

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

Бадмаева Римма  
Ипаев Алексей

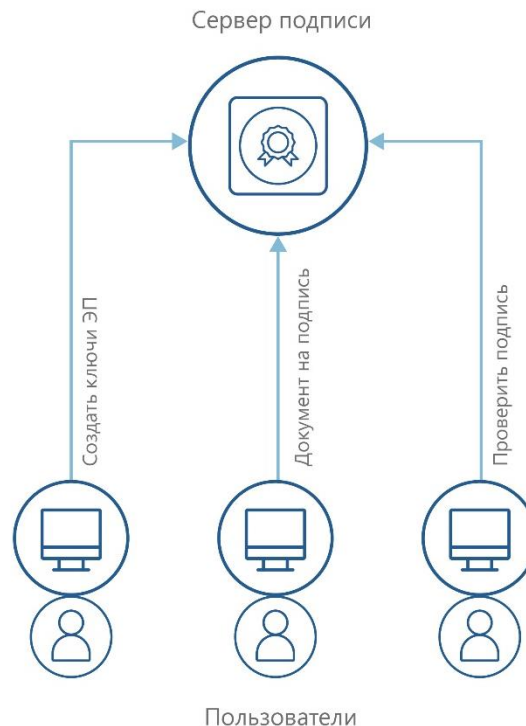


техно infotecs  
2023 Фест  
ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

# Что такое сервер подписи?

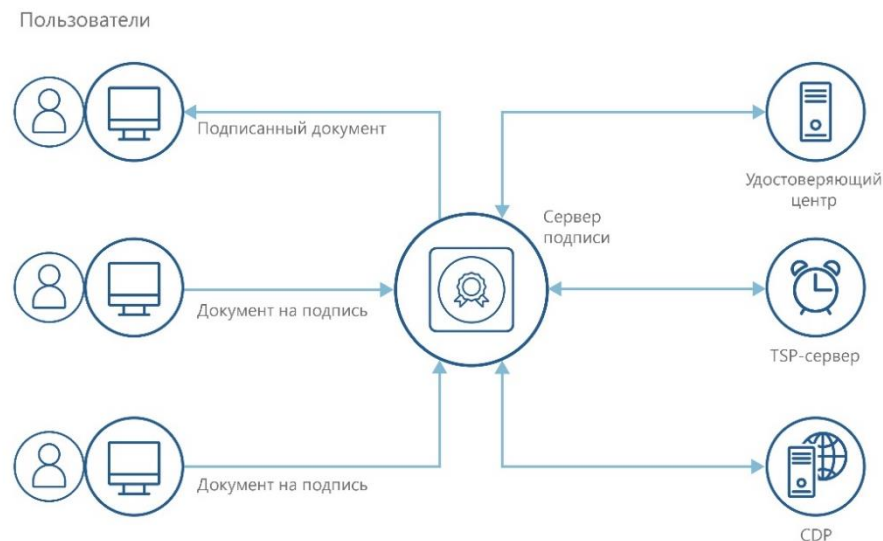
Сервер подписи обеспечивает централизованное выполнение следующих основных функций:

- 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

# 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

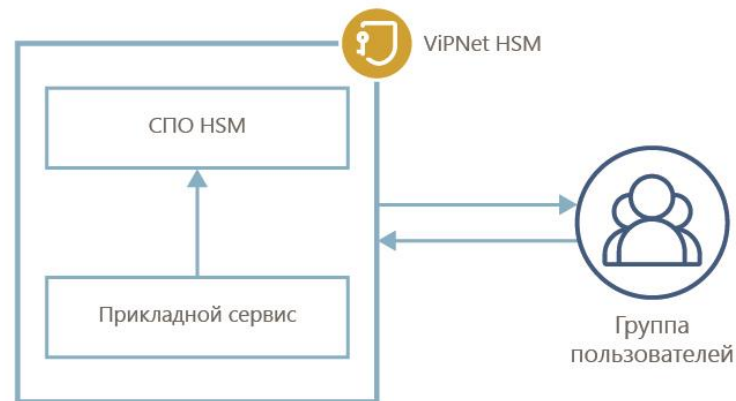
Допускается  
встраивание  
прикладных  
сервисов



# VIPNet HSM: внутренний прикладной сервис

## Основные преимущества:

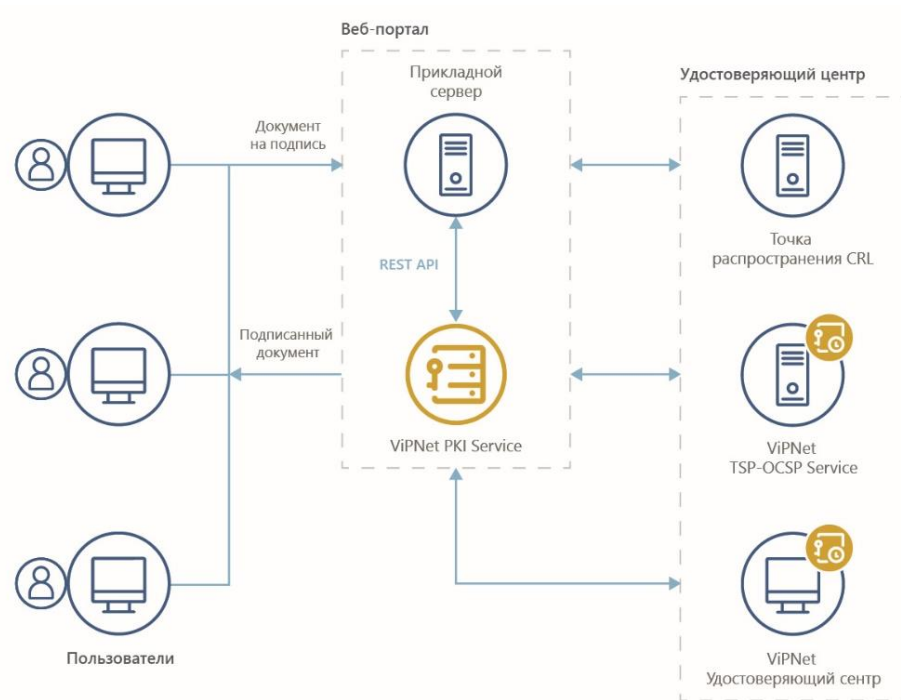
- Проще достичь классов KB/KB2
- Запуск и контроль функционирования ПС
- Сброс к заводскому состоянию
- Экспорт/импорт данных ПС
- Резервное копирование



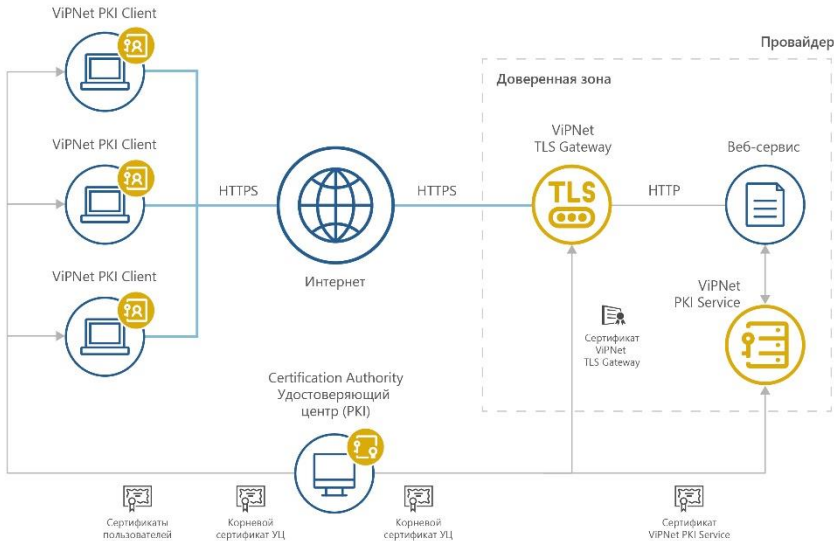
**Например:** VIPNet PKI Service

# VIPNet PKI Service

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



# VIPNet PKI Service: ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

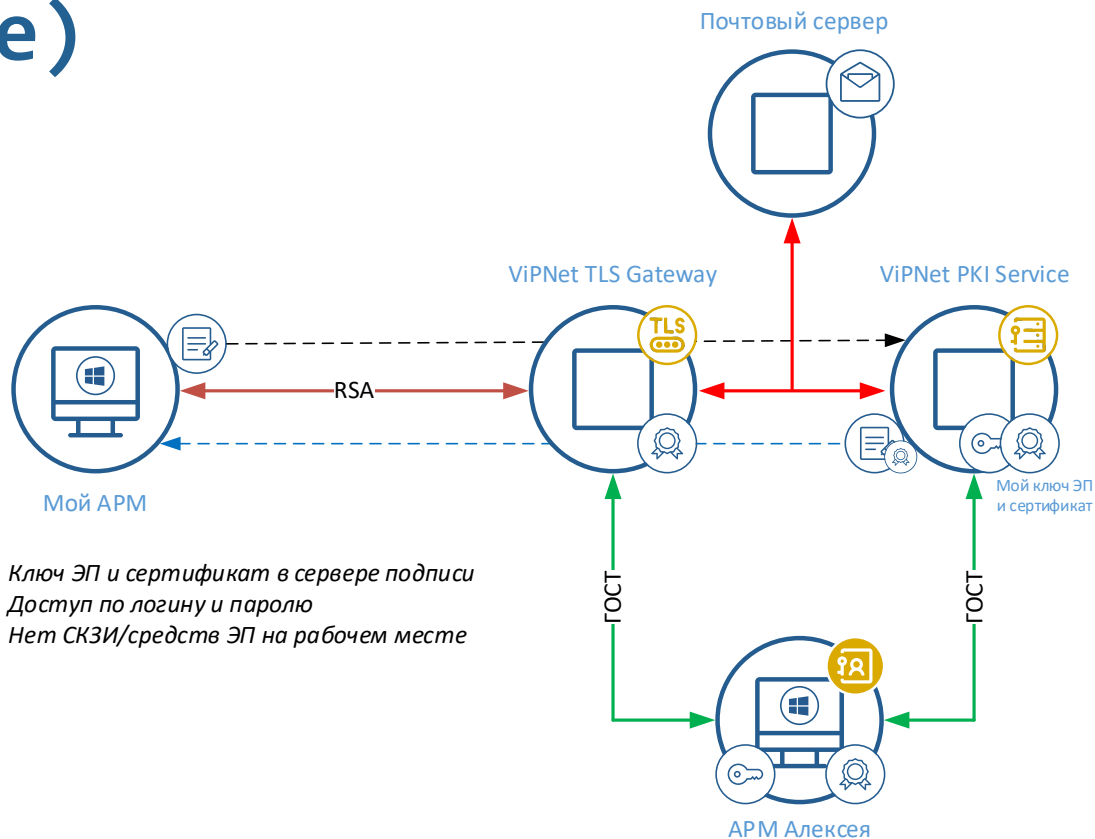


## Взаимодействие с другими компонентами PKI:

- 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

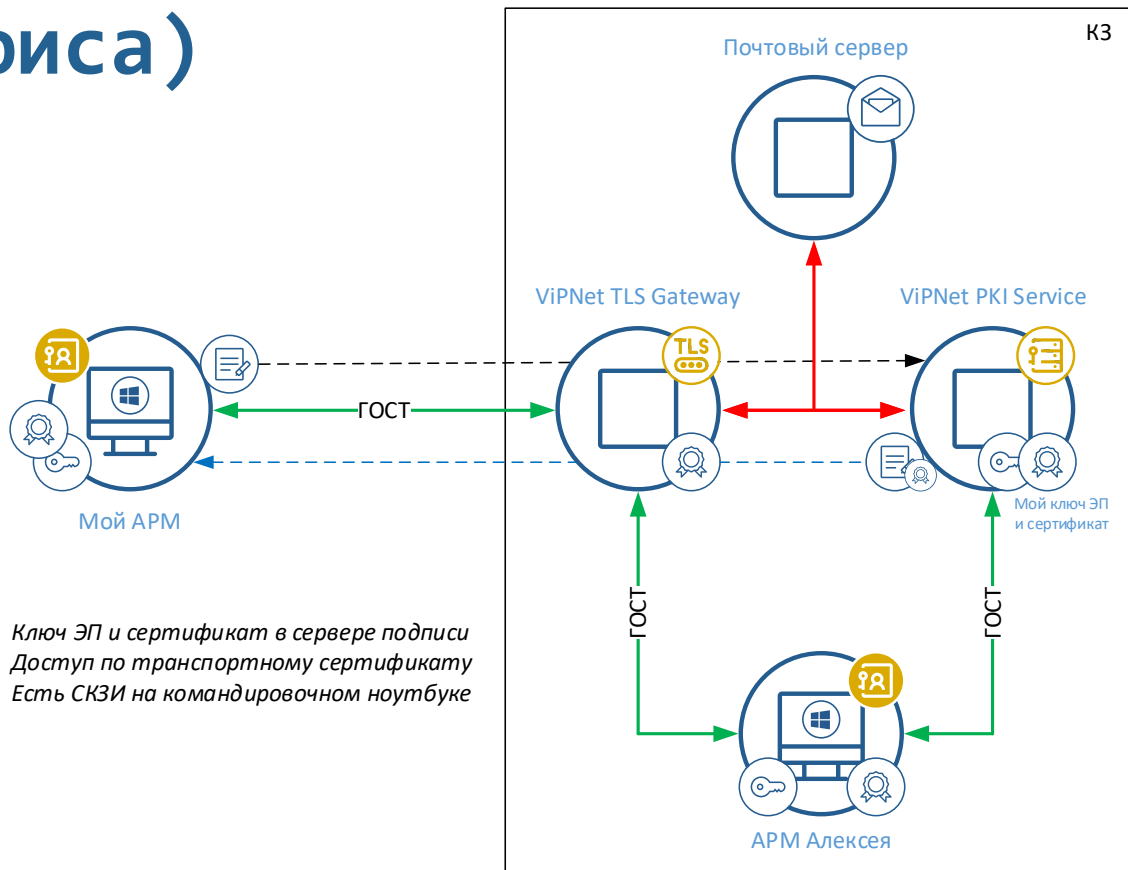
**Демонстрация .  
Переходим к практике !**

# Оформление командировки (в офисе)



- Ключ ЭП и сертификат в сервере подписи
- Доступ по логину и паролю
- Нет СКЗИ/средств ЭП на рабочем месте

# Оформление отпуска (вне офиса)



- Ключ ЭП и сертификат в сервере подписи
- Доступ по транспортному сертификату
- Есть СКЗИ на командировочном ноутбуке

техно infotecs  
2023 Фест

Спасибо  
за внимание!

---

Подписывайтесь на наши соцсети



[vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)