

Серверная, дистанционная, удаленная, облачная ЭП (нужное подчеркнуть)

Бадмаева Римма
Ведущий менеджер продуктов

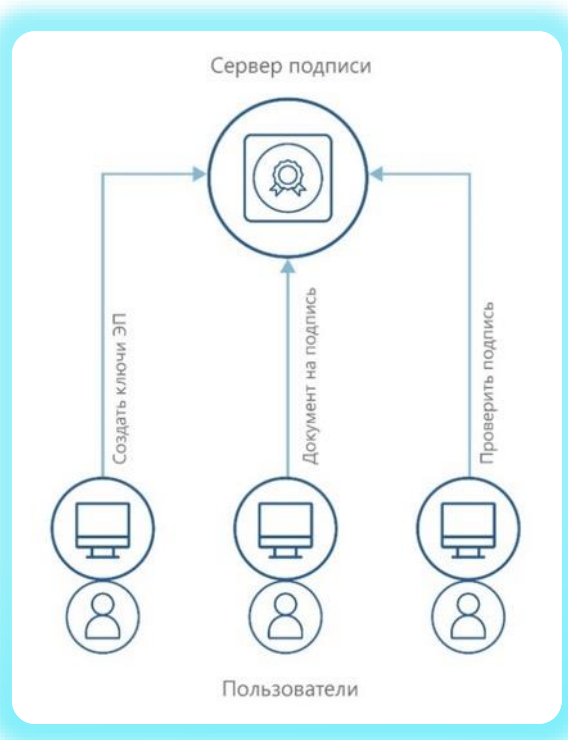
Ипаев Алексей
Менеджер по тестированию



Что такое сервер подписи?

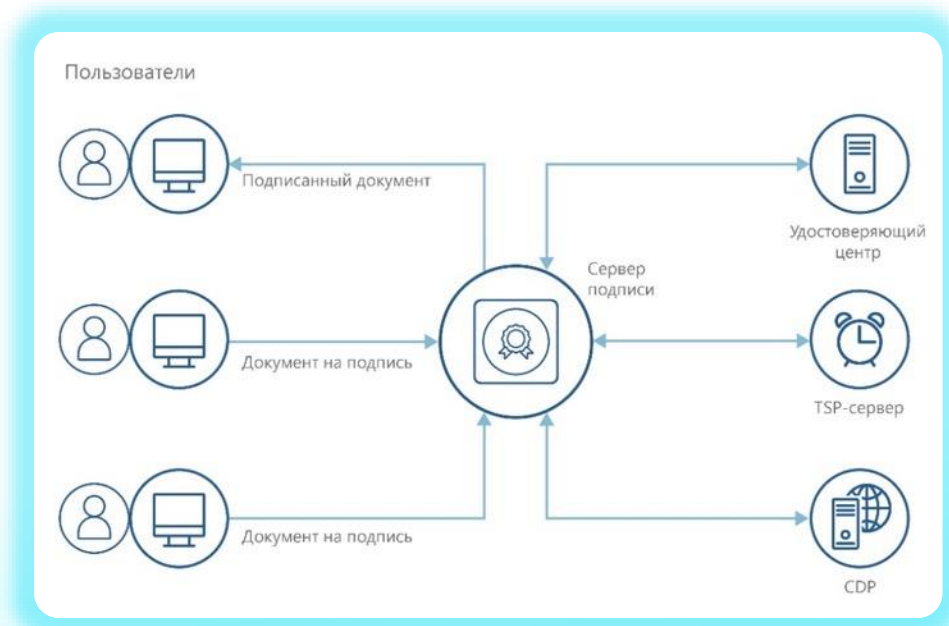
Сервер подписи обеспечивает централизованное выполнение следующих основных функций:

- генерация ключей электронной подписи
- формирование и проверка электронной подписи

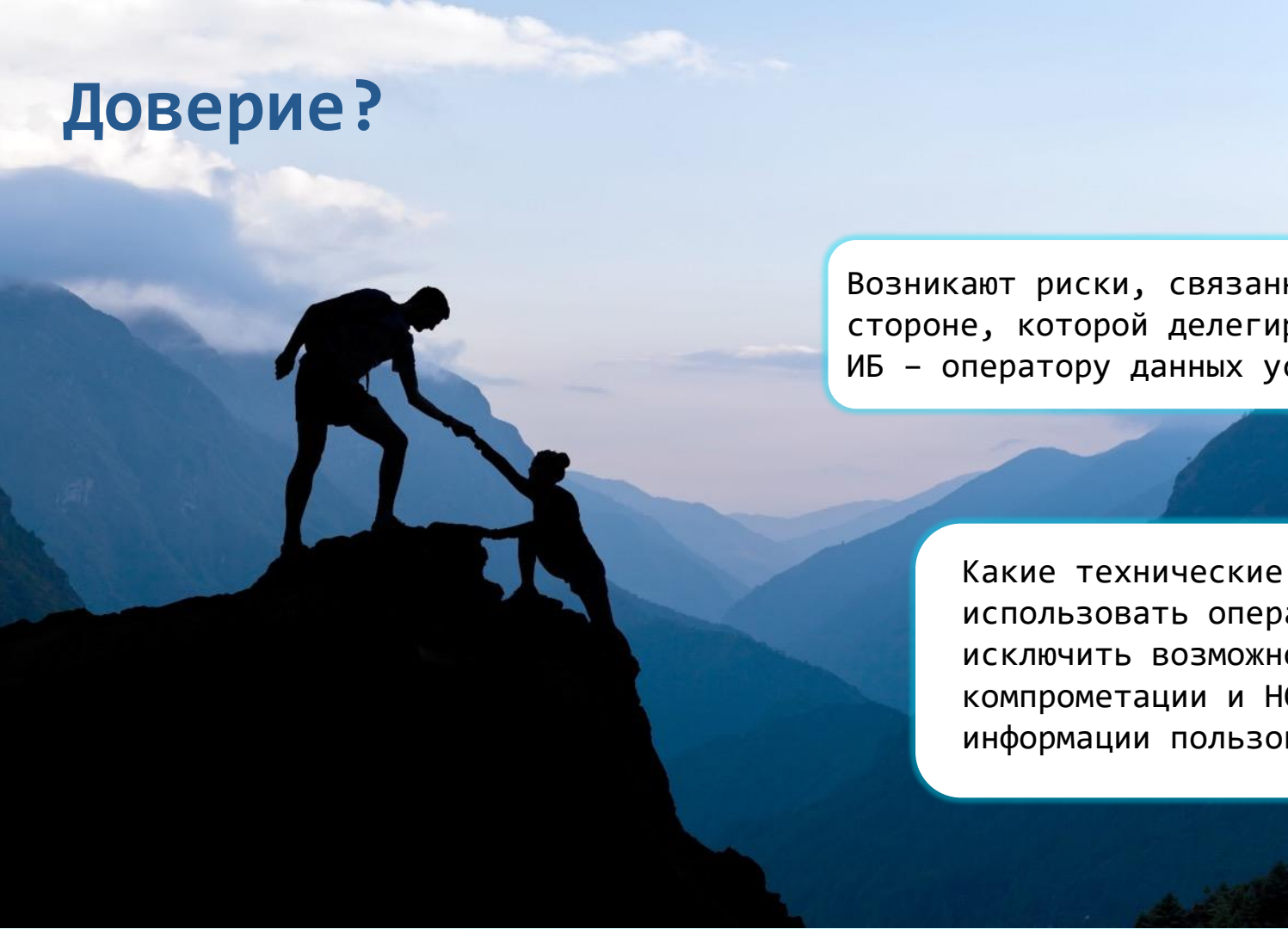


Преимущества использования серверной подписи

- 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?

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

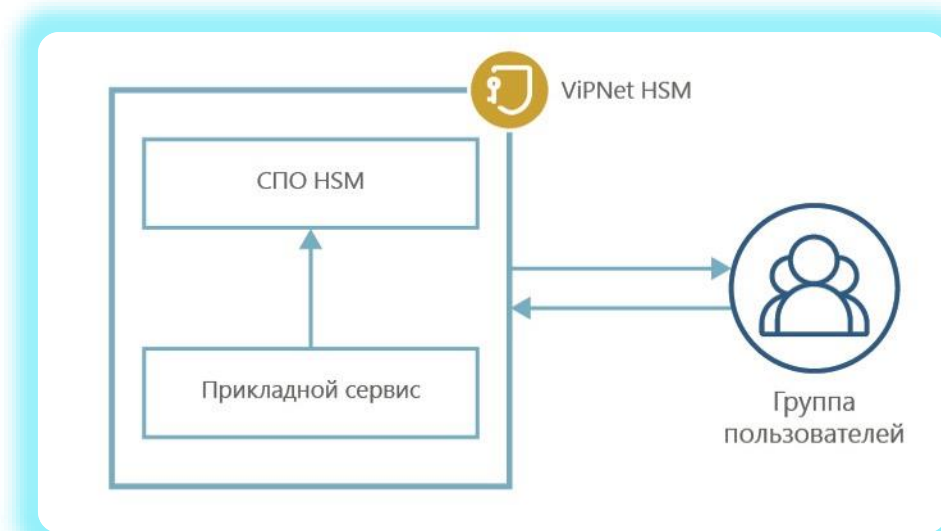
Подключение
сервисов под
защитой TLS
ГОСТ

Допускается
встраивание
прикладных
сервисов

VIPNet HSM: внутренний прикладной сервис

Основные преимущества:

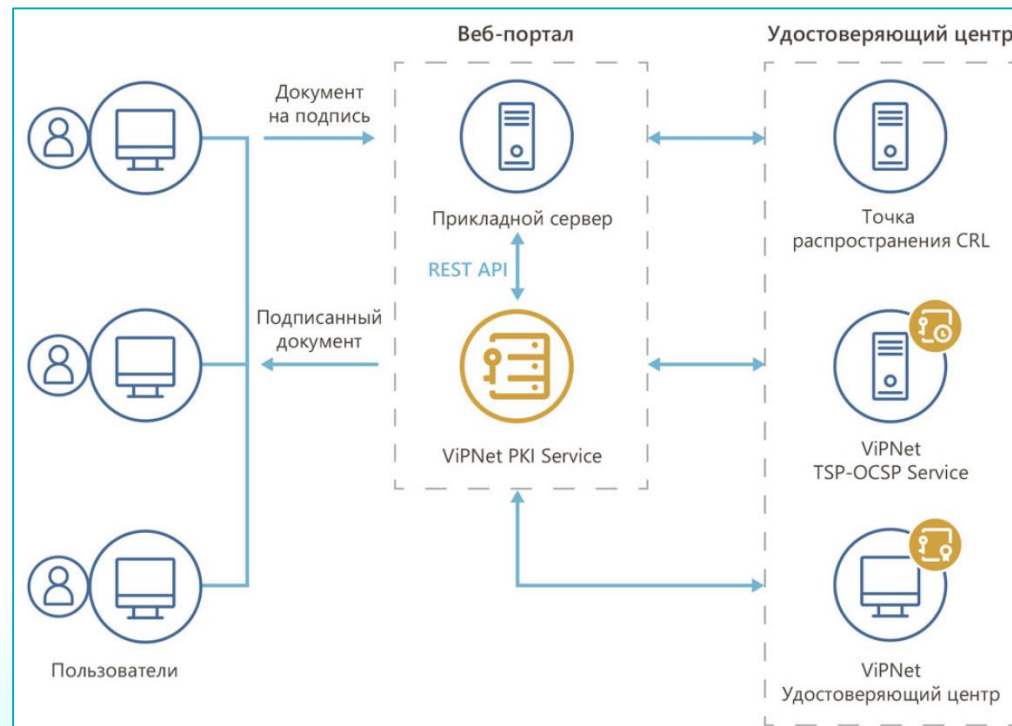
- Проще достичь классов KB/KB2
- Запуск и контроль функционирования ПС
- Сброс к заводскому состоянию
- Экспорт/импорт данных ПС
- Резервное копирование



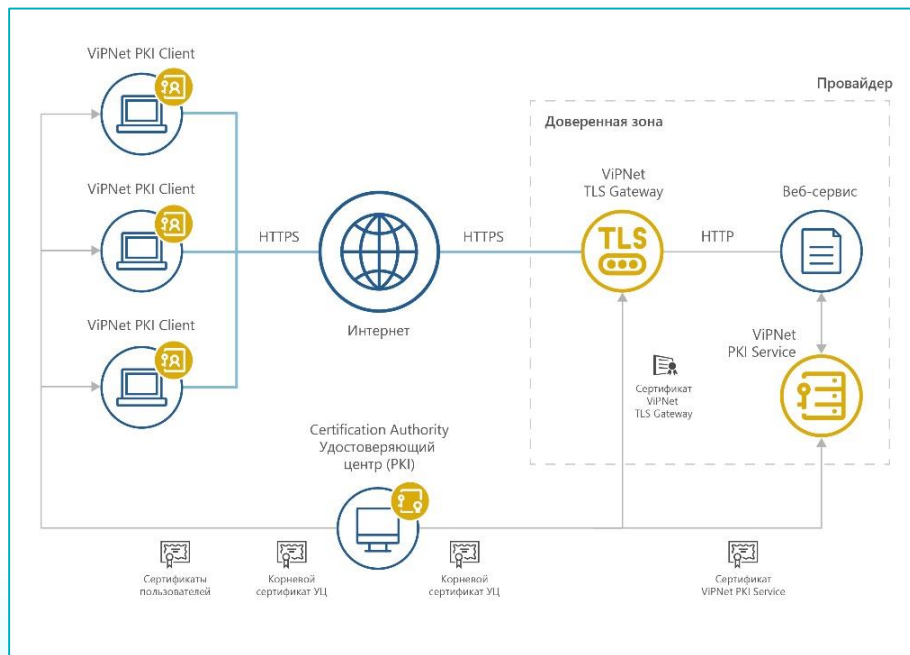
Например: VIPNet PKI Service

ViPNet PKI Service

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



VIPNet PKI Service: дополнительные возможности

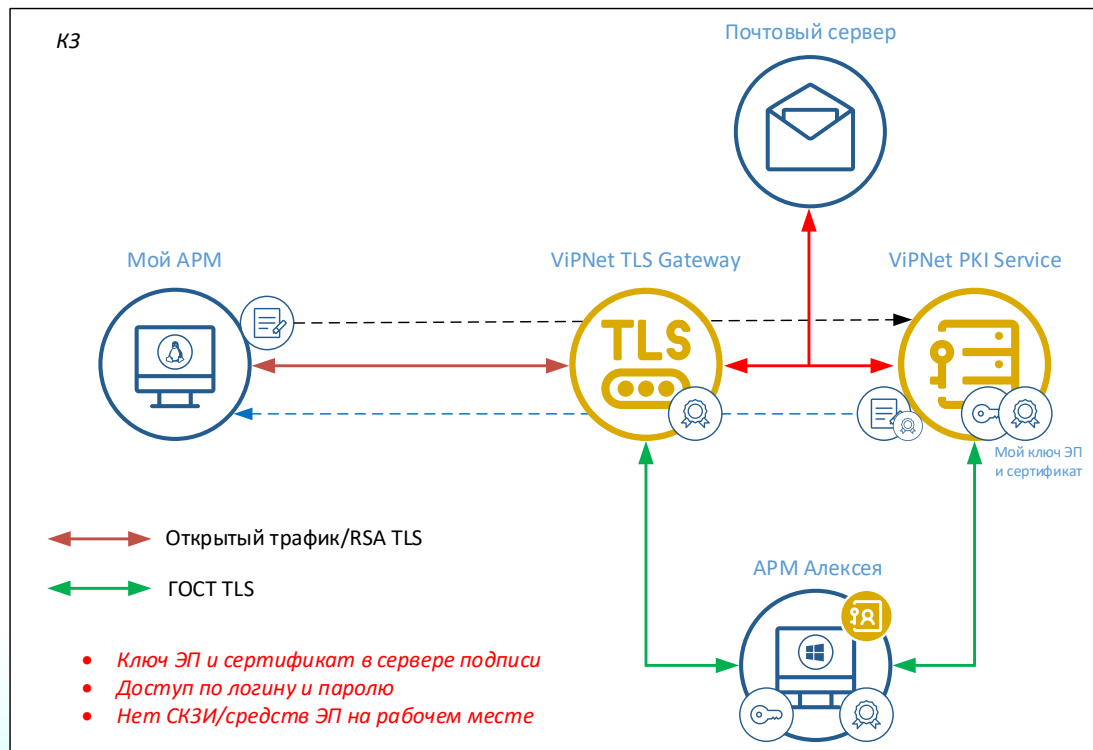


Взаимодействие с другими компонентами PKI:

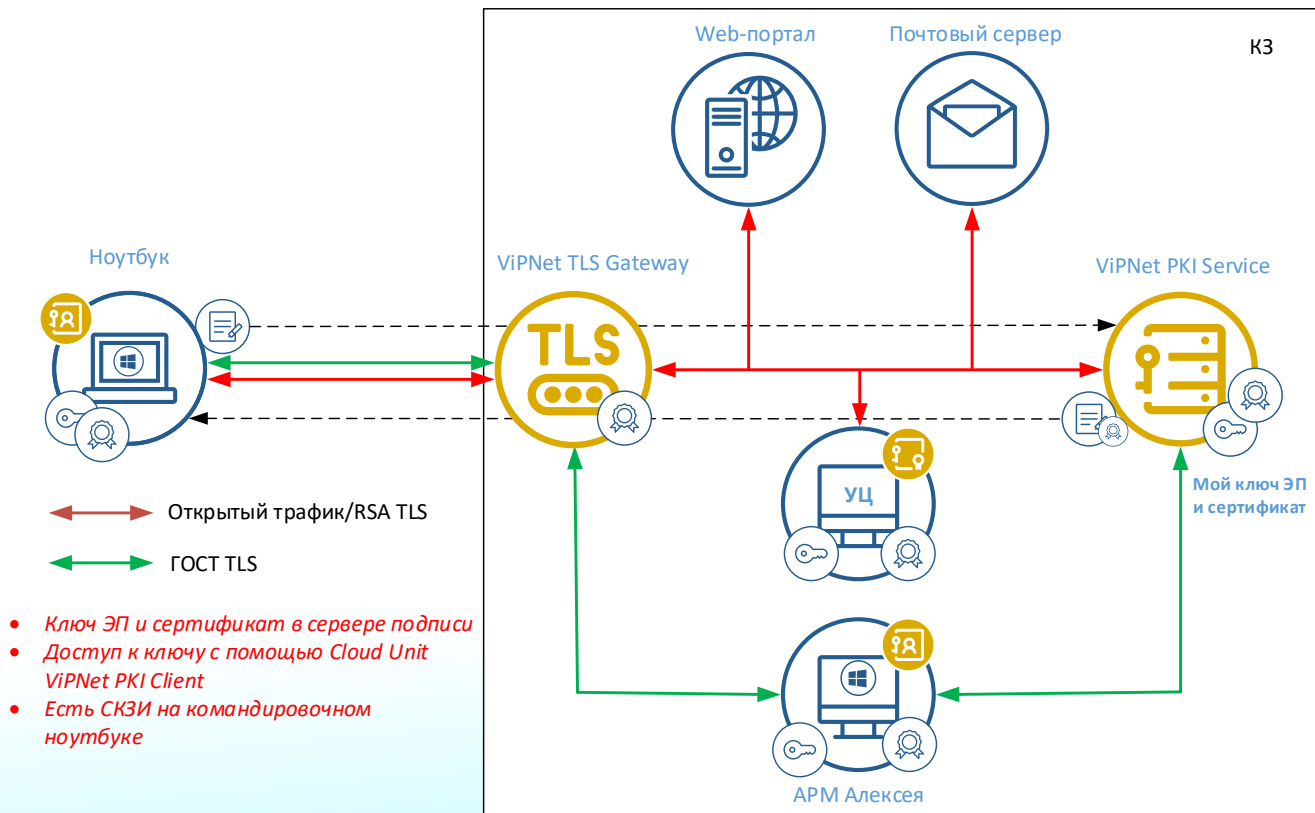
- УЦ: VIPNet УЦ, КриптоПРО УЦ 2.0
- поддержка меток времени (TSP)
- возможность проверки статусов сертификатов по протоколу OCSP
- поддержание CRL в актуальном состоянии (CDP)
- совместная работа с VIPNet PKI Client (Cloud Unit) в сценарии облачной подписи
- совместная работа с VIPNet TLS Gateway для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

**Демонстрация.
Переходим
к практике!**

Оформление командировки (в офисе)



Оформление отпуска (вне офиса)



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





VIPNet PKI Client

Универсальный клиент для работы
в инфраструктуре открытых ключей



ТЕХНО infotecs Фест

Бадмаева Римма
Ведущий менеджер продуктов

Ипаев Алексей
Менеджер по тестированию

Подписывайтесь
на наши соцсети,
там много интересного

