Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
Московский Государственный Технический Университет им. Н.Э. Баумана

Факультет «Информатика и системы управления»
Кафедра «Компьютерные системы и сети»

Сурков Л.В.

Методические рекомендации к лабораторной работе
по курсу
«Корпоративные сети»

Развертывание служб сертификации корпоративной сети

2009

Основные принципы и понятия

В настоящее время через общедоступные сети передается значительное количество конфиденциальной информации, и объем такой информации непрерывно растет. Поэтому развитие средств обеспечения конфиденциальности и целостности передаваемой информации приобретает все большее значение. Windows предоставляет целый ряд подобных средств, одним из которых является *система цифровых сертификатов.* Применение цифровых сертификатов позволяет решать такие задачи как:

- аутентификация участников соединения. Для обеспечения аутентификации при установлении соединения клиент и сервер обмениваются своими сертификатами и проверяют их подлинность. Аутентификация участников соединения позволяет гарантировать, что к серверу подключился авторизованный клиент, а клиент устанавливает подлинность сервера, с которым установлено соединение.
- обеспечение конфиденциальности передаваемой информации. Конфиденциальность информации может быть обеспечена при помощи шифрования передаваемых сообщений.
- обеспечение целостности передаваемой информации. В некоторых случаях бывает важна не столько конфиденциальность сообщения, сколько его неизменность. В этом случае информация передается в незашифрованном виде, но к сообщению в зашифрованном виде добавляется некий параметр, позволяющий удостовериться в неизменности сообщения. В качестве такого параметра, например, может использоваться контрольная сумма исходного сообщения или некоторая функциональная выборка () передаваемого сообщения. Тогда отправитель строит контрольную сумму/hash исходного сообщения, зашифровывает полученное значение и отправляет его вместе с сообщением. При приеме сообщения получатель строит контрольную сумму/hash полученного сообщения и сравнивает ее с расшифрованным значением. Если значения совпадают, то сообщение получено в неизмененном виде. Для обеспечения целостности данных требуется значительно меньше вычислительных ресурсов, чем для шифрования всего сообщения целиком, поэтому в некоторых случаях оптимальным является обеспечение целостности, а не конфиденциальности данных.

Система цифровых сертификатов Windows Server 2008/2003 основана на стандарте инфраструктуры открытых ключей IETF X.509 v3, что позволяет обеспечить взаимодействие со множеством приложений сторонних производителей. Рассмотрим основные принципы, положенные в основу системы цифровых сертификатов.

Шифрование является наиболее эффективным способом обеспечения конфиденциальности сообщений. Для шифрования сообщений алгоритм шифрования использует специальный параметр - ключ шифрования. Именно он обеспечивает уникальность работы алгоритма в каждом конкретном случае и позволяет говорить о конфиденциальности зашифрованного сообщения даже при общеизвестном алгоритме шифрования. Все алгоритмы шифрования можно разделитьна две большие группы:

- шифрование с использованием симметричного ключа;
- шифрование с использованием открытого ключа.

В системах шифрования *с симметричным ключом* как прямое, так и обратное преобразования сообщения производятся с использованием одного и того же секретного ключа (Secret Key). Знание секретного ключа позволяет как просмотреть, так и создать

или изменить содержимое сообщения, поэтому этот ключ должен храниться в строжайшей тайне. Популярность алгоритмов шифрования с симметричным ключом объясняется их низкой вычислительной сложностью и быстротой. Широко распространенными системами шифрования с симметричным ключом являются шифрование по стандарту DES, 3DES, AES, IDEA, Blowfish/Twofish, RC4. Однако, несмотря на все преимущества, шифрование с симметричным ключом имеет весьма существенный недостаток. Для того, чтобы получатель сообщения мог его прочесть, ему необходимо знать секретный ключ. В случае, если во время обмена сторон ключами злоумышленник смог перехватить ключ, то вся зашифрованная с его применением информация будет скомпрометирована.

В системах шифрования *с открытым ключом* используется принцип асимметричного шифрования. В этих системах используются два ключа - секретный (Private Key) и открытый (Public Key) ключи. Сообщение, зашифрованное с использованием секретного ключа, может быть расшифровано только при помощи открытого и наоборот. Поэтому такую систему шифрования также называют шифрованием с асимметричным ключом. Секретный и открытый ключи создаются одновременно, причем таким образом, что, зная открытый ключ, вычислить при помощи него секретный ключ очень сложно или невозможно. В дальнейшем все заинтересованные лица обмениваются открытыми ключами и используют их для шифрования передаваемой информации. В отличие от шифрования с секретным ключом при шифровании с открытым ключом перехват открытого ключа не приведет к раскрытию шифра.

Алгоритмы генерации пары секретный/открытый ключ и шифрования данных с их помощью должны обеспечивать высокую стойкость шифра таким образом, что, имея открытый ключ и зашифрованное сообщение, злоумышленник не сможет вычислить секретный ключ и расшифровать сообщение. Известны несколько алгоритмов, из которых наиболее распространены:

- алгоритм RSA (Rivest-Shamir-Adleman. Для вычисления секретного ключа, используемого в этом алгоритме, необходимо разложить на простые множители большое (порядка трехсот десятичных знаков) число. Такая процедура требует больших вычислительных ресурсов.
- алгоритм Эль-Гамаля (Ale-Hamale). Для вычисления секретного ключа требуется провести процедуру дискретного логарифмирования, что является более сложной задачей, чем разложение числа на простые множители. Поэтому алгоритм Эль-Гамаля считается более стойким, чем алгоритм RSA, однако в случае вскрытия секретного ключа под угрозой оказываются все участники, тогда как при использовании RSA только один участник, чей ключ был взломан.
- алгоритм Диффи-Хэллмана (Diffie-Hellman) используется в протоколе открытого распределения ключей Oakley. Этот алгоритм нельзя в полной мере назвать алгоритмом шифрования с открытым ключом. Однако в его основе лежат принципы, характерные именно для систем шифрования с открытым ключом. Алгоритм Диффи-Хеллмана позволяет участникам соединения совместными усилиями выработать секретный ключ (Secret Key), который будет использоваться для симметричного шифрования передаваемых сообщений.

Основным недостатком систем с открытым ключом является высокая вычислительная сложность применяемых алгоритмов, что делает их трудно применимыми при интенсивном обмене сообщениями. Для решения этой проблемы поступают следующим образом: для шифрования передаваемых данных используются алгоритмы с симметричным ключом, а для обмена необходимыми для его функционирования ключами используется алгоритм шифрования с открытым ключом. При этом обеспечивается безопасный обмен секретными ключами, что позволяет с высокой степенью безопасности

использовать менее ресурсоемкий алгоритм шифрования с симметричным ключом для обеспечения конфиденциальности передаваемого потока данных.

Цифровые подписи (digital signature) используются для аутентификации отправителя сообщения и обеспечения целостности данных, например пересылаемого программного кода.

При асимметричном шифровании открытый ключ использовался для шифрования сообщения, а расшифровать его мог только тот, кто обладает секретным ключом. При построении цифровой подписи все происходит наоборот. В текст сообщения включается заголовок, зашифрованный при помощи секретного ключа отправителя. При этом каждый может получить открытый ключ отправителя и прочесть зашифрованный заголовок. Такой заголовок и называется цифровой подписью отправителя. Никто не может создать сообщение с соответствующим образом зашифрованным заголовком, не зная нужного секретного ключа.

Рассмотренные выше алгоритмы нашли свое отражение в различных стандартах. Так, Национальный институт стандартов и технологий США (ANSI) принял в качестве стандарта шифрования алгоритм Эль-Гамаля, а Международная организация стандартизации (ISO) приняла в качестве такого стандарта алгоритм RSA. Microsoft реализовала в Windows Server Server 2008/2003 поддержку алгоритма RSA и алгоритма Диффи—Хеллмана, включив в состав операционной системы соответствующие службы (Cryptographic Service Providers, **CSP**).

Службы цифровых сертификатов

Основу службы цифровых сертификатов составляют следующие компоненты:

- цифровые сертификаты;
- центры сертификации.

Рассмотрим каждую из этих компонент подробнее.

Цифровой сертификат - специальная структура данных, предназначенная для идентификации владельца открытого ключа. Цифровые сертификаты выдаются специальными доверенными центрами сертификации.

Цифровой сертификат содержит следующую информацию:

- сведения о субъекте. Содержит описание владельца сертификата. В качестве такой информации может выступать имя, адрес электронной почты и т.п.
- открытый ключ владельца сертификата. Содержит собственно открытый ключ, принадлежность которого субъекту требуется подтвердить.
- срок действия сертификата. Указывает срок, в течение которого сертификат остается действительным. Хотя задача вычисления секретного ключа и чрезвычайно сложна и ее решение требует большого количество времени, однако она не является невыполнимой. Кроме того, существует вероятность получения секретного ключа каким-либо другим способом. Ограничение срока действия сертификата позволяет, например, сменить ключ прежде, чем тот будет взломан. Срок действия сертификата определяется политикой сертификации выдавшего его центра сертификации.
- сведения об издателе сертификата. Содержит информацию об издателе сертификата, позволяющую его определить. Эта информация используется при проверке подлинности сертификата. Если система считает, что издатель данного сертификата заслуживает доверия, то может быть произведен запрос к нему для выяснения действительности данного сертификата.

– цифровая подпись издателя сертификата. Подпись создается издателем сертификата при его создании. Данная цифровая подпись гарантирует целостность данных сертификата и позволяет аутентифицировать издателя сертификата.

Кроме описанных данных, которые необходимы для функционирования сертификата в принципе, в сертификате содержатся и другие данные, такие, как сведения об области возможного применения сертификата (например, для создания цифровых подписей или для аутентификации пользователя в системе), использованных алгоритмах шифрования и т.д.

Цифровые сертификаты применяются как клиентами, так и серверами. При этом каждый сертификат идентифицирует одну из сторон устанавливаемого соединения. Сертификат сервера позволяет клиенту удостоверится в подлинности сервера, с которым он собирается работать. Сертификат клиента позволяет серверу аутентифицировать клиента, желающего получить доступ к его ресурсам.

Центр сертификации (Certification Authority, **CA**)**.** В случае использования сертификатов каждый участник соединения, проверив цифровую подпись полученного сертификата, сможет проверить его подлинность, а значит и подлинность указанного в нем открытого ключа. Цифровая подпись сертификата выполняется некой третьей стороной, которой доверяют все участники соединения. Центр сертификации выполняет роль той самой третьей стороны, которой доверяют все участники соединения, которая удостоверяет, хранит и предоставляет информацию о сертификатах.

Центры сертификации предназначены для выдачи, отзыва и предоставлении информации о выданных ими сертификатах.

Считается, что открытый ключ ЦС общеизвестен и поэтому не может быть подменен. В качестве примера общеизвестных в Интернет центров сертификации можно привести VerySign, Thawte, KeyWitness и др. Сертификаты с открытыми ключами крупнейших из таких **CA** включены в поставку ОС Windows Server 2008/2003.

Чтобы получить сертификат, пользователь посылает запрос центру сертификации. Запрос содержит данные, необходимые для аутентификации пользователя. Получив заявку, центр сертификации проверяет данные, указанные в ней пользователем. Если данные верны и однозначно идентифицируют пользователя, которому разрешено выдавать сертификат запрошенного типа, то центр сертификации генерирует пару секретный/открытый ключ и передает их клиенту либо клиент генерирует пару секретный/открытый ключ и передает открытый ключ центру. Для формирования цифровой подписи в созданных сертификатах центр сертификации использует свой секретный ключ. Таким образом фактически, выдавая сертификаты, центр сертификации берет на себя ответственность за аутентификацию пользователя.

При проверке сертификата клиент анализирует, кем был выдан данный сертификат, его подлинность и целостность. Сертификат считается недействительным, если нарушена его целостность, подлинность или если он был выдан центром сертификации, которого нет в списке доверенных центров сертификации (**CTL** - Certificate Trust List).

В процессе работы может потребоваться отозвать уже выданный сертификат прежде, чем истечет срок его действия. Для этого отозванный сертификат заносится в специальный список отзыва. По истечению срока действия отозванного сертификата центр сертификации удаляет его из списка отозванных сертификатов.

При проверке действительности сертификата клиент проверяет, нет ли этого сертификата в списке отзыва соответствующего центра сертификации. Если сертификат обнаружен в списке отзыва, то он считается недействительным, даже если срок его действия еще не истек.

Иерархия центров сертификации Центры сертификации могут объединяться в иерархические структуры. Центр сертификации, находящийся на вершине иерархической цепочки, называется корневым, нижележащие - промежуточными, подчиненными или издающими. Связь между вышестоящими и подчиненными центрами сертификации достигается за счет того, что первые удостоверяют подлинность вторых, выдавая им специальный сертификат центра сертификации.

Иерархическая модель построения системы центров сертификации делает данную службу более гибкой и эффективной.

Использование иерархии ЦС позволяет учесть требования различных служб к политике выдачи сертификатов. Возможно создать несколько ЦС, каждый из которых будет специализироваться на работе с сертификатами, предназначенными для какой-либо конкретной цели. К примеру, один центр сертификации может выдавать сертификаты клиентам веб-магазина, а другой - сертификаты для аутентификации сотрудников предприятия.

При использовании иерархии ЦС возможно учесть различные требования к безопасности каждого конкретного сервера сертификации, передать управление некоторыми из них системным администраторам соответствующих подразделений.

Установка в каждом узле собственного сервера сертификации позволит сократить сетевой трафик между сайтами. Клиенты будут обращаться к ЦС своего сайта, не создавая дополнительного межсайтового трафика

Пользователи, доверяющие корневому или промежуточному центру сертификации, автоматически доверяют и всем подчиненным центрам сертификации. Поэтому корневые и промежуточные центры сертификации должны обладать наиболее высокой степенью доверия и иметь наиболее жесткую политику выдачи сертификатов. Обычно не рекомендуется, чтобы промежуточные и тем более корневые ЦС выдавали сертификаты конечным пользователям.

Если планируется использовать систему сертификации не только внутри организации, но и в Интернет, то в качестве корневого центра сертификации потребуется прибегнуть к услугам общественного центра сертификации, такого, как, например, VerySign. В этом случае любой пользователь Интернет, доверяющий соответствующему общественному центру сертификации, будет доверять и подчиненным ему центрам сертификации вашего предприятия. Такие пользователи смогут проверить подлинность сертификата и использовать его для защиты информации.

Реализация службы цифровых сертификатов в ОС Windows Server 2008/ 2003.

Windows Server 2008/2003 включает все компоненты, необходимые для развертывания системы цифровых сертификатов, при этом сервер сертификации поставляется как часть операционной системы. Интеграция служб сертификации с ОС позволяет получить дополнительные преимущества в их эксплуатации и администрировании.

Windows Server 2008/2003 позволяет использовать цифровые сертификаты для:

- обеспечения безопасности Web-коммуникаций. Веб-сервер может использовать сертификаты для аутентификации клиентов при доступе к конфиденциальной информации. Также возможно шифрование передаваемых веб-сервером документов.

- обеспечения целостности и конфиденциальности сообщений электронной почты. Цифровые сертификаты могут использоваться как для создания подписи сообщения, так и для его шифрования.
- цифровой подписи программного кода. Программный код, распространяемый в открытых сетях, представляет особую угрозу как безопасности отдельных компьютеров, так и корпоративной сети в целом. Цифровая подпись программного кода позволяет удостовериться в неизменности кода и определить его автора. В зависимости от результатов проверки пользователь может определить степень доверия к полученным данным и принять решение о возможности их использования..
- аутентификации клиентов при входе в сеть. Windows Server 2008/2003 предоставляет возможность использования сертификатов, выданных корпоративным ЦС, для входа в систему.
- аутентификации клиента при использовании IPSec;
- шифрования ключей в EFS. Для обеспечения защиты секретного ключа, используемого при шфровании файловой системы, применяется шифрование с открытым ключом. Ключ шифруется с использованием открытых ключей из сертификатов пользователей, имеющих доступ к защищенным данным. Аналогичным образом создается список ключей восстановления.

Windows Server 2008/2003 предоставляет две базовые модели развертывания службы сертификатов:

- модель корпоративных ЦС.
- модель одиночных ЦС;

Модель корпоративных центров сертификации (Enterprise CA)

Корпоративные центры сертификации позволяют выдавать сертификаты для:

- создания цифровых подписей;
- защиты сообщений электронной почты;
- аутентификации на веб сервере;
- входа в домен с помощью смарт-карты.

Корпоративные центры сертификации требуют, чтобы сервер был членом домена Active Directory. Active Directory используется для автоматической аутентификации пользователей, публикации сертификатов и списка отзыва сертификатов и другой информации службы цифровых сертификатов. Для того, чтобы сервер сертификации мог публиковать данные в Active Directory, необходимо, чтобы он входил в группу “Certificate Publishers”.

Корпоративные центры сертификации могут автоматически принимать решение о выдаче сертификата определенного типа или отклонении запроса, а могут делать это по решению администратора. Решение принимается на основании текущей политики безопасности и прав доступа, установленных для сертификатов данного типа.

При установке корневого корпоративного центра сертификации он автоматически добавляется в список доверенных корневых центров сертификации своего домена и группу “Certificate Publishers”. Однако для публикации сертификатов в других доменах установленному центру сертификации потребуется делегировать соответствующие права.

В больших сетях Инфраструктуры открытого ключа Корневой ЦС предприятия обычно используется для выпуска сертификатов только для подчиненных ЦС предприятия, которые в свою очередь выпускают сертификаты для пользователей и компьютеров.

Подчиненный ЦС предприятия – это сервер сертификатов, который располагается в иерархии под корневым ЦС предприятия. Часто подчиненный ЦС используется для специфической цели – для выдачи сертификатов или пользователям, или компьютерам, или некоторой части организации. Подчиненный ЦС требует всех тех же служб и привилегий как корневой ЦС и не может быть создан до тех пор, пока не создан корневой ЦС предприятия. Заметьте, что хотя корневым ЦС организации может быть любой внутренний сервер сертификации Windows Server 2008/2003, это также может быть внешний ЦС, такой как Verisign. Фактически, если вы хотите, чтобы окружающий мир доверял подлинности ваших сертификатов, вам просто необходимо будет использовать Внешний Корневой ЦС, такой как Verisign. В противном случае, внешним пользователям потребуется копия сертификата вашего Корневого ЦС, которой у них, скорее всего, нет.

Одним из главных преимуществ настройки Служб сертификации в качестве ЦС предприятия является то, что в данном случае они могут не только интегрироваться с Active Directory, но также получают возможность управлять большим количеством черновой работы через настройки Групповых политик, например, автоматически обрабатывать запросы на сертификаты (этот процесс также известен как авто-регистрация). Групповые политики Windows Server 2008/2003 могут выполнять следующие задачи:

• Позволяют клиентским компьютерам домена автоматически запрашивать и устанавливать сертификаты компьютера. Этот сертификат идентифицирует компьютер и может быть использован для целей IPSec шифрования/аутентификации и также рекомендуется для основанных на L2TP соединений VPN (так как оба – пользователь и компьютер должны быть идентифицированы для данного вида соединений). Эта опция устанавливается в узле Computer Configuration/Windows Settings/Security Settings/Public Key Policies/Automatic Certificate Request Settings в Групповой политике. Любая система, к которой будет применяться данная политика, будет автоматически запрашивать, загружать и устанавливать данный сертификат.

• Создают и распределяют список доверия сертификатов. Это позволяет снабдить клиентские компьютеры списком доверенных Корневых ЦС и связанной с ними иерархией ЦС. Это опция устанавливается в папке Computer Configuration/Windows Setting/Security Setting/Public Key Policies/Enterprise Trust в оснастке Групповая политика. Реальная настройка осуществляется при помощи специального мастера Certificate Trust List wizard.

• Устанавливают доверительные отношения с другими внешними корневыми центрами, например, такими, которые не являются частью вашей организации. Это может быть использовано для осуществления безопасных партнерских отношений между организациями. Соответствующие настройки выполняются в папке Computer Configuration/Windows Setting/Security Setting/Public Key Policies/Trusted Root Certification Authorities в оснастке Групповая политика.

• Добавлять Агентов восстановления для использования Encrypted File System (EFS). И хотя учетная запись администратора является агентом восстановления по умолчанию, могут быть добавлены и другие в папке Computer Configuration/Windows Setting/Security Setting/Public Key Policies/Encrypted Data Recovery Agents.

Модель одиночных центров сертификации(Stand-Alone CA)

Одиночные центры сертификации позволяют выдавать сертификаты для:

- создания цифровых подписей;
- защиты сообщений электронной почты;
- аутентификации на веб-сервере

- туннеля IPSec
- проверки подлинности клиента.

Одиночные центры сертификации могут не являться членом домена Windows Server 2008/2003 и не требуют наличия Active Directory, хотя могут его использовать. Одиночные ЦС не могут выдавать сертификаты, предназначенные для входа в домен. Такие ЦС применяются при интеграции сети предприятия в Интернет или при использовании собственного модуля политик сертификации.

Для получения сертификата у одиночного ЦС пользователю необходимо предоставить полную информацию о себе. Все полученные запросы на выдачу сертификатов ставятся в очередь, пока администратор не проверит предоставленную в них информацию и явно не разрешит или не запретит выдачу сертификата по соответствующему запросу, но данный процесс можно и автоматизировать.

В случае, если одиночный ЦС использует Active Directory, то он получает дополнительные возможности.

Если ЦС имеет разрешение на запись в Active Directory, то при установке корневого одиночного ЦС он автоматически добавляется в список доверенных корневых ЦС, поэтому надо быть осторожным при определении правил выдачи сертификатов. По умолчанию все запросы ставятся в очередь для проверки данных администратором.

Также одиночный ЦС, имеющий право на запись в Active Directory, получает возможность публикации в каталоге выданных им сертификатов.

Важным моментом при выборе типа ЦС, является характер вашей сети и то, для каких целей вы собираетесь использовать сертификаты. Если это сугубо внутреннее использование, тогда ваш выбор будет строиться исходя из характеристик вашей сети (например, если в сети установлена AD, тогда вы можете использовать как Изолированные, так и ЦС предприятия). Если же вы будете использовать сертификаты для обеспечения безопасности открытого web-сайта, тогда должен обязательно привлекаться внешний ЦС, либо для предоставления сертификата самому сайту, либо через создание структуры доверия. Например, если вы получаете доступ к безопасному web-сайту и щелкаете мышкой на значок lock в нижнем левом углу вашего броузера, вы сможете увидеть путь сертификации для данного сайта

Сервер сертификации Windows Server 2008/2003

Microsoft Certificate Server выполнен в виде службы Windows Server 2008/2003, которая обрабатывает запросы сертификатов, ведет журнал операций и очереди запросов. Сервер можно разбить на следующие основные функциональные блоки:

- входной модуль;
- выходной модуль;
- исполнительный модуль;
- модуль политик сертификации;
- очередь запросов;
- журнал.

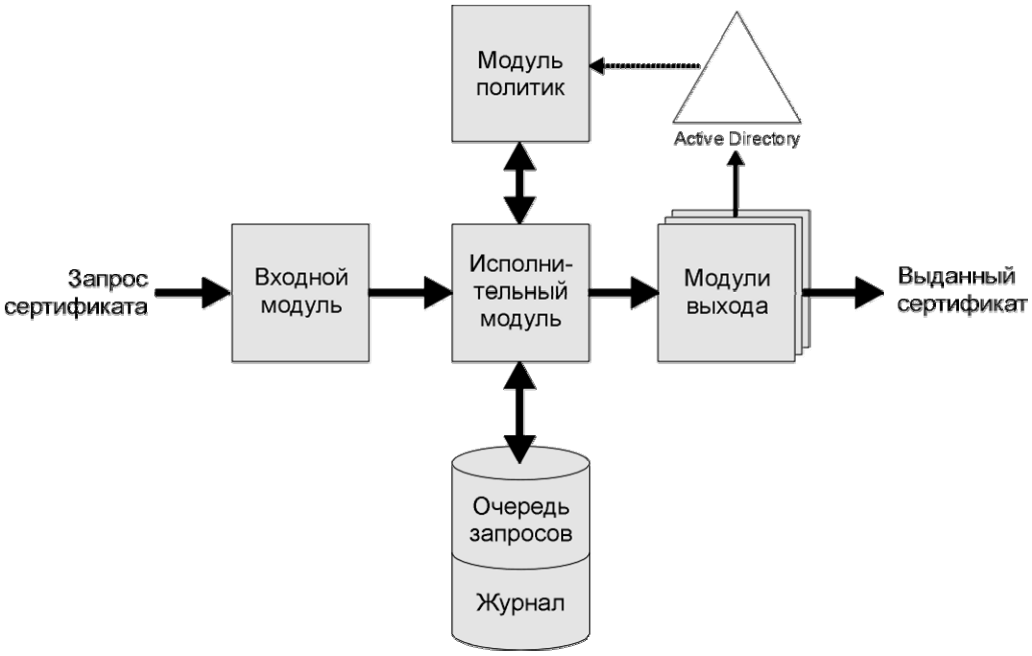

Рис. 1
Функциональная схема сервера сертификации

Исполнительный модуль, очередь запросов и журнал выполнены как единая служба Windows Server 2008/2003. Входной и выходной модули, модуль правил и утилиты администрирования исполняются в отдельных процессах. Рассмотрим каждый модуль более подробно.

Входной модуль

Все запросы клиентских приложений, таких как веб-сервер или почтовый клиент, принимаются входным модулем. Основная задача входного модуля – распознать запрос клиентского приложения и передать его исполнительному модулю. Наличие входного модуля позволяет реализовать специфические потребности клиентских приложений, отсутствующие в стандартном входном модуле.

Выходной модуль

Входной модуль обеспечивает публикацию готовых сертификатов и списков отзыва, используя необходимые транспортные механизмы и поротоколы. К примеру, выходной модуль может публиковать выданный сертификат в Active Directory или отправлять сертификат запросившему его клиенту по электронной почте. По умолчанию исполнительный модуль передает информацию всем установленным модулям выхода.

Как для входного, так и для выходного модулей разработаны специальные COM-интерфейсы, позволяющие создавать свои модули. Такие модули могут решать задачи, специфические для данного конкретного применения сервера сертификатов.

Исполнительный модуль

Исполнительный модуль является ядром сервера сертификатов. Он обеспечивает взаимодействие всех составляющих сервера, обеспечивая его функционирование в соответствии с выполняемой в текущий момент задачей.

Модуль политик сертификации

Выполняет проверку данных запросов выдачи сертификатов на соответствие правилам политики сертификации. Также модуль политики сертификации применяется для анализа дополнительной информации, содержащейся в запросе, и соответствующей настройки дополнительных параметров сертификата.

Очередь запросов

Все поступившие запросы к серверу сертификации на время ожидания обработки помещаются в очередь запросов.

Журнал

В журнал заносятся все данные о выдаче, отказах в выдаче и отзыве сертификатов. Журнал позволяет администраторам отслеживать и анализировать сведения о деятельности сервера. Также в журнал помещаются данные о планируемых отзывах сертификатов. Журнал может быть использован для восстановления данных сервера сертификации после сбоя.

Практическая часть

Установка Microsoft Certificate Services

Для установки сервера цифровых сертификатов в мастере установки программного обеспечения (Пуск | Панель управления | Установка и удаления программ) выберите (Установка и удаление компонентов Windows | Службы сертификации)

Заметьте, что если вы попытаетесь установить Службы сертификации, вам будет предложено диалоговое окно, из которого следует, что в последствии вы не сможете переименовать систему, примкнуть или удалить ее из домена до тех пор, пока не будут удалены Службы сертификации.

