ViPNet OSSL
Обзор продукта

Арина Эм

Средства криптографической защиты

САМОСТОЯТЕЛЬНЫЕ

ViPNet PKI Client

ВСТРАИВАЕМЫЕ

ViPNet CSP

ViPNet OSSL

Что нужно для разработки СКЗИ?

ДЛИННЫЙ ПУТЬ

Модель угроз нарушителя

Бюджеты

Лицензии на разработку СКЗИ

Эксперты, разработчики

Реализация алгоритмов

...

Что нужно для разработки СКЗИ?

ДЛИННЫЙ ПУТЬ

Модель угроз нарушителя

Бюджеты

Лицензии на разработку СКЗИ

Эксперты, разработчики

Реализация алгоритмов

...

КОРОТКИЙ ПУТЬ

Готовое решение от вендора:

Криптографическая библиотека

TLS Gateway

ViPNet PKI Client

ViPNet PKI Service

ViPNet OSSL

ViPNet HSM

ViPNet SIES Unit

ViPNet SIES MC

ViPNet OSSL

продукт, позволяющий использовать российские криптоалгоритмы в криптографических форматах и протоколах, которые реализованы в библиотеке с открытым исходным кодом OpenSSL.

Функции ViPNet OSSL

ФОРМИРОВАНИЕ/ПРОВЕРКА ЭП СОЗДАНИЕ КЛЮЧЕЙ ЭП

ГОСТ Р 34.10-2001*
ГОСТ Р 34.10-2012

ОРГАНИЗАЦИЯ ЗАЩИЩЕННЫХ СОЕДИНЕНИЙ

TLS 1.2
TLS 1.3

ХЭШИРОВАНИЕ

ГОСТ Р 34.11-94*
ГОСТ Р 34.11-2012

ПОДДЕРЖКА ФОРМАТОВ

PKCS#7 (CMS) CAdES X.509
PKCS#12 (PFX) XMLDSig

ШИФРОВАНИЕ

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

ИНТЕРФЕЙСЫ

Интерфейс OpenSSL
Интерфейс PKCS#11
Интерфейс ViPNet OpenSSL Extensions

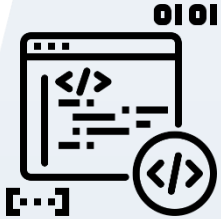
РАБОТА С КЛЮЧАМИ НА ВНЕШНИХ УСТРОЙСТВАХ

ПОДДЕРЖКА ПРОТОКОЛОВ

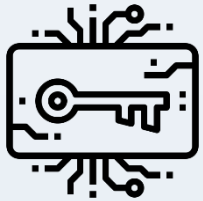
TSP OCSP

Как работает ViPNnet OSSL?

Приложение

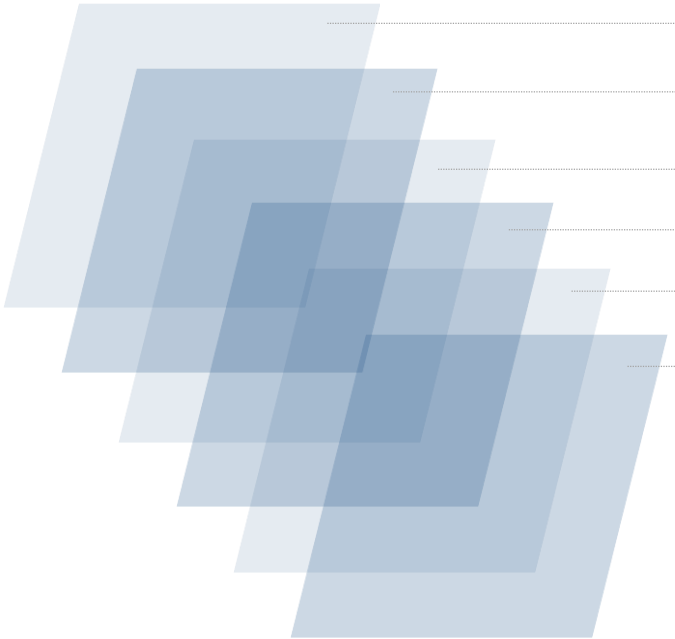


ViPNet OSSL



ViPNet SoftToken
(PKCS#11)

Как устроен ViPNnet OSSL?



Интерфейс OpenSSL

OpenSSL Cryptography and SSL/TLS Toolkit

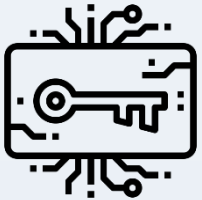
Интерфейс OpenSSL Engine

ViPNet OSSL Engine

Интерфейс PKCS#11

ViPNet SoftToken

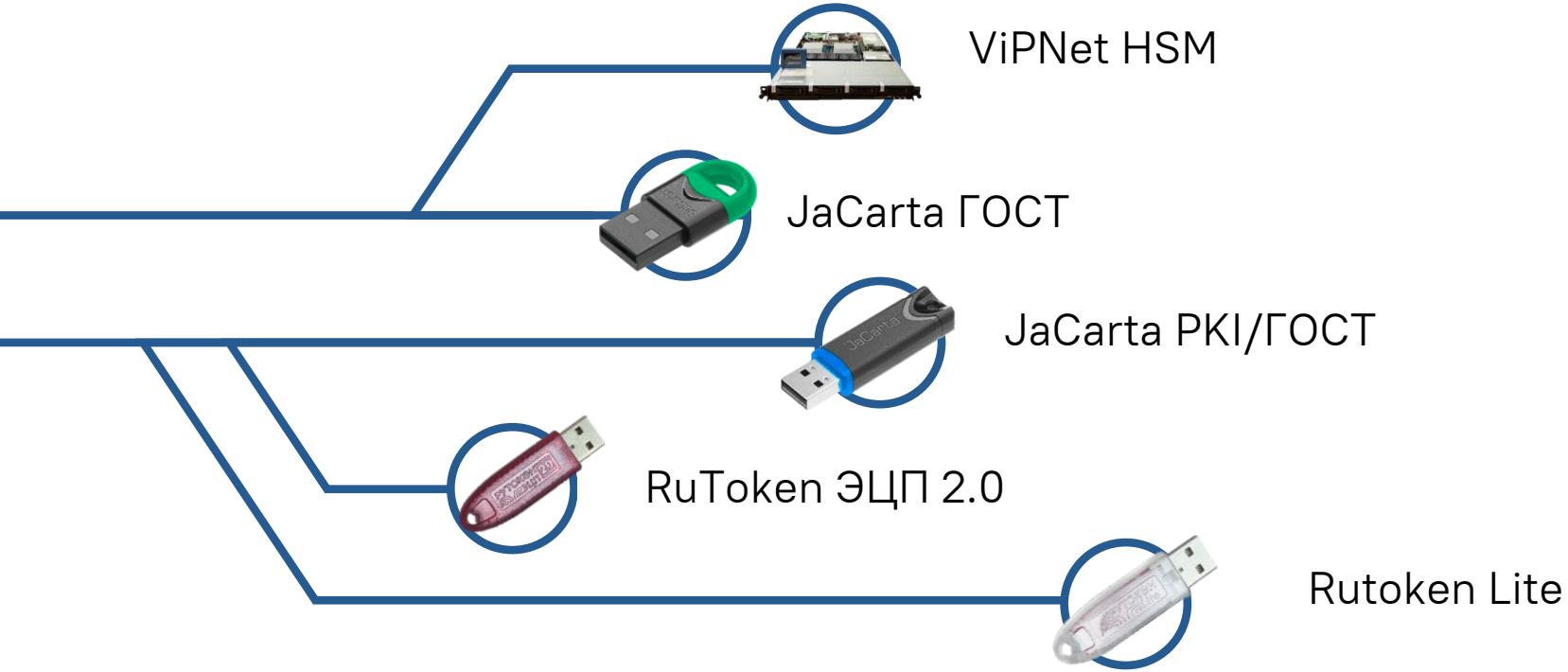
Реализации интерфейса PKCS#11



ViPNet SoftToken
(PKCS#11)

1. Выполнение криптографических операций через интерфейс PKCS#11 с учётом методических рекомендаций ТК26
2. Использование ключевых носителей разного типа, поддерживающих работу через интерфейс PKCS#11
3. Использование токенов с поддержкой алгоритмов ГОСТ на неизвлекаемых долговременных ключах

Какие устройства поддерживаем



Лицензирование

ПРОИЗВОДИТЕЛЬ/ДИСТРИБЬЮТОР

ШАГ 1: Приобретение продукта и получение серийного номера

ШАГ 2: Регистрация на сервере регистрации ИнфоТеКС

МАГАЗИНЫ ПРИЛОЖЕНИЙ

Разработчик

ШАГ 1: Присвоение серийного номера продукту Заказчика

ШАГ 2: Встраивание серийного номера в сценарий регистрации своего приложения

Пользователь

ШАГ 1: Отправка учетных данных

ШАГ 2: Получение кода через SMS

ШАГ 3: Регистрация на сервере регистрации ИнфоТеКС

ШАГ 4: Получение кода активации продукта

Как начать работать с библиотекой

НАСТРОЙКА

Первичная инициализация

Установка пакетов
Регистрация ViPNet OSSL
Инициализация ДСЧ
Настройка SoftToken

Выработка ключей

Генерация ключевой пары
Создание PKCS#10-запроса на сертификат
Установка сертификата

РАБОТА СТАНДАРТНЫХ ПРИЛОЖЕНИЙ

Настройка сервера nginx, apache

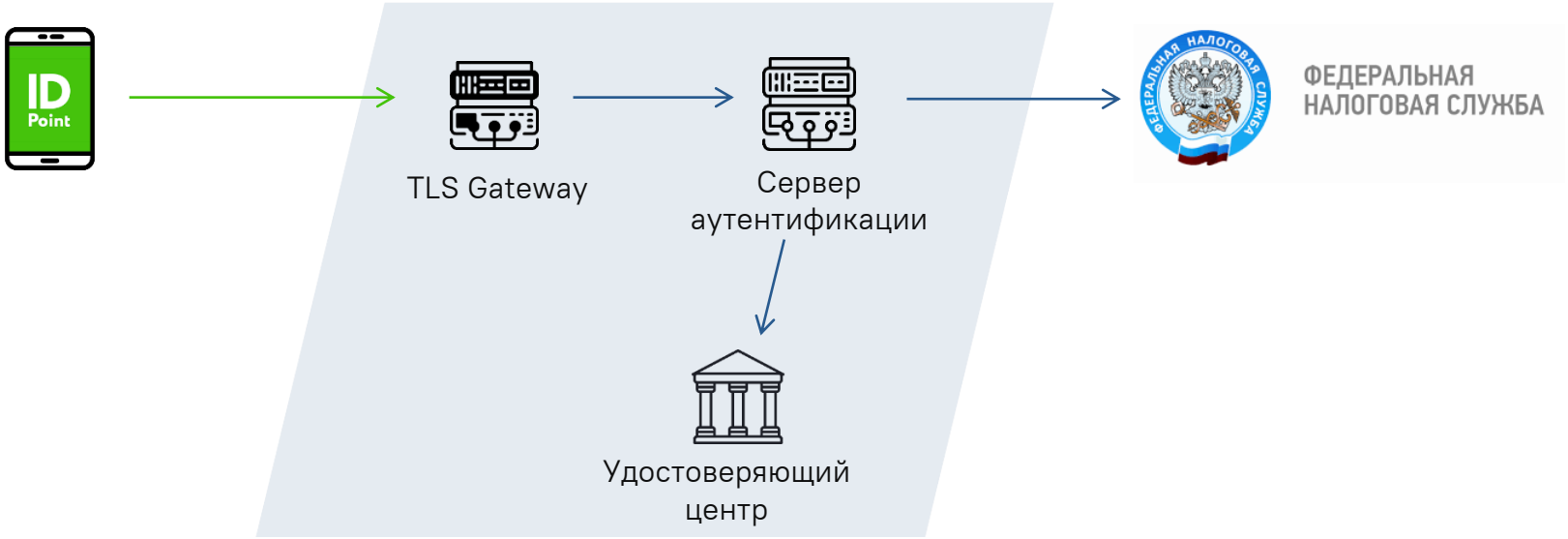
Запись доверенных корневых сертификатов в формате Base64
Настройка конфигурации
Проверка TLS-соединения

РАЗРАБОТАННЫЕ ПРИЛОЖЕНИЯ С OPENSSL

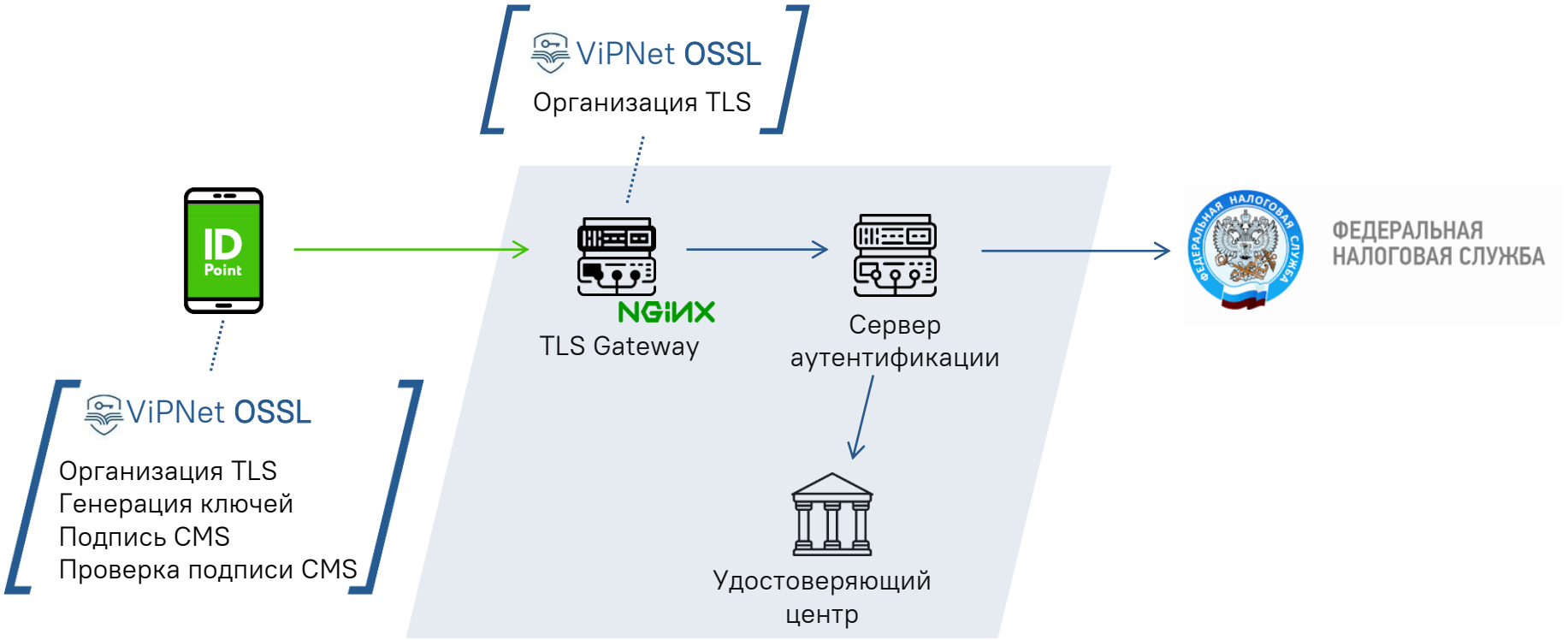
Реализация функций

Создание подписанного CMS-сообщения
Проверка подписанного CMS-сообщения
Создание зашифрованного CMS-сообщения
Расшифрование CMS-сообщения
Создание TLS-соединения

Успешные кейсы



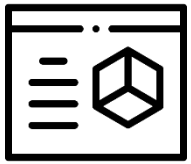
Успешные кейсы



Какие еще могут быть бизнес-сценарии?

- Доступ к ресурсам по защищенному каналу (ГОСТ TLS)
- ЭДО
- Телемедицина

Что входит в комплект

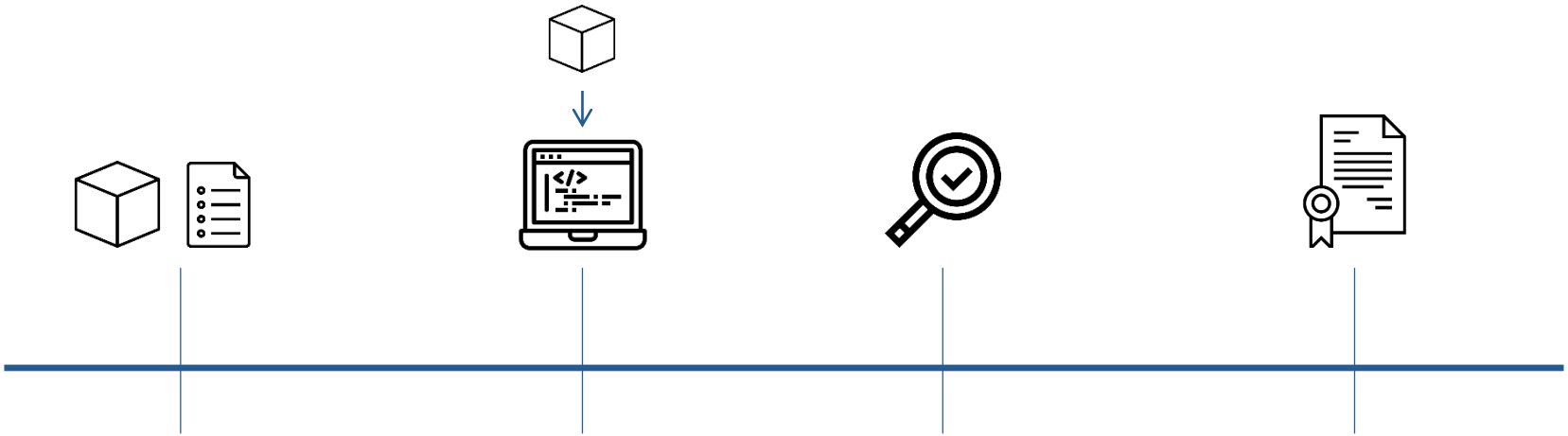


ПО ViPNet OSSL

Руководство разработчика ViPNet OSSL

Руководство разработчика ViPNet SoftToken

Сертификация



Сертификация ПО
и списка белых функций

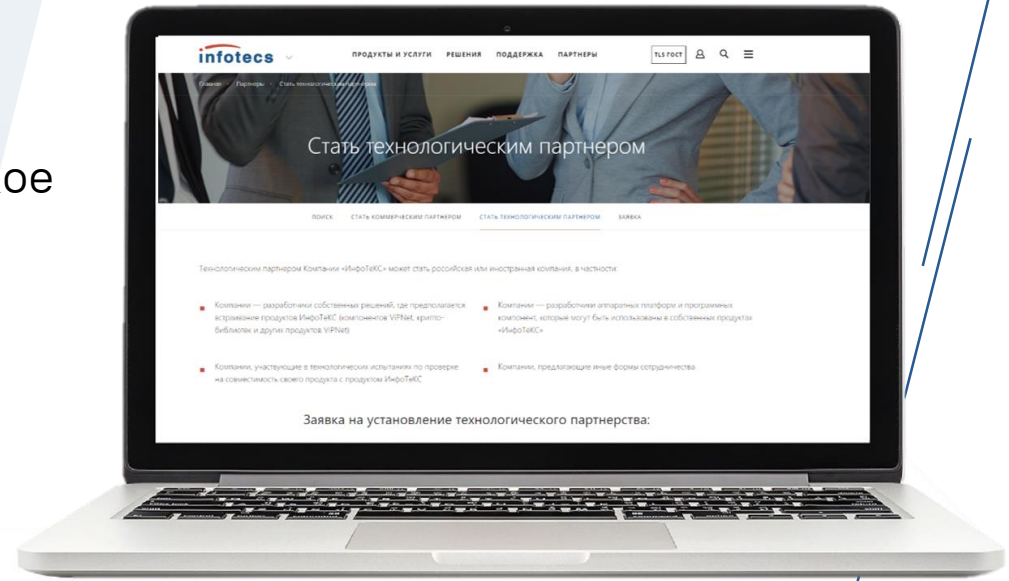
Встраивание ПО
в приложение

Контроль встраивания

Сертификат на
конечное ПО

Как ознакомиться с продуктом

1. Написать в наше коммерческое подразделение soft@infotecs.ru
2. Получить библиотеку протестировать
3. Оформить технологическое партнерство



Спасибо!

Арина Эм

Менеджер отдела
развития продуктов

E-mail:
Arina.Em@infotecs.ru