Практика использования электронной цифровой подписи.Основные принципы обеспечения информационной безопасности с использованием инфраструктуры открытых ключей. Архитектура удостоверяющего центра на базе Крипто-Про CSP. Использование ЭЦП для организации защищенного электронного документооборота.

Курепкин И.А., Южанин Н.С.,
Ротков Л.Ю., Соганов С.В

Цели криптографической защиты

- **Аутентификация пользователей**
- **Авторизация доступа к ресурсам**
- **Конфиденциальность информации**
- **Целостность информации**
- **Невозможность отказа от совершенных действий**

Классификация алгоритмов шифрования

- **Симметричные**
  (с секретным, единым ключом, одноключевые, single-key).

Потоковые

- на основе генератора псевдослучайных чисел (ПСЧ)

Блочные

- составные (ГОСТ 28147-89, DES, IDEA, RC5, B-Crypt и др.)

- **Асимметричные**
  (с открытым ключом, public-key)

- Эль-Гамаль ElGamal

Процедура создания ЭЦП сообщения

```
Date: Apr 04 2002 11:02
From: Иванов А.В. <iab@mail.ru>
To: Петров В.К. <pvk@hotmail.ru>
Subject: Received file
```

Целостность сообщения проверяетс вычислением контрольной функции (check function) от сообщения - некоего числа небольшой длины. Эта контрольная функция должна с высокой вероятностью изменяться даже при малых изменениях сообщения (удаление, включение, перестановки или переупорядочивание информации). Называют и вычисляют контрольную функцию по-разному: букву буквой, отстоящей от исходной на три

$M \rightarrow H(M) = h$

S

$S = D_Z(h)$

ЭЦП

«дайджест» документа (хэш-функция), однозначно идентифицирует содержимое документа

автор документа **шифрует дайджест** своим персональным закрытым ключом - **Z**

Сертификат открытого ключа

Сертификат представляет собой документ, подтверждающий
ьных атрибутов
й Удостоверяющим

Версия: 3
Имя Пользователя: C=RU, org=ACME, cn=UserName
Имя Издателя: C=RU, org=ACME, cn=CA
Номер Сертификата: #12345678
Алгоритм ЭЦП: GOST R 34.11-94/ R 34.10-94 (1.2.643.2.2.4)
Открытый ключ пользователя
- **Алгоритм ключа:** GOST R 34.10-94 (1.2.643.2.2.20)
- **Значение ключа:** 01001110100100101001010 1

Сертификат действует с: 01.01.2001 00:00:00
Сертификат действует до: 31.12.2006 23:59.59
Дополнительная информация (X.509 v3 Extensions)
- **Регламент использования сертификата:** Корпорация ACME
- **Секретный ключ действует с:** 31.12.1999 23:59.59
- **Секретный ключ действует до:** 31.12.2000 23:59.59
- **Область применения ключа:** Защита почты (1.3.6.1.5.5.7.3.4)
- **Область применения ключа:** Аутентификация клиента (1.3.6.1.5.5.7.3.2)
- **Атрибуты пользователя:** IP, DNS, URI, RFC822, Адрес,...

Подпись Центра Сертификации:
- **Алгоритм:** GOST R 34.11-94/ R 34.10-94 (1.2.643.2.2.4)
- **Значение:** 01001110100100101001010 1

```
er,


DEFAULT v1,
Number,
er,


nfo,
entifier OPTIONAL,
rsion shall be v2 or v3
entifier OPTIONAL,
rsion shall be v2 or v3
ns OPTIONAL
rsion shall be v3
```

Инфраструктура PKI

Позволяет реализовать:

- Защищенная электронная почта:

Шифрование ЭлД открытым ключом получателя заверенным сертификатом УЦ

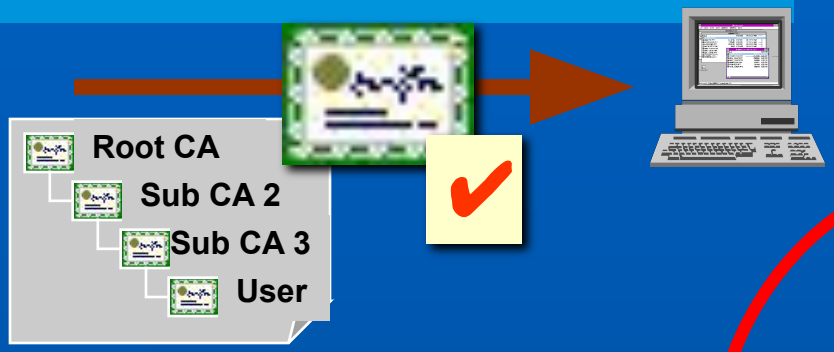
- Защита соединений в Интернете:

Выработка общего секретного ключа сессии с помощью открытых ключей сервера и клиента заверенных сертификатом доверенного УЦ

- Контроль ПО (Authenticode)

Проверка целостности ПО с по мощью открытого ключа фирмы-производителя заверенного сертификатом УЦ

Проверка сертификата



Тип сертификата

Сертификат разрешено использовать в данном режиме.

Срок действия

Сертификат действителен в данный момент.

Целостность

Цифровая подпись CA, выдавшего сертификат, верна.

Легитимность

Сертификат не был отозван.

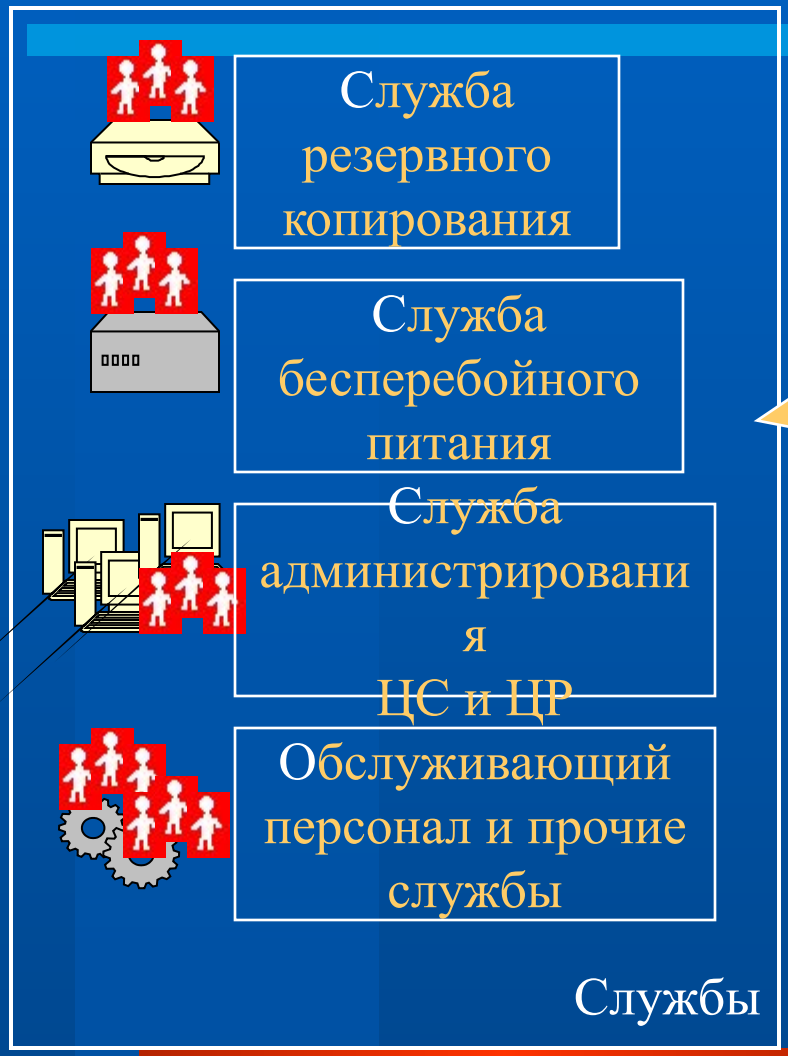
Запреты

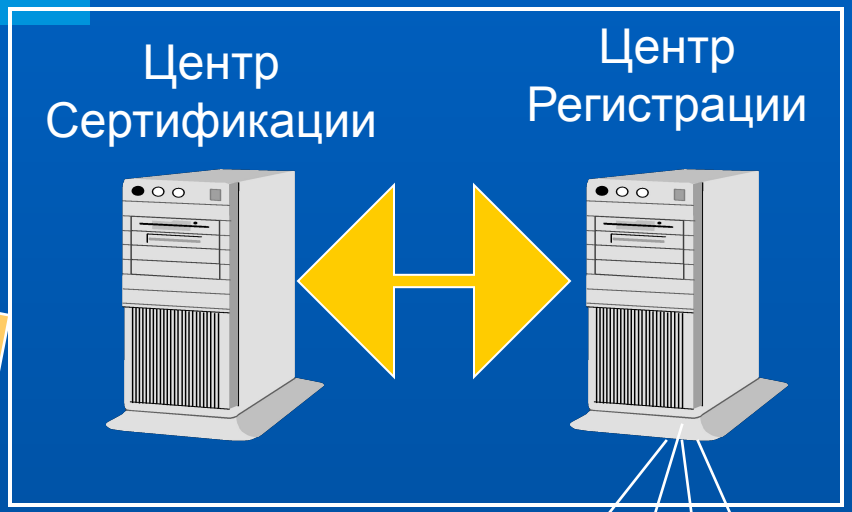
Списки CTL не запрещают использование сертификата для данной задачи.

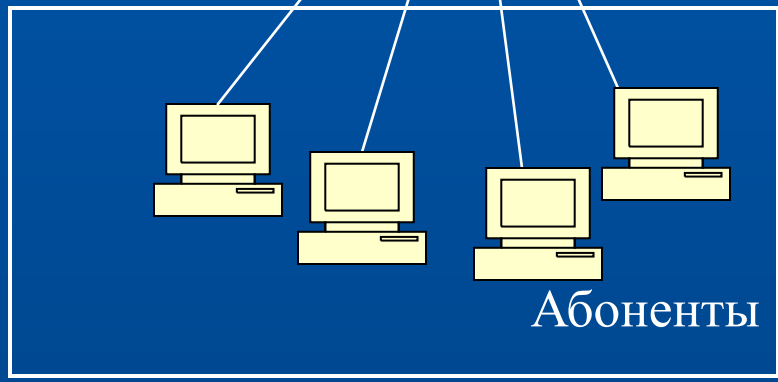
Доверие

Сертификат корневого CA присутствует в хранилище Trusted Root Certification Authorities.

Структура удостоверяющего центра







Службы сертификации Microsoft

- **Центр сертификации (Certification Authority)**
  - **Выдача сертификатов клиентам**
    - **Генерация ключей, если нужно**
  - **Отзыв сертификатов**
    - **Публикация списка отзыва сертификатов (Certificate Revocation List)**
  - **Хранение истории всех выданных сертификатов**
- **Web-сервис (Web Enrollment Support)**
  - **Запрос и получение сертификата через Web-интерфейс**

Отсутствие реализации
отече
крипто

Отсутствие аутентификации
пользователя
центру сер

Трудности масштабируемости

СКЗИ CryptoPro CSP

- Позволяет использовать стандартные приложения фирмы Microsoft с надежной российской криптографией

- Позволяет создавать новые, надежно защищенные приложения с использованием инструментария разработки фирмы Microsoft

Архитектура криптографических функций Windows

COM интерфейсы

Certificate Services

CAPICOM 1.0

Certificate Enrollment Control

Smart Card Enrollment Control

Приложения

Certification Authority

Outlook Express

Outlook

Authenticode

Internet Explorer

IIS

Интерфейс CryptoAPI 2.0

Цели интерфейса CryptoAPI

Единый интерфейс доступа к криптографическим функциям генерации ключей, формирования/проверки электронной цифровой подписи, шифрования/расшифрования данных.

Не требуется детального изучения особенностей реализации того или иного алгоритма или изменения кода в зависимости от алгоритма.

Изолирование прикладного уровня от криптографических функций позволяет одновременно использовать разные алгоритмы и различные реализации этих алгоритмов, включая аппаратные.

Интерфейс CryptoAPI 2.0

Функции работы со справочниками сертификатов
Certificate Store

Высокоуровневые функции обработки криптографических сообщений
Simplified Message Functions

Функции кодирования декодирования
CryptEncodeObject
CryptDecodeObject

Низкоуровневые функции обработки криптографических сообщений
Low Level Message Functions

Базовые функции Base Cryptography Functions

Cryptographic Service Providers

Cryptographic Service Providers

Cryptographic Service Providers

Microsoft Base Cryptographic Provider v1.0

Crypto-Pro Cryptographic Service Provider

Microsoft Enhanced DSS and

Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider

Gemplus GemSAFE Card CSP v1.0

Microsoft Enhanced Cryptographic Provider v1.0

Microsoft Base DSS Cryptographic Provider

Microsoft Strong Cryptographic Provider

Microsoft Base DSS and Diffie-Hellman Cryptographic Provider

КриптоПро CSP

КриптоПро CSP реализует российские криптографические алгоритмы и разработано в соответствии с криптографическим интерфейсом фирмы Microsoft - Cryptographic Service Provider (CSP).

Операционные системы:
Windows 95, Windows 95 OSR2, Windows 98, Windows 98 SE, Windows ME, Windows NT, Windows 2000, Windows XP, Windows Whistler (beta 2).

Сертификаты ФАПСИ:
СФ/114-0441 от 11 марта 2001 г.
СФ/124-0460 от 20 апреля 2001 г.

Основные функции

- Генерация секретных (256 бит) и открытых (1024 бита) ключей ЭЦП и шифрования;
- Возможность генерации ключей с различными параметрами в соответствии с ГОСТ Р 34.10-94 ("*Информационная технология. Криптографическая защита информации. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма.*");
- Хэширование данных в соответствии с ГОСТ Р 34.11-94 ("*Информационная технология. Криптографическая защита информации. Функция хэширования.*");·
- Формирование электронной цифровой подписи в соответствии с ГОСТ Р 34.10-94 (ГОСТ Р 34.10-01);
- Шифрование данных во всех режимах, определенных ГОСТ 28147-89 ("*Системы обработки информации. Защита криптографическая.*");
- Имитозащита данных в соответствии с ГОСТ 28147-89;
- Использование пароля (пин-кода) для дополнительной защиты ключевой информации.

Ключевые носители

- **дискета 3,5";**
- **российские интеллектуальные карты (РИК) и процессорные карты MPCOS-EMV;**
- **таблетки Touch-Memory DS1993 - DS1996 с использованием устройств Аккорд 4+, электронный замок "Соболь" или устройство чтения таблеток Touch-Memory DALLAS;**
- **реестр Windows;**
- **USB ключ eToken.**

Реализация

СКЗИ КриптоПро CSP может функционировать в двух режимах:

- в памяти приложения.
- в **Службе хранения ключей**, которая реализована в виде системного сервиса Windows.

Удостоверяющий Центр

База - сервис сертификации Microsoft

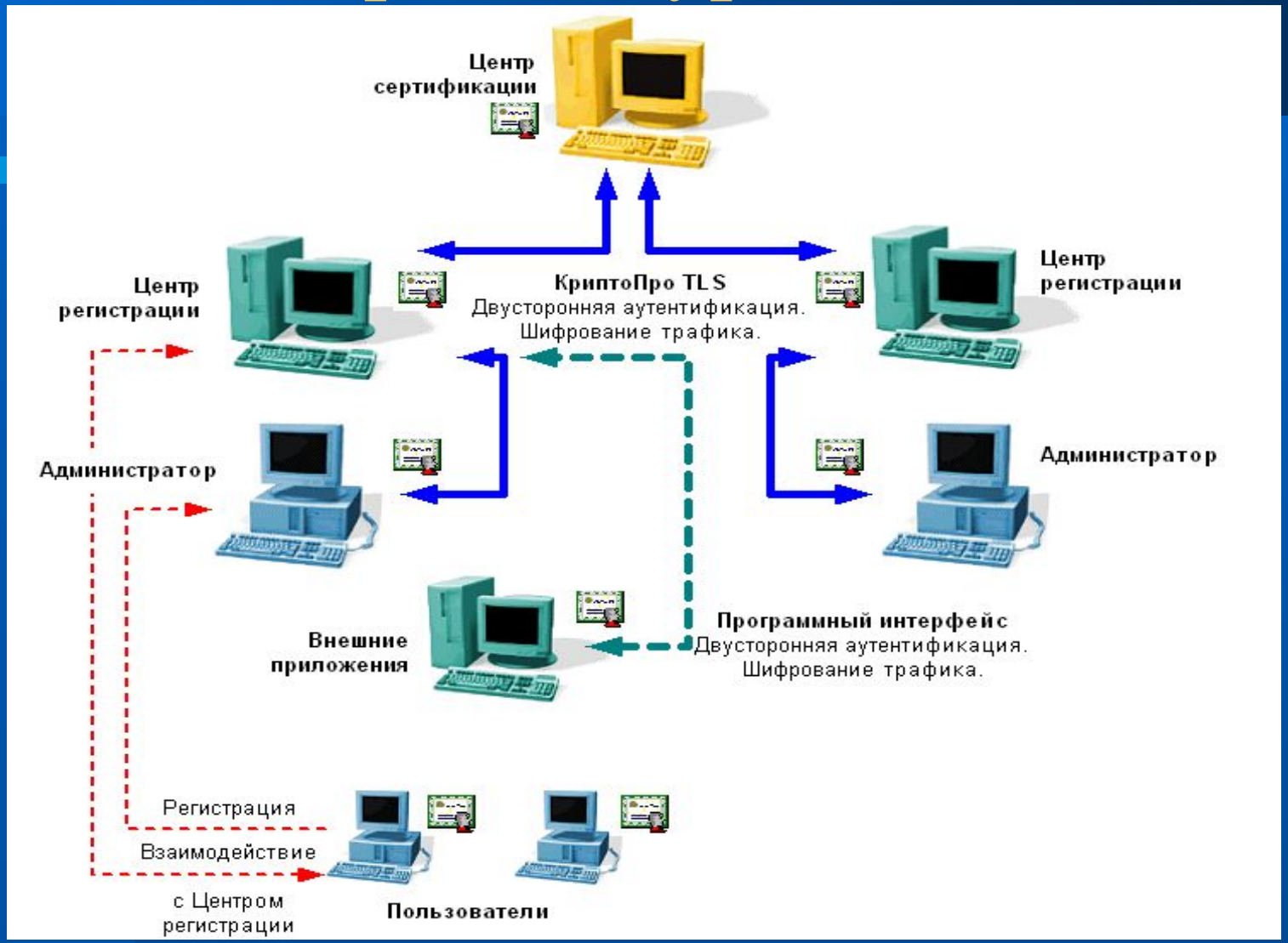
Основные функции:

- -Регистрация пользователей
- -Изготовление сертификатов открытых ключей
- -Ведение реестра сертификатов открытых ключей
- -Управление сертификатами открытых ключей
- -Предоставление владельцам сертификатов функций генерации ключей и управления личными сертификатами

Обеспечивает:

- -Централизованное управление ключевой информацией
- -Распределенное управление ключевой информацией
- -Печать сертификатов на бумажных бланках

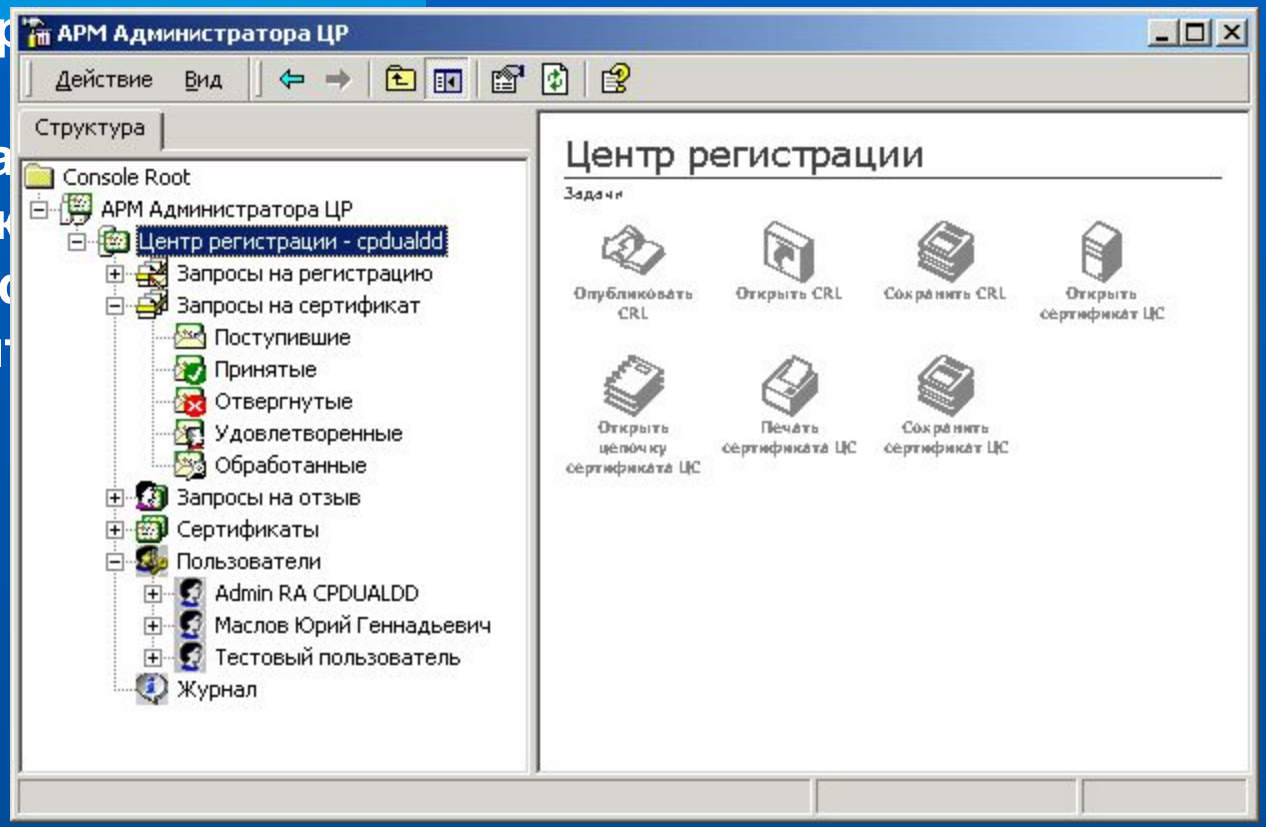
Архитектура УЦ



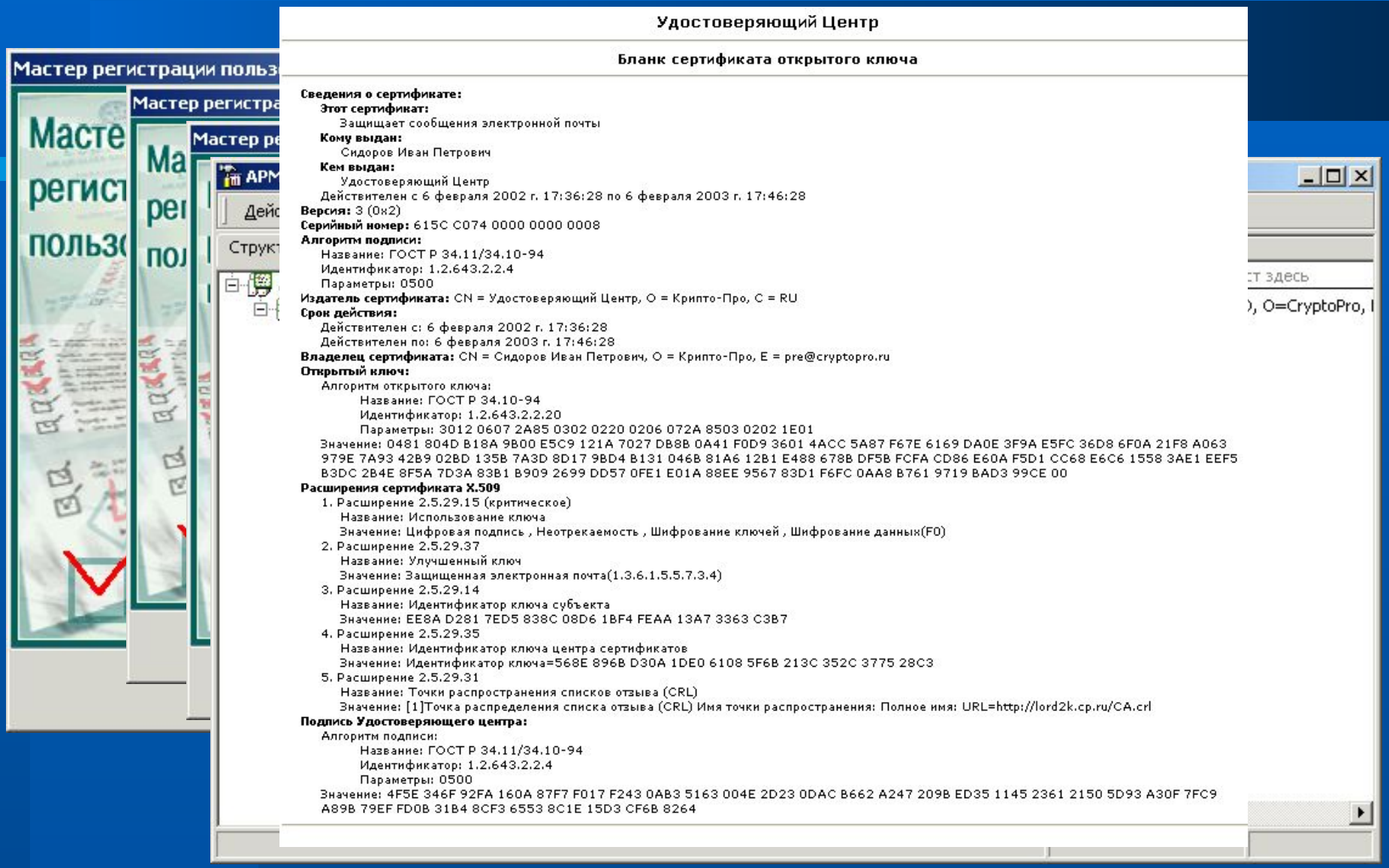
АРМ Администратора

Основные функции:

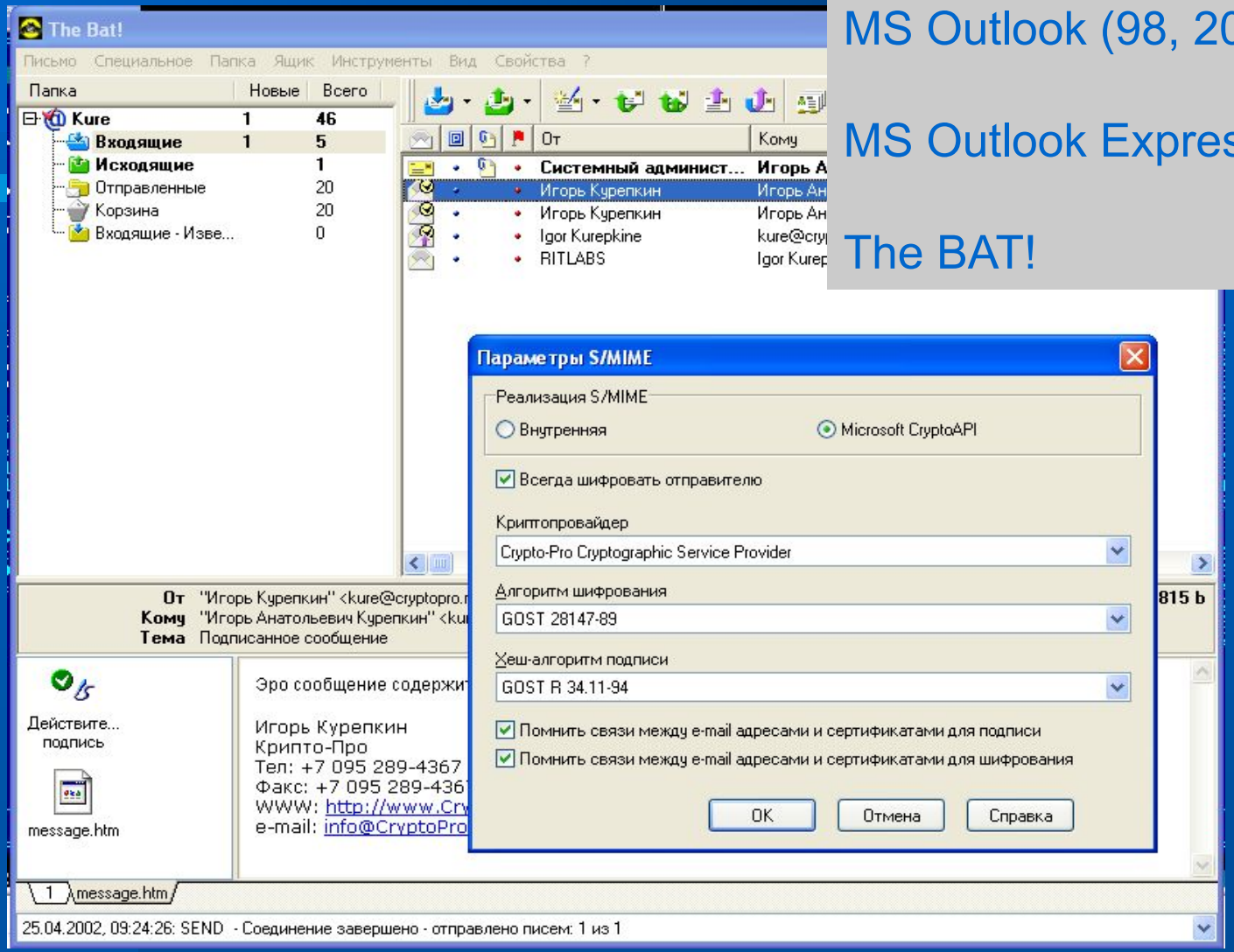
- Регистрация пользователей
- Мониторинг инфор
  сертификатов
- Выполнение регла
  отзывом сертифик
  отозванных сертис
- Аудит работы Цент



Регистрация пользователей



Электронная почта

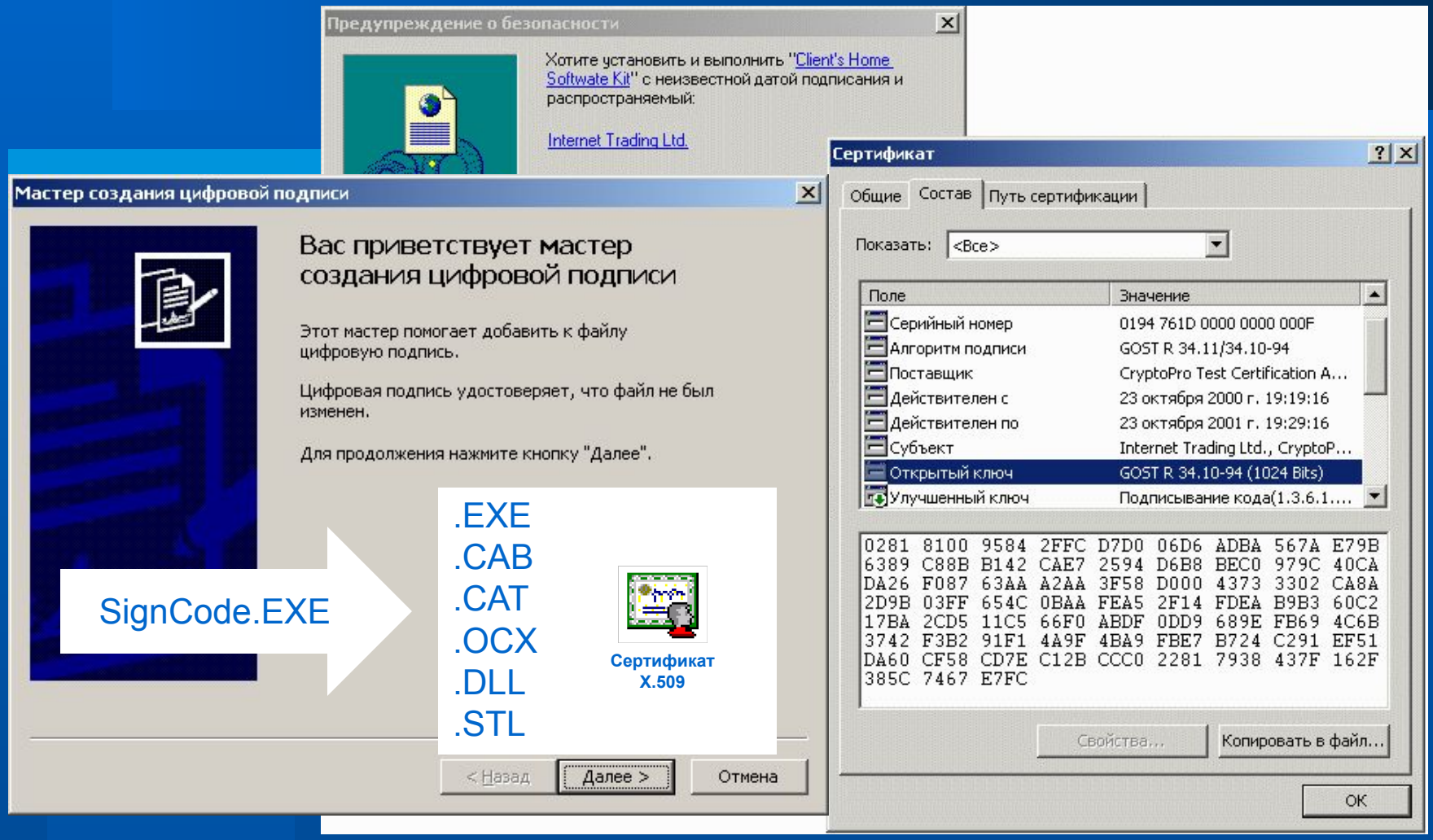


MS Outlook (98, 2000, XP)

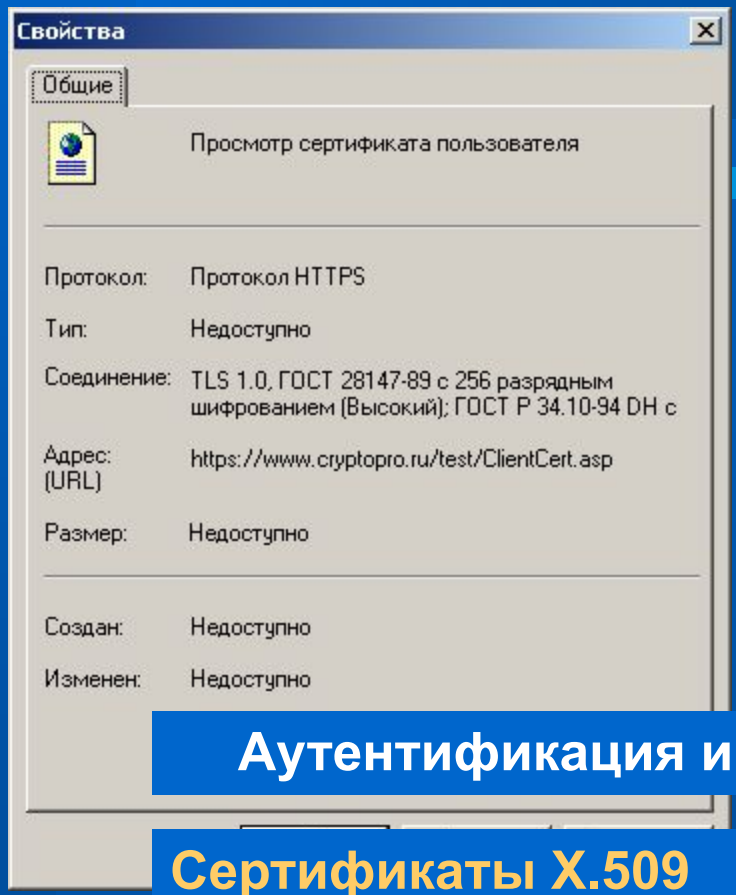
MS Outlook Express

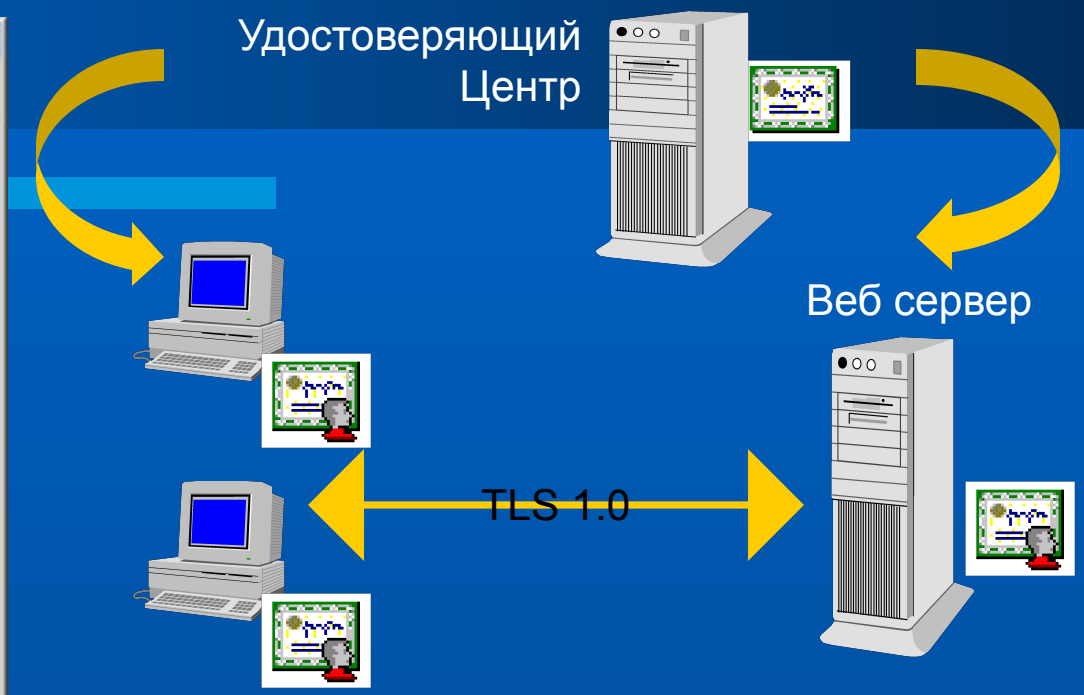
The BAT!

Контроль ПО (Authenticode)



Защита соединений в Интернете



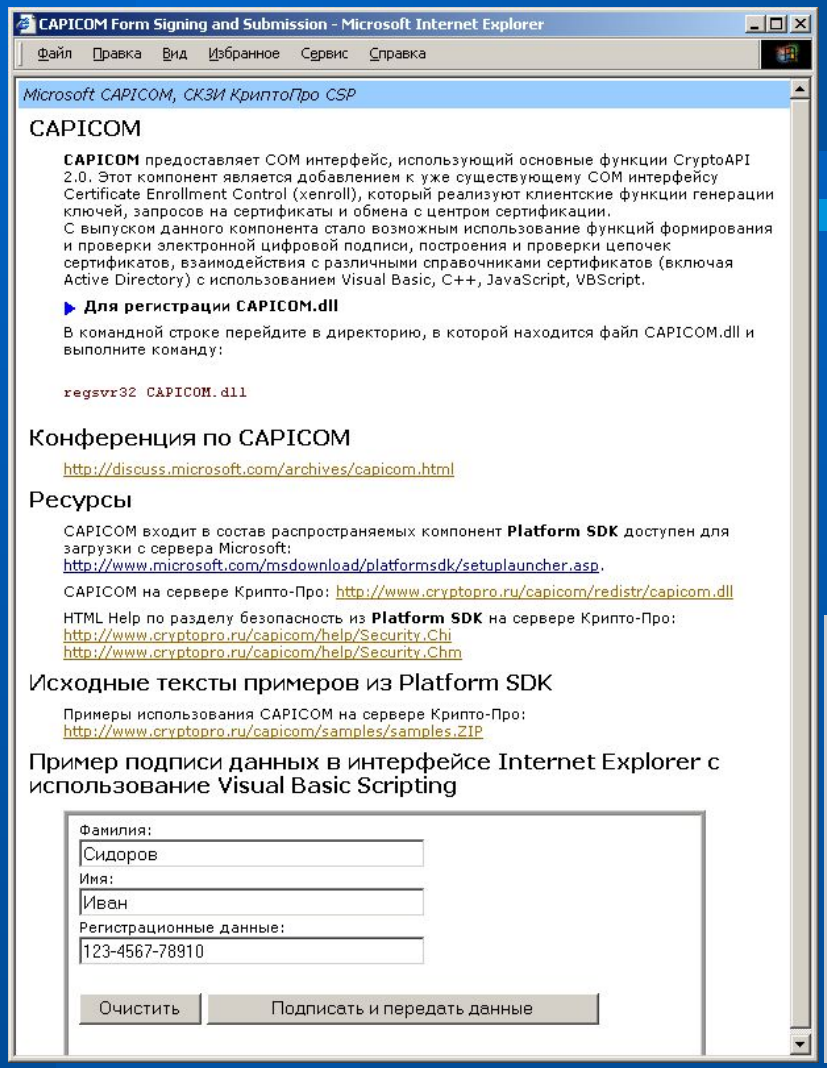


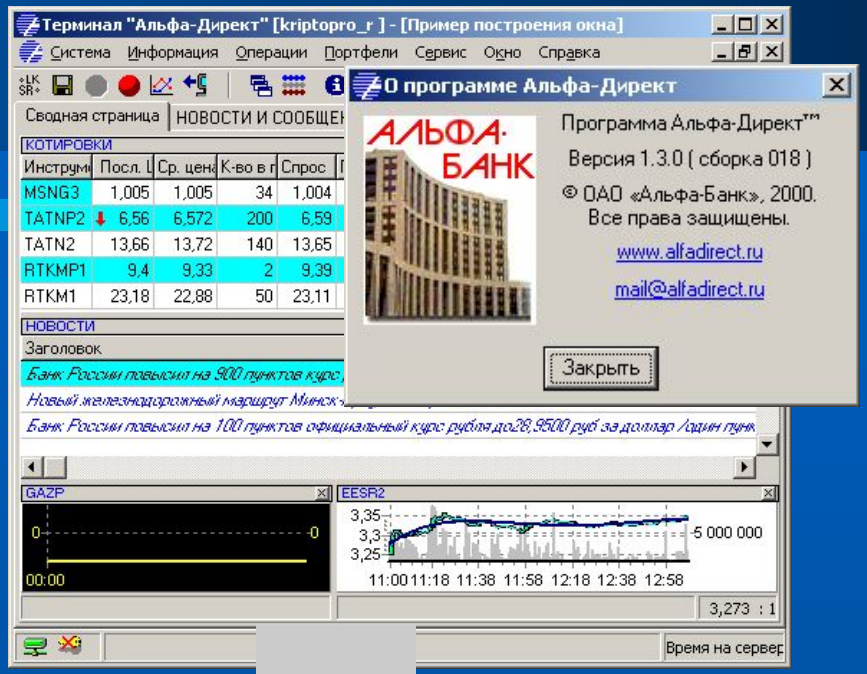
Аутентификация и защита трафика Internet Explorer - IIS

Сертификаты X.509
Аутентификация ГОСТ Р 34.10-94
Шифрование ГОСТ 28147-89
Имитозащита ГОСТ 28147-89

Разграничение доступа к ресурсам сервера на основе данных аутентификации

Приложения





CAPICOM 1.0

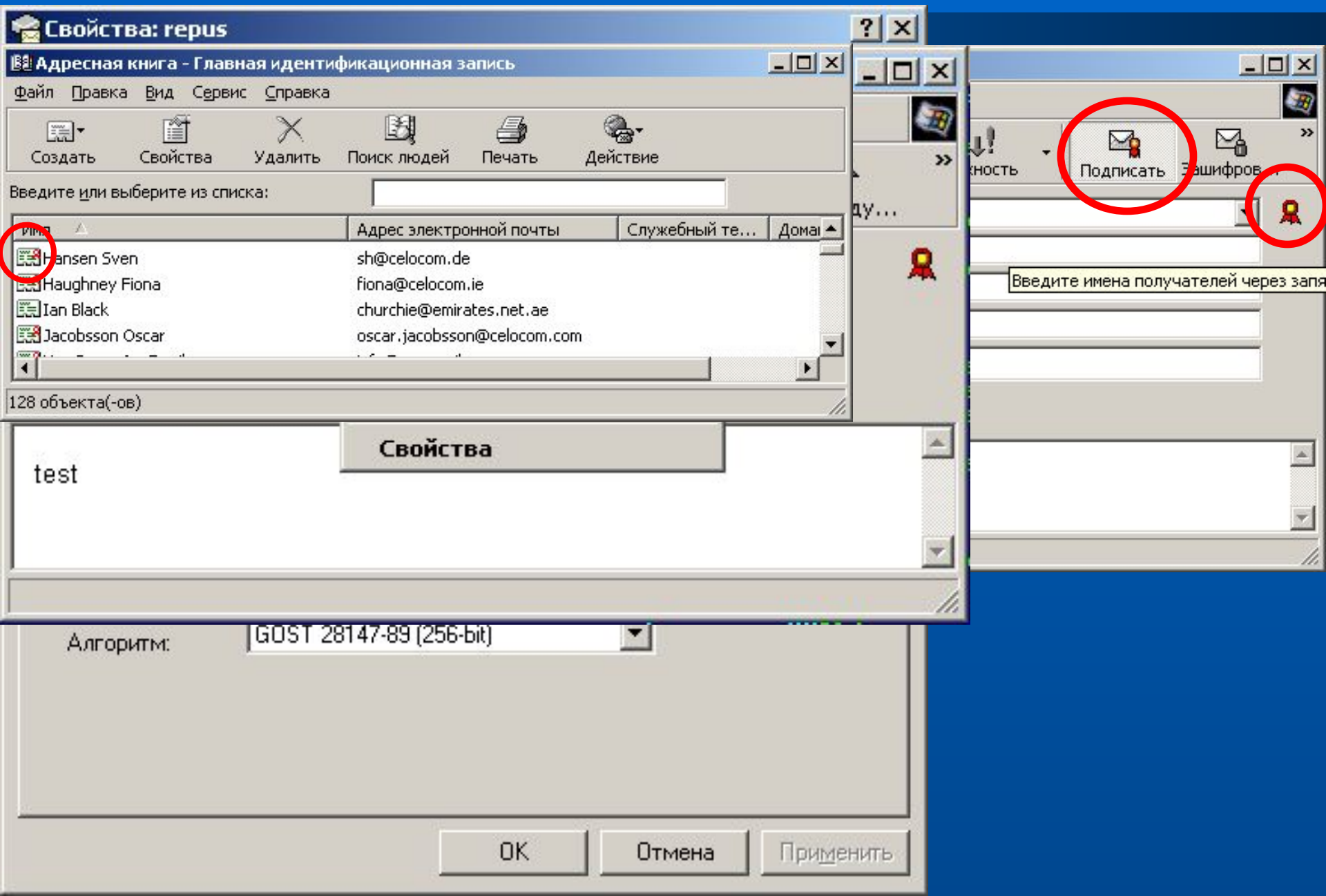
CryptoAPI 2.0
КриптоПро CSP

Интеграция российских алгоритмов

Интеграция российских криптографических средств с RSA Keon

- Интеграция на платформе Windows 2000
- Официальная бета-версия для Windows 2000
- Локализация версии для Windows 2000
- Подготовка версии для платформы Sun Solaris

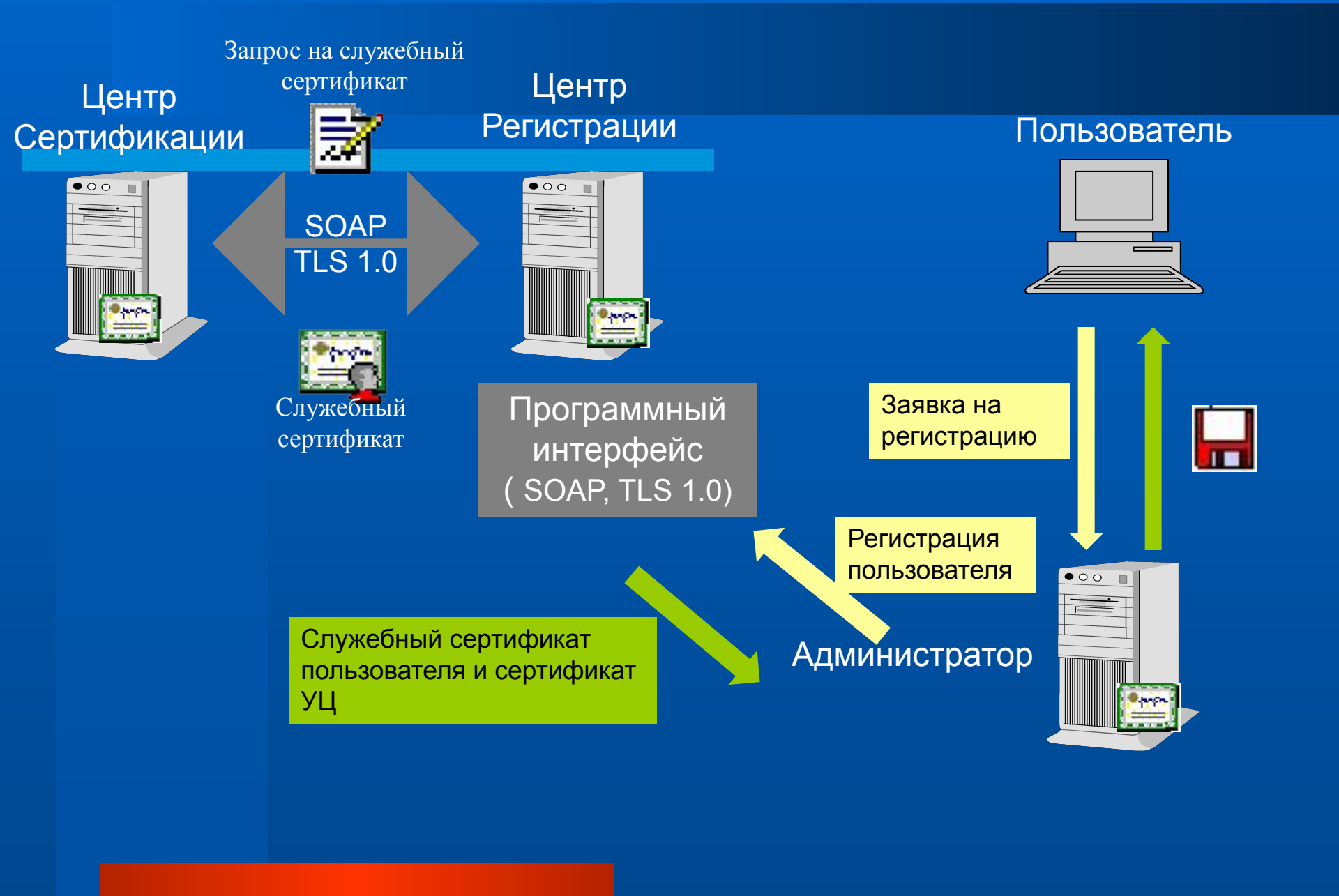
Использование КриптоПРО CSP в Outlook Express



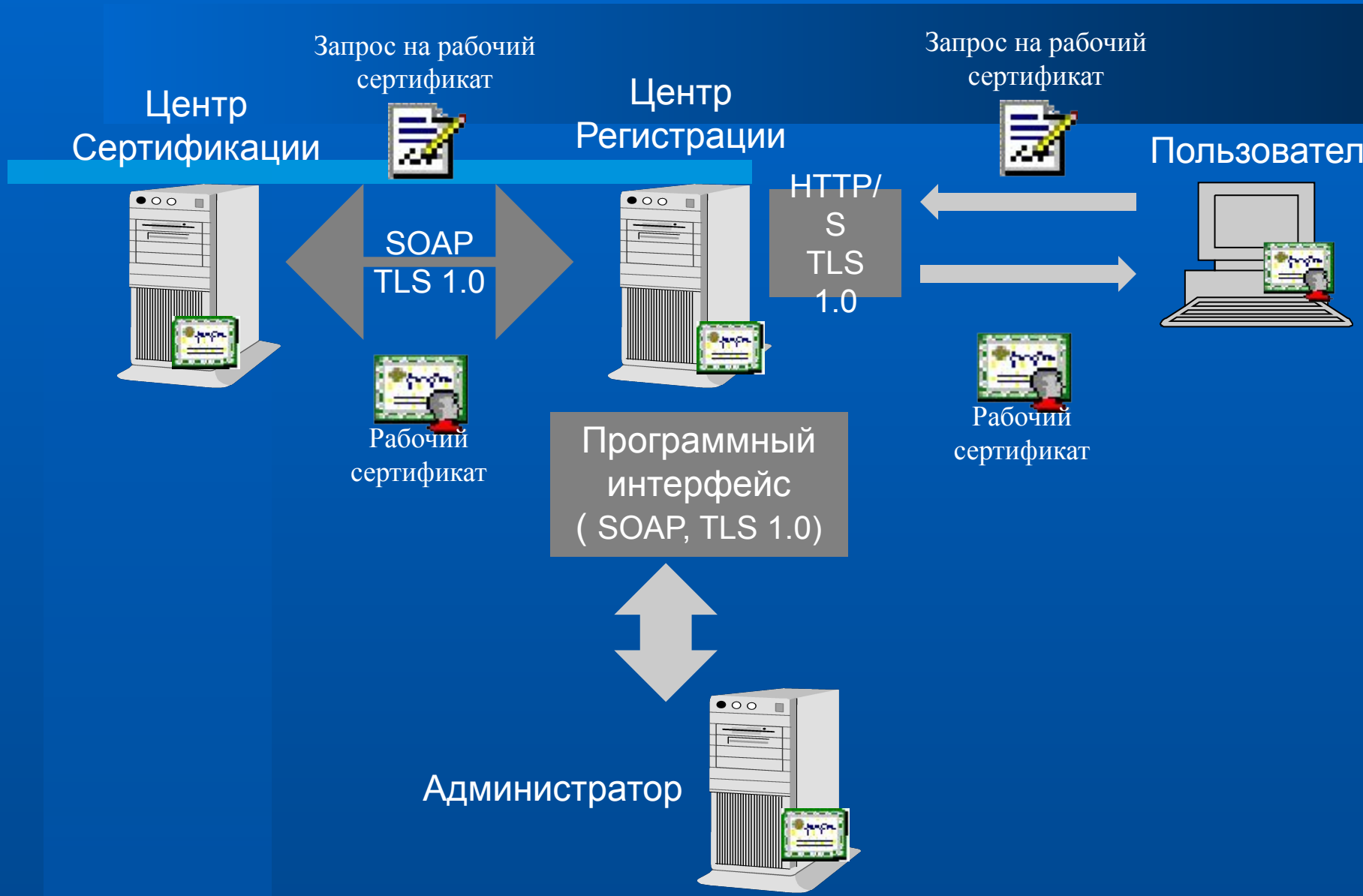
Иерархия Удостоверяющих Центров

НТЦ «Атлас»

Получение служебного сертификата



Получение рабочего сертификата



Конец презентации