Росинформтехнологии

Аутентификация и идентификация пользователей ГИЦ

КРИПТО ПРО

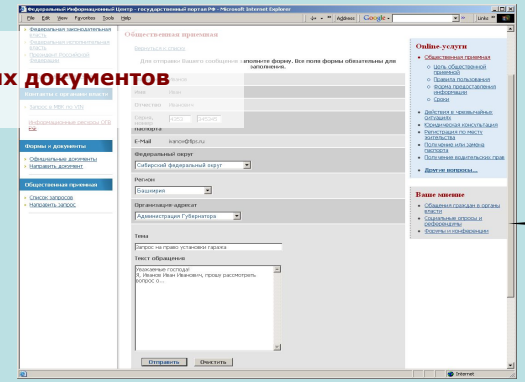
Архитектура публичного контура Государственного информационного центра

Росинформтехнологии

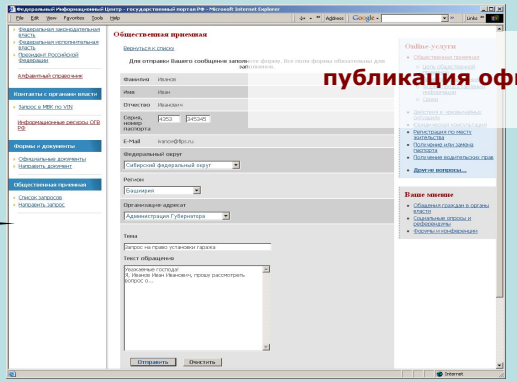
Публичный контур ГИЦ

Открытый сегмент
публичный доступ

информирование
публикация официальных документов
обращения в ОГВ



Защищенный сегмент
авторизованный доступ



информирование
публикация официальных документов
обращения в ОГВ

Интернет
(публичная телекоммуникационная инфраструктура)

Защищенный канал связи

пользователи ведомств

Население, организации

Население, организации

Программно-технические комплексы

Подсистема Аутентификации и Регистрации ФИЦ

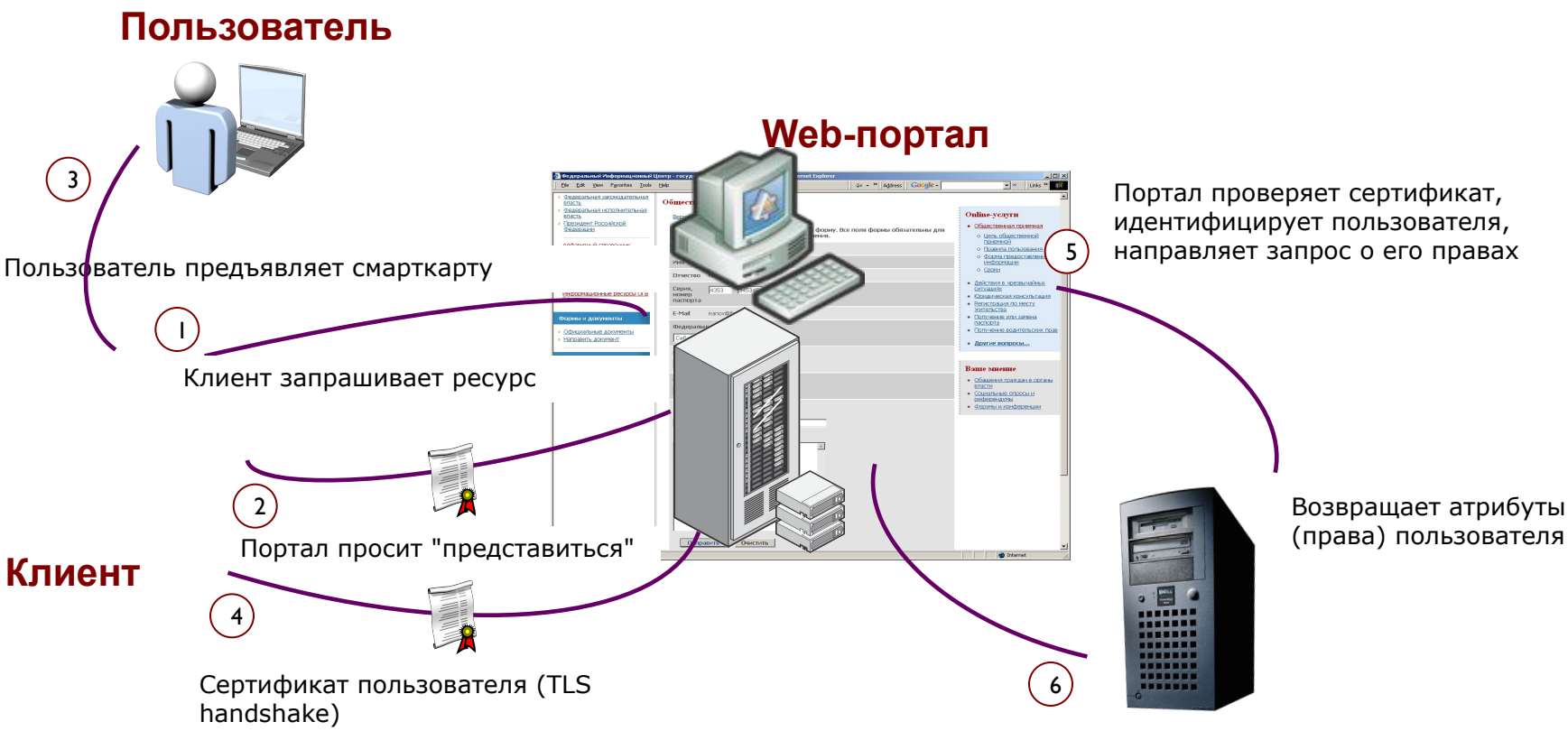
Процедуры аутентификации с использованием сертификатов открытых ключей (ГОСТ)

- взаимная двухсторонняя строгая аутентификация для Web-служб по протоколу TLS с использованием российских криптографических алгоритмов
- Kerberos аутентификация (терминальный доступ, и т. д.)
- RADIUS (EAP-TLS) (PPTP, беспроводные точки доступа, и т. д.)

Единое, общее пространство идентификаторов пользователей

- иерархическая территориально-распределенная подсистема Регистрации Пользователей ФИЦ (LDAP, MS Active Directory), реализованная в виде связанного "леса" ("дерева") Центров Регистрации компонент ФИЦ (федерального, территориальных)

Авторизованный доступ



Центр Регистрации пользователей

Развитие системы идентификации

Росинформтехнологии

Проблемы существующих систем

- отсутствие реализации процедур первичной аутентификации на некоторых платформах с поддержкой российских криптоалгоритмов
- каждая из компонент ФИЦ использует одну или несколько независимых точек входа (проблема централизованного аудита, биллинга)
- жесткие требования к формату (шаблонам) сертификатов открытых ключей пользователей
- механизмы обеспечения распределенности реализуются только через единый связанный каталог (LDAP, MS AD)
- ограниченность информации, предоставляемой сервису в результате идентификации (только аутентифицирующая информация)

КРИПТО ПРО

Развитие системы идентификации

Росинформтехнологии

Кто вы в реальной жизни?

Способ идентификации меняется в зависимости от жизненной ситуации.

Государство - общегражданский паспорт

Граница - паспорт (вы гражданин некоторой страны)

ГИБДД - водительское удостоверение (регион, категория и т.д.)

Услуги - кредитная карта (ФИО, счет, банк)

Разные ситуации (услуги) требуют разных удостоверений с разной информацией

Каждое из удостоверений:

- выдано разными поставщиками удостоверений
- содержит разный набор информации
- ему доверяют разные доверяющие стороны

КРИПТО ПРО

Развитие системы идентификации

Росинформтехнологии

Единое цифровое удостоверение

- сертификат ключа подписи - единый идентифицирующий гражданина электронный "паспорт"
- закрытый ключ, хранящийся на электроном идентификаторе (социальной карте) подтверждение правомерности обладания электронным "паспортом"
- цифровое удостоверение - маркер доступа единого формата (XML)
- метасистема - единообразный способ работы с разными цифровыми удостоверениями, независимо от типа доступа и информации в удостоверении
- веб-сервисы (WS-Security, WS-Trust, WS-MetadataExchange, WS-SecurityPolicy)

КРИПТО ПРО

Авторизованный доступ ГИЦ

Росинформтехнологии

Пользователь

3 Предъявляет смарткарту

Клиент

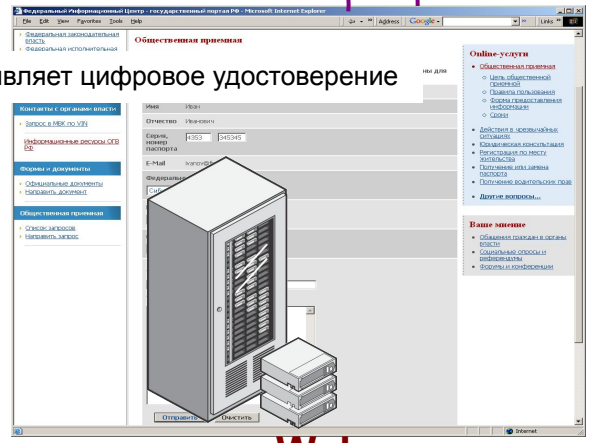
1 Клиент запрашивает ресурс

2 Портал просит представиться с помощью цифрового удостоверения, определяя **перечень поставщиков "доверия"**

4 Запрашивает цифровое удостоверение, предъявляя сертификат пользователя (TLS handshake)

5 Возвращает цифровое удостоверение, содержащее атрибуты/права пользователя и дополнительную информацию

6 Предъявляет цифровое удостоверение



Web-портал

Центр Идентификации
(Identity Provider)
доверенная третья сторона

КРИПТО ПРО

Росинформтехнологии

Развитие системы аутентификации и идентификации

Процедуры аутентификации с использованием сертификатов открытых ключей

- аутентификация с использованием сертификата пользователя (TLS handshake) на Центре Идентификации (доверенная третья сторона) и получение цифрового удостоверения для доступа к конкретному сервису
- решение о доступе к конкретному ресурсу принимается в результате проверки полученного цифрового удостоверения

Единое, общее пространство идентификаторов пользователей

- Центр Идентификации позволяет использовать различные типы сертификатов для аутентификации и создания цифрового удостоверения, обеспечивается уникальность идентификатора пользователя
- Сервис получает с цифровым удостоверением идентификатор, атрибуты пользователя и необходимую ему информацию в стандартизированном виде

Авторизованный доступ ГИЦ

Росинформтехнологии

Решаемые задачи

- авторизованный доступ населения, организаций и ведомств к информационным ресурсам и услугам в соответствии с устанавливаемыми регламентами
- доступ посредством идентификации пользователей с помощью единых универсальных цифровых идентификаторов
- гарантированная криптографическая аутентификация
- предоставление новым сервисам необходимой только им информации, выданной доверенной третьей стороной
- возможность использование информации из цифрового идентификатора для обеспечения юридической значимости электронного документа, заверенного ЭЦП
- возможность масштабируемости сервисов за счет расширения Центров Идентификации
- использование унифицированной электронной карты в качестве идентификатора пользователя ГИЦ

КРИПТО ПРО

Электронный идентификатор

Защищенность

Надежность

Универсальность

- Соответствие международным стандартам
- Соответствие российским требованиям в области информационной безопасности
- Поддержка контактного и бесконтактного (радио) интерфейсов

Электронный идентификатор

Росинформтехнологии

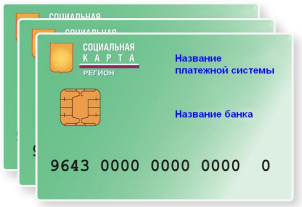
Применение микропроцессорной карты обеспечивает

Приложения идентификационной карты

Социальное идентификационное приложение
- Аутентификация с использованием карты
- Аутентификация персональных идентификационных и социальных данных
- Идентификация держателя карты

Приложение ЭЦП
- Юридически значимый документооборот

Дополнительные приложения
- Платежное приложение
- Транспортное приложение
- Медицинское приложение
- Приложение ЖКХ
- ...



КРИПТО ПРО

Заключение

Росинформтехнологии

Реализованы

- в 2006 году - подсистема Аутентификации и Регистрации ФИЦ, которая в данный момент функционирует и обеспечивает использование сервисов;
- в 2007 - системный проект территориально распределенной системы аутентификации и идентификации пользователей ФИЦ, который определяет пути дальнейшего развития в русле современных информационных технологий.

В 2008 с использованием результатов проекта планируется реализация системы аутентификации и идентификации пользователей ГИЦ.

КРИПТО ПРО