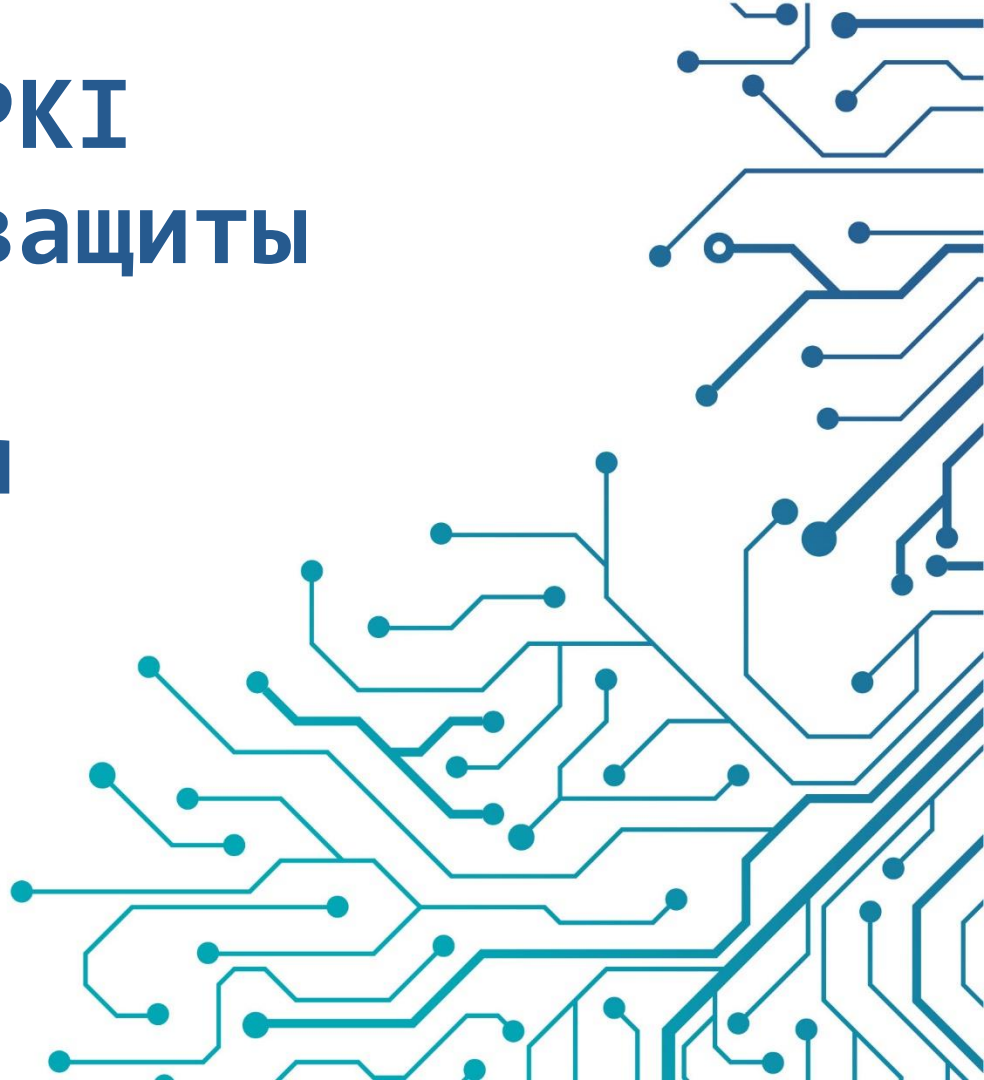


Использование РКИ продуктов для защиты инфраструктуры Цифрового рубля

Бадмаева Римма
Ведущий менеджер продуктов



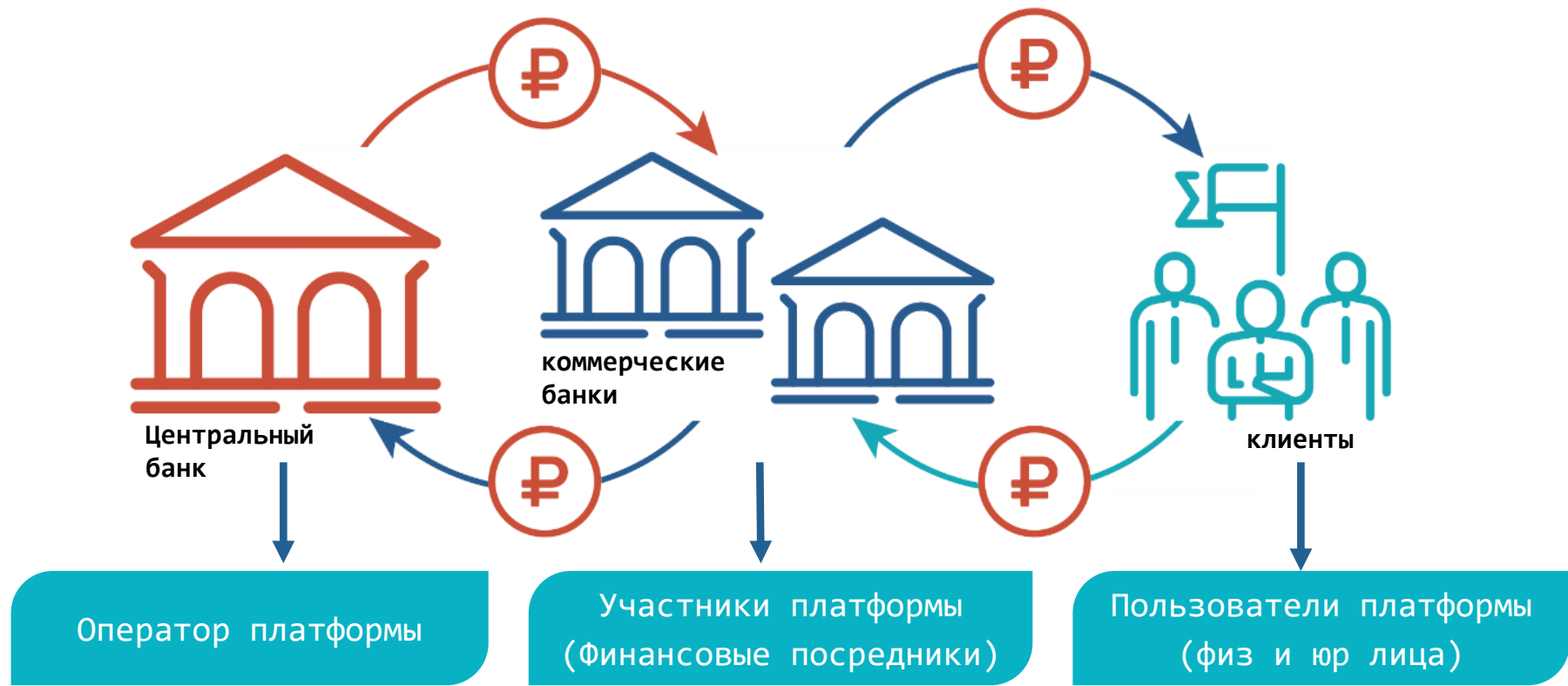
Ключевые аспекты

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

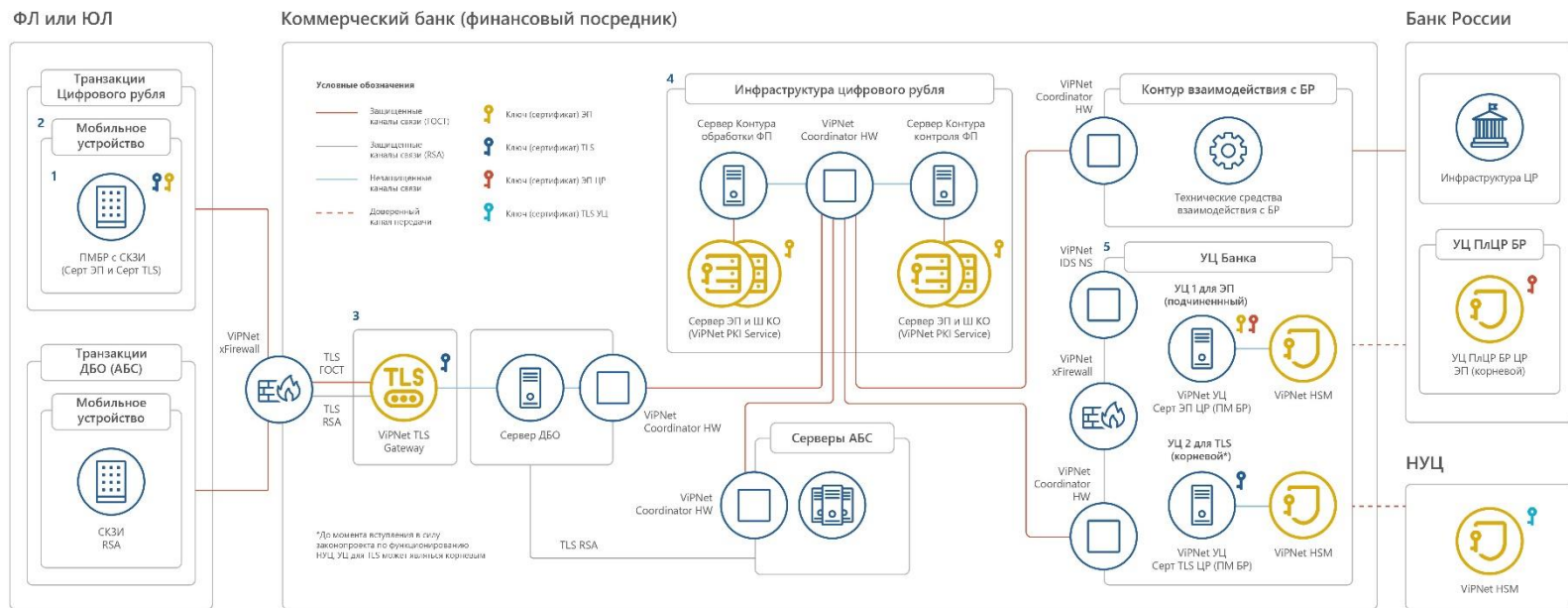


- Эмитентом цифрового рубля является Банк России
- Банк России открывает кошельки банкам и Федеральному казначейству, а также кошельки физическим и юридическим лицам по их поручению через банки
- Клиентам, банкам и Федеральному казначейству открывается только один кошелек в цифровых рублях
- На размещенные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

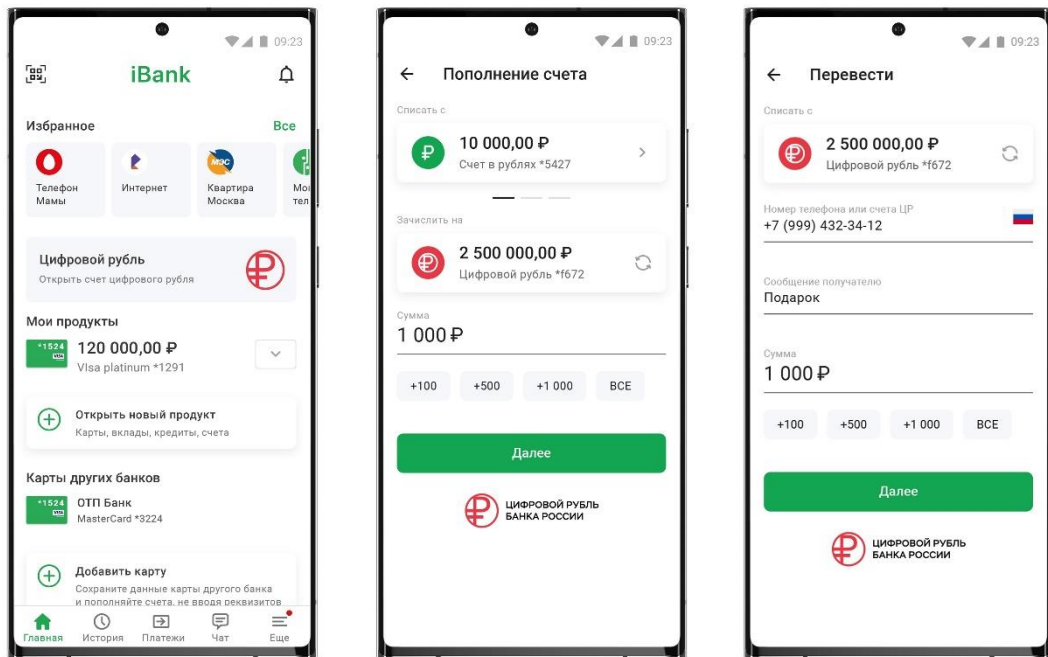
Роли сторон в платформе ЦР



Общая схема инфраструктуры ЦР с продуктами PKI



Пользователи ПлЦР



В мобильном приложении банка появится соответствующий стандарту платформы цифрового рубля интерфейс для совершения операций с цифровым рублем (открытие счета, пополнение, вывод и т.д.)

ВІFІT

Программный модуль Банка России

Основа:



Ядро - СКЗИ ГОСТ
(ViPNet OSSL, КриптоПро CSP,
Валидата CSP)



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

Функции:

- Создание запросов на сертификат
- Организация TLS-соединений
- Подпись сообщений
- Шифрование/расшифрование сообщений

ПМ БР: опыт ИнфоТеКС



ПМ БР (с ViPNet OSSL) – разработка АО «ИнфоТеКС» по заданию Банка России



ПМ БР - Исключительные права принадлежат Банку России

I Этап:

- Разработка ПМ БР с ViPNet OSSL 5.4 с функциональностью ЭП и шифрования
- Передача банкам для встраивания в МП

II Этап:

- Разработка ПМ БР с ViPNet OSSL 5.4 с функциональностью TLS
- Передача банкам для встраивания в МП

Участники ПлЦР: коммерческие банки

Требуются СКЗИ для:

1. Организации TLS ГОСТ соединений
2. Шифрования/расшифрования
3. Формирования и проверки ЭП

Участники ПлЦР – коммерческие банки

На стороне банка:

- TLS шлюз класса СКЗИ **КС2** (п.14.2, абз 6, 833-П, **вступают в силу с 1.01.2025**)
- УНЭП с использованием средств ЭП не ниже **КС3** (п.14.1, 833-П, **вступают в силу с 1.01.2025**)
- Шифрование (расшифрование) с использованием СКЗИ не ниже **КС3** (п.14.1, 833-П, **вступают в силу с 1.01.2025**)





VIPNet TLS Gateway

Шлюз безопасности
для организации
TLS-соединений



- Аутентификация клиента и сервера
- Управление доступом на основе сертификатов
- «Дуальный» режим работы: поддержка отечественных и иностранных криптоалгоритмов
- Удаленное управление
- Кластеризация
- TLS 1.2, 1.3



VipNet PKI Service

Сервер подписи,
разработанный
на базе VipNet HSM



- Централизованное выполнение криптографических операций
- REST API
- СКЗИ класса KB, средство ЭП класса KB2

Для УНЭП и TLS ГОСТ нужно 2 УЦ



Решаемые задачи:

УЦ для выпуска сертификатов ЭП

УЦ для выпуска сертификатов
безопасности (для реализации
TLS ГОСТ)



ViPNet Certification Authority



Совместная работа с ViPNet HSM

- УЦ – класса КСЗ (п. 13.4, 833-П)
- Ключ ЭП УЦ должен храниться в HSM
- Аккредитация УЦ не требуется

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

Опрос

Вы готовы стать пользователями ПЛЦР?



Спасибо за внимание!

Подписывайтесь на наши соцсети

