Защита инфраструктуры Цифрового Рубля для коммерческих банков «под ключ»

Бадмаева Римма
Ведущий менеджер продуктов

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

Нормативные документы 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

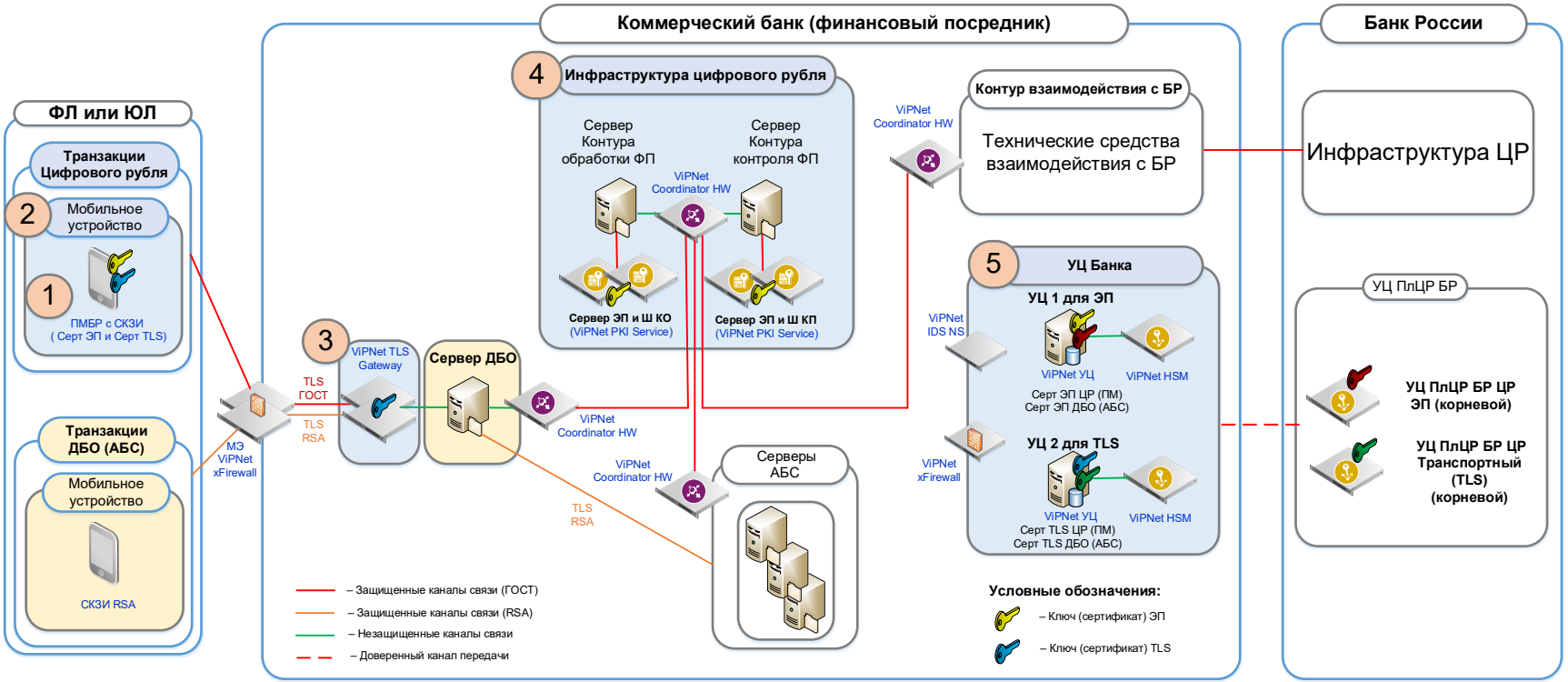
Стандарты платформы цифрового рубля:

- 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/

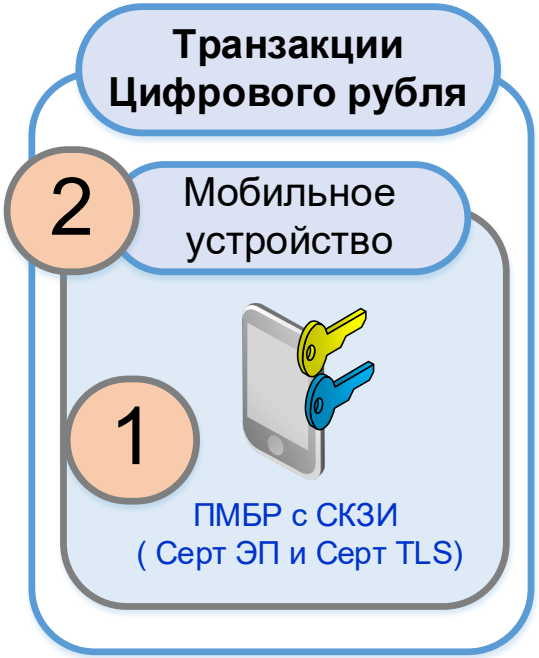
Роли сторон в платформе ЦР

Оператор платформы	Участники платформы (финансовые посредники)	Пользователи платформы (физ. и юр. лица)

ViPNet для защиты платформы Цифрового рубля



1-2.ПМ БР – 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:

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

1-2.ПМ БР – программный модуль Банка России

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

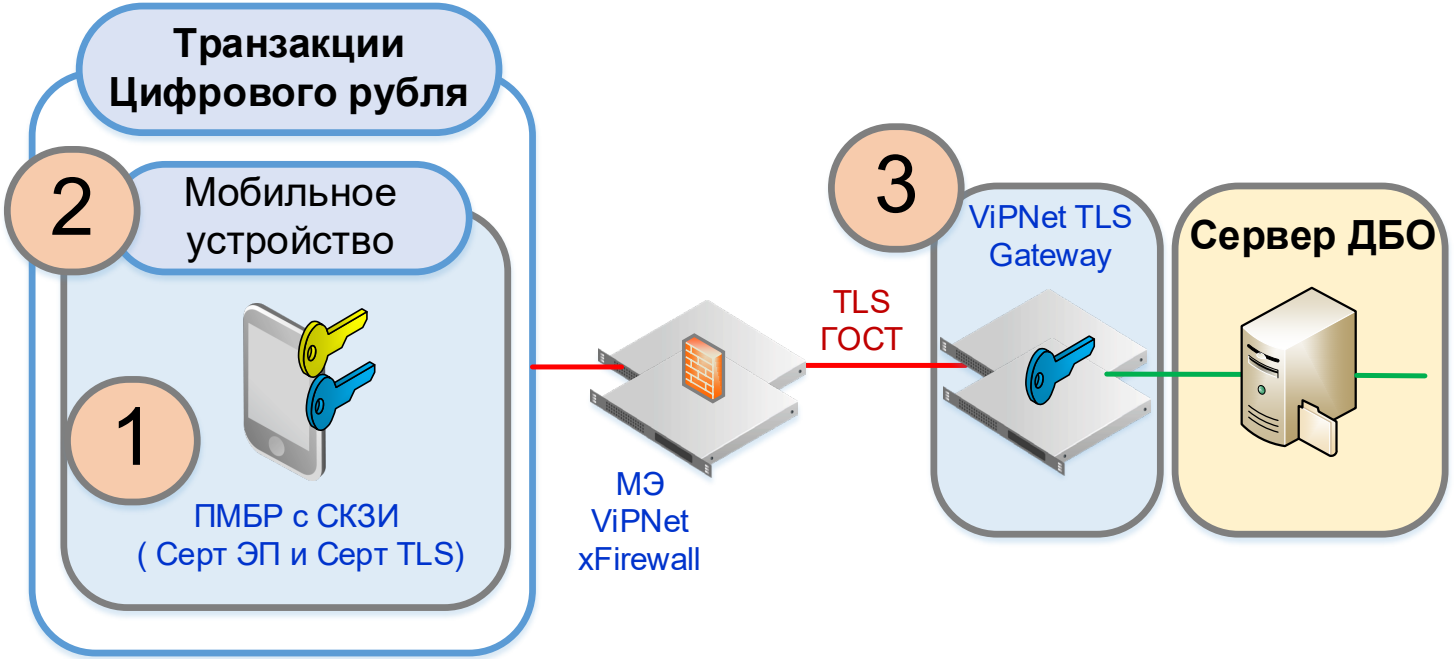
ПМ БР - исключительные права принадлежат Банку России

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

Где взять ПМ БР: обратиться в Банк России

! Но окончательно вопрос стоимости ПМ БР для банков не решен

1-2-3.Сегмент Пользователь – Банк



1-2-3.Сегмент Пользователь – Банк

На стороне банка:

- Двусторонний TLS
- TLS шлюз класса КС2 (п.14.2, абз 6, 833-П, вступают в силу с 1.01.2025)

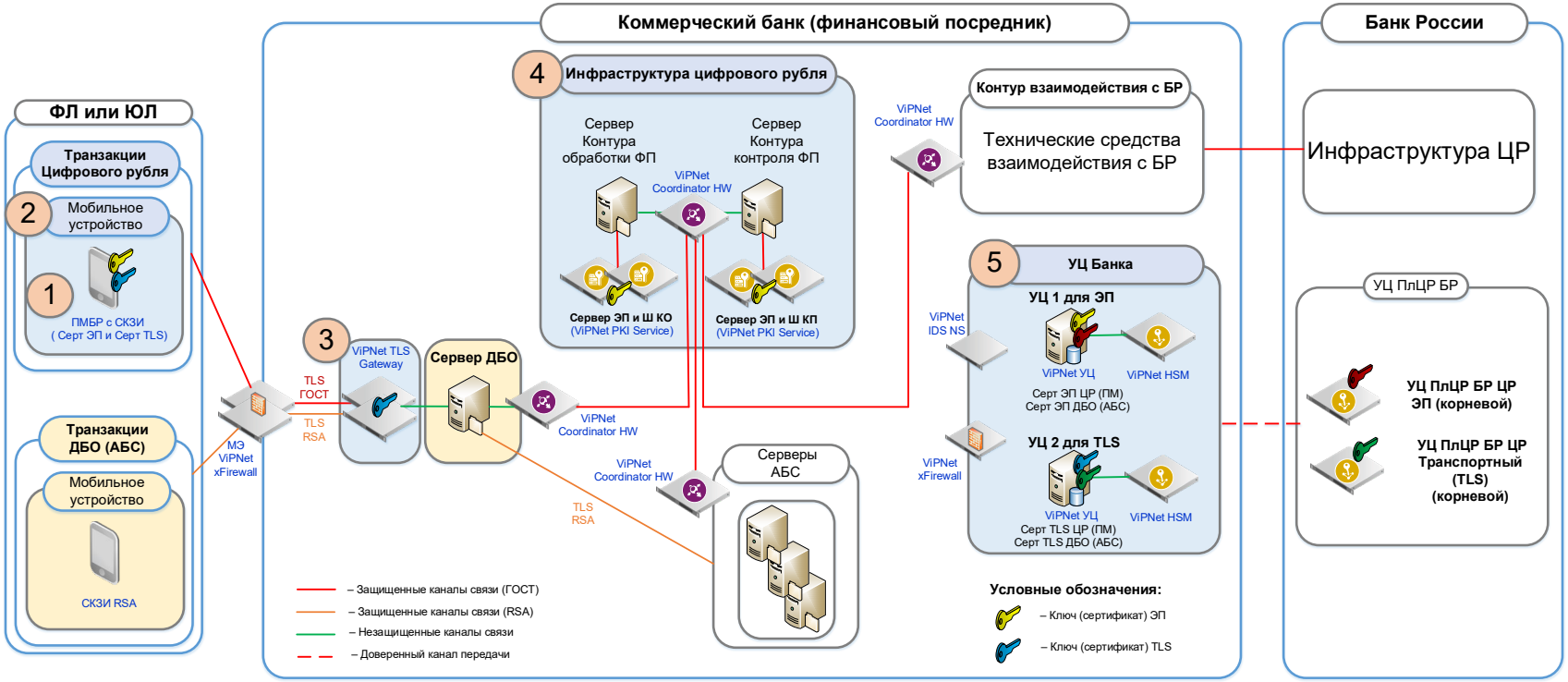
На устройстве пользователя:

- Двусторонний TLS КС1 (п.14.2, абз.6, 833-П, вступают в силу с 1.01.2025)
- СКЗИ класса КС1 (п.14.2, абз.3, 833-П, вступают в силу с 1.01.2025)

1-2-3.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

4.Контур обработки. Контур контроля

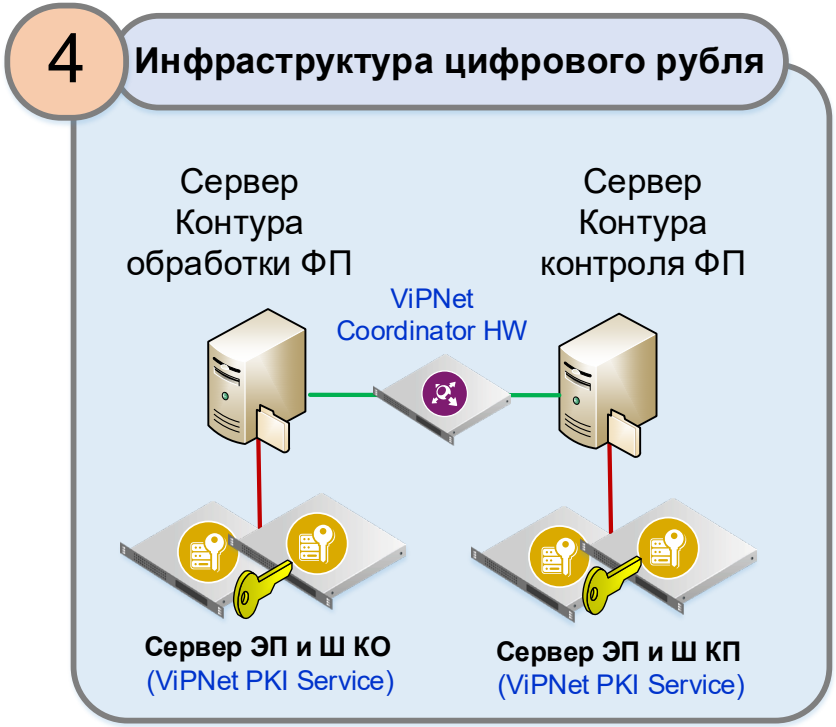


4.Контур обработки. Контур контроля

СЗИ:
- ViPNet PKI Service
- ViPNet PKI Client для АРМ Администратора

Решаемые в КО и КК задачи:
- Проверка/простановка ЭП
- Шифрование/расшифрование сообщений (транзакций)

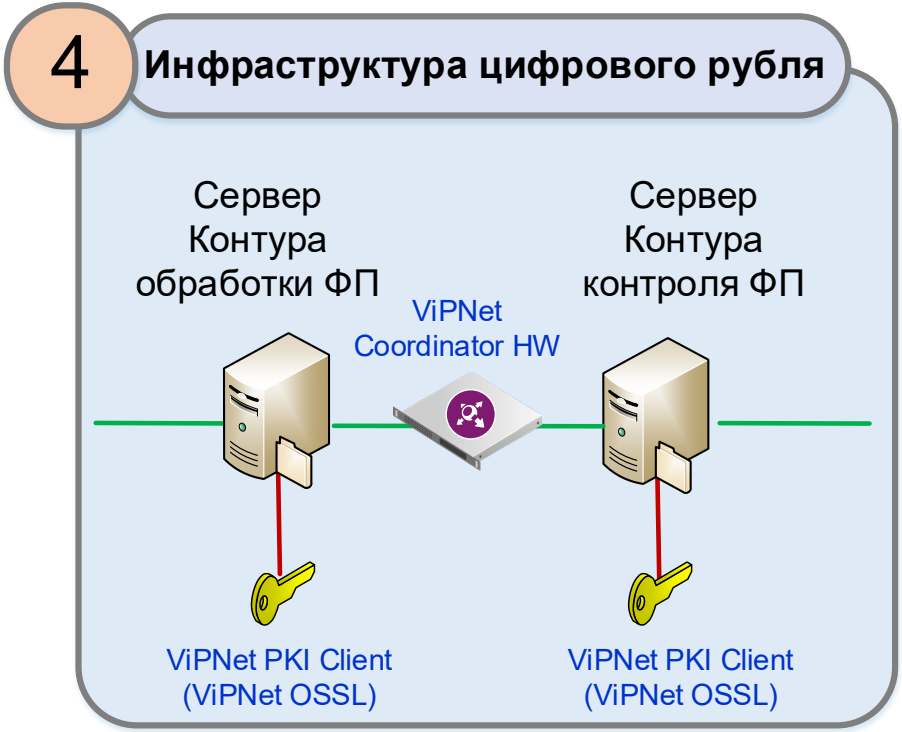
Требования к серверу ЭП и Ш:
- УНЭП средствами ЭП не ниже КС3 (п.14.1, 833-П, вступают в силу с 1.01.2025)
- СКЗИ не ниже КС3 (п.14.1, 833-П, вступают в силу с 1.01.2025)



4.Контур обработки. Контур контроля

Комплектация ЭкстраЭконом (вместо ПАК PKI Service):

- ПО ViPNet OSSL
- ПО ViPNet PKI Client



4.Контур обработки. Контур контроля

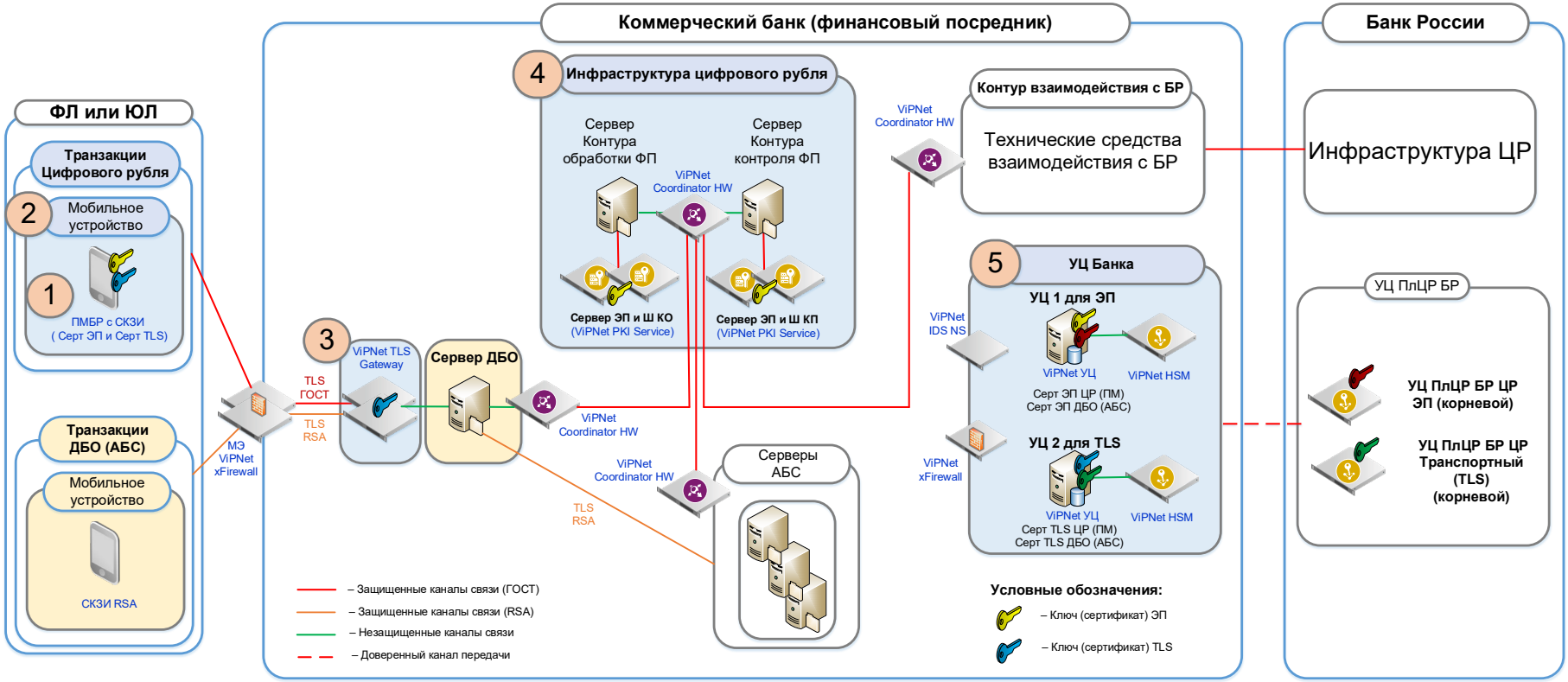
Важные нюансы

- две отдельных ЭП для контура обработки (КО) и контура контроля (КК) (п.4.1.2 порядка подключения)
- СКЗИ класса КС3 для проверки/простановки 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

4.Ключевые преимущества ViPNet PKI Service

- Высокая производительность в сравнении с конкурентами
- Высокая надежность (хранение ключей в неизвлекаемом виде)
- Легитимная возможность использования неограниченного кол-ва 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

5.Удостоверяющие центры



5.Удостоверяющие центры

СЗИ:

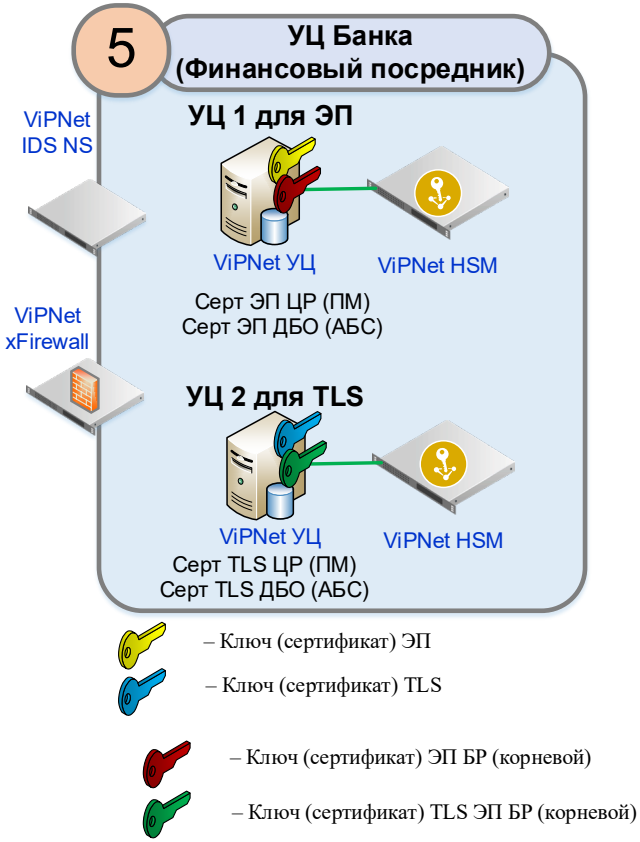
УЦ класса не ниже КС3 (п. 13.4, П-833)
Наличие HSM или токена для хранения ключа ЭП

Решаемые задачи:

УЦ 1 - Выпуск сертификатов ЭП
УЦ 2 – Выпуск сертификатов TLS

Опционально:

IDS (СОА с сертификатом ФСБ)
МЭ (класса не ниже 4 класса, ФСТЭК)



5.Удостоверяющие центры

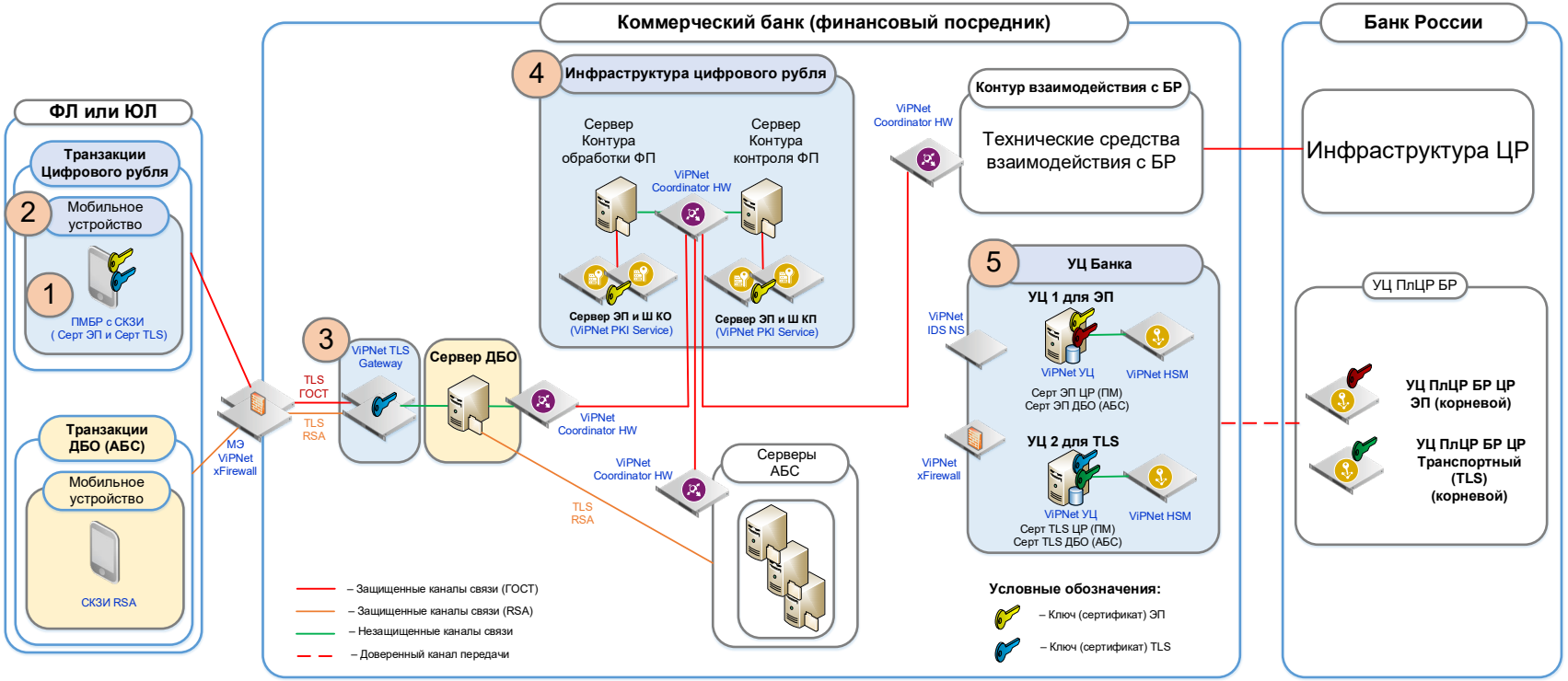
Важные нюансы

- Два отдельных УЦ для сертификатов ЭП и сертификатов TLS
- Ключ УЦ должен хранится на внешнем носителе в неизвлекаемом виде (HSM, Токен)
- Наличие API для взаимодействия с УЦ
- УЦ – класса КС3
- Аккредитация обоих УЦ не требуется

5. 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

6.Дополнительные СЗИ



6.Дополнительные СЗИ для инфраструктуры ЦР банка

СЗИ и решаемые задачи:

- ViPNet IDS – СОВ и/или СОА (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

ТЕХНО 2024 infotecs Фест

Бадмаева Римма

Ведущий менеджер продуктов

Подписывайтесь на наши соцсети