

Криптографические продукты инфраструктуры открытых ключей

Мухин Иван



ViPNet PKI: состав

Удостоверяющий центр

- ViPNet УЦ 4.6
- ViPNet УЦ 5

Клиентские компоненты

- ViPNet PKI Client
- ViPNet OSSSL
- ViPNet CSP

Серверные компоненты

- ViPNet HSM
- ViPNet PKI Service
- ViPNet TLS Gateway
- ViPNet OSSSL

ViPNet УЦ 4.6: состав



ViPNet Administrator

УКЦ выступает в качестве Центра сертификации



ViPNet Registration Point или ViPNet CA Web Service

Выступают в качестве Центра регистрации



ViPNet CA Informing

Сервис информирования



ViPNet Publication Service

Сервис публикации



ViPNet TSP-OCSP Service*

Сервис выдачи меток (штампов) времени и проверки статусов сертификатов в онлайн-режиме

** Обязательный компонент для сертификации по КСЗ, но не необходим УЦ. Требуется ViPNet CSP, может использоваться совместно с ViPNet HSM*

Сертификация

- СКЗИ КС2/КС3
- Средство УЦ КС2/КС3
- Зарегистрирован в реестре российского ПО


**ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/128-4946 от "17" июля 2024 г.

Действителен до "28" февраля 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программный комплекс «ViPNet Удостоверяющий центр 4 (версия 4.6)» (исполнения 1, 2) в комплектации согласно формуляру ФРКЕ.00114-07.30.01 ФО

соответствует требованиям ФСБ России к информационной безопасности удостоверяющих центров класса КС2 (для исполнения 1), класса КС3 (для исполнения 2), предназначенных для обработки информации не содержащей сведений, составляющих государственную тайну. Требования к средствам удостоверяющего центра, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС2 (для исполнения 1), класса КС3 (для исполнения 2), и Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 795, и может использоваться для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ-Лаборатория»

сертификационных испытаний образцов продукции №№ 769С-000507, 769С-000508.

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00114-07.30.01 ФО.

Временно исполняющий обязанности
начальника Центра защиты информации
и специальной связи ФСБ России


В.А. Шурин

ViPNet УЦ 5: состав



Центр сертификации

- ПАК ViPNet Certification Authority 5
- АРМ администратора УЦ с СКЗИ ViPNet PKI Client 2.0 для подключения к web-интерфейсу ViPNet CA



Центр регистрации

АРМ оператора УЦ с СКЗИ ViPNet PKI Client 2.0 для подключения к web-интерфейсу ViPNet CA



ViPNet TSP-OCSP Service*

Сервис выдачи меток (штампов) времени и проверки статусов сертификатов в онлайн-режиме

Без изменений



VIPNet Certification Authority 5

Центр сертификации,
разработанный
на базе VIPNet HSM

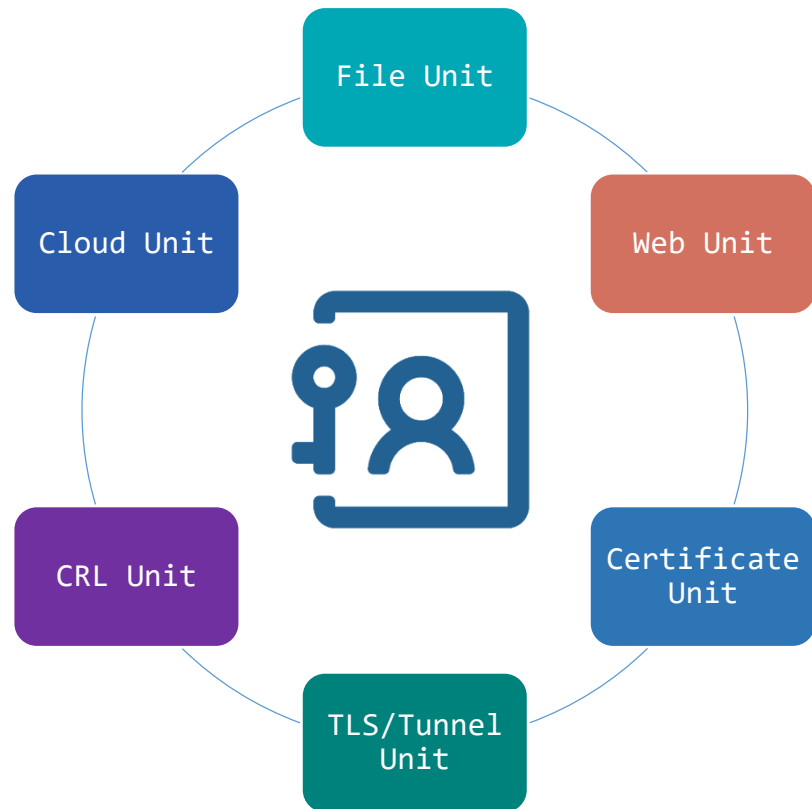


- Удобство размещения: не требуется отдельный HSM, меньшие радиусы
- Высокая производительность
- В рамках модернизации предоставляется специальная цена



ViPNet PKI Client

Универсальный клиент
для работы в инфраструктуре
открытых ключей



ViPNet PKI Client:

функциональные возможности

- Поддерживаемые криптоалгоритмы: ГОСТ 28147-89, ГОСТ 34.12-2018, ГОСТ 34.13-2018, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012
- Поддержка форматов подписи CMS, CAdES, XMLDSig, WS-Security, XAdES.
- Поддержка меток времени (TSP) и возможность проверки статусов сертификатов по протоколу OCSP.
- Поддержка протокола TLS v.1.2, 1.3.
- Поддержка аппаратных токенов.



Сертификация

- СКЗИ KC1-KC3 (Win&Lin, исп. 1-6).
- Средство ЭП KC1-KC3 (Win&Lin, исп. 1-6).
- СКЗИ KC1, средство ЭП KC1 (Android, исп. 7)

- Зарегистрирован в Реестре российского ПО
- Имеются нотификации





VIPNet TLS Gateway

Шлюз безопасности
для организации
TLS-соединений

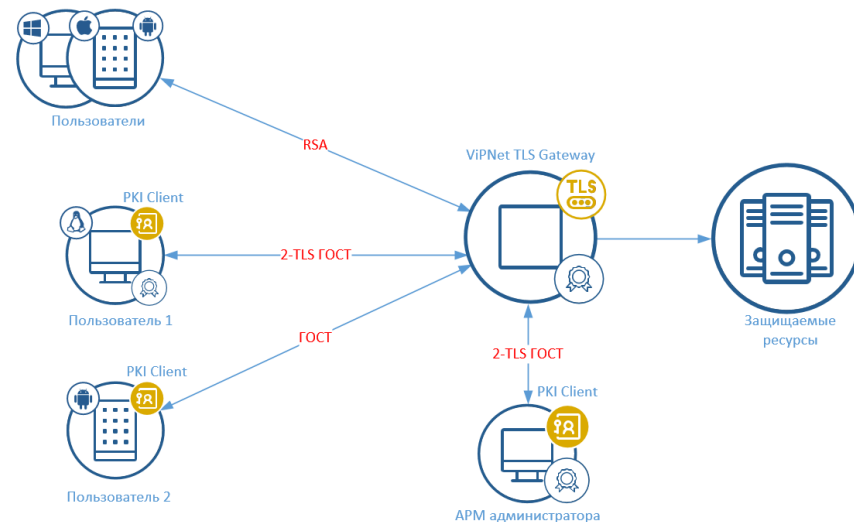


TLS шлюз

- Аутентификация клиента и сервера
- Управление доступом по сертификатам
- «Дуальный» режим работы: поддержка отечественных и иностранных криптоалгоритмов
- Кластеризация
- TLS 1.2, 1.3

ViPNet TLS Gateway: дуальный режим

- Поддерживаемые криптоалгоритмы ГОСТ:
ГОСТ 28147-89, ГОСТ 34.12-2018,
ГОСТ 34.13-2018, ГОСТ Р 34.10-2012,
ГОСТ Р 34.11-2012
- Поддержка иностранных
криптоалгоритмов* (RSA, ECDSA, AES)
для работы в дуальном режиме
- Импорт ключей в формате PFX

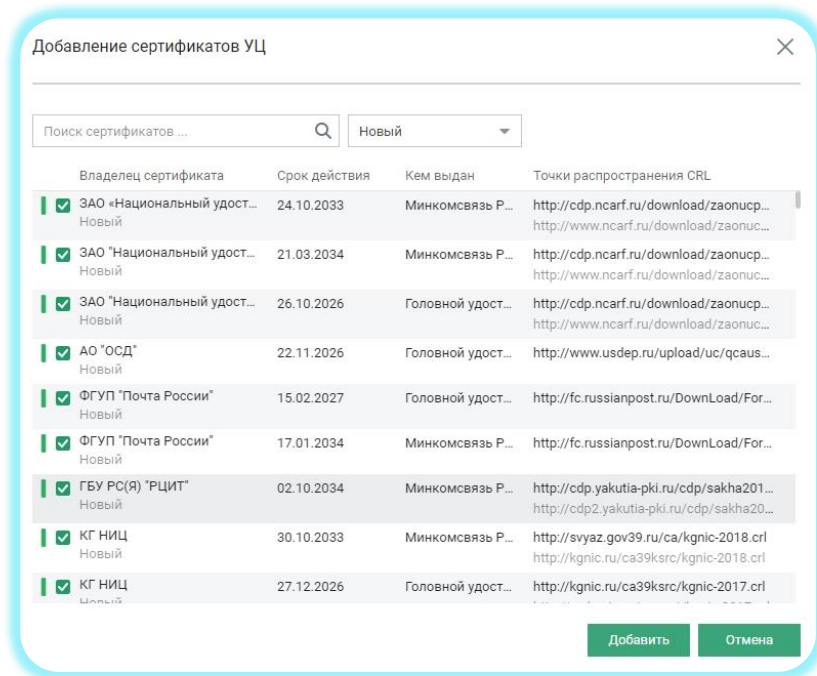


**Не могут использоваться для защиты конфиденциальной информации*

VIPNet TLS Gateway: поддержка УЦ

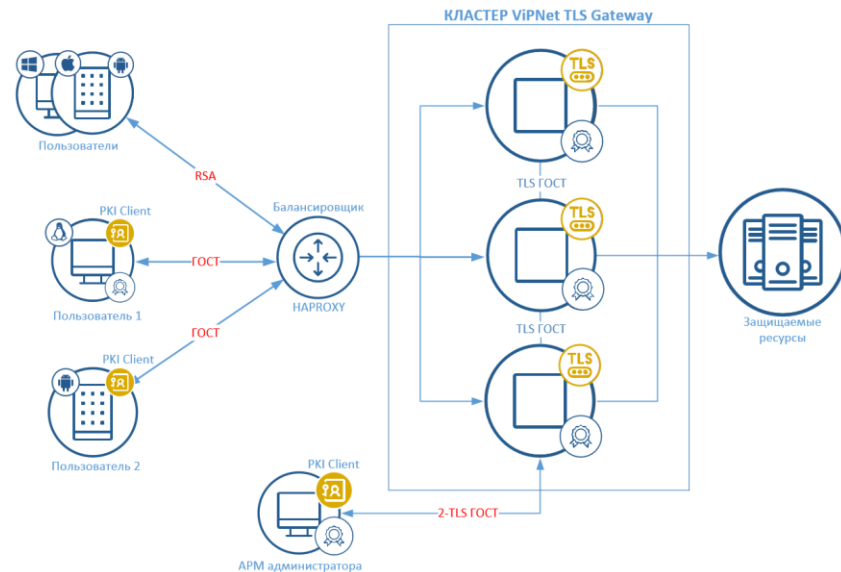
Требования 63-ФЗ и приказов 795 и 796 на VIPNet TLS Gateway не распространяются

- Запрос на сертификат в формате PKCS#10.
- Использование сертификатов, изданных различными УЦ.
- Поддержка TSL-списка аккредитованных УЦ от Минцифры для установки корневых и CRL.
- Поддержка OCSP



ViPNet TLS Gateway: кластер

- От 2 до 64 узлов
- Работа Active-Active
- Внешний балансировщик для распределения нагрузки
- Поддержка Proxy Protocol
- Защищенное соединение между узлами (TLS ГОСТ)
- Не нужен дополнительный центр управления
- Устойчивость к разделению сети — продолжает обслуживание пользователей на всех работоспособных узлах



VIPNet TLS Gateway

- СКЗИ КСЗ (исполнения ПАК)
- СКЗИ КС1 (исполнение VA)
- Зарегистрирован в реестре российского ПО, в реестре российской промышленности, реестре ПАК Минцифры
- Клиентское ПО: ViPNet PKI Client, ViPNet CSP или любое сертифицированное СКЗИ





ViPNet HSM

Программно
аппаратный модуль
(HSM – Hardware Secure
Module)



- Генерация ключей ЭП
- Хранение ключей ЭП
- Создание и проверка ЭП
- Шифрование/расшифрование
- Интерфейс PKCS#11

Сертификация

- СКЗИ KB
- Средство ЭП KB2
- Зарегистрирован в реестре российского ПО, в реестре российской промышленности, в реестре ПАК Минцифры





ViPNet PKI Service

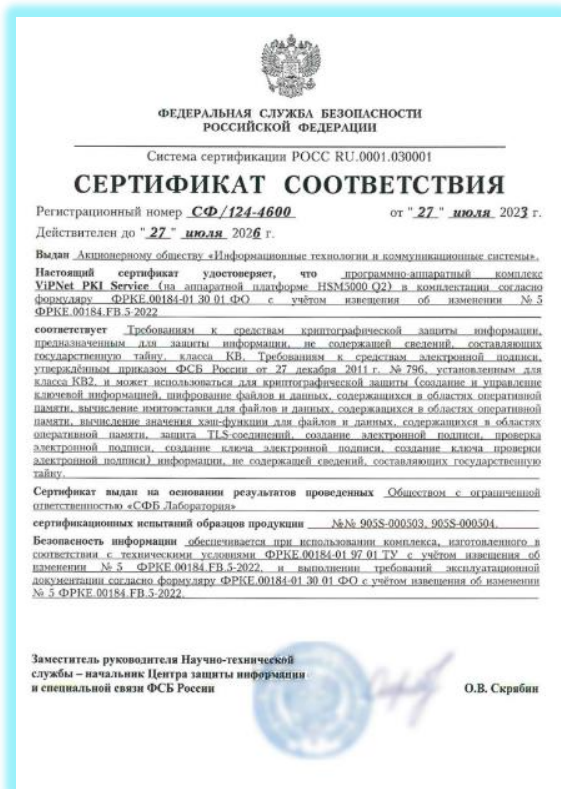
Универсальный
криптографический модуль/
сервер подписи



- Шифрование/расшифрование
- Простановка/проверка ЭП
- Кластеризация
- REST API

Сертификация

- СКЗИ КВ
- Средство ЭП КВ2
- Зарегистрирован в реестре российского ПО, в реестре российской промышленности, в реестре ПАК Минцифры





VipNet HSM

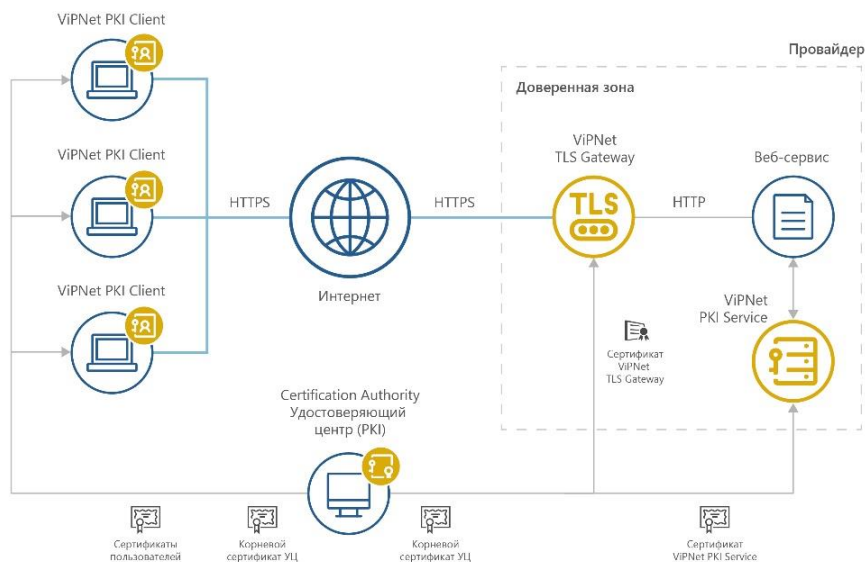
- API – PKCS#11
(предоставляется HSM SDK)
- Поддержка иностранных криптоалгоритмов
- Может потребоваться сертификация



VipNet PKI Service

- API - REST
- Взаимодействие с другими PKI-продуктами
- Может потребоваться оценка влияния (есть список «белых функций»)

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

ViPNet HSM: поддержка иностранной криптографии

- Создание асимметричных ключей, создание и проверка ЭП по FIPS 186-4
- Создание симметричных ключей по FIPS 197, FIPS 46-3, NIST SP 800-132
- Шифрование данных по NIST SP 800-38A
- Вычисление функции хэширования по FIPS 180-4
- Формирование производных ключей по NIST SP 800-108 и т.д.



Применение продуктов ViPNet PKI в проекте Цифровой рубль



ViPNet YU



ViPNet PKI
Client



ViPNet TLS
Gateway



ViPNet OSSL



ViPNet PKI
Service



ViPNet CSP



ViPNet HSM

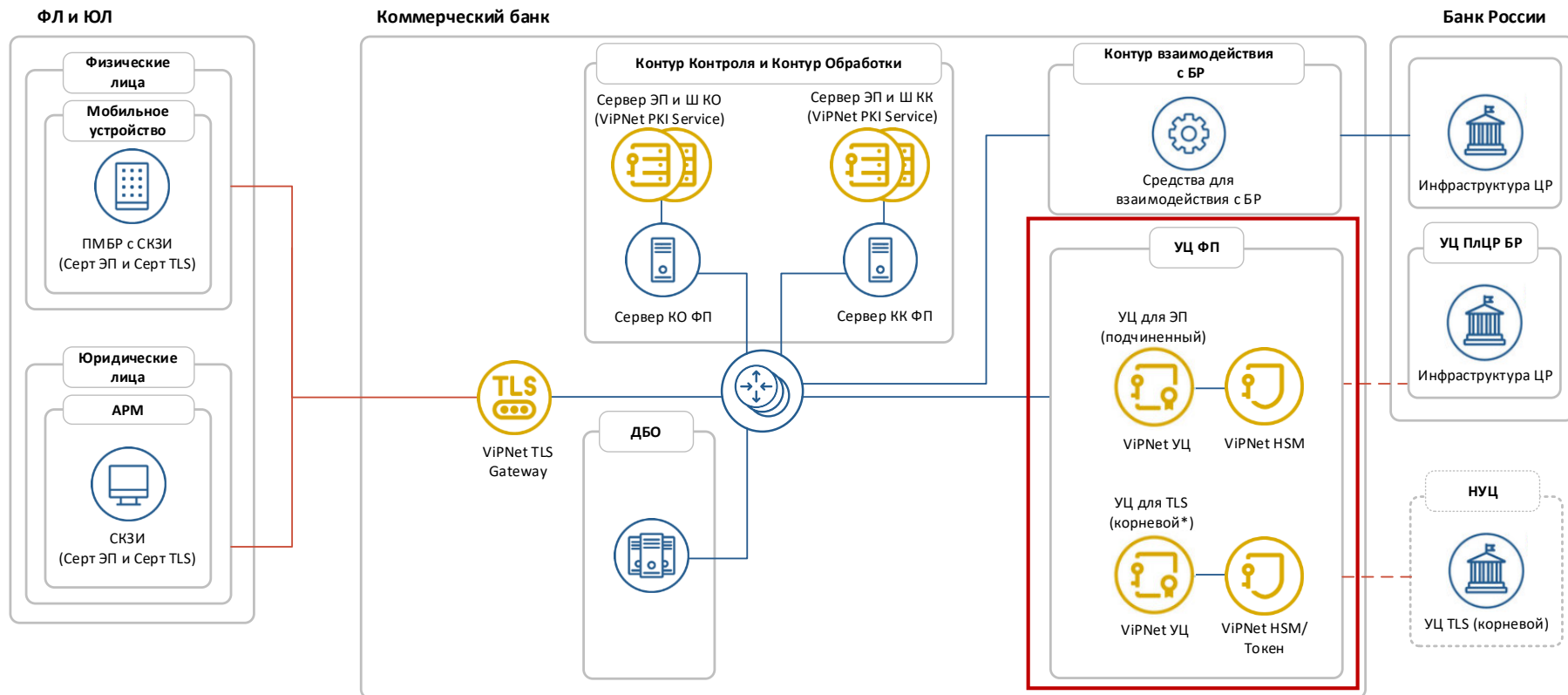


Цифровой рубль – цифровая форма российской национальной валюты, которую Банк России планирует выпускать в дополнение к существующим формам денег

Роли сторон в платформе ЦР



Общая схема инфраструктуры



Сегмент УЦ



Удостоверяющие центры ФП

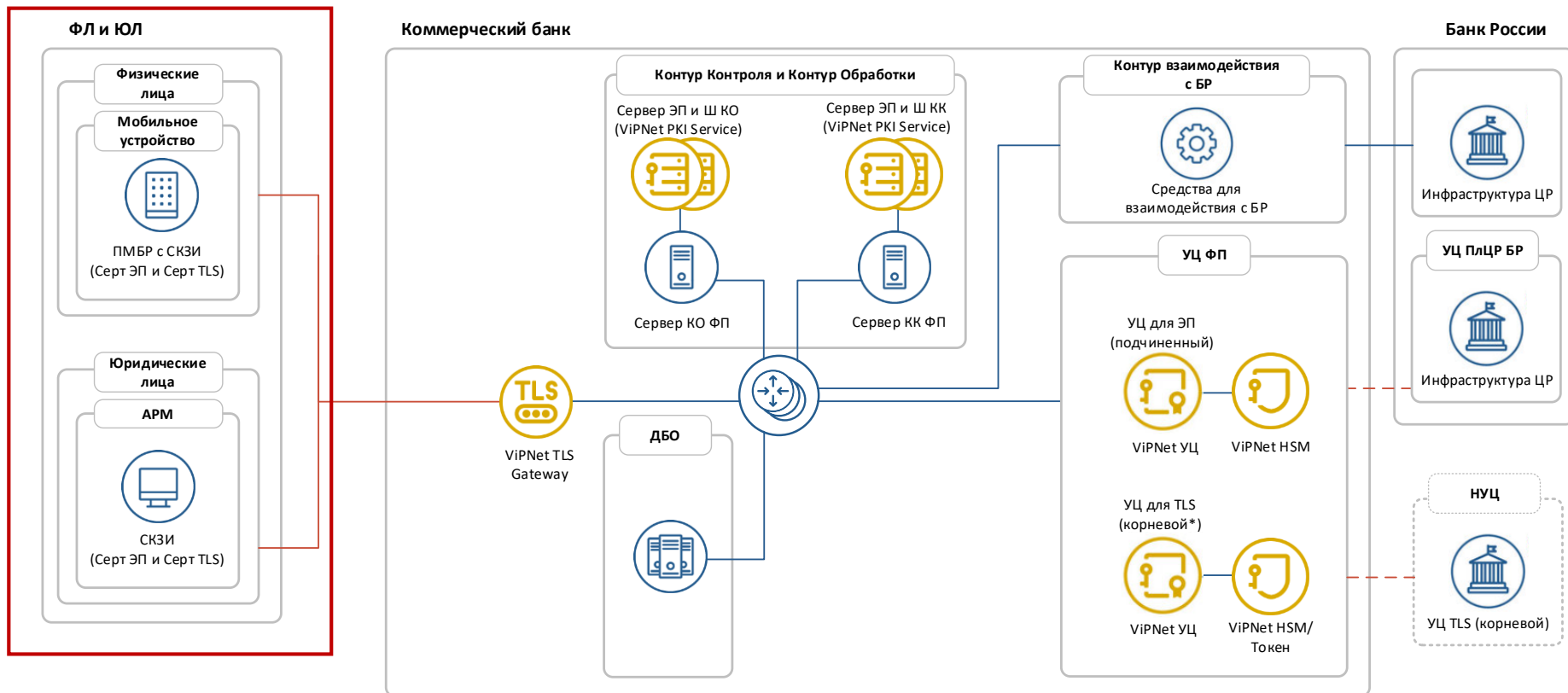


ViPNet УЦ



ViPNet HSM

Общая схема инфраструктуры



Сегмент пользователей



ПМ БР с ViPNet OSSL

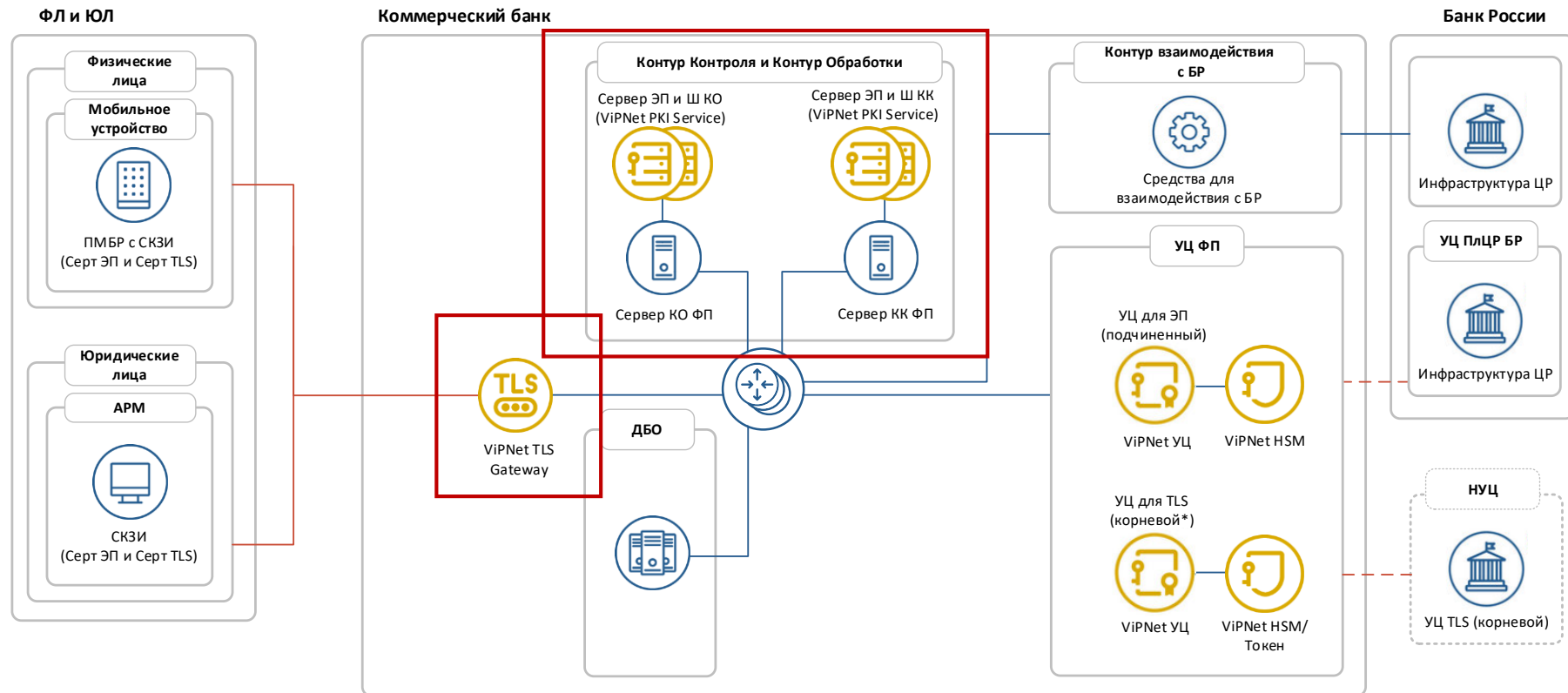


Браузер с ViPNet PKI Client
и ViPNet CSP

Функции:

- запросы на сертификат
- TLS-соединения
- подпись сообщений
- шифрование/расшифрование сообщений

Общая схема инфраструктуры



СКЗИ КО и КК



СКЗИ для КО и КК:



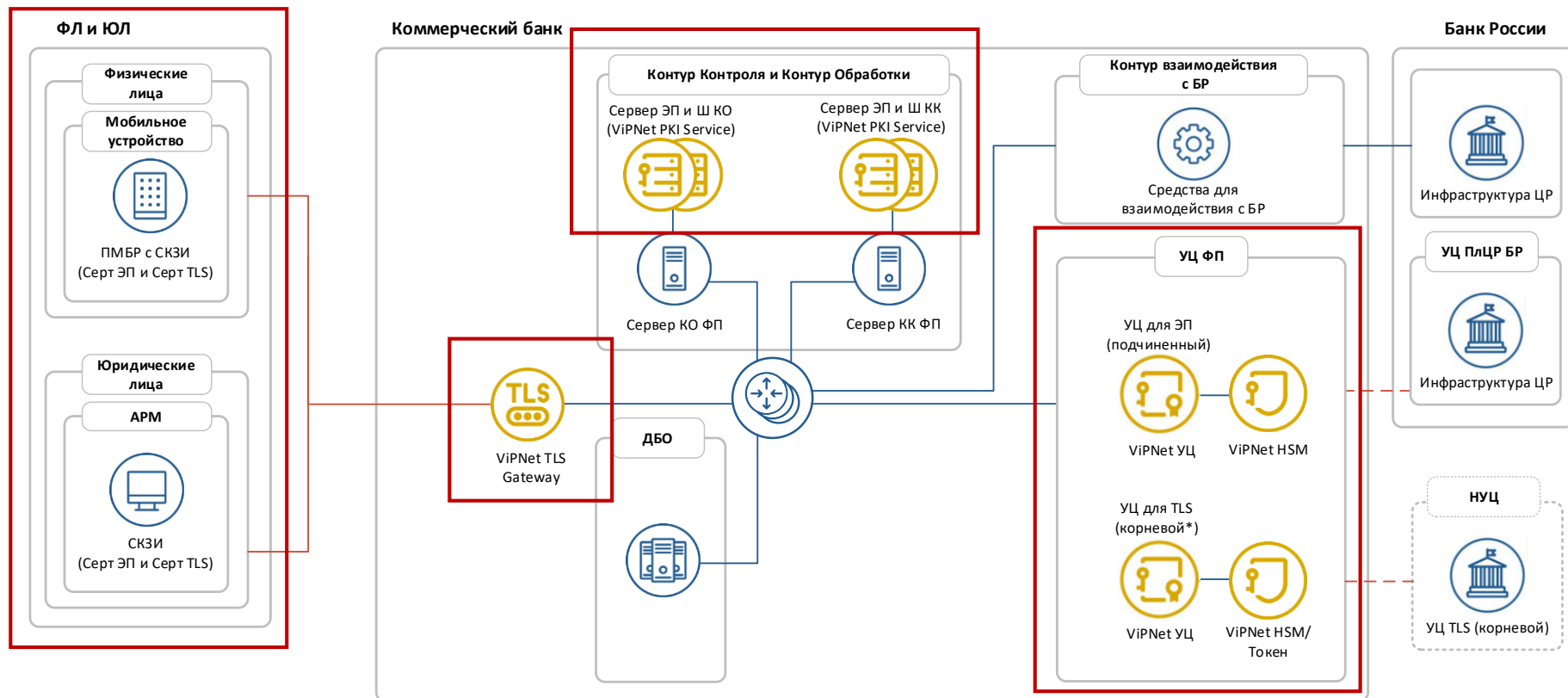
ViPNet PKI Service

ИЛИ



ViPNet OSSL

Общая схема инфраструктуры



А также!



Криптография в финтехе

Официальный канал ИнфоТеКС, посвященный защите информации в банковской сфере. Мы рассказываем о том, как с помощью криптографических операций, например, шифрования, электронной подписи, обеспечивается информационная безопасность современного финтех



TECH infotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного

