

Модернизация механизмов защиты пользователей ЕСИА с использованием РКИ и сопутствующие задачи

РТЛабс

Кондратенко Роман Сергеевич, РТ ЦР

Лебедева Серафима Александровна, РТЛабс

Мелузов Антон Сергеевич, к.ф.-м.н., РТЛабс

Чижевский Игорь Евгеньевич, РТЛабс

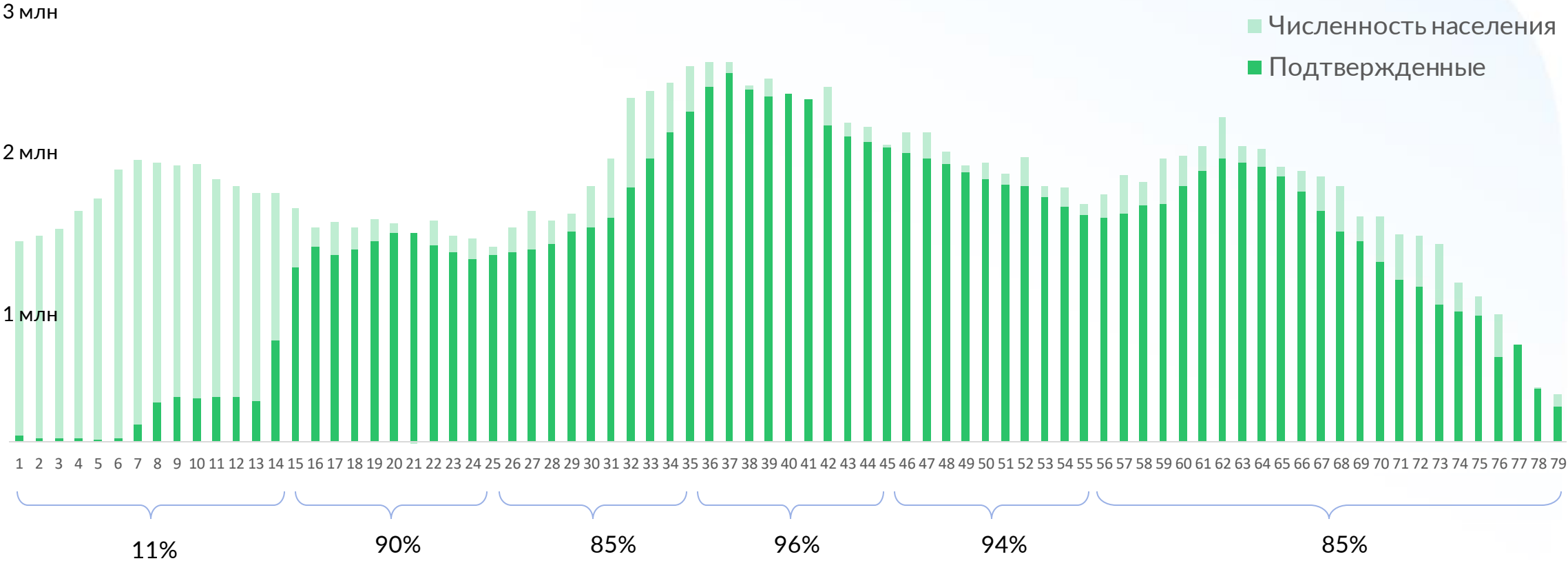
PKI-forum 2024

Что такое ЕСИА?

112 млн
подтверждённых УЗ

более 5 млрд
аутентификаций в год

более 3,5 тысяч подключенных
информационных систем



Введение 2ФА для аутентификации в ЕСИА

С октября 2023 года использование второго фактора при аутентификации **через ЕСИА обязательно**

90% активных пользователей ЕСИА уже **подключили 2ФА** (СМС, ТОТР, ЕБС)

Теперь пользователь чаще всего понимает, что отдал коды доступа мошенникам, но часто **постфактум** 😞

Социальная инженерия

- Использование уязвимостей «естественного» интеллекта
 - Срочное принятие решений в стрессовой ситуации
 - Благодарность за «услугу» и т.д.
- Любые меры по снижению массового фрода с использованием социальной инженерии — работа с «воронкой» мошенников
- Волшебной пилюли нет, но...



Криптографическая аутентификация



Пользователь владеет ключом и не может его легко самостоятельно извлечь или передать мошенникам



Управление доступом конкретных устройств



Разграничение уровней доступа с различных устройств или в зависимости от надёжности идентификации

Что для этого нужно?



Новый протокол аутентификации



Инфраструктура, которая поддерживает PKI
в масштабе всей страны



УЦ, который готов выдавать ~5 млн
сертификатов в месяц



МП Госуслуги с отечественной криптографией

Что такое МП Госуслуги?

DAU: ~7 млн

Новых инсталляций за 2023 год: 45 млн

MAU: 50+ млн

Запускалось за 2023 год на 107 млн уникальных устройств

Количество релизов за год:
от 12



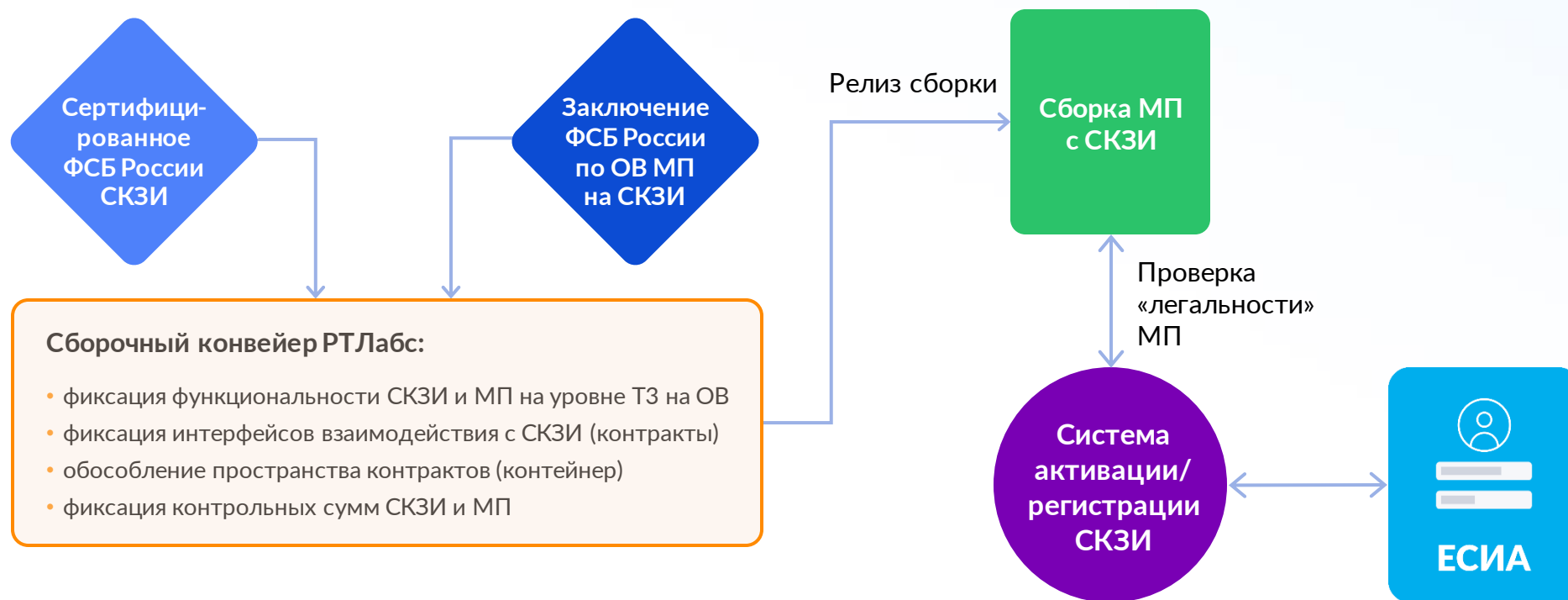
а нужно еще:

- Поддержка криптографических протоколов в рамках Госдоков
- Встраивание функциональности Госключа
- Поддержка криптографических протоколов ЕСИА
- Как проводить оценку влияния???!?

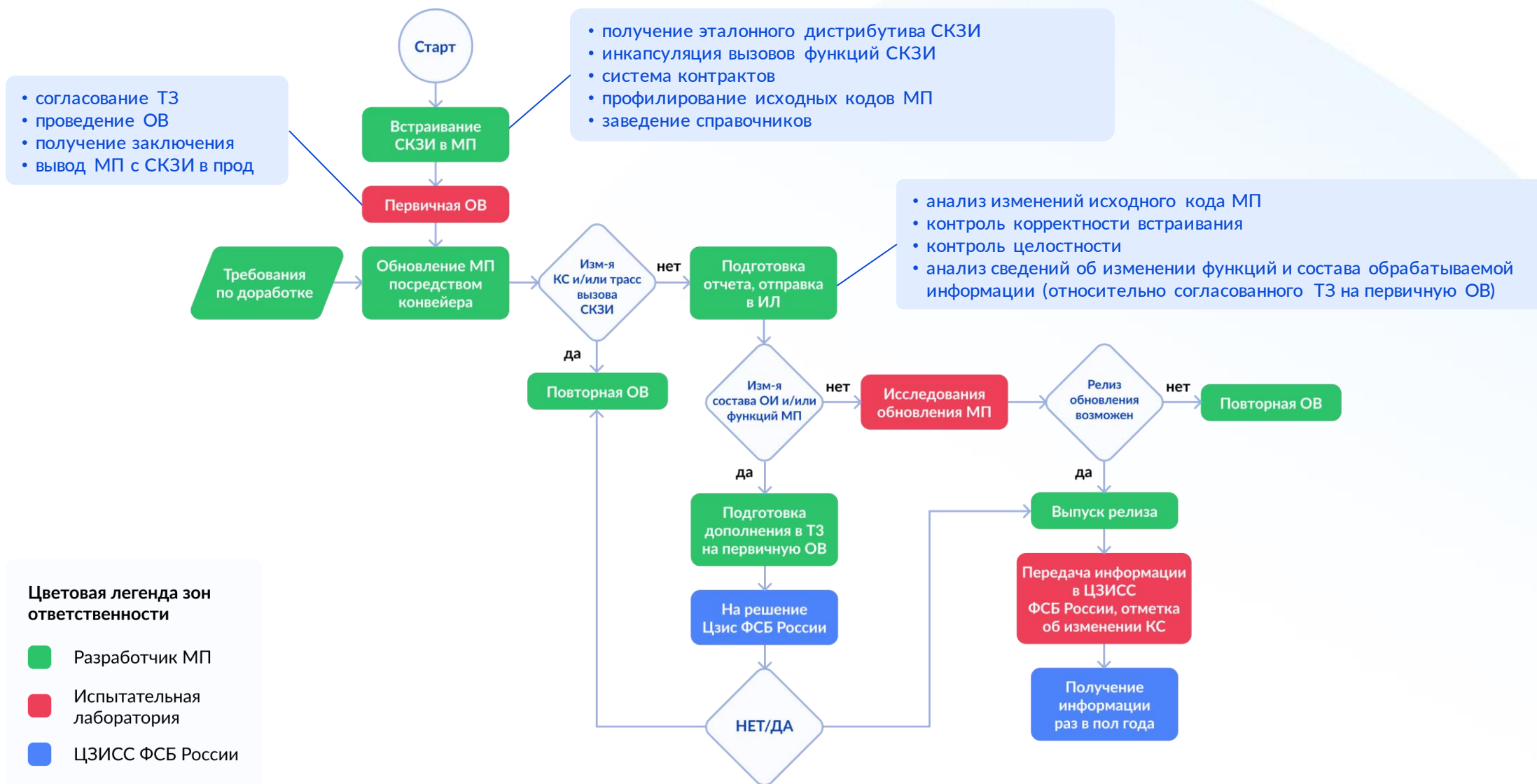
Что мы сделали?

✔ Разработали специальную архитектуру приложения

Схема выпуска релиза МП с встроенным СКЗИ с использованием сборочного конвейера

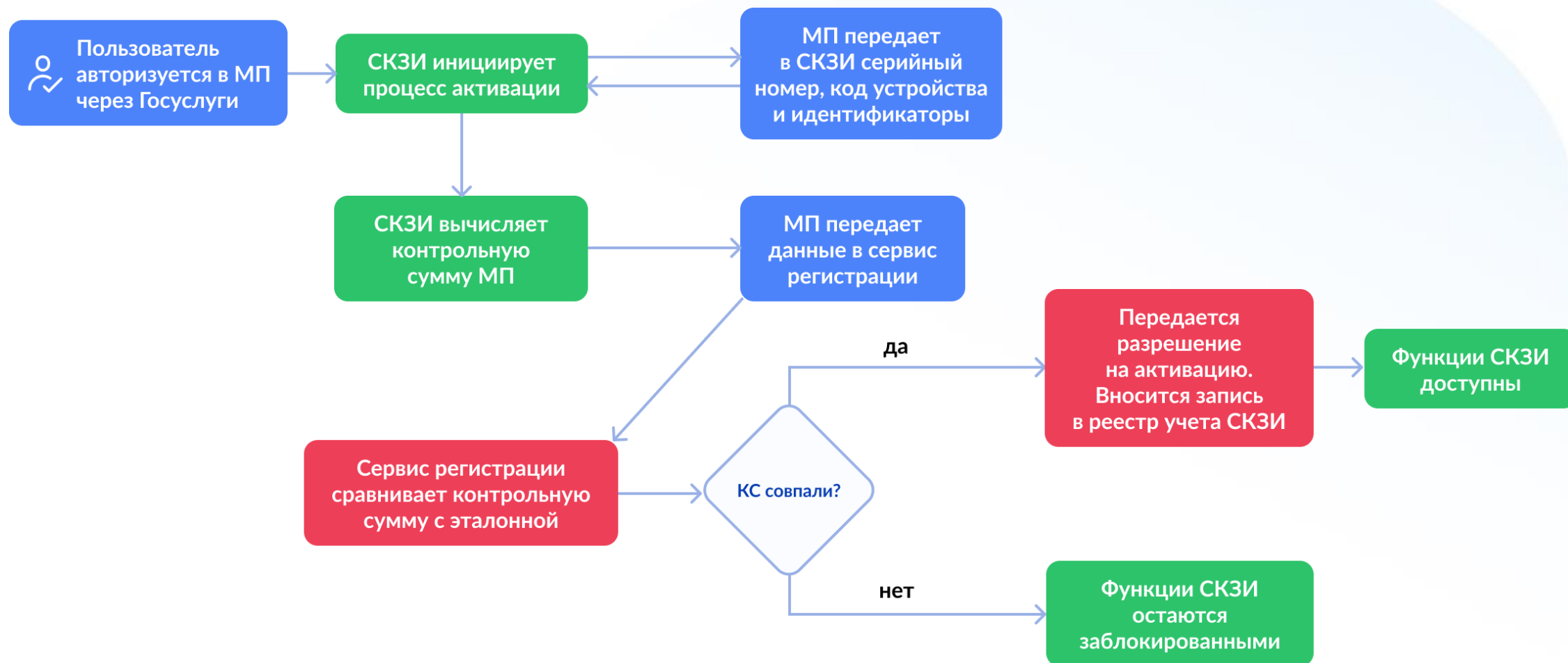


Как соответствовать требованиям?



Как контролировать легальность сборки?

Схема активации СКЗИ в составе приложения



Результат

- ✓  Согласован Регламент проведения оценки влияния в условиях регулярного изменения бизнес-функций приложения
- ✓  Ожидаемые сроки рассмотрения релиза лабораторией сравнимы со сроками рассмотрения приложения магазинами приложений, процессы проходят параллельно
- ✓  Реализован ТЕХНОЛОГИЧЕСКИЙ подход к контролю исполнения требований ПКЗ-2005 при коротком релизном цикле мобильного приложения