

# Предоставление государственных услуг и электронная идентификация

## Система идентификации Общероссийского государственного информационного центра

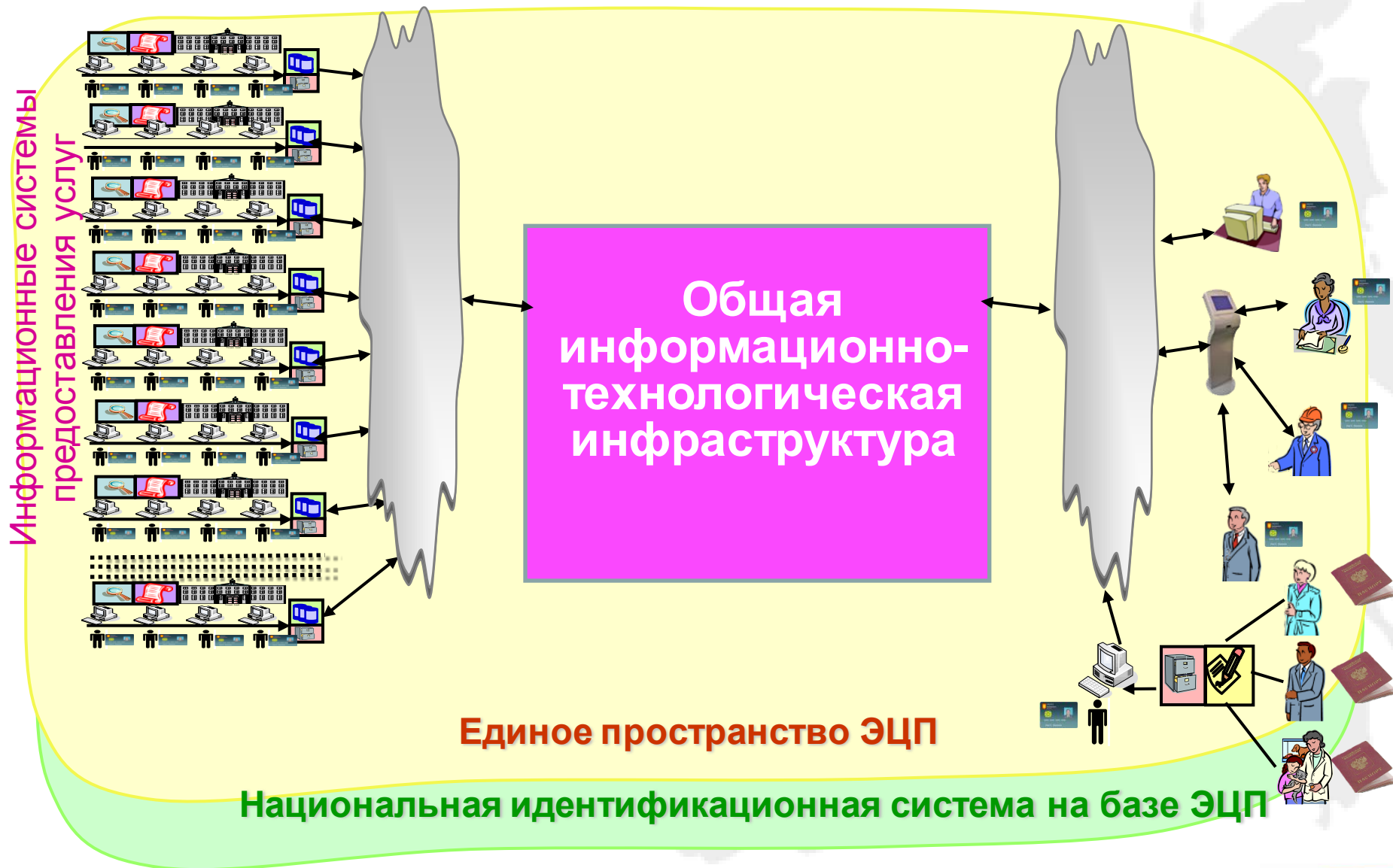
### Общие подходы

# Системы идентификации в РФ



- Паспорт
- Ведомственные идентификаторы (ИНН, СНИЛС и пр.)
- Идентификаторы коммерческих систем (банки)
- Социальные карты

# Технологическая инфраструктура «электронного государства»



# Идентификационная система

- Построена на инфраструктуре РКІ
- Состоит из распределённой системы удостоверяющих центров, системы эмиссии и технологических регистров
- Технологически может объединяться с другими системами
- Позволяет осуществлять взаимодействие с существующими ведомственными системами

# Системные требования

## Обязательные

- Идентификация и аутентификация пользователя
- Аутентификация терминала идентификатором
- Реализация ЭЦП

## Желательные

- Возможность размещения дополнительных электронных приложений
- Возможность нанесения полиграфической информации
- Бесконтактный интерфейс

# Идентификация

- Данные для идентификации:
  - ФИО + место жительства (ст. 19-20 ГК РФ)
  - Сертификат
  - Номер (идентификатор)
- Носители:
  - Сам человек
    - пароли
    - биометрия
  - Внешний носитель
    - RFID, контактная метка, карта памяти, смарткарта
    - USB-устройство
    - КПК, смартфоны, коммуникаторы
    - прочие (штрихкод, номер...)

# Аутентификация

- Аутентификация
  - по субъекту:
    - Оператором
    - Автоматически
  - по используемому признаку:
    - Что мы знаем (пароли, ПИНЫ...)
    - Что у нас есть (карта, токен...)
    - Кто мы (отпечаток пальца, 2D и 3D лицо...)
  - по степени защиты:
    - Простая
    - Усиленная (ОТР)
    - Строгая (2 и более факторов)

# Крайне заманчивая идея

## Человек (биометрия) + пароль

### Почему не подходит:

- проблемы технологии (ошибки 3 рода)
- уровень развития (FAR/FRR, защита от муляжей)
- затраты на терминальную сеть
- только онлайн (нужны БД)
- не решает проблему ЭЦП



# Крайне заманчивая идея № 2

## Существующие идентификаторы (паспорт)

### Почему не подходит:

- не предназначен для машинного распознавания
- сложности с распознаванием подделок
- не решает проблему ЭЦП

# Идентификационный элемент ОГИЦ

- Технические характеристики
  - Контактный интерфейс ISO 7816
  - Бесконтактный (радио) интерфейс ISO 14443
  - EEPROM – 66 Кбайт
  - 1088 – битовый криптографический сопроцессор для криптографии с открытым ключом
- Соответствие международным стандартам
  - ISO 7816, 14443-1,2,3,4
  - PKI for Machine Readable Travel Documents offering ICC Read - Only Access (Version 1.1. October 01, 2004)
- Обеспечение безопасности карты
  - Сертификация криптомодуля в уполномоченных российских компетентных органах
  - Сертификат соответствия стандарту ISO/IEC 15408 (Common criteria) с уровнем доверия EAL 5+



Благодарю за внимание

***ДУНАЕВ Дмитрий Юрьевич***

***Директор ФГУП ВНИИПВТИ***

***Тел. +7 495 235 1919***

***Email: [dunaev@pvti.ru](mailto:dunaev@pvti.ru)***

***Web: <http://pvti.ru>***