Использование продуктов ViPNet для защиты инфраструктуры цифрового рубля в банках

Римма Бадмаева
Ведущий менеджер продуктов

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

Планируемые сроки внедрения ЦР

Срок	Финансовые посредники*	Торговые предприятия**
До 01.09.2026	Системно значимые банки (18 банков)	Клиенты системно значимых банков с годовой выручкой более 120 млн рублей
До 01.09.2027	Банки с универсальной лицензией	Клиенты с годовой выручкой более 30 млн рублей
До 01.09.2028	Остальные банки	Продавцы с годовой выручкой менее 30 млн рублей

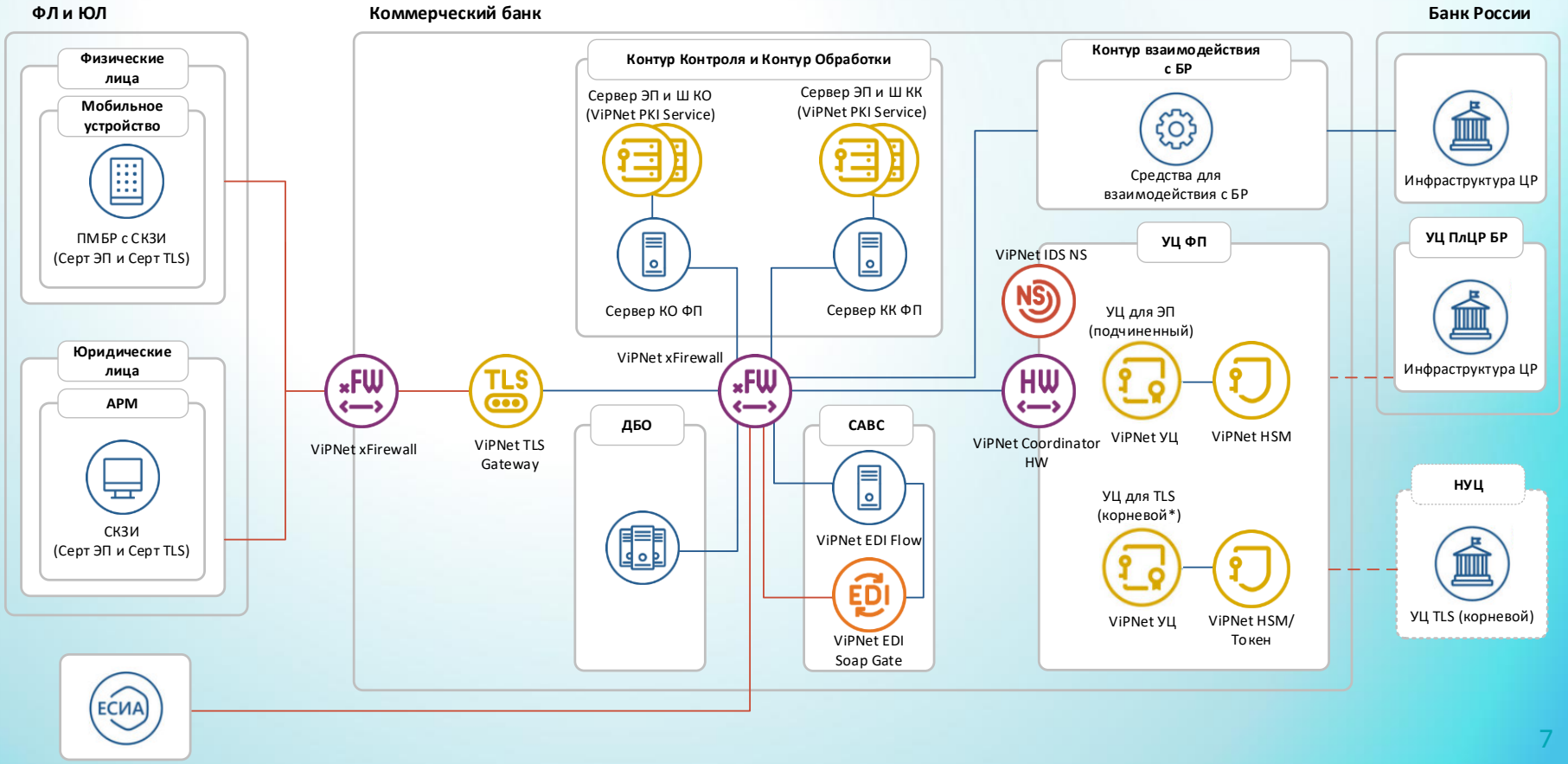
** Открытие и пополнение счета, переводы и т.п.*

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

Исключение: торговые точки, у которых выручка за год составляет менее 5 млн рублей

Продукты ViPNet для создания защищенного взаимодействия участников платформы цифрового рубля

Общая схема инфраструктуры



Программный модуль Банка России

ПМ БР разрабатывался по заданию Банка России, исключительные права принадлежат Банку России

«Надстройка» в виде API для работы СКЗИ с мобильным приложением банка, ядро – сертифицированное СКЗИ (ViPNet OSSL, ...)

Требуется оценка влияния

ViPNet OSSL

Криптобиблиотека для разработки мобильных и серверных решений

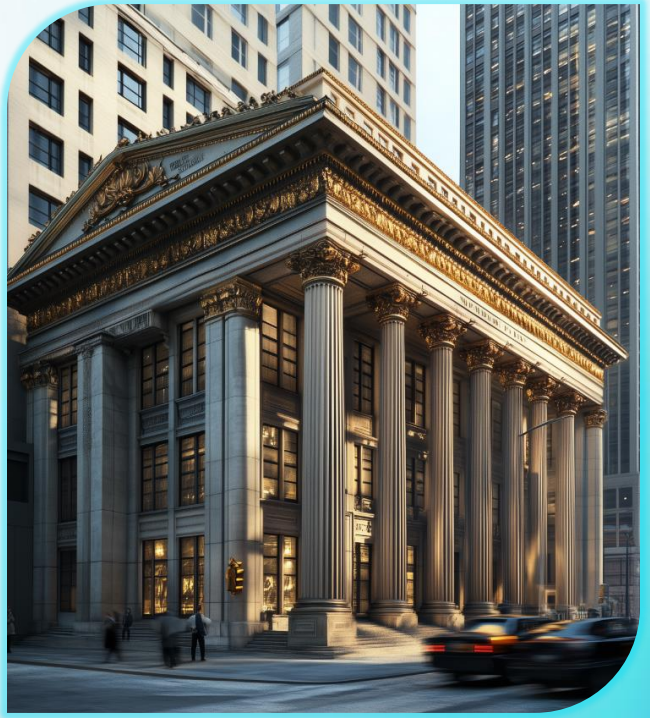
Функции для ПМБР:

- Формирование запросов на сертификат
- Организация ГОСТ TLS соединений
- Подпись/проверка подписи сообщений
- Шифрование/расшифрование сообщений

Участники ПлЦР – коммерческие банки

На стороне банка:

- TLS шлюз класса СКЗИ КС2 (п.14.2, абз 6, 833-П, **вступили в силу с 1 января 2025**)
- УНЭП с использованием средств ЭП не ниже КС3 (п.14.1, 833-П, **вступили в силу с 1 января 2025**)
- Шифрование (расшифрование) с использованием СКЗИ не ниже КС3 (п.14.1, 833-П, **вступили в силу с 1 января 2025**)



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, реестре Минпромторга и реестре ПАК Минцифры

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
- Требуется оценка влияния

Два разных УЦ

Решаемые задачи:

1. УЦ для выпуска сертификатов ЭП
2. УЦ для выпуска сертификатов безопасности (для реализации TLS ГОСТ)

О смене поколений ViPNet УЦ

Эпизод 4: ViPNet УЦ 4

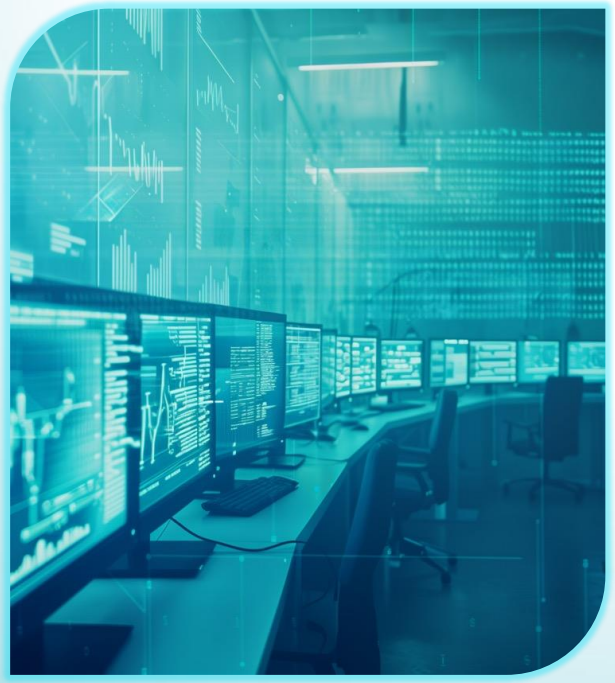
Эпизод 5: ViPNet УЦ 5

ViPNet УЦ 5

Центр сертификации ViPNet Certification Authority 5

- 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 CABC: Сервис Автоматизации Выпуска Сертификатов



ПАК ViPNet EDI Soap Gate 3

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

ПК ViPNet EDI Flow

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

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

ТехноФест infotecs

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

Дополнительные СЗИ

СЗИ и решаемые задачи:

- ViPNet IDS – СОВ и/или СОА (для УЦ)
- ViPNet xFirewall – межсетевой экран, разделение сегментов ЦР внутри инфраструктуры банка
- ViPNet Coordinator HW – защита трафика ЦР в инфраструктуре банка

Не забываем об оценке влияния!

Аккредитованная испытательная лабораторией 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

О криптографии в финтехе

Телеграм-канал Криптография в финтехе

ТЕХНО infotecs ФЕСТ

Бадмаева Римма
Ведущий менеджер продуктов

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA · NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ · GLOBAL DIGITAL SPACE · CISOCLUB · РУТОКЕН · ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АВАНГАРД · AR integ · АТБ ЭЛЕКТРОНИКА · infotecs {/-cademy} · merlion · УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС