



Электронная- цифровая ПОДПИСЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Microsoft[®]
CERTIFIED
Database Administrator

Старыгин Артем
Викторович
НПО Компьютер



Электронная цифровая подпись

✓ Назначение

- Подтверждение авторства
- Неотрекаемость
- Гарантия неизменности

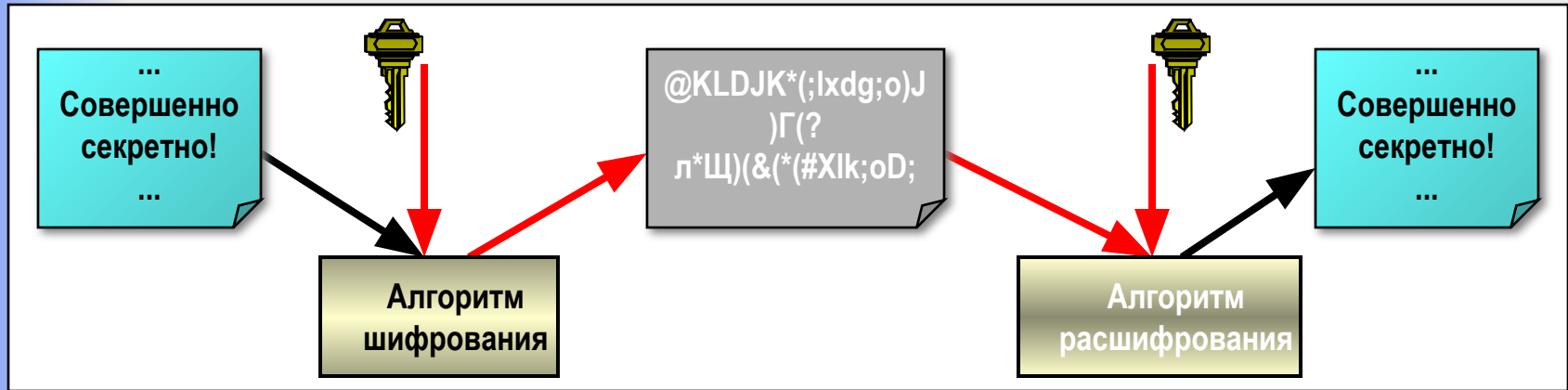
✓ Преимущества

- Сложность подделки
- Ускорение документооборота
- Безопасность коммуникаций

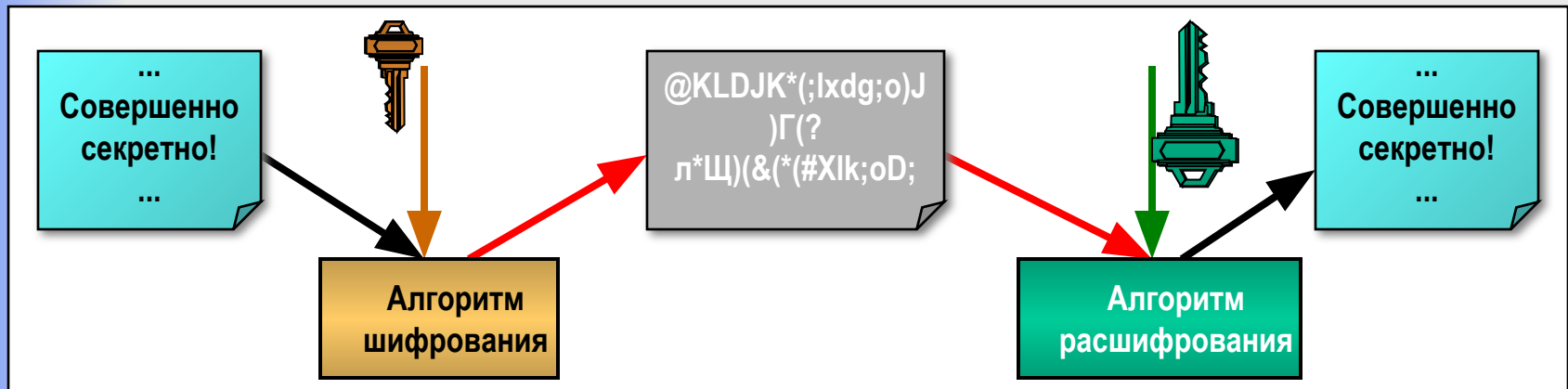


Технологическая основа ЭЦП

Симметричное шифрование – один ключ



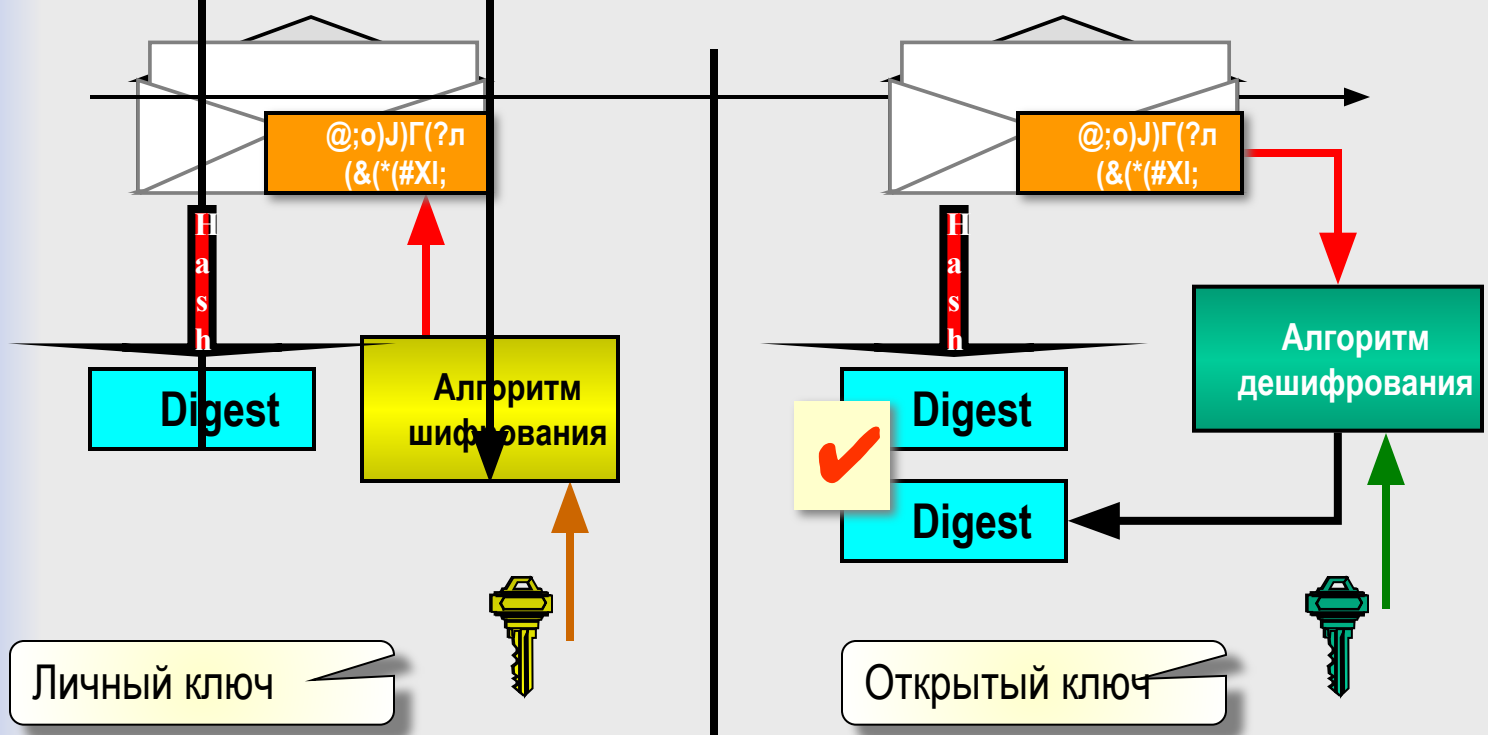
Асимметричное шифрование – пара ключей: открытый и личный





