Развертывание и настройка дуального TLS ГОСТ | RSA

Еранов Сергей
Долгополов Игорь

ТЕХНО infotecs 2022 ФЕСТ

Зачем нам ГОСТ TLS?

Стандартизация

- ГОСТ
- RFC
- Рекомендации ТК26
- Контрольные примеры

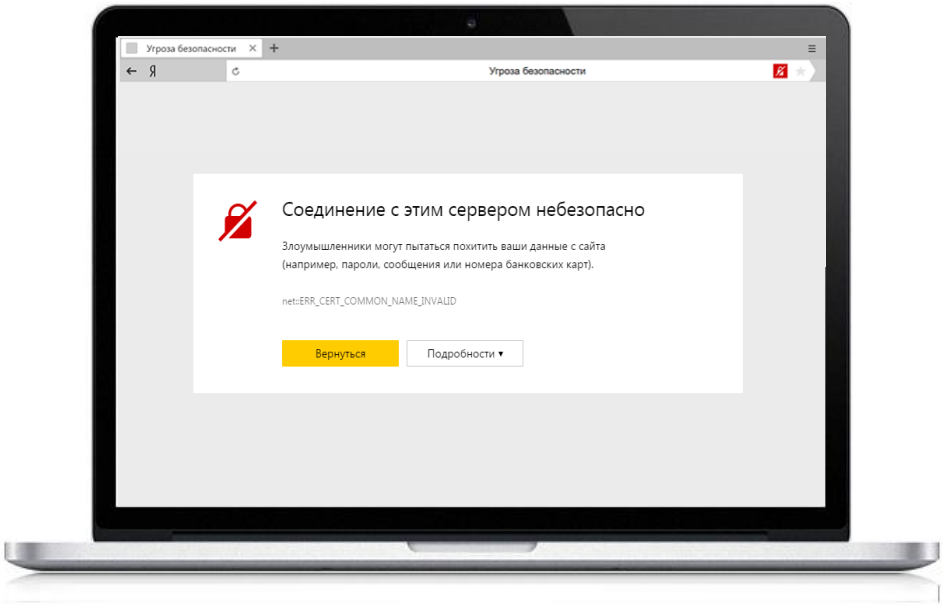
IETF

Результат: мультивендорность для конечных потребителей

Распространенность

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

Независимость и безопасность



Какие возникают проблемы

Отзыв сертификатов со стороны зарубежных УЦ

Как решаются эти проблемы

Используется УЦ Минкомсвязи на NIST-алгоритмах

Ведется запуск **Национального удостоверяющего центра**

Проблемы и вопросы

Где получить сертификат сервера

Где брать сертификат для ГОСТ TLS?

Минцифры выдает RSA-сертификаты для организаций

Корневой скачивается по https на сертификате Sectigo

Кому выдан:	*.gosuslugi.ru
Кем выдан:	Sectigo RSA Domain Validation Secure Server CA

Получение ГОСТ сертификата не встроено в инфраструктуру провайдеров хостинга

Если я физлицо или ИП, где мне взять сертификат для своего сайта?

Как настроить TLS ГОСТ на сервере

Провайдеры хостинга сайтов не предлагают такой услуги

VPS/VDS провайдеры не предлагают готового решения

NGINX + APACHE HTTP SERVER PROJECT + OpenSSL Cryptography and SSL/TLS Toolkit

Требуется квалификация

Только аутентификация и защита канала

Нет дуального режима «из коробки»

** Вопросы юридического характера не рассматриваем*

Где пользователю взять СКЗИ?

Что пользователю нужно?

- Чтобы работало
- Бесплатно
- Просто
- Разные платформы
- Разные браузеры

Проблемы пользователей

- Установка корневых
- Обновление CRL
- Поддержка различных ОС
- Возможность работы в любимом браузере

ViPNet TLS Gateway

ViPNet TLS Gateway

Высокопроизводительный TLS-криптошлюз

- Аутентификация клиента и сервера
- Управление доступом на основе сертификатов
- Дуальный режим работы
- Удаленное управление
- Кластеризация
- TLS 1.0 – 1.3
- IPv6

Модификации

Исполнение	TLS 550	TLS 1100	TLS 5500
Форм-фактор	ПАК 19” Rack 1U	ПАК 19” Rack 1U	ПАК 19” Rack 1U
Предельная пропускная способность (Мбит/с)	до 600	до 1800	до 7600
Число одновременных соединений	до 7000	до 14000	до 65000
Интерфейсы	6x Ethernet 10/100/1000	8x Ethernet 10/100/1000 4x 1G Ethernet Fiber SFP	4x Ethernet 10/100/1000 8x 10G Ethernet Fiber SFP+

Платформы виртуализации

ViPNet TLS Gateway сертифицирован

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

Клиентское СКЗИ

ViPNet CSP

ViPNet PKI Client

Любое сертифицированное СКЗИ

ТЕХНО infotecs 2022 ФЕСТ

Отдаем на полгода бесплатно

- TLS Gateway VA
- Бесплатная лицензия на полгода

Акция «За безопасность!»

ТЕХНО infotecs 2022 ФЕСТ

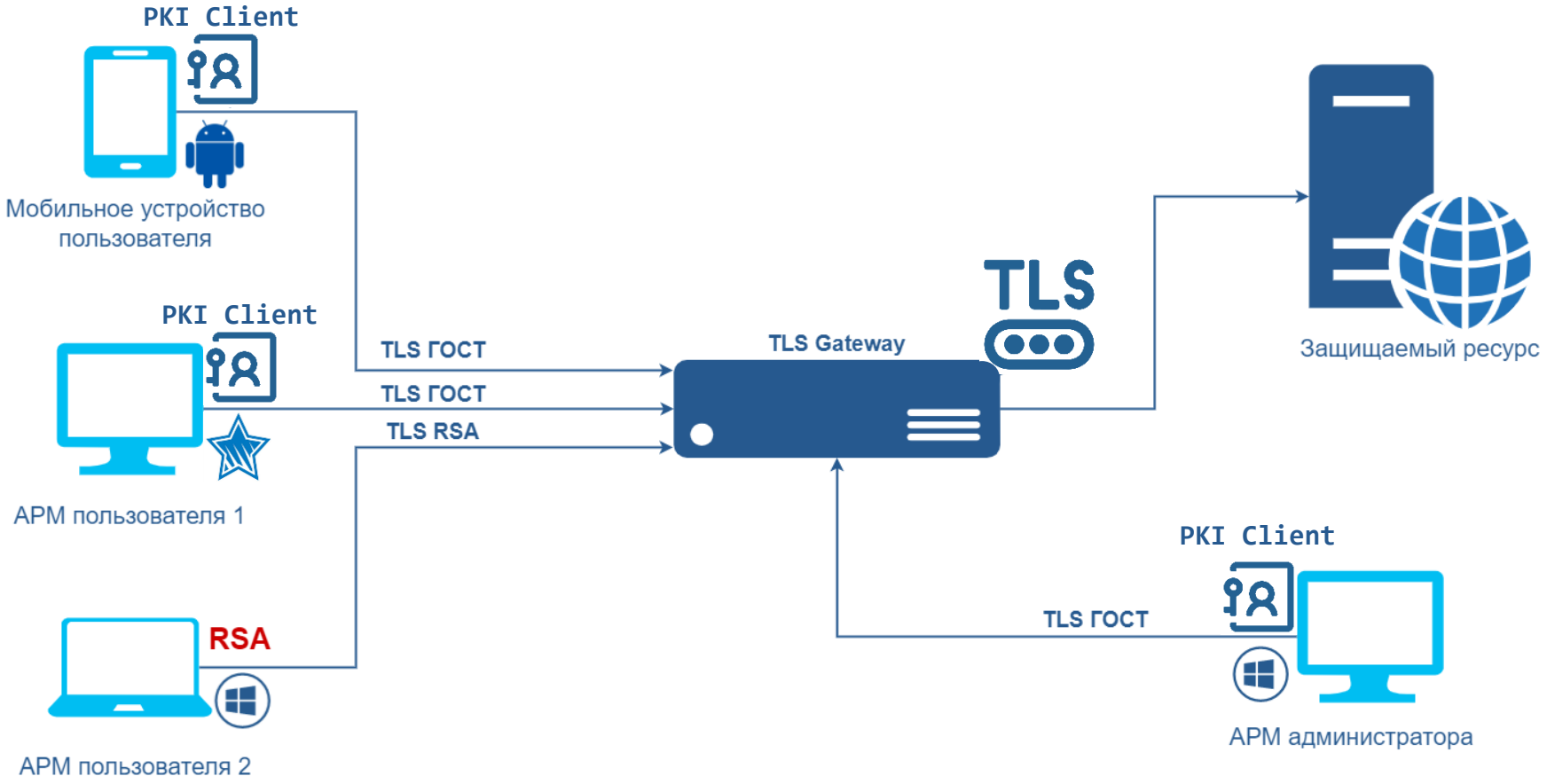
Лицензии на перечисленные продукты предоставляются **на безвозмездной основе** на 6 месяцев!!!

Защита каналов связи	Системы управления и мониторинга	Защита рабочих станций и серверов	Обнаружение и предотвращение компьютерных атак
• ViPNet Coordinator VA • ViPNet xFirewall VA • ViPNet TLS Gateway VA • ViPNet PKI Client • ViPNet Client	• ViPNet Administrator • ViPNet Policy Manager	• ViPNet SafeBoot • ViPNet SafePoint • ViPNet IDS HS*	• ViPNet TIAS VA • ViPNet IDS MC VA • ViPNet IDS NS VA • ViPNet IDS HS*

Перевод отдела технической поддержки на усиленный режим работы и предоставление консультаций по подбору оптимальных решений для обеспечения информационной безопасности в рамках импортозамещения. Для получения консультации вы можете отправить электронное письмо с вопросами и контактными данными на адрес sos@infotecs.ru.

Демонстрация

Сценарий: Дуальный режим



ТЕХНО 2022 infotecs Фест

Спасибо за внимание!

Еранов Сергей

e-mail: sergey.eranov@infotecs.ru

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news