ГОСТ в российском сегменте Интернета: фундамент построен – что дальше?

Смышляев Станислав Витальевич,
заместитель генерального директора КриптоПро

КРИПТОПРО

X симпозиум
«Современные тенденции в криптографии»
CTCrypt 2021

Массовая криптография на примере дистанционного оказания услуг

- Дистанционное получение сертификатов электронной подписи
- Дистанционное предоставление услуг ФЛ и ЮЛ, требующих конфиденциального канала взаимодействия
- Системы дистанционного формирования электронной подписи
- Протоколы дистанционного электронного голосования
- Протоколы, предполагающие дистанционную идентификацию личности

– в части соответствия требованиям по безопасности требуют TLS с ГОСТ с использованием сертифицированных СКЗИ в качестве фундамента.

Массовая криптография: фундамент

- Необходимым условием для безопасности любой дистанционной услуги через Интернет является защищенное TLS-соединение.
  - Порталы дистанционного банковского обслуживания.
  - Системы дистанционного электронного голосования.
  - Почтовые сервисы.
  - Системы государственных и муниципальных услуг.
  - Дистанционная выдача сертификатов ключей проверки ЭП.
  - ЕСИА, ЕБС, идентификация и аутентификация на сторонних ресурсах.
- Веб-сайты в России оснащены TLS-сертификатами, выданными зарубежными удостоверяющими центрами. Риск отзыва TLS-сертификата. Прецеденты были: отзыв TLS-сертификата Общественной Палаты РФ 4 июня 2018 года.
- На решение проблемы направлено поручение Президента от 16 июля 2016 года № Пр-1380, дорожные карты.

Требуемые действия

Сделано:

- Стандартизация алгоритмов, параметров и сопутствующих механизмов в Росстандарте.
- Стандартизация алгоритмов, параметров и сопутствующих механизмов в ISO и IETF.
- Стандартизация криптонаборов TLS в Росстандарте.
- Международно признаваемые идентификаторы российских криптонаборов TLS.
- Поддержка российских криптонаборов TLS в браузерах.
- Поддержка российских криптонаборов TLS в мобильных приложениях.
- Серверные решения с поддержкой российских и зарубежных криптонаборов TLS.
- Средства УЦ для выпуска отечественных TLS-сертификатов.

В процессе:

- Внедрение двух сертификатов (зарубежного и российского) на веб-порталах для граждан.

Предстоит сделать:

- RFC по российским криптонаборам TLS.
- Упрощение встраивания поддержки TLS с ГОСТ в мобильные приложения.
- Упрощенная выдача TLS-сертификатов владельцам массовых веб-сайтов.

TLS с ГОСТ: стандартизация

- Алгоритмы: ГОСТ 34.10-2018, ГОСТ 34.11-2018, ГОСТ 34.12-2018, RFC 6986, RFC 7091, RFC 7801, RFC 8891, ISO/IEC 14888-3, ISO/IEC 10118-3:2018,
- Параметры и сопутствующие механизмы: Р 50.1.113–2016, Р 1323565.1.024–2019, RFC 7836
- Режим CTR-ACPKM: Р 1323565.1.017-2018, RFC 8645, ISO/IEC 10116 AMD 1
- Режим MGM: Р 1323565.1.026–2019, draft-smyshlyaev-mgm
- TLS 1.2 с ГОСТ: МР 26.2.001-2013, Р 1323565.1.020-2020, draft-smyshlyaev-tls12-gost-suites
- TLS 1.3 с ГОСТ: Р 1323565.1.030-2020, draft-smyshlyaev-tls13-gost-suites
- Идентификаторы IANA:

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]
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]

TLS с ГОСТ: обеспечение совместимости

IETF®

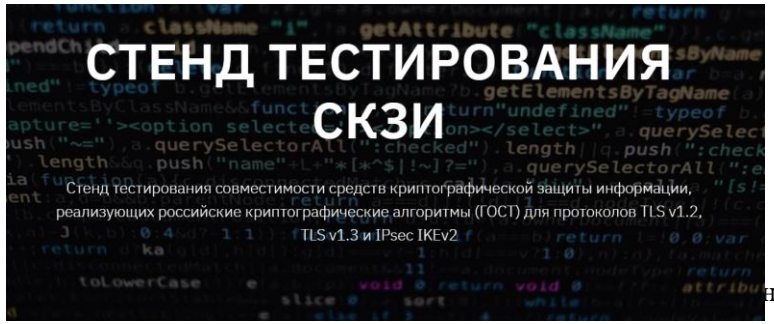
Акционерное общество
«Научно-производственная компания «Криптонит»

«УТВЕРЖДАЮ»

Генеральный директор
АО «НПК «Криптонит»

В. М. Хачатуров

«____» _____ 2020 г.



ния 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

ТК 26

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.