Создание подписи

✓ Хеширование





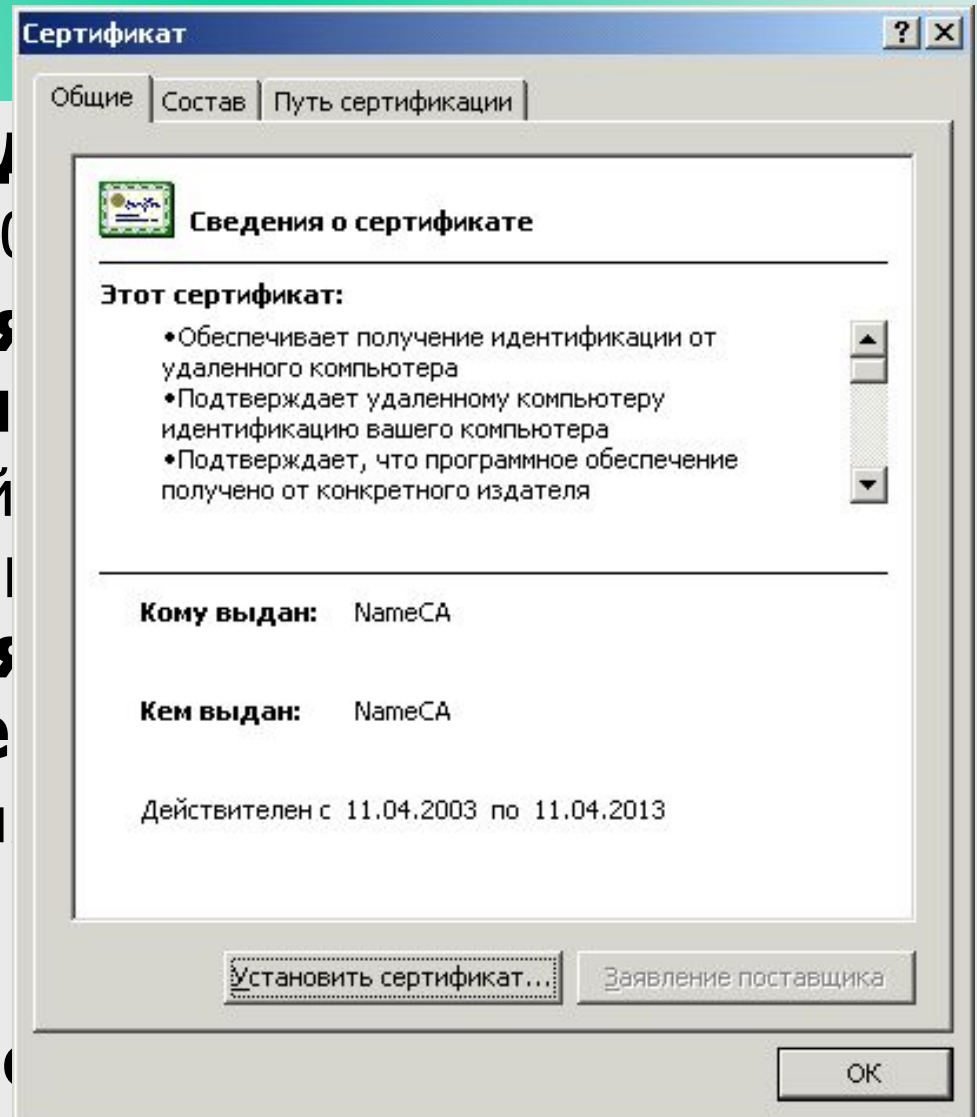
Инфраструктура открытого ключа

- ✓ **Необходимость создания инфраструктуры**
- ✓ **Составляющие инфраструктуры:**
 - Цифровые сертификаты открытых ключей
 - Службы управления сертификатами



Сертификат

- ✓ **Цифровое удостоверение**
 - Стандарт X.509
- ✓ **Информация об идентифицируемом объекте**
 - Его открытый ключ
 - Допустимые приложения
- ✓ **Информация о проверке сертификата**
 - Срок действия
 - Информация о поставщике сертификата
- ✓ **Цифровая подпись**





Назначение Центра Сертификации

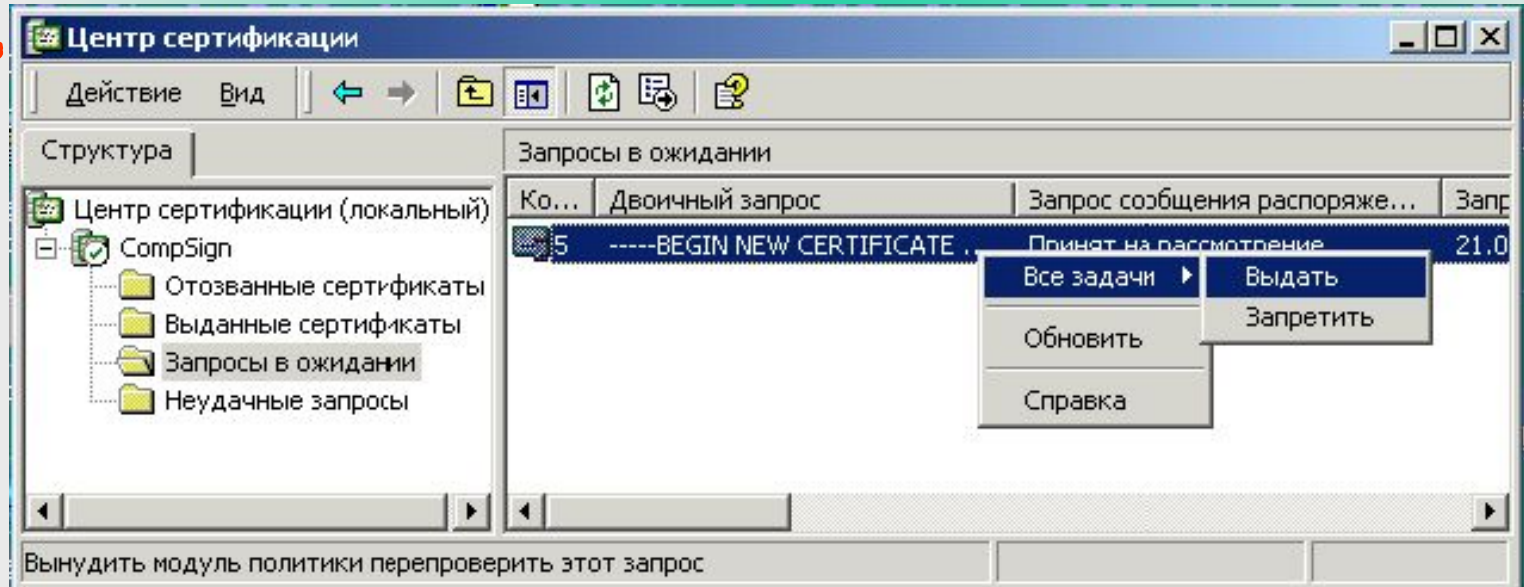
✓ **Certification Authority – Центр сертификации**

- Выдача сертификатов клиентам
 - Генерация ключей, если нужно
- Отзыв сертификатов
 - Публикация Certificate Revocation List
- Хранение истории всех выданных сертификатов

✓ **Web Enrollment Support**

- Запрос и получение сертификата через Web-интерфейс

Центр Сертификации Microsoft

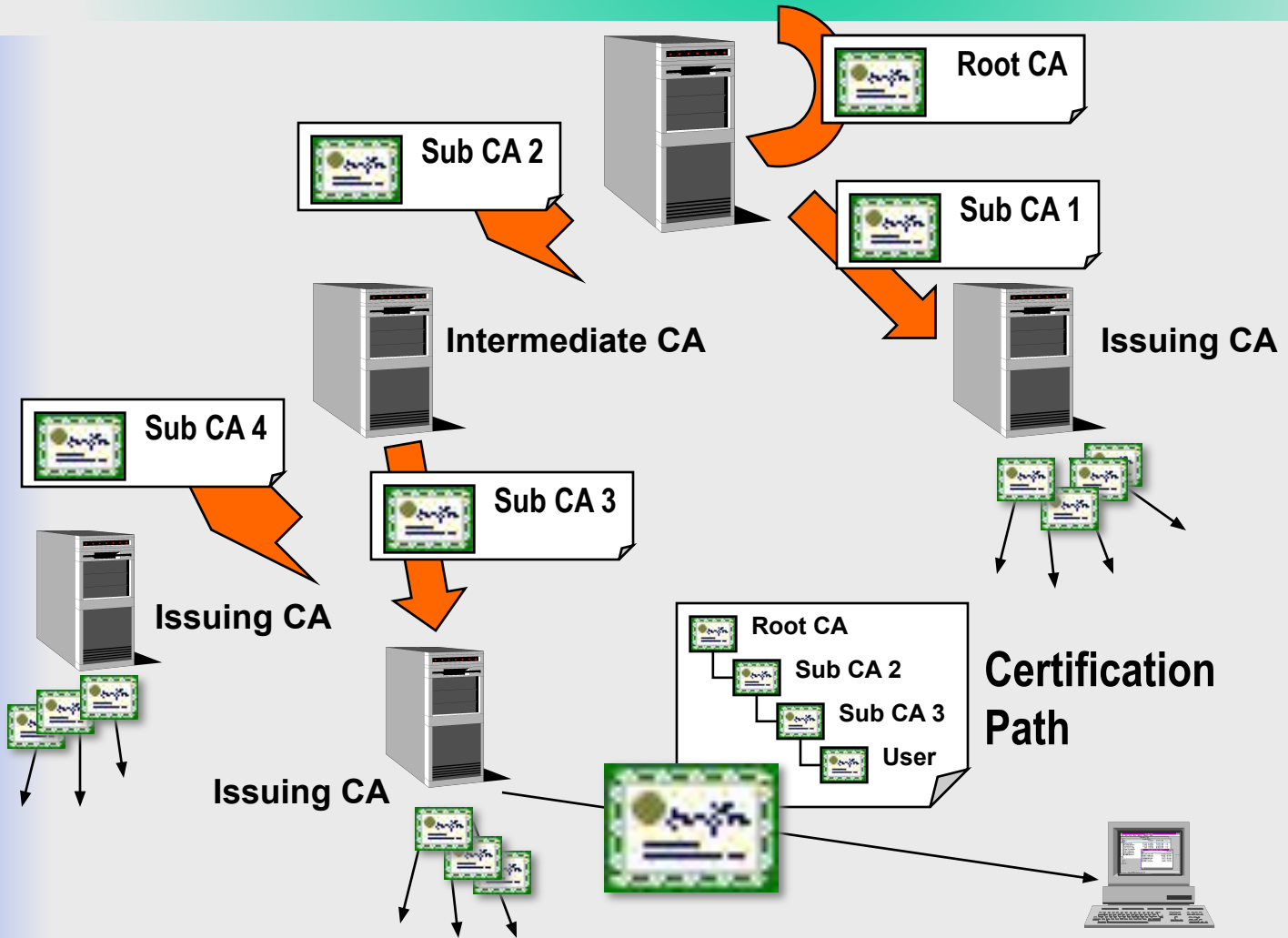


Stand-Alone – независимый

- Не зависит от Active Directory
- Может использоваться в качестве независимого центра сертификации для любых объектов



Иерархия ЦС



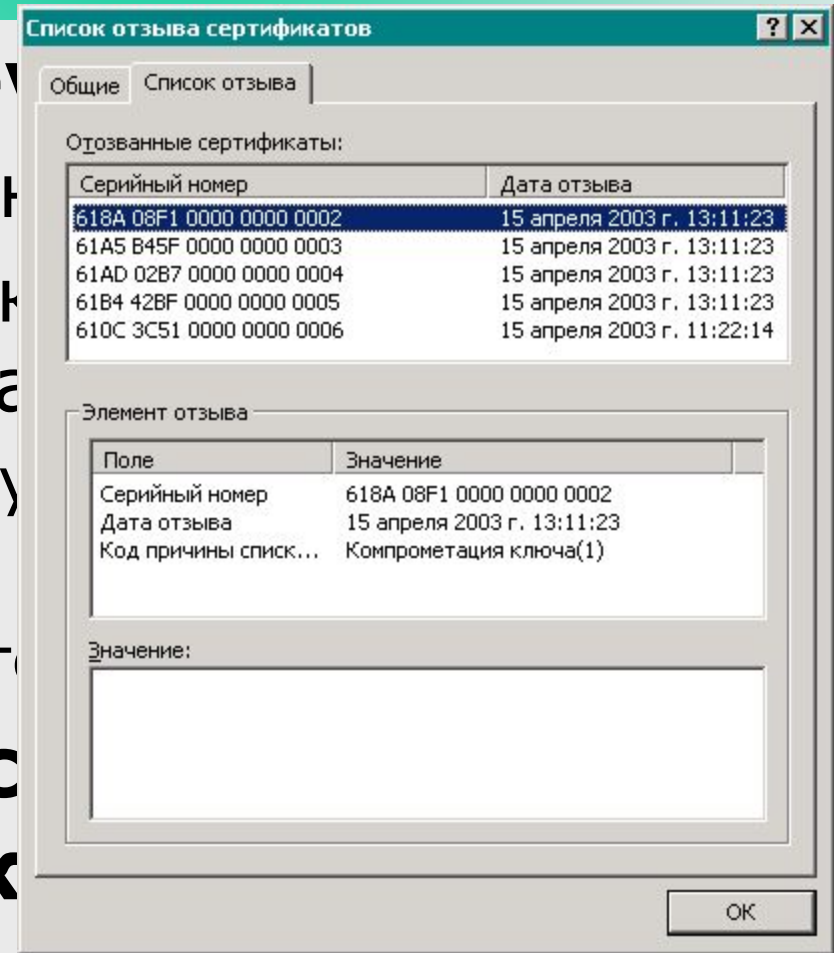


Список отозванных сертификатов

✓ Certificate Revocation

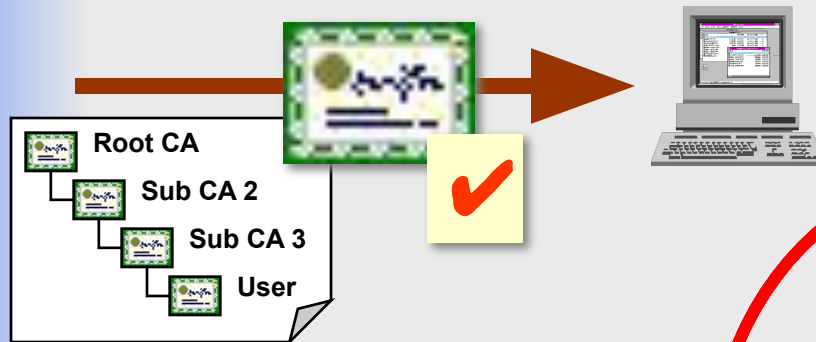
- Список отозванных сертификатов
- Должен публиковаться и обновляться как
 - Active Directory
 - Web
 - Файловая система

✓ Сертификат с отозванными узлами публиковаться





Проверка сертификата



Тип

Сертификат
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.

Запреты

Списки CTL не запрещают использование сертификата для данной задачи.

Доверие

Сертификат корневого CA присутствует в хранилище Trusted Root Certification Authorities.



Хранилища сертификатов



Физ

□ Act

□ Ре

□ Фа



Лог

□ Ли

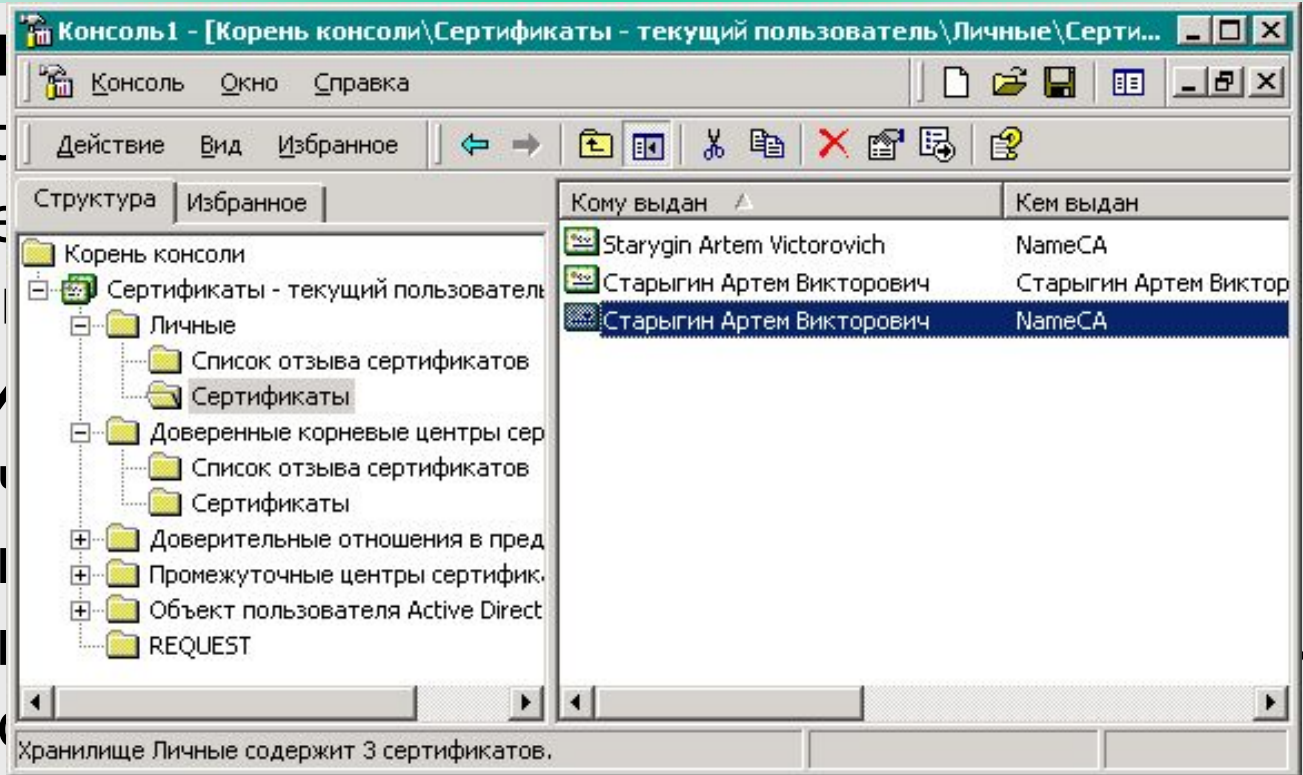
□ До

□ До

□ Пр

□ Объект пользователя Active Directory

□ REQUEST



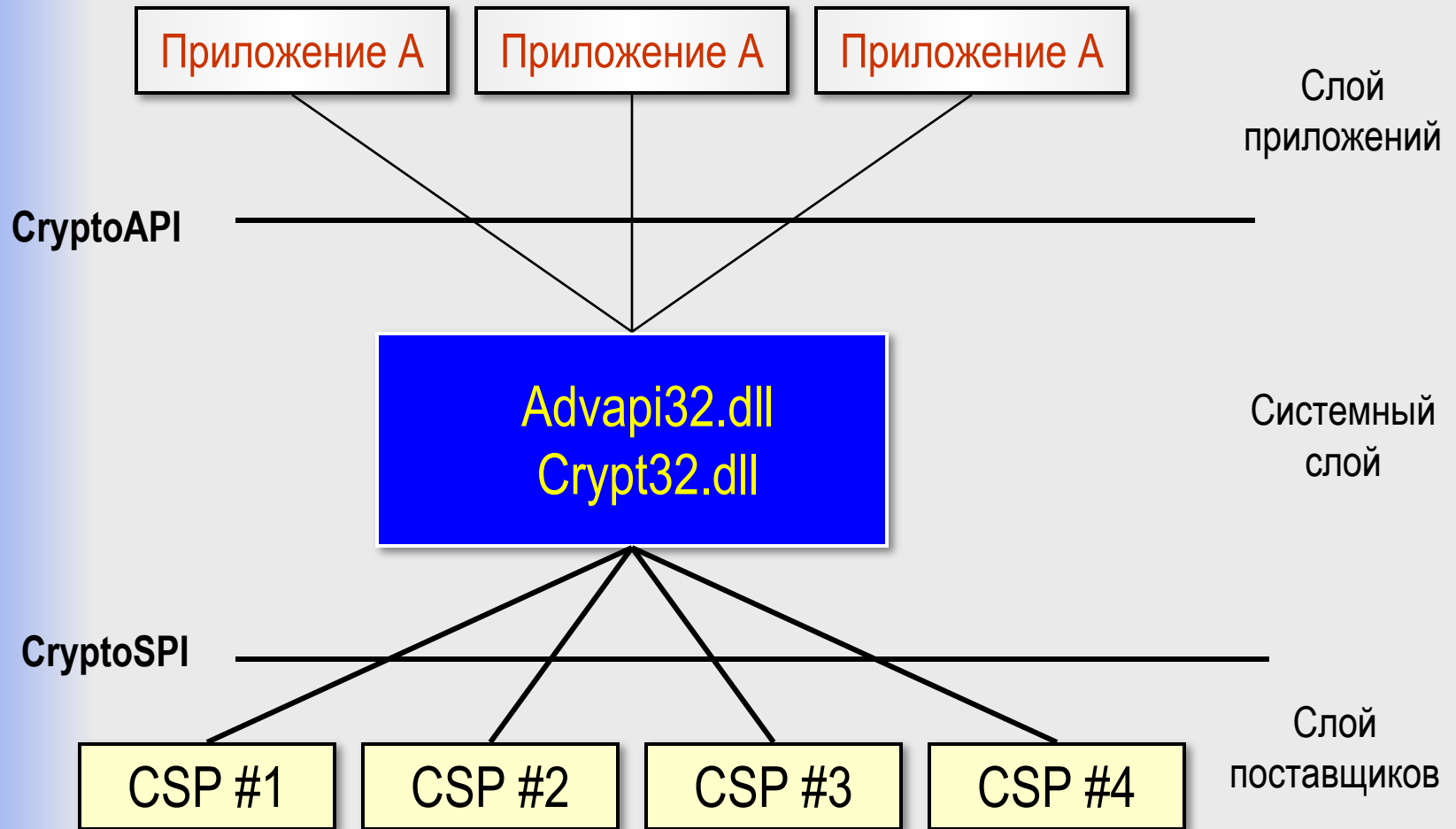


Криптография в Windows

- ✓ **Cryptographic Service Provider**
 - Криптографические операции
 - Генерация и хранение ключей
- ✓ **CryptoAPI**
 - Программные интерфейсы к криптографическим службам Windows 2000
- ✓ **Microsoft CSPs**
 - Базовый набор
 - High Encryption Pack



Архитектура служб криптографии





Разработка криптопровайдера

- ✓ **Создание модуля CSP с помощью *Microsoft Cryptographic Service Provider Developer's Kit***
 - <http://msdn.microsoft.com/downloads/>
 - Раздел "Security"
- ✓ **Цифровая подпись Microsoft**
 - Модуль с описанием нужно передать Microsoft
 - Процесс подписи занимает 1 – 2 рабочих дня



Существующие криптопровайдеры

✓ Встроенные в Windows

- Microsoft Base CSP
- Microsoft DSS CSP

□ Microsoft

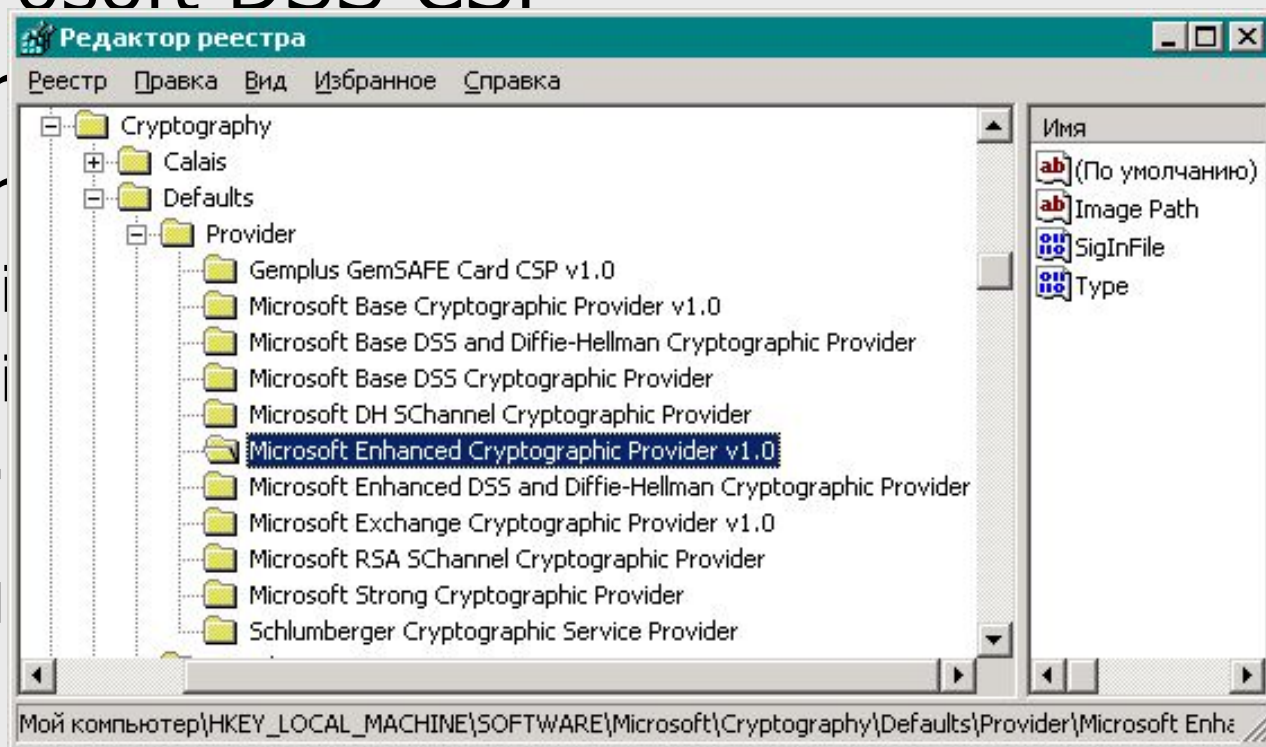
□ High

• Mi

• Mi

✓ Серт

□ Кри





ЭЦП в Windows

- ✓ **Поддержка смарт-карт**
- ✓ **Шифрующая файловая система (EFS)**
- ✓ **Безопасность сетевого взаимодействия**
 - IP (IPSec) – шифрование IP-пакетов
 - SSL – безопасность для приложений
- ✓ **Подпись драйверов**
- ✓ **Подпись макросов**



Практика использования ЭЦП

- ✓ **Безопасность электронной почты**
- ✓ **Электронные платежи (клиент банк)**
- ✓ **Системы электронного документооборота**
 - Подпись документов
- ✓ **Государственные закупки**
- ✓ **Размещение заказов**



Законодательство об ЭЦП

- ✓ **Федеральный закон об ЭЦП**
 - Цель закона
 - Основные понятия
 - Условия использования ЭЦП
 - Удостоверяющие центры
 - Особенности использования ЭЦП
- ✓ **ГОСТ 34.10-2001**



Проблемы

использования закона

- ✓ **Ограничение на технические решения**
- ✓ **Не определен формат сертификата**
- ✓ **Несовместимость средств криптографической защиты**
- ✓ **Запрет выдачи сертификатов юридическим лицам**
- ✓ **Отсутствие электронного нотариата**



Поддержка ЭЦП в системе DIRESTUM

✓ Действия администратора

- Создание инфраструктуры

-

№	*Кому выдан	*ИД сертификата	*Состояние
1	Старыгин Артем Викторович	A64907E0AC58F6CB0E	Действующая
2	Старыгин Артем Викторович	316619BDB1D6E96C71	Действующая

Записей: 1 Изменение ИД: 97689 Утверждена

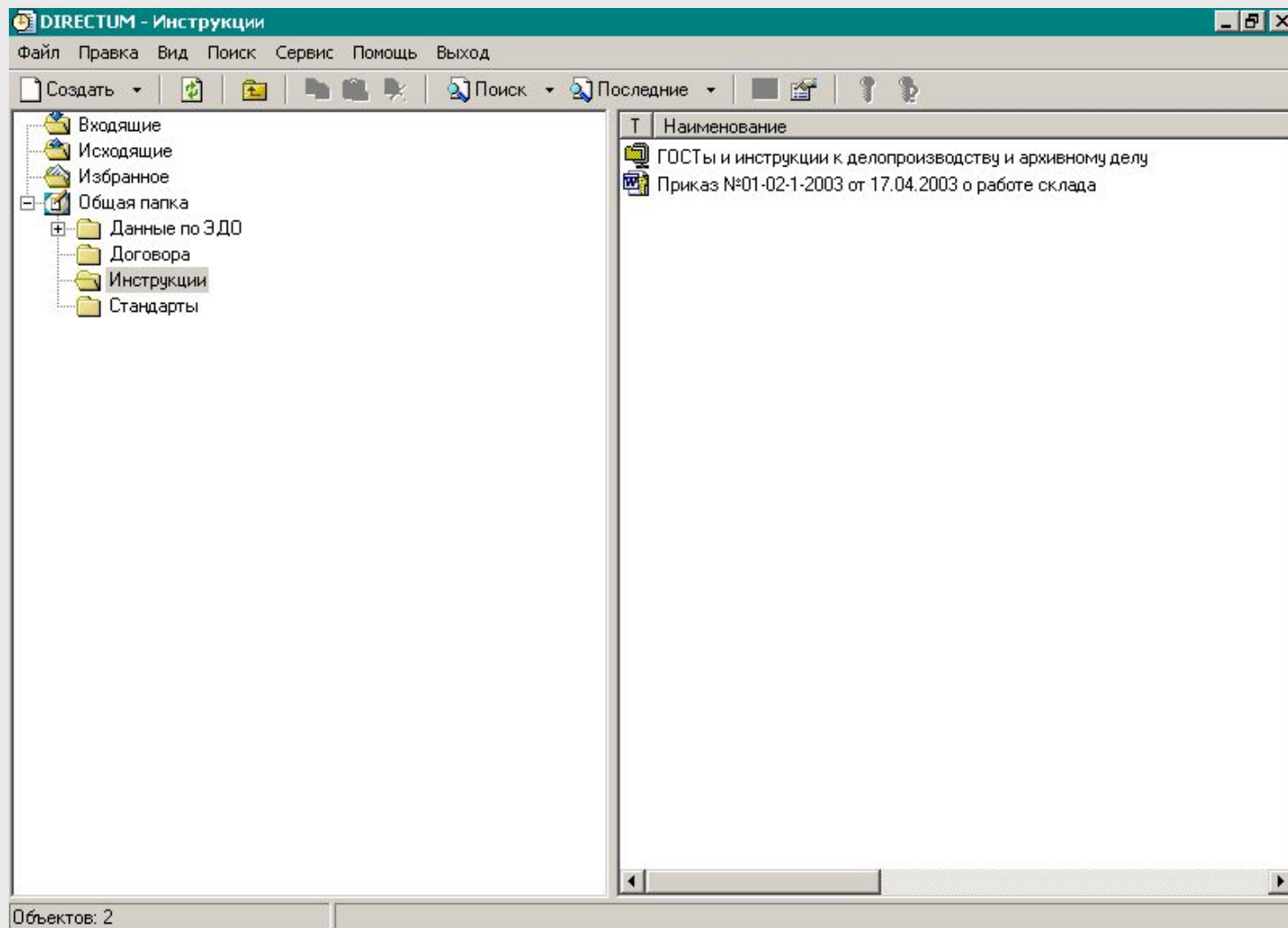


Поддержка ЭЦП в системе DIRECTUM

- ✓ **Действия пользователя**
 - Подписание документов
 - Подписание версий
 - Проверка цифровой подписи
 - Автоматические проверки



Подписание документа





Ответы

Вопросы?

