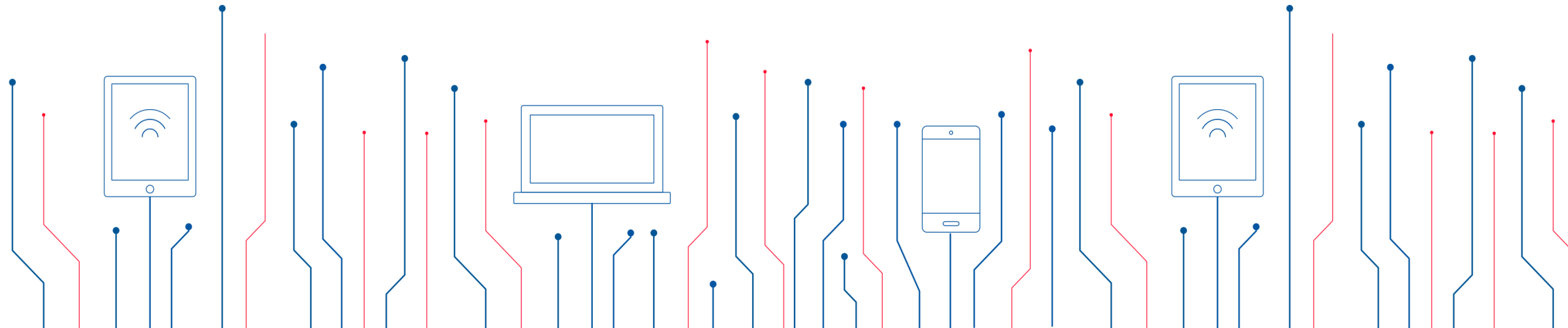
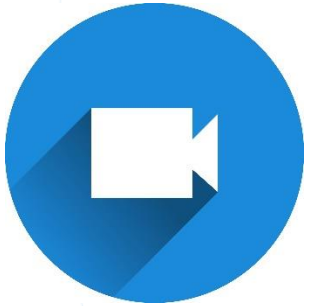
КРИПТОПРО | Ключевое слово в защите информации

Платформа цифрового рубля

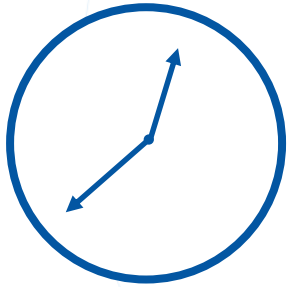
Павел Луцик, директор по развитию бизнеса и работе с партнерами
Дмитрий Багин, начальник лаборатории



Организационная информация



Запись вебинара ведется



Длительность вебинара 1-1,5 ч.

Вопросы задаем на вкладке «Вопросы»

Подарки за самые интересные вопросы

План

- Текущий статус проекта Цифрового рубля (ЦР)
- Нормативное регулирование
- Схема взаимодействия участников платформы ЦР
- Применение продуктов КриптоПро для реализации требований
- Детали выполнения требований ИБ
- Необходимость и порядок проведения исследований по оценке влияния
- Автоматизация выпуска сертификатов

Опрос 1

Что это такое?

Цифровой рубль - это новая форма национальной валюты, равнозначная наличным и безналичным рублям.

- Деньги хранятся в едином кошельке на платформе Банка России

Этапы реализации проекта Цифрового рубля

- **Декабрь 2021 г.** — создание прототипа платформы ЦР
- **2022 г.** — тестирование прототипа, разработка дорожной карты по внедрению
- **2022 г.** — разработка законодательства для внедрения ЦР
- **Август 2023 г.** — старт пилотирования операций с реальными ЦР с привлечением узкого круга клиентов нескольких банков

Банки-участники пилота

1. АО «АЛЬФА-БАНК»
2. АО «Банк ДОМ.РФ»
3. АО Ингосстрах Банк
4. Банк ВТБ (ПАО)
5. Банк ГПБ (АО)
6. ПАО «АК БАРС» БАНК
7. ПАО «МТС-Банк»
8. ПАО «Промсвязьбанк»
9. ПАО «Совкомбанк»
10. АО Банк Синара
11. ПАО РОСБАНК
12. ТКБ БАНК ПАО

Банки, планирующие присоединиться к пилоту

1. АО «АБ «РОССИЯ»
2. АО «БАНК ОРЕНБУРГ»
3. АО «Банк Русский Стандарт»
4. АО «МСП Банк»
5. АО «ПЕРВОУРАЛЬСКБАНК»
6. АО «Россельхозбанк»
7. АО «Тинькофф Банк»
8. АО «Экспобанк»
9. АО АКБ «НОВИКОМБАНК»
10. Банк «ВБРР» (АО)
11. КБ «Кубань Кредит» ООО
12. ООО «Банк Точка»
13. ООО «Примтеркомбанк»
14. ПАО «РосДорБанк»
15. ПАО «Сбербанк России»
16. ПАО АКБ «Металлинвестбанк»
17. ПАО КБ «Центр-инвест»
18. Прио-Внешторгбанк (ПАО)
19. РНКБ Банк (ПАО)
20. РНКО «ВК Платежные решения» (ООО)
21. АО КБ «Хлынов»

Нормативные документы

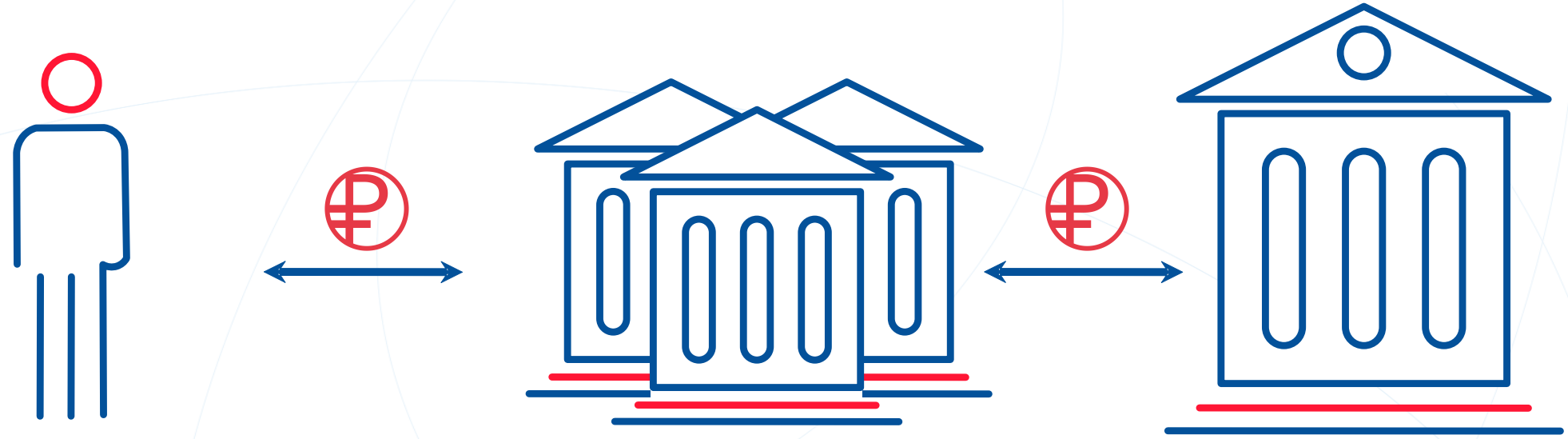
Положения Банка России

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

Документы, выдаваемые Банком России по запросу

- «Временные требования по обеспечению информационной безопасности для автоматизации выпуска сертификатов пользователя платформы цифрового рубля»
- «Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирования программного модуля Банка России, на выполнение предъявленных к входящему в его состав СКЗИ требований»

Участники взаимодействия Платформы ЦР (ПлЦР)



Пользователь ПлЦр

Клиент платформы

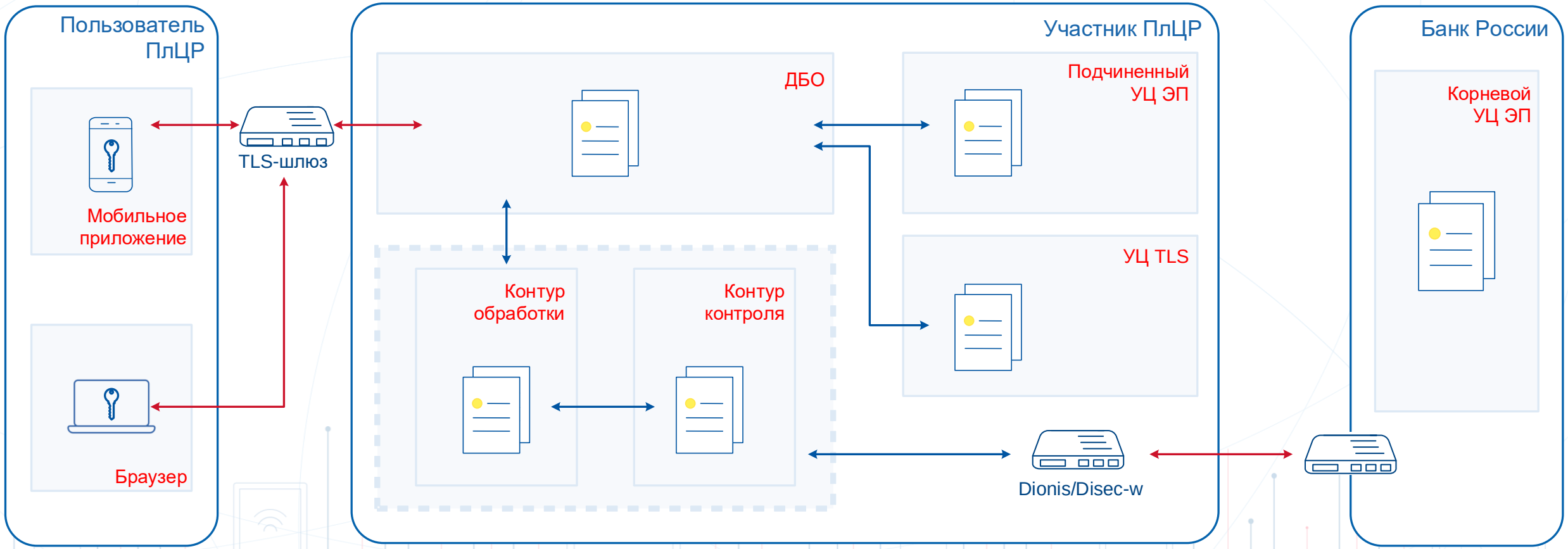
Участник ПлЦр

Коммерческий банк

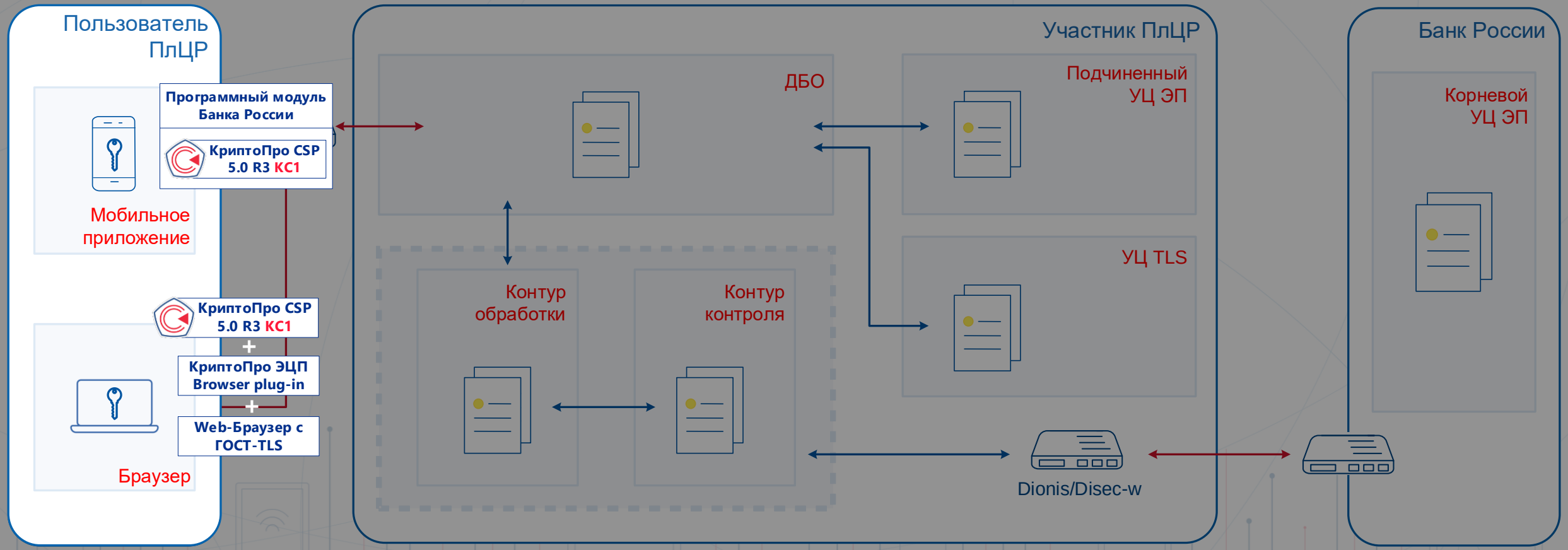
Оператор ПлЦр

Центральный Банк РФ

Общая схема взаимодействия



Пользователь



Пользователь

КриптоПро CSP 5.0

R3 KC1

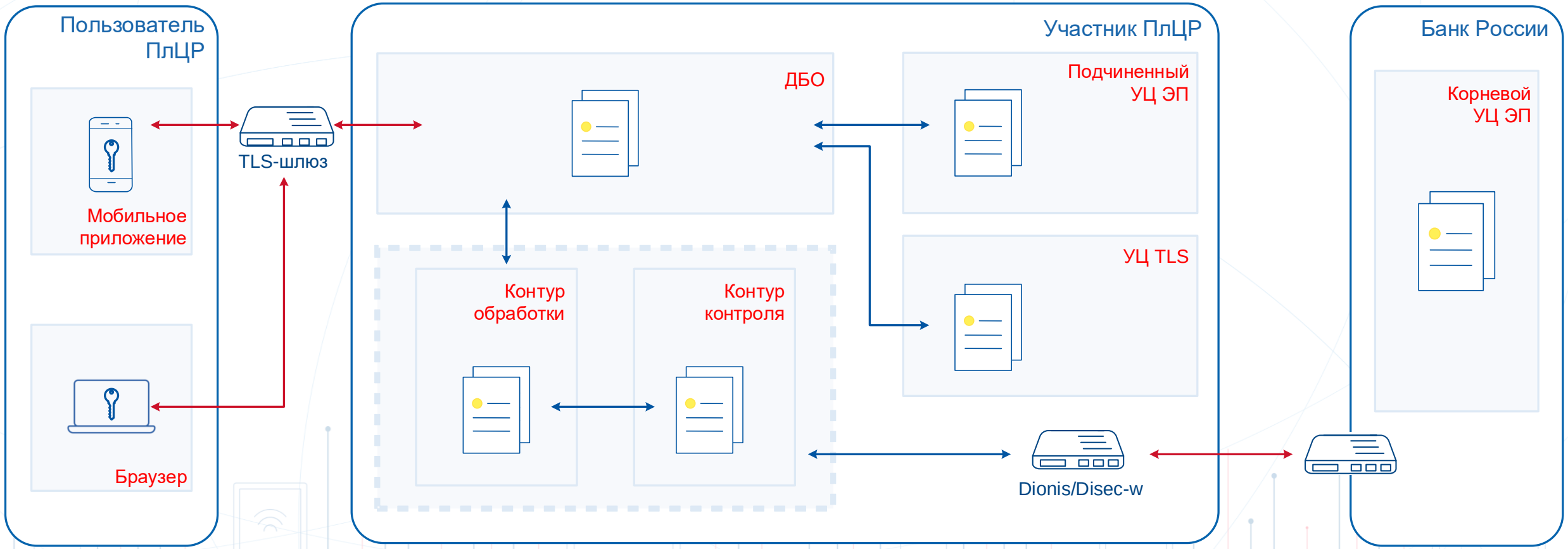
- Создание/проверка ЭП ЭС и транзакций
- Шифрование/расшифрование ЭС и транзакций
- Обеспечение двустороннего ГОСТ-TLS соединения

КриптоПро ЭЦП

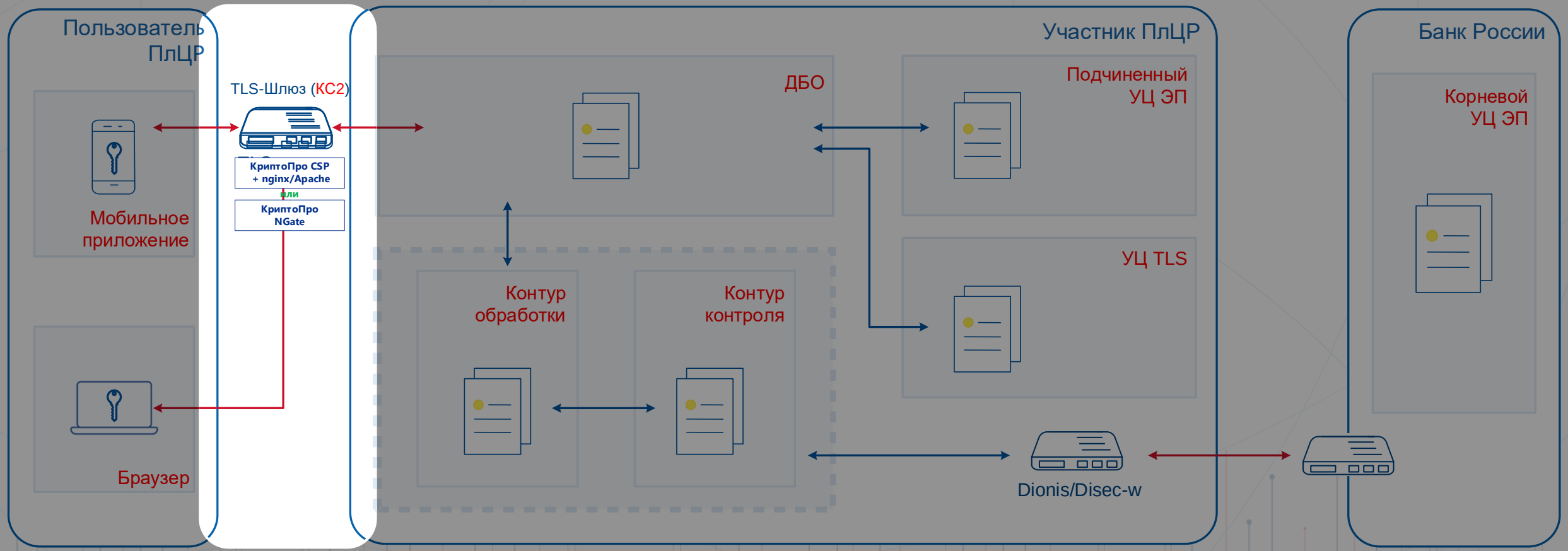
Browser plug-in

- Для встраивания в web-браузер

Общая схема взаимодействия



Пользователь - Участник



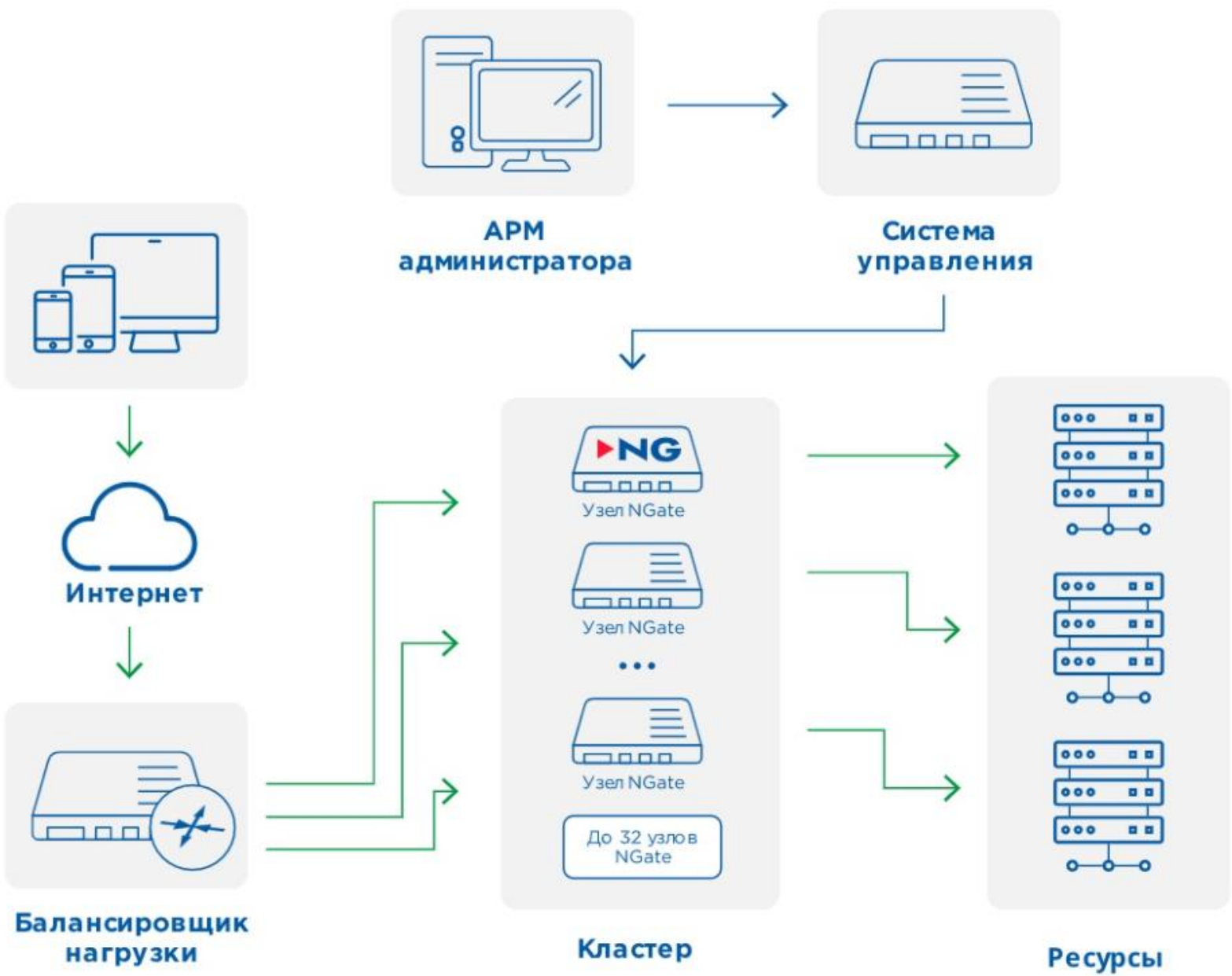
Пользователь - Участник

КриптоПро NGate

TLS-шлюз на стороне Участника ПлЦР

Архитектура NGate (все в одном)

Архитектура NGate (в кластере)



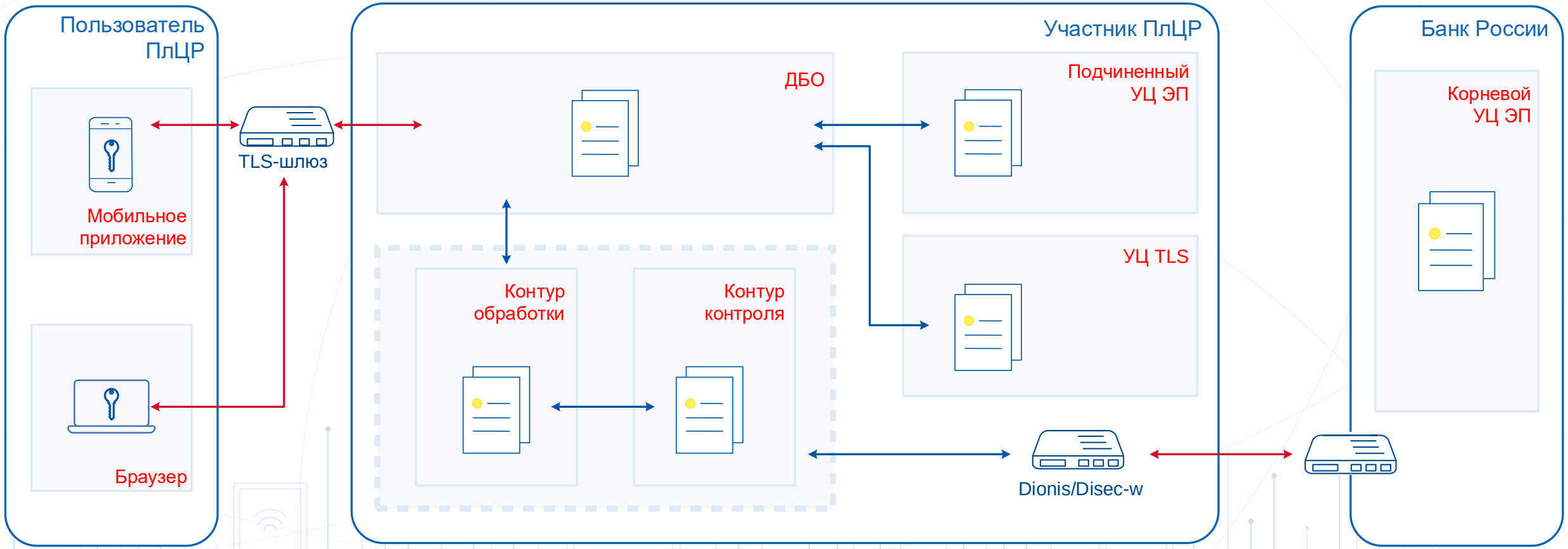
Четыре типа доступа

- VPN-сервер удаленного доступа (Point-to-Site TLS VPN)
- VPN-сервер доступа между площадками (Site-to-Site IPsec VPN)
- TLS-сервер доступа к веб-сайтам (WEB TLS)
- Сервер портального доступа (WEB Portal TLS)

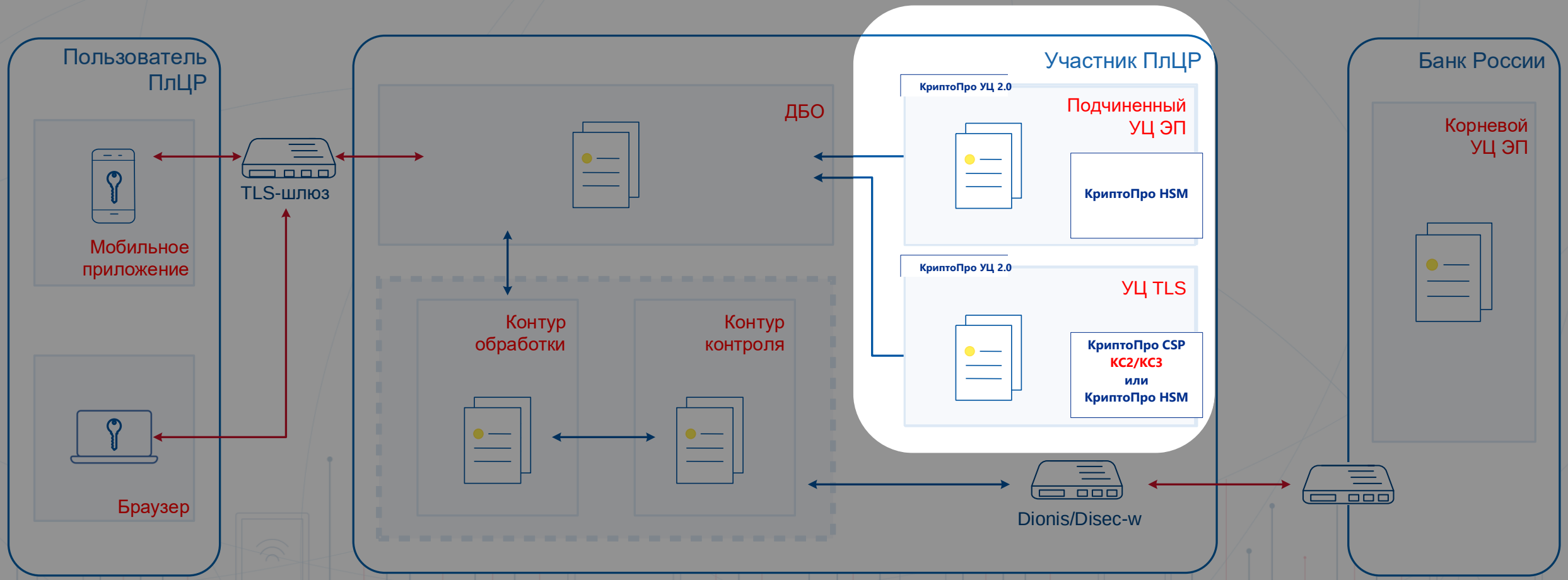
Общие преимущества NGate

- Единое устройство для всех видов доступа
- Наличие сертификатов ФСБ по классам КС1, КС2, КС3
- Одновременная поддержка ГОСТ и не ГОСТ подключений
- Поддержка всех современных ОС, в т.ч. мобильных
- Двухфакторная аутентификация (AD, LDAP, RADIUS, сертификаты)

Общая схема взаимодействия



Участник: УЦ ЭП и УЦ TLS



Участник: УЦ ЭП и УЦ TLS

КриптоПро CSP 5.0 R3 КС2/КС3

- Создание/проверка ЭП ЭС и транзакций
- Шифрование/расшифрование ЭС и транзакций
- Двустороннее ГОСТ-TLS соединение

КриптоПро УЦ 2.0

- Издание сертификатов ключей ЭП и сертификатов безопасности (для TLS)

КриптоПро HSM

- Обработка, хранение и использование ключей

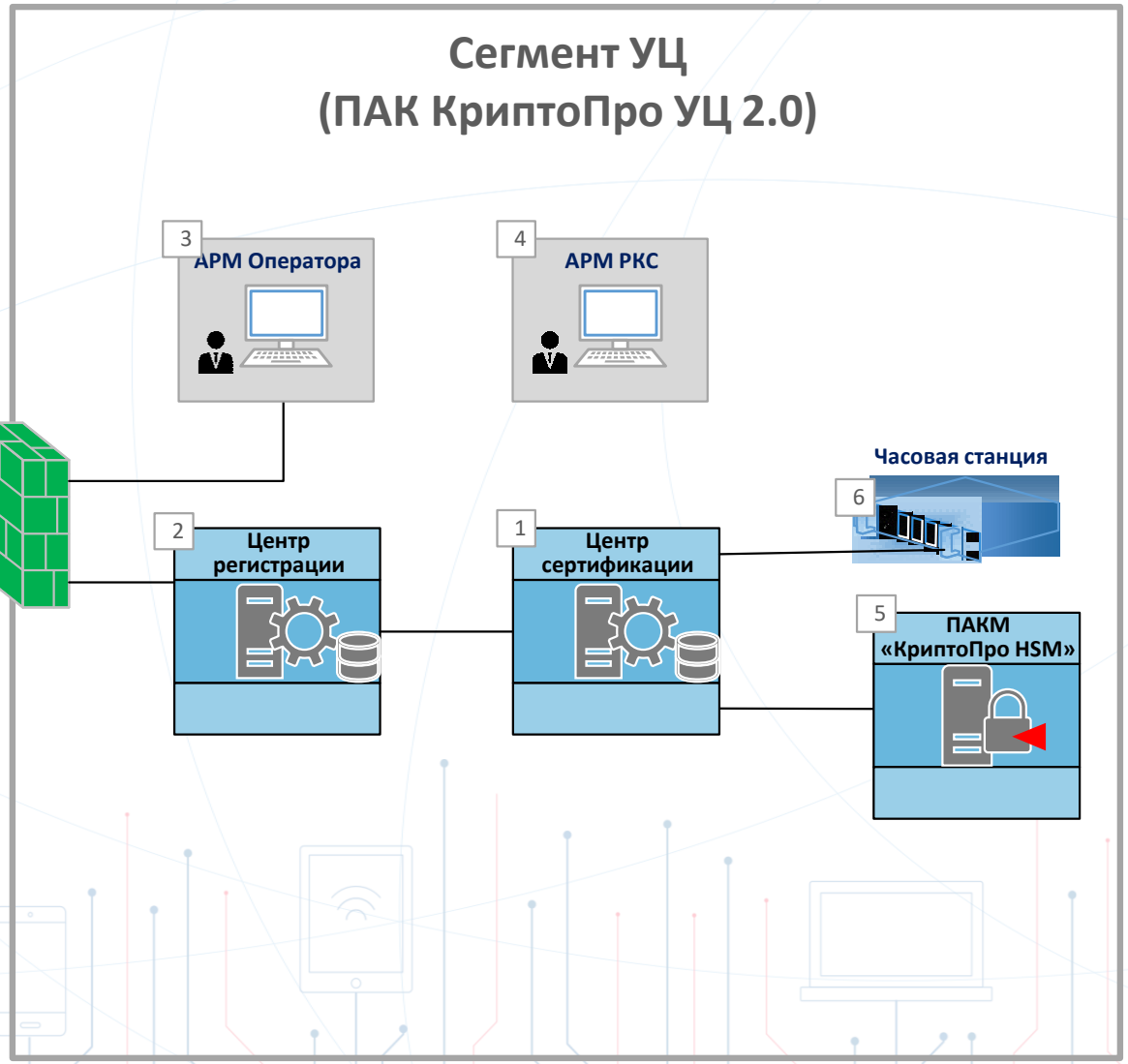
Особенности ПАК КриптоПро УЦ 2.0

- Сертифицирован под Windows и Astra Linux
- Разные API-УЦ под Windows и Astra Linux
- При миграции на Astra Linux потребуется доработка смежного ПО
- Специальная лицензия под «Цифровой рубль» (единая для Windows и Astra Linux)
- Для тестирования можно запросить единую тестовую лицензию
- Для внедрения на Astra Linux рекомендуется пройти обучение

Комплектации ПАК КриптоПро УЦ 2.0

КС2	КС3
Программные компоненты ПАК КриптоПро УЦ 2.0	
Межсетевой экран не ниже 4 класса защиты ФСБ	
СКЗИ КриптоПро CSP или ПАКМ КриптоПро HSM 2.0	
Средства защиты от НСД типа «Электронный замок»	
-	СЗИ SPR – для ОС Windows (для **Astra Linux** – не требуется, достаточного встроенного режима ЗПС)
Часовая станция единого времени (только для **Astra Linux**)	Часовая станция единого времени

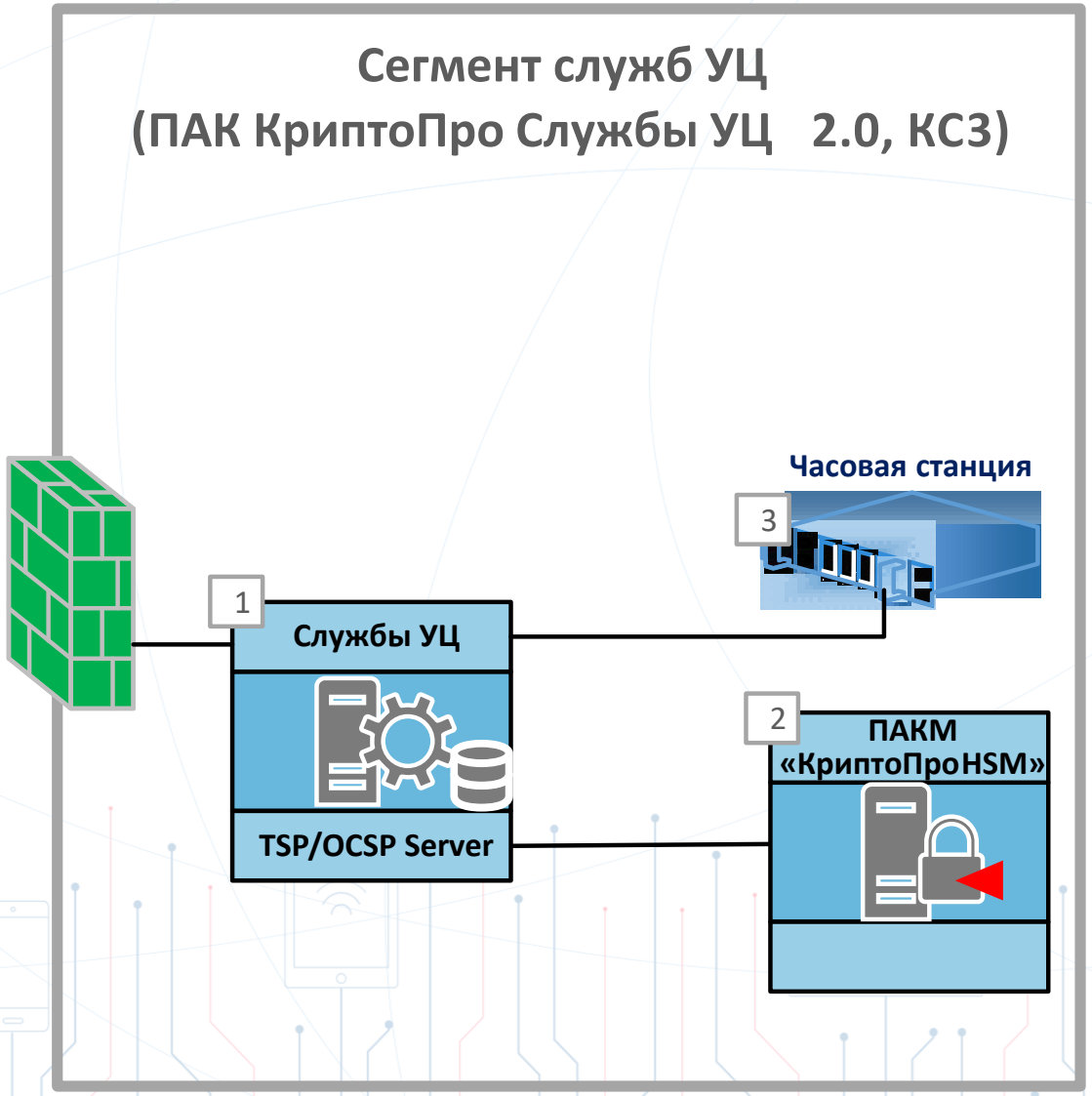
Структурная схема компонент УЦ



Состав компонент

Основные	Дополнительные
(1) ЦС, включающий: • СЗИ НСД типа ПАК Соболь/Аккорд (серт. ФСБ) • SPR (**для КС3 для Win**)	(5) HSM позволяет увеличить срок действия ключа ЦС до 3-х лет
(2) ЦР, включающий: • СЗИ НСД типа ПАК Соболь/Аккорд (серт. ФСБ) • SPR (**для КС3 для Win**)	(6) Часовая станция типа ИВЧ 1/СП с свидетельством Фед. агентства по тех. рег. и метрологии (обязательно **для КС3 и для КС2 на Astra Linux**)
(3,4) АРМ Оператора/РКС, включающий: • СЗИ НСД типа ПАК Соболь/Аккорд (серт. ФСБ) • SPR (**для КС3 для Win**)	

Структурная схема Служб УЦ



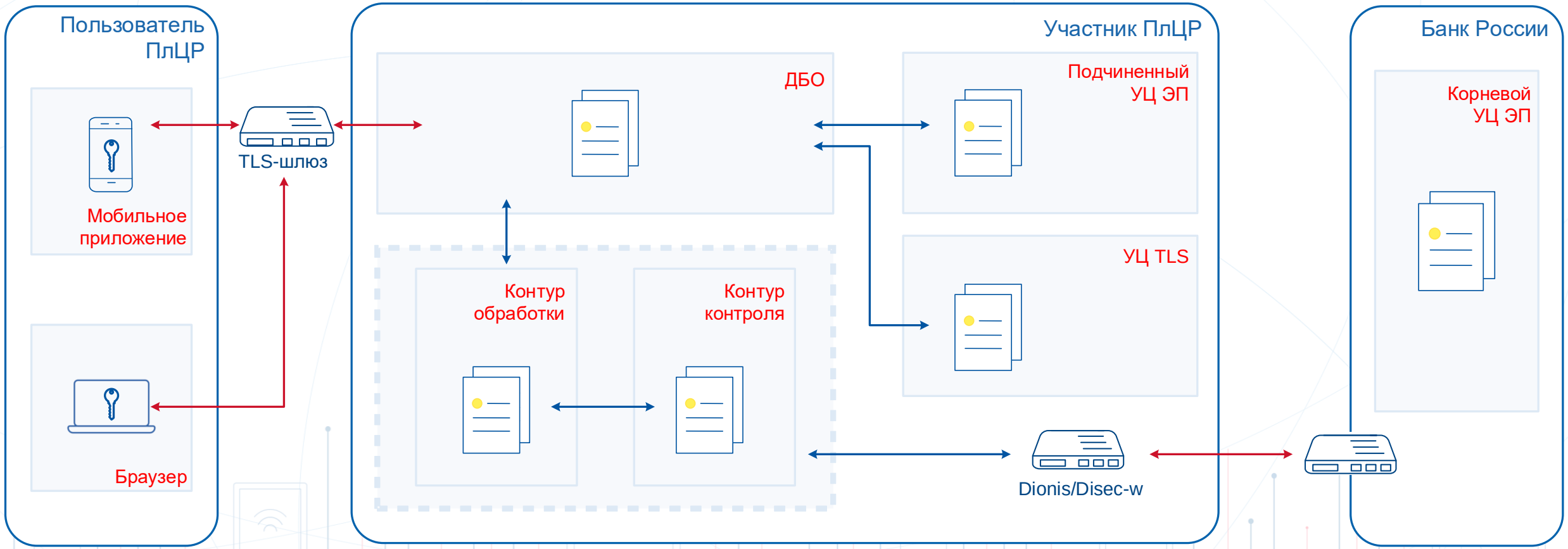
Состав компонент Сегмента Служб УЦ

(1) OCSP, TSP, включающий:
- СЗИ НСД типа ПАК Соболь/Аккорд (сертификат ФСБ)
- SPR (для Windows)

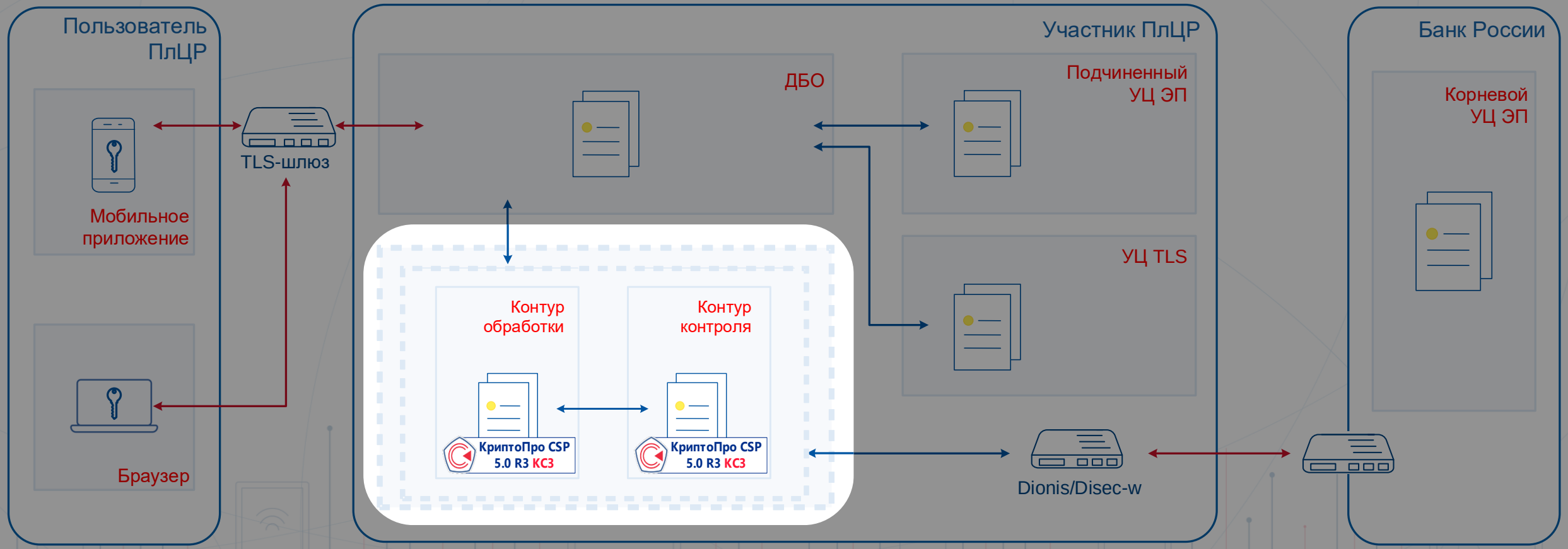
(2) HSM для хранения ключей OCSP и TSP Server и выполнения операций

(3) Часовая станция с свидетельством Федерального Агентства по техническому регулированию и метрологии типа ИВЧ 1/СП

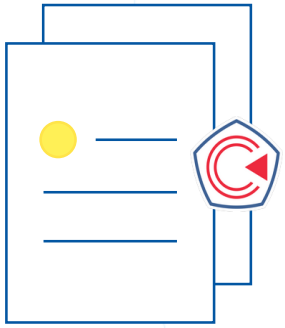
Общая схема взаимодействия



Участник: КО и КК



Участник: КО и КК



КриптоПро CSP 5.0 R3

КС3

- Создание/проверка ЭП ЭС
- Шифрование/расшифрование ЭС

Основные преимущества КриптоПро CSP 5.0

- Сертифицирован ФСБ России по классам КС1, КС2, КС3
- Поддержка российских и зарубежных криптографических алгоритмов
- Возможность хранения ключей удаленно (технология Cloud CSP)
- Поддержка носителей с неизвлекаемыми ключами (ФКН)

- Поддержка всех современных ОС, в т.ч. мобильных
- Имеется графический интерфейс для выполнения базовых операций электронной подписи и шифрования
- Высокая производительность

КриптоПро CSP 5.0 R2/R3

Поддержка алгоритмов шифрования «Кузнечик» и «Магма»

Класс КС3 можно реализовать не только на Windows, но и на Astra Linux

Встраивание клиентского TLS в свое ПО не требует тематических исследований

Встраивание ГОСТ в Apache и nginx возможно без оценки влияния

Работа с Яндекс.Браузером возможна без оценки влияния

КриптоПро CSP 5.0, 5.0 R2, 5.0 R3 сертифицированы ФСБ России

Зачем обновляться с КриптоПро CSP 4.0 на 5.0?

- Сертификаты на КриптоПро CSP 4.0 не вечны (действуют до 15.01.2026)
- Ключевые носители с неизвлекаемыми ключами (ФКН) работают с КриптоПро CSP 5.0 и выше
- Некоторые современные системы работают с КриптоПро CSP 5.0 и выше
- Банк России ведет внутренние работы по переходу на использование алгоритмов шифрования «Кузнечик» и «Магма»
- Банк России предписал Банкам переходить на использование алгоритмов шифрования «Кузнечик» и «Магма» при взаимодействии с ЦБ
- При переходе на современные ОС

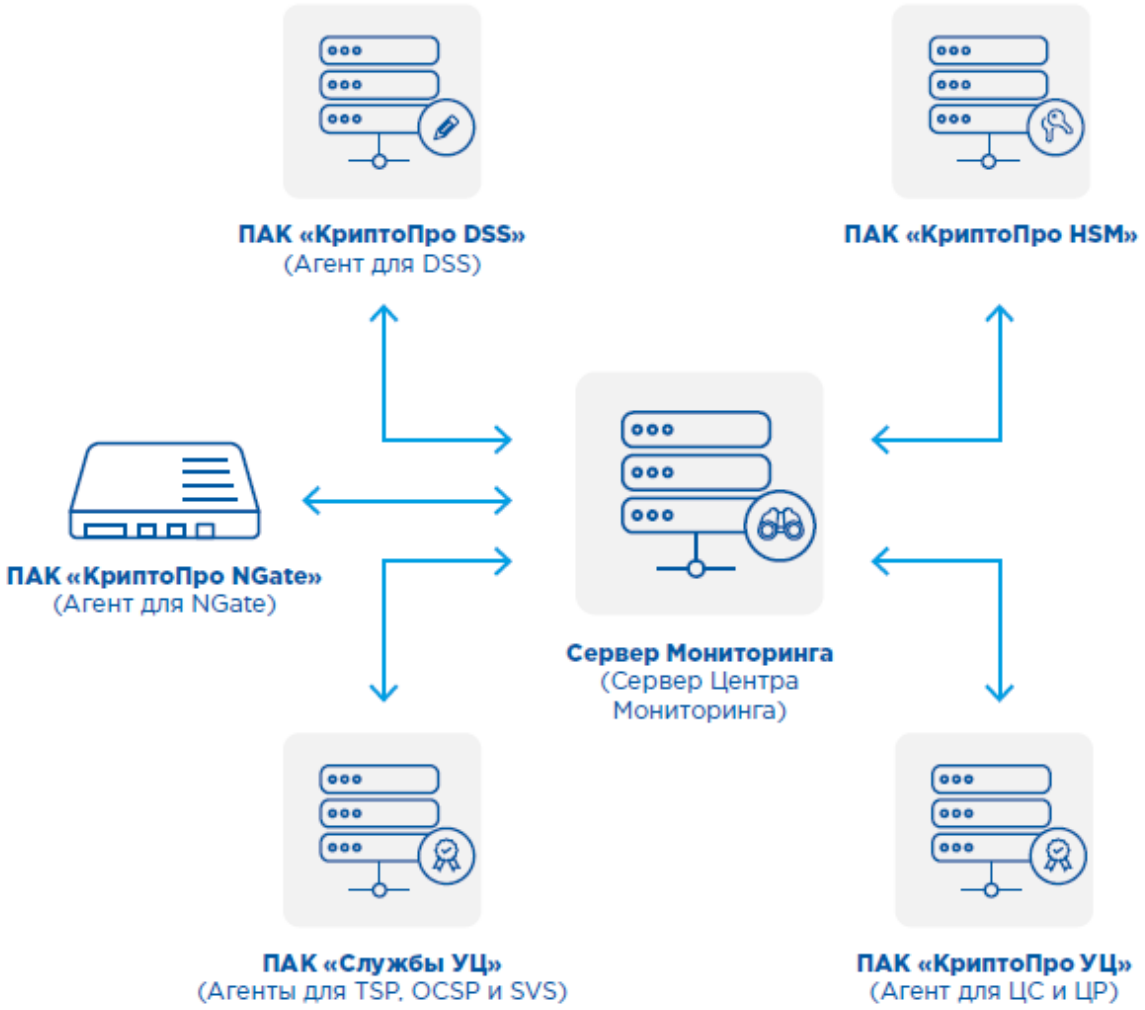
Ценообразование КриптоПро CSP 4.0 и 5.0

1. Новые лицензии лучше сразу приобретать на КриптоПро CSP 5.0 (а не на 4.0)
2. При обновлении приобретается лицензия на обновление
3. Стоимость лицензий на КриптоПро CSP 4.0 и 5.0 является одинаковой
4. На КриптоПро CSP 4.0 и 5.0 есть бессрочные лицензии и годовые
5. Бессрочная лицензия есть клиентская и серверная, годовая – только клиентская
6. Появились отдельные серверные лицензии на КриптоПро CSP 5.0 для TLS-сервера по количеству одновременных подключений (для всех ОС кроме Windows)
7. Лицензия на КриптоПро CSP 4.0 или 5.0 может быть встроена в сертификат от УЦ
8. При обновлении все настройки сохраняются и предоставляется тестовый период на 3 месяца

КриптоПро Центр Мониторинга

Система мониторинга компонентов PKI и эл.подписи

Архитектура Центра Мониторинга



Проверки (примеры):

- Лицензий
- Процедур аутентификации
- Процедур подписи
- Криптопровайдеров
- Сертификатов
- CRL и срока действия CRL
- Баз данных
- Служб TSP, OCSP, SVS и VPN
- Состояния HSM
- Используемой оперативной памяти
- Используемого места на диске
- Выполнение указанных скриптов

Сервер Мониторинга

- Поддержка ОС Windows и Astra Linux
- Централизованный сбор информации с Агентов
- Мониторинг серверов с помощью локальных и удаленных тестов
- Рассылка почтовых уведомлений и СМС-сообщений
- Передача внешним системам результатов проверок

Детали выполнения требований ИБ

- Особенности использования в решении СКЗИ указанных классов
- Необходимость и порядок проведения исследований

Детали выполнения требований ИБ

Особенности использования в решении СКЗИ

- СКЗИ класса КС1 в составе ПМ БР
- Встраивание в соответствии с документацией на ПМ БР и СКЗИ
- Выполнение требований в части защиты от НСД, парольной защите и пр.
- Выполнение требований в части ОС
- Разработка документа Регламент для «упрощенной» оценки влияния

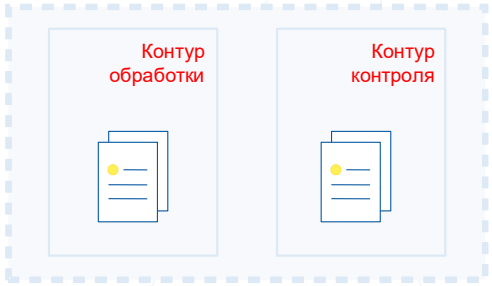
Детали выполнения требований ИБ

Особенности использования в решении СКЗИ указанных классов

- СКЗИ класса КС1
- Встраивание в соответствии с документацией на СКЗИ
- Выполнение требований в части защиты от НСД, парольной защите и пр.
- Использование web-браузера с поддержкой ГОСТ-TLS

Детали выполнения требований ИБ

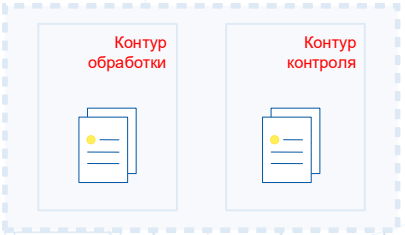
Особенности использования в решении СКЗИ указанных классов



- СКЗИ класса КС3
- Встраивание в соответствии с документацией на СКЗИ
- Выполнение требований в части защиты от НСД, парольной защите и пр.
- Использование одной из сертифицированных ОС, АПМДЗ и т.п.
- Наличие ограничений на используемые для разработки языки программирования

Детали выполнения требований ИБ

Необходимость и порядок проведения исследований



- Регламентируется 833-П и «Порядок …»
- Фиксированная версия ПМ БР и СКЗИ
- Возможно проведение работ по оценке влияния по «упрощенному» порядку

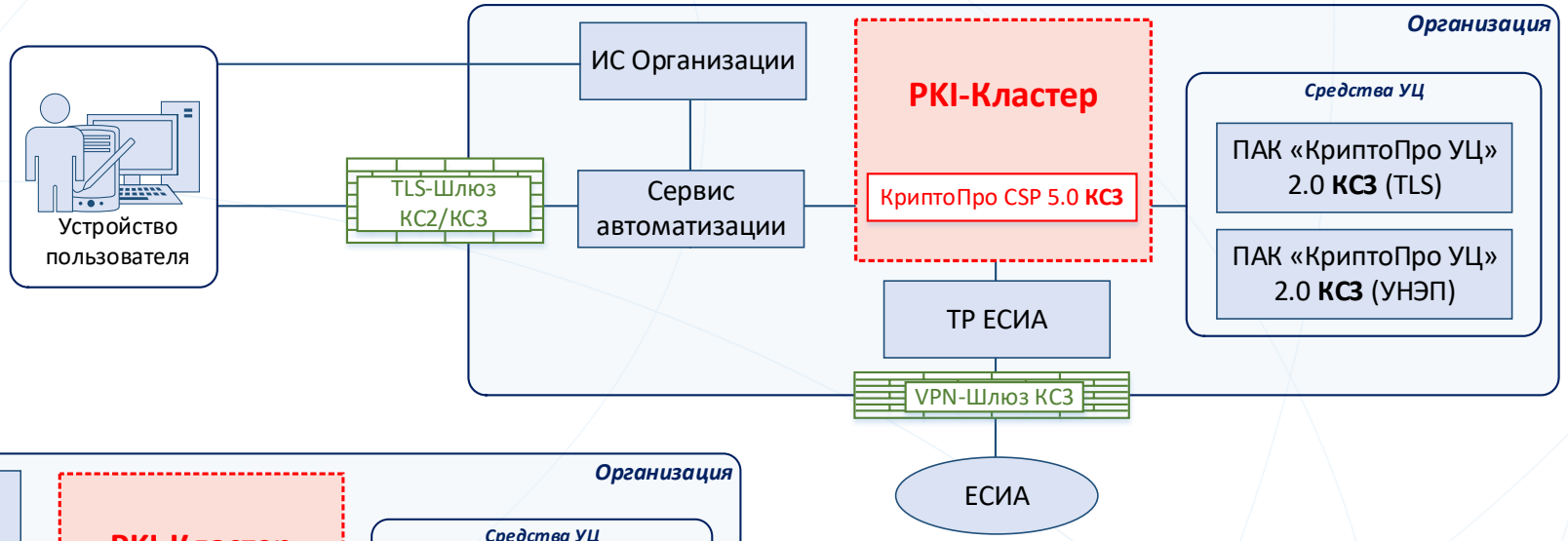
- Необходимость проведения работ по оценке влияния «на общих основаниях»

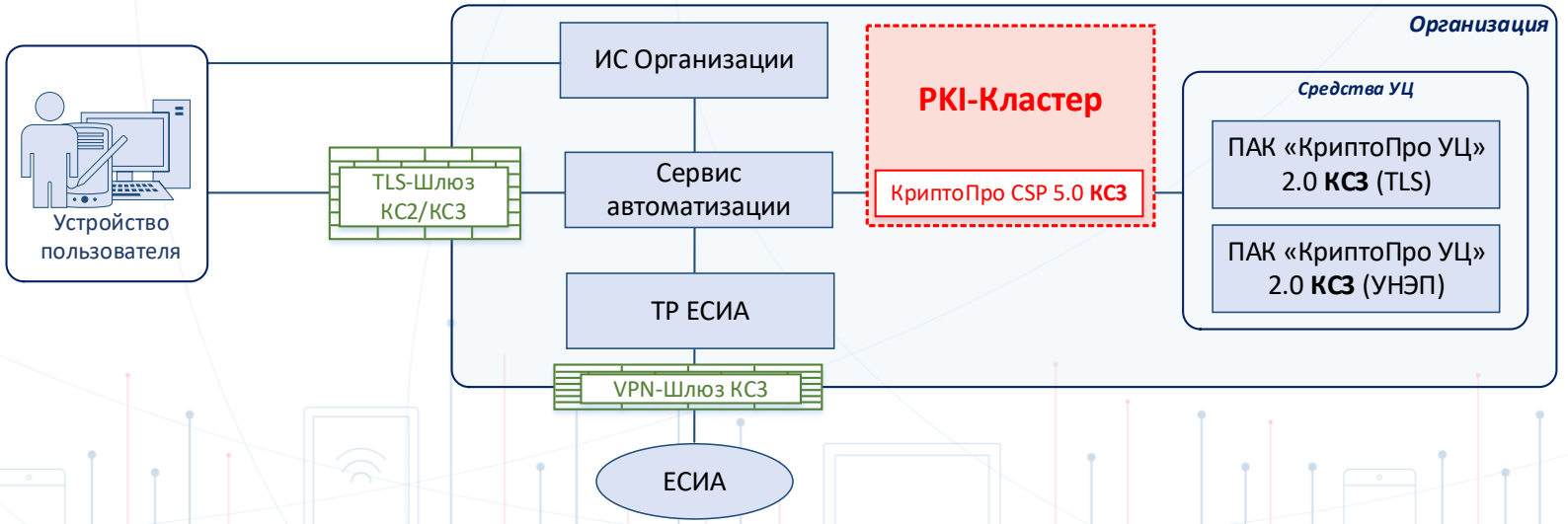
Автоматизация выпуска сертификатов

- Аутентификация пользователя
- Контроль данных (в запросе и изданном сертификате)
- Интеграция с УЦ

Автоматизация выпуска сертификатов

Исполнение 1





Исполнение 2

КРИПТОПРО

Ключевое слово
в защите информации

СПАСИБО ЗА ВНИМАНИЕ!

127018, г. Москва, ул. Сущевский Вал, д.18
Тел./факс: +7 (495) 995-48-20

https://cryptopro.ru

Павел Луцик: **plutsik@cryptopro.ru**
Общие вопросы: **info@cryptopro.ru**
Контрактный отдел: **kpo@cryptopro.ru**
Для дилеров: **dealer@cryptopro.ru**

Опрос 2