Использование продуктов ViPNet для защиты инфраструктуры Цифрового рубля в банках

Мухин Иван
Руководитель направления

Что такое цифровой рубль?

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

- Эмитентом цифрового рубля является Банк России
- Банк России открывает кошельки банкам и Федеральному казначейству, а также кошельки физическим и юридическим лицам по их поручению через банки
- Клиентам, банкам и Федеральному казначейству открывается только один кошелек в цифровых рублях
- На размещенные в кошельках цифровые рубли не начисляется процентный доход на остаток
- Средства на кошельке доступны клиенту через любой банк, где он обслуживается

Нормативные документы по цифровому рублю

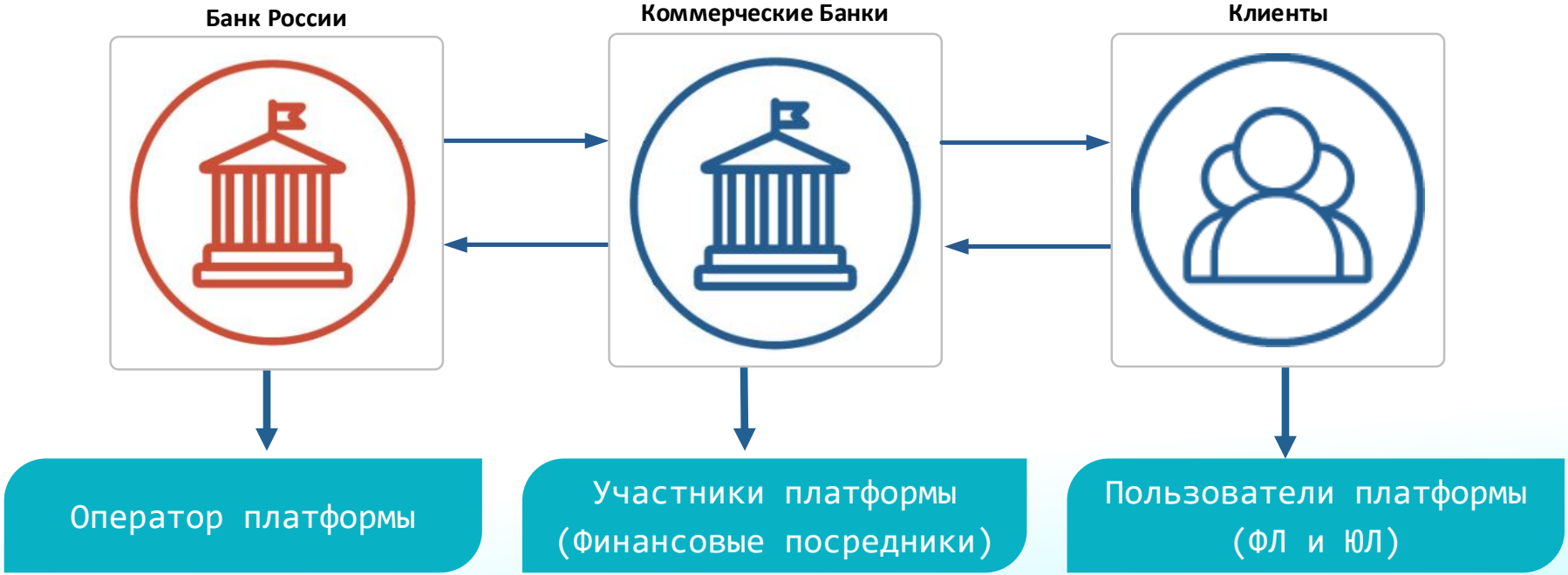
Положения Банка России:

- «О платформе цифрового рубля» №820-П от 03.08.2023 с учетом изменений от 12.07.2024
- «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля» №833-П от 07.12.2023

Стандарты платформы цифрового рубля:

- ЦВЦБ. Стандарт. Порядок подключения Финансового посредника к Платформе Цифрового Рубля. Версия 1.2
- Стандарт платформы цифрового рубля. «Порядок подключения участника платформы к платформе цифрового рубля» версия 1.3
- и другие, см. http://www.cbr.ru/fintech/dr/doc_dr/standarts/

Роли сторон в платформе ЦР



Продукты ViPNet для создания защищенного взаимодействия участников платформы цифрового рубля

ViPNet TLS Gateway

ViPNet PKI Service

ViPNet OSSL

ViPNet УЦ

ViPNet HSM

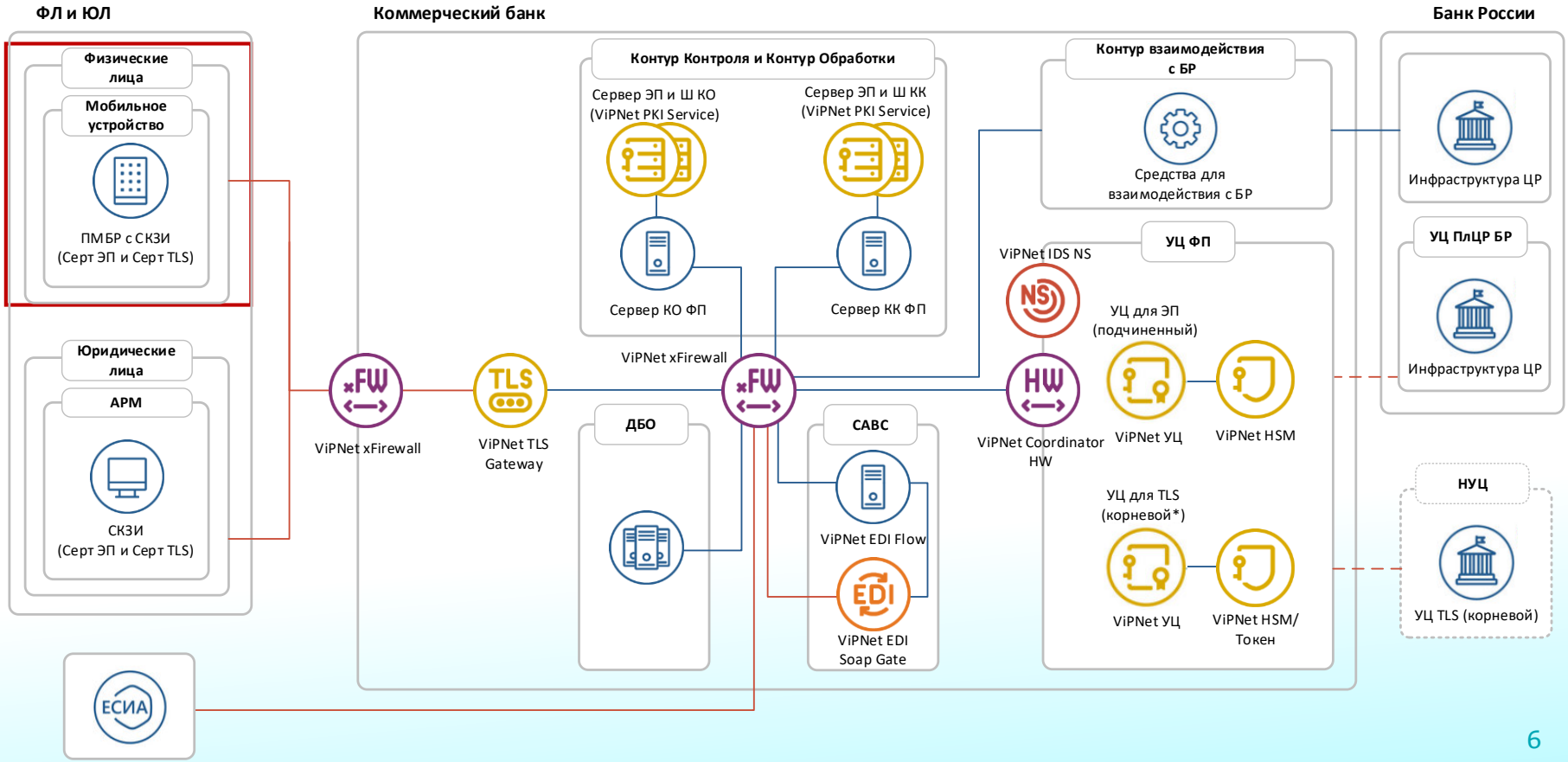
ViPNet IDS NS

ViPNet Coordinator HW

ViPNet xFirewall

ViPNet SafeBoot

Общая схема инфраструктуры



Программный модуль Банка России

Ядро – СКЗИ ГОСТ
(ViPNet OSSL, ...)

«Надстройка» в виде API
для работы СКЗИ с мобильным
приложением банка

Программный модуль Банка России

ПМ БР с ViPNet OSSL – разработка ИнфоТеКС по заданию Банка России

ПМ БР – исключительные права принадлежат Банку России

Функции:

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

ViPNet OSSL

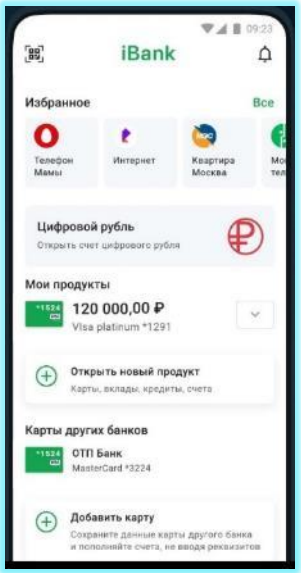
Криптобиблиотека для разработки мобильных и серверных решений

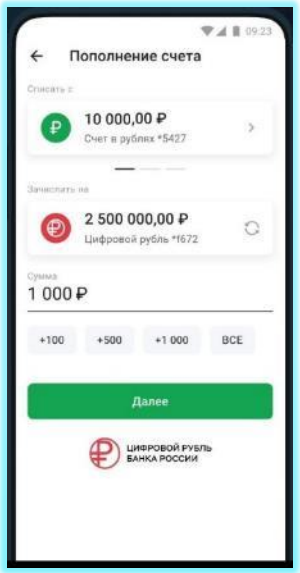
- Электронная подпись/проверка подписи
- Шифрование/расшифрование
- Защищенные соединения TLS
- Хеширование
- Работа с токенами
- Интерфейсы OpenSSL и PKCS#11
- СКЗИ/Средство ЭП класса КС1, КС2, КС3

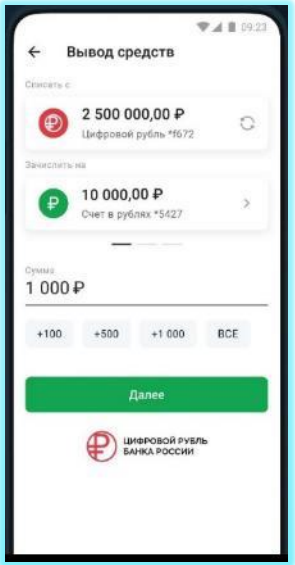
Пользователи платформы ЦР

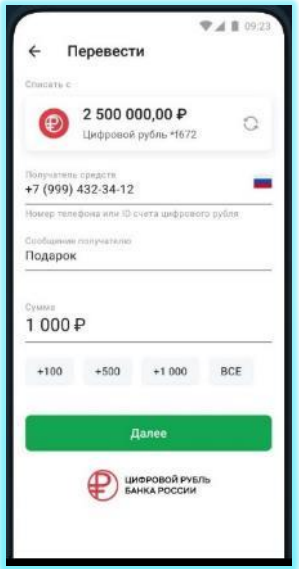
BIFIT

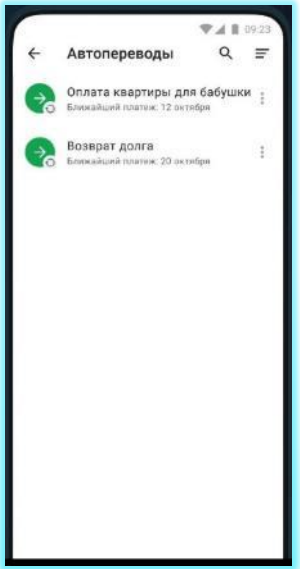
В мобильном приложении банка появится соответствующий стандарту платформы интерфейс для совершения операций



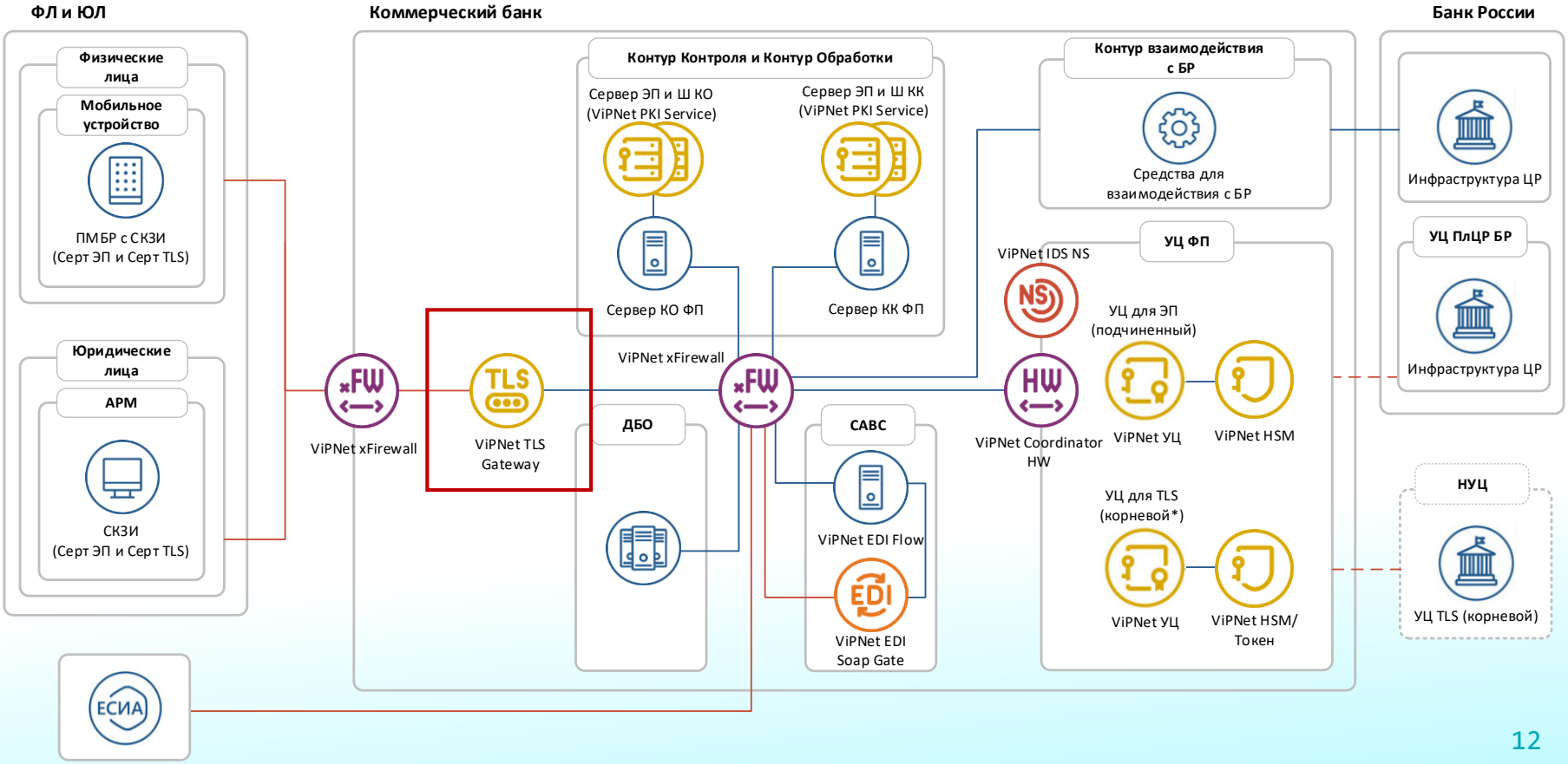








Общая схема инфраструктуры

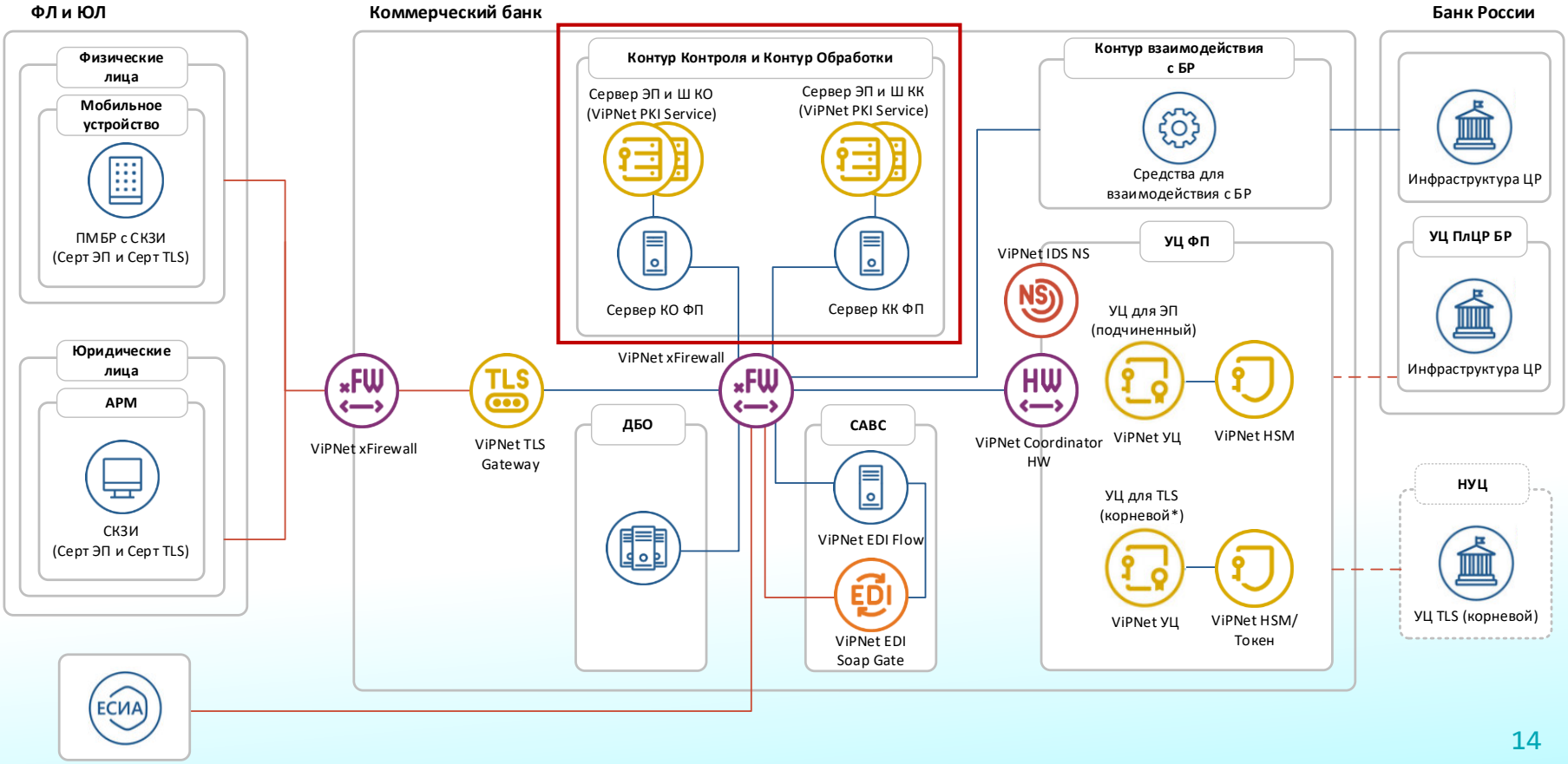


ViPNet TLS Gateway

Шлюз безопасности для организации TLS-соединений

- Аутентификация клиента и сервера
- Управление доступом по сертификатам
- «Дуальный» режим работы: поддержка отечественных и иностранных криптоалгоритмов
- Кластеризация
- TLS 1.2, 1.3
- СКЗИ класса КС3
- Зарегистрирован в реестре российского ПО, рестре Минпромторга и реестре ПАК Минцифры

Общая схема инфраструктуры



СКЗИ КО и КК

СКЗИ для КО и КК:

ViPNet PKI Service

ИЛИ

ViPNet OSSL

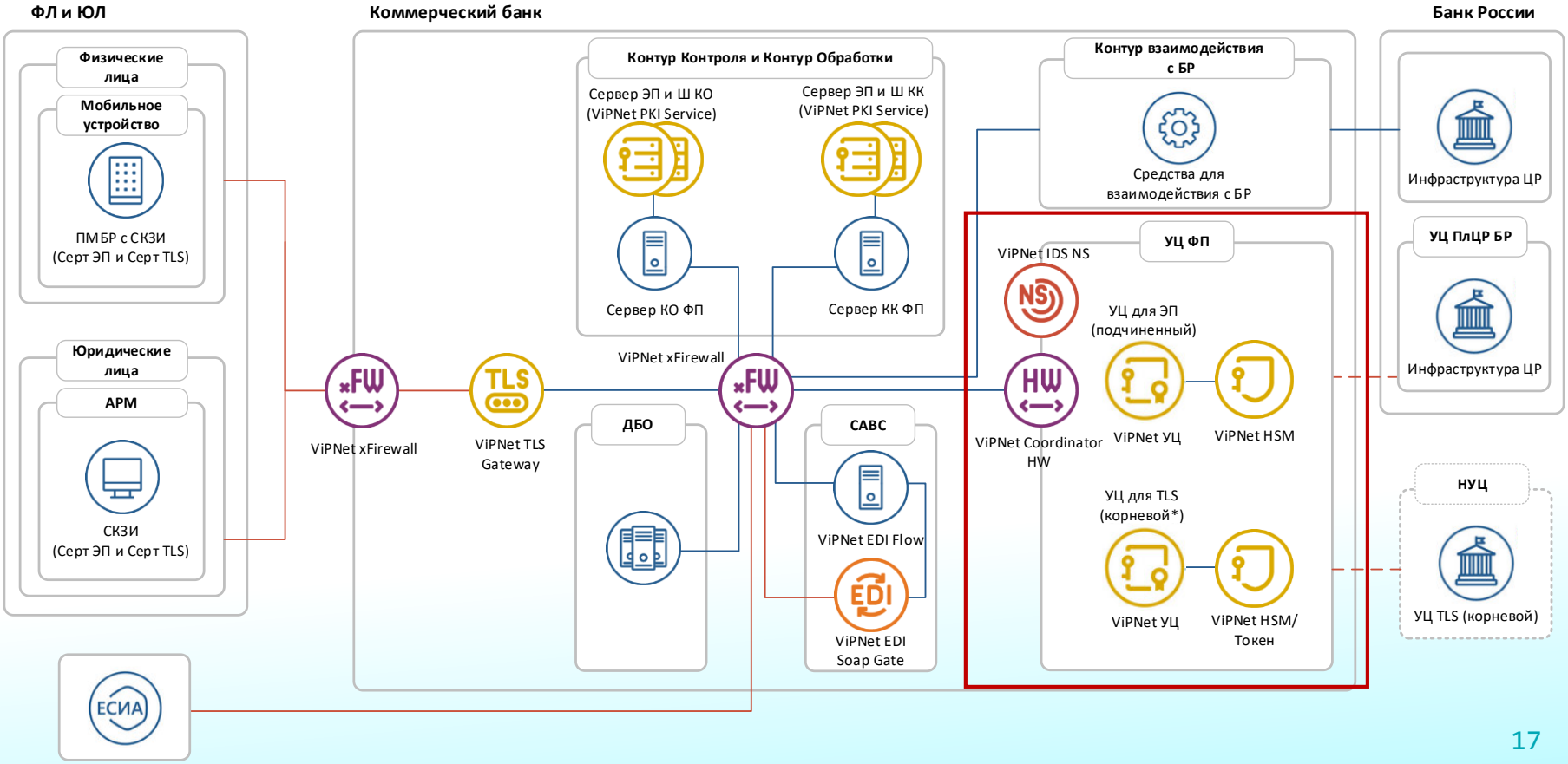
- СКЗИ не ниже КС3 (с 1 января 2025, п.14.1, 833-П)
- Средство ЭП не ниже КС3 (с 1 января 2025, п.14.1, 833-П)

ViPNet PKI Service

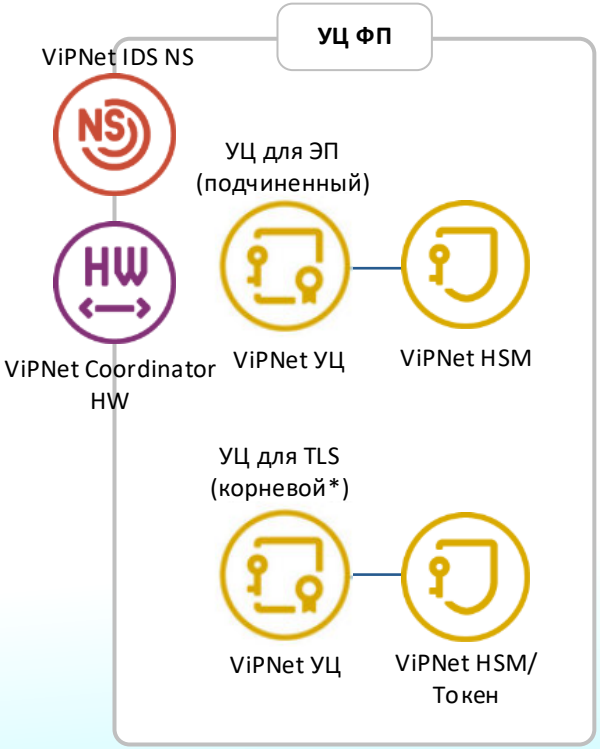
Сервер подписи, разработанный на базе ViPNet HSM

- Шифрование/расшифрование
- Простановка/проверка ЭП
- Кластеризация
- REST API
- СКЗИ класса КВ, средство ЭП класса КВ2
- Зарегистрирован в реестре российского ПО, реестре Минпромторга и реестре ПАК Минцифры

Общая схема инфраструктуры



Инфраструктура УЦ коммерческого банка



Удостоверяющие центры ФП

ViPNet УЦ

ViPNet HSM

Средства для защиты УЦ ФП

ViPNet Coordinator HW

ViPNet IDS NS

ViPNet УЦ

Удостоверяющий центр для издания и обслуживания сертификатов ключа проверки электронной подписи

- Создание сертификатов ключей проверки ЭП
- Проверка уникальности ключей проверки ЭП
- Ведение реестра сертификатов ключей проверки ЭП
- Аннулирование и досрочное прекращение действия созданных сертификатов
- Средство УЦ класса КС3

ViPNet HSM

Программно-аппаратный модуль (HSM – Hardware Secure Module)

- Генерация ключей ЭП
- Хранение ключей ЭП
- Создание и проверка ЭП
- Шифрование/расшифрование
- Интерфейс PKCS#11
- СКЗИ класса КВ, средство ЭП класса КВ2
- Зарегистрирован в реестре российского ПО, реестре Минпромторга и реестре ПАК Минцифры

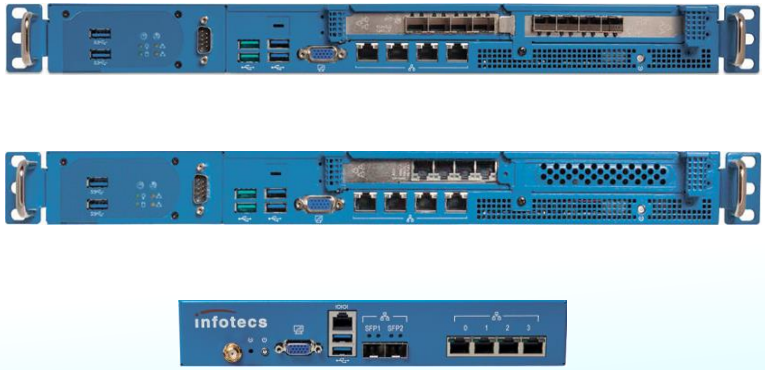
ViPNet Coordinator HW

Межсетевой экран/ Криптошлюз

- Защита каналов передачи данных с использованием алгоритмов ГОСТ
- Фильтрация сетевых соединений и поддержка политик безопасности
- Сегментация сети, организация DMZ
- Сокрытие адресов и информации о структуре сети
- Отказоустойчивый кластер
- МЭ 4 класса, СКЗИ класса КС3

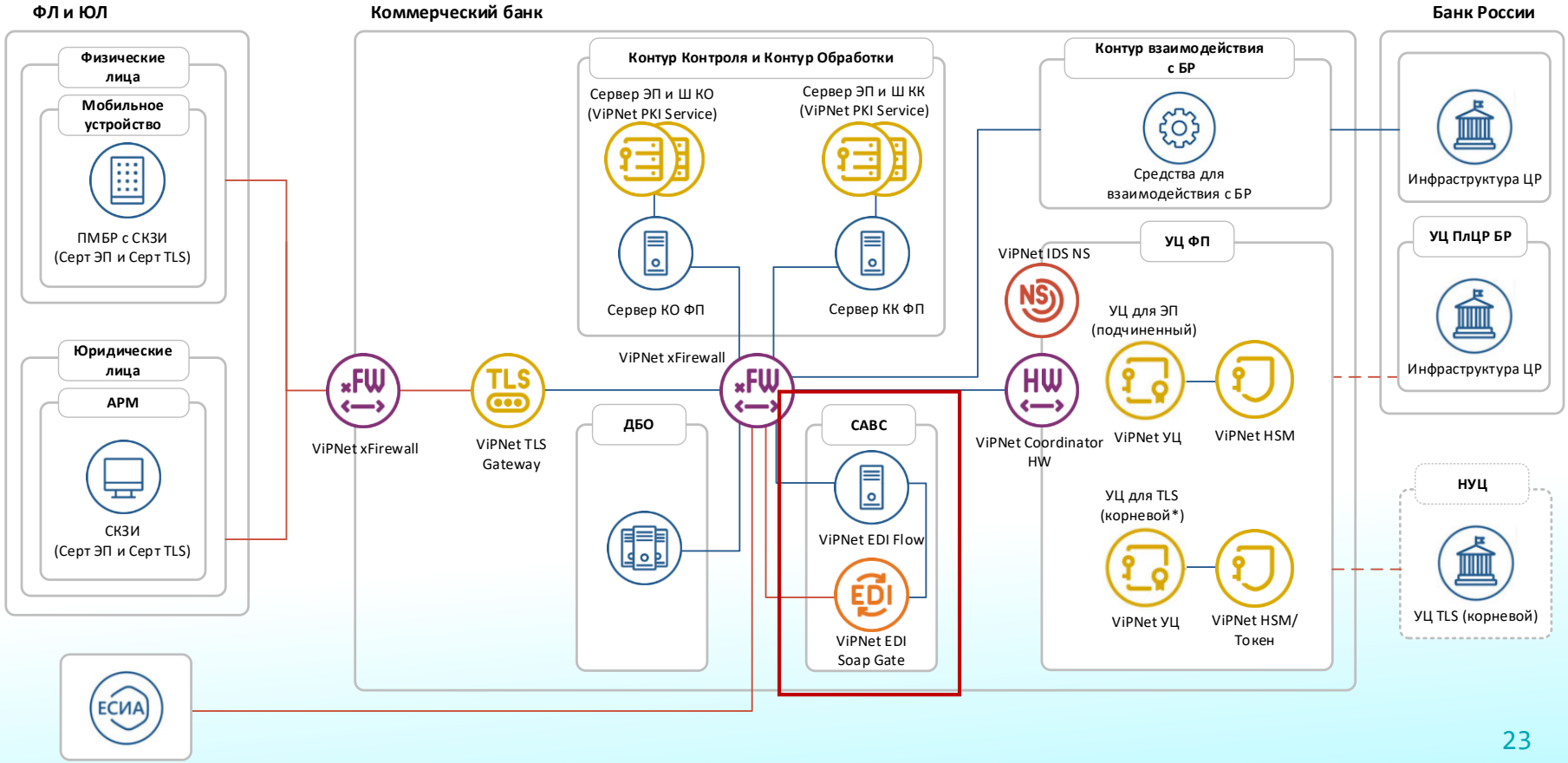
ViPNet IDS NS

Система обнаружения атак (вторжений) уровня сети

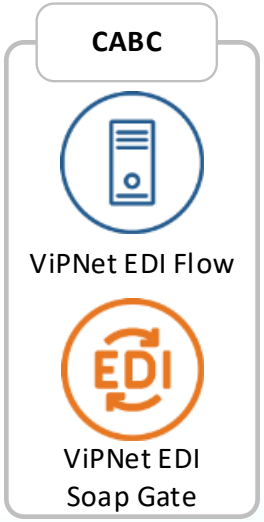


- Сбор информации о сетевом трафике
- Динамический анализ собранных данных о сетевом трафике
- Анализ собранных данных о сетевом трафике сигнатурным и эвристическим методами
- Анализ собранных данных о сетевом трафике с целью обнаружения фактов передачи файлов, содержащих вредоносное ПО
- Средство обнаружения компьютерных атак класса В

Общая схема инфраструктуры



Сервис Автоматизации Выпуска Сертификатов



ПК ViPNet EDI Flow

- управление ViPNet САВС
- выполнение процессов, связанных с выпуском сертификатов безопасности и сертификатов ЭП

ПАК ViPNet EDI Soap Gate 3

- СКЗИ и средство ЭП для идентификации пользователей ПлЦР в ЕСИА
- проставление и проверка ЭП по классу КС3

ViPNet EDI Soap Gate

ПАК для обмена электронными сведениями с применением электронной подписи

- Авторизация пользователей в ЕСИА и ЦПГ
- Получение данных в СМЭВ, ЕСИА, ЦПГ, ЦПО
- Подпись и проверка подписи ГОСТ
- Построение TLS ГОСТ
- СКЗИ и средство ЭП КС3
- Возможность интеграции с ИС (без оценки влияния)
- Зарегистрирован в реестре российского ПО, реестре Минпромторга и реестре ПАК Минцифры

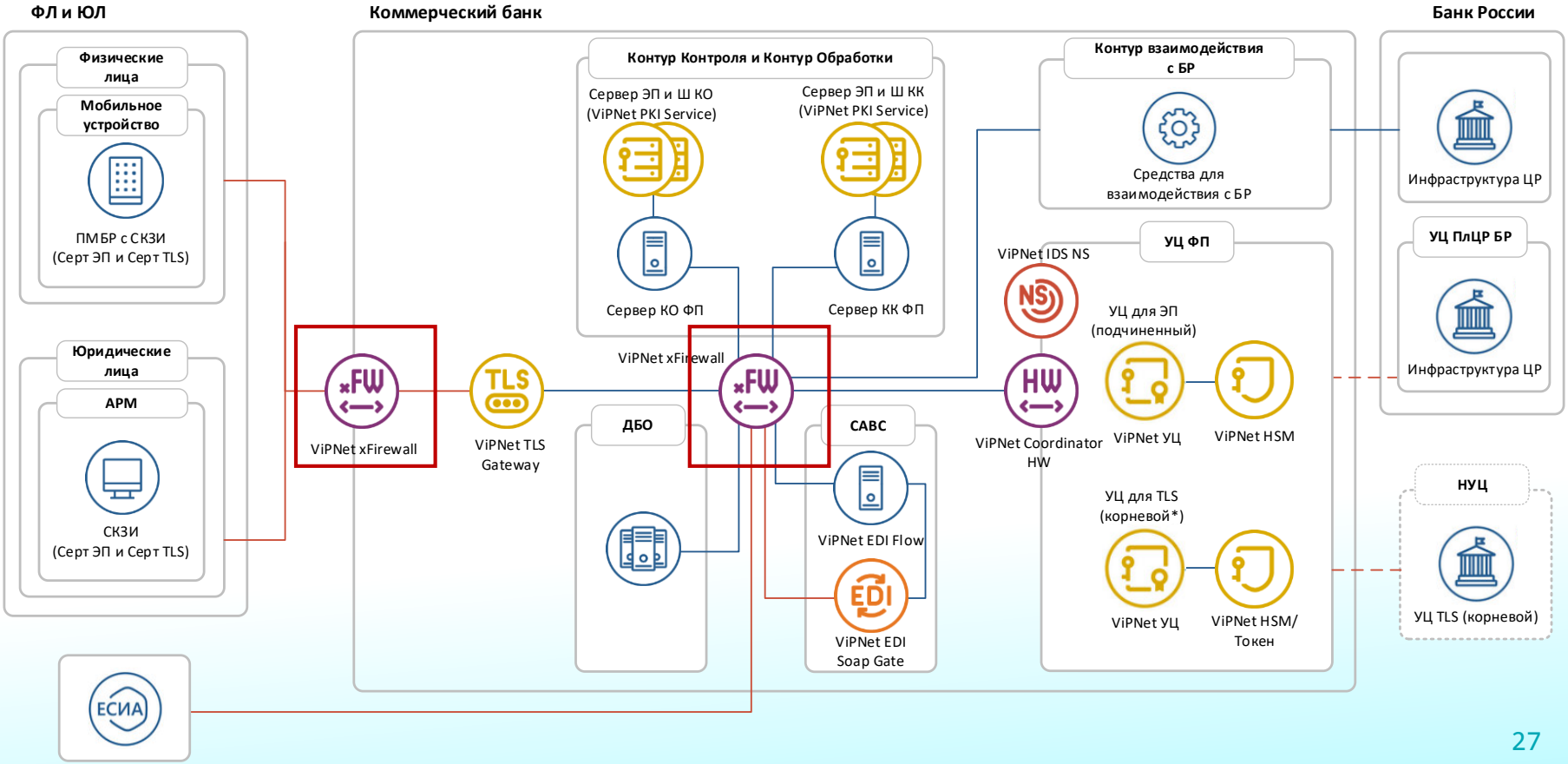
ViPNet EDI Flow

ТЕХНО infotecs ФЕСТ

ViPNet EDI Flow – программный комплекс, который обеспечивает взаимодействие с ViPNet EDI Soap Gate и удостоверяющими центрами

ViPNet EDI Flow является управляющим компонентом ViPNet CABC и обеспечивает выполнение всех процессов, связанных с выпуском сертификатов безопасности и сертификатов ЭП пользователя ПлЦР

Общая схема инфраструктуры

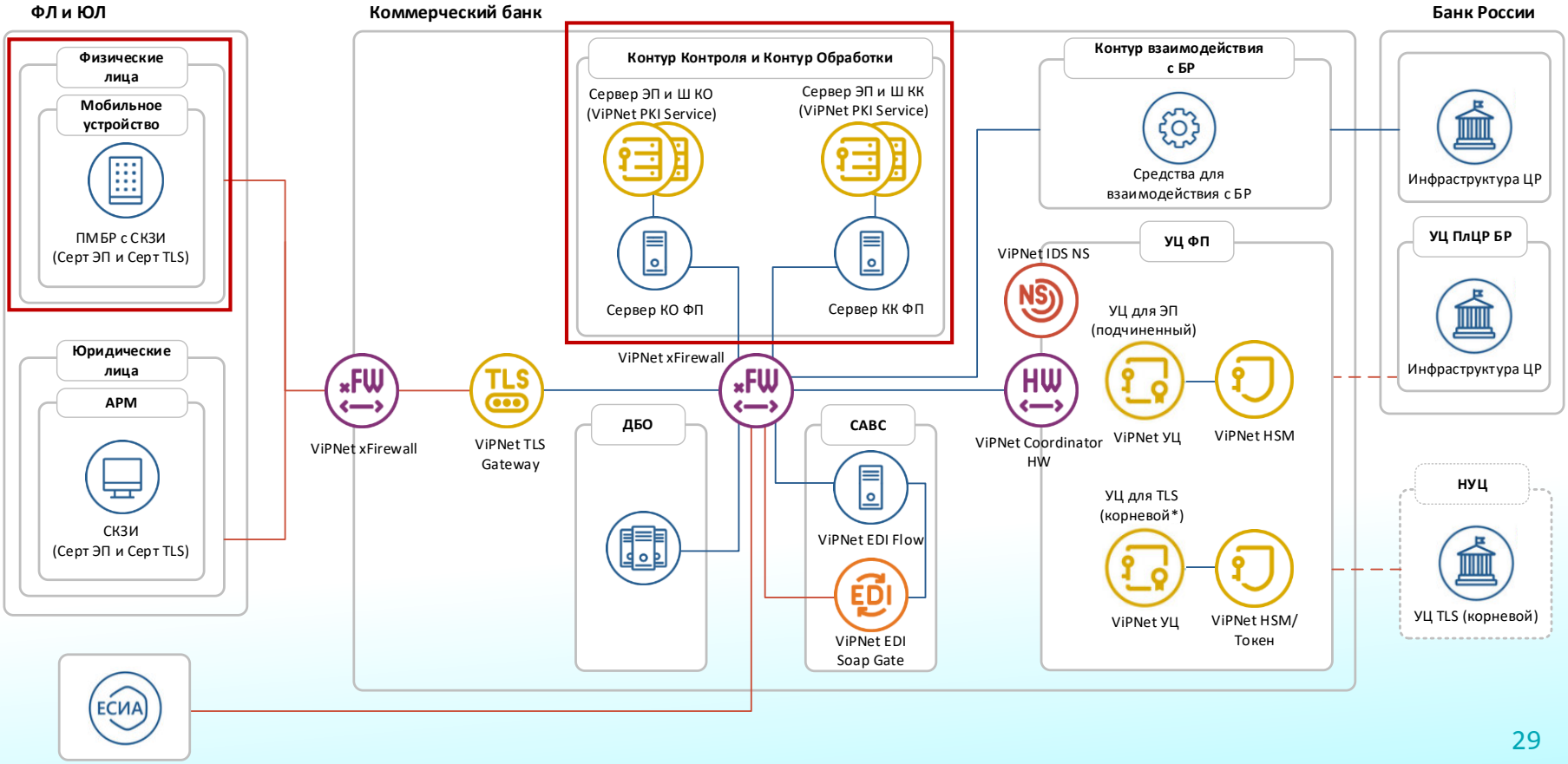


ViPNet xFirewall

NGFW

- Мониторинг и контроль сетевой активности пользователей и приложений
- Контроль взаимодействия с внешними сетями на сетевом и транспортном уровнях модели OSI
- Обнаружение и нейтрализация сетевых вторжений
- Интеграция с другими решениями в области информационной безопасности и сетевых технологий
- Соответствует требованиям к МЭ и СОВ по 4 классу защиты

Общая схема инфраструктуры



Встраивание и оценка влияния

В соответствии с №833-П от 07.12.2023 «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля»

6. Обеспечение защиты информации участниками платформы с использованием СКЗИ должно осуществляться в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года N 66, требованиями технической документации на СКЗИ, включая требования к проведению оценки влияния аппаратных, программно-аппаратных и программных средств сети (систем) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований

Встраивание и оценка влияния

Аккредитованная испытательная лаборатория в системах сертификации ФСБ России и ФСТЭК России, имеющая право и опыт проведения тематических исследований (сертификационных испытаний) программных и программно-аппаратных средств на соответствие требованиям ФСБ России к средствам криптографической защиты информации

Стандарт платформы цифрового рубля «Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы)…»

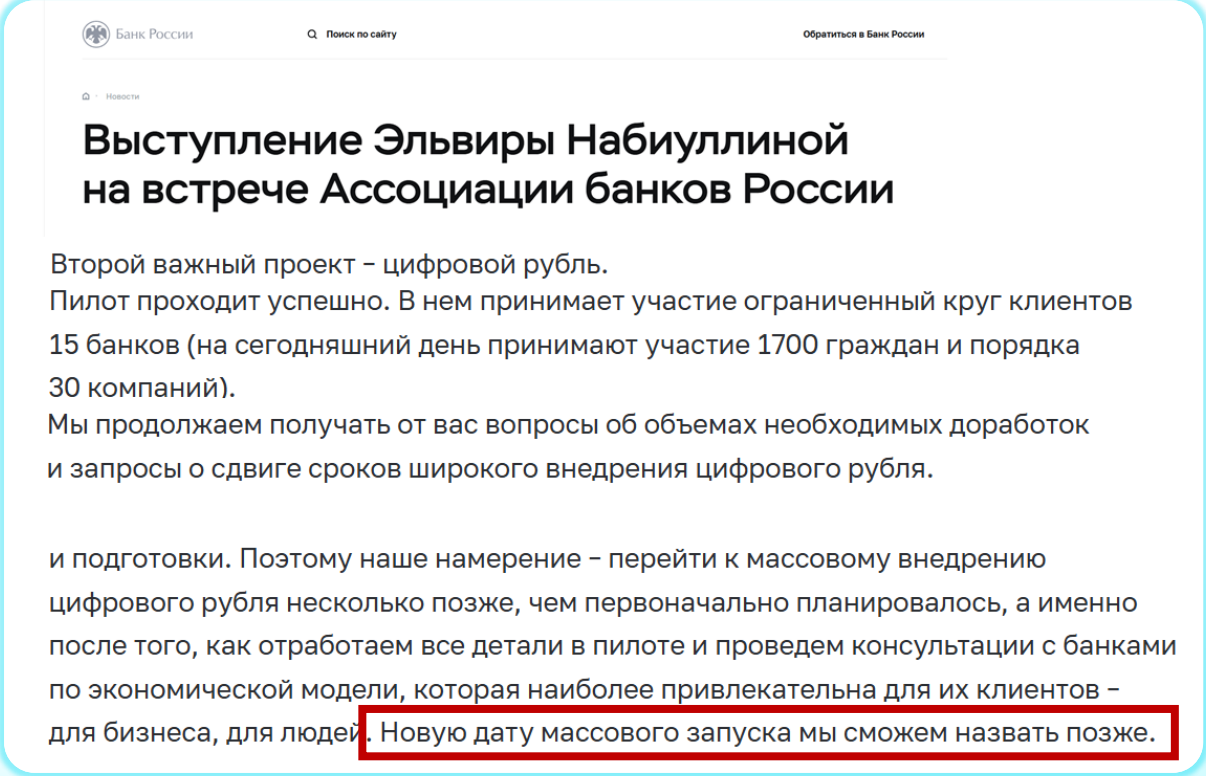
Планы по внедрению ЦР

Срок	Финансовые посредники*	Предприятия с выручкой в год **
До 01.07.2025*	Системно значимые банки	более 30 млн рублей
До 01.07.2026*	Банки с универсальной лицензией	более 20 млн рублей
До 01.07.2027*	Прочие кредитные организации	Все другие

* Открытие и пополнение счета, переводы и т.п.

** Прием оплаты в ЦР по универсальному QR-коду на базе НСПК

Планы по внедрению ЦР



Банк России Поиск по сайту Обратиться в Банк России

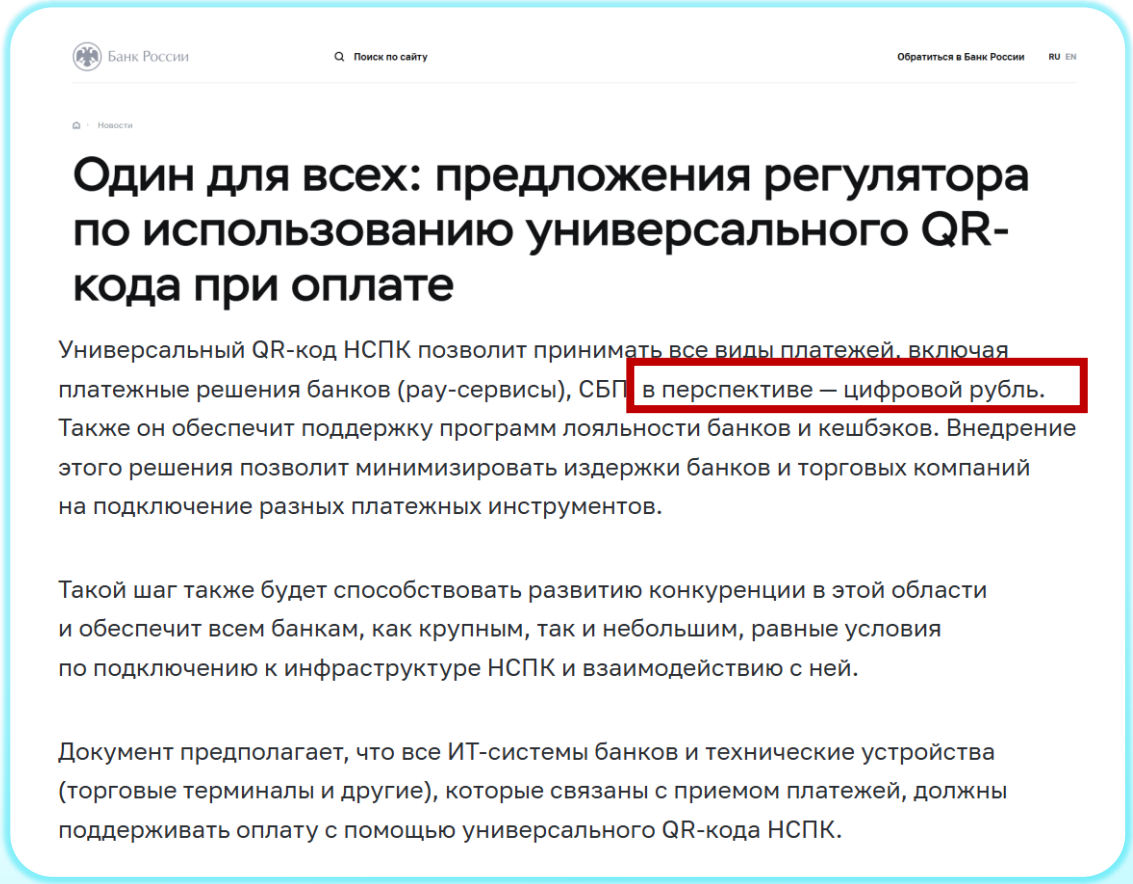
Новости

Выступление Эльвиры Набиуллиной на встрече Ассоциации банков России

Второй важный проект – цифровой рубль.
Пилот проходит успешно. В нем принимает участие ограниченный круг клиентов 15 банков (на сегодняшний день принимают участие 1700 граждан и порядка 30 компаний).
Мы продолжаем получать от вас вопросы об объемах необходимых доработок и запросы о сдвиге сроков широкого внедрения цифрового рубля.

и подготовки. Поэтому наше намерение – перейти к массовому внедрению цифрового рубля несколько позже, чем первоначально планировалось, а именно после того, как отработаем все детали в пилоте и проведем консультации с банками по экономической модели, которая наиболее привлекательна для их клиентов – для бизнеса, для людей. Новую дату массового запуска мы сможем назвать позже.

Использование цифрового рубля



Банк России Поиск по сайту Обратиться в Банк России RU EN

Новости

Один для всех: предложения регулятора по использованию универсального QR-кода при оплате

Универсальный QR-код НСПК позволит принимать все виды платежей, включая платежные решения банков (pay-сервисы), СБП в перспективе — цифровой рубль. Также он обеспечит поддержку программ лояльности банков и кешбэков. Внедрение этого решения позволит минимизировать издержки банков и торговых компаний на подключение разных платежных инструментов.

Такой шаг также будет способствовать развитию конкуренции в этой области и обеспечит всем банкам, как крупным, так и небольшим, равные условия по подключению к инфраструктуре НСПК и взаимодействию с ней.

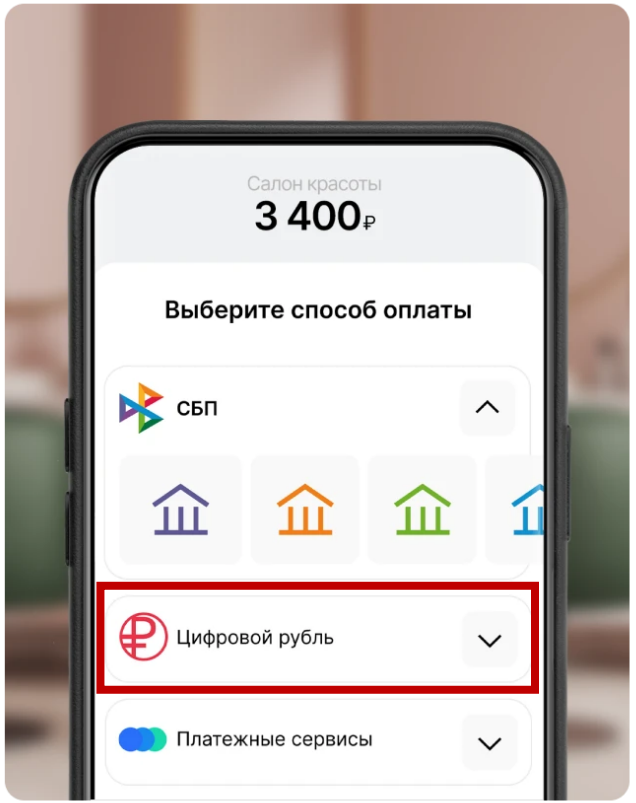
Документ предполагает, что все ИТ-системы банков и технические устройства (торговые терминалы и другие), которые связаны с приемом платежей, должны поддерживать оплату с помощью универсального QR-кода НСПК.

Использование цифрового рубля

Преимущества Универсального QR

Множество способов оплаты в одном QR

В одном QR могут быть доступны различные способы платежа, сохраняются все привилегии от банков и СБП. Вы продолжите получать привычные кешбэки, которые предназначены вам по выбранной программе лояльности



А также!

- ViPNet SafeBoot
- ViPNet Coordinator KB
- и другие СЗИ…

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 финтеха

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного