

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 проверяется 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

«дайджест»

документа (хэш-функция), однозначно идентифицирует содержимое документа

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

$$M \rightarrow H(M) = h$$

S

$$\underline{S} = D_{\underline{Z}}(h)$$

ЭЦП

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: 010011101001001010010101

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: 010011101001001010010101

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 РКІ

Позволяет реализовать:

- Защищенная электронная почта:

Шифрование Элд открытым ключом получателя
заверенным сертификатом УЦ

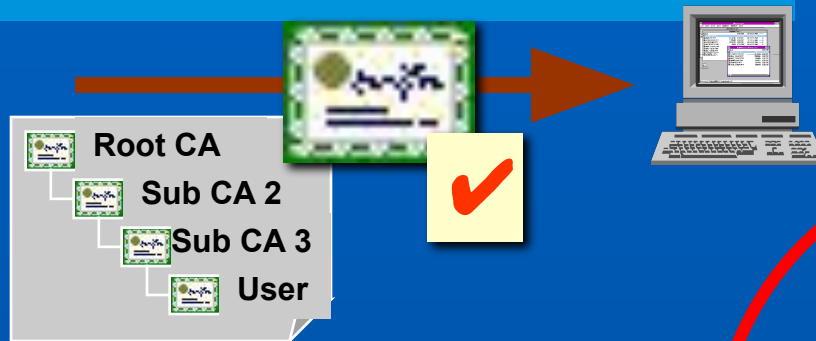
- Защита соединений в Интернете:

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

- Контроль ПО (Authenticode)

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

Проверка сертификата



Запреты

Списки CTL не запрещают использование сертификата для данной задачи.

Доверие

Сертификат корневого CA присутствует в хранилище Trusted Root Certification Authorities.

Тип

Сертификат можно использовать в данном режиме.

Срок действия

Сертификат действителен в данный момент.

Целостность

Цифровая подпись CA, выдавшего сертификат, верна.

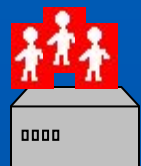
Легитимность

Сертификат не был отозван.

Структура удостоверяющего центра



Служба резервного копирования



Служба бесперебойного питания



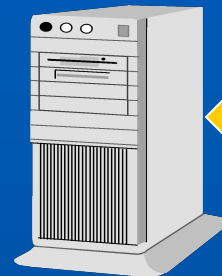
Служба администрирования ЦС и ЦР



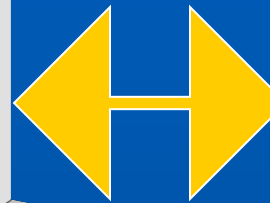
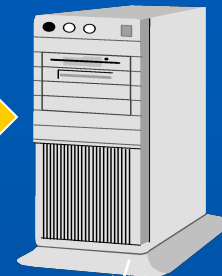
Обслуживающий персонал и прочие службы

Службы

Центр Сертификации



Центр Регистрации



Абоненты

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

отечес
крипто

Отсутствие аутентификации

пользователя
центру сер

Трудности масштабируемости

СКЗИ CryptoPro CSP

- Позволяет использовать стандартные приложения фирмы Microsoft с надежной российской криптографией



TLS/SSL для Internet Explorer

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



CAPICOM 1.0

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

Запрос на сертификат
PKCS#10

Сертификат
X.509

Криптографические сообщения
PKCS#7

CRL X.509

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

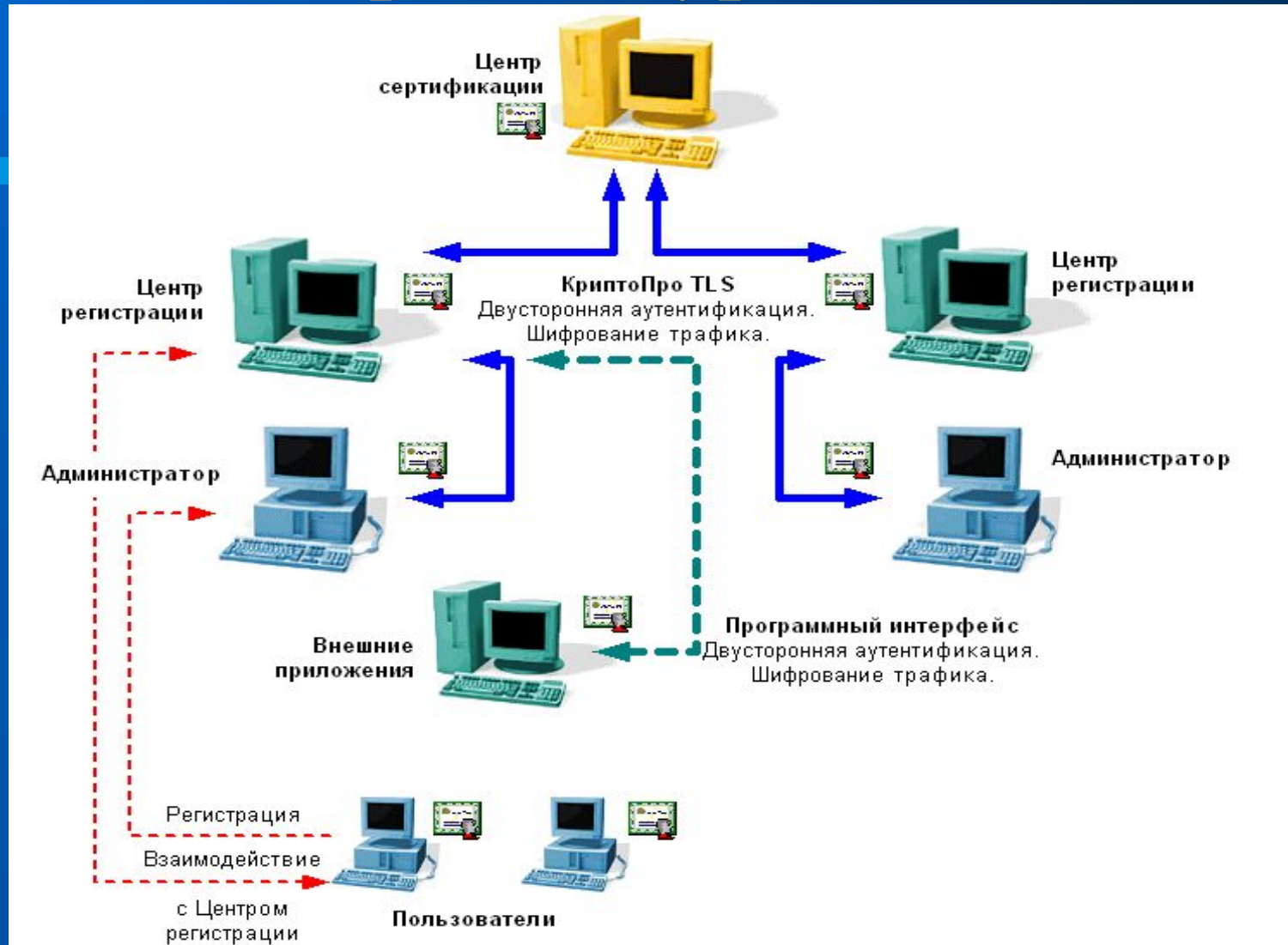
Основные функции:

- 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

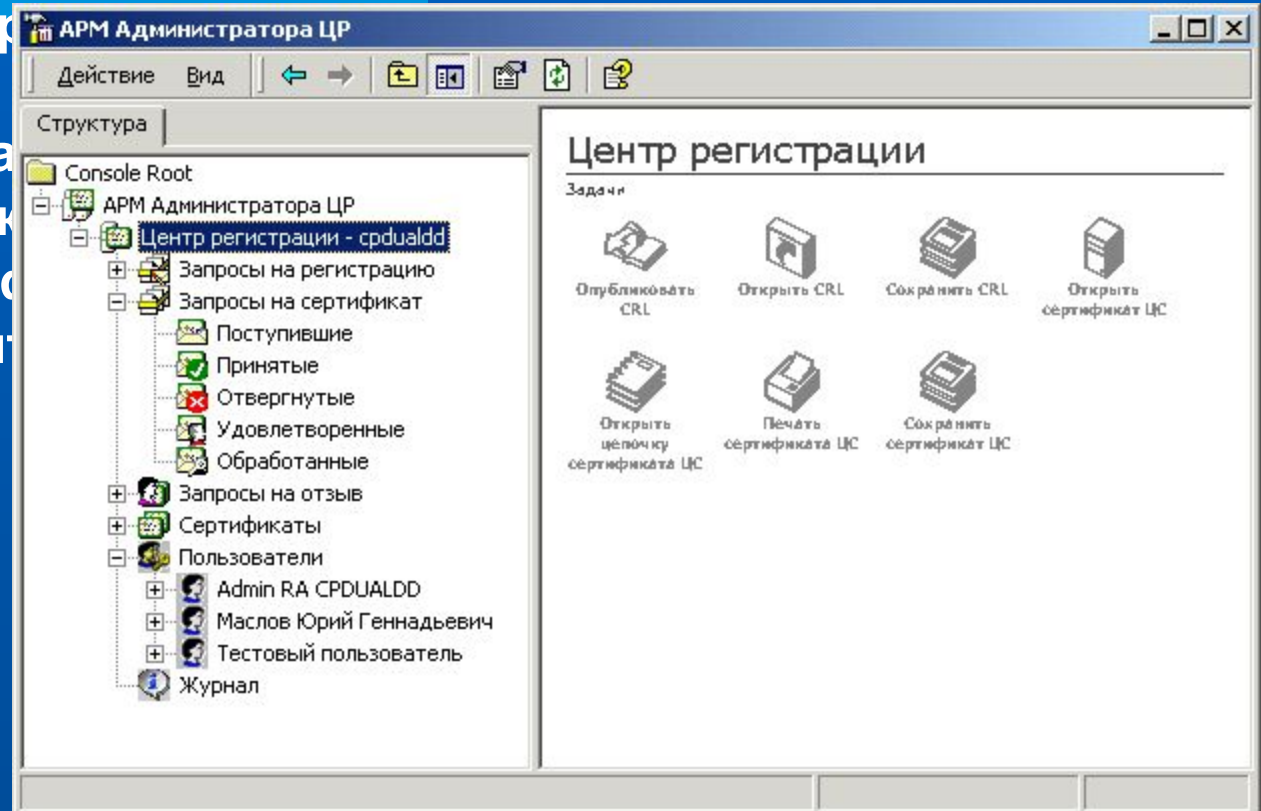
Архитектура УЦ



АРМ Администратора

Основные функции:

- Регистрация пользователей
- Мониторинг информации о сертификатах
- Выполнение регламентных операций с отзывом сертификатов
- Аудит работы Центра



Регистрация пользователей



Удостоверяющий Центр

Бланк сертификата открытого ключа

Сведения о сертификате:

Этот сертификат:

Защищает сообщения электронной почты

Кому выдан:

Сидоров Иван Петрович

Кем выдан:

Удостоверяющий Центр

Действителен с 6 февраля 2002 г. 17:36:28 по 6 февраля 2003 г. 17:46:28

Версия: 3 (0x2)

Серийный номер: 615C C074 0000 0000 0008

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-94

Идентификатор: 1.2.643.2.2.4

Параметры: 0500

Издатель сертификата: CN = Удостоверяющий Центр, O = Крипто-Про, C = RU

Срок действия:

Действителен с: 6 февраля 2002 г. 17:36:28

Действителен по: 6 февраля 2003 г. 17:46:28

Владелец сертификата: CN = Сидоров Иван Петрович, O = Крипто-Про, E = pre@cryptopro.ru

Открытый ключ:

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-94

Идентификатор: 1.2.643.2.2.20

Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01

Значение: 0481 804D B18A 9B00 E5C9 121A 7027 DB8B 0A41 F0D9 3601 4ACC 5A87 F67E 6169 DA0E 3F9A E5FC 36D8 6F0A 21F8 A063 979E 7A93 42B9 02BD 135B 7A3D 8D17 9BD4 B131 046B 81A6 12B1 E488 678B DF5B FCFA CD86 E60A F5D1 CC68 E6C6 1558 3AE1 EEF5 B3DC 2B4E 8F5A 7D3A 83B1 B909 2699 DD57 0FE1 E01A 88EE 9567 83D1 F6FC 0AA8 B761 9719 BAD3 99CE 00

Расширения сертификата X.509

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа

Значение: Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)

2. Расширение 2.5.29.37

Название: Улучшенный ключ

Значение: Защищенная электронная почта(1.3.6.1.5.5.7.3.4)

3. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта

Значение: EE8A D281 7ED5 838C 08D6 1BF4 FEAA 13A7 3363 C3B7

4. Расширение 2.5.29.35

Название: Идентификатор ключа центра сертификатов

Значение: Идентификатор ключа=568E 896B D30A 1DE0 6108 5F6B 213C 352C 3775 28C3

5. Расширение 2.5.29.31

Название: Точки распространения списков отзыва (CRL)

Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://lord2k.cp.ru/CA.crl

Подпись Удостоверяющего центра:

Алгоритм подписи:

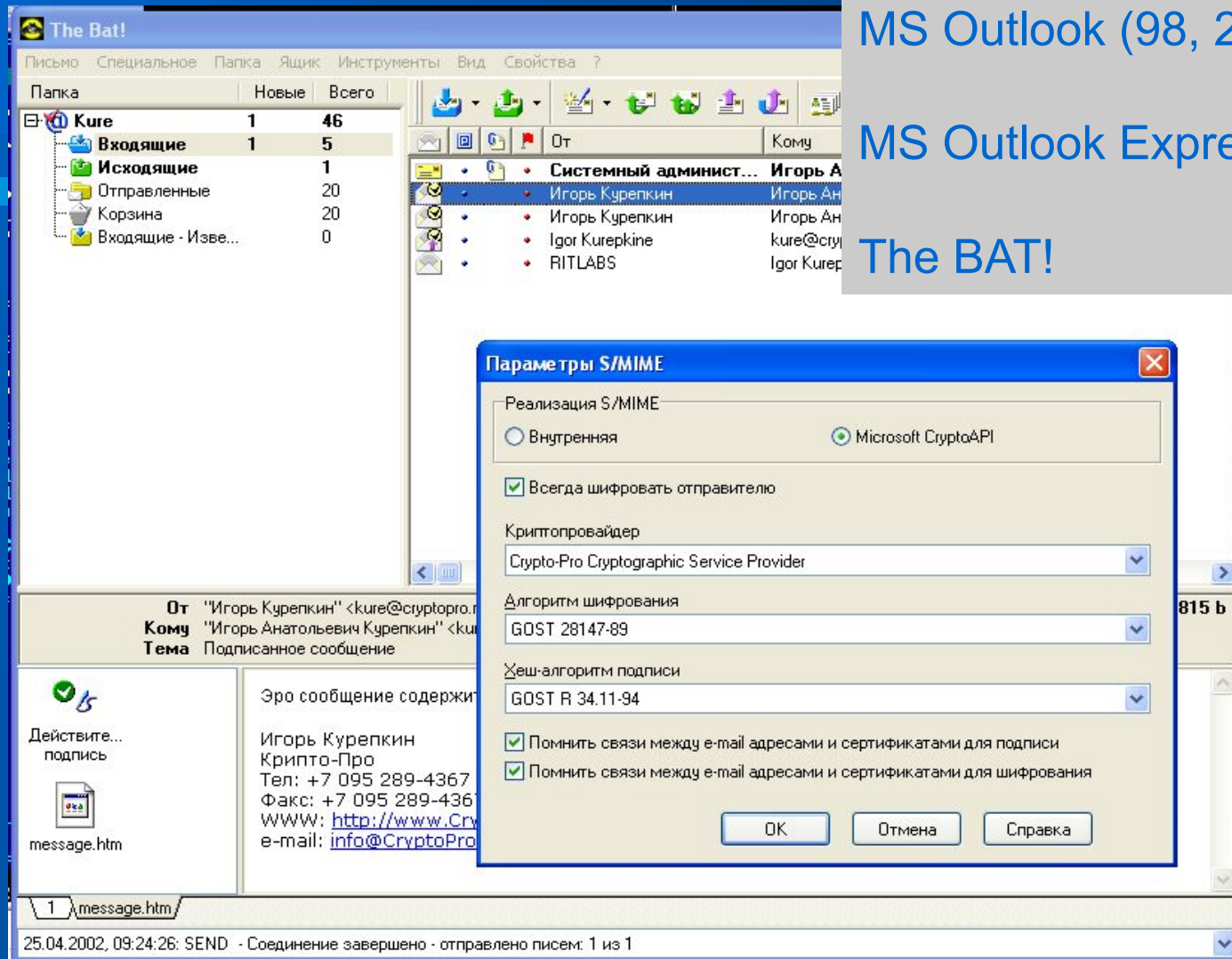
Название: ГОСТ Р 34.11/34.10-94

Идентификатор: 1.2.643.2.2.4

Параметры: 0500

Значение: 4F5E 346F 92FA 160A 87F7 F017 F243 0AB3 5163 004E 2D23 0DAC B662 A247 209B ED35 1145 2361 2150 5D93 A30F 7FC9 A89B 79EF FD0B 31B4 8CF3 6553 8C1E 15D3 CF6B 8264

Электронная почта

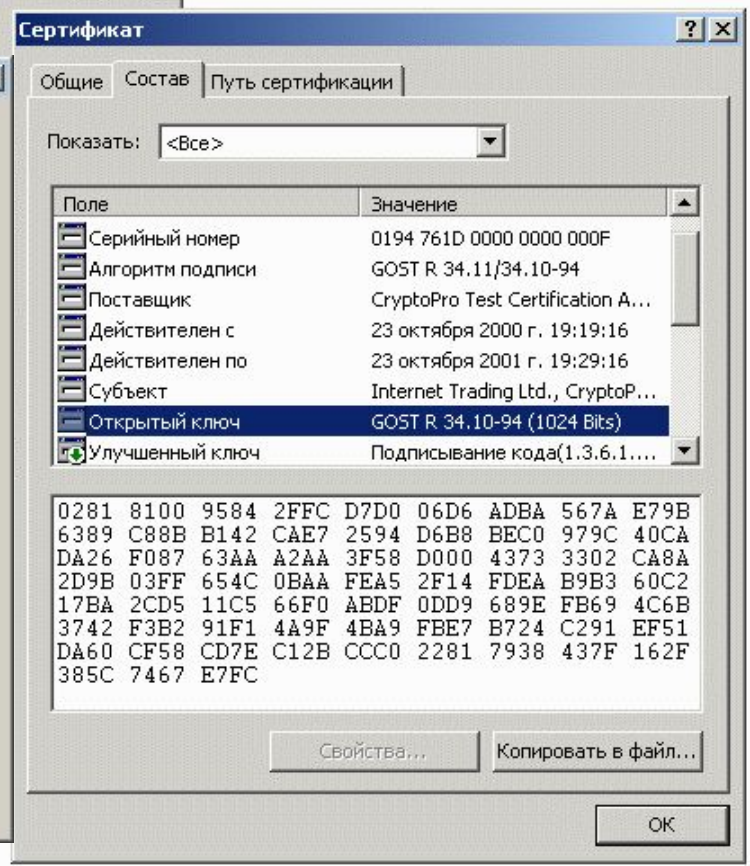
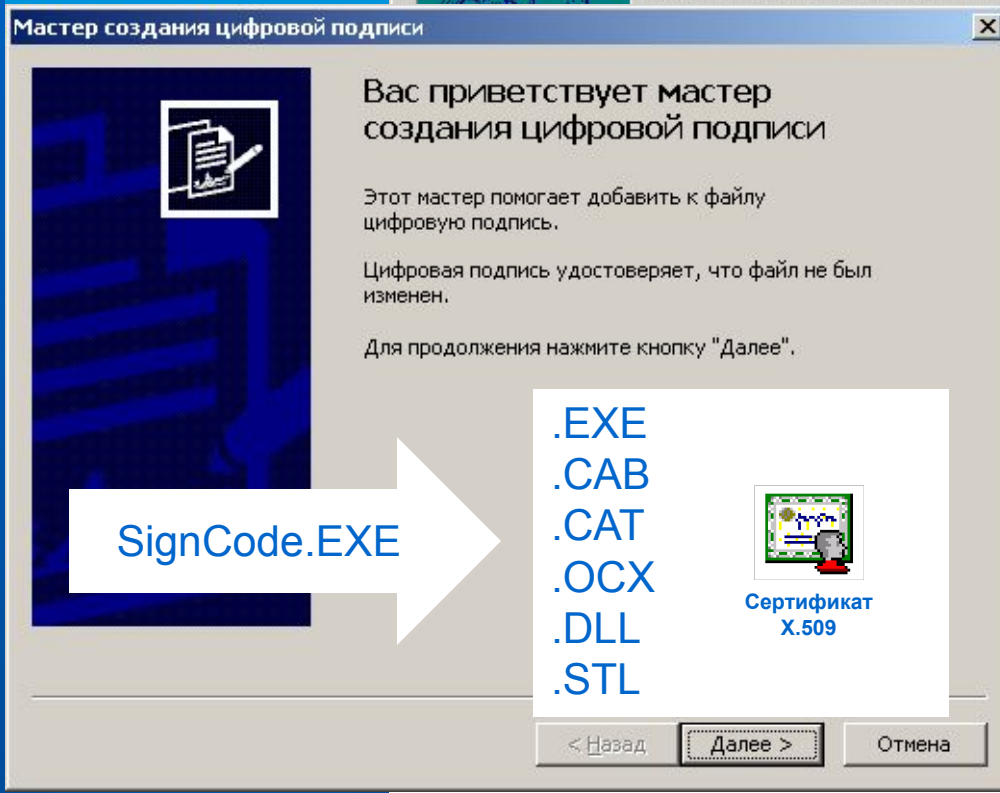
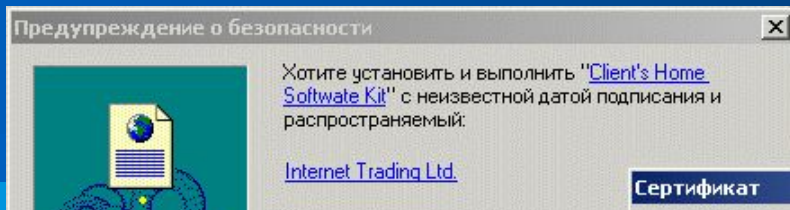


MS Outlook (98, 2000, XP)

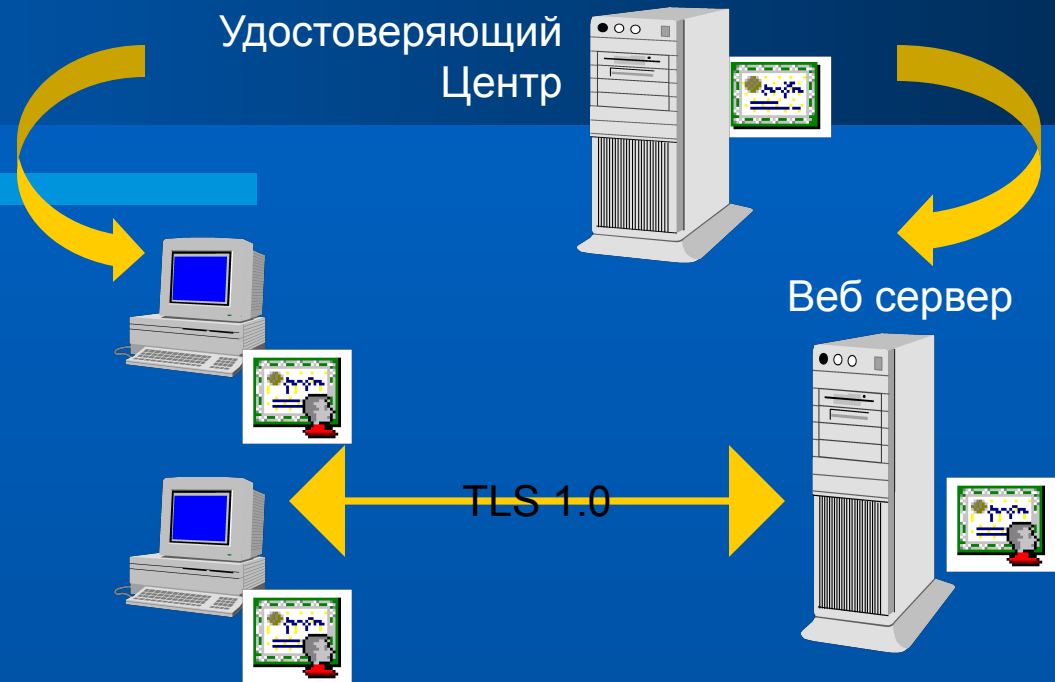
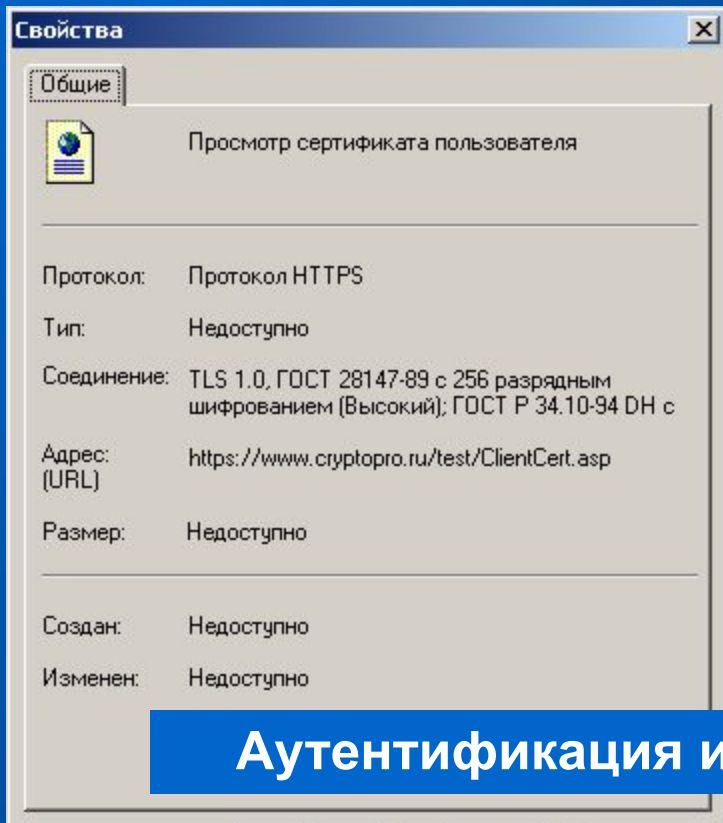
MS Outlook Express

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

Microsoft CAPICOM, СКЗИ КриптоПро CSP

CAPICOM

CAPICOM предоставляет COM интерфейс, использующий основные функции CryptoAPI 2.0. Этот компонент является добавлением к уже существующему COM интерфейсу Certificate Enrollment Control (xenroll), который реализуют клиентские функции генерации ключей, запросов на сертификаты и обмена с центром сертификации. С выпуском данного компонента стало возможным использование функций формирования и проверки электронной цифровой подписи, построения и проверки цепочек сертификатов, взаимодействия с различными справочниками сертификатов (включая Active Directory) с использованием Visual Basic, C++, JavaScript, VBScript.

► Для регистрации CAPICOM.dll

В командной строке перейдите в директорию, в которой находится файл CAPICOM.dll и выполните команду:

```
regsvr32 CAPICOM.dll
```

Конференция по CAPICOM

<http://discuss.microsoft.com/archives/capicom.html>

Ресурсы

CAPICOM входит в состав распространяемых компонент Platform SDK доступен для загрузки с сервера Microsoft:
<http://www.microsoft.com/msdownload/platformsdk/setuplauncher.asp>

CAPICOM на сервере Крипто-Про: <http://www.cryptopro.ru/capicom/redistr/capicom.dll>

HTML Help по разделу безопасность из Platform SDK на сервере Крипто-Про:
http://www.cryptopro.ru/capicom/help/Security_Chi
http://www.cryptopro.ru/capicom/help/Security_Chm

Исходные тексты примеров из Platform SDK

Примеры использования CAPICOM на сервере Крипто-Про:
<http://www.cryptopro.ru/capicom/samples/samples.ZIP>

Пример подписи данных в интерфейсе Internet Explorer с использованием Visual Basic Scripting

Фамилия:

Имя:

Регистрационные данные:

CAPICOM 1.0

Терминал "Альфа-Директ" [криптопр_р] - [Пример построения окна]

Своя страница | НОВОСТИ И СООБЩЕНИЯ

КОТИРОВКИ

Инструм	Посл.	Ср. цен	К-во в г	Спрос
MSNG3	1,005	1,005	34	1,004
TATNP2	↓ 6,56	6,572	200	6,59
TATN2	13,66	13,72	140	13,65
RTKMP1	9,4	9,33	2	9,39
RTKM1	23,18	22,88	50	23,11

НОВОСТИ

Заголовков

Банк России повысил на 900 пунктов курс

Новый железнодорожный маршрут Минск

Банк России повысил на 100 пунктов официальный курс рубля до 28,9500 руб за доллар / один пункт

АЛЬФА-БАНК

Программа Альфа-Директ™
Версия 1.3.0 (сборка 018)
© ОАО «Альфа-Банк», 2000.
Все права защищены.

www.alfadirect.ru
mail@alfadirect.ru

GAZP | EESR2

3,35
3,3
3,25

11:00 11:18 11:38 11:58 12:18 12:38 12:58

3,273 : 1

Время на сервер

CryptoAPI 2.0
КриптоПро CSP

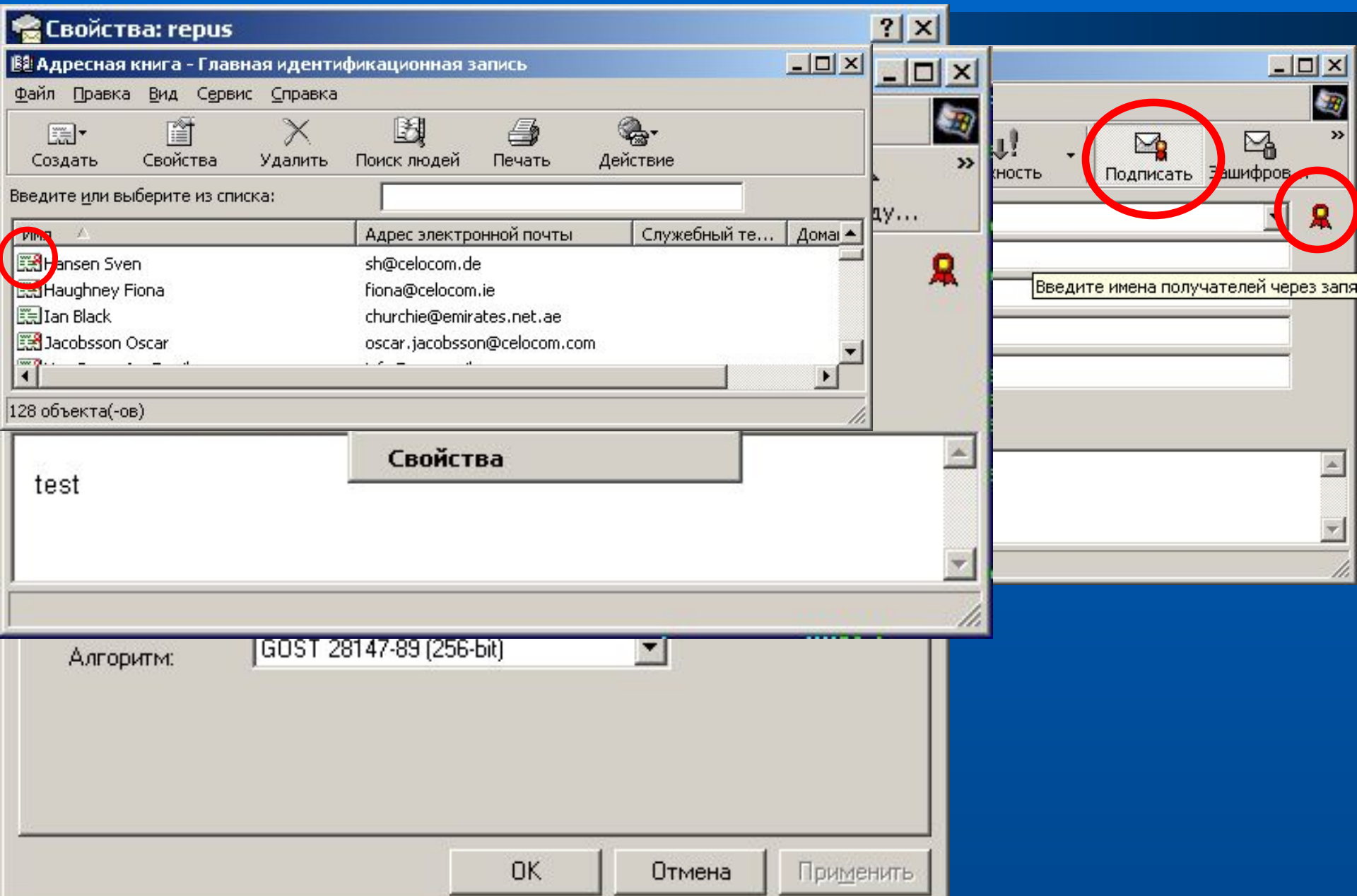
Интеграция российских алгоритмов



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

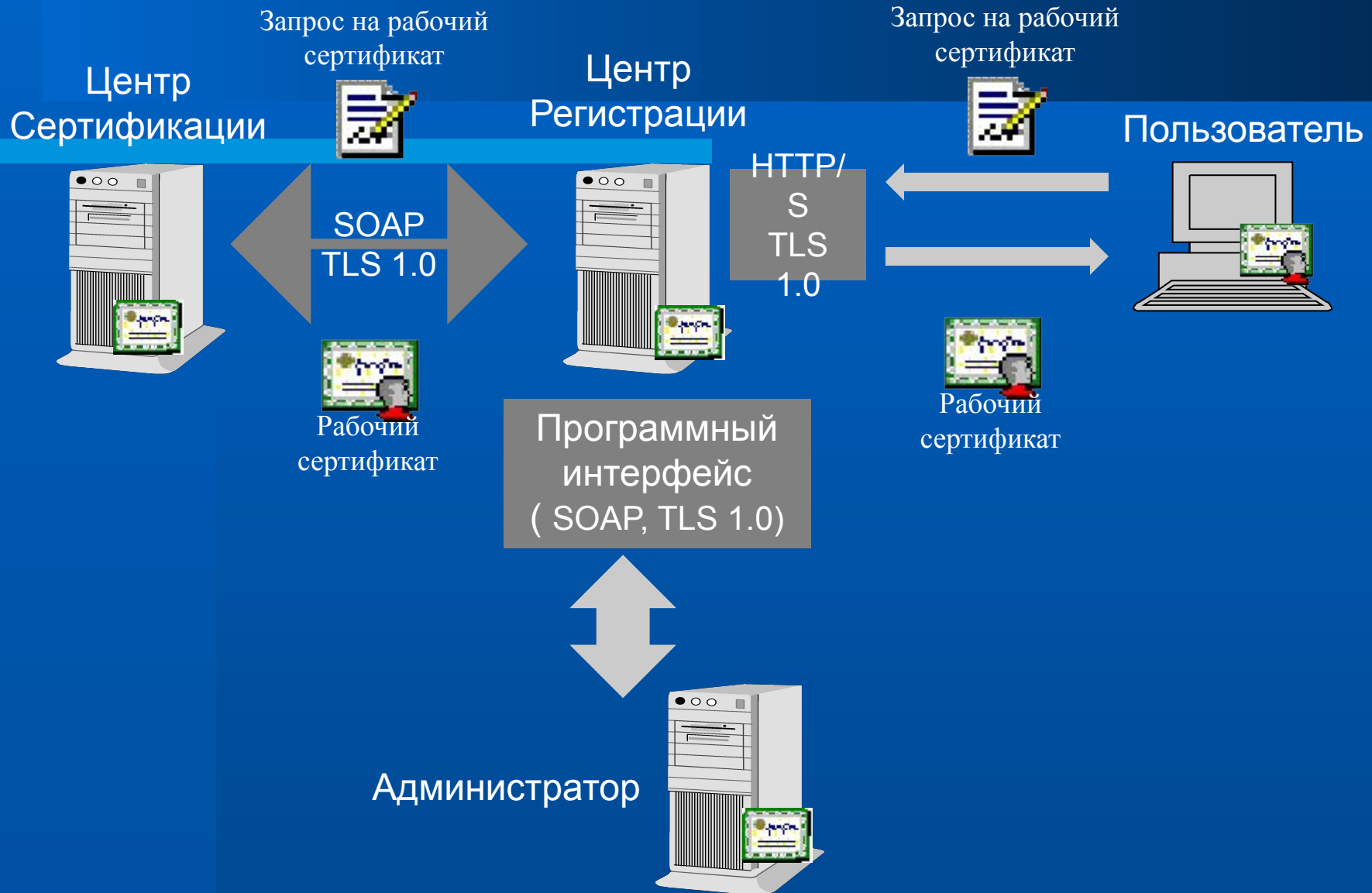
НТЦ «Атлас»



Получение служебного сертификата



Получение рабочего сертификата



Конец презентации

