

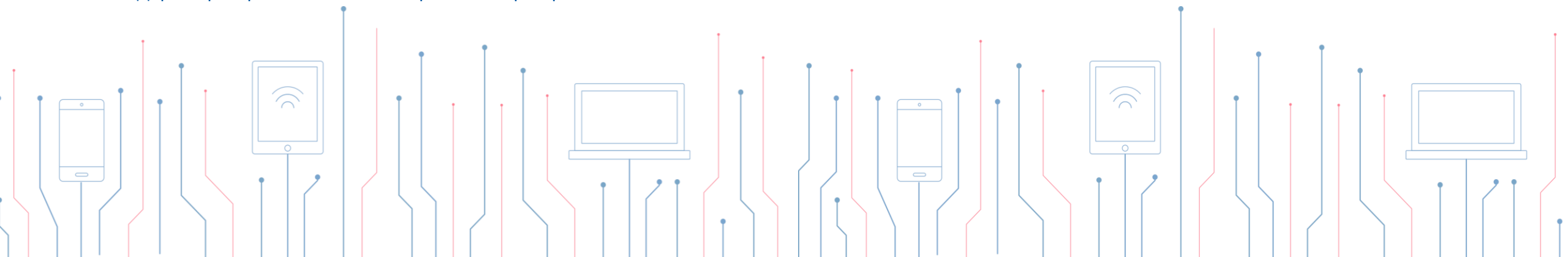


Ключевое слово
в защите информации

Особенности криптографической защиты информации платформы цифрового рубля

Павел Луцик

Директор по развитию бизнеса и работе с партнёрами





«Платформа цифрового рубля в рамках пилота показала свою работоспособность и функциональность. Теперь нужно сделать следующий шаг, а именно: перейти к более широкому, полномасштабному внедрению цифрового рубля в экономику, в хозяйственную деятельность и в сферу финансов»

В.В. Путин, совещание по экономическим вопросам,
17 июля 2024 г.

Этапы работ по проекту Цифрового рубля



Источник: Банк России.

Банки-участники пилота (первая волна)

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

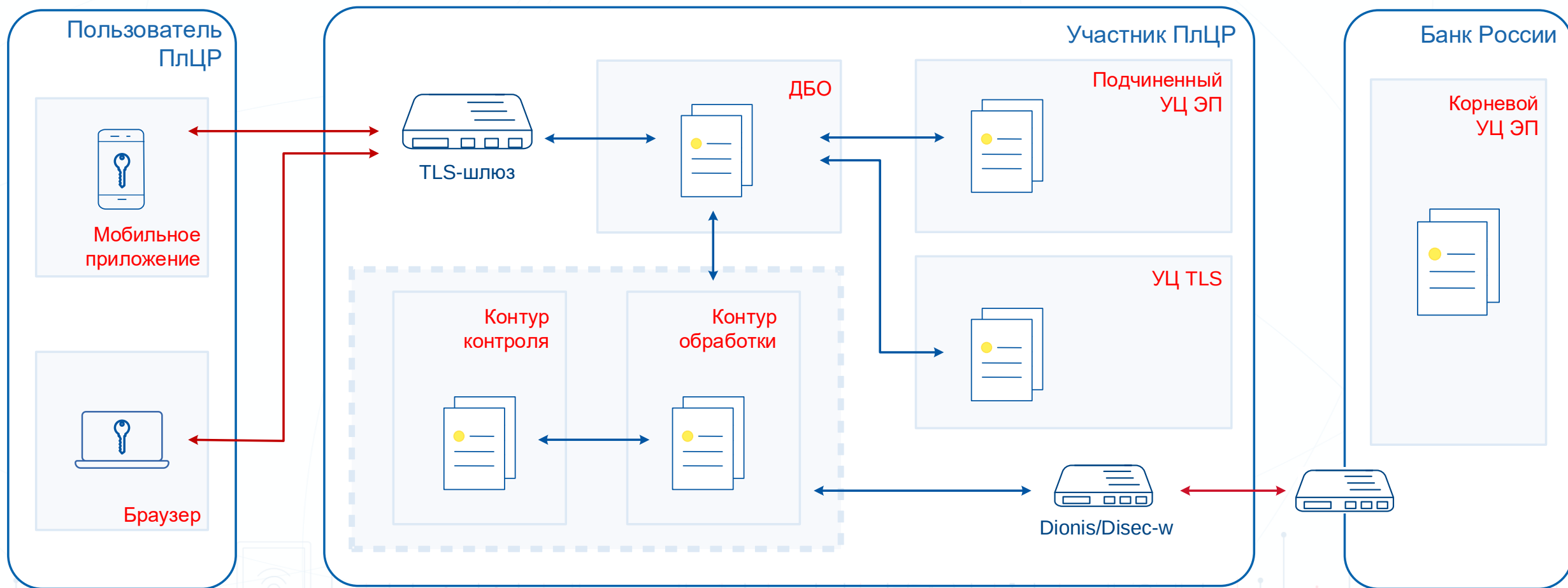


1. АБ РОССИЯ
2. БАНК ОРЕНБУРГ
3. Банк Русский Стандарт
4. МСП Банк
5. ПЕРВОУРАЛЬСКБАНК
6. Россельхозбанк
7. ТБанк
8. Экспобанк
9. АКБ НОВИКОМБАНК
10. Банк ВБРР
11. КБ Кубань Кредит
12. Банк Точка
13. РосДорБанк
14. Сбербанк России
15. АКБ Металлинвестбанк
16. КБ Центр-инвест
17. Прио-Внешторгбанк
18.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

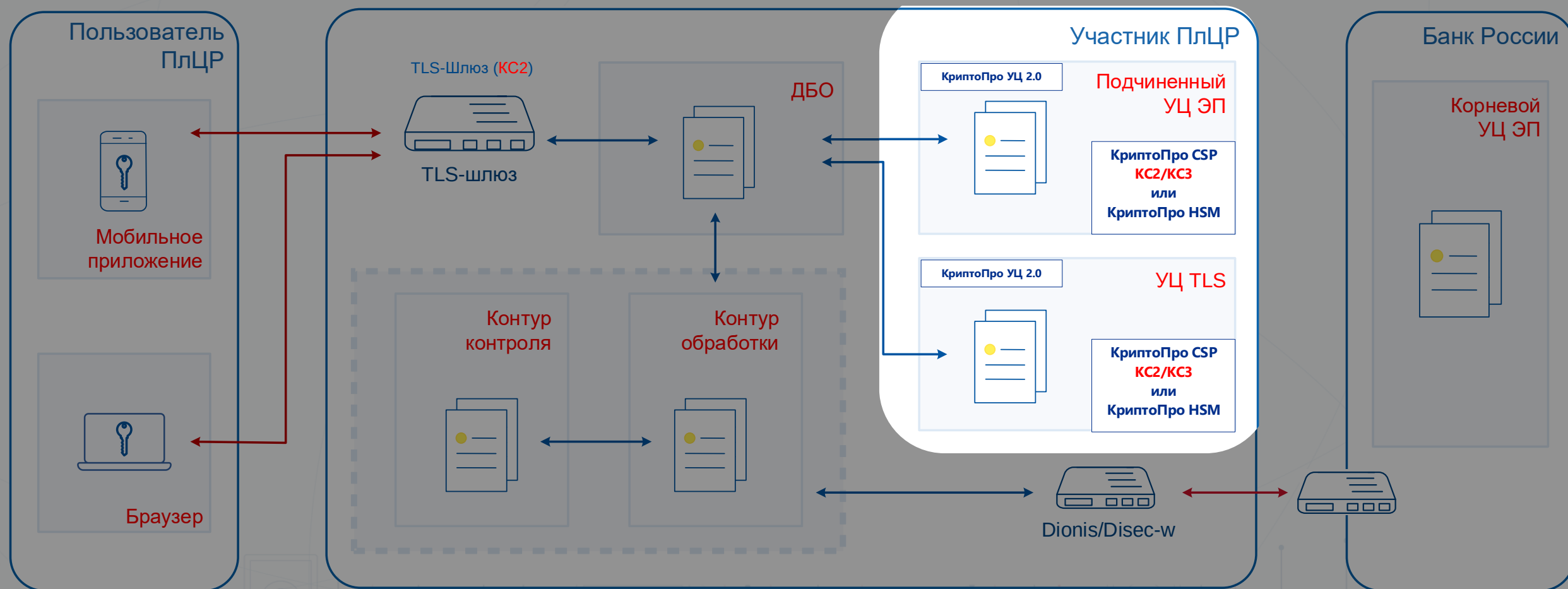
Срок ввода	Кредитные организации (кол-во)	Торговые и сервисные предприятия (ТСП)
01.07.2025	Системно значимые банки (13)	С годовой выручкой более 30 млн.р.
01.07.2026	Остальные банки с универсальной лицензией (221)	С годовой выручкой более 20 млн.р.
01.07.2027	Прочие кредитные организации (134)	Все другие

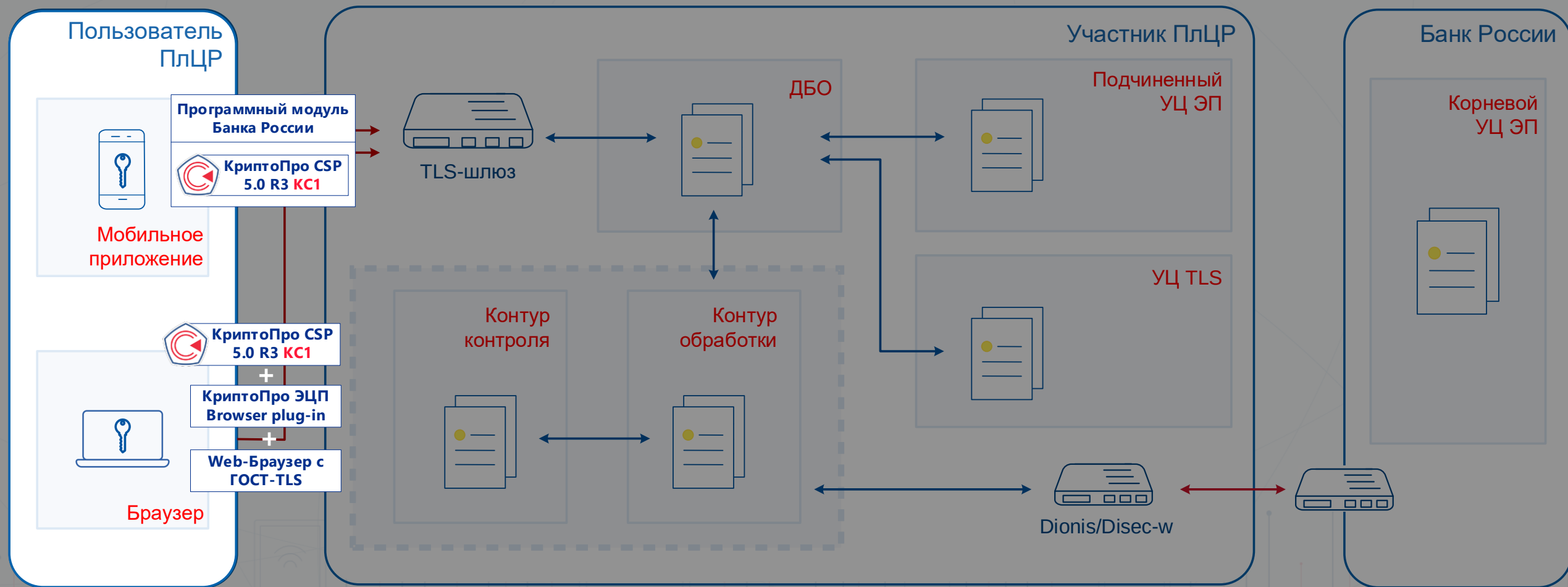
*Оплата покупок цифровыми рублями будет проходить по универсальному QR-коду на базе НСПК

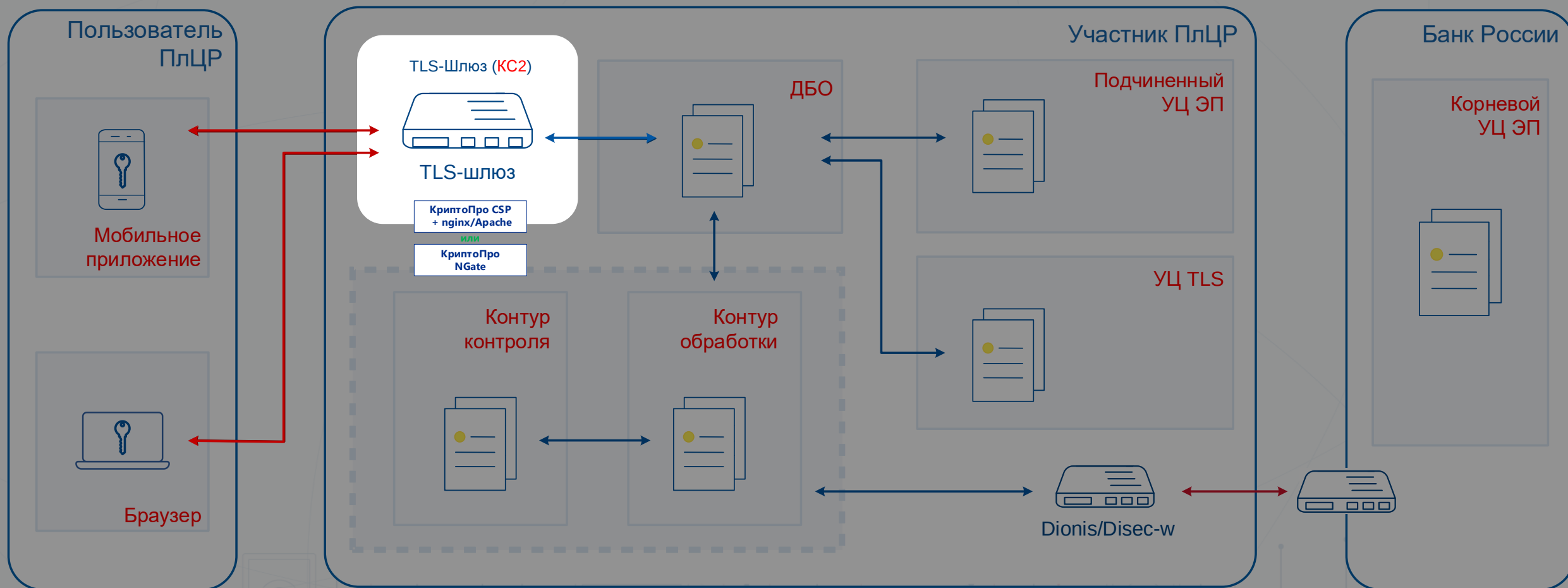
Общая схема взаимодействия (без сервиса автоматизации и ЕСИА)

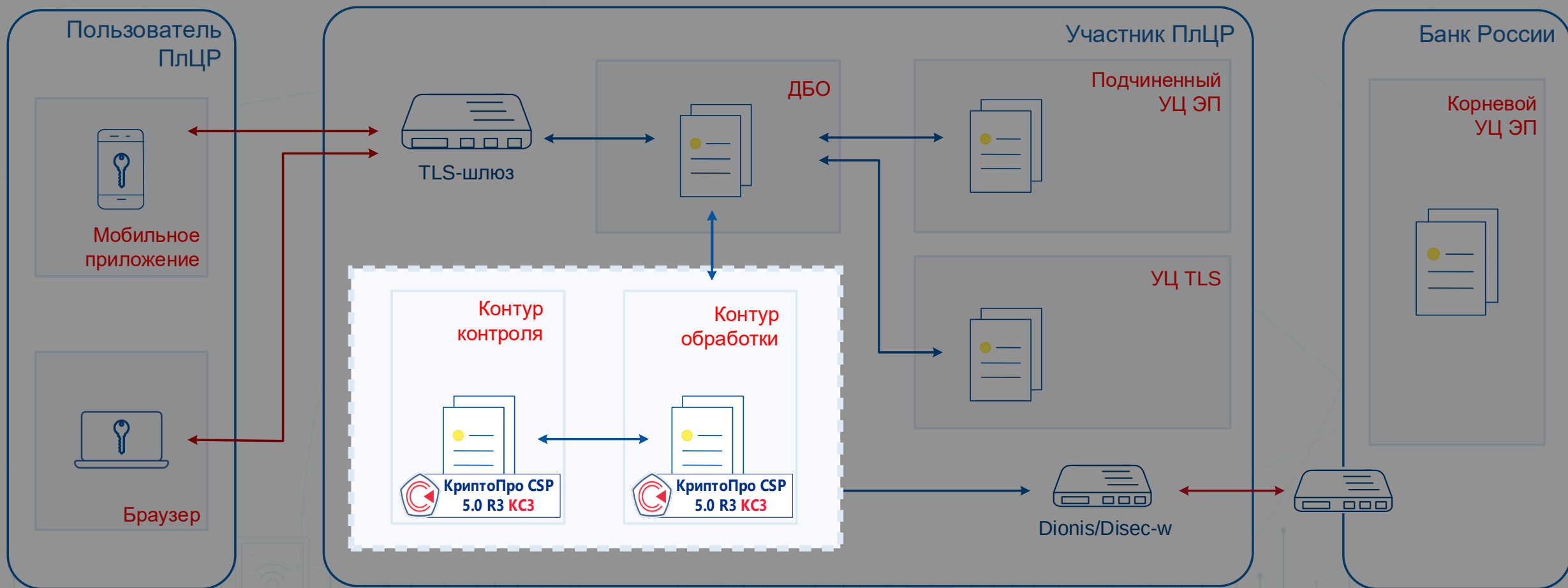


- Для выполнения операций с цифровыми рублями клиент банка должен получить сертификаты безопасности и УНЭП
- Сертификат безопасности необходим для реализации защищённого двустороннего ГОСТ TLS-соединения между МП клиента и банком
- Сертификат УНЭП необходим для осуществления операций с цифровыми рублями и подписания распоряжений на операции
- Выпуск обоих типов сертификатов может осуществляться с использованием сервиса автоматизации выпуска сертификатов









01

Особенности использования в решении СКЗИ указанных классов

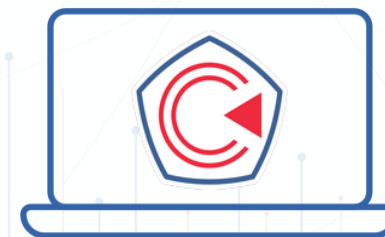
02

Необходимость и порядок проведения исследований

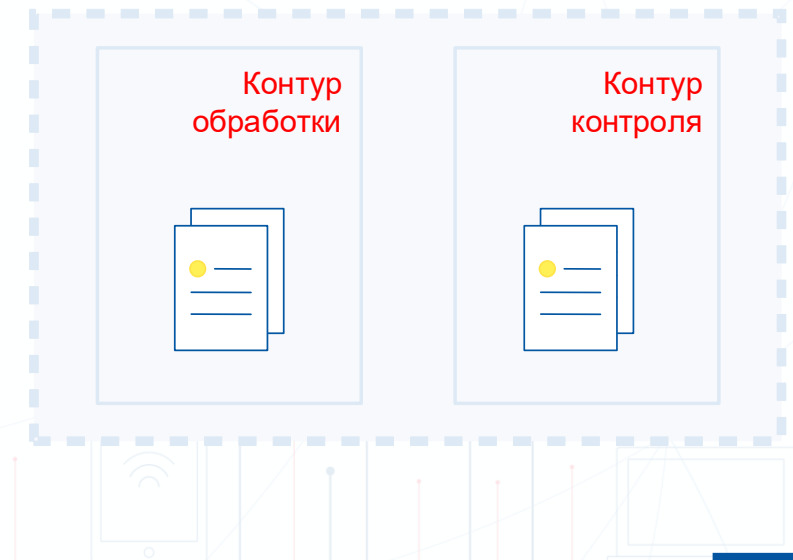
- СКЗИ класса КС1 в составе ПМ БР
- Встраивание в соответствии с документацией на ПМ БР и СКЗИ
- Выполнение требований в части защиты от НСД, парольной защиты и пр.
- Выполнение требований в части ОС
- Разработка документа Регламент для «упрощенной» оценки влияния



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

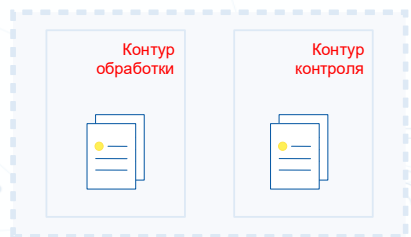


- СКЗИ класса КСЗ
- Встраивание в соответствии с документацией на СКЗИ
- Выполнение требований в части защиты от НСД, парольной защиты и пр.
- Использование одной из сертифицированных ОС, АПМДЗ и т.п.
- Наличие ограничений на используемые для разработки языки программирования

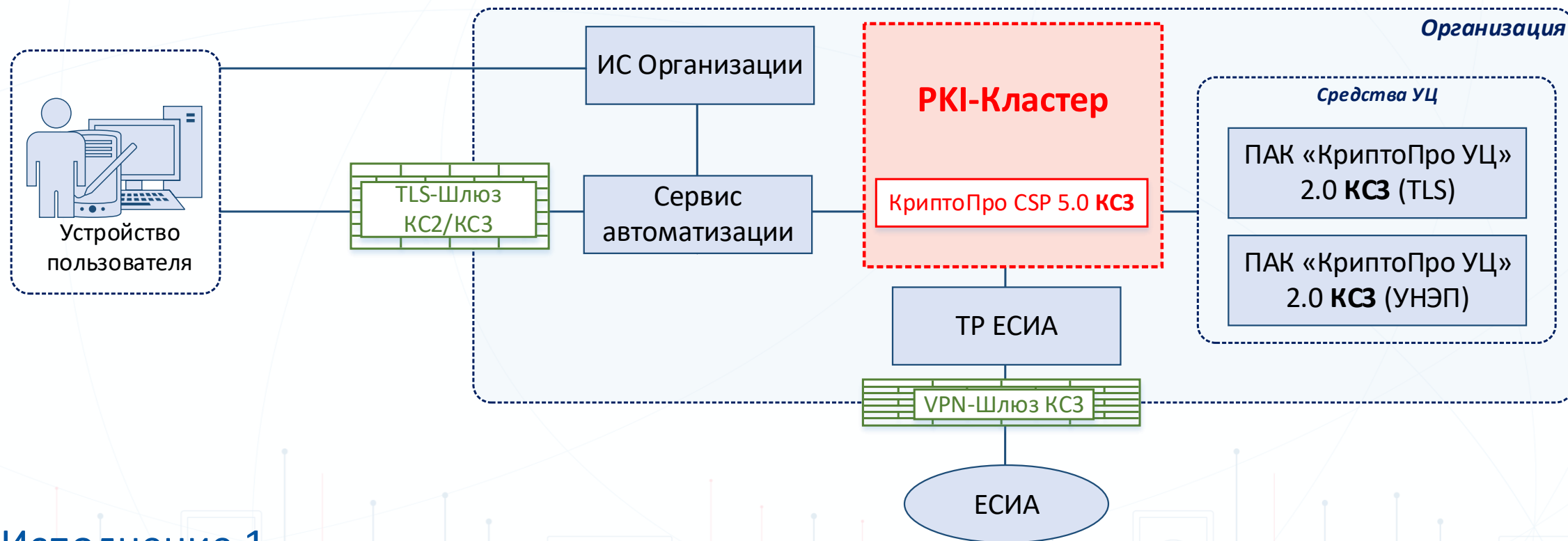




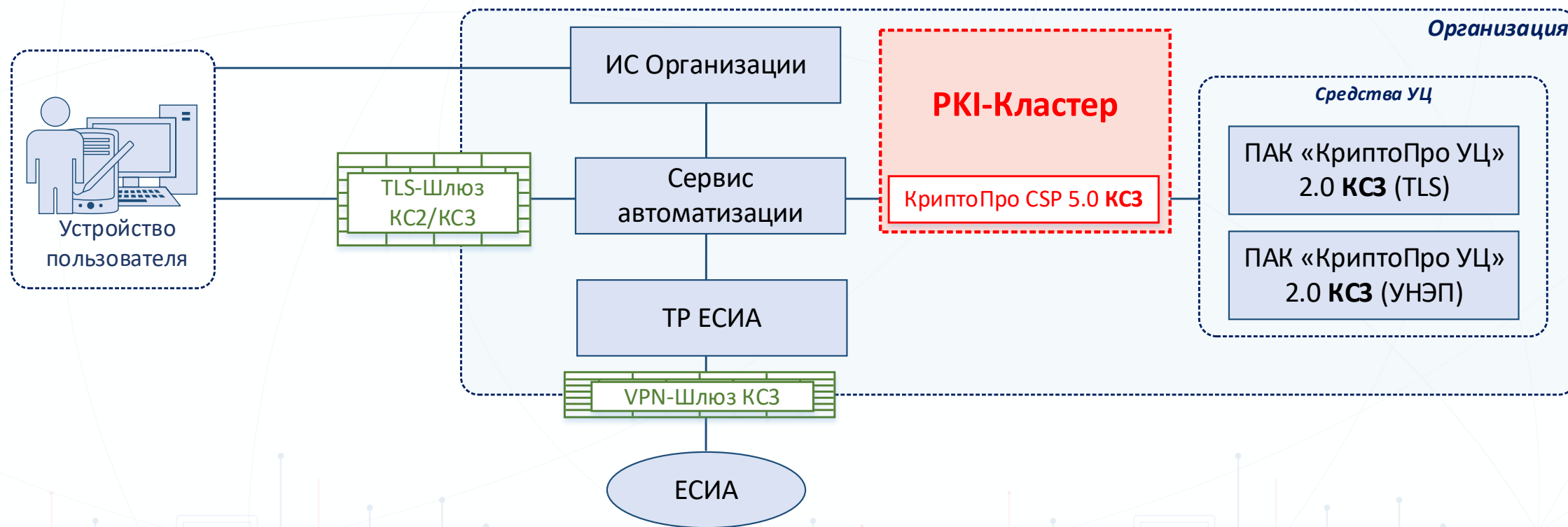
- Регламентируется 833-П и «Порядок ...»
- Фиксированная версия ПМ БР и СКЗИ
- Возможно проведение работ по оценке влияния по «упрощенному» порядку
- Необходимость проведения работ по оценке влияния «на общих основаниях»



- Аутентификация пользователя
- Контроль данных (в запросах и изданных сертификатах)
- Интеграция с УЦ



Исполнение 1



Исполнение 2

- Аутентификация пользователей по протоколу OIDC в соответствии с методическими рекомендациями и НПА по использованию ЕСИА
- Предоставление PKI-Кластеру и Сервису автоматизации идентификационной информации пользователей из ЕСИА
- Проверка информации о пользователе в рамках протокола OIDC
- Выполнение криптографических операций с использованием встроенного СКЗИ класса не ниже КСЗ
- Наличие положительного заключения ФСБ России



Проверка ЭП запросов на сертификат (PKCS#10) и подписанных сообщений (PKCS#7) с помощью КриптоПро CSP 5.0 R3 KC3



Передача в УЦ прошедших проверки запросов на сертификат



Проверка идентификационных данных при первичном и повторном выпуске сертификата



ФЛК выпущенных средствами УЦ сертификатов



Форматно-логический контроль (ФЛК) запросов на сертификат (PKCS#10) и подписанных сообщений (PKCS#7), передаваемых в сторону средств УЦ



Передача выпущенных сертификатов Сервису автоматизации

- КриптоПро CSP 5.0 R3 KC3
- ОС Astra Linux SE
- СЗИ (СОВ, МЭ, САВЗ, АПМДЗ)
- СУБД PostgreSQL



**Ключевое слово
в защите информации**

СПАСИБО ЗА ВНИМАНИЕ!



info@cryptopro.ru
plutsik@cryptopro.ru

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

<https://cryptopro.ru>