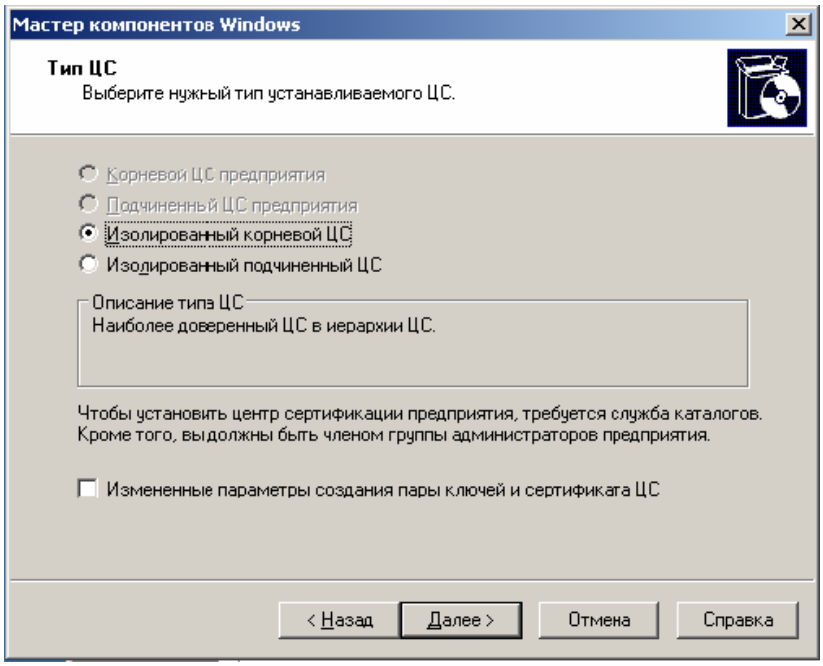

Рис. 2
Мастер установки Microsoft Certificate Services

На первом этапе предлагается определить роль устанавливаемого сервера сертификатов. Имеются 4 варианта:

- Корневой ЦС предприятия;
- Подчиненный ЦС предприятия;
- Изолированный корневой ЦС;
- Изолированный подчиненный ЦС.

В случае установки ЦС не в Active Directory, первые два варианта недоступны.

Если установлен флаг “Измененные параметры создания пары ключей и сертификата ЦС”, то появляется возможность дополнительно указать используемые: службу криптографии, алгоритм шифования и имена имеющихся сертификатов.

В случае установки подчиненного ЦС вам будет предложено указать соответствующий доверенный ЦС, который выдаст соответствующий сертификат ЦС. При установке корневого ЦС он сам выдает себе необходимый сертификат.

На следующем шаге необходимо указать идентификационную информацию создаваемого ЦС.

На последнем шаге предлагается указать расположение журнала и базы данных сервера сертификатов.

После того, как Службы сертификации установлены, сервер готов принимать запросы на выдачу сертификатов от клиентов. Для Изолированного ЦС эти запросы должны быть сделаны через web-броузер, по адресу URL http://<имя компьютера>/certsrv. Соответствующий мастер проведет вас через процесс осуществления запроса шаг за шагом.

Процесс запроса сертификата также включает в себя предоставление информации о пользователе, об использовании сертификата и т.д.

Задание *– установите изолированный корневой ЦС вместе со службой WWW (сервер приложений|служба IIS| служба WWW).*

Управление Certificate Services.

– Для управления службой сервера цифровых сертификатов служит оснастка “Certificate Authority”, устанавливающаяся вместе с сервером сертификатов.

–

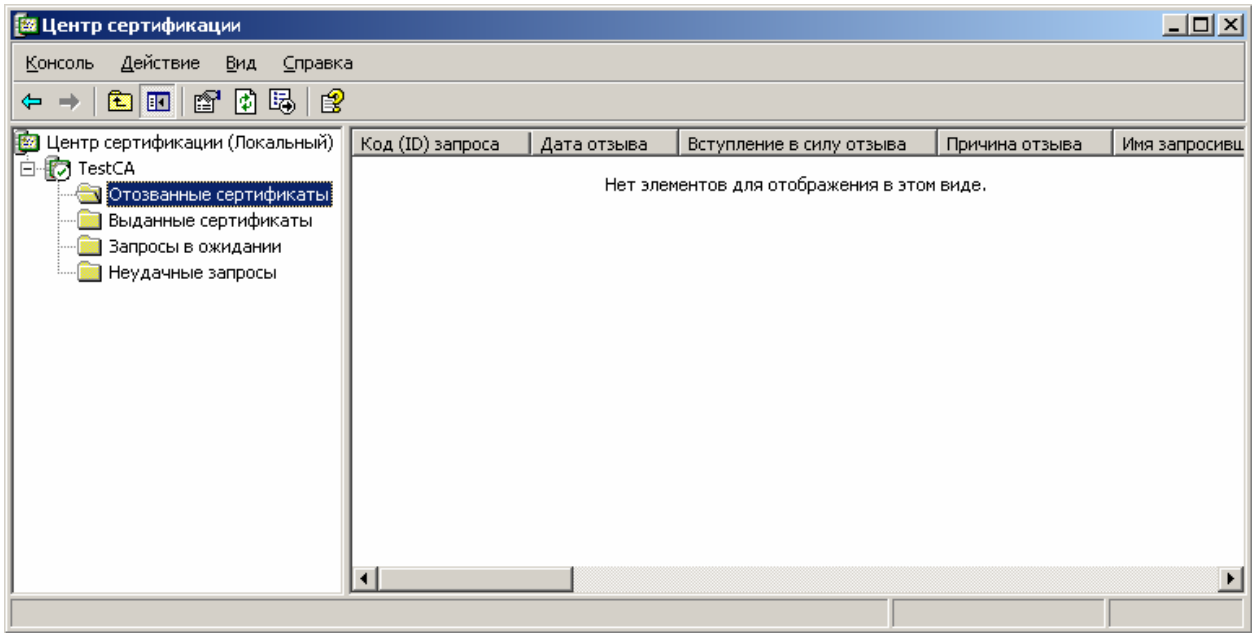

Рис. 3
Оснастка “Центр сертификации”

Дерево управления серверов сертификатов содержит следующие ветви:

- Выданные сертификаты – позволяет просмотреть список выданных сертификатов;
- Запросы в ожидании – позволяет просмотреть список текущих запросов на выдачу сертификатов;
- Неудачные запросы – позволяет просмотреть список отклоненных запросов;
- Отозванные сертификаты – позволяет просмотреть список отозванных сертификатов;

Управление модулями сервера сертификации

Для управления модулями сервера сертификации в оснастке “Центр сертификации” выберите (<имя сервера сертификатов> | R-Click | Свойства).

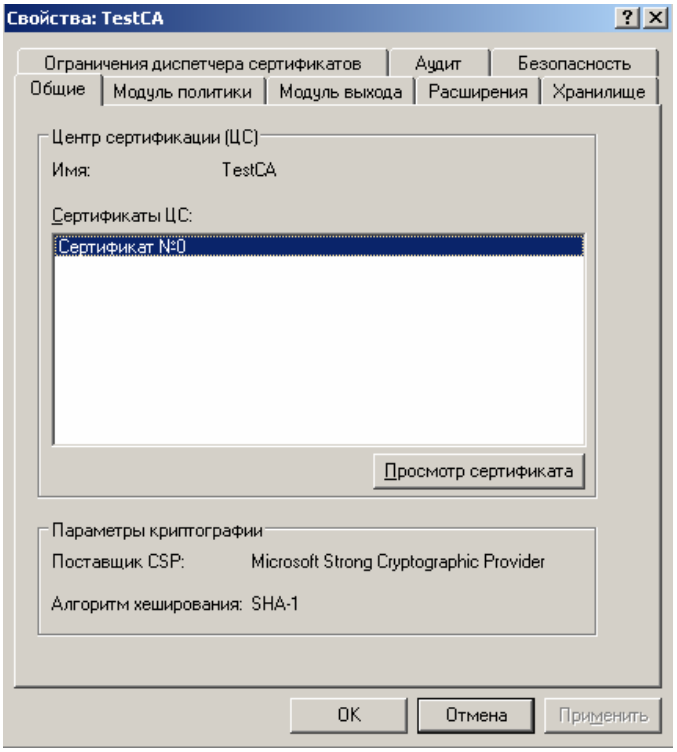

Рис. 4
Свойства центра сертификации

На странице “Общие” вы можете просмотреть общие настройки сервера и его сертификат ЦС.

Страница “Модуль политики” позволяет выбрать и настроить используемый модуль политик сертификации. Здесь определяется действие, производимое сервером сертификатов при получении запроса на выдачу сертификата. Сервер может либо ставить запросы в очередь для дальнейшей проверки предоставленной информации системным администратором, либо работать в автоматическом режиме.

Страница «Модуль выхода» определяет, разрешается ли публикация сертификатов в файловой системе или нет.

На странице “Расширения” указываются URL и точки распространения, по которым будут доступны список отзыва сертификатов и сертификат данного сервера сертификации.

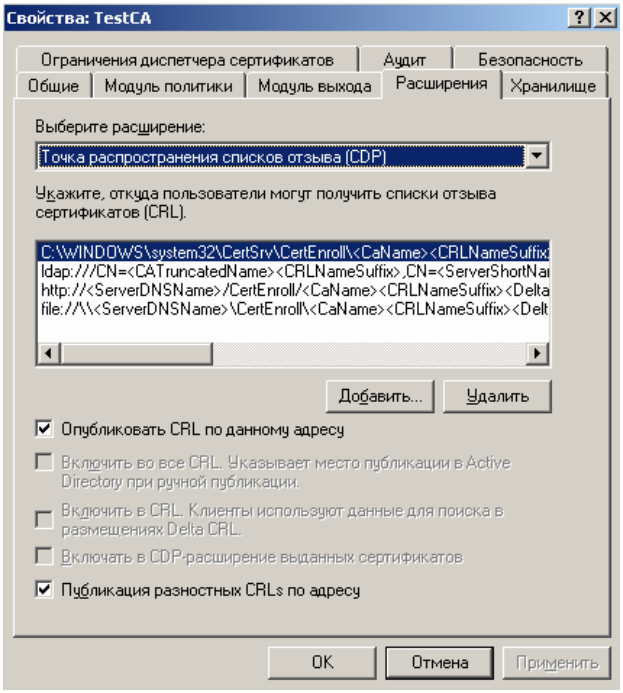

Рис. 5
Параметры модуля "Расширения"

Страница "Хранилище" позволяет просмотреть расположение:
- базы данных сертификатов;
- журнала запросов;
- папки, в которой публикуются сертификаты в случае недоступности Active Directory.

Станица "Безопасность" позволяет управлять доступом к серверу сертификатов.

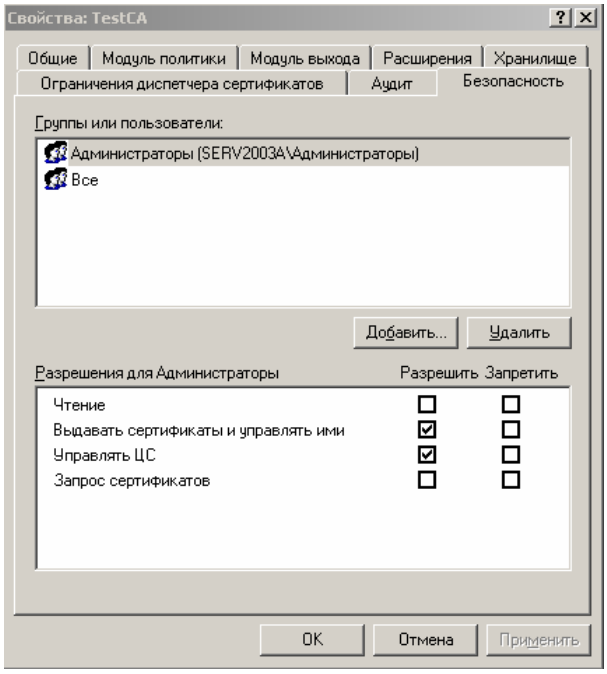

Рис. 6
Управление доступом к серверу сертификатов

Станица "Аудит" отражает политику аудита ЦС.

Задание *–изучите настройки модулей сервера ЦС.*

Управление шаблонами выдаваемых сертификатов в Active Directory

Для определения списка шаблонов, выдаваемых данным сервером сертификатов, используется раздел “Policy Settings” оснастки “Certificate Authority”.

Для добавления шаблона в список выберите (<имя сервера> | Policy Settings | R-Click | New | Certificate to issue), после чего вам будет предложено выбрать один из стандартных шаблонов сертификатов.

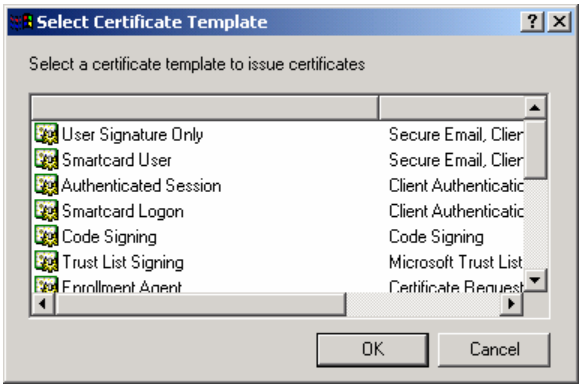

Рис. 7
Выбор шаблона сертификата

– Чтобы определить, какие типы сертификатов разрешено выдавать тому или иному пользователю, каждый шаблон сертификата имеет список контроля доступа. Права доступа пользователей к шаблонам могут быть отредактированы в оснастке “Active Directory Sites and Services” в разделе (Services | Public Key Services | Certificate Templates).

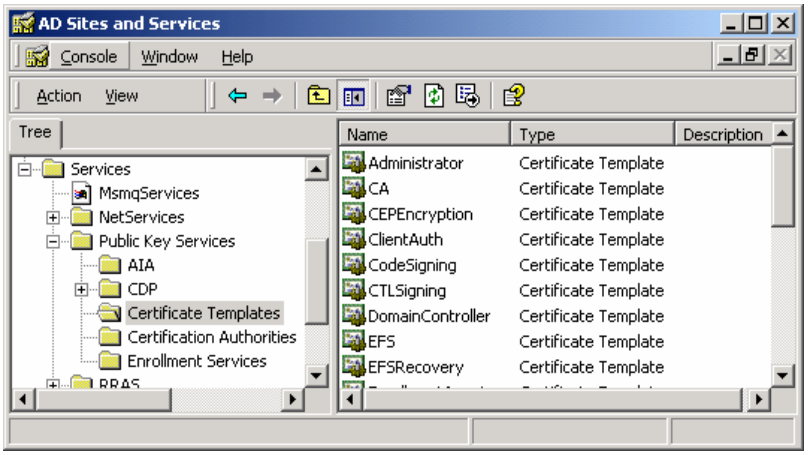

Рис. 8
Шаблоны цифровых сертификатов в оснастке “Active Directory Sites and Services”

Работа с сертификатами

Большинство пользовательских задач по использованию цифровых сертификатов может быть выполнено при помощи оснастки MMC “Сертификаты”. Для ее установки в MMC выберите (Консоль | Добавить удалить оснастку | Добавить | Сертификаты | Для моей учетной записи). Для управления сертификатами пользователей, компьютеров и служб требуется установить по отдельной оснастке.

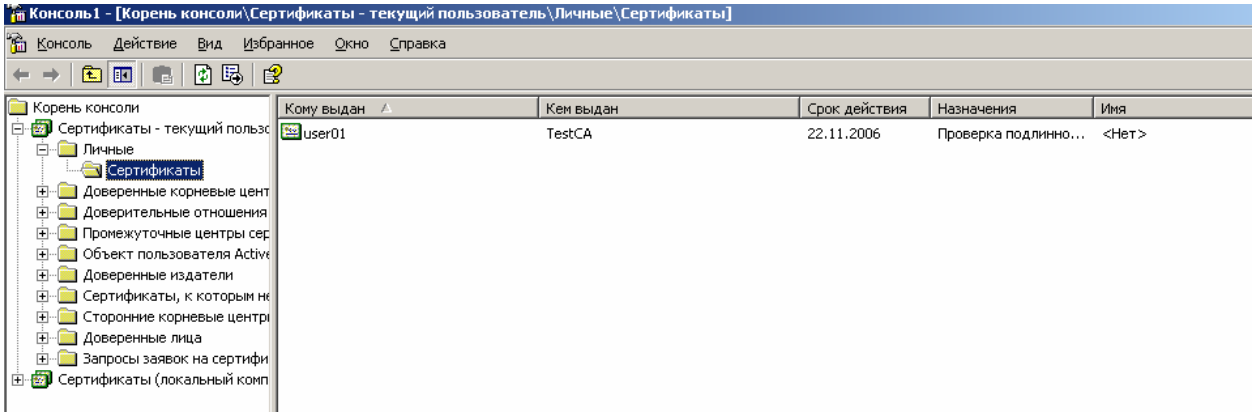

Рис. 9
Оснастка MMC, "Сертификаты".

Запрос сертификата

Любой пользователь может запросить в свое хранилище сертификат. Для того, чтобы запросить сертификат необходимо зайти на сайт http://<имя компьютера>/certsrv/. Эта страничка устанавливается вместе центром сертификации и службой WWW.

На появившейся странице необходимо выбрать «Запрос сертификата». Далее будет предложены шаблоны сертификатов. Если выбрать пункт «расширенный запрос сертификата», то на следующих шагах будет предложено указать используемых: поставщика служб криптографии и сервер сертификатов, к которому будет отослан запрос, а также выбор способа задания запроса (явным образом или через файл запроса PKCS#10).

На последнем шаге формирования запроса сертификата задается его имя и комментарий, описывающий данный сертификат в списке сертификатов.

Обратите внимание на параметры расширенный запрос сертификата. Тип сертификата определят возможную область применения выдаваемого сертификата. Возможно «Пометить ключ как экспортируемый» для дальнейшей возможность импортировать сертификат с закрытым ключом в файл. Это бывает необходимо для переноса сертификата на другой компьютер, либо для сохранения его на отдельном носителе.

Рис. 10

Форма расширенного запроса на сертификат.

После этого запрос отсылается на ЦС. Дальнейшие действия зависят от настройки модуля политики сертификатов. Если он настроен на автоматическую выдачу сертификатов, то на следующей странице будет предложено установить сертификат с закрытым ключом в личное хранилище. При не автоматической работе ЦС, администратору необходимо вручную выпустить сертификат.

Процесс подтверждения для запрошенного сертификата достаточно прост. Используя инструмент Центр Сертификации в Администрировании, откройте опцию Запросы в ожидании и выберите Выпустить или Отвергнуть запрос.

После этого пользователь запросившей сертификат должен будет заново зайти на страничку http://<имя компьютера>/certsrv/, и выбрать «Просмотр состояния ожидаемого запроса сертификата», а затем уже установить его.

Просмотр сертификата

Для просмотра списка выданных вам сертификатов в оснастке “Сертификаты” выберите (Личные | Сертификаты). В правой части окна появится список соответствующих сертификатов. Для просмотра содержимого сертификата выберите нужный сертификат, (R-Click | Открыть).

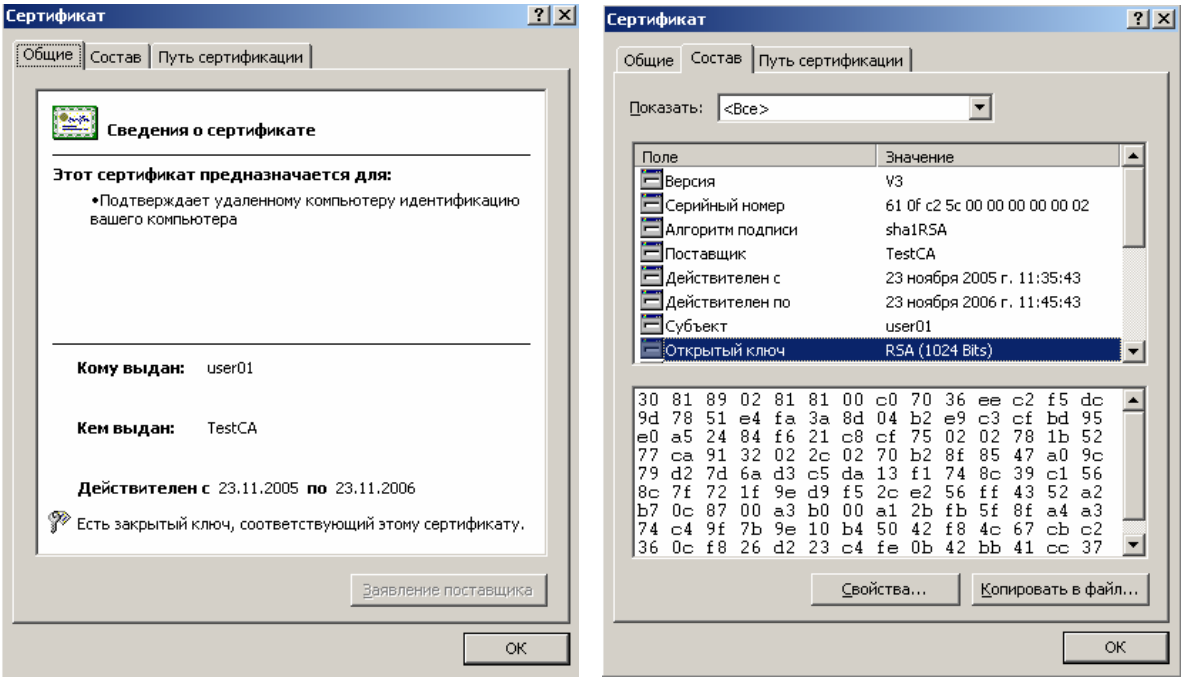

Рис. 11

Просмотр содержимого сертификата.

На вкладке "Общие" отображается, является ли этот сертификат доверяемым. Если да, то ниже будут перечислены его назначения, а также кто, кому и на какой срок его выдал.

На вкладке “Состав” можно просмотреть значения полей сертификата, а на вкладке “Путь сертификации” – положение сертификата в иерархии центров сертификации.

Для редактирования свойств сертификата выберите нужный сертификат, (R-Click | Свойство). Редактор свойств сертификата позволяет изменить имя сертификата, комментарий и список задач, для которых он будет использоваться.

Задание *– Установите необходимые средства управления сертификатами и запросите новый сертификат, поместите его в хранилище сертификатов вашего пользователя. Изучите свойства и содержимое сертификата.*

Управление отзывом сертификатов

Для отзыва выданного сертификата в оснастке “Центр сертификации” выберите (Выданные сертификаты | <отзываемый сертификат> | R-Click | Все задачи | Отзыв сертификата) и укажите причину отзыва сертификата.

Списки отзыва (CRL) ЦС хранятся по адресу: WINDOWS\system32\certsrv\CertEnroll. Устанавливаются списки отзыва через контекстное меню. Там же находится и корневой сертификат ЦС.

В оснастке Сертификаты CRL располагаются в (Промежуточные центры сертификации | Списки отзыва сертификатов)

Список отзыва обновляется с заданным периодом, который устанавливается в свойствах «Отозванные сертификаты» в оснастке Центр сертификации. Там же через контекстное меню можно опубликовать новый CRL.

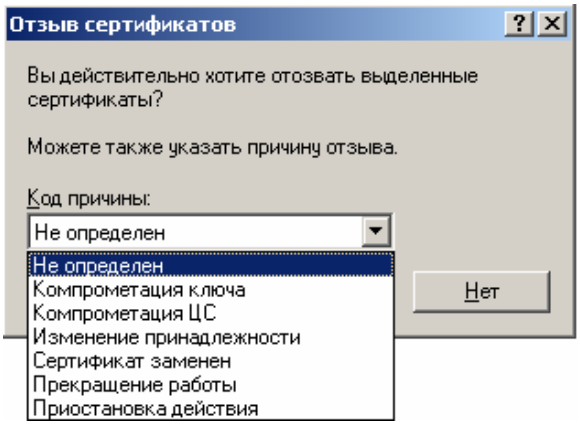

Рис. 12
Отзыв цифрового сертификата

Задание *– Просмотрите список выданных ЦС сертификатов. Отзовите один из выданных сертификатов. Опубликуйте список отзыва сертификатов. Установите новый CRL и убедитесь что он обновился в оснастке «Сертификаты».*

Экспорт сертификата

Сертификаты можно экспортировать и хранить в виде отдельных файлов. Для этого выберите нужный сертификат, (R-Click | Все задачи | Экспорт). Запустится мастер экспорта сертификатов.

На первом этапе нужно выбрать, будет ли экспортироваться закрытый ключ. Затем указывается формат, в котором будет экспортирован сертификат. Если экспортируется закрытый ключ, то потребуется ввести пароль для его шифрования. Далее указывается собственно имя файла, в котором будет сохранен сертификат.

Импорт сертификата

При импорте сертификата он переносится из файла в указанное хранилище сертификатов. Для импорта сертификата выберите нужное хранилище сертификатов, (R-Click | Все задачи | Импорт). Запустится мастер импорта сертификатов.

На первом шаге потребуется указать имя файла, из которого будет импортироваться сертификат. Затем, если файл содержит зашифрованный пароль, потребуется ввести соответствующий пароль. В завершение указывается хранилище, в которое будет помещен импортированный сертификат.

Задание *– Изучите возможности импорта и экспорта сертификатов. Для этого экспортируйте полученный сертификат в файл, удалите сертификат из хранилища и импортируйте его обратно.*

Аутентификация пользователей на Web-серверах с установлением SSL соединения

Технологическая схема работы

Технологическая схема аутентификации пользователей на Web-серверах представлена на Рис. 13.

1. Клиент инициализирует соединение с сервером;
2. Сервер отправляет клиенту служебное сообщение;
3. Далее сервер отправляет свой сертификат открытого ключа и служебное сообщение, которое свидетельствует о завершение фазы приветствия сервера.
4. Клиент, получив служебное сообщение, убеждается, что сервер предоставил действительный сертификат открытого ключа и проводит проверку сертификата открытого ключа сервера;
5. Далее клиент отправляет сообщение о изменение параметров шифрования и вслед за этим сообщением отправляется служебное сообщение. Данное сообщение подтверждает, что процесс обмена ключами и аутентификации завершился успешно;
6. В ответ на эти сообщения сервер также формирует два служебных сообщения.

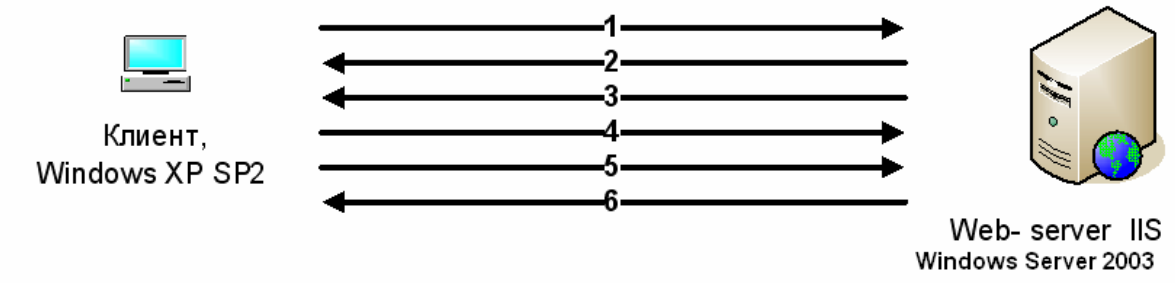

Рис. 13 Аутентификация пользователей на Web-серверах

Порядок настройки продуктов

IIS был установлен во время инсталляции сервера ЦС. После установки необходимо проверить свойства IIS. Для этого запускаем из меню Пуск | Программы | Администрирование | IIS. В появившемся окне выбираем Веб-узел по умолчанию (Рис. 14)

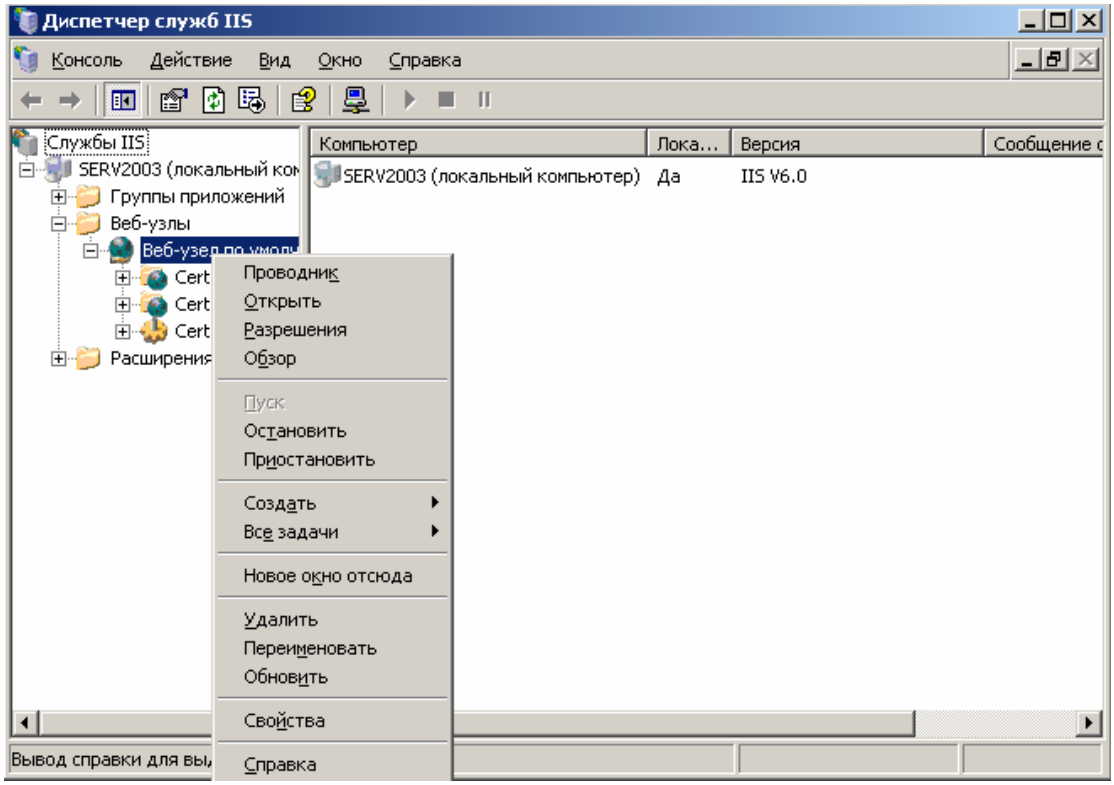

Рис. 14 Internet Information Services

Далее щелчком левой кнопки мыши по «Веб-узел по умолчанию» и в появившемся списке выбираем пункт Свойства. В открывшемся окне Рис. 15.

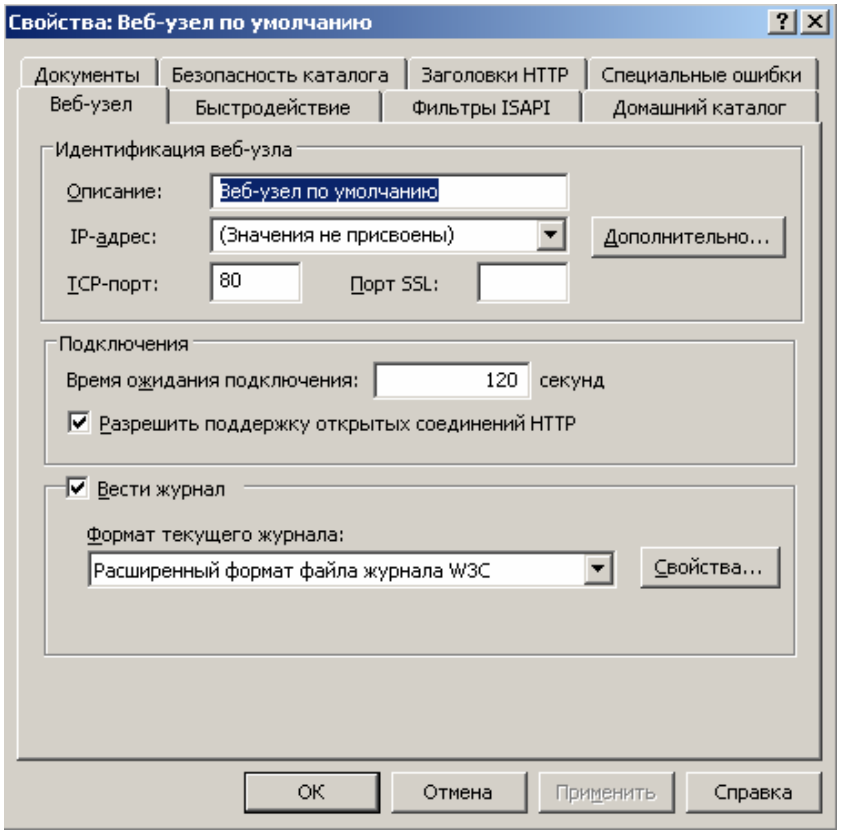

Рис. 15 Свойства Web Site

Нажимаем кнопку Дополнительно и проверяем порты установленные по умолчанию. Для SSL необходимо добавить порт 443.

Для того чтобы увидеть веб страничку на узле по умолчанию, необходимо в папку \Inetpub\wwwroot скопировать любой htm файл, и назвать его «default.htm». Тогда при открытии этого веб узла там будет отображаться ваша страничка.

Следующим этапом является создания ключевой пары и сертификата для web-сервера. Для этого необходимо с помощью http://<имя компьютера>/certsrv/ выпустить сертификат для проверки подлинности web сервера, установив соответствующий тип сертификата. Так же необходимо установить параметр «Использовать локальное хранилище компьютера для сертификата».

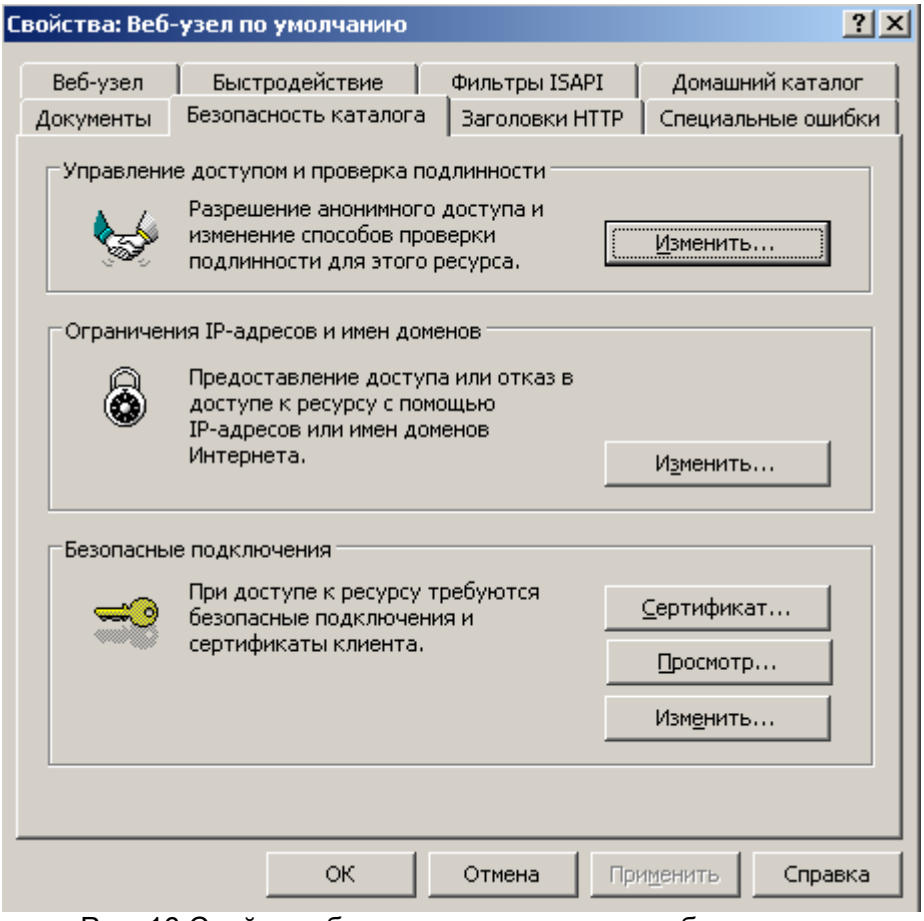

Рис. 16 Свойства безопасности каталога веб узла

Необходимо нажать кнопку Сертификат. По нажатию этой кнопки запустится мастер установки сертификата для Web-сервера. Выбираем «Назначение существующего сертификата» и следуя подсказкам мастера выбираем сертификат выпущенный для веб сервера.

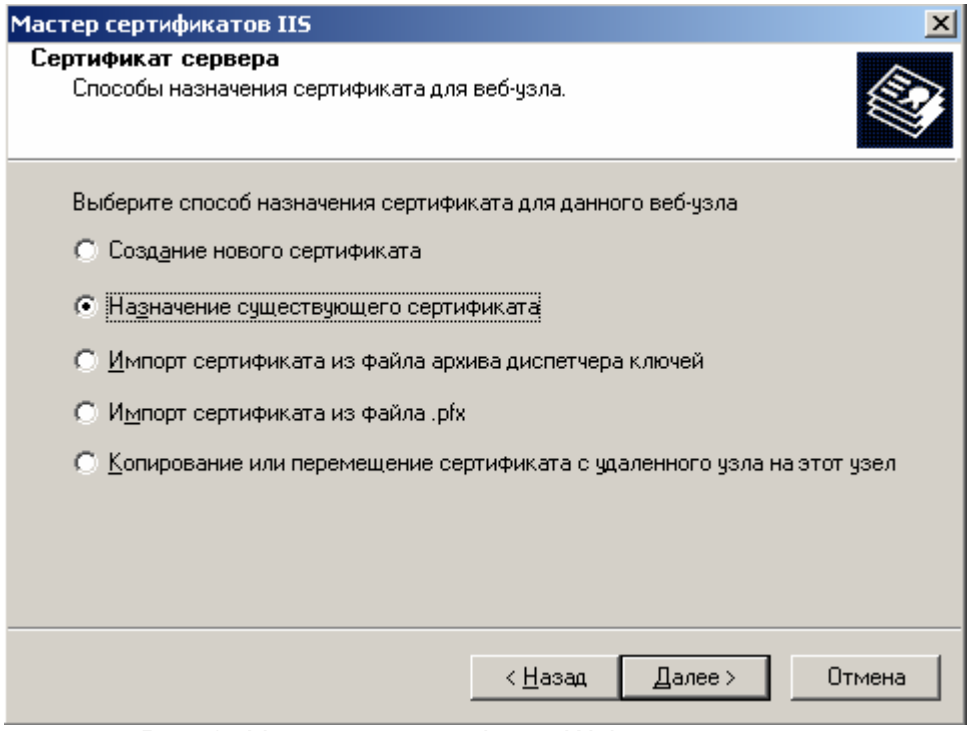

Рис. 17 Установка сертификат Web-сервера.

Второй способ создания ключевой пары и сертификата для web сервера: с помощью этого мастера можно также сначала сформировать запрос на сертификат в формате PKCS#10. Результатом работы мастера будет являться создание и сохранение на локальном диске файла запроса на сертификат открытого ключа, который будет необходимо передать удостоверяющему центру для выдачи по этому запросу сертификата открытого ключа Web-сервера.

Выпустить сертификат открытого ключа используя данный запрос на ЦС (Рис. 18) либо используя web интерфейс службы сертификации (Рис.19). В последнем случае необходимо вставить содержимое текстового файла запроса в соответствующее окно web интерфейса.

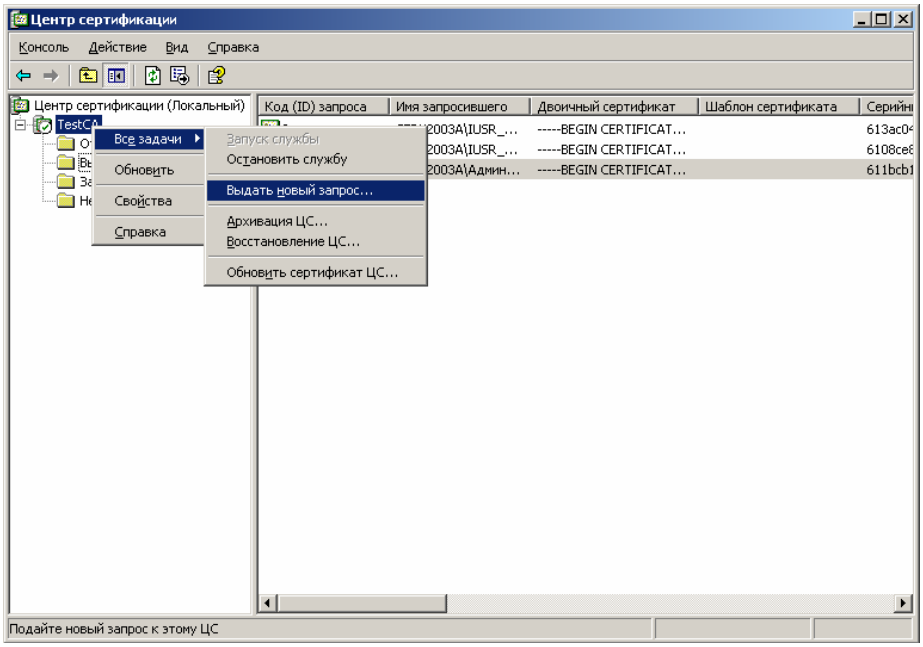

Рис. 18 Выпуск сертификата web сервера по запросу из файла

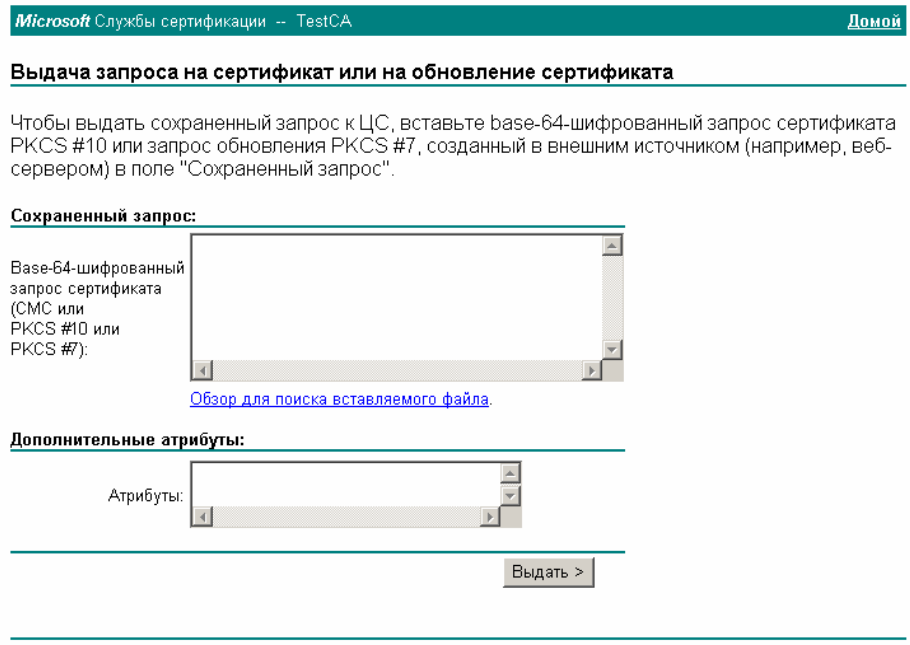

Рис. 19 Web интерфейс службы сертификации

Следующим шагом является установка сертификата Web-сервера. Данная операция производится следующим образом:

1. Запускаем Диспетчер служб IIS;
2. В открывшемся окне выбираем «web узел по умолчанию»;
3. Далее щелчком левой кнопки мыши выбираем пункт Свойства. В открывшемся окне и переходим на закладку «Безопасность каталога» и нажимаем кнопку «Сертификат»;
4. После нажатия данной кнопки происходит запуск мастера установки сертификата открытого ключа Web-сервера;
5. Следуя указаниям мастера необходимо выбрать пункт «Обработать ожидающий запрос и установить сертификат» Рис. 20 и произвести установку сертификата открытого ключа;

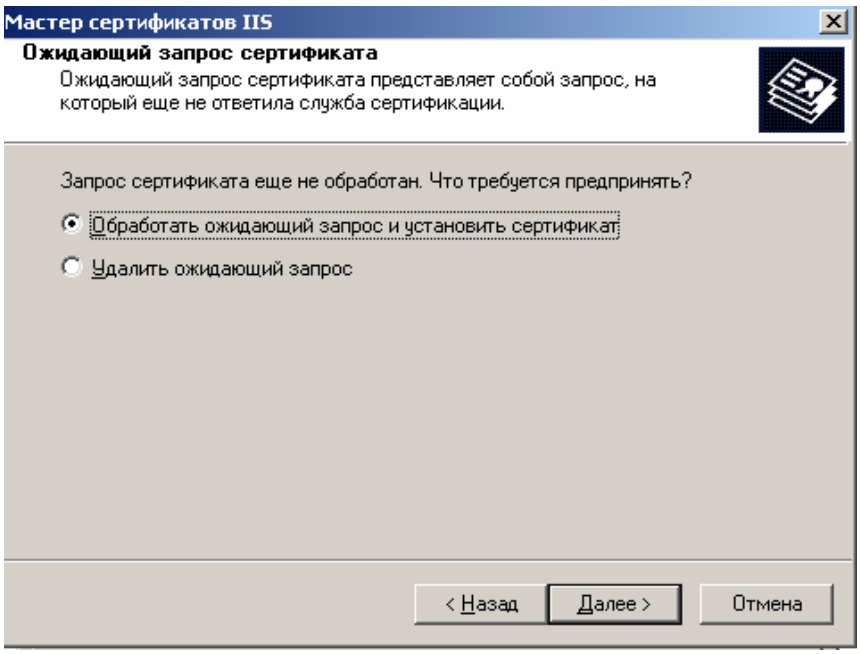

Рис. 20 Установка сертификата Web-сервера

Следующим шагом является настройка параметров соединения. Для этого необходимо в окне «Свойства web узла по умолчанию» в закладке «Безопасность каталога» нажать кнопку Изменить. В открывшемся окне Рис. 21 и произвести настройка необходимых параметров.

