Рецепты приготовления облачной подписи

Бадмаева Римма
Руководитель продуктового направления

Ипаев Алексей
Менеджер по тестированию

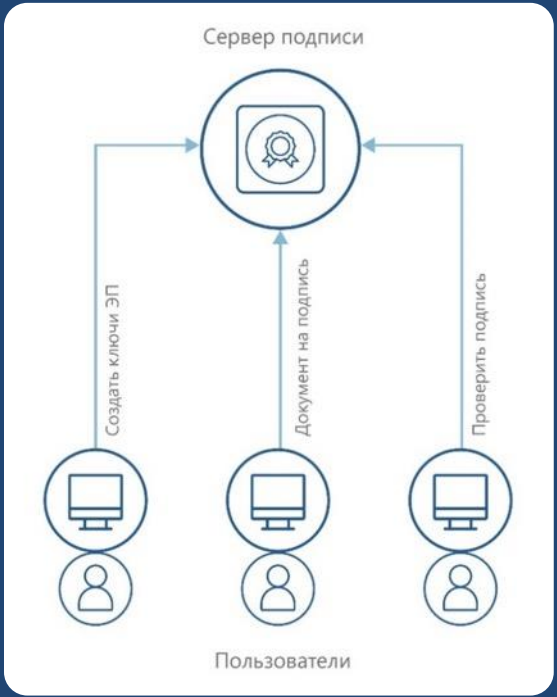
инфотекс ТЕХНОФЕСТ

Красный поток

Что такое сервер подписи?

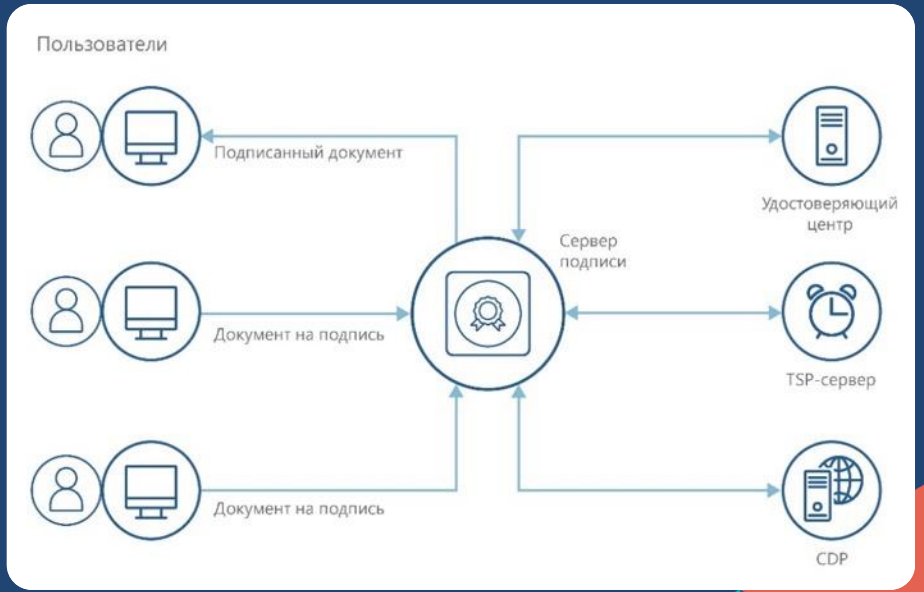
Сервер подписи обеспечивает централизованное выполнение следующих основных функций:

- генерация ключей электронной подписи
- формирование и проверка электронной подписи



Преимущества использования серверной подписи

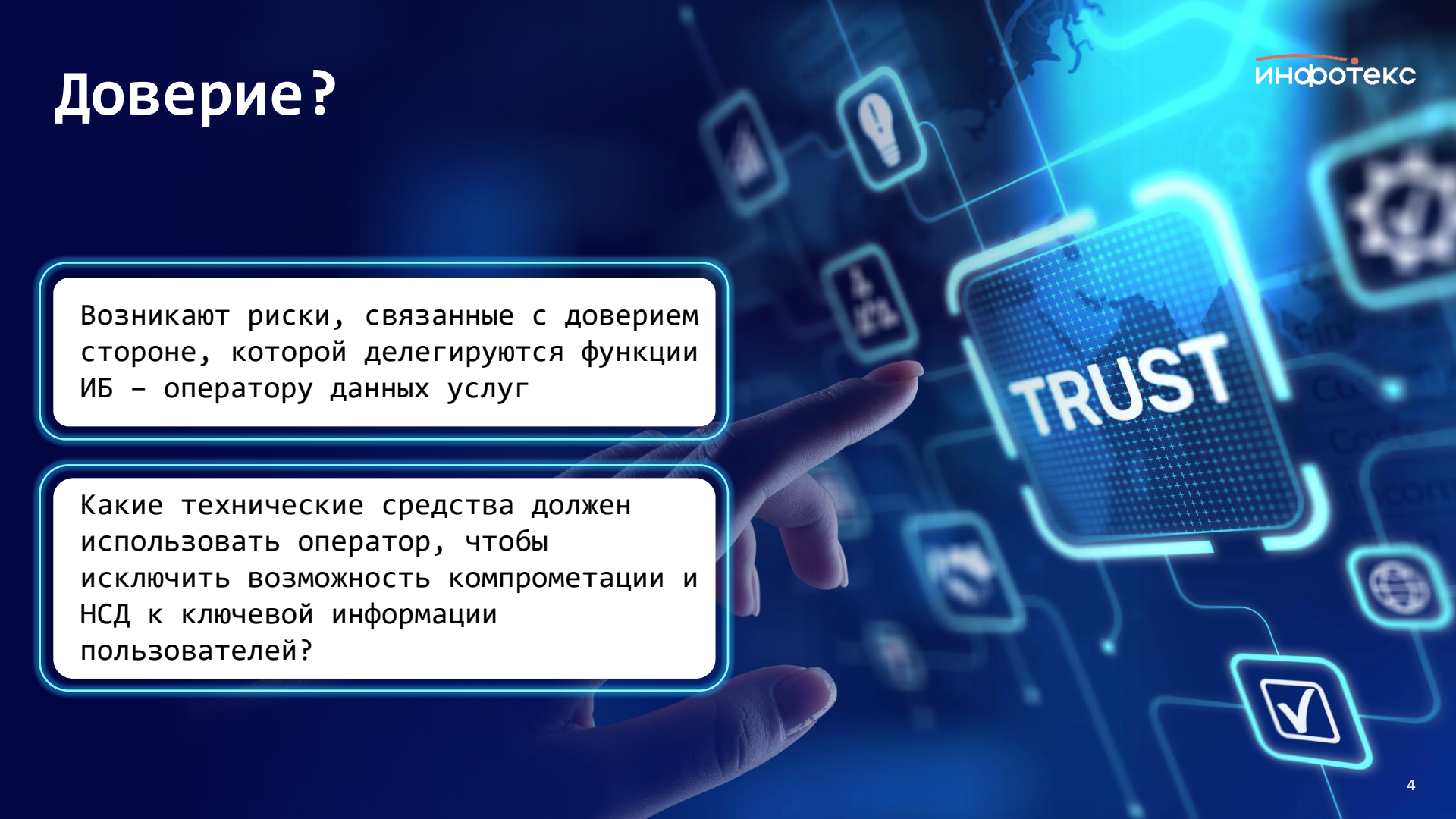
- Ключи ЭП пользователей хранятся централизованно – нельзя потерять, как токены
- Поддержание PKI в актуальном состоянии: доступ к УЦ, серверу меток времени, к актуальным CRL
- Аудит действий пользователей и т.п.



Доверие?

Возникают риски, связанные с доверием стороне, которой делегируются функции ИБ – оператору данных услуг

Какие технические средства должен использовать оператор, чтобы исключить возможность компрометации и НСД к ключевой информации пользователей?



HSM – доверенные криптографические модули

Криптографическая стойкость реализуемых алгоритмов и протоколов

Подтверждение корректности и полноты реализации мер защиты со стороны аккредитованной испытательной лаборатории, сертификация

Гарантии сопровождения, устранения неисправностей и уязвимостей со стороны производителя на всем протяжении жизненного цикла изделия

Платформа безопасности ViPNet HSM

инфотекс

ViPNet HSM

Программно-аппаратный модуль (HSM – Hardware Secure Module)

Повышенные меры безопасности

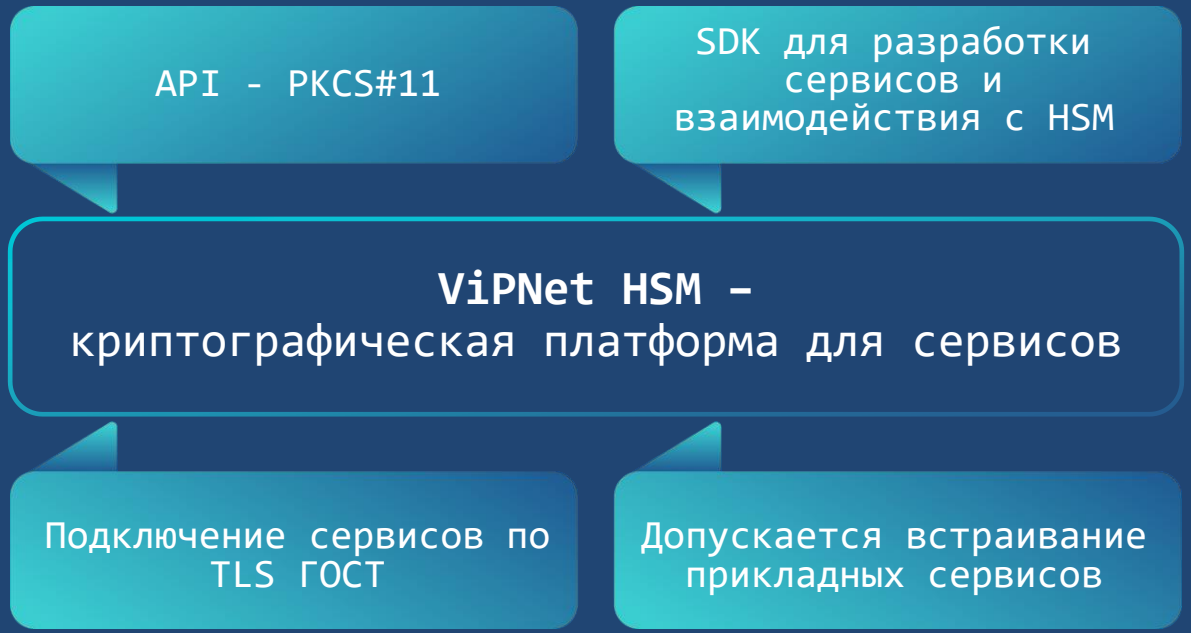
СКЗИ класса КВ

Выполняет криптографические операции по запросам различных сервисов («большой токен»)

Поддержка актуальных криптоалгоритмов

Средство ЭП класса КВ2

ViPNet HSM: подключение прикладных сервисов



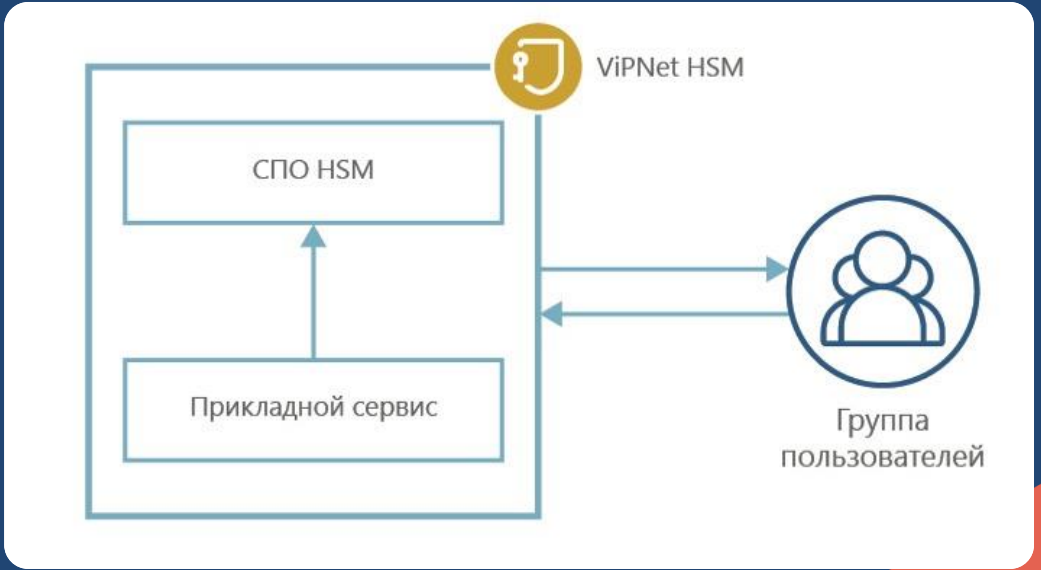
ViPNet HSM: внутренний прикладной сервис

Основные преимущества:

- Проще достичь классов КВ/КВ2
- Запуск и контроль функционирования ПС
- Сброс к заводскому состоянию
- Экспорт/импорт данных ПС
- Резервное копирование

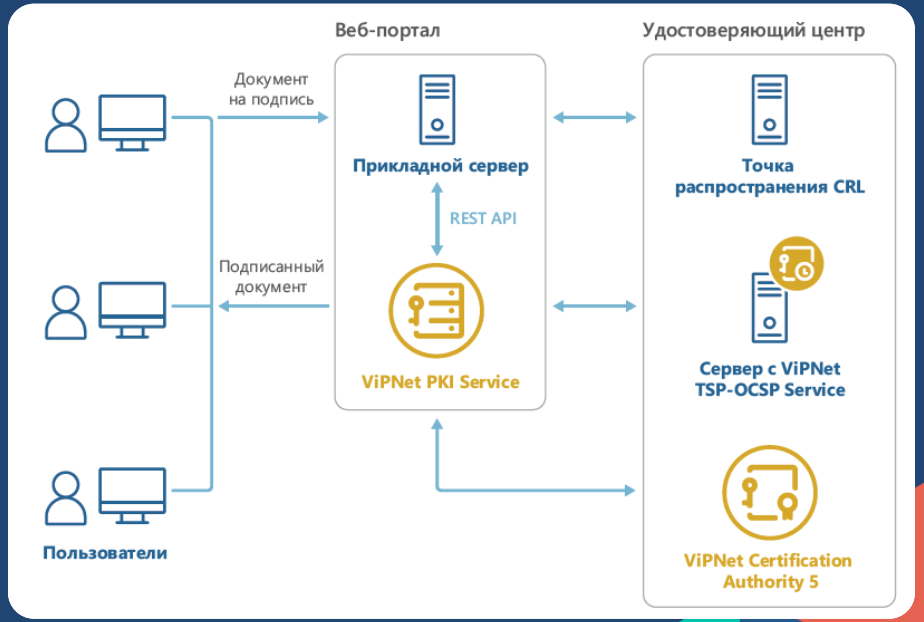
Пример:

ViPNet
PKI Service

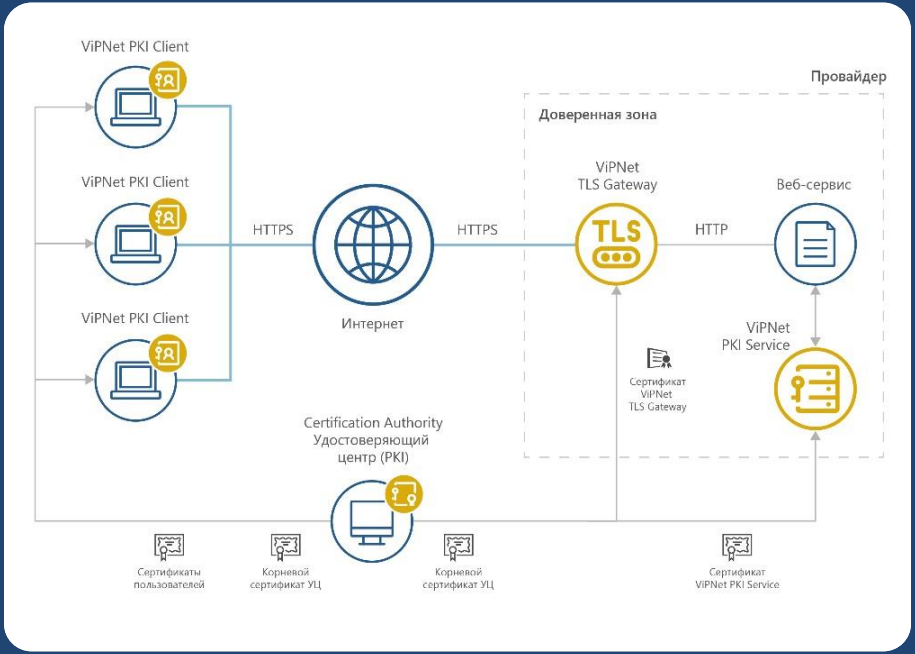


ViPNet PKI Service

- Сервер подписи, разработанный на базе ViPNet HSM
- Централизованное выполнение криптографических операций
- REST API
- СКЗИ класса КВ
- Средство ЭП класса КВ2



ViPNet PKI Service: дополнительные возможности



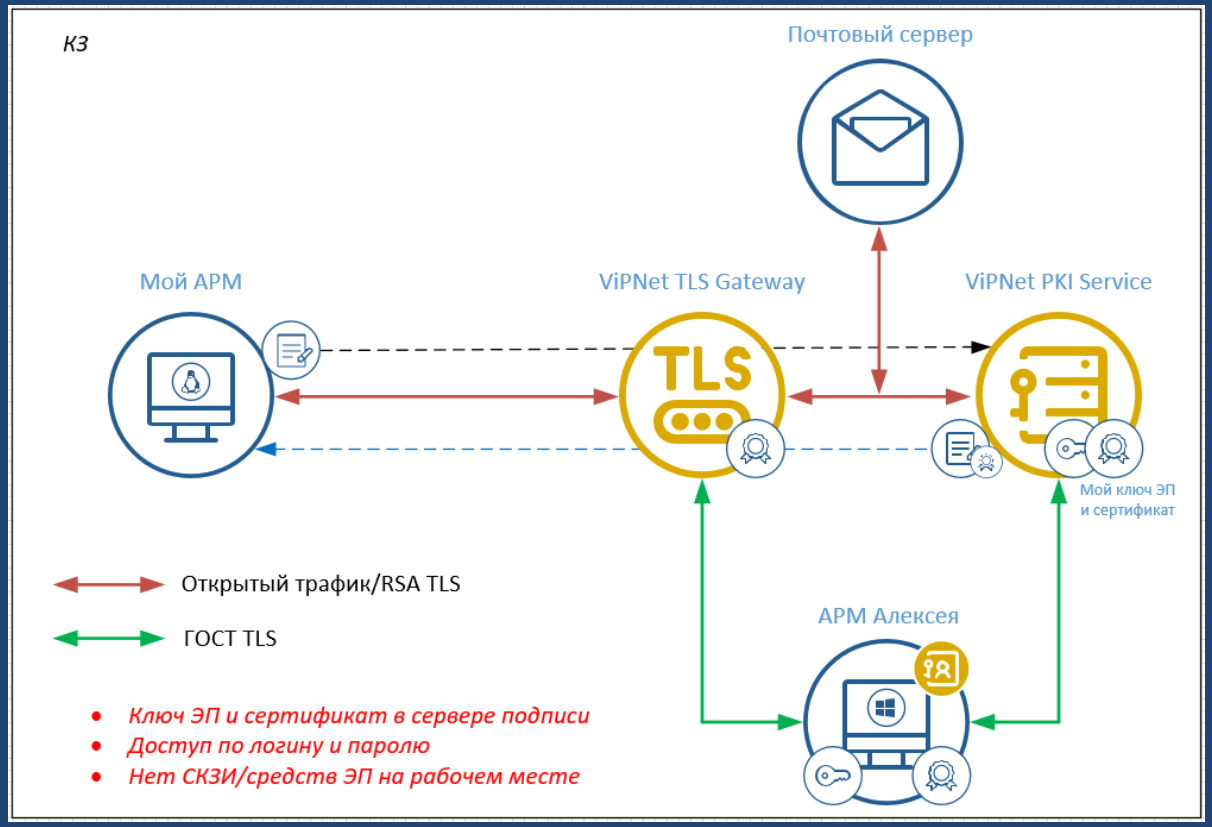
Взаимодействие с другими компонентами PKI:

- УЦ: ViPNet УЦ, КриптоПРО УЦ 2.0
- поддержка меток времени (TSP)
- возможность проверки статусов сертификатов по протоколу OCSP
- поддержание CRL в актуальном состоянии (CDP)
- совместная работа с ViPNet PKI Client (Cloud Unit) в сценарии облачной подписи
- совместная работа с ViPNet TLS Gateway для организации TLS-соединений при доступе пользователей к своим ключам

Демонстрация. Переходим к практике!

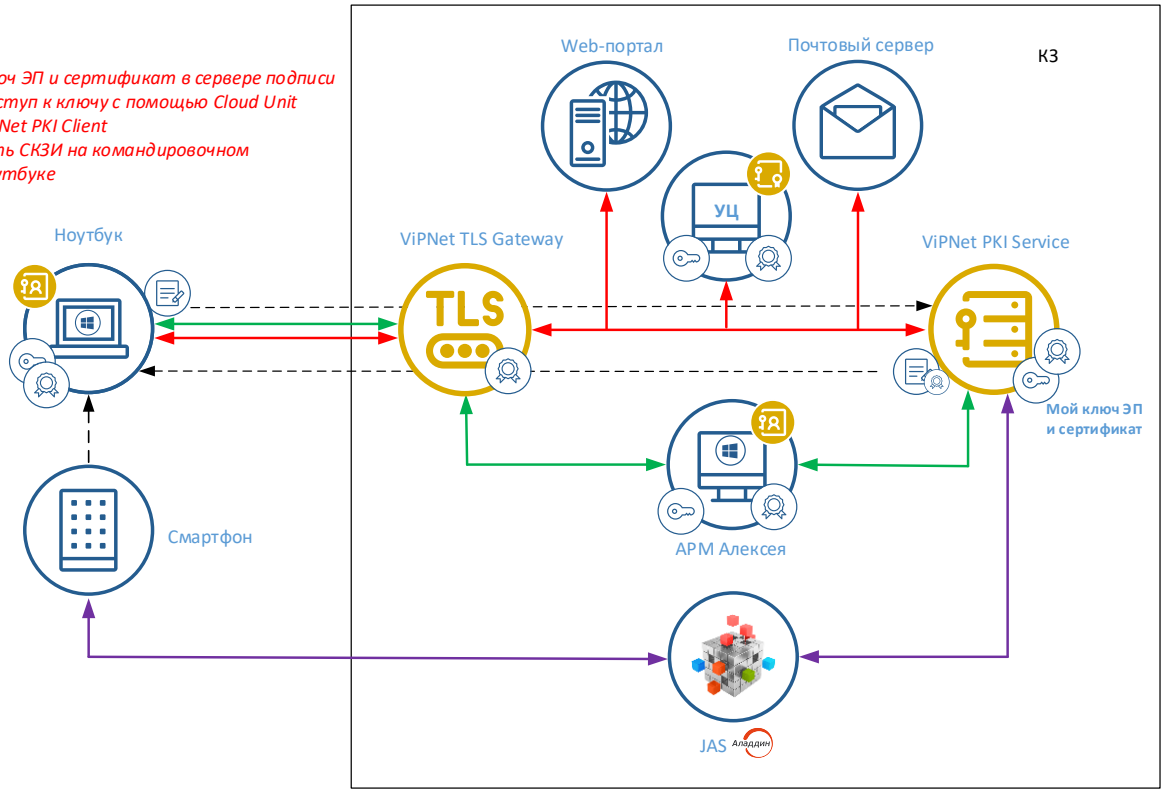
инфотекс

Оформление командировки в офисе



Оформление отпуска вне офиса

- *Ключ ЭП и сертификат в сервере подписи*
- *Доступ к ключу с помощью Cloud Unit ViPNet PKI Client*
- *Есть СКЗИ на командировочном ноутбуке*

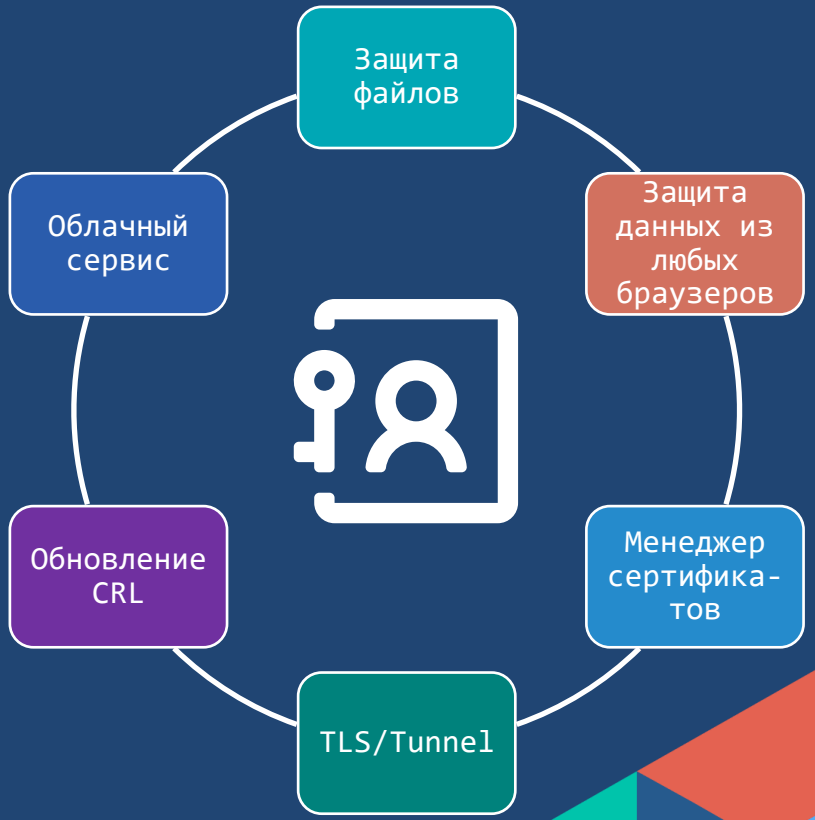


Спидран ViPNet PKI Client

- Скачать и установить PKI Client
- Настроить PKI Client с помощью файла настроек
- Выпустить сертификат безопасности ГОСТ TLS
- Активировать PKI Client
- Подписать заявление с использованием ключа ЭП, который хранится на сервере подписи PKI Service, получив код от JAS

ViPNet PKI Client

Универсальный клиент для работы в инфраструктуре открытых ключей



САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Подписывайтесь на наши соцсети