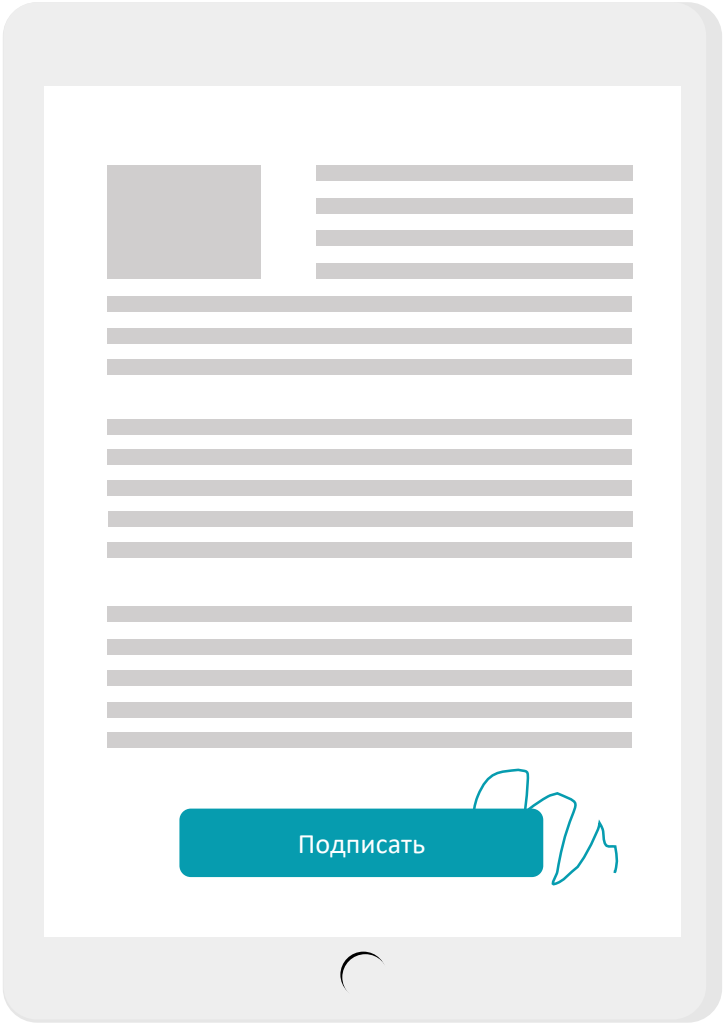
Криптография для разработчиков прикладных систем

Арина Эм



Сразу пример

- Аутентификация пользователя
- Загрузка документа по защищенному каналу
- Подпись

В таких приложениях используются криптографические функции

- Электронная подпись
- Хеширование
- Шифрование
- Организация TLS

СКЗИ: какое выбрать?

Самостоятельные	Серверные	TLS Gateway PKI Service
	Мобильные	PKI CLient
Прикладные	Серверные Мобильные	ViPNet OSSL ViPNet CSP

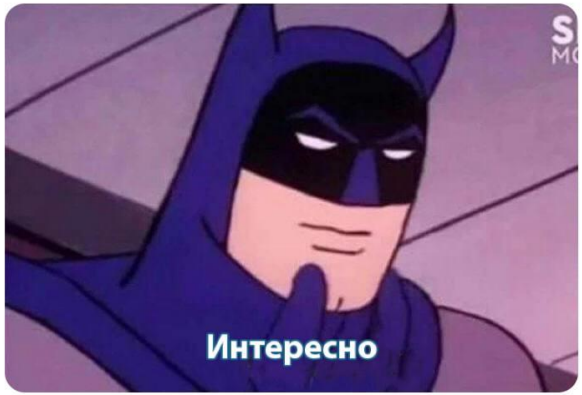
Зачем использовать криптобиблиотеки?

Потому что это проще и дешевле

Что нужно учитывать при разработке

Математика
Алгоритмы
ГОСТы
Требования
Лицензии
Сертификация
Ответственность
Безопасность
Корректность
Разработка
Сроки
Бюджет

Когда потратил 4 часа на создание функции, а потом нашёл библиотеку, в которой она реализована проще и лучше:



Криптобиблиотеки ИнфоТеКС помогают разработчикам

- Берегут время разработки
- Сложно неправильно использовать
- Реализуют сильную криптографию
- Кроссплатформенные
- Используют стандартные интерфейсы

Криптобиблиотеки ИнфоТеКС используют для вызова криптофункций

И для реализации

- Электронной подписи
  - ГОСТ Р 34.10-2012
- Хеширования
  - ГОСТ Р 34.11-2012
- Шифрования
  - ГОСТ Р 34.12-2015
  - ГОСТ Р 34.13-2015
- Организации TLS-соединений
- Работы с ключами на внешних устройствах

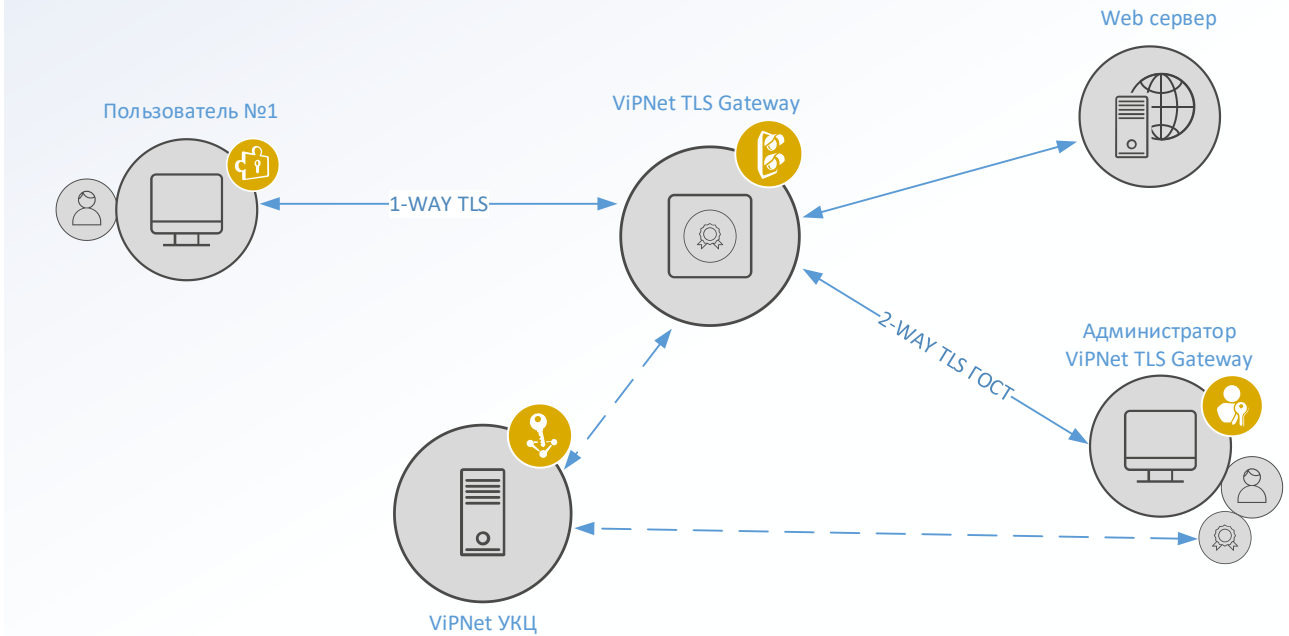
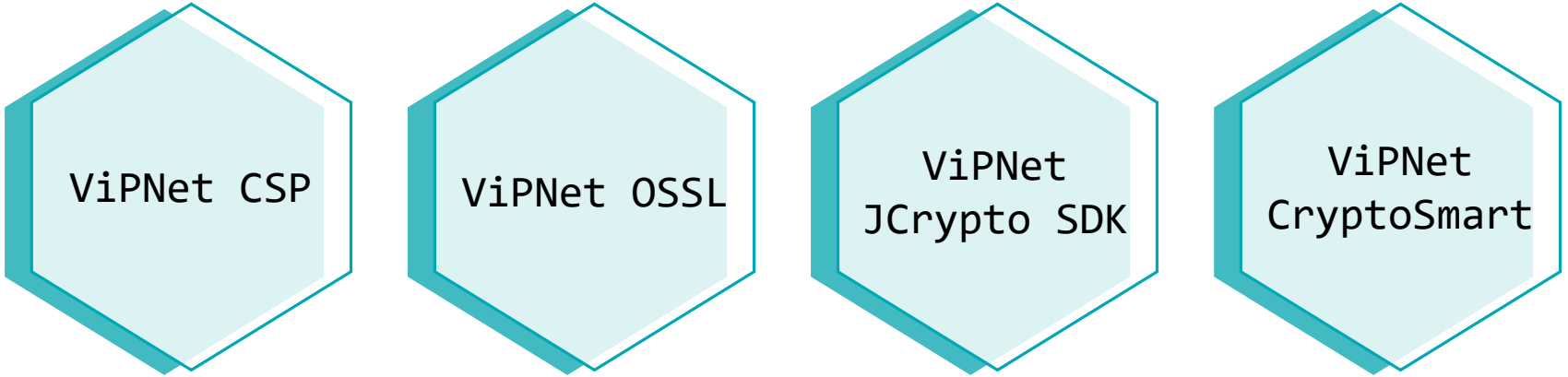


Схема удаленных защищенных подключений

Задачи:

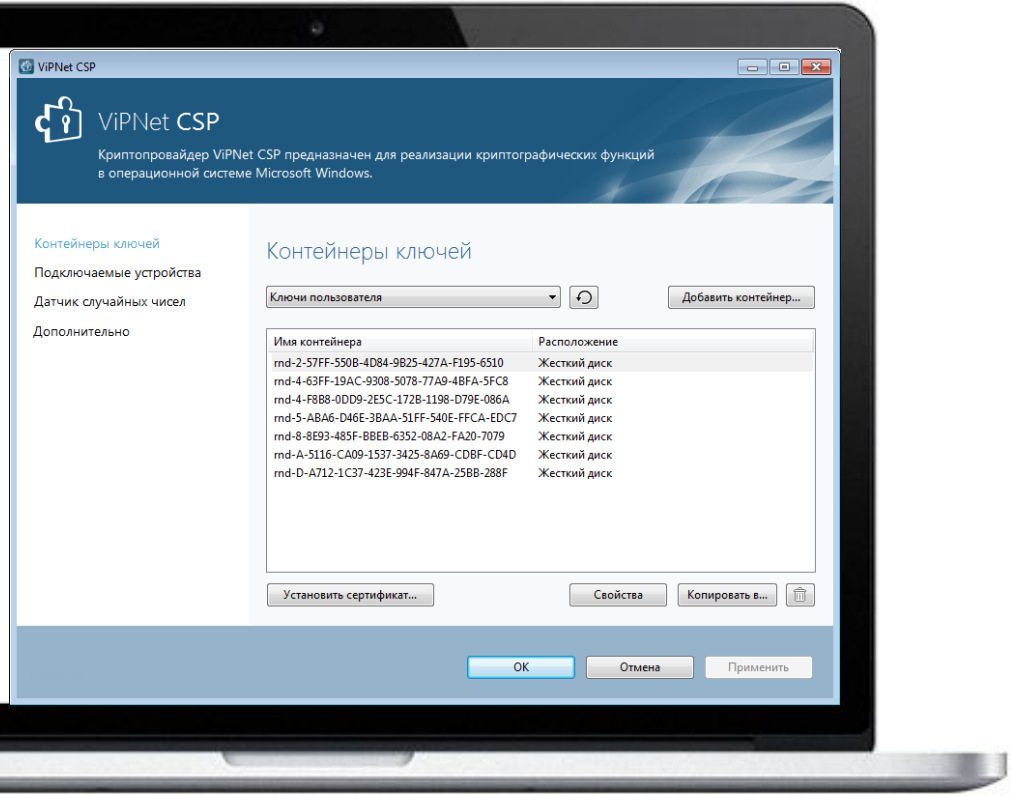
- Подтверждение подлинности сервера
- Защита передаваемых данных
- Защита соединений
- Аутентификация клиентов

Криптобиблиотеки ИнфоТеКС



ViPNet CSP

Сертифицированный криптопровайдер (КС1, КС2, КС3)



Интерфейсы

MS CryptoAPI
MS CNG (BCrypt)
PKCS#11

Токены

ViPNet HSM
RuToken
JaCarta
R301 Форос
eSmart token
eSmart token ГОСТ
Gemalto

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-4103** от "**10**" **августа** 2021 г.

Действителен до "**10**" **августа** 2024 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **ViPNet CSP 4.4 (Версия 4.4.2)** (исполнения 1, 2, 3, 4, 5, 6) в комплектации согласно формуляру ФРКЕ.00106-07 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 исполнений 3, 6), 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 исполнений 3, 6) 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 №№ 637Д-000506, 637Д-000507, 637Д-000508, 637Д-000509, 637Д-000510, 637Д-000511.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00106-07 30 01 ФО.

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

ТЕХНО infotecs ФЕСТ 2021

ViPNet CSP 4.4 сертифицирован ФСБ

По классам КС1, КС2, КС3

ViPNet OSSL

Криптобиблиотека на базе OpenSSL (КС1, КС2, КС3)

ViPNet OSSL используют

- ViPNet TLS Gateway
- ViPNet PKI Service
- ViPNet PKI Client
- ViPNet SIES Unit
- ViPNet SIES MC
- ViPNet HSM

Интерфейсы

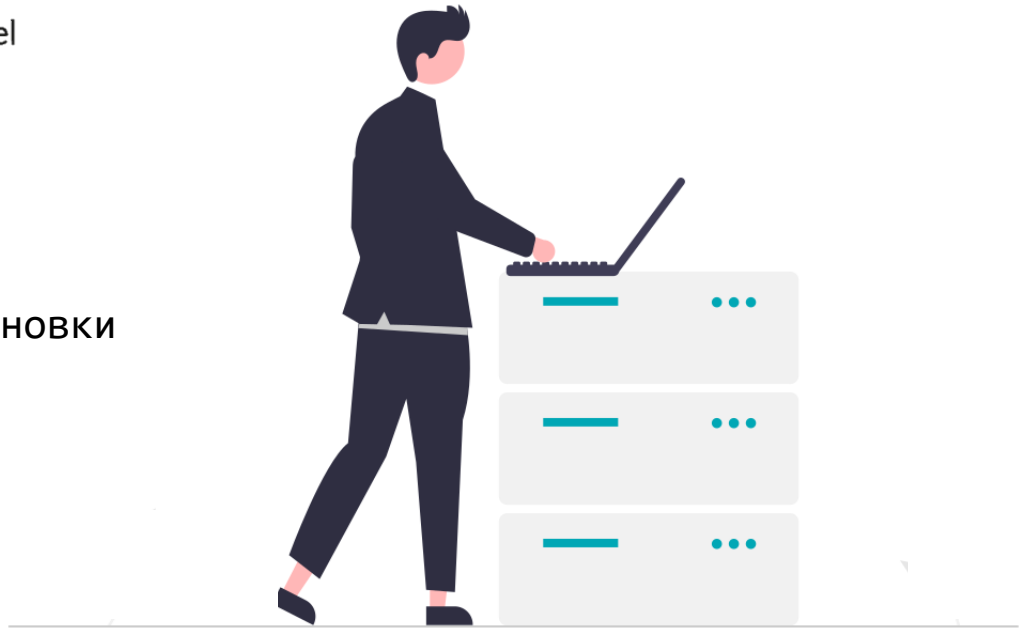
PKCS#11
OpenSSL

Токены

ViPNet HSM
Рутокен
JaCarta

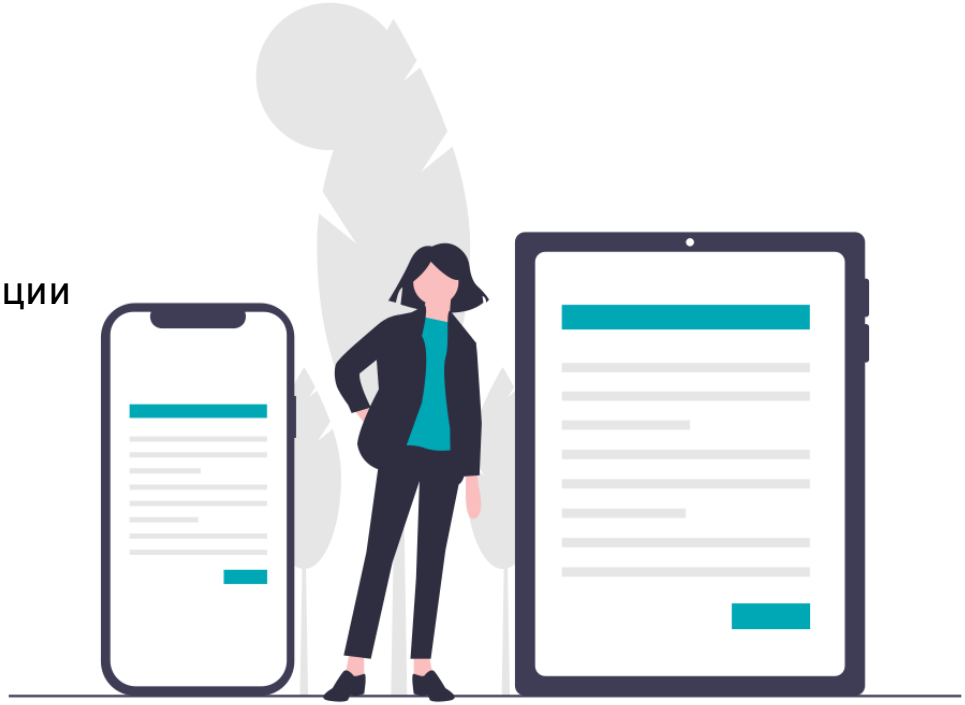
ViPNet OSSL для серверов

- Не нужна оценка влияния
- Гибкость в выборе места установки
- Распараллеливание процессов



ViPNet OSSL для клиентов

- Возможность использовать функции подписи и шифрования на клиентских устройствах
- Нужна оценка влияния (кроме stunnel)



Место для сертификата

Сертификация

Заключение ФСБ – ориентировочно осенью 2021 года

ViPNet JCrypto SDK

Криптобиблиотека на JAVA (КС1)

Интерфейсы

JNI
JCA
PKCS#11

Токены

ViPNet HSM
Рутокен
JaCarta

ViPNet JCrypto SDK использует

Hauberk Pro

Криптография в блокчейне

Электронная подпись

Аутентификация участника

Хеширование

Связывание блоков

Организация TLS-соединений

Взаимодействие между сегментами организаций

ViPNet CryptoSmart

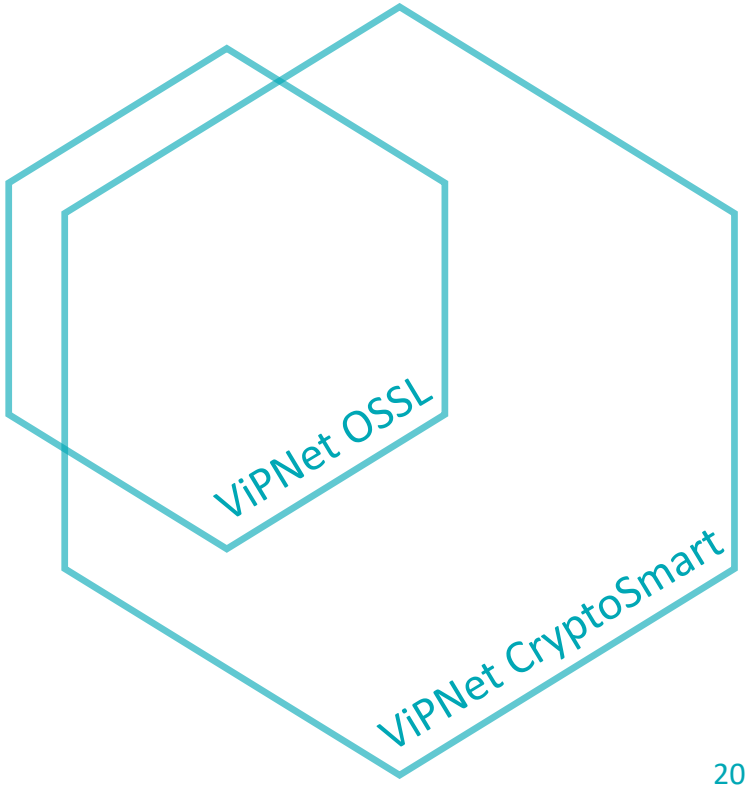
СКЗИ для блокчейн-платформ

- Защита конфиденциальных данных
- Юридическая значимость транзакций
- Интеграция с отечественной PKI
- Соответствие требованиям ПКЗ-2005

ViPNet CryptoSmart

Использует ViPNet OSSL для

- Выполнения всех операций ЭП
- Шифрования и имитозащиты данных
- Построения TLS-соединений
- Хеширования данных



Место для сертификата

ViPNet CryptoSmart на сертификации ФСБ

Проходит сертификационные испытания по классам КС1 и КС2

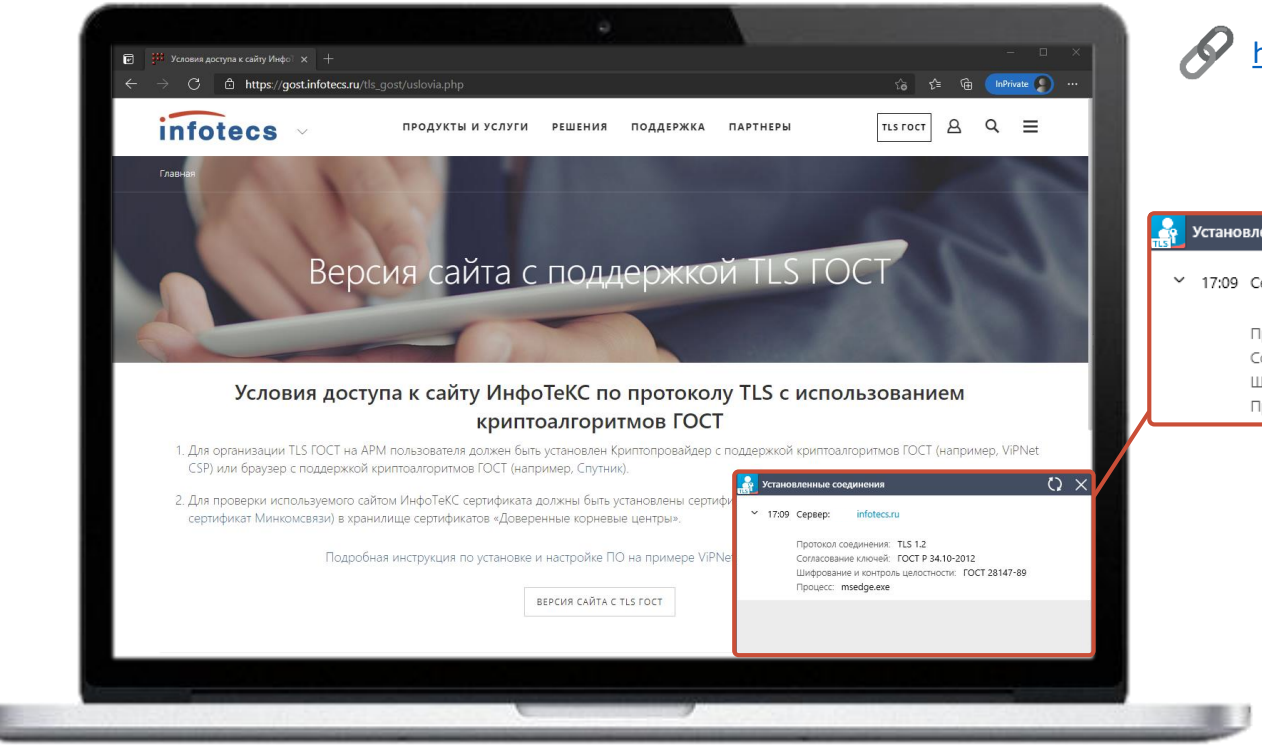
Саммари

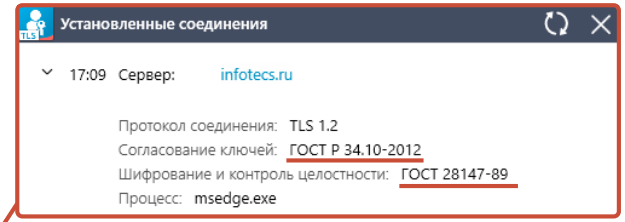
Продукт	ViPNet CSP	ViPNet OSSL	ViPNet JCrypto SDK	ViPNet CryptoSmart
Платформы				
Интерфейсы	MS CryptoAPI MS CNG	PKCS#11 OpenSSL	JNI/JCA PKCS#11	MSP NetCSP BCCSP Lite
Класс защиты	КС1-КС3	КС1-КС3	КС1	КС1, КС2

Как можно попробовать

1. Подключиться к сайту ИнфоТеКС по TLS ГОСТ
2. Протестировать TLS 1.2 и 1.3 на нашем стенде
3. Купить или взять на тесты: soft@infotecs.ru

Подключиться к сайту ИнфоТеКС по TLS ГОСТ



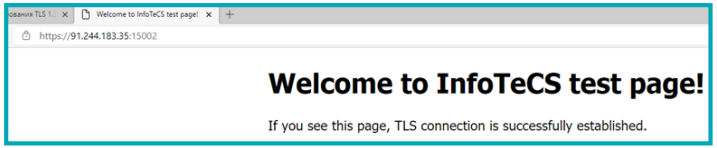


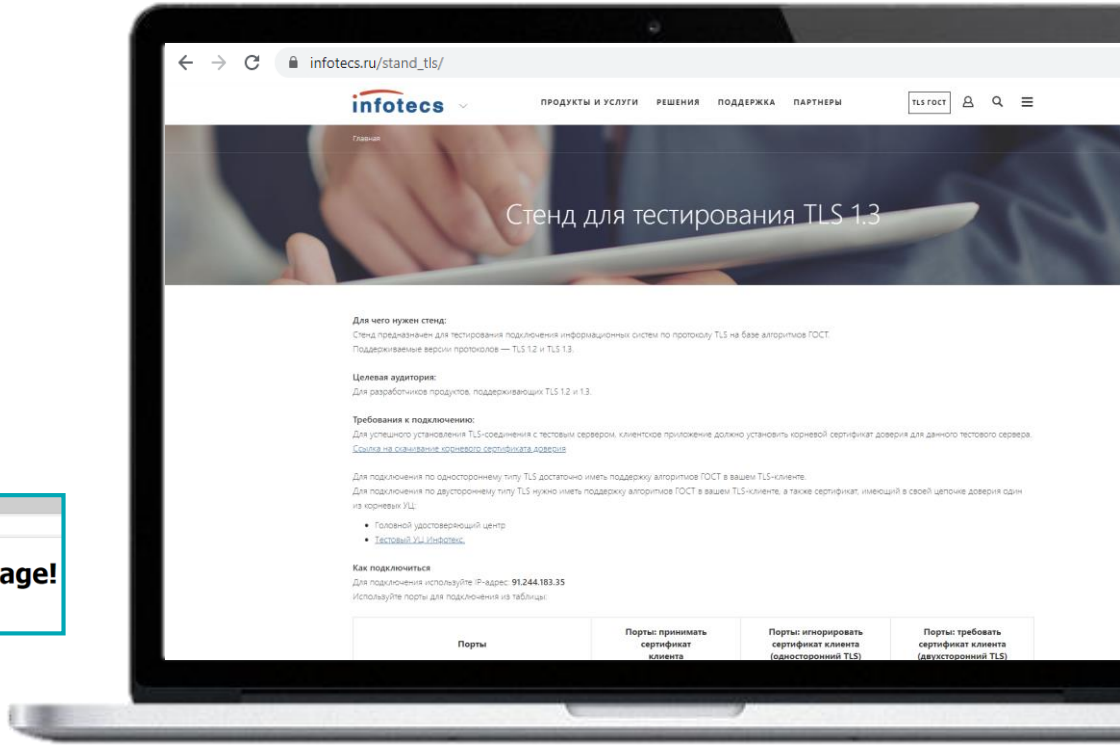
https:/infotecs.ru/

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:





Вы могли пропустить

Вебинары по этой теме

ViPNet OSSL. Обзор продукта

26 ноября 2020

ViPNet OSSL: криптопровайдер на базе OpenSSL

26 августа 2021

Криптобиблиотеки или как научить свое приложение подписывать документы

08 апреля 2021

ViPNet CSP. Что нового?

14 октября 2021

https://infotecs.ru/webinars/archive/

ТЕХНО infotecs 2021 Фест

На связи!

Арина Эм

Arina.Em@infotecs.ru

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow