



**Вопросы применения инфраструктуры
открытых ключей при использовании
Единого портала государственных услуг**

Электронное правительство

- Новая форма организации деятельности органов государственной власти, обеспечивающая за счет широкого применения информационно-коммуникационных технологий (ИКТ) качественно новый уровень оперативности и удобства получения организациями и гражданами государственных услуг и информации о результатах деятельности государственных органов.

Инфраструктура электронного правительства

- Совокупность автоматизированных и телекоммуникационных систем, обеспечивающих поддержку процессов информационного взаимодействия всех субъектов электронного правительства с целью обеспечения необходимого уровня предоставления государственных услуг

АС федеральных и региональных органов исполнительной власти

- Множество автоматизированных и телекоммуникационных систем, обеспечивающих поддержку отдельных процессов деятельности при предоставлении государственных услуг



Масштаб - проект должен обеспечивать работу сотен систем по всей территории РФ



Динамика – проект реализуется в предельно короткие сроки



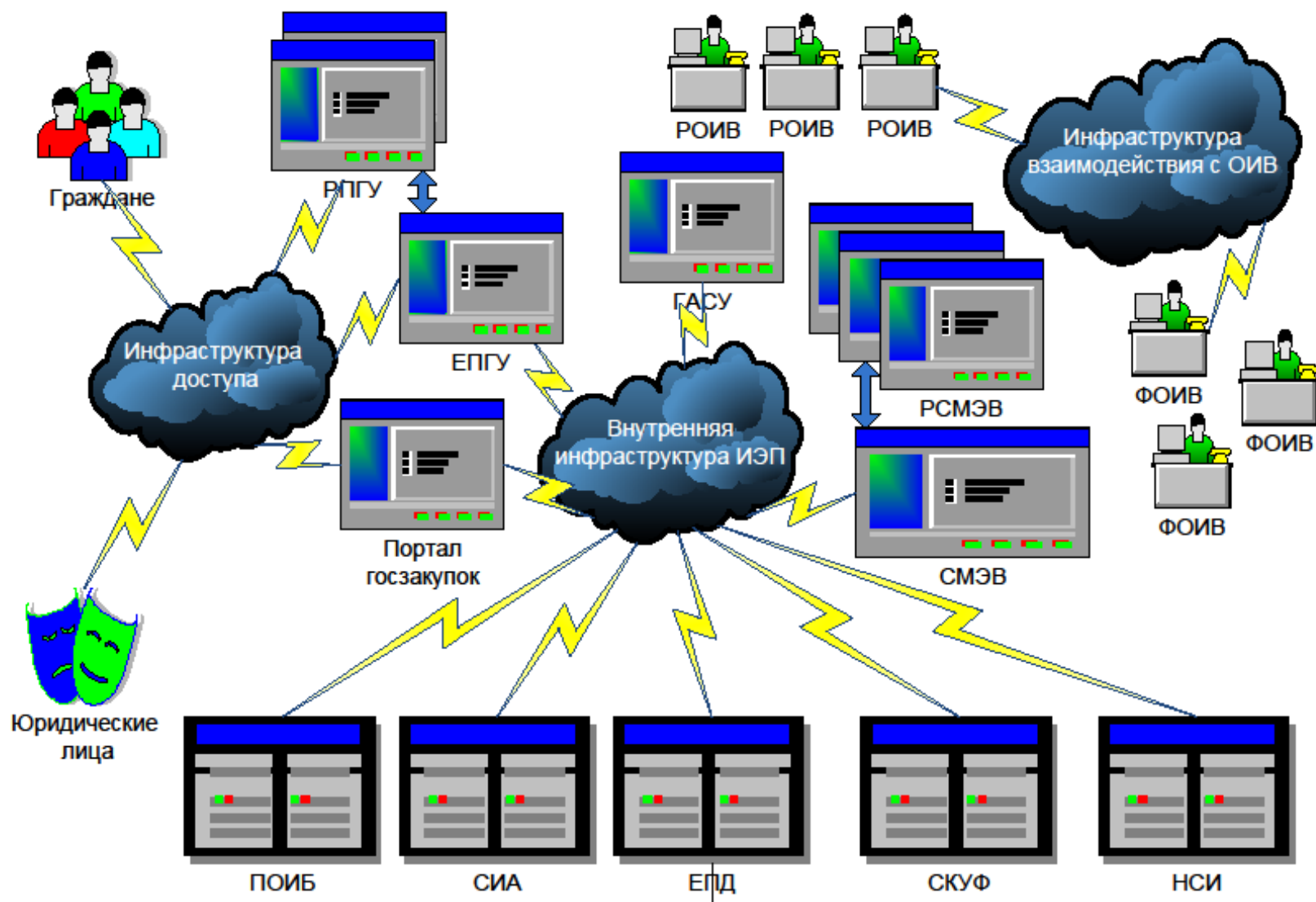
Массовость – услуги должны предоставляться всем



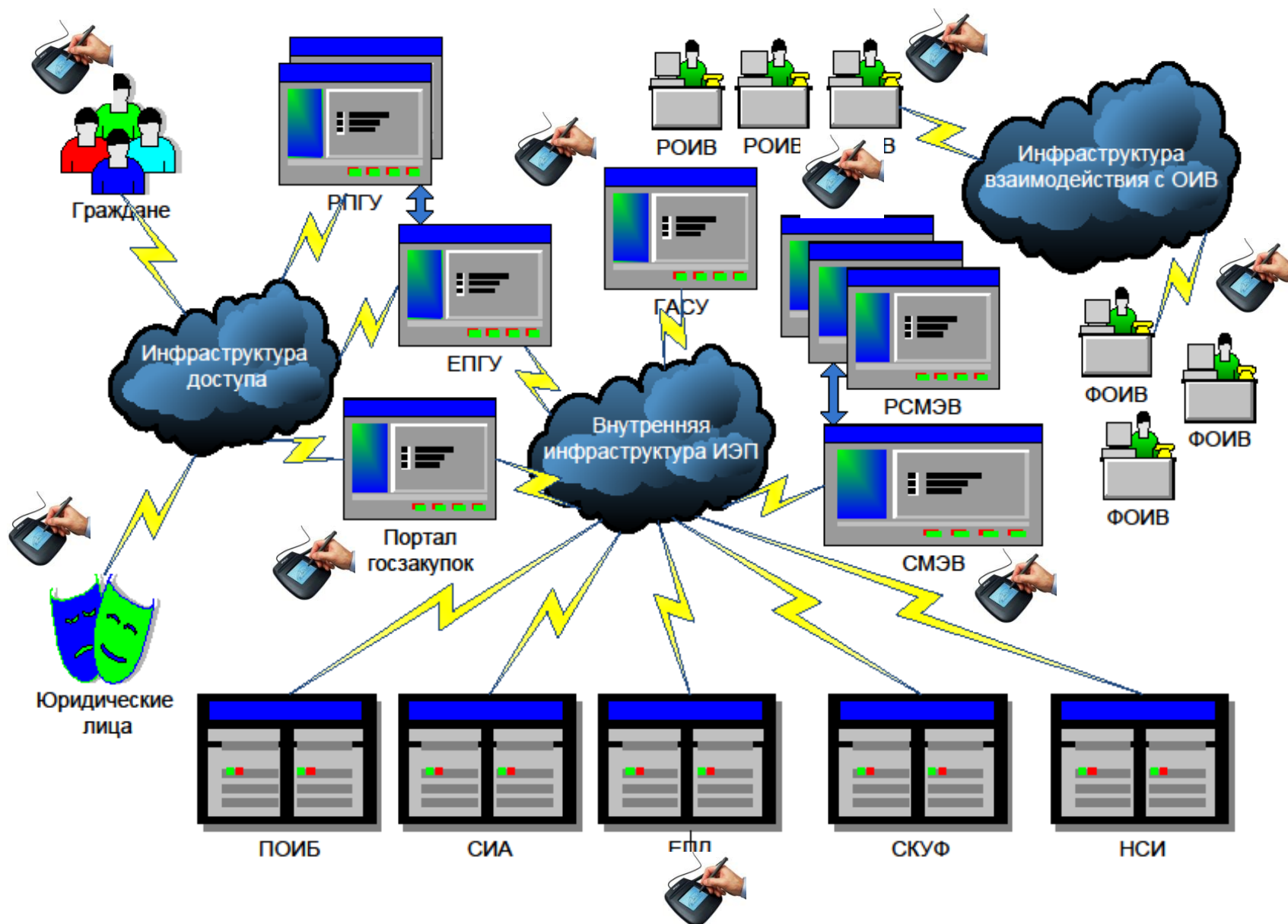
Неоднородность – проблемы информационного неравенства и отсутствия стандартизации



Проблемы с нормативным обеспечением



ИЭП- применение электронной подписи





Пользователи ЕПГУ

- Среднемесячное посещение портала 7 млн. чел
- Активировали личный кабинет 1 млн чел.



Услуги ЕПГУ

- На Портале размещено 20 676 услуг, из них:
 - Федеральных услуг: 935
 - Региональных услуг: 8 815
 - Муниципальный услуг: 10 911
 - Прочие услуги: 15
- В электронном виде предоставляется 191 услуг, из них:
 - Федеральных : 103
 - Региональных услуг : 98





Обеспечение взаимной идентификации и аутентификации пользователей с ПГУ

Обеспечение ЭП запросов к ПГУ

Обеспечение конфиденциальности передаваемых ПД

Обеспечение контроля пользовательской среды

Определение политик доступа в соответствии с типом услуги и способом доступа к ПГУ

Аудит действий пользователей ПГУ



Компьютер

- Обеспечение взаимной идентификации и аутентификации пользователей с ПГУ
- Обеспечение ЭП запросов к ПГУ
- Обеспечение конфиденциальности передаваемых ПД
- Обеспечение контроля пользовательской среды
- Определение политик доступа в соответствии с типом услуги и способом доступа к ПГУ
- Аудит действий пользователей ПГУ



Мобильное устройство

- Аутентификация пользователя – по одноразовому паролю, сервера – средствами GSM/3G
- ЭП на стороне оператора (HSM)
- Конфиденциальность данных обеспечивается средствами GSM/3G и VPN между мобильным оператором и ГПУ
- Контроль пользовательской среды невозможен
- Контроль прав доступа осуществляется средствами мобильного оператора и средствами ИЭП (СИА и ПОИБ)

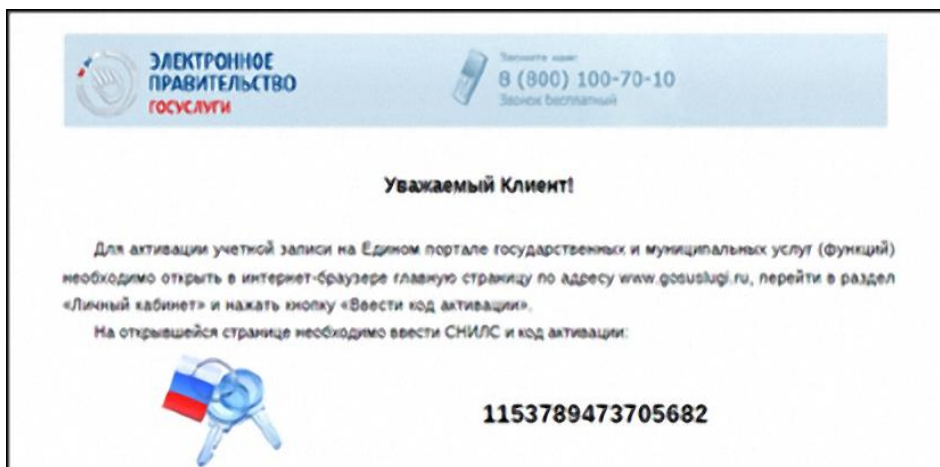


Инфомат

- Аутентификация пользователя по паролю, сервера – по VPN-ключу
- ЭП на внешнем устройстве (токене, карте)
- Конфиденциальность данных обеспечивается VPN туннелем
- Контроль пользовательской среды оператором инфоматов
- Контроль прав доступа и аудит осуществляется средствами ИЭП (СИА и ПОИБ)

Возможности:

- выдача кода активации Личного кабинета пользователю портала государственных услуг;
- выдача носителя с электронной подписью пользователю портала государственных услуг.



Один или много УЦ

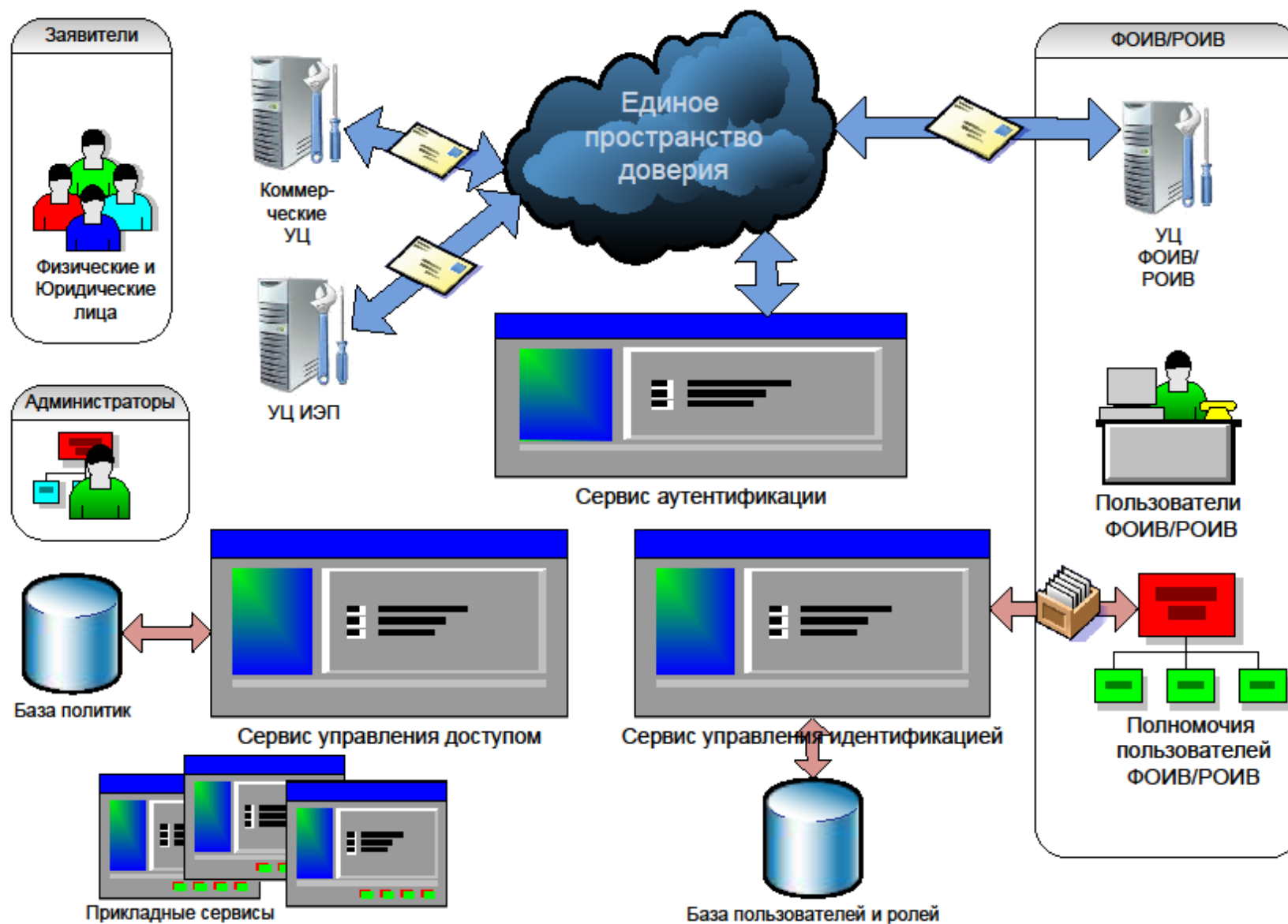
- Более полный контроль процессов
- Массовое применение технологии

Централизованное или локальное хранение ключей

- Большая надежность хранения и универсальность доступа
- Локализация рисков компрометации и унификация механизмов

Полномочия в рамках УЦ или отдельно

- Возможность множественных или неактуальных полномочий
- Проблемы производительности и масштабируемости





Обеспечить идентификацию заявителя

Использовать средства с неизъемаемыми ключами

Работа с системой мониторинга «в реальном времени»

Решение проблемы управления полномочиями

Страхование рисков

Нормативное обеспечение (регламент присоединения, регламент контроля деятельности)



Назначение

- Обеспечение аутентификации при взаимодействии участников услуг электронного правительства
- Обеспечение механизмов использования ЭЦП
- Обеспечение доверенного времени

Состав

- Удостоверяющие центры регионов, ведомств и независимые УЦ
- Система взаимной проверки УЦ на основе списка доверенных УЦ
- Мониторинг УЦ
- Система предоставления доверенного времени
- Нормативная база и регламенты взаимодействия



Портал государственных услуг является ключевым элементом инфраструктуры электронного правительства

Обеспечение информационной безопасности при доступе к portalу государственных услуг является сложной задачей и требует применения нестандартных комплексных решений

Идентификация, аутентификация и подтверждение – ключевые сервисы инфраструктуры электронного правительства, реализуемые с помощью системы удостоверяющих центров

Работа удостоверяющего центра в интересах портала государственных услуг накладывает дополнительные ограничения на удостоверяющий центр и может потребовать формирования дополнительных сервисов

Функционал ЕПД должен быть существенно расширен в сторону контроля УЦ, входящих в ЕПД

Наряду с ЕПД ключевым элементом является сервис определения полномочий, реализуемый в рамках СИА

СПАСИБО ЗА ВНИМАНИЕ!

