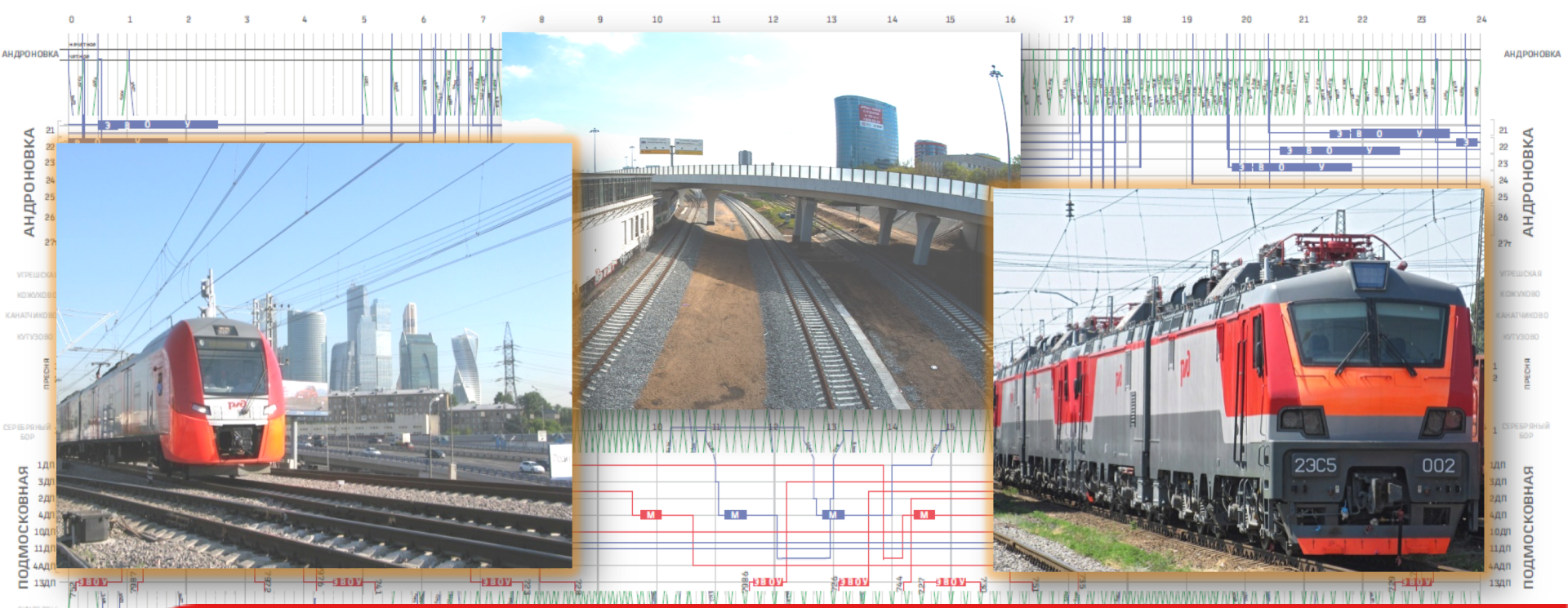
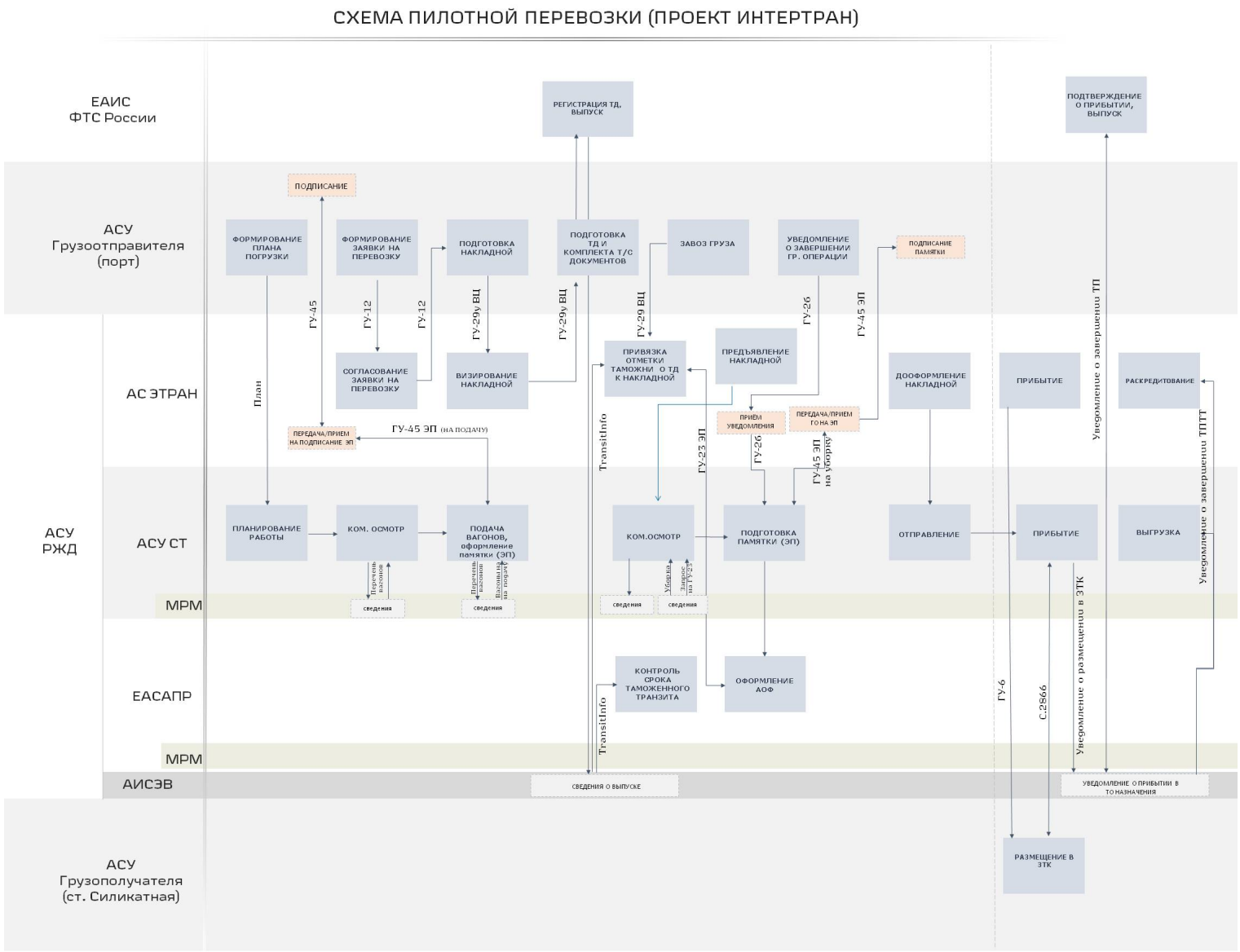


Механизмы единой аутентификации пользователей АС ОАО «РЖД»

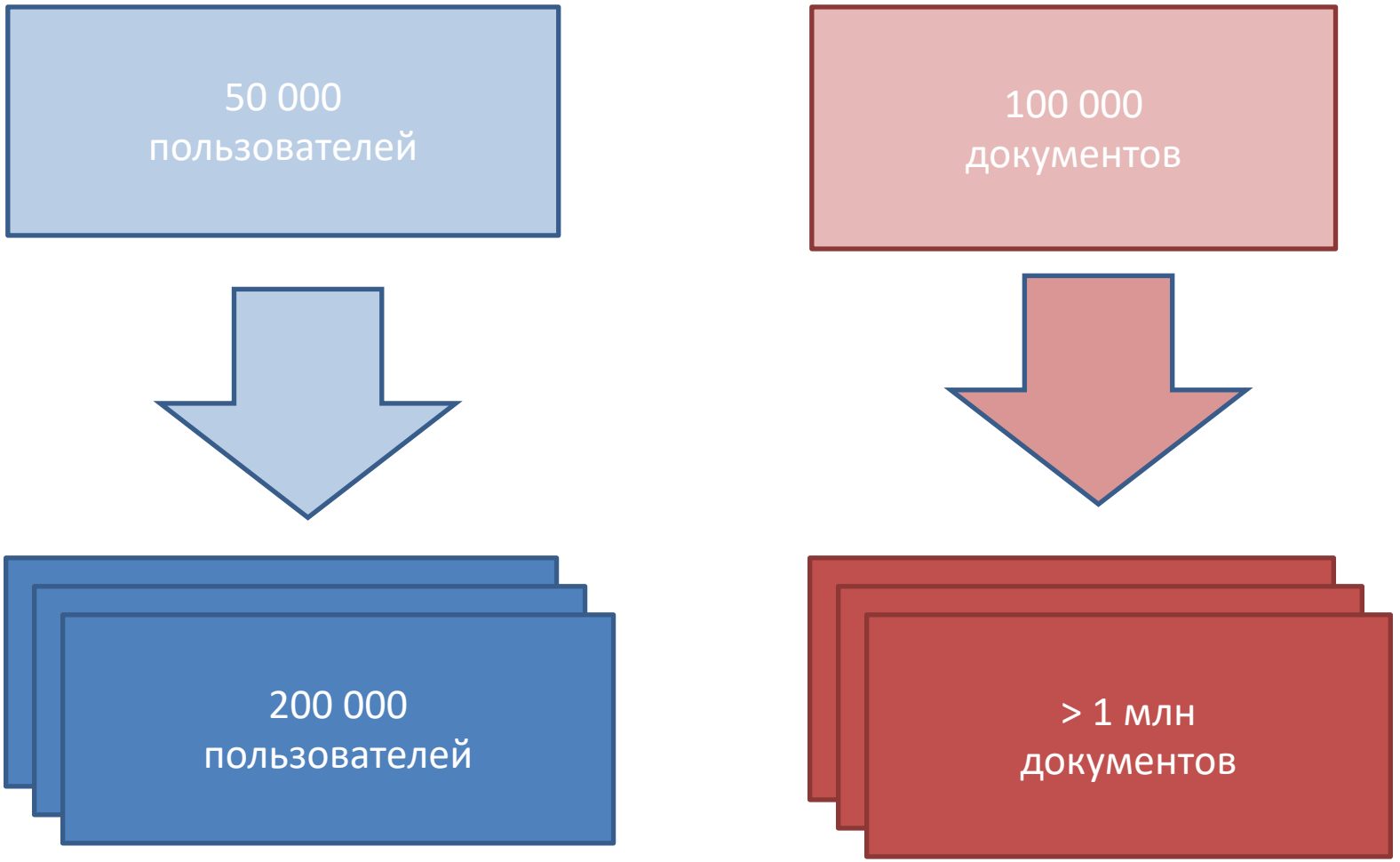
Калашников Александр Михайлович, начальник Отделения разработки программного обеспечения сервисов электронной подписи АО «НИИАС»

Нутович Вероника Евгеньевна, заведующий научно-исследовательской лабораторией «Грузовая и коммерческая работа», заместитель заведующего кафедрой «Логистические транспортные системы и технологии» Российского университета транспорта (МИИТ), кандидат технических наук

Схема взаимодействия систем



Подсистема электронной подписи



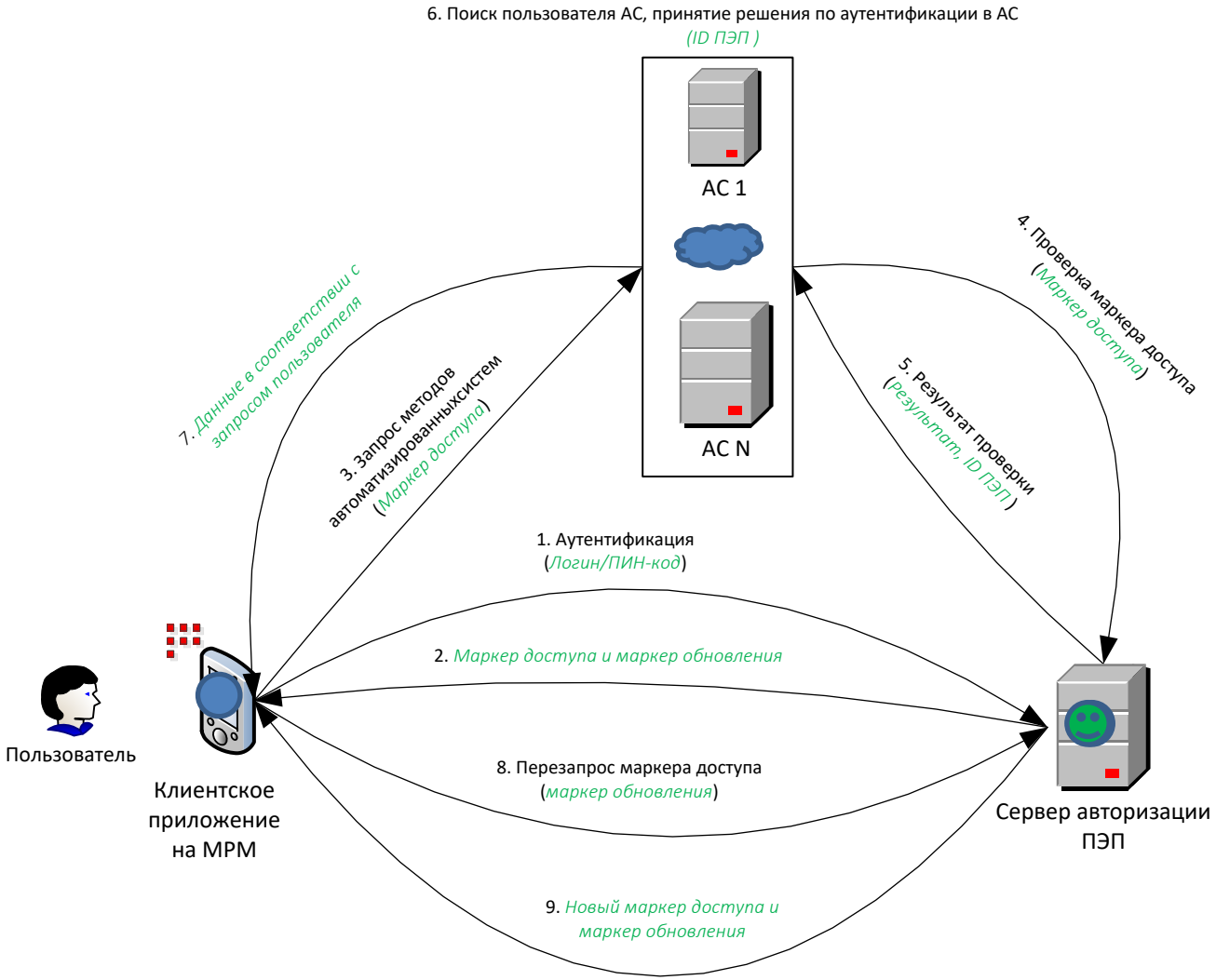
OAUTH 2.0

- OAuth 2.0 (RFC 6749) - протокол авторизации, позволяющий выдать одному сервису (приложению) права на доступ к ресурсам пользователя на другом сервисе. Протокол избавляет от необходимости доверять приложению логин и пароль, а также позволяет выдавать ограниченный набор прав, а не все сразу.
- OAuth протокол в ПЭП основан на использовании базовых веб-технологий: HTTP-запросах, редиректах, SSL в т.ч. с использованием **отечественных алгоритмов безопасности**.
- Использование OAuth возможно на **любой** платформе с доступом к сети и браузеру: на сайтах, в мобильных и desktop-приложениях, плагинах для браузеров…

Стандарт имеет поддержку крупнейших площадок:

- Портал Госуслуг
- Портал налоговой службы РФ
- Портал госуслуг г.Москвы
- Mail.ru
- Vkontakte.ru
- И многие другие…

Схема авторизации

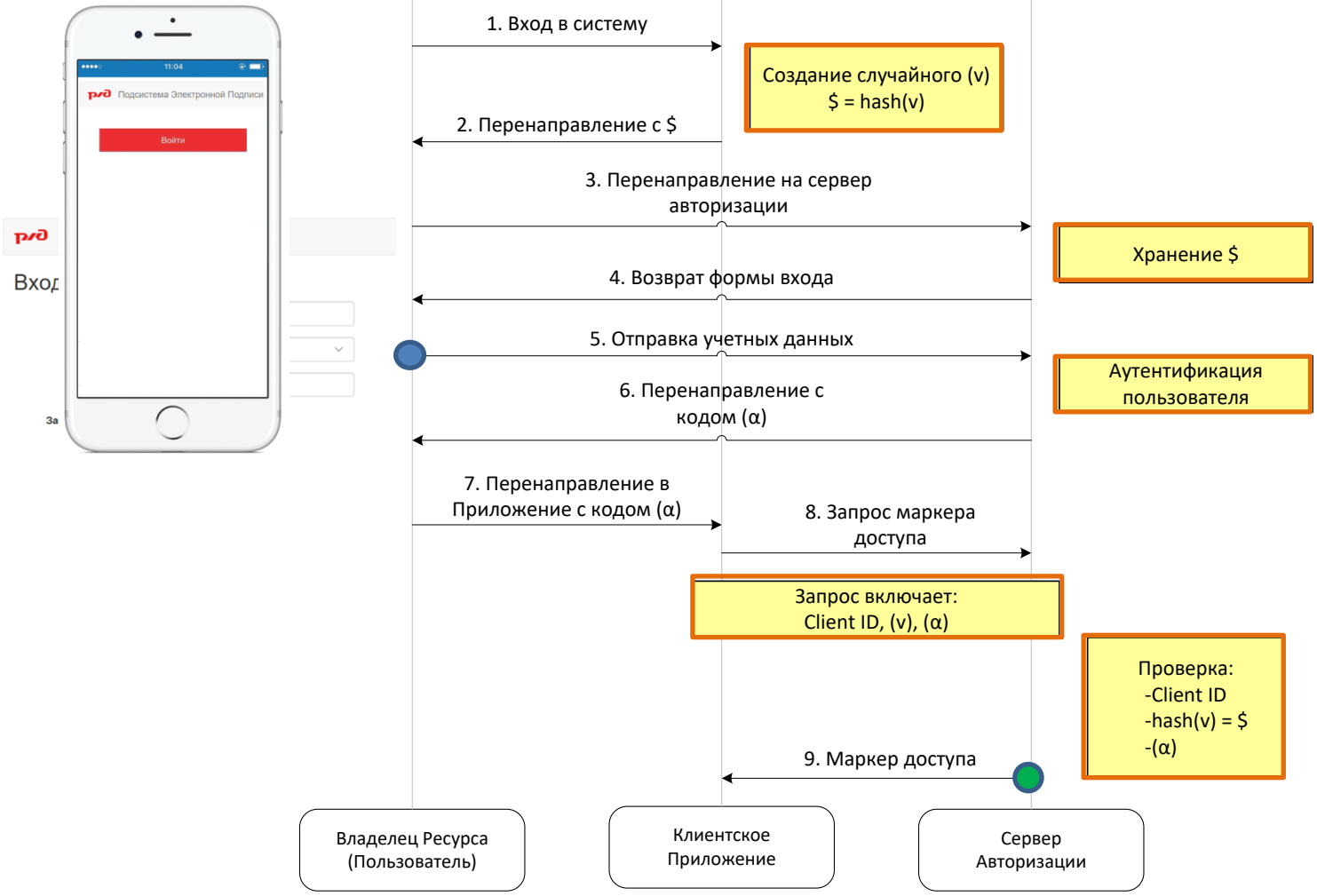


Варианты получения маркера доступа

- Неявный (**Implicit**);
- Пароль пользователя (**Resource Owner Password Credentials Grant**);
- Код авторизации (**Authorization Code**);
- Код авторизации с ключом подтверждения для обмена кода (**Authorization Code with PKCE**);
- Учетные данные клиента (**Client Credentials**).

Код авторизации

с ключом подтверждения для обмена кода



Заключение

- Упрощение процедуры администрирования пользователей
- Возможность аутентификации с использованием УЭП
- Повышение общей защищенности системы с использованием единых механизмов аутентификации
- Упрощение процедур ведения мониторинга и разбора инцидентов ИБ
- Возможность работы с полноценным использованием технологии тонкий клиент
- Безопасная передача логина/ПИН-кода без компрометации на стороне внешних систем с использованием отечественной криптографии
- Использование единой базы клиентов ПЭП для аутентификации во внешних системах

Спасибо за внимание!