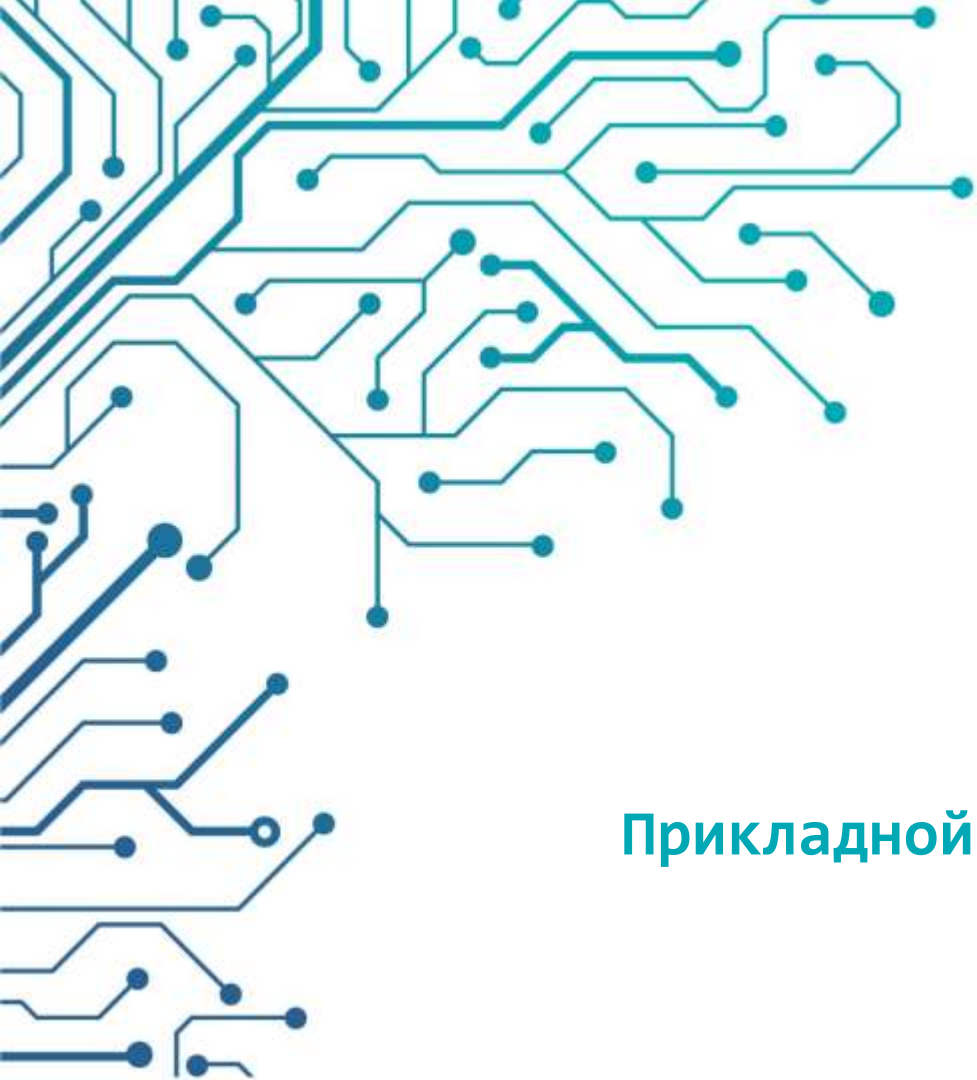


TLS ГОСТ

Прикладной. Мобильный. Серверный.

Еранов Сергей
АО «ИнфоТеКС»

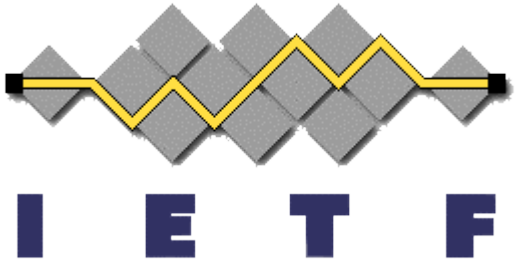
Зачем нам ГОСТ TLS?

Стандартизация





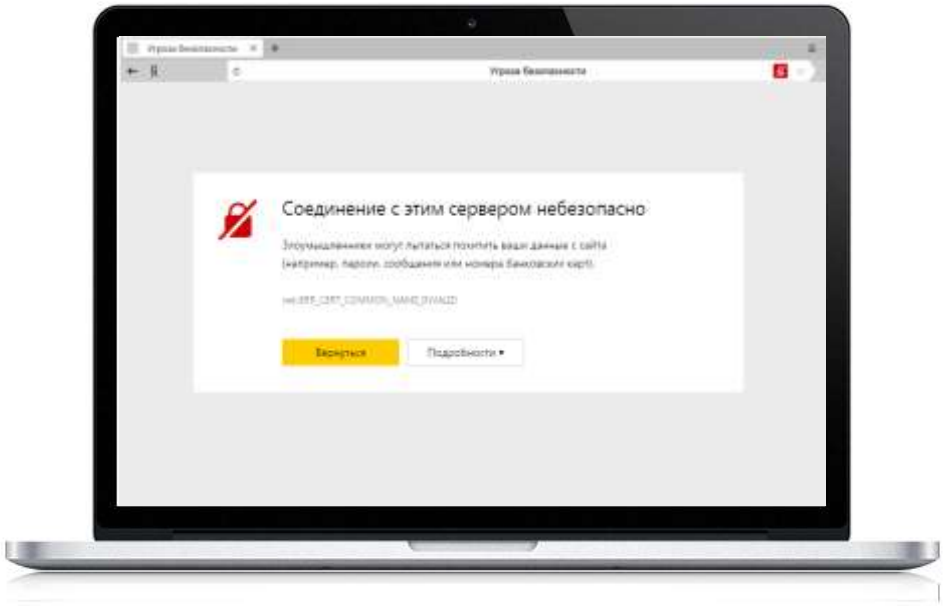
- ГОСТ
- RFC
- Рекомендации ТК26
- Контрольные примеры





Результат: Мультивендорность для конечных потребителей

Независимость и безопасность



Какие возникают проблемы

SSL-сертификат, выданный иностранным УЦ, могут отозвать из-за санкций:

GeoTrust отозвала сертификат для сайта Общественной палаты из-за «аффилированности» с ДНР

Как решаются эти проблемы

Ведется запуск **Национального удостоверяющего центра**

Распространенность



- ✓ Популярность систем с веб-интерфейсом, REST API и т.д.
- ✓ Наличие СКЗИ на рабочих местах для задач ЭП

Активное продвижение со стороны государства

- Пр-1380. Поручение об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования

- Постановление Правительства № 963 «О реализации пилотного проекта по использованию российских криптографических алгоритмов и средств шифрования в государственных информационных системах»

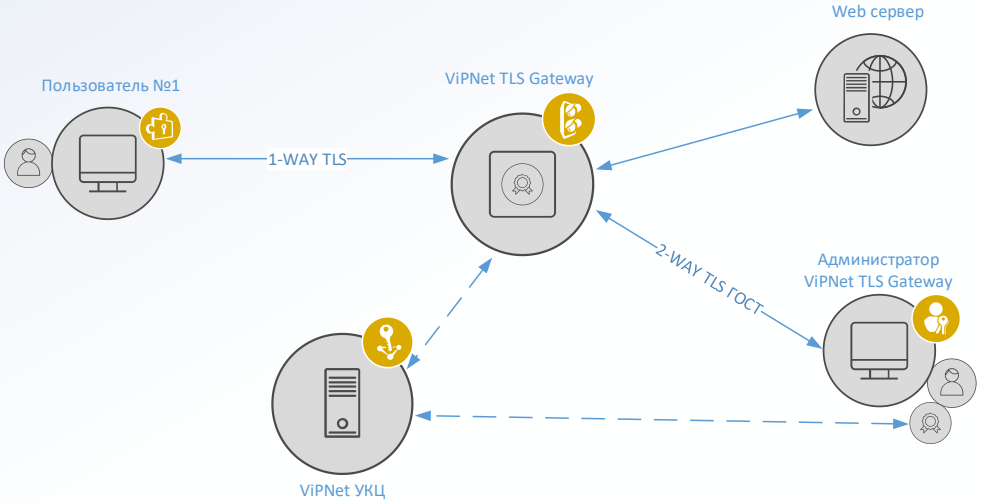
- Проект Приказа Минкомсвязи «Об утверждении требований к технологиям взаимодействия средств информатизации, реализующих российские криптографические алгоритмы, с иными средствами информатизации»



Сценарии применения

Сценарий 1

Публичный портал



Задачи:

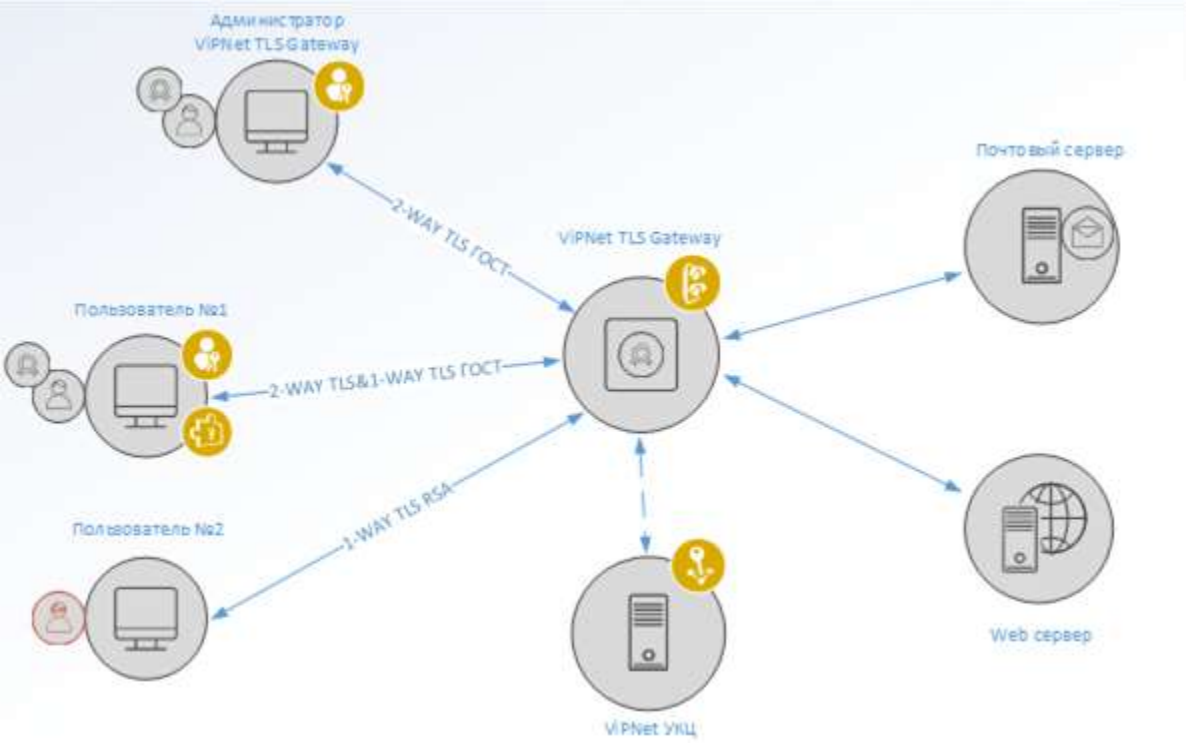
1. Подтверждение подлинности сервера
2. Защита передаваемых данных

Для этого требуется:

- Единое пространство доверия – НУЦ
- Аутентификация сервера
- Общедоступность клиентского СКЗИ
- Дуальный режим

Сценарий 2

Доступ к корпоративным ресурсам



Задачи:

1. Подтверждение подлинности сервера
2. Разграничение доступа
3. Защита передаваемых данных
4. TCP-трафик

Для этого требуется:

- Аутентификация сервера
- Аутентификация клиента
- TLS-туннель

Что для этого нужно

Для порталов

- ✓ Высокопроизводительные криптошлюзы
- ✓ Средства установления TLS соединений для веб-серверов

Для разработчиков

- ✓ Библиотеки и SDK для установки TLS соединений из приложений

Для пользователей

- ✓ Готовое СКЗИ для TLS

TLS ГОСТ. Серверный

ViPNet TLS Gateway

ViPNet TLS Gateway

Высокопроизводительный TLS-криптошлюз



- Аутентификация клиента и сервера
- Управление доступом на основе сертификатов
- «Дуальный» режим работы
- Удаленное управление

Модификации

Исполнение	TLS 500	TLS 1000	TLS 5000	TLS VA
Форм-фактор	ПАК 19” Rack 1U	ПАК 19” Rack 1U	ПАК 19” Rack 1U	виртуальная машина
Предельная пропускная способность (Мбит/с)	до 300	до 750	до 3000	зависит от характеристик аппаратного обеспечения
Число одновременных соединений	до 4700	до 8900	до 44000	зависит от характеристик аппаратного обеспечения
Интерфейсы	4x Ethernet 10/100/1000	4x Ethernet 10/100/1000	4x Ethernet 10/100/1000 4x 10G Ethernet Fiber SFP+	зависят от характеристик аппаратного обеспечения

Платформы виртуализации

Oracle VM VirtualBox
5.1, 5.2, 6.0

VMware vSphere ESXi
6.0, 6.5, 6.7

VMware Workstation
14, 15

Kernel
Virtual Machine



«УТВЕРЖДАЮ»

Генеральный директор
АО «ИнфоТеКС»

А. А. Чаганов

«2» февраля 2021 г.

«УТВЕРЖДАЮ»

Генеральный директор
АО «НПК «Криптонит»

В. М. Хачатуров

«__» февраля 2021 г.

Протокол

испытаний совместимости средств криптографической защиты информации,
реализующих российские криптографические алгоритмы
для протокола TLS 1.2

МОСКВА 2021

Клиентское СКЗИ

ViPNet CSP

ViPNet PKI Client

?

Любое
сертифицированное СКЗИ



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3676 от "12" апреля 2019 г.

Действителен до "12" апреля 2022 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»),
Обществу с ограниченной ответственностью «Линия защиты» (ООО «Линза»).

Настоящий сертификат удостоверяет, что изделие ViPNet TLS Gateway (исполнения 1, 2, 3, 5) в комплектации согласно формуляру ФРКЕ.00169-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 5), класса КС3 (для исполнений 1, 2, 3), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС» сертификационных испытаний образцов продукции №№ 906-000501, 906-000502, 906-000503, 906-000504.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00169-01 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Ивашко

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 12 апреля 2019 г.

Первый заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России В.Н. Мартынов

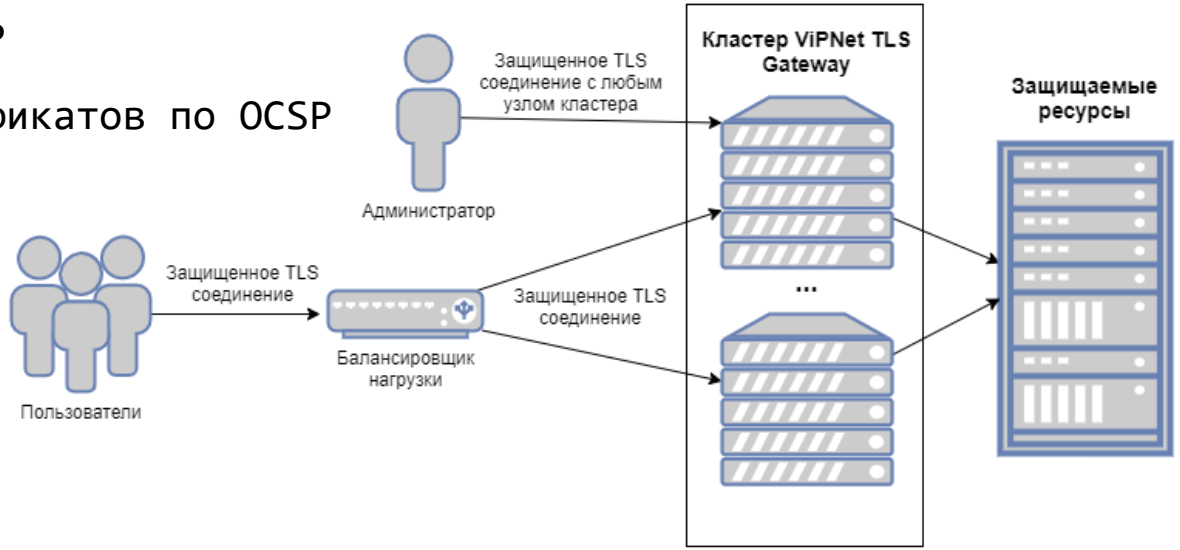
ViPNet TLS Gateway сертифицирован

- СКЗИ КС3 (исполнения ПАК)
- СКЗИ КС1 (исполнение VA)
- Зарегистрирован в Реестре российского ПО

ViPNet TLS Gateway 2

Новые возможности

- Кластер (2 - 64 узла)
- Настройка сети с IPv6
- Мониторинг шлюза по SNMP
- Проверка статусов сертификатов по OCSP

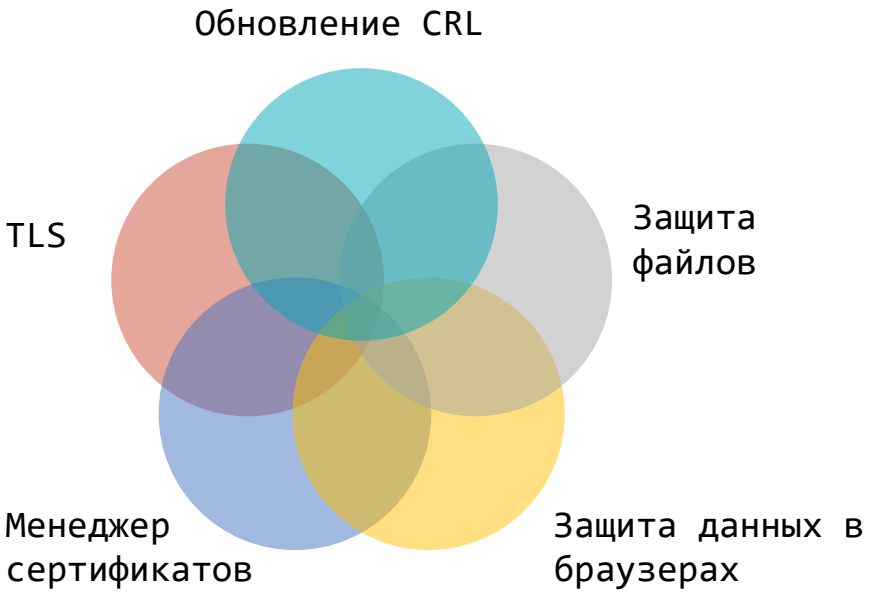


TLS ГОСТ. Клиентский. Мобильный

ViPNet PKI Client

ViPNet PKI Client

Клиент для работы в инфраструктуре открытых ключей



- СКЗИ и средство ЭП
- Кроссплатформенный
- Кроссбраузерный
- Модульный
  - TLS Unit
  - File Unit
  - Web Unit
  - Certificate Unit
  - CRL Unit

ViPNet PKI Client: TLS Unit

Функции:

- локальный TLS-proxy
- аутентификация клиента
- TLS-туннель для TCP-трафика

Преимущества:

- Кроссбраузерный

- совместим с ViPNet TLS Gateway и TLS-шлюзами других производителей


«УТВЕРЖДАЮ»
Генеральный директор
АО «ИнфоТеКС»
А. А. Чаучаев
«2_» февраля 2021 г.

«УТВЕРЖДАЮ»
Генеральный директор
АО «НПЦ «Криптонит»
В. М. Хачатуров
«__» февраля 2021 г.

Протокол
испытаний совместимости средств криптографической защиты информации, реализующих российские криптографические алгоритмы
для протокола TLS 1.2

МОСКВА 2021

ViPNet PKI Client

Сертификация

- СКЗИ КС1-КС3
- Средство ЭП КС1-КС3
- Получена нотификация на вывоз



TLS ГОСТ. Прикладной

Криптографические библиотеки и компоненты

ViPNet CSP

Сертифицированный криптопровайдер (КС1, КС2, КС3)

Работа с ЭП	• ГОСТ Р 34.10-2001* • ГОСТ Р 34.10-2012
Хэширование	• ГОСТ Р 34.11-94* • ГОСТ Р 34.11-2012
Шифрование	• ГОСТ 28147-89 • ГОСТ Р 34.12-2015 • ГОСТ Р 34.13-2015
Интерфейсы	• MS CryptoAPI • MS CNG (BCrypt) • PKCS#11



Работа с ключами
на внешних устройствах

Бесплатный TLS в браузере

* В режиме совместимости



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-4027* от "*01*" *марта* 2021 г.

Действителен до "*31*" *декабря* 2021 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы» (АО «ИнфоТеКС»).

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **ViPNet CSP 4.4** (исполнения 1, 2, 3, 4, 5) в комплектации согласно формуляру ФРКЕ.00106-06.30.01.ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнений 1, 4), класса КС2 (для исполнений 2, 5), класса КС3 (для исполнения 3). Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнений 1, 4), класса КС2 (для исполнений 2, 5), класса КС3 (для исполнения 3) и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 6З7Д-000501, 6З7Д-000502.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00106-06.30.01.ФО

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрибин**



ViPNet CSP 4.4 сертифицирован ФСБ

ViPNet OSSL

Криптобиблиотека на базе OpenSSL (КС1, КС2, КС3)

Работа с ЭП
- ГОСТ Р 34.10-2001*
- ГОСТ Р 34.10-2012

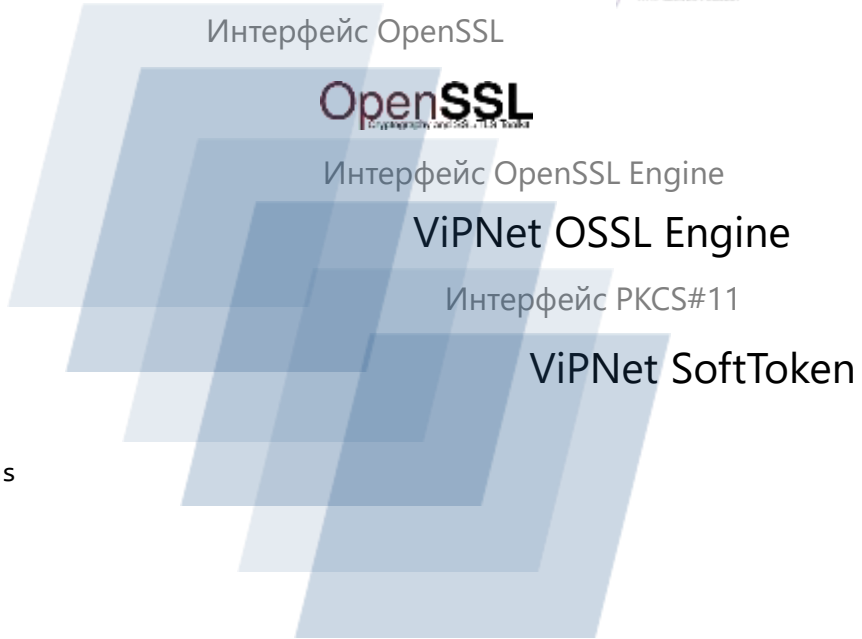
Хэширование
- ГОСТ Р 34.11-94*
- ГОСТ Р 34.11-2012

Шифрование
- ГОСТ 28147-89
- ГОСТ Р 34.12-2015
- ГОСТ Р 34.13-2015

Организация TLS
- TLS 1.2
- TLS 1.3

Интерфейсы
- OpenSSL
- PKCS#11
- ViPNet OpenSSL Extensions

Работа с ключами на внешних устройствах



* В режиме совместимости

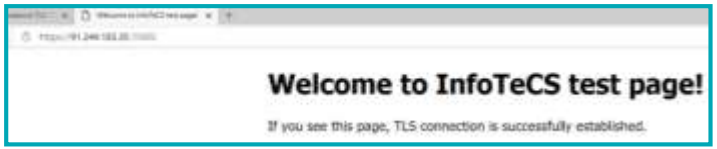
Встречное тестирование

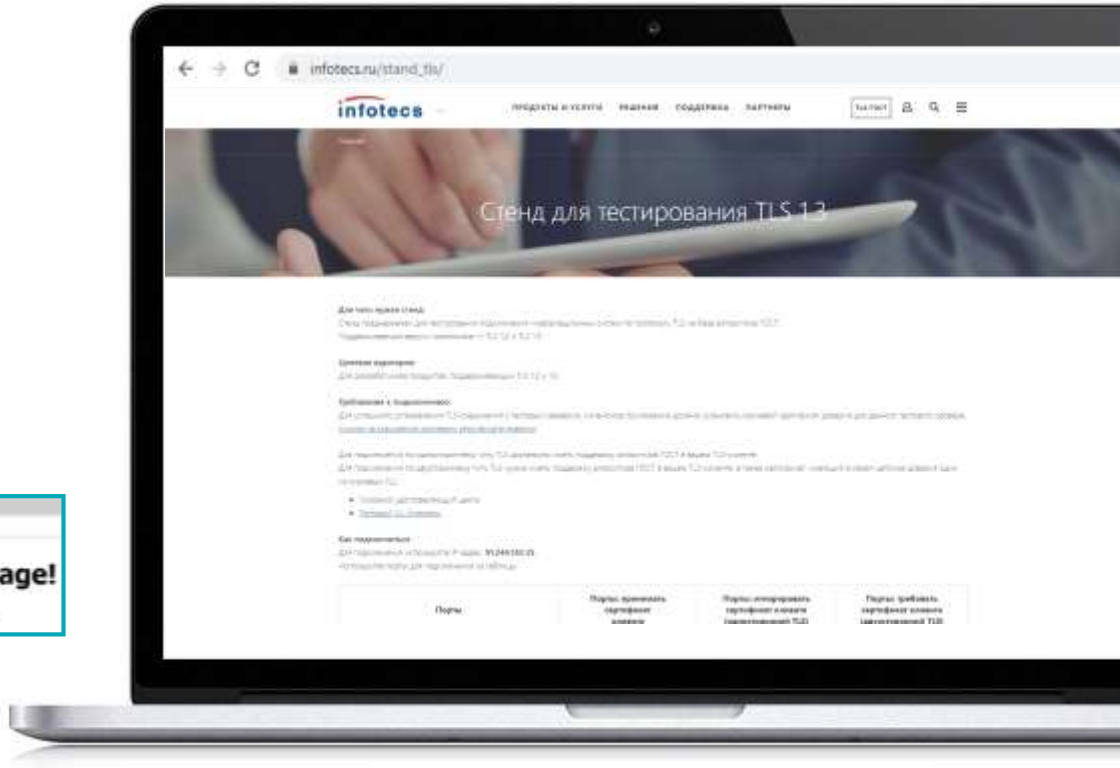
Протестировать TLS 1.2 и 1.3

на нашем стенде

https://infotecs.ru/stand_tls/

1. Подключиться по IP
2. Выбрать необходимый режим: односторонний/двусторонний
3. Получить сообщение об успешном подключении:





Спасибо за внимание!

Еранов Сергей

e-mail: sergey.eranov@infotecs.ru

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow