ViPNet OSSL:

криптопровайдер на базе OpenSSL

Арина Эм
Менеджер продукта

Вебинар про ViPNet OSSL vol.1

СКАЧАТЬ ПРЕЗЕНТАЦИЮ

ViPNet OSSL. Обзор продукта

ViPNet PKI

26 ноября 2020

26 ноября прошел вебинар **«ViPNet OSSL. Обзор продукта»**.

Вебинар был посвящен криптографической библиотеке для встраивания ViPNet OSSL. Спикер Арина подробно рассказала о самом продукте и о его возможностях.

Спикер Вебинара

Арина Эм

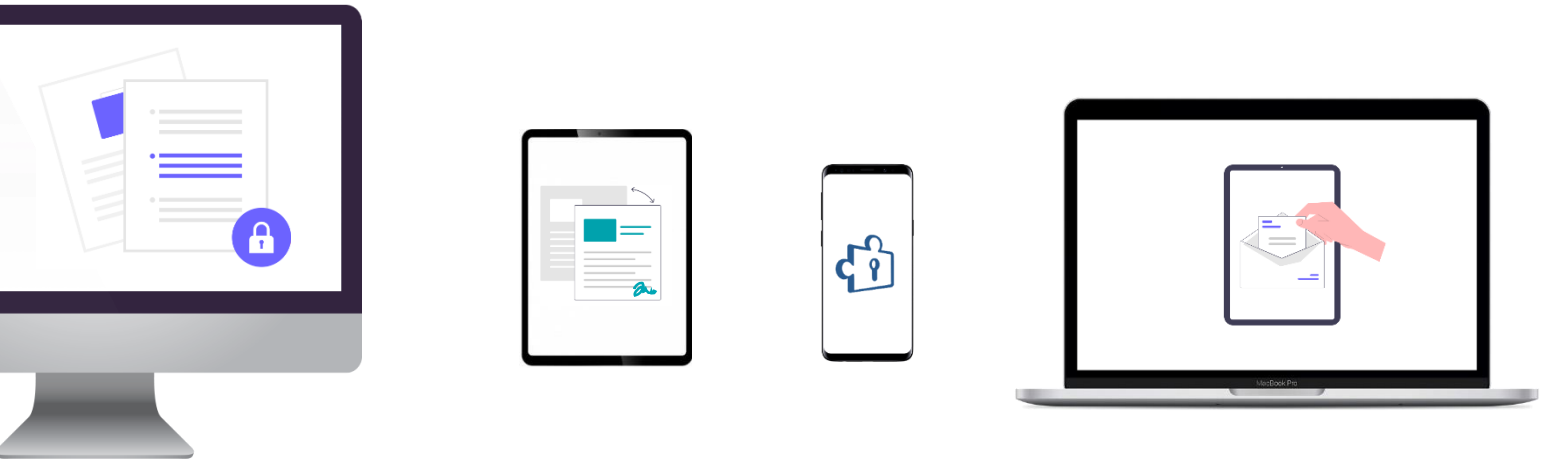
Менеджер отдела развития продуктов

Ссылка на вебинар:
https://infotecs.ru/webinars/archive/vipnet-ossl-obzor-produkta.html

Про ViPNet OSSL

ViPNet OSSL

ПО на базе библиотеки OpenSSL



ViPNet OSSL используется для вызова криптофункций

И для реализации

- Электронной подписи
- Хэширования
- Шифрования
- Организации TLS 1.2, TLS 1.3
- Работы с ключами на внешних устройствах

Функции ViPNet OSSL

Форматы

CMS
XML
PFX
CAdES
XAdES
X.509

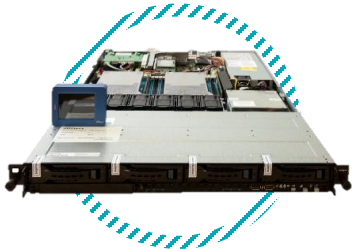
Интерфейсы

OpenSSL
PKCS#11
ViPNet OpenSSL Extensions

Протоколы

TSP
OCSP

Какие токены поддерживаем



ViPNet HSM

JaCarta 2 ГОСТ
JaCarta 2 PKI
JaCarta 2 PKI/ГОСТ

RuToken ЭЦП 2.0
Rutoken Lite

Преимущества

Кросс-платформенность

Актуальные протоколы

ГОСТ Р 34.10-2012
ГОСТ Р 34.11-2012
ГОСТ Р 34.12-2015
ГОСТ Р 34.13-2015
TLS 1.2
TLS 1.3

Стандартные интерфейсы

OpenSSL
PKCS#11

Поддержка разработчика

Комплект SDK
Сопровождение
Консультации

ViPNet OSSL: TLS

цифры

	Односторонний TLS	Двусторонний TLS
Скорость передачи данных	8300 Мбит/с	8200 Мбит/с
Скорость установления соединений	8425 соед/с	5 260 соед/с
Время установления соединения	11 мс	17 мс

Условия:
Debian 9.12.0
nginx 1.14.0
ViPNet OSSL 5.0
ViPNet Coordinator HW 5000 Q1
12 ядер, HyperThreading ON
GOST2012-GOST8912-GOST8912
Длина ключа 256
TLS 1.2

ViPNet OSSL: Подпись

цифры

Потоки	Подпись, шт/с	Проверка подписи, шт/с
1	23,1k	3,5k
24	255,1k	35,9k

Условия:
Алгоритм ГОСТ 34.10-2012 (256)

Место для сертификата

Сертификация

Заключение ФСБ - ориентировочно осенью 2021 года

Для кого этот продукт?

Для кого этот продукт?

Для разработчиков прикладного ПО

Продукты Инфотекс используют ViPNet OSSL

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

СКЗИ: какое выбрать?

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

ViPNet TLS Gateway использует ViPNet OSSL

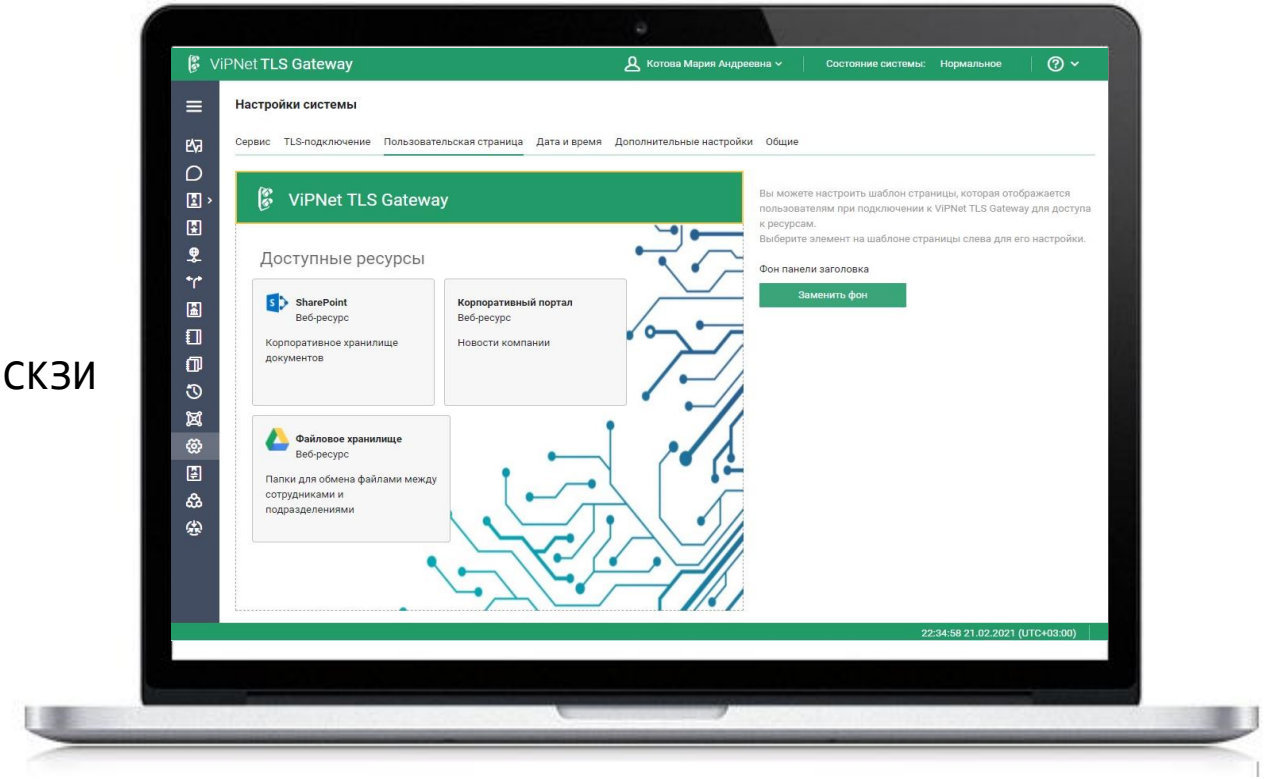
– высокопроизводительный TLS-криптошлюз

- Односторонняя/двусторонняя аутентификация
- Управление доступом на основе сертификатов
- Поддержка центров доверия
- Удаленное управление

ViPNet TLS Gateway

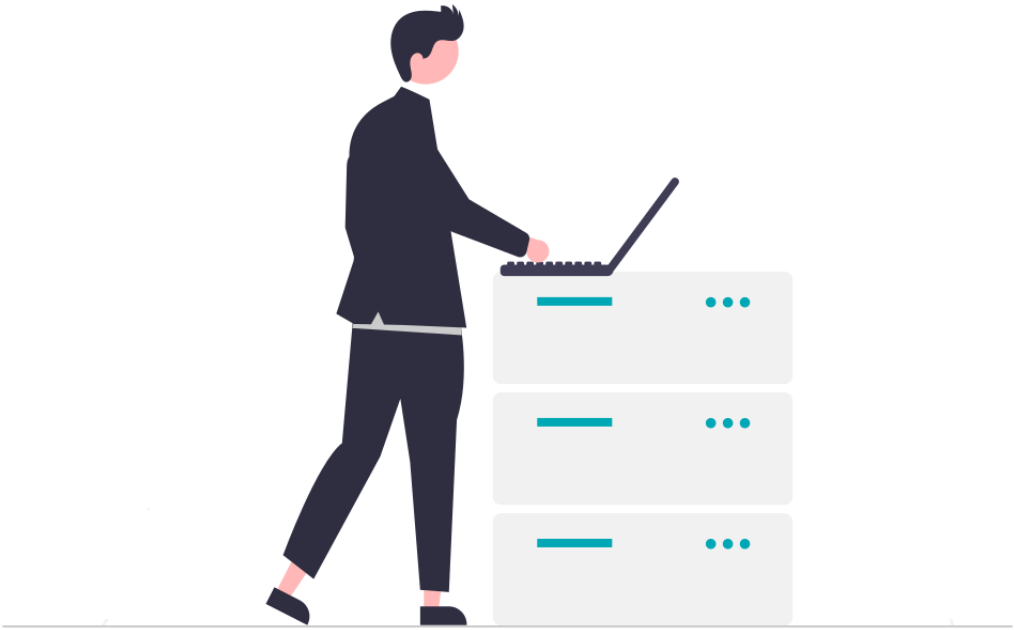
Клиентское ПО – СКЗИ:

- ViPNet CSP
- ViPNet OSSL
- ViPNet PKI Client
- Сертифицированное СКЗИ

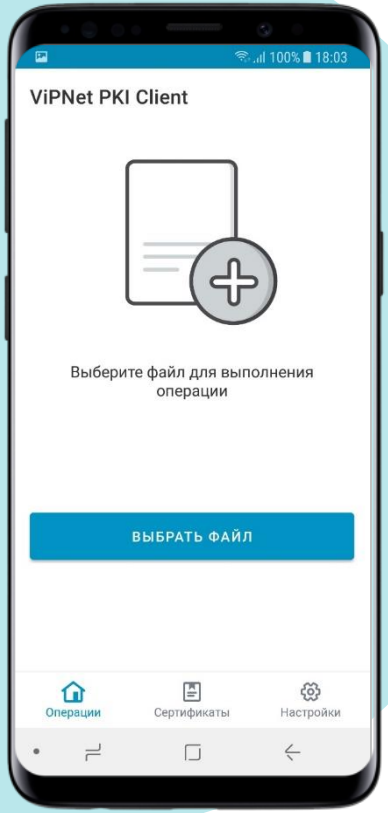


ViPNet OSSL для серверов

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



PKI Client использует ViPNet OSSL



– клиент для работы в инфраструктуре открытых ключей

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

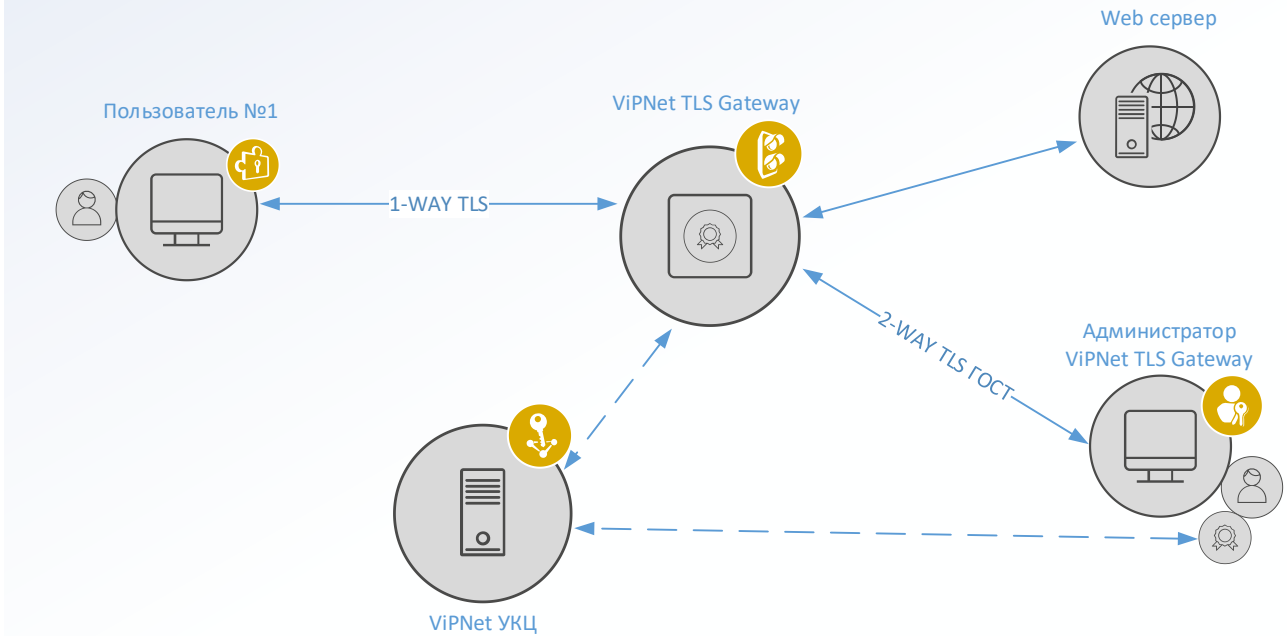


Схема удаленных защищенных подключений

Задачи:

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

Лицензирование

Для серверов

Для клиентов

Десктоп

Мобильные

Лицензирование

Приложение поставляется от производителя

Приобретение продукта
и получение серийного номера

Регистрация на сервере
регистрации ИнфоТеКС

Лицензирование

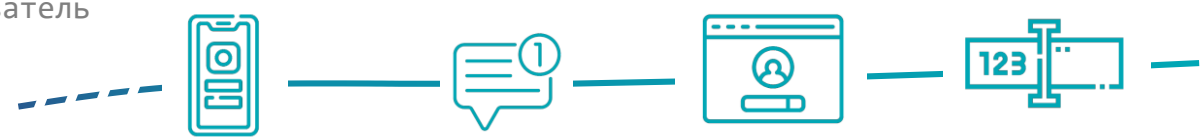
Приложение поставляется через магазины

Разработчик

Присвоить серийный номер продукту

Встроить серийный номер в сценарий регистрации ПО

Пользователь



Отправить учетные данные

Получить код по SMS

Регистрация

Получение кода активации продукта

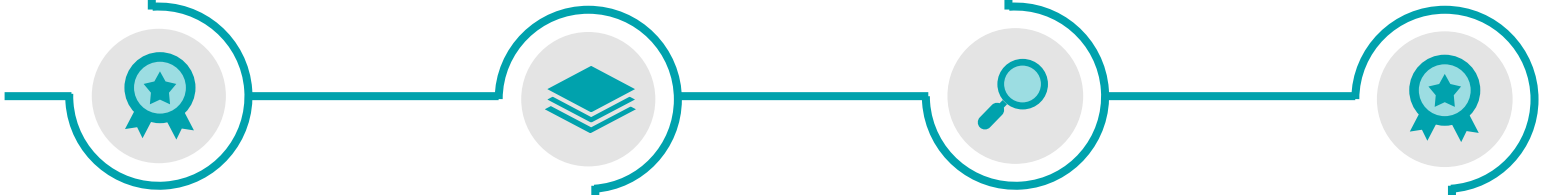
Заключение на прикладное ПО

Сертификат на библиотеку

Сертифицируем СКЗИ и список белых функций

Оценка влияния на СКЗИ

В Исследовательской лаборатории



Встраивание в ПО

С использованием белых функций

Заключение о проведении оценки влияния

На прикладное ПО

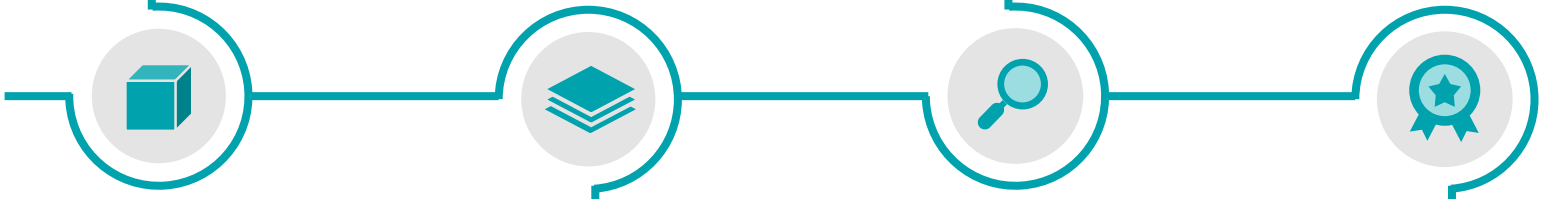
Сертификация прикладного ПО

Библиотека

Без ограничений на использование белых функций

Тематические исследования СКЗИ

В Исследовательской лаборатории

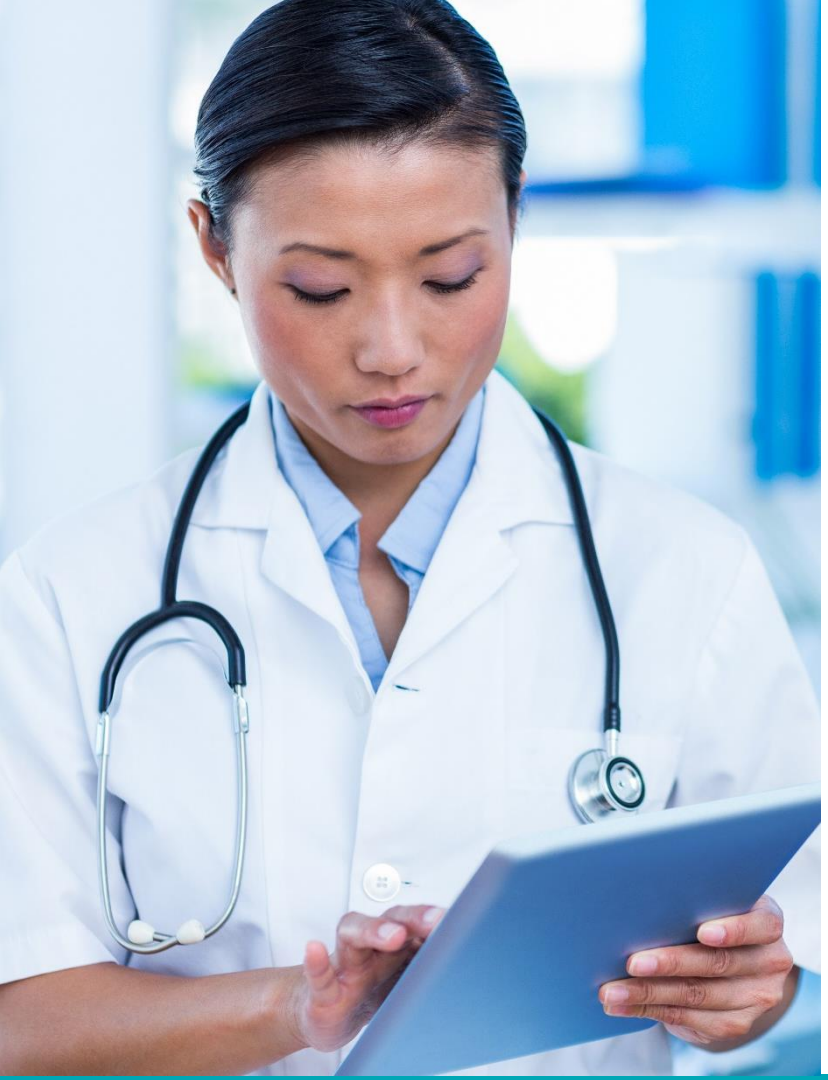


Встраивание в ПО

Сертификат

На прикладное ПО

Сценарии применения



ПО для медицинских организаций

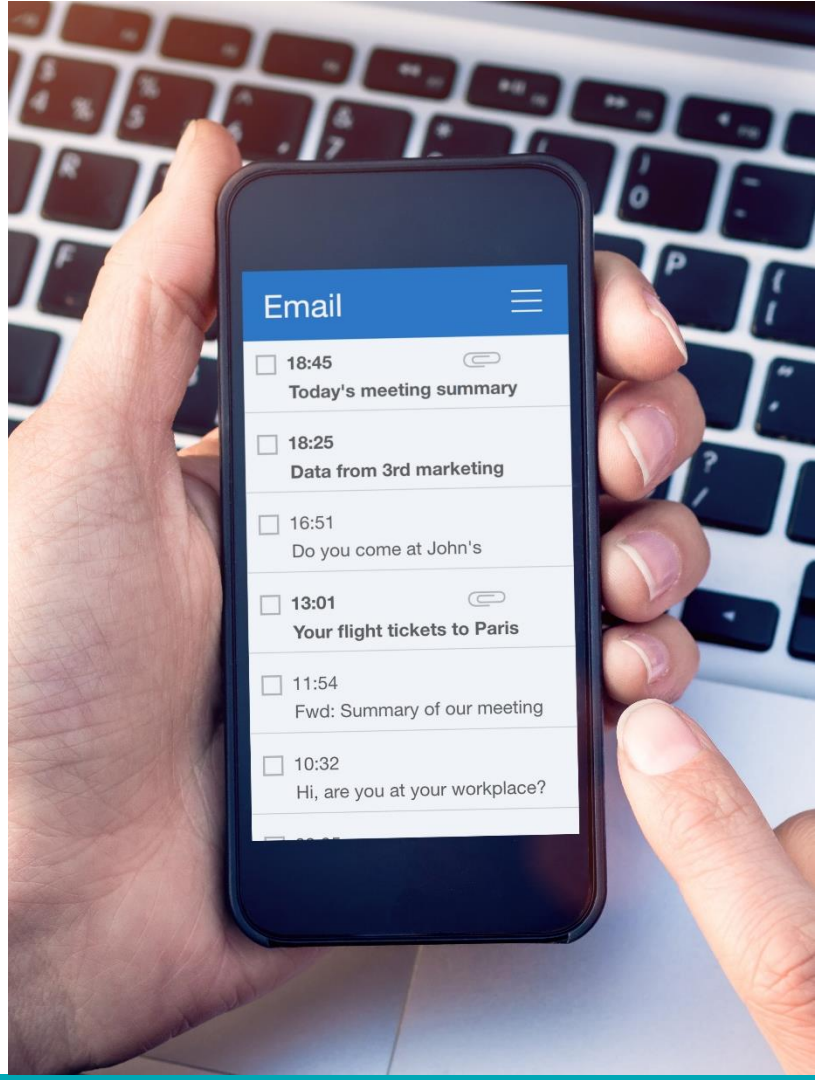
Безопасно загружать медицинские карты, вносить в них изменения

ПО для сотрудников на производстве

- Загружать документы на мобильные устройства
- Шифровать файлы в приложении

Офисные приложения

- Формировать ЭП
- Шифровать сообщения и файлы внутри приложения



Частые вопросы

А можно как-то обойтись без сертификации своего ПО?

Все равно нужно проводить оценку влияния.

Без сертификационных испытаний можно обойтись, если использовать Apache, NGINX, stunnel

Частые вопросы

Работает с браузерами?

ViPNet OSSL напрямую не работает с браузерами.

Для работы через браузер подойдет ViPNet PKI Client

Как с нами связаться

Купить или взять на тесты:
soft@infotecs.ru

Есть идея реализации совместного решения на базе ViPNet OSSL:
techpartners@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: