ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ «ВОСХОД»

На пороге внедрения удостоверения личности гражданина: баланс между возможностями и безопасностью

Докладчик: Мелузов Антон Сергеевич

Дата: 16 сентября 2014 г.

Удостоверение личности гражданина России

- Распоряжения Правительства Российской Федерации от 19.09.2013 №1699-р (Концепция и план)
  и от 23.09.2013 № 1742-р (Ответственность)

- УЛГ – пластиковая карта с электронным носителем информации
- УЛГ – основной документ, удостоверяющий личность гражданина Российской федерации (в том числе в при электронном взаимодействии)

- Гарантированная идентификация
- Развитие государственных услуг
- Перевод взаимодействия в электронный вид

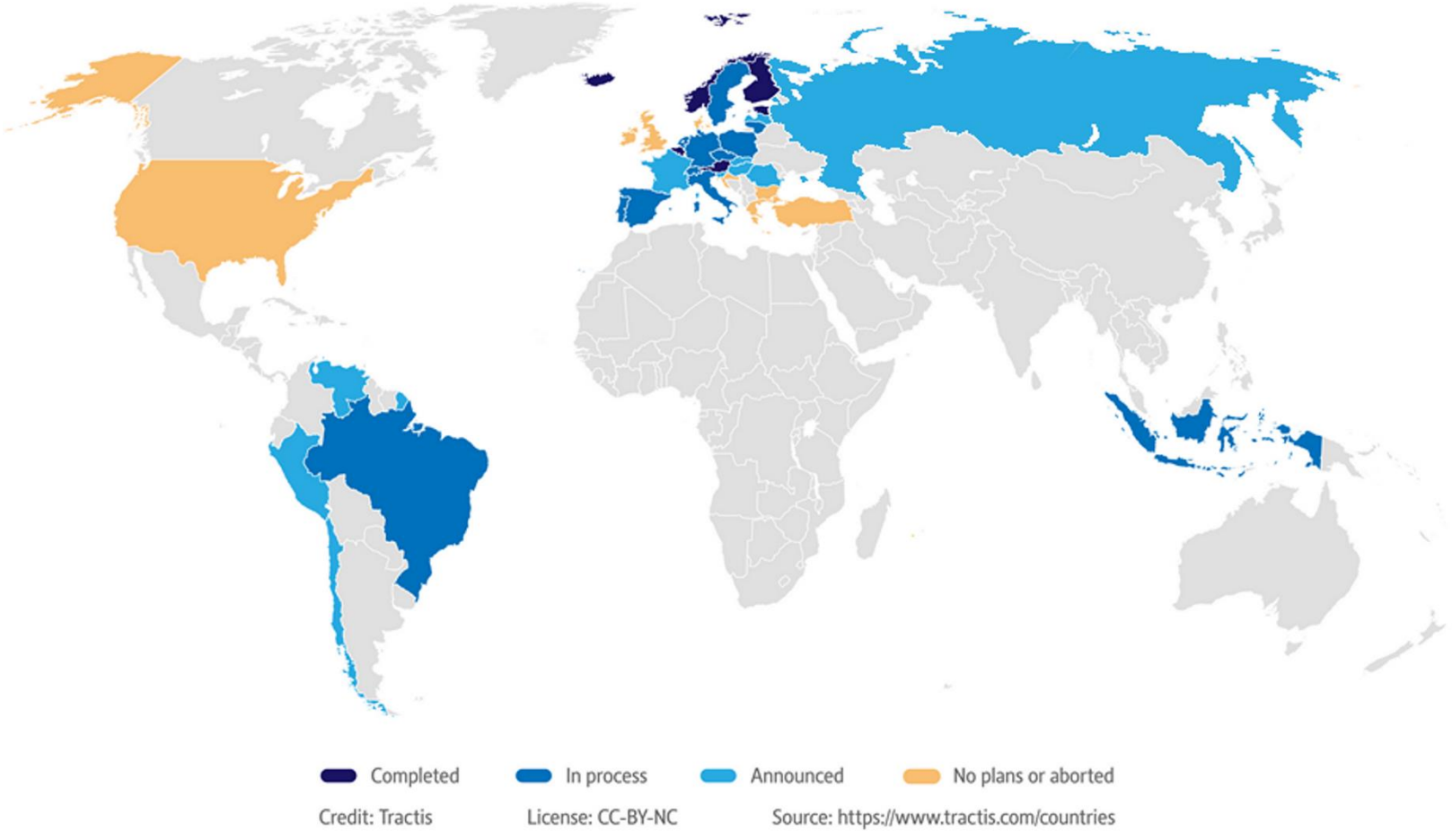
В I квартале 2015 года – выдача первых экземпляров Удостоверений Личности Гражданина и проведение комплексных испытаний в пилотной зоне

1 января 2016 года – начало выдачи Удостоверений Личности Гражданина параллельно с общегражданскими паспортами на территории Российской Федерации

УЛГ

- электронное удостоверение личности, аналогичное общегражданскому паспорту;
- содержит метрические и биометрические данные владельца (в том числе в электронном виде);
- содержит ключи и сертификат КЭП гражданина.

Внедрение электронных документов



Перспективы внедрения УЛГ

- Защита документа от подделки, внесения несанкционированных записей, защита данных паспорта от несанкционированного чтения.

- Усиление связи между владельцем и УЛГ путем внесения биометрических характеристик в УЛГ

- Широкие возможности по использованию электронного документа в различных информационных системах за счет надежной взаимной аутентификации владельца УЛГ и поставщика частных или государственных электронных услуг

- Электронная подпись – каждому гражданину!

Возможности применения УЛГ

- В качестве удостоверения личности – в полиции, в банке, в магазине, поезде, самолете, страховой, МФЦ, ЗАГСе, ФНС, ГИБДД, отделе кадров, военкомате, и т.д. – ускорение работы с локальными информационными системами

- В качестве носителя ключей ЭП, средства формирования ЭП – у каждого гражданина удобный и защищенный ключевой носитель

- В качестве средства доступа к услугам в электронном виде – простая, но надежная аутентификация гражданина, быстрый доступ к данным

Задачи функциональные

- Работа в оффлайн-режиме: легкость и скорость доступа, независимость от каналов связи, интероперабельность

- Работа с онлайн-сервисами: простота для пользователя, простота для разработчика, онлайн-доступ к данным, унификация формата обмена данными

- Работа с ЭП: простота для пользователя, скорость работы.

Задачи информационной безопасности

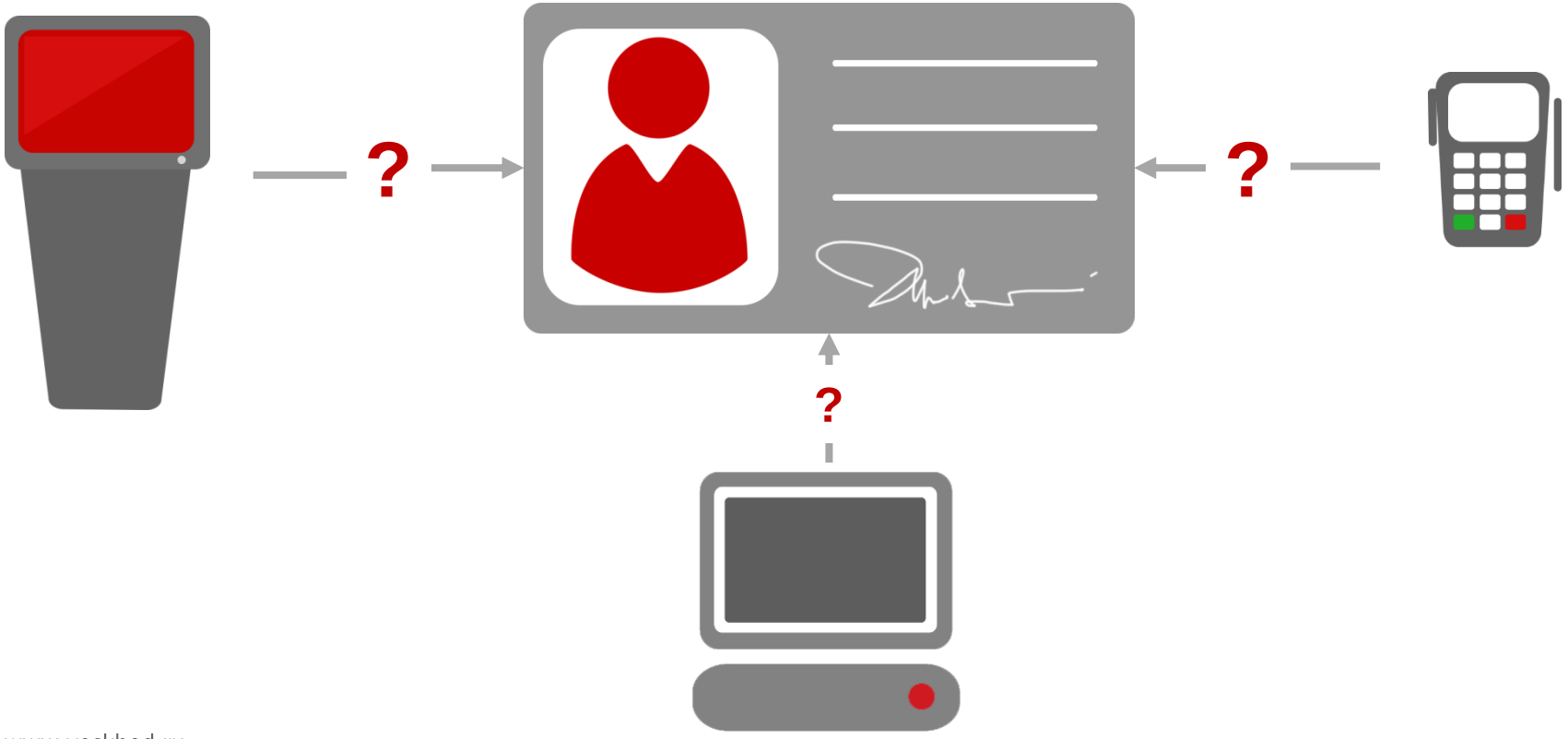
- Защита данных УЛГ от подделки и от несанкционированного доступа

- Обеспечение корректных механизмов разграничения доступа

- Защита системы изготовления, оформления и контроля УЛГ от разнообразных угроз ИБ

Контроль доступа к УЛГ

Организация контроля доступа к данным и функциям Удостоверения Личности Гражданина



Противоречия или архитектурные задачи?

- Легкость доступа для всех
- Доступ только к разрешенным данным

- Электронная подпись «на каждом углу»
- Надежная защита владельца ключей ЭП от махинаций

- Возможность изменения данных при необходимости
- Обеспечение целостности данных

Предлагаемые подходы построению УЛГ

- Три приложения: ePassport, eID и eSign

- Расширенный контроль доступа к данным и функциям на основе cv-сертификатов

- Стандартизация форматов взаимодействия для унификации устройств для работы с УЛГ

Структура УЛГ

Биометрическое приложение

- фото владельца;
- отпечатки пальцев.

Приложение электронного удостоверения личности

- данные; общегражданского паспорта
- ИНН;
- СНИЛС.

Приложение электронной подписи

- СКПЭП;
- функция вычисления КЭП.

Предлагаемые подходы к организации контроля доступа

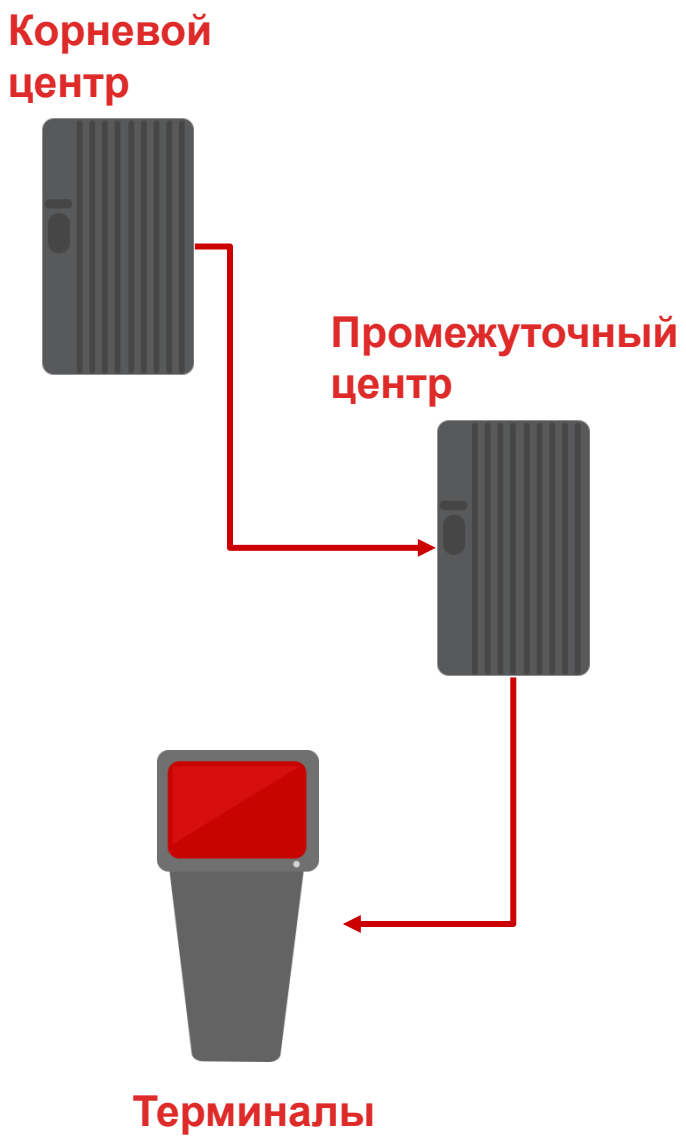
- Применение современных механизмов расширенного контроля доступа

- Учет используемых в настоящее время механизмов (ГС ПВДНП, УЭК)

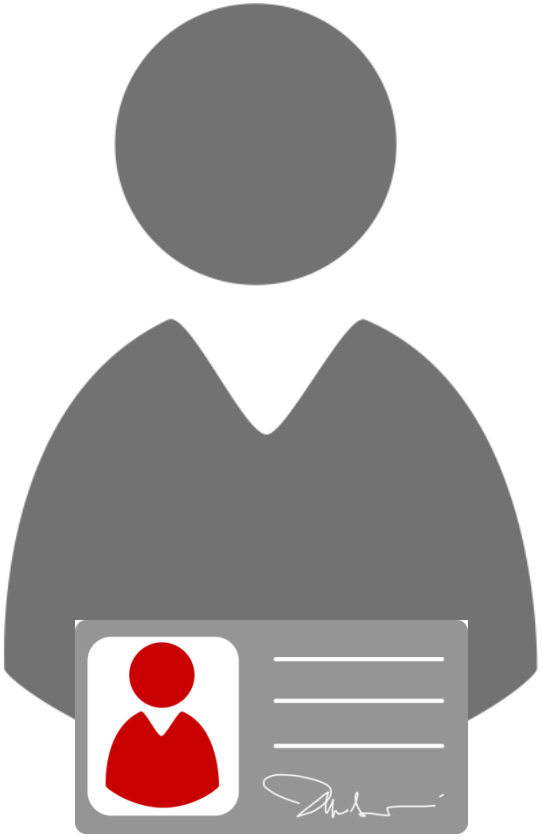
- Адаптация протоколов расширенного контроля доступа для использования отечественных криптографических алгоритмов

Особенности инфраструктуры доступа

- Цепочка доверия у каждого приложения своя
- Трехуровневая структура цепочек
- Возможность работы с документом оффлайн
- Короткий срок действия сертификатов терминалов



Особенности системы паролей



- Обеспечивается невозможность чтения документа без визуального контакта
- Сохраняется возможность чтения данных в случае необходимости, без согласия со стороны владельца
- Для выработки КЭП применяется многофакторная авторизация

Система паролей

Четыре различных «пароля» для использования УЛГ:

<IVANOV<IVAN<<<<<<<<< <043720498398420389334 8	123456	ПИН 1	ПИН 2
Машиночитаемая строка – задается международным стандартом, считывается оптически для доступа к биометрическому приложению.	Код доступа карты – числовой код, печатается на карте, может применяться для доступа некоторых терминалов к идентификацион-ному и биометрическому приложениям.	ПИН 1 – секретный, числовой код для доступа к идентификацион-ному приложению.	ПИН 2 – секретный, числовой код для подтверждения выработки КЭП на ключе владельца.

Терминалы

- Для работы с УЛГ должны использоваться специальные терминалы
- Все терминалы для доступа к УЛГ должны обладать CV-сертификатами
- CV-сертификатом определяются права терминала на доступ к данным и функциям УЛГ
- Взаимодействие с УЛГ требует проведения взаимной аутентификации и установления защищенного соединения

Совместимость решений – разработка рекомендаций в рамках ТК26

- Разработка / адаптация протоколов без применения сопутствующих стандартов / рекомендаций затрудняет независимую разработку

- Единые правила и форматы – совместимость решений
- Стандартные решения – большой выбор решений

- Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в профиле сертификатов открытых ключей в формате CV
- Протоколы взаимной аутентификации электронных документов и терминалов провайдеров услуг на базе ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012
- Методические рекомендации по организации инфраструктуры открытых ключей на базе CV-сертификатов

Дополнительные механизмы для эффективного использования УЛГ

- Частная (ограниченная) идентификация – архитектурное решение для защиты персональных данных и обезличенных списков документов, основанное на криптографических примитивах

- Контроль возраста владельца без разглашения даты
- Контроль места проживания без разглашения адреса

- Смена ключа ЭП по необходимости
- Отзыв документа

Применение ограниченной идентификации

- Иван Иванович серьёзно болен и хочет получить медицинскую страховку.
- В ИС больницы ведется медицинская карта Ивана Ивановича, под местным идентификатором. Связь пациента и карты возможна только при предъявлении УЛГ.
- **Решена задача защиты ПДн при хранении на уровне архитектуры**
- Больница обладает ключом ограниченной идентификации и может работать с картой, если пациент предъявил УЛГ.
- Даже если вся база данных больницы украдена, страховая фирма не может узнать диагноз гражданина, даже при предъявлении им УЛГ в страховой.

Выводы

- УЛГ – инструмент, который открывает перспективы повышения эффективности взаимодействия гражданина, бизнеса и государства
- Взаимная аутентификация и авторизация – важнейший элемент системы обращения УЛГ
- Богатые функциональные возможности и информационная безопасность совместимы, если заложены на уровне архитектуры
- Стандартизация механизмов взаимодействия – путь к совместной открытой работе всех участников рынка над развитием системы эмиссии и применения УЛГ