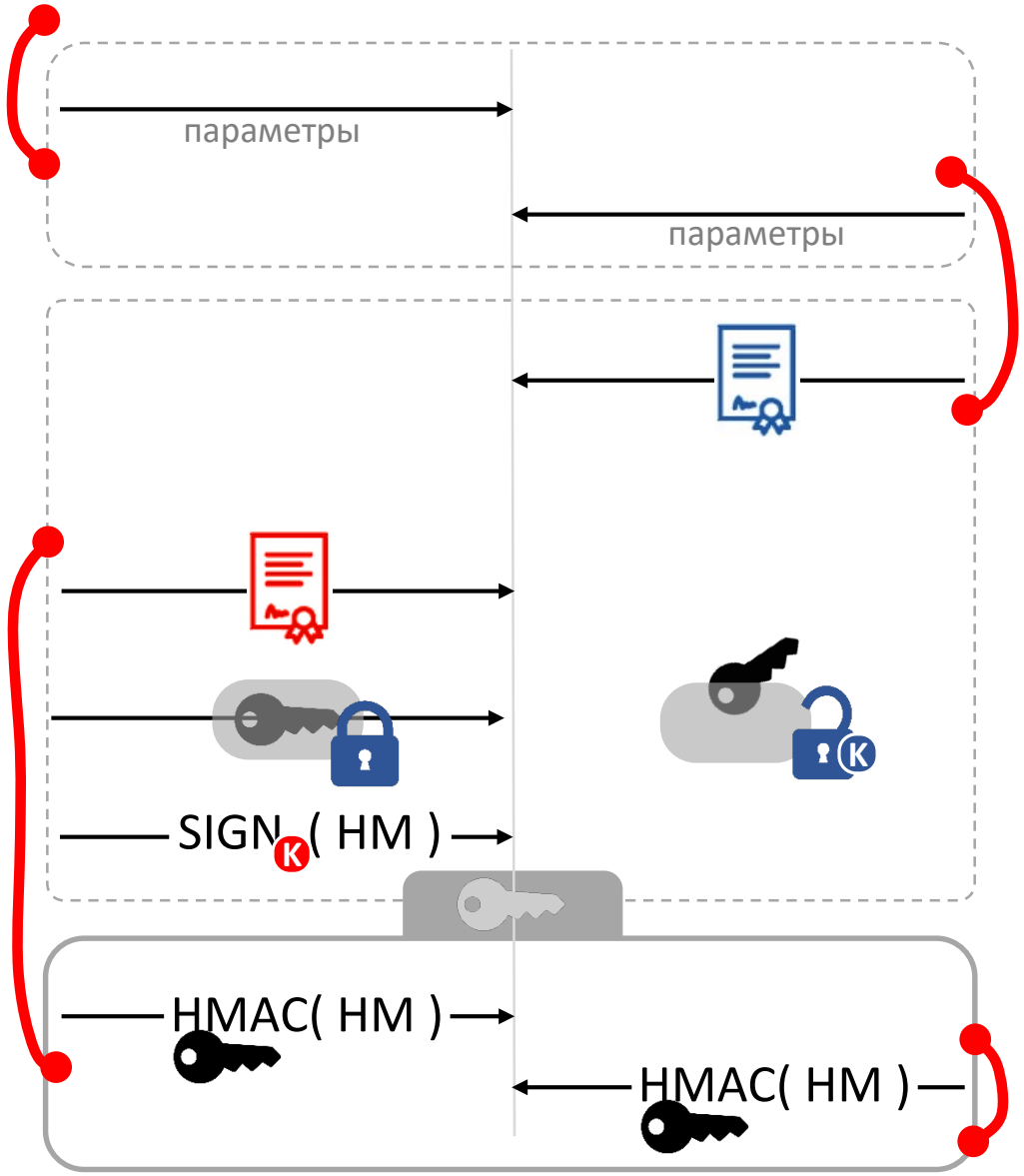
SSL 2.0 (1995) → SSL 3.0 (1996)

I E T F®

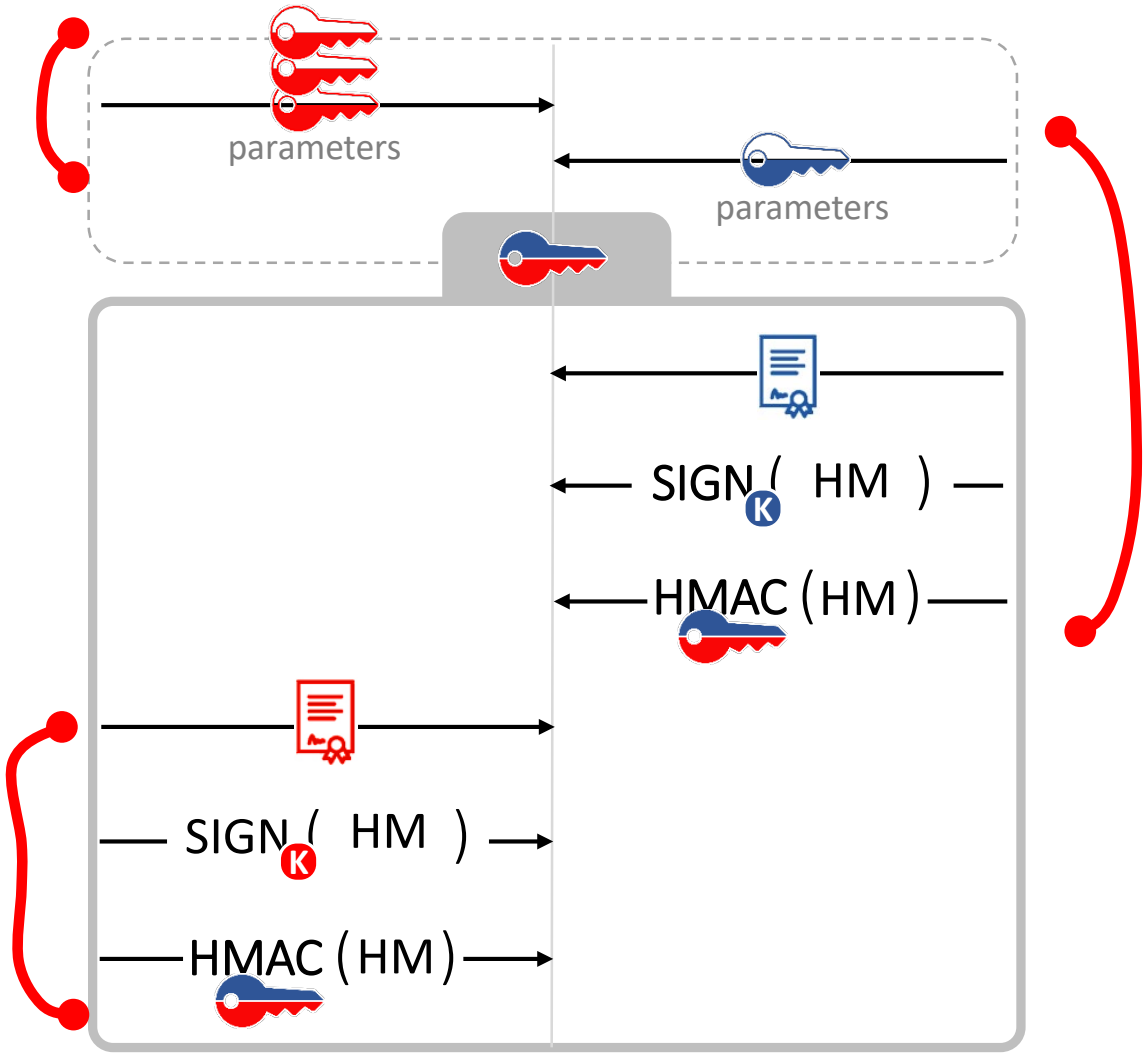
TLS 1.0 (1999) → TLS 1.1 (2006) → TLS 1.2 (2008)

TLS 1.3 (2018)

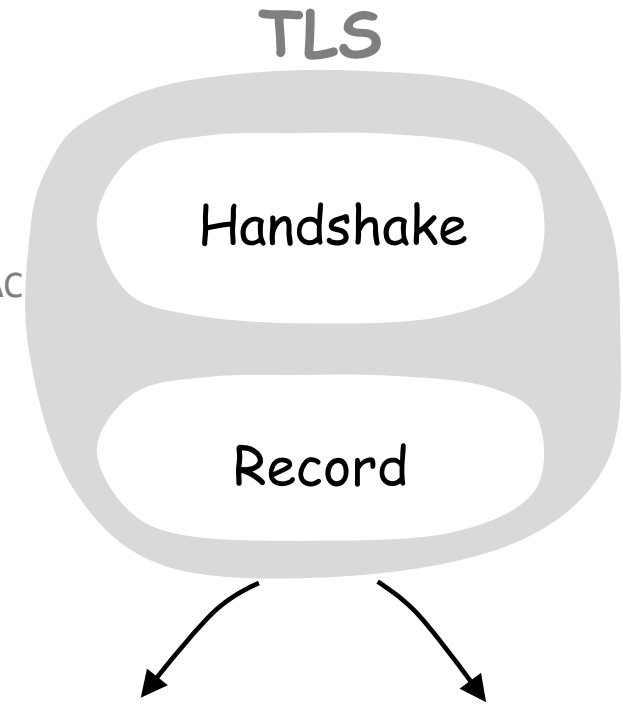
TLS 1.2



TLS 1.3



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: 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.

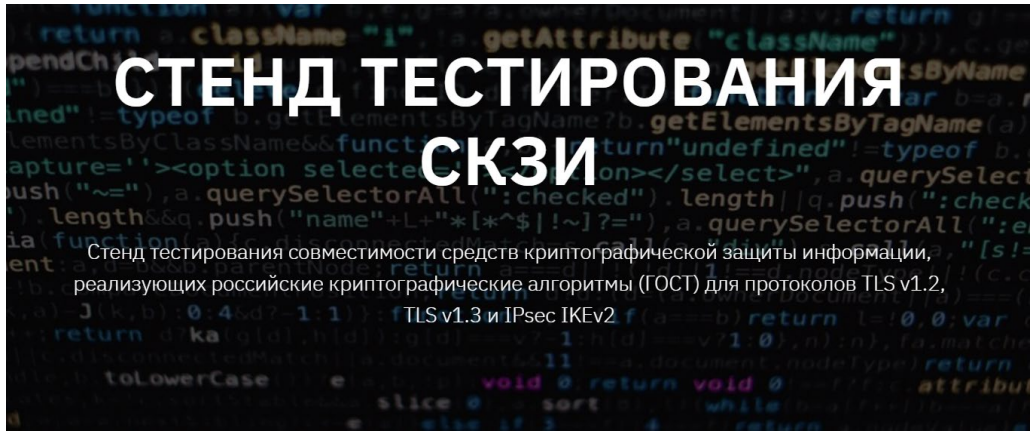
Подкомитет № 2

«Криптографические алгоритмы и протоколы для применения в поставляемых для федеральных государственных нужд шифровальных (криптографических) средствах защиты информации, содержащей сведения, относимые к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа»

Рабочая группа 2.1

по сопутствующим криптографическим алгоритмам и протоколам

Руководители: Смышляев С.В. (ООО КРИПТО-ПРО), Бондаренко А.И.



Спасибо за внимание!

svs@cryptopro.ru