

Рецепты приготовления облачной подписи

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  ФЕСТ

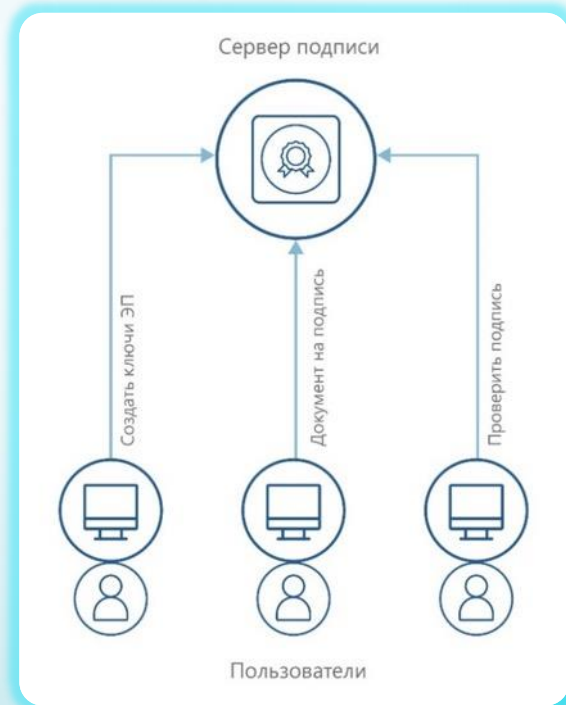
Бадмаева Римма
Ведущий менеджер продуктов

Ипаев Алексей
Менеджер по тестированию

Что такое сервер подписи?

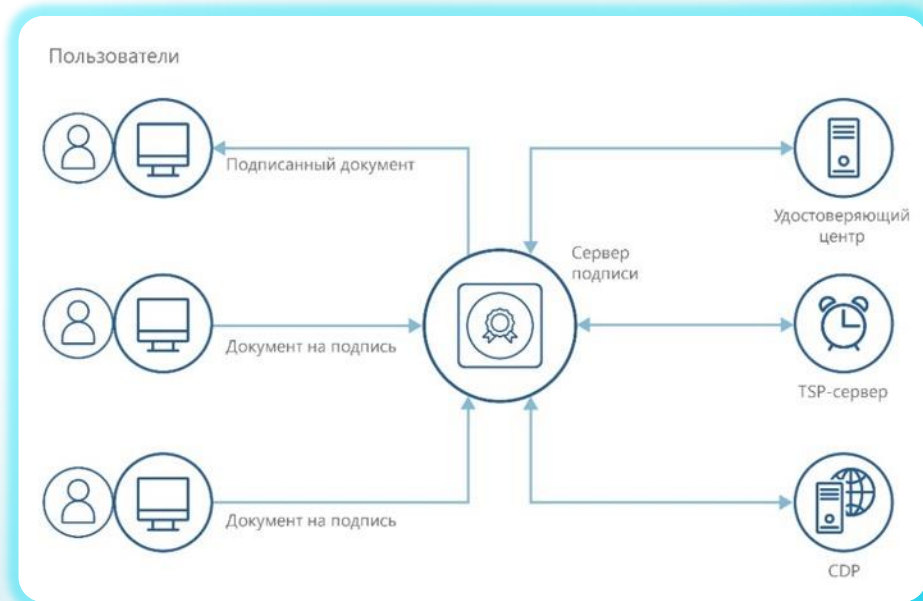
Сервер подписи обеспечивает централизованное выполнение следующих основных функций:

- генерация ключей электронной подписи
- формирование и проверка электронной подписи



Преимущества использования серверной подписи

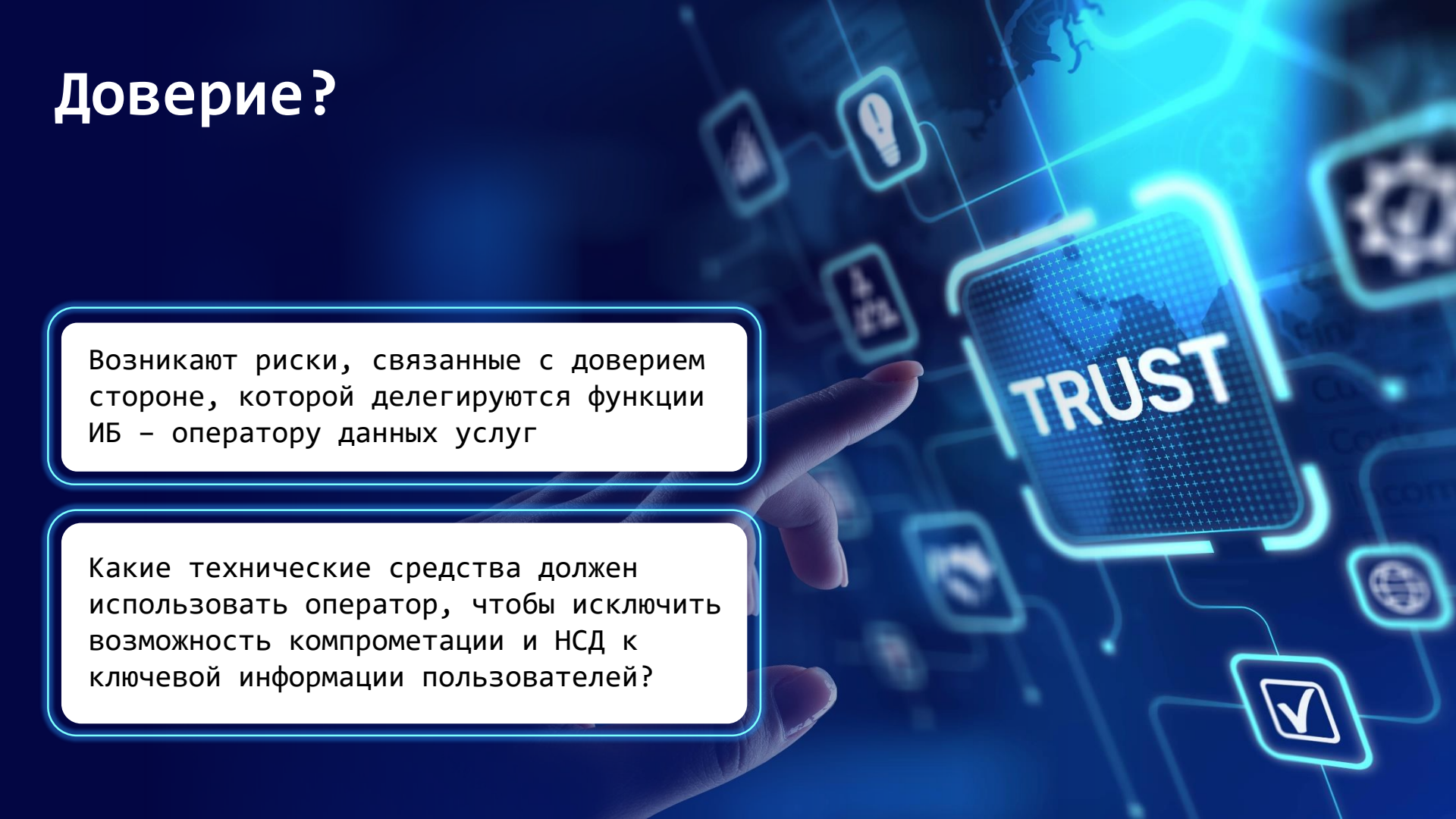
- Ключи ЭП пользователей хранятся централизованно – нельзя потерять, как токены
- Поддержание PKI в актуальном состоянии: доступ к УЦ, серверу меток времени, к актуальным CRL
- Аудит действий пользователей и т.п.



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?

A hand is pointing towards a glowing blue digital interface. The interface features a central square with a grid pattern and the word "TRUST" in white capital letters. Surrounding this central element are various icons in rounded squares, including a lightbulb, a gear, a checkmark, a globe, and a person. The background is dark blue with glowing lines and a faint world map.

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

1

Программно-аппаратный модуль (HSM – Hardware Secure Module)

2

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

3

Повышенные меры безопасности

4

Поддержка актуальных криптоалгоритмов

5

СКЗИ класса КВ

6

Средство ЭП класса КВ2

ViPNet HSM: подключение прикладных сервисов

ViPNet HSM –
криптографическая платформа для сервисов

API – PKCS#11

SDK для
разработки
сервисов и
взаимодействия
с HSM

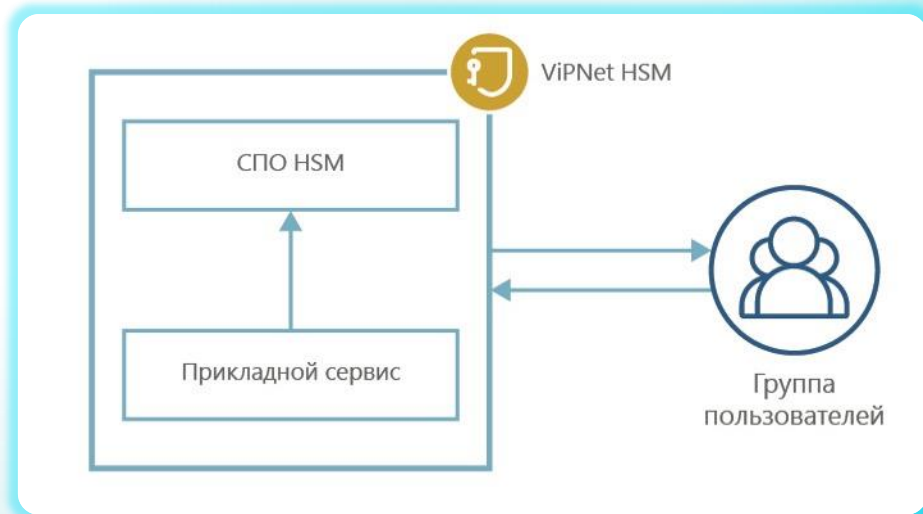
Подключение
сервисов под
защитой TLS
ГОСТ

Допускается
встраивание
прикладных
сервисов

ViPNet HSM: внутренний прикладной сервис

Основные преимущества:

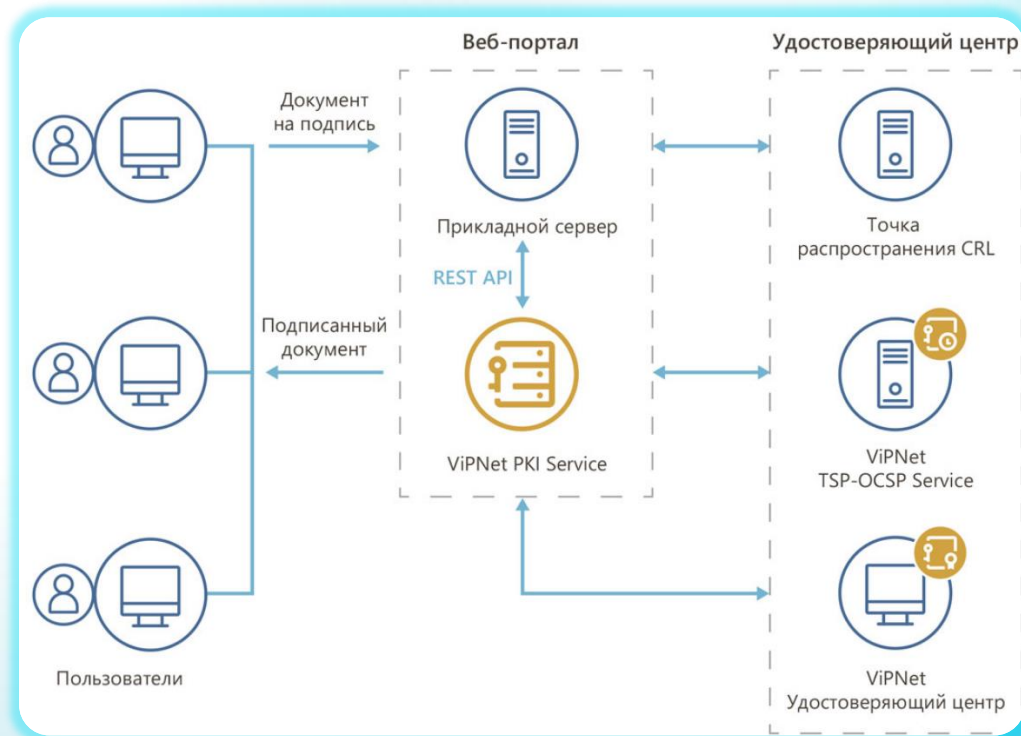
- Проще достичь классов KB/KB2
- Запуск и контроль функционирования ПС
- Сброс к заводскому состоянию
- Экспорт/импорт данных ПС
- Резервное копирование



Например: ViPNet PKI Service

ViPNet PKI Service

- Сервер подписи, разработанный на базе ViPNet HSM
- Централизованное выполнение криптографических операций
- REST API
- СКЗИ класса KB
- Средство ЭП класса KB2

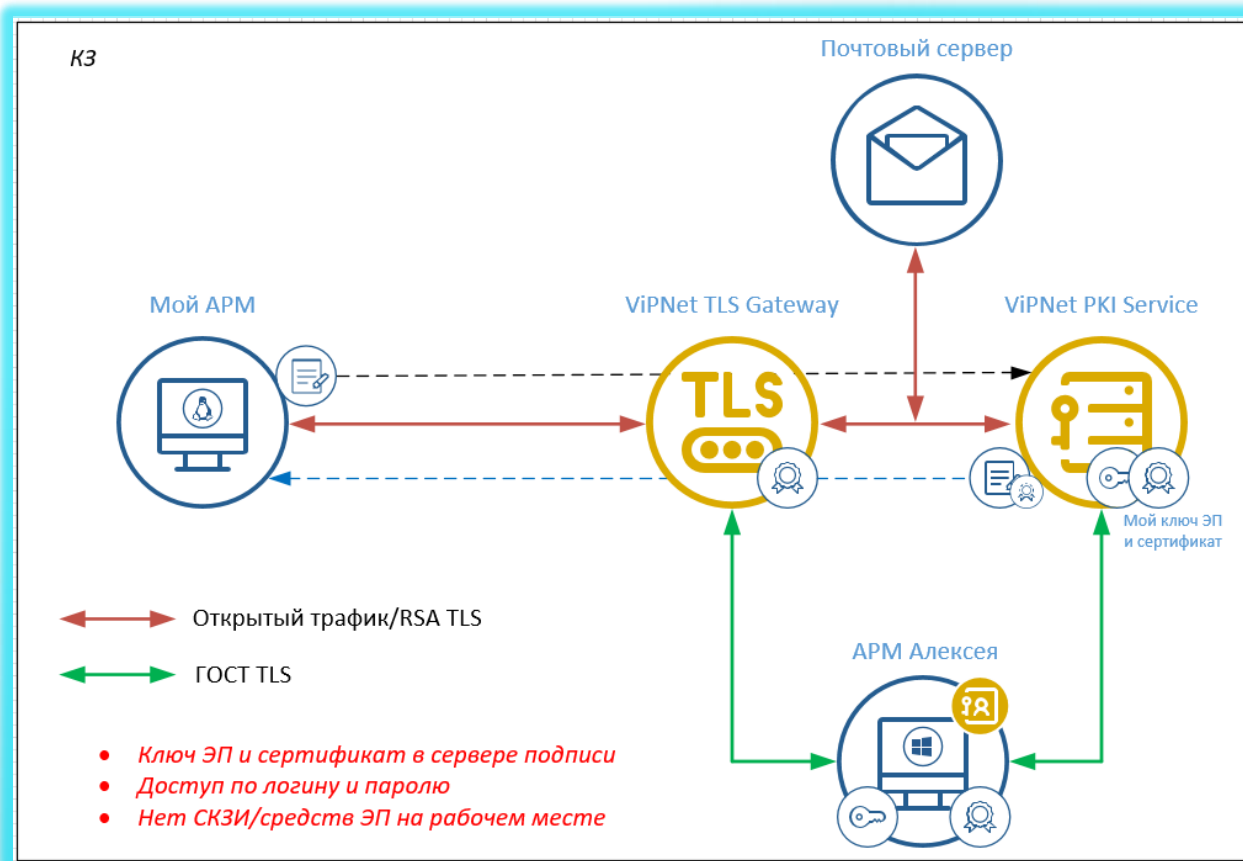




- 11

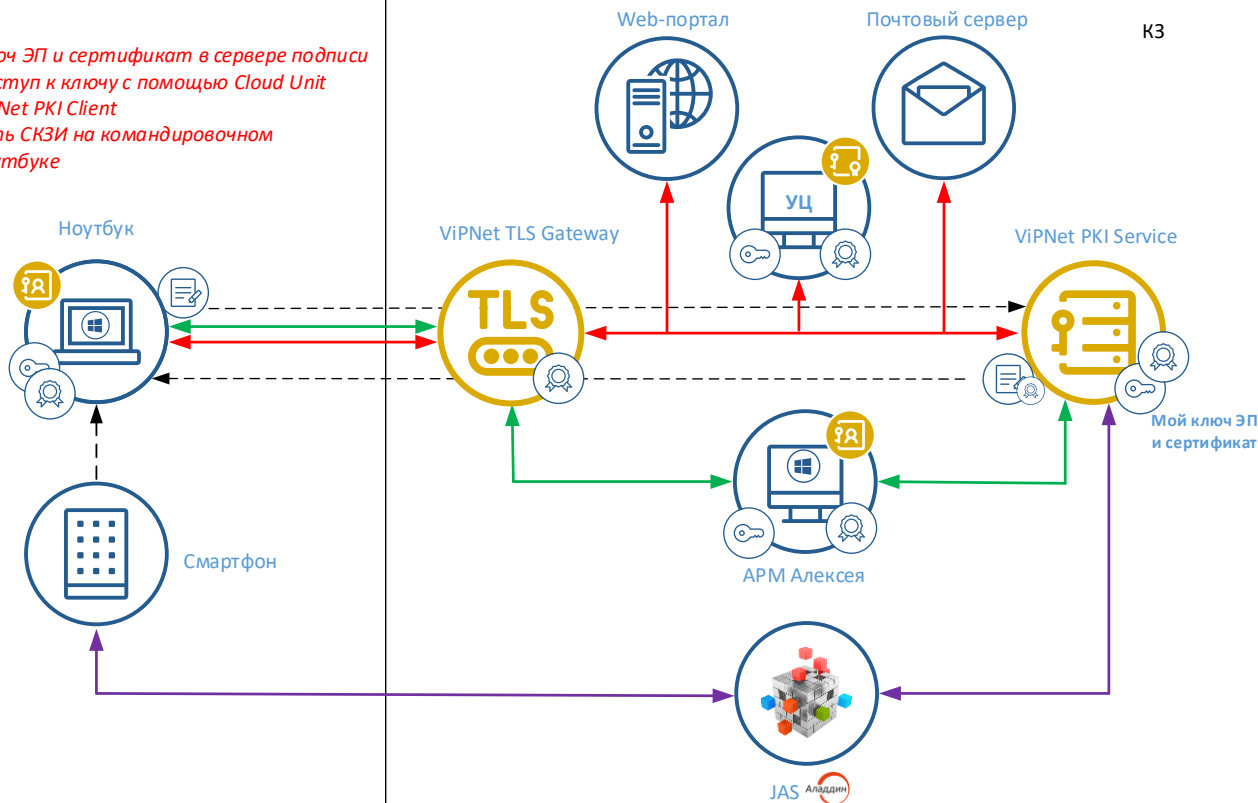
**Демонстрация.
Переходим
к практике!**

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



ТЕХНО infotecs Фест

Бадмаева Римма
Ведущий менеджер
продуктов

Ипаев Алексей
Менеджер
по тестированию



NBJ НАЦИОНАЛЬНЫЙ
БАНКОВСКИЙ ЖУРНАЛ



РУТОКЕН
Бизнес-ПРАКТИВ



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ



PR integ

АТБ
ЭЛЕКТРОНИКА

infotecs
{-cademy}

m=rlion



Подписывайтесь
на наши соцсети,
там много интересного

