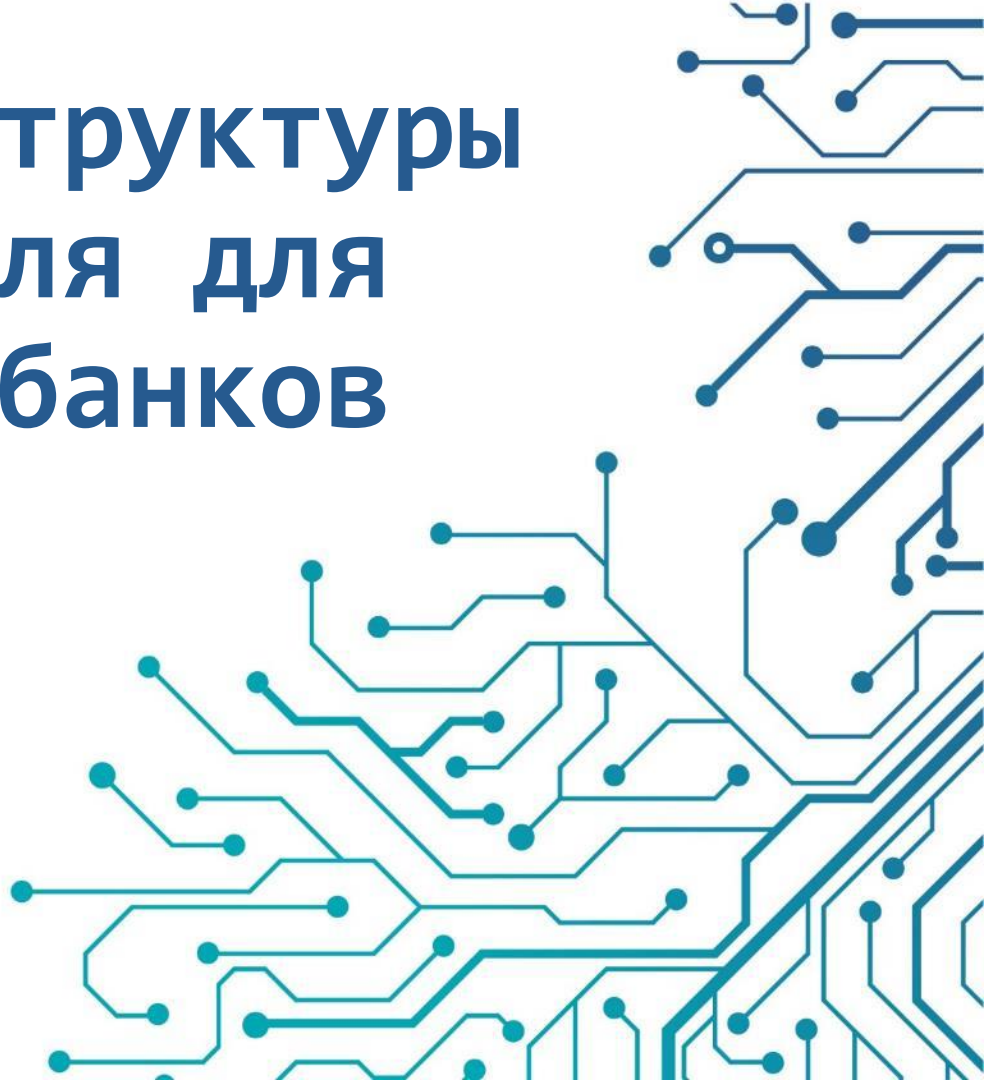


Защита инфраструктуры Цифрового Рубля для коммерческих банков ПОД «КЛЮЧ»

Римма Бадмаева
ведущий менеджер продуктов

Сергей Дурягин
вице-президент

 **infotecs**



Назначение, возможности ЦР



Формы национальной валюты:

- Наличная
- Безналичная
- Цифровая



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

Источник: официальный сайт Банка России

Нормативные документы по Цифровому Рублю



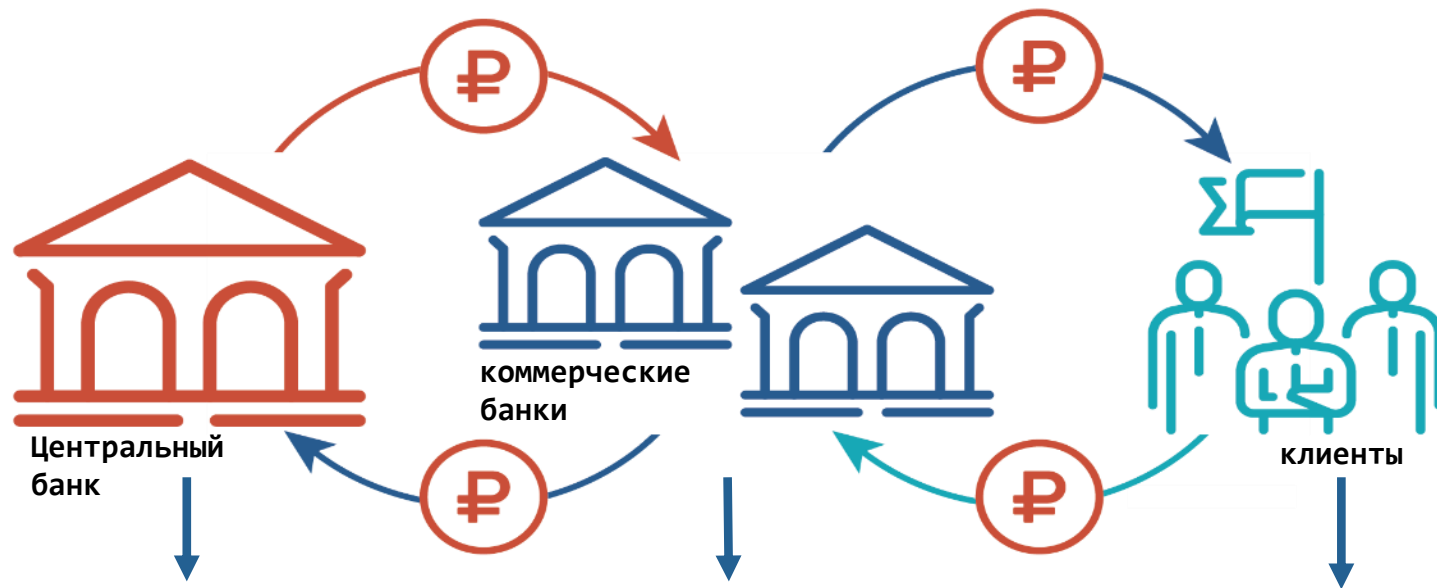
Положения Банка России:

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

Стандарты платформы цифрового рубля:

- Стандарт. Порядок подключения Финансового посредника к Платформе Цифрового Рубля. Версия 1.2
- ЦВЦБ. Требования по обеспечению информационной безопасности для Финансового посредника
- и другие, см. http://www.cbr.ru/fintech/dr/doc_dr/standarts/

Роли сторон в платформе ЦР



Оператор платформы

Участники платформы
(Финансовые посредники)

Пользователи платформы
(физ и юр лица)

Продукты ViPNet для защищенного взаимодействия участников платформы Цифрового рубля

Обозначения и термины

БР – Банк России

ЦР – цифровой рубль

ФП – финансовый посредник;

ЭС – электронное сообщение (информация о транзакции)

МП – мобильное приложение финансового посредника

ПМ БР с СКЗИ – программный модуль Банка России – СКЗИ для функций ЭП, шифрования и TLS

ДБО АБС – система дистанционного банковского обслуживания (ДБО) автоматизированной банковской системы (АБС)

КО – контур обработки

КК – контур контроля

Сервер ЭП и Ш – средство электронной подписи и шифрования

МЭ VipNet xFirewall – межсетевой экран

VipNet TLS Gateway – TLS шлюз (до класса KC3)

VipNet Coordinator HW – криптошлюз до класса KC31

VipNet Coordinator HW VA – криптошлюз до класса KC1

VipNet IDS NS – система обнаружения атак/вторжений

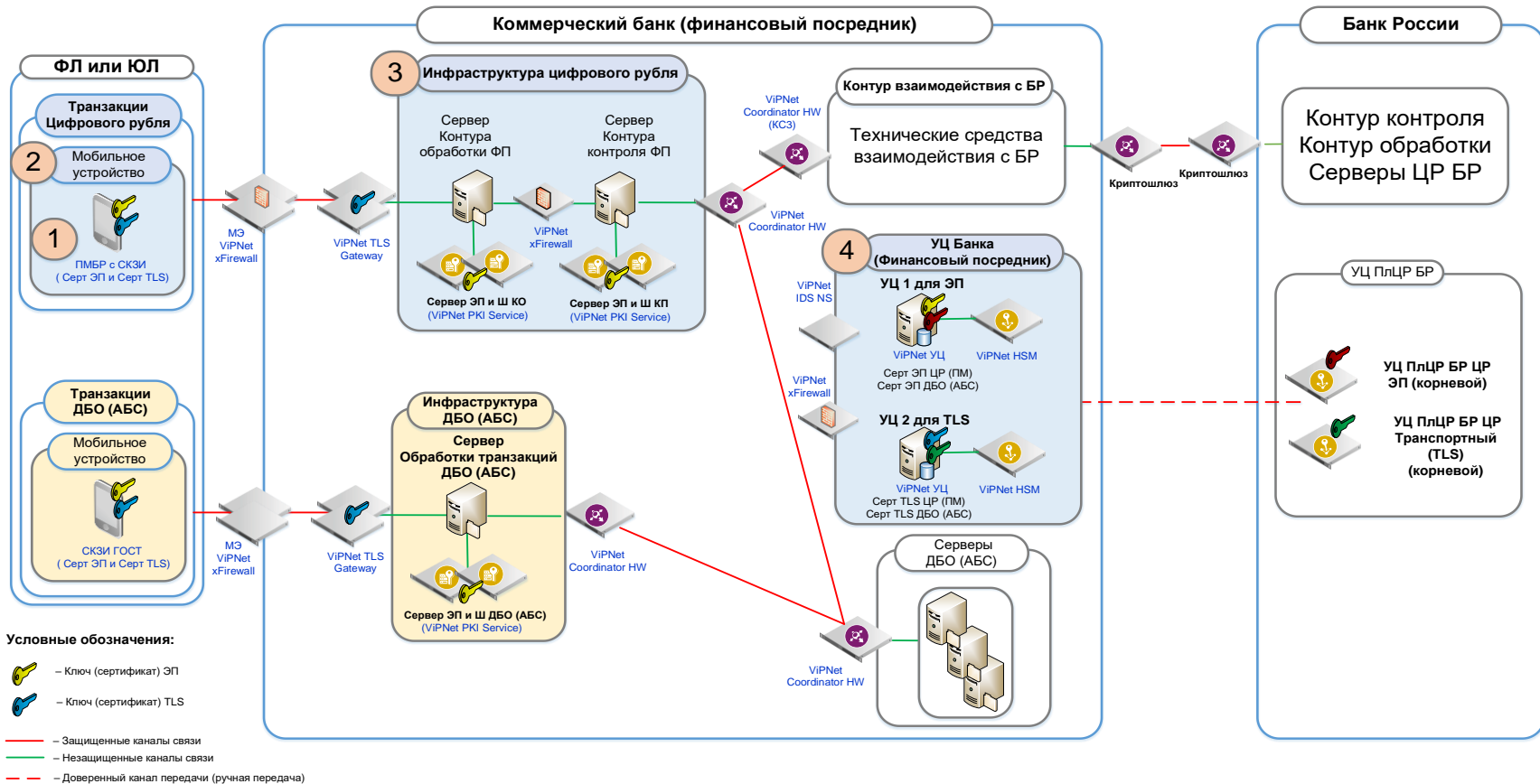
УЦ 1 ЭП – удостоверяющий центр финансового посредника для выдачи сертификатов ЭП

УЦ 2 TLS – удостоверяющий центр финансового посредника для выдачи сертификатов TLS

УЦ ПлЦР БР ЦР ЭП (корневой) – УЦ Банка России для прикладных операций с ЦР

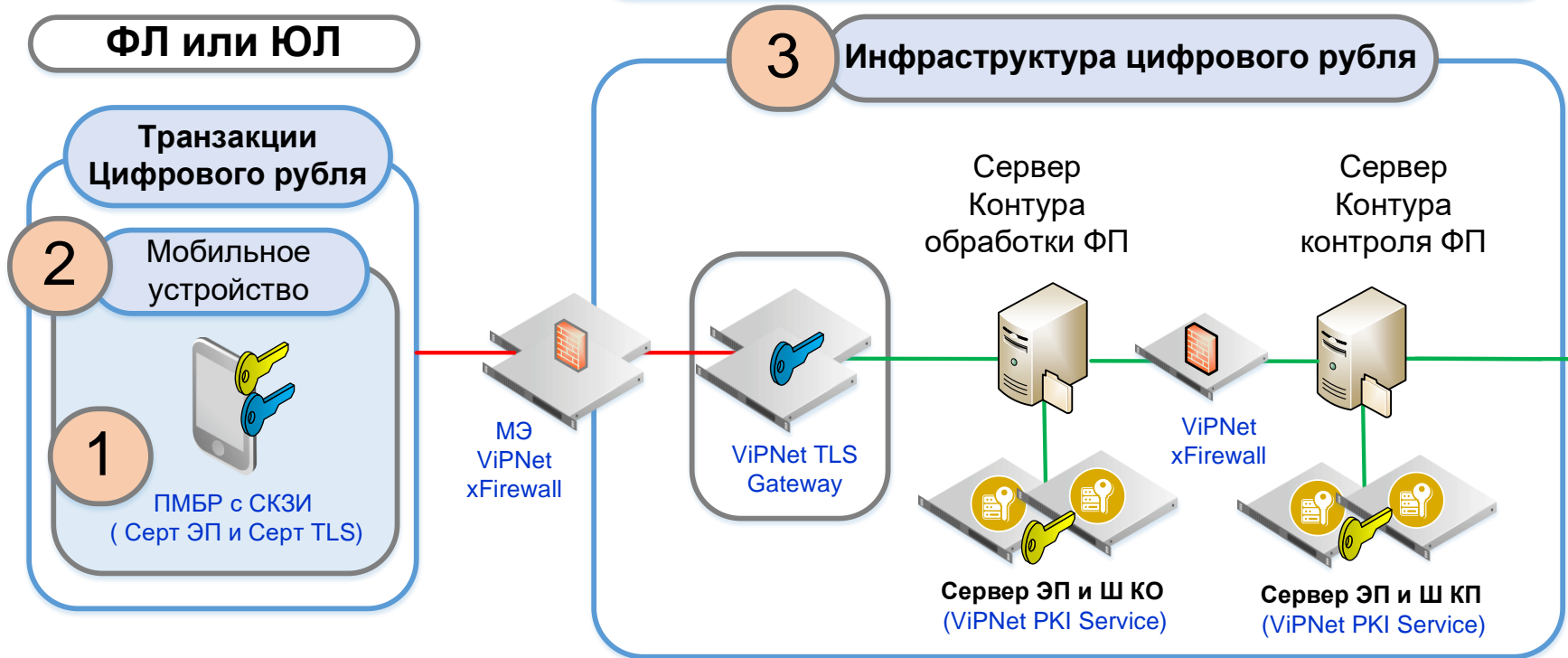
УЦ ПлЦР БР ЦР Транспортный (TLS) (корневой) – УЦ Банка России для транспортных сертификатов (TLS)

Продукты ViPNet для защищенного взаимодействия участников платформы Цифрового рубля



1. Сегмент Пользователь – Банк

Коммерческий банк (финансовый посредник)



1. ПМ БР – программный модуль Банка России



Основа:

- Ядро - СКЗИ ГОСТ (ViPNet OSSSL, КриптоПро CSP, Валидата CSP)
- «Надстройка» в виде API для работы СКЗИ с мобильным приложением банка

Функции:

- Двусторонний TLS
- Подпись сообщений (транзакций)
- Шифрование/расшифрование сообщений (транзакций)

1. ПМ БР – программный модуль Банка России



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



ПМ БР - Исключительные права принадлежат Банку России



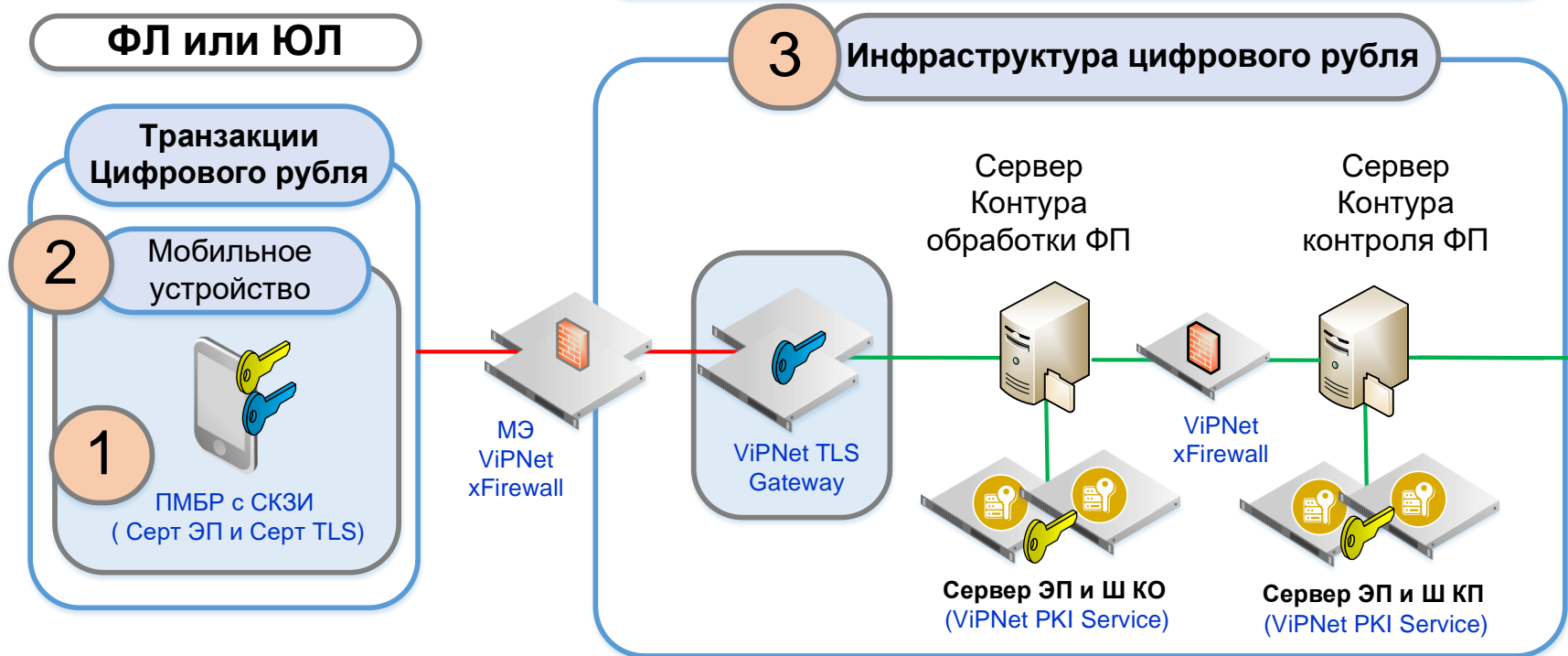
В 2023г. 9 из 13 банков выбрали ПМ БР с ViPNet OSSL

Где взять ПМ БР: обратиться в Банк России с заявкой

! Но окончательно вопрос стоимости ПМ БР для банков не решен

2-3. Сегмент Пользователь – Банк

Коммерческий банк (финансовый посредник)



2-3. Сегмент Пользователь – Банк



На стороне банка:

- Двусторонний TLS
- TLS шлюз класса **KC2** (п.14.2, абз 6, 833-П, вступают в силу с.1.01.2025)

На устройстве пользователя:

- Двусторонний TLS **KC1** (п.14.2, абз.6, 833-П, вступают в силу с.1.01.2025)
- СКЗИ класса **KC1** (п.14.2, абз.3, 833-П, вступают в силу с.1.01.2025)

2-3. Ключевые преимущества ViPNet TLS Gateway



Легитимная работа с любым СКЗИ на стороне пользователя (ViPNet, КриптоПро, Валидата)



Легитимная одновременная работа с ГОСТ-шифрованием и RSA шифрованием, т.е. возможность работы с другими банковскими приложениями по иностранным криптоалгоритмам

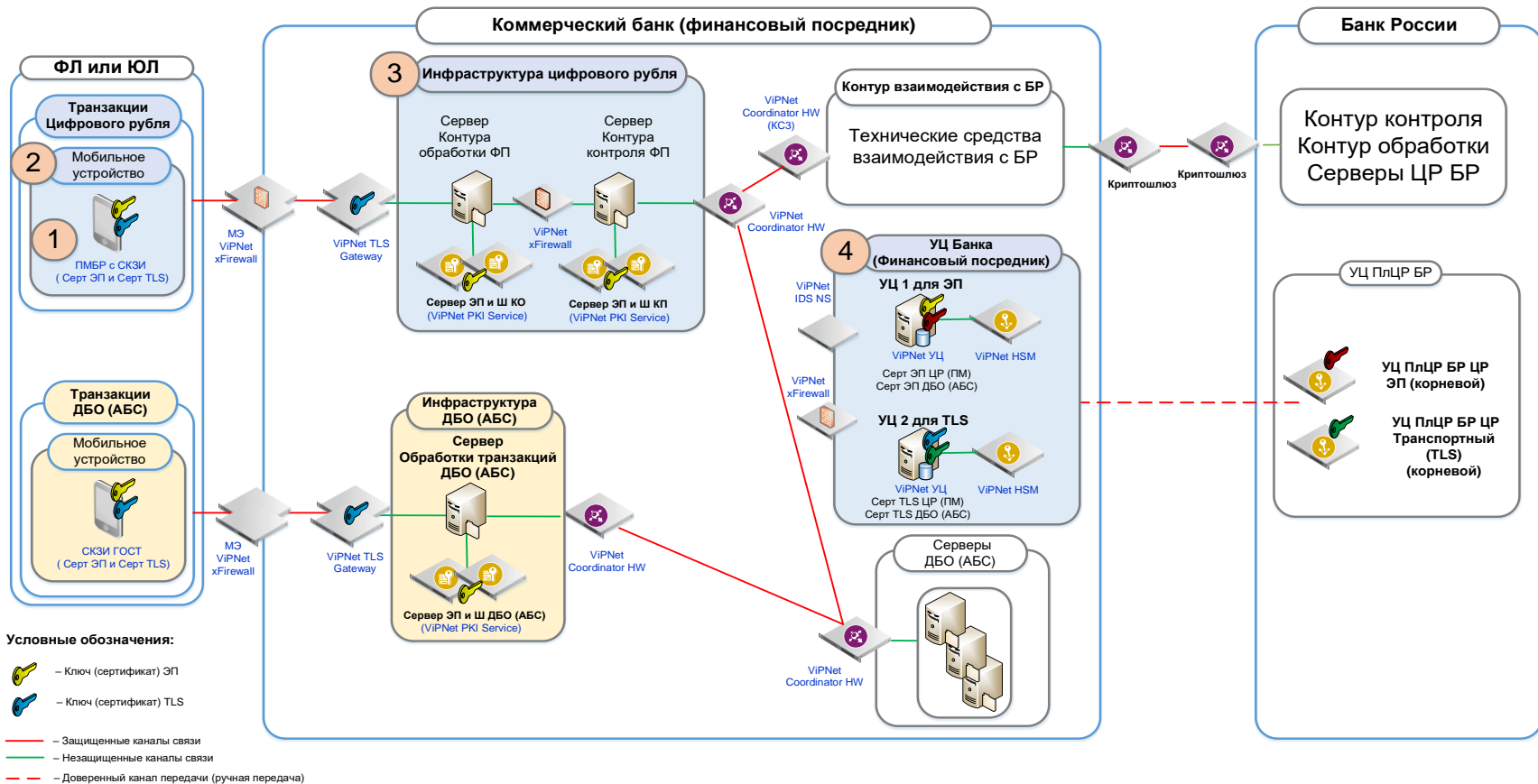


Высокая производительность по кол-ву одновременных подключений – гарантировано до 65 000



Полная линейка продуктов PKI в отличие от других вендоров

3. Контур обработки. Контур контроля



3. Контур обработки. Контур контроля

СЗИ:

- ViPNet PKI Service
- ViPNet PKI Client для АРМ Администратора

Решаемые в КО и КК задачи:

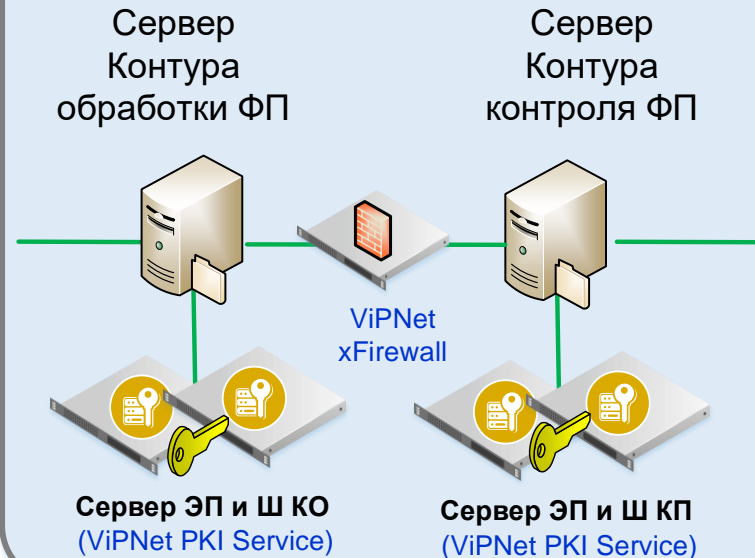
- Проверка/проставка ЭП
- Шифрование/расшифрование сообщений (транзакций)

Требования к серверу ЭП и Ш:

- УНЭП средствами ЭП не ниже КСЗ (п.14.1, 833-П, **вступают в силу с 1.01.2025**)
- СКЗИ не ниже КСЗ (п.14.1, 833-П, **вступают в силу с 1.01.2025**)

3

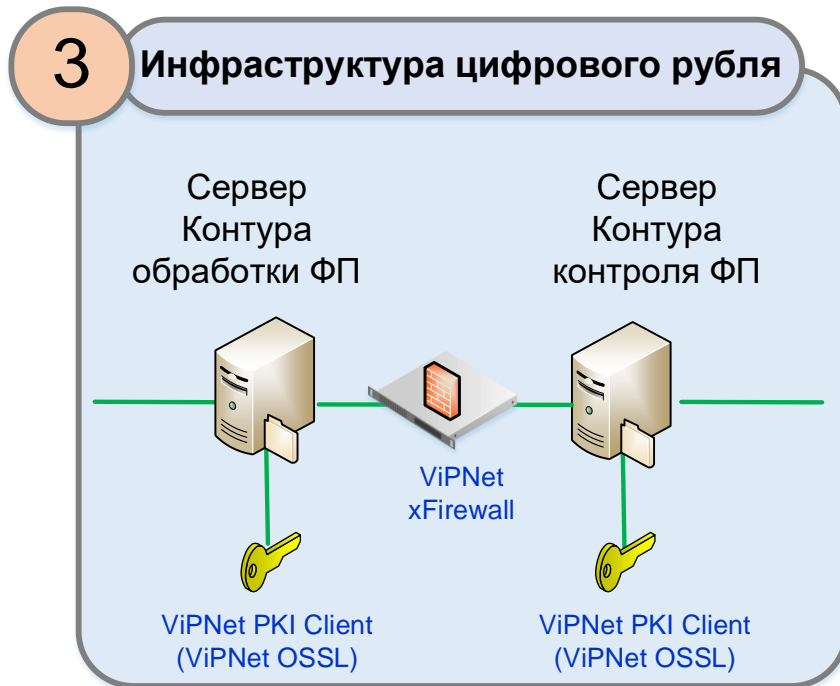
Инфраструктура цифрового рубля



3. Контур обработки. Контур контроля

Комплектация ЭкстраЭконом:

- PKI Client или OSSL вместо PKI Service



3. Контур обработки. Контур контроля

Важные Нюансы



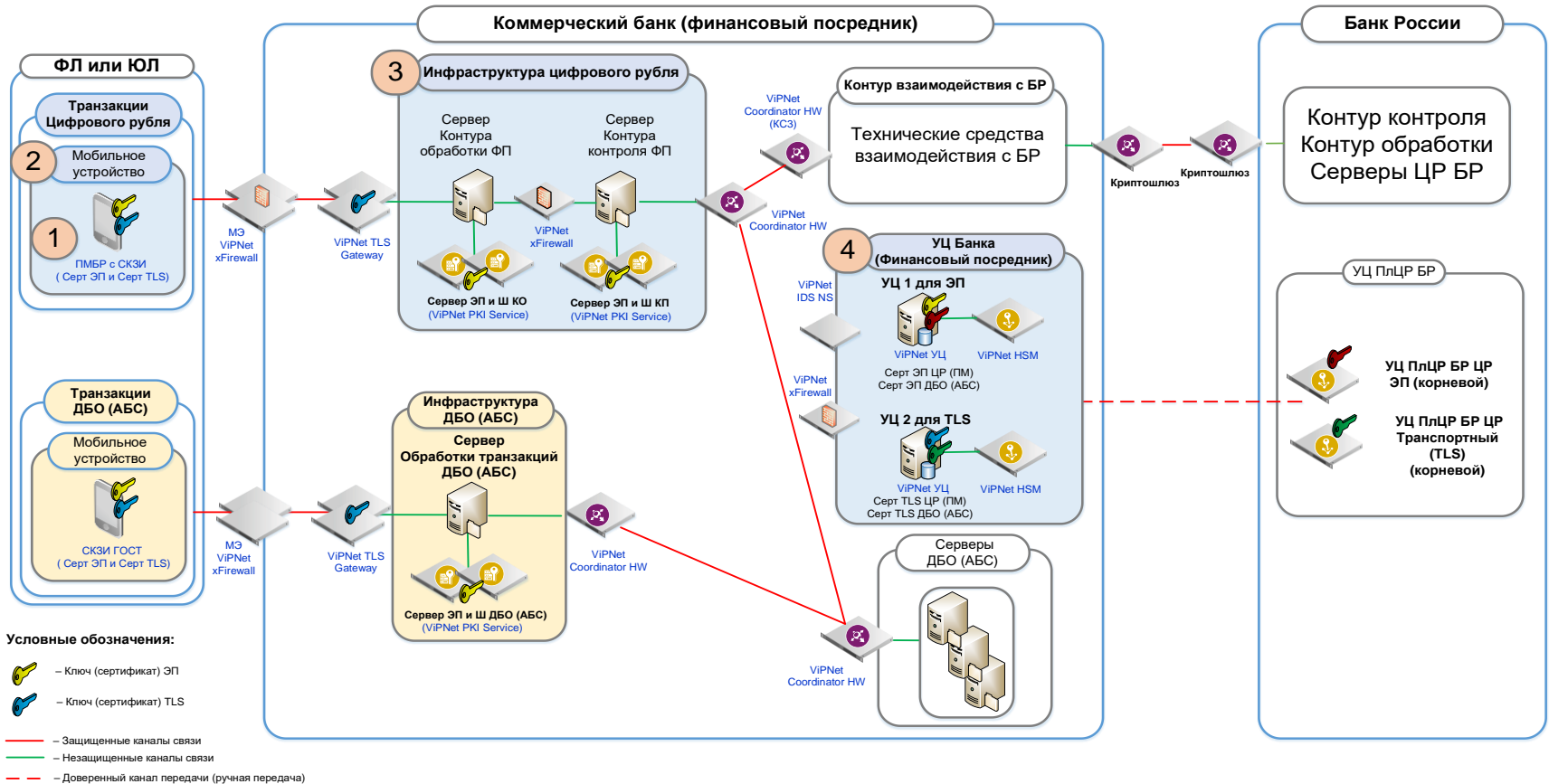
- две отдельных ЭП для контура обработки (КО) и контура контроля (КК) (п.4.1.2 порядка подключения)
- СКЗИ класса КСЗ для проверки/проставки подписи и шифрования/расшифровки сообщений (транзакций)
- используется УНЭП (не нужна аккредитация УЦ)
- требуется оценка влияния (информация, защищаемая по закону)
- рассчитать производительность серверов подписи и шифрования

3. Ключевые преимущества ViPNet PKI Service



- Высокая производительность в сравнении с конкурентами
- Высокая надежность (хранение ключей в неизвлекаемом виде)
- Легитимная возможность использования неограниченного количества сертификатов разных внешних систем (например, сертификата КО и сертификата КК на 1-ом PKI Service)
- Простота внедрения за счет наличия REST API для взаимодействия с сегментами КО и КК в отличие от сложного PKCS#11 в классическом HSM
- Существенная экономия за счет использования единой аппаратной платформы в сравнении с конкурентами, где надо использовать HSM в связке с доп приложением
- ДСДР не нужны

4. Удостоверяющие центры



4. Удостоверяющие центры

СЗИ:

УЦ класса не ниже КСЗ (п. 13.4, П-833)

Наличие HSM или токена для хранения ключа ЭП

Решаемые задачи:

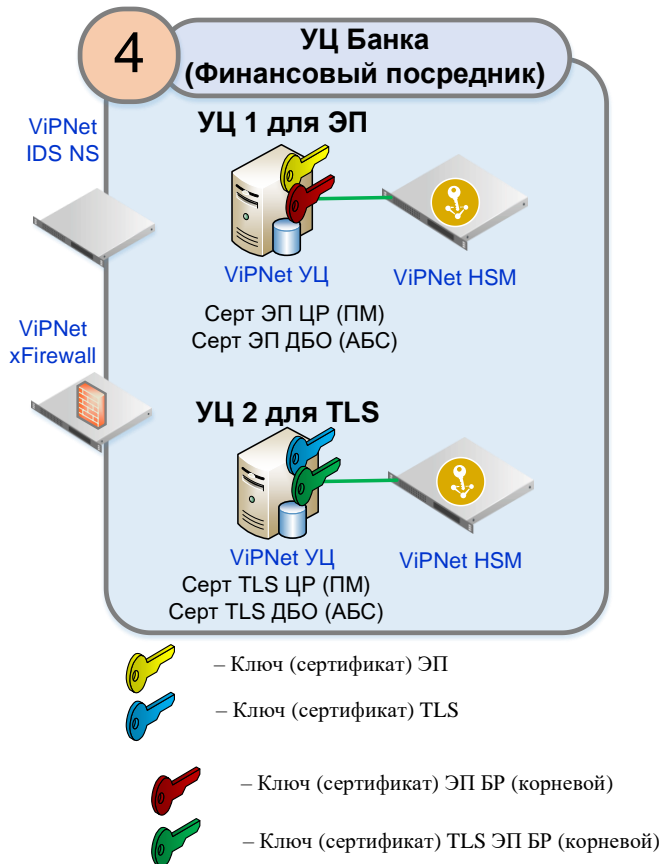
УЦ 1 - Выпуск сертификатов ЭП

УЦ 2 - Выпуск сертификатов TLS

Опционально:

IDS (COA с сертификатом ФСБ)

МЭ (класса не ниже 4 класса, ФСТЭК)



4. Удостоверяющие центры

Важные нюансы



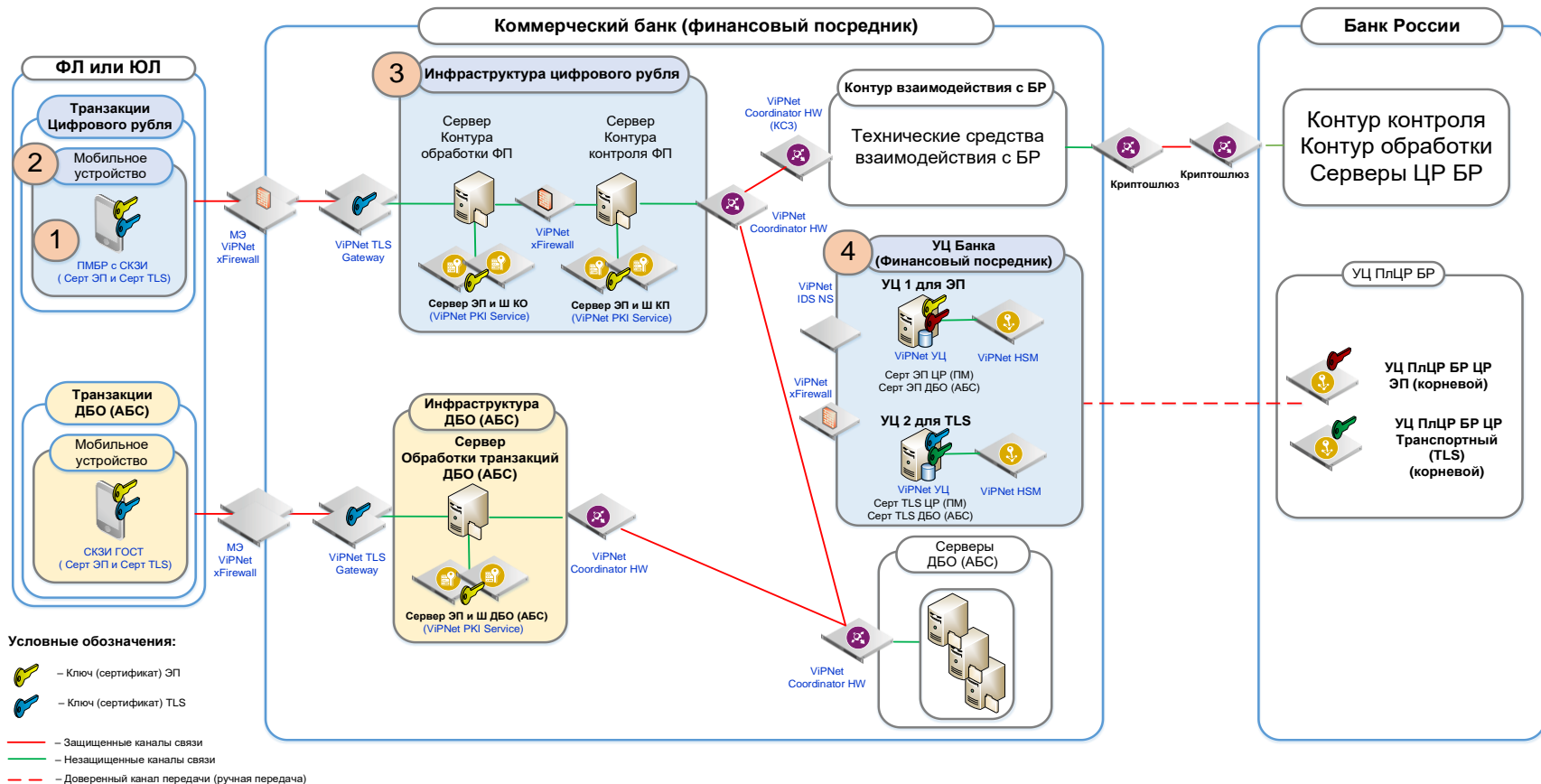
- ✓ Два отдельных УЦ для сертификатов ЭП и сертификатов TLS
- ✓ Ключ УЦ должен храниться на внешнем носителе в неизвлекаемом виде (HSM, Токен)
- ✓ Наличие API для взаимодействия с УЦ
- ✓ УЦ – класса КСЗ
- ✓ Аккредитация обоих УЦ не требуется

4. Ключевые преимущества УЦ ViPNet



- ✓ Низкая стоимость ядра УЦ
- ✓ Низкая стоимость владения УЦ, стоимость лицензии на 1 ЭП – 10 рублей
- ✓ Возможность работы с HSM и ТОКЕНОМ

5. Дополнительные СЗИ для инфраструктуры ЦР банка



5. Дополнительные СЗИ для инфраструктуры ЦР банка

СЗИ и решаемые задачи:

- ViPNet IDS – COB и/или COA (для УЦ)
- ViPNet xFirewall – межсетевой экран для разделения выделения сегментов ЦР внутри инфраструктуры банка
- ViPNet Coordinator HW – для защиты трафика ЦР в инфраструктуре банка



Coordinator HW VA

xFirewall VA



Требования к СЗИ определяются в соответствии с моделью угроз и нарушителя безопасности информации для АС банка

Работы встраиванию и оценке влияния ПМ БР в МП ФП, КО и КК

Стандарт. Порядок подключения Финансового посредника к Платформе Цифрового Рубля.

- Получить ПМ БР и выполнить **встраивание ПМ БР в Мобильное приложение ФП** в соответствии с порядком и требованиями на встраиваемый ПМ БР (П.3.4.2 Порядка подключения ФП)
- Проведение исследований по оценке влияния Мобильного приложения Финансового посредника на штатное функционирование ПМБР и СКЗИ

Требования по обеспечению информационной безопасности для Финансового посредника.

- **Требования к АС ФП** - Для реализации бизнес-процессов ЦР во внутренних АС ФП требуется проведение **оценки влияния среды функционирования СКЗИ** в соответствии с требованиями документации на используемое СКЗИ и (7) (п.3.2.3 Мероприятий ИБ к Требованиям). Заключение по результатам оценке влияния среды функционирования СКЗИ

Требования к Мобильному приложению ФП

- **Оценка влияния среды функционирования ПМ БР** на выполнение предъявленных к СКЗИ требований в соответствии с документом (п.3.2.7 Мероприятий ИБ к Требованиям)

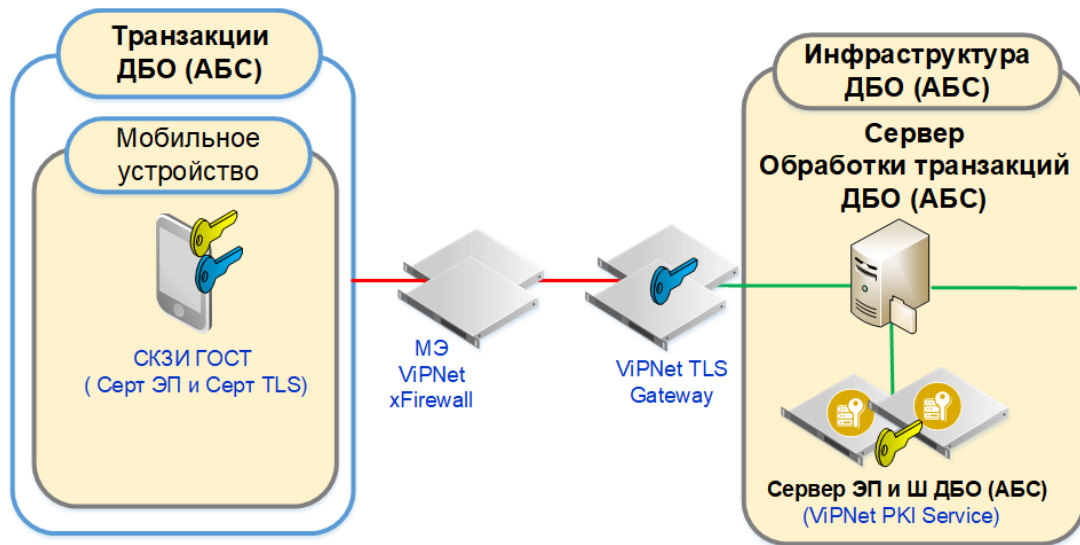
Работы встраивания и оценке влияния ПМ БР в МП ФП, КО и КК



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

И еще №1...

Работа на будущее сегодня



Использовать ГОСТ шифрование в ДБО (АБС)

№683-П от 17.04.2019 «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»

Информационное письмо ИН-017-56/22 от 16.03.2023 «О применении требований нормативных актов Банка России об обеспечении целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом»

И еще №2...

ViPNet совместим с другими производителями



УЦ другого вендора в банке может работать с:

- ПМ БР с ViPNet OSSSL
- ViPNet TLS Gateway
- ViPNet PKI Service

ПМБР с СКЗИ другого вендора в банке может работать с:

- ViPNet УЦ
- ViPNet TLS Gateway
- ViPNet PKI Service

УЦ, ПМБР, TLS GW другого вендора в банке может работать с:

- ViPNet PKI Service (*)

* Опыт общения и тестирования с несколькими банками

И еще №3...

ИнфоТеКС – надежный производитель



Строительство собственного завода ИнфоТеКС в Томске по производству квантового оборудования

ИнфоТеКС – крупнейший разработчик СКЗИ в РФ:

- 33 года опыта разработки СЗИ
- более 1800 сотрудников
- 11 филиалов

Оценка банков пилотного проекта 2023 г.:

- **высокое качество документации** по ПМ БР с СКЗИ VipNet
- **оперативная обратная связь** по вопросам встраивания/эксплуатации, в т.ч. по телеграмм



Дурягин Сергей

DSA@infotecs.ru

+7(964)589-46-86

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363