Что есть

- В 2021 году планируется введение в действие НУЦ (Национального Удостоверяющего Центра), будут созданы условия для выдачи TLS-сертификатов безопасности государственным ресурсам.
- Разработаны и начинают внедряться серверные средства, поддерживающие как зарубежные, так и российские криптонаборы TLS (необходимо для плавного, бесшовного внедрения).
- Разработаны и начинают внедряться SDK для создания мобильных приложений с поддержкой TLS с ГОСТ для ОС iOS, Android.
- 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.
- Средства удостоверяющего центра, клиентские и серверные решения для OCSP.

Что требуется

- Условия для выполнения первого требования создаются (все средства есть).
- Требуется также массовое внедрение отечественных TLS-сертификатов не только на веб-сайты ОГВ: 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).
- Максимально безопасное получение сертификатов для веб-сайтов ОГВ.
- Обеспечить условия для получения отечественных TLS-сертификатов одновременно с приобретением доменного имени
- Обеспечить возможность владельцам сайтов быстро получать отечественные TLS-сертификаты 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.

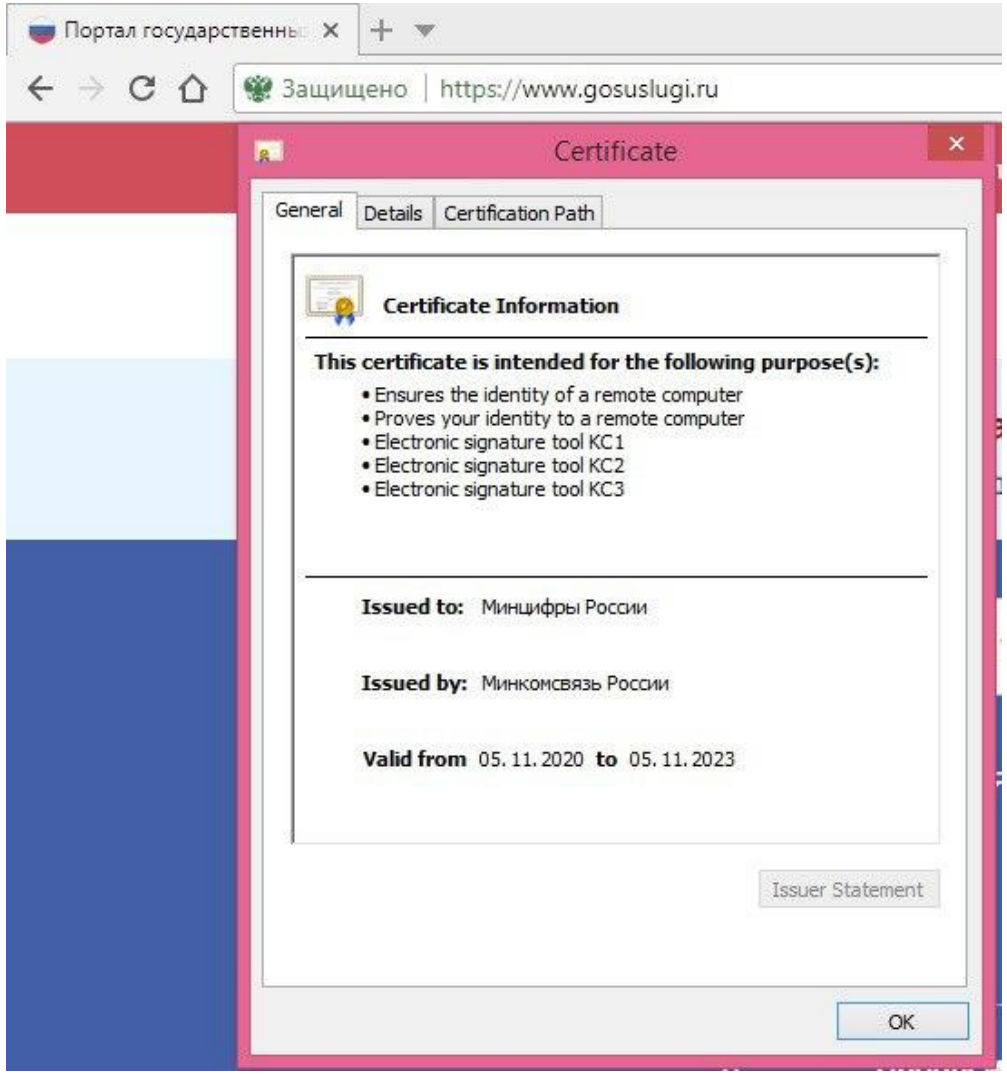
TLS с ГОСТ: поддержка на сайтах

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



Вопросы

1. Что еще требуется из технических средств для решения обозначенных задач?

2. Возможно ли в принципе стабильное развитие «массовой криптографии» без массового использования российских ОС и/или аппаратных средств?

3. Какая дополнительная нормативная база требуется для решения задач внедрения на веб-сайты массовой криптографии с использованием сертифицированных СКЗИ?

4. TLS с ГОСТ – это необходимая база для направления «массовых СКЗИ в Интернете». А что еще необходимо создавать для стабильного развития «отечественной криптографии в российском сегменте Интернета»?

5. Какие практические задачи информационной безопасности необходимо решать наряду с перечисленными?

6. Какие еще задачи по российской или международной стандартизации требуют решения в свете данной тематики?