## Инфраструктура открытых ключей. Цифровые сертификаты

- Использование асимметричной криптографии сделало возможным безопасный обмен криптографическими ключами между **A** и **B** без использования **центров распределения ключей**.
- Возникает проблема - как убедиться в том, что имеющийся у Вас открытый ключ другого абонента принадлежит именно ему: проблема аутентификации ключа.

Проблема приводит к тому, что на криптографический протокол может быть осуществлена **атака "человек посередине"** (man-in-the-middle).

# Атака "человек посередине"

Интруз **I** имеет возможность **подменять открытые ключи рользователей в общедоступном источнике (БД).**

Абонент **A** хочет послать абоненту **B** зашифрованное сообщение **M** и берет его открытый ключ из общедоступного источника.
Но Интруз **I** до этого подменил (в общедоступном источнике) открытый ключ **B** (**Кв**) своим открытым ключом, $К_I$:

$$C_I = E_{Ki}(M).$$

Теперь **I** может расшифровать $C_I$, ознакомиться с его содержимым, зашифровать **M** (или его модификацию, **M'**) настоящим ключом **B** (**Кв**)и переслать ему:

$$C = E_{Кв}(M)$$

или

$$C = E_{Кв}(M').$$

# Инфраструктура публичных ключей и цифровые сертификаты

- Избежать атаки **"человек посередине"** можно, подтвердив подлинность используемого ключа.
- Но **A** и **B** лично не могут встретиться, и передать, например, ключ из рук в руки не могут.
- Решение задачи подтверждения подлинности берет на себя **третья (доверенная) сторона,** которой доверяют оба абонента.
- Заверяется ключ с помощью **цифрового сертификата.**
- Подобный способ применяется и вне компьютерных систем. Нп., для подтверждения подлинности человека используется паспорт, в роли третьей стороны выступает государство (от имени которого действовали в выдавшем паспорт отделе милиции).

•Для подтверждения подлинности открытых ключей создается **инфраструктура открытых ключей** (англ. Public Key Infrastructure, **PKI**).

• **PKI** - набор средств, мер и правил, предназначенных для управления ключами, политикой безопасности и обменом защищенными сообщениями.

Структура **PKI**

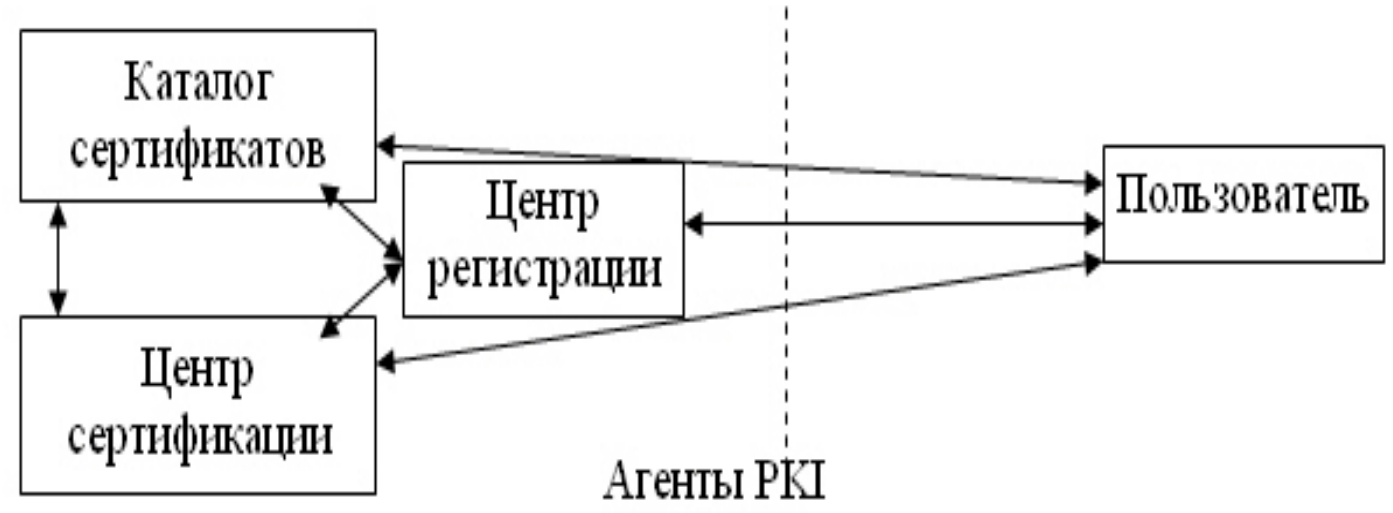



Рис. 1

•Представляем сеть на рисунке 1 в виде совокупности **удостоверяющих центров** (другое название - **центр сертификации**, от англ. Certification Authority, **CA**) и **пользователей**.

•**Центр сертификации** - абонент, которому доверено право удостоверять своей подписью сертификаты, связывающие открытые ключи абонентов с их идентификационной информацией.

• Сами **центры сертификации тоже получают сертификаты своих ключей у центров более высокого уровня**.

•Центры сертификации и пользователи формируют **древовидную иерархическую структуру** ( рис. 2).

•В вершине дерева находится **корневой центр сертификации**, на рисунке - **CA_1**. Он использует самоподписанный сертификат, т.е. сам заверяет свой ключ.

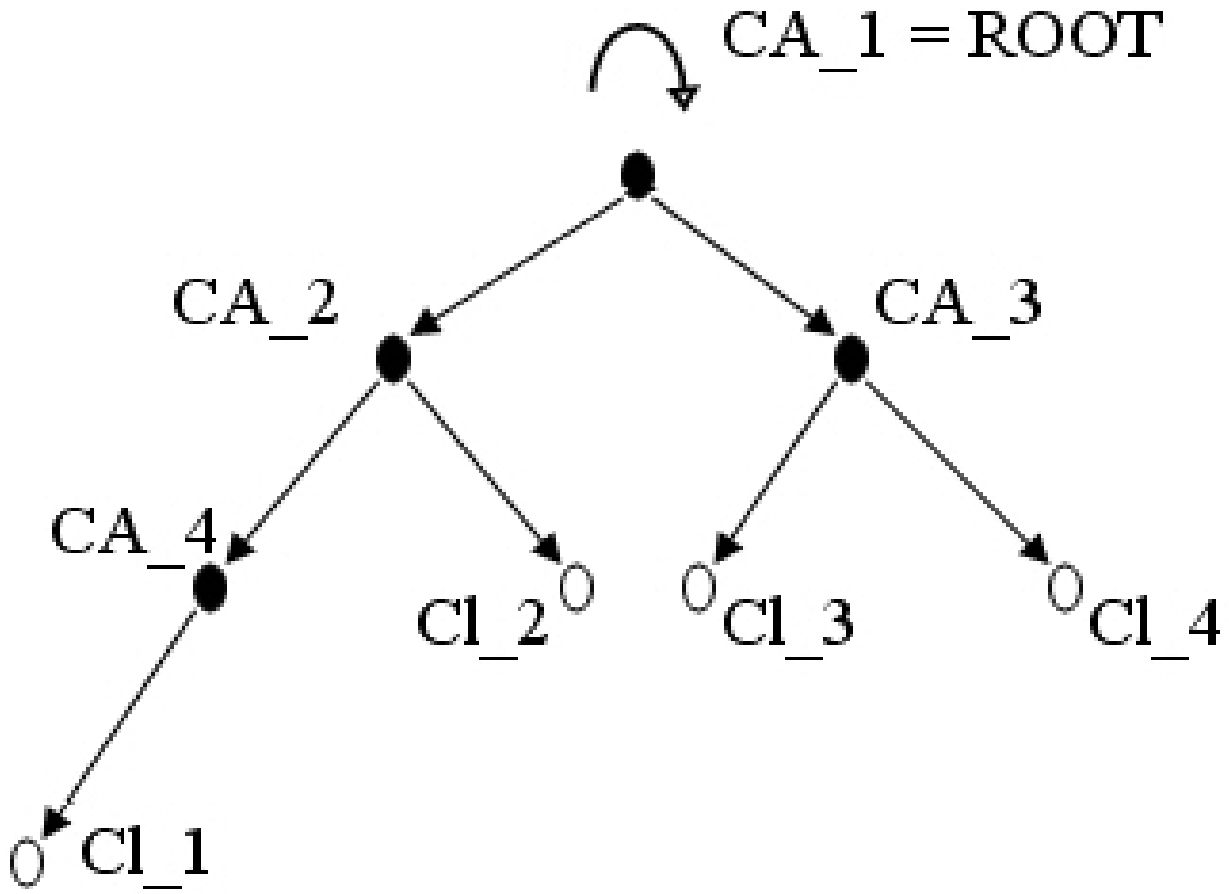



Рис. 2

Источник: https://www.intuit.ru/studies/courses/531/387/lecture/8998?page=2

# Основные компоненты PKI

1 **Удостоверяющий центр** (УЦ) является основной структурой, формирующей цифровые сертификаты подчиненных центров сертификации и конечных пользователей.
УЦ является главным управляющим компонентом PKI:
он является доверенной третьей стороной (trusted third party),
это - сервер, который осуществляет управление сертификатами.

2 **Сертификат открытого ключа** (чаще всего просто сертификат) - это данные пользователя и его открытый ключ, скрепленные подписью удостоверяющего центра.
Выпуская сертификат открытого ключа, удостоверяющий центр тем самым подтверждает, что лицо, поименованное в сертификате, владеет секретным ключом, который соответствует этому открытому ключу.

3 **Регистрационный центр** (РЦ) - необязательный компонент системы, предназначенный для регистрации пользователей.

Для этих целей РЦ обычно предоставляет web-интерфейс.
Удостоверяющий центр (УЦ) доверяет регистрационному центру проверку информации о субъекте.
Регистрационный центр, проверив правильность информации, подписывает её своим ключом и передаёт удостоверяющему центру, УЦ, проверив ключ регистрационного центра, выписывает сертификат.

- Один регистрационный центр может работать с несколькими удостоверяющими центрами (т.е. состоять в нескольких PKI).
- Один удостоверяющий центр может работать с несколькими регистрационными центрами.
- Иногда, удостоверяющий центр выполняет функции регистрационного центра.

4 **Репозиторий** - хранилище, содержащее сертификаты и списки отозванных сертификатов (COC) и служащее для распространения этих объектов среди пользователей.

5 **Архив сертификатов** - хранилище всех изданных когда-либо сертификатов (включая сертификаты с закончившимся сроком действия). Архив используется для проверки подлинности электронной подписи, которой заверялись документы.

6 **Центр запросов** - необязательный компонент системы, где конечные пользователи могут запросить сертификата, или отзыв сертификата.

7 **Конечные пользователи** - пользователи, приложения или системы, являющиеся владельцами сертификата и использующие инфраструктуру управления открытыми ключами.

Основные задачи системы информационной безопасности, которые решает инфраструктура управления открытыми ключами:
- обеспечение конфиденциальности информации;
- обеспечение целостности информации;
- обеспечение аутентификации пользователей и ресурсов, к которым обращаются пользователи;
- обеспечение возможности подтверждения совершенных пользователями действий с информацией (неотказуемость, или апеллируемость - англ. non-repudiation).

PKI напрямую не реализует авторизацию, доверие, именование субъектов криптографии, защиту информации или линий связи, но может использоваться как одна из составляющих при их реализации.

## Архитектуры PKI

В основном выделяют 5 видов архитектур PKI, это:
- простая PKI (одиночный УЦ),
- иерархическая PKI,
- сетевая PKI,
- кросс-сертифицированные корпоративные PKI,
- архитектура мостового УЦ

В основном PKI делятся на разные архитектуры по следующим признакам:
- количество УЦ (а также количество УЦ, которые доверяют друг другу),
- сложность проверки пути сертификации,
последствия выдачи злоумышленника себя за УЦ.

# SSL-сертификат

•**SSL-сертификат** создается на основе **п**ротокола SSL (SSL/TLS) для проверки соединения между компьютерами.

•**Сертификаты расположены на безопасном сервере** и используются для шифрования данных и идентификации Web-сайта.

•**SSL-сертификат состоит из двух частей** (двух ключей):

- public-часть - для шифрования трафика от клиента к серверу;
- private-часть – для расшифровывания полученного от клиента зашифрованного трафика на сервере.

•После того как пара ключей (приватный/публичный) сгенерированы, на **основе публичного ключа формируется запрос на SSL-сертификат** в Центр сертификации.

•Существует возможность создать такой сертификат, не обращаясь в Центр сертификации. Подписываются такие сертификаты этим же сертификатом и называются самоподписанными (**self-signed**).

Для активации защищенного соединения для вашего сайта вам потребуется приобрести услугу **"Выделенный IP-адрес"** и **SSL-сертификат**.

SSL-сертификат можно сгенерировать самостоятельно (**self-signed,** в этом случае клиент будет видеть предупреждение в браузере о использовании самоподписанного сертификата), либо приобрести сертификат подписанный **центром сертификации** для своего домена (субдомена или всех субдоменов)

**!!!!! Для создания сертификатов и их подписи можно воспользоваться известной библиотекой *OpenSSL***

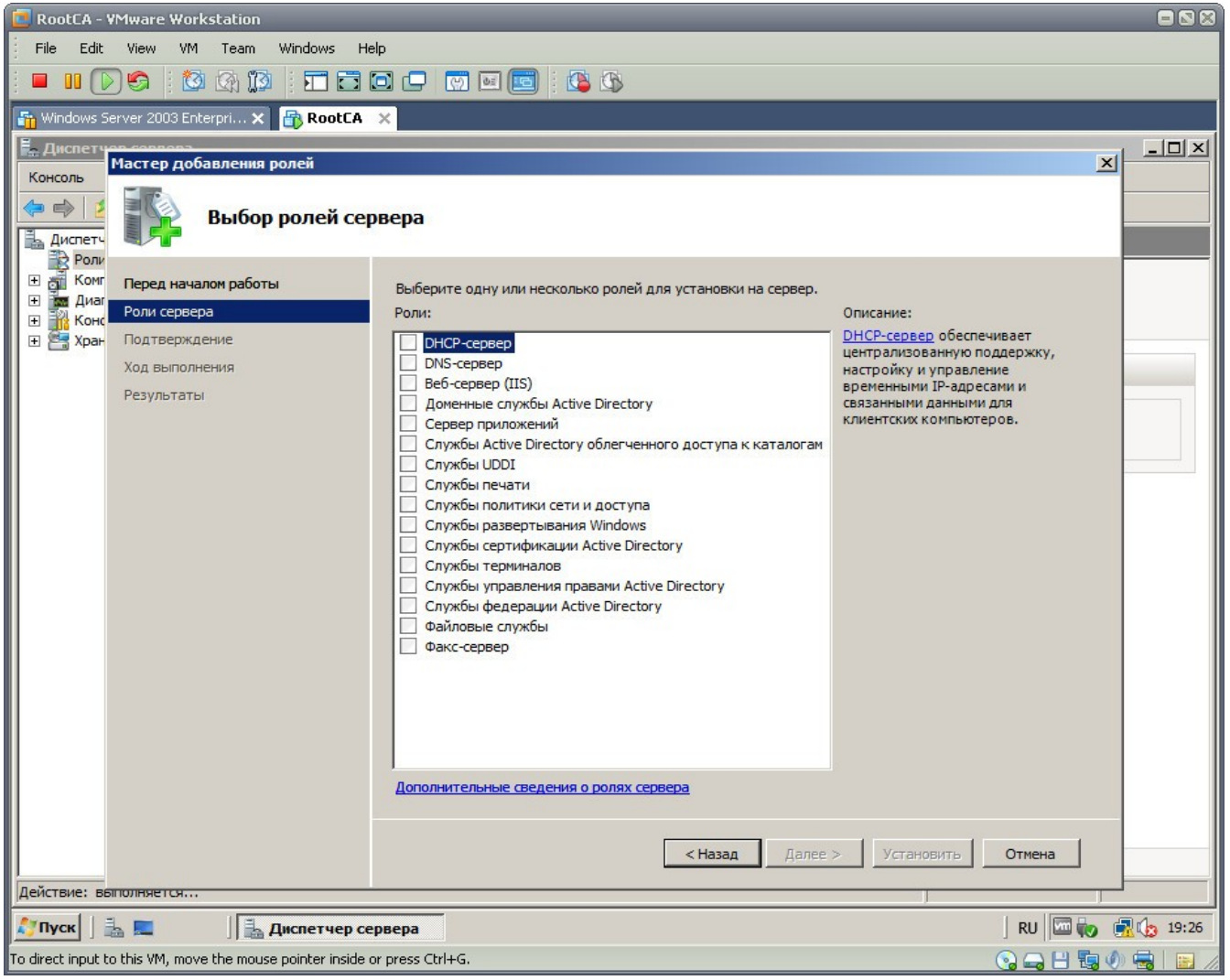
См., например,
https://www.xolphin.com/support/OpenSSL/OpenSSL_-_Installation_under_Windows

**Пример организации двухуровневой иерархической структуры PKI** (В Windows Server 2008 )

- Настроены корневой центр и подчиненный центр сертификации.
- Выдан SSL-сертификат web-узлу и организовано безопасное соединение с ним.

Примерный порядок.

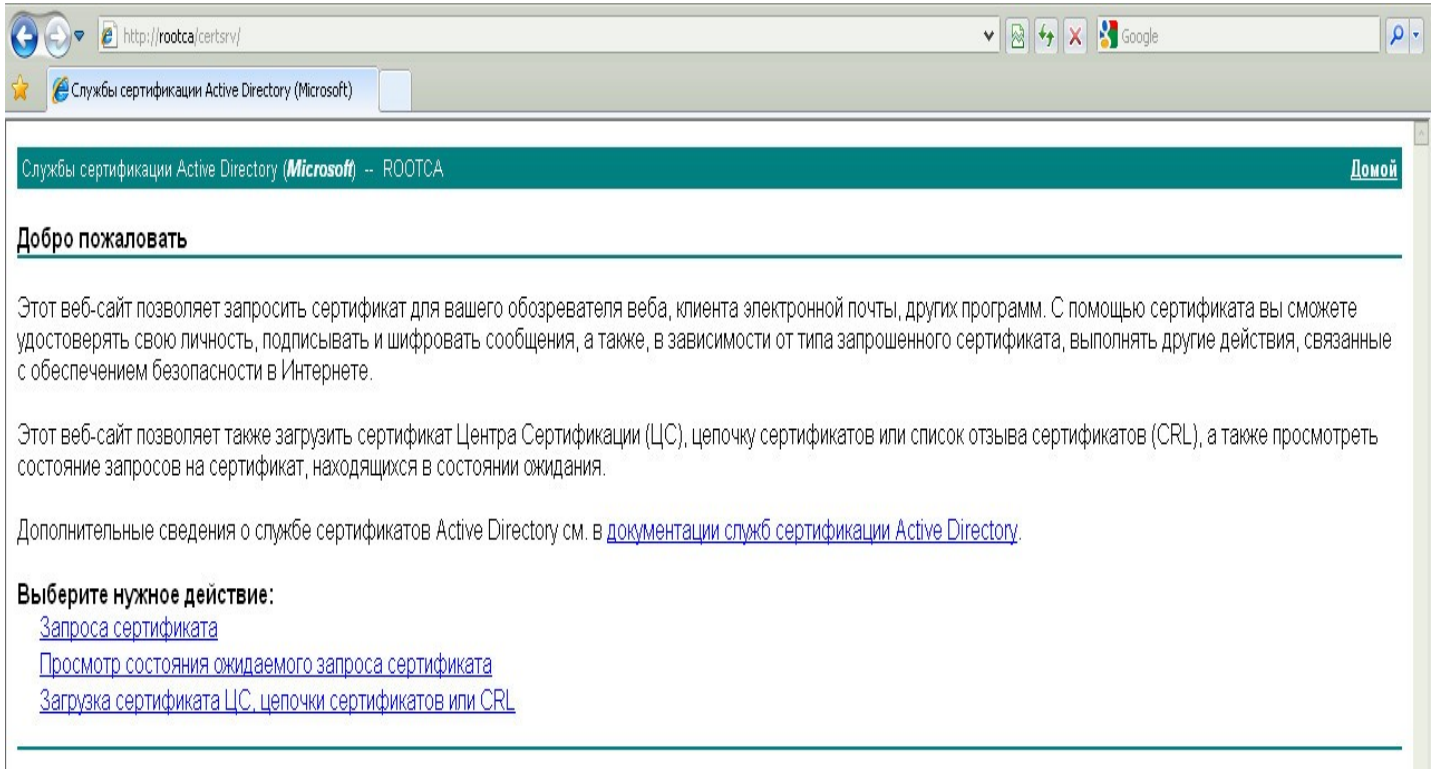
1. Необходимо установить роль “Служба сертификации ActiveDirectory” (рис. 1).


RootCA - VMware Workstation
File Edit View VM Team Windows Help
Windows Server 2003 Enterpri...
RootCA
Мастер добавления ролей
Выбор ролей сервера
Перед началом работы
Роли сервера
Подтверждение
Ход выполнения
Результаты
Выберите одну или несколько ролей для установки на сервер.
Роли:
DHCP-сервер
DNS-сервер
Веб-сервер (IIS)
Доменные службы Active Directory
Сервер приложений
Службы Active Directory облегченного доступа к каталогам
Службы UDDI
Службы печати
Службы политики сети и доступа
Службы развертывания Windows
Службы сертификации Active Directory
Службы терминалов
Службы управления правами Active Directory
Службы федерации Active Directory
Файловые службы
Факс-сервер
Описание:
DHCP-сервер обеспечивает централизованную поддержку, настройку и управление временными IP-адресами и связанными данными для клиентских компьютеров.
Дополнительные сведения о ролях сервера
< Назад
Далее >
Установить
Отмена
Пуск
Диспетчер сервера
RU
19:26
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2. При установке этой службы необходимо выбрать уровень, на котором будет функционировать Центр Сертификации:
- Предприятия,
- Автономный.

Центр сертификации на уровне Предприятия работает совместно с ActiveDirectory.
Это расширяет его функциональные возможности. Например, именно этот цент сертификации можно настроить для автоматической выдачи сертификатов клиентам.

Автономный цент сертификации устанавливается вместе с web службой подачи заявок на сертификаты (рис. 2), что позволяет подавать заявки на сертификаты всем клиентам которые смогут подключиться к этому серверу.

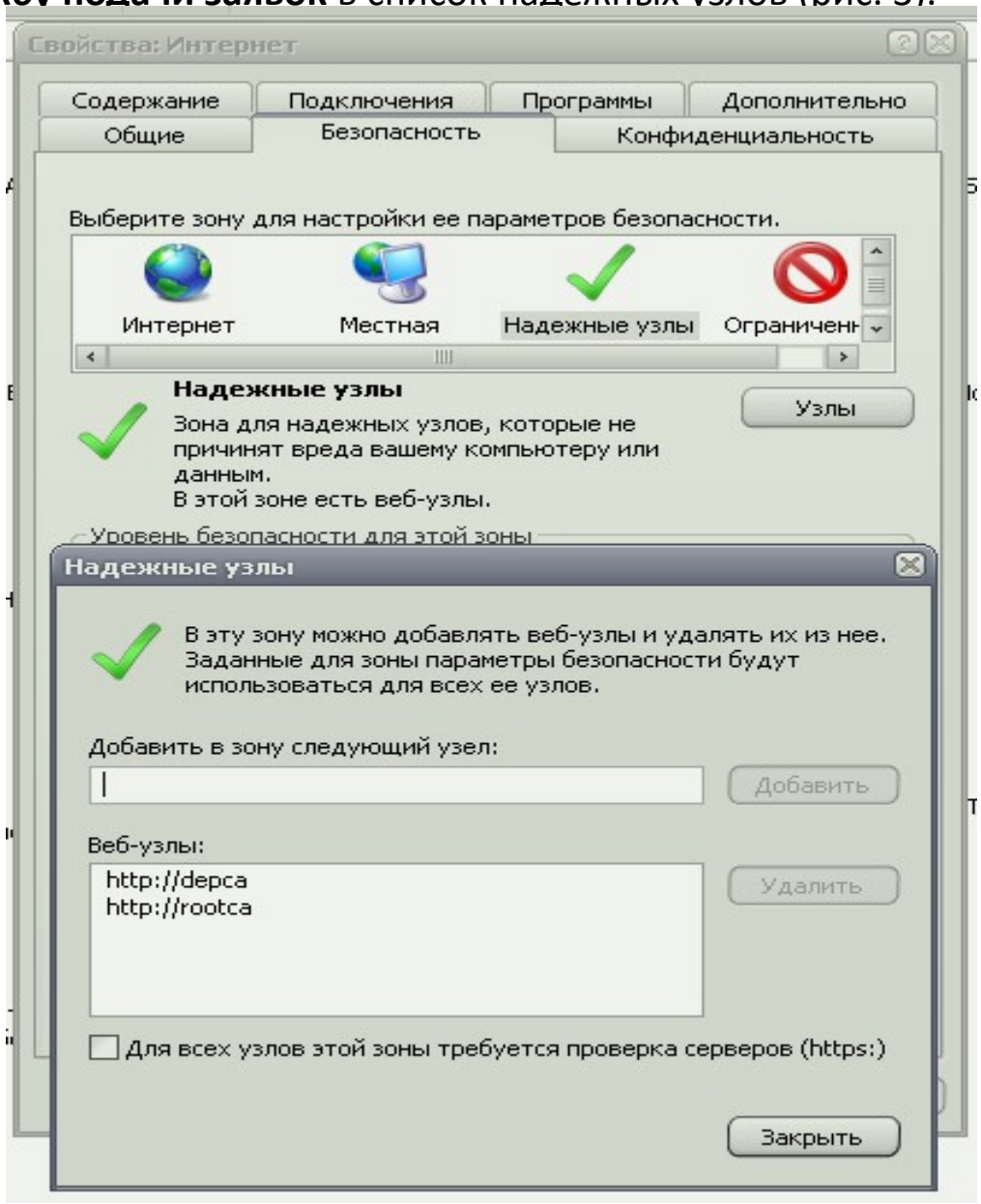

http://rootca/certsrv/
Google
Службы сертификации Active Directory (Microsoft)
Службы сертификации Active Directory (Microsoft) -- ROOTCA
Домой
Добро пожаловать
Этот веб-сайт позволяет запросить сертификат для вашего обозревателя веба, клиента электронной почты, других программ. С помощью сертификата вы сможете удостоверять свою личность, подписывать и шифровать сообщения, а также, в зависимости от типа запрошенного сертификата, выполнять другие действия, связанные с обеспечением безопасности в Интернете.
Этот веб-сайт позволяет также загрузить сертификат Центра Сертификации (ЦС), цепочку сертификатов или список отзыва сертификатов (CRL), а также просмотреть состояние запросов на сертификат, находящихся в состоянии ожидания.
Дополнительные сведения о службе сертификатов Active Directory см. в документации служб сертификации Active Directory.
Выберите нужное действие:
Запроса сертификата
Просмотр состояния ожидаемого запроса сертификата
Загрузка сертификата ЦС, цепочки сертификатов или CRL

4. Необходимо **выбрать тип центра сертификации**:
- Корневой,
- Подчиненный,

В инфраструктуре открытых ключей обязательно должен присутствовать один корневой центр сертификации. Все подчиненный центры сертификации будут обращаться к этому Центру сертификации за сертификатами.

5. **Выбор общего имени нашего центра сертификации**, на какой срок он выдает себе сертификат, и расположения базы сертификатов.
При установке подчиненного центра сертификации также необходимо будет **указать имя корневого центра сертификации** и затем на корневой центр сертификации должен выдать запрошенный сертификат.

6. **Добавить Web-службу подачи заявок** в список надежных узлов (рис. 3).



7. **Загрузить сертификат центра сертификации** или загрузить всю цепочку сертификатов, состоящую из сертификата данного центра сертификации и сертификатов корневых центров сертификации.

8. **Установить полученные сертификаты на компьютер клиента**.
С этого момента клиент будет всегда доверять сертификатам, выданным этими центрами сертификации.
Также можно запросить необходимые сертификаты при помощи службы подачи заявок на сертификаты.
Запрос на сертификат должен быть рассмотрен в течение 10 дней.
Клиент может просмотреть состояния обработки заявки в любой момент зайдя на Web-узел службы подачи заявок с того же браузера и с теми же параметрами сети.

9. **Просмотреть сертиф**
“сертификаты”.

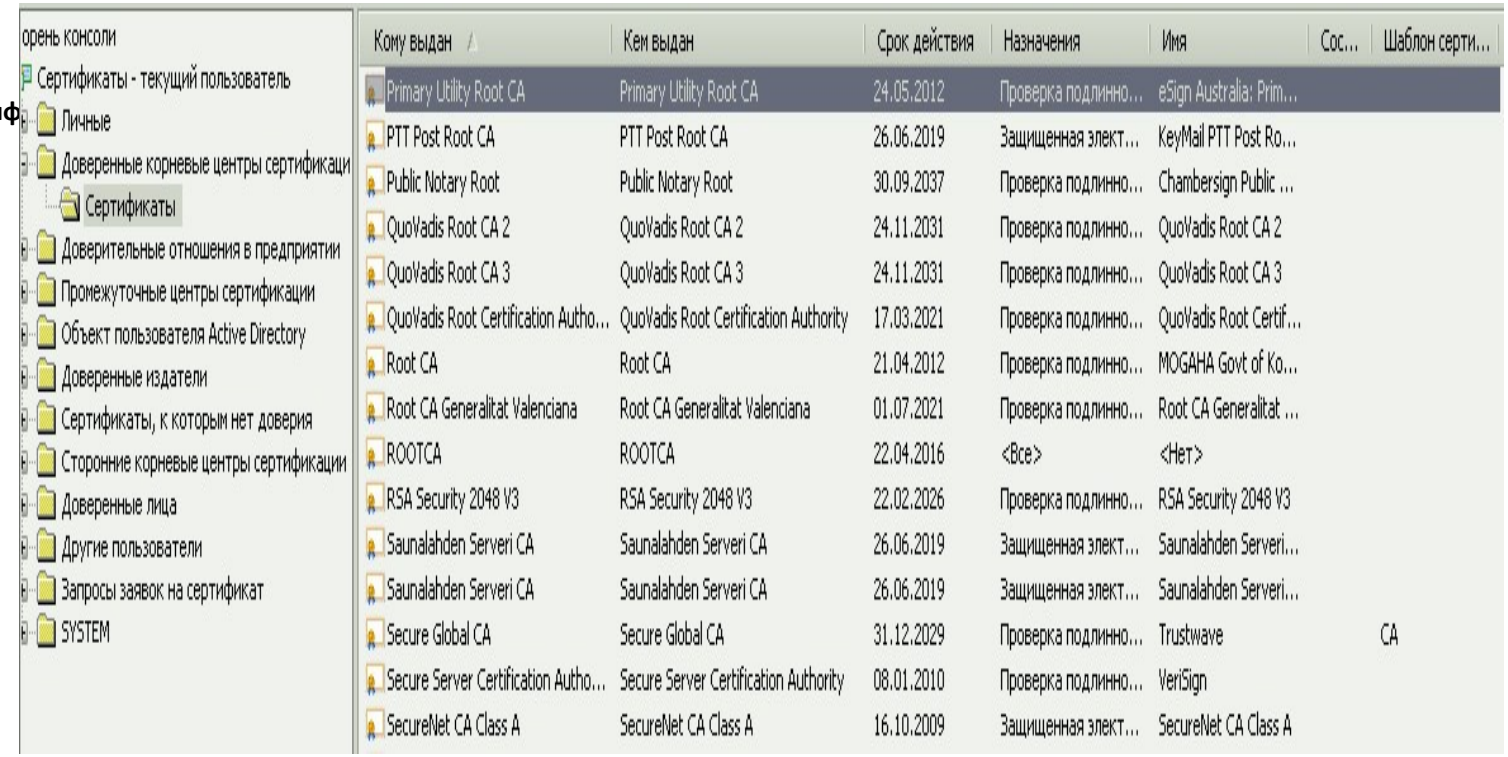



Рис.4

10. **Установка SSL-сертификата**

Сертификат SSL устанавливается и выдается только определенному web-узлу. Для того, чтобы  запросить такой сертификат в IIS6.0 достаточно зайти в меню настройки web-узла, затем во вкладку «Безопасность каталога» и нажать на кнопку “Сертификаты”.

В этом меню можно запросить сертификаты, просмотреть состояние запроса на сертификат, а также получить сертификат (рис. 5).

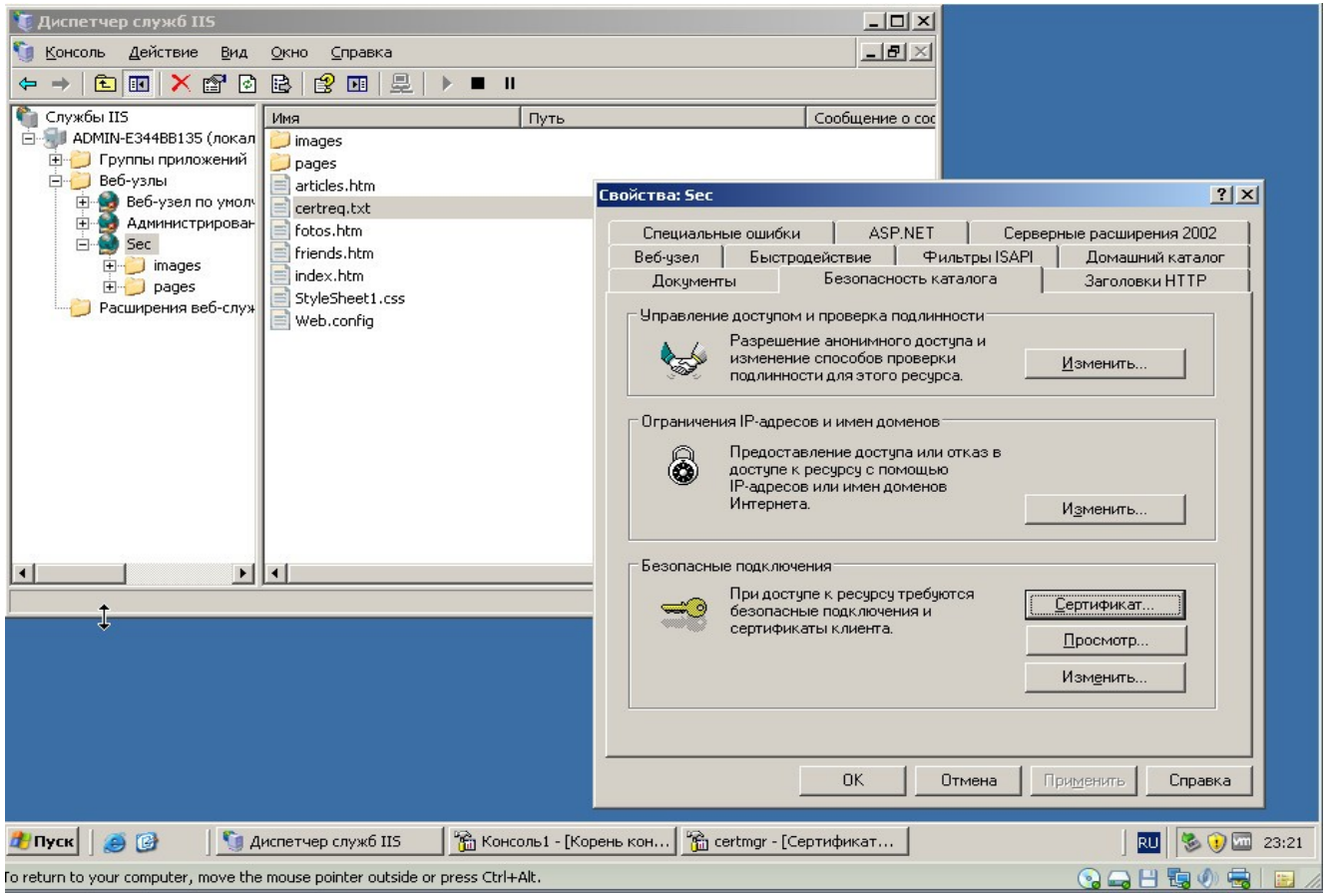



Рис. 5

Нажав на кнопку “Просмотр” , можно **просмотреть текущий установленный сертификат.**

Чтобы **изменить параметры требований к клиенту**, можно нажать кнопку “Изменить”.

Также необходимо **настроить привязки для данного web-узла**.

**Инфраструктура PKI и основные требования к сертификатам регламентируются стандартом X.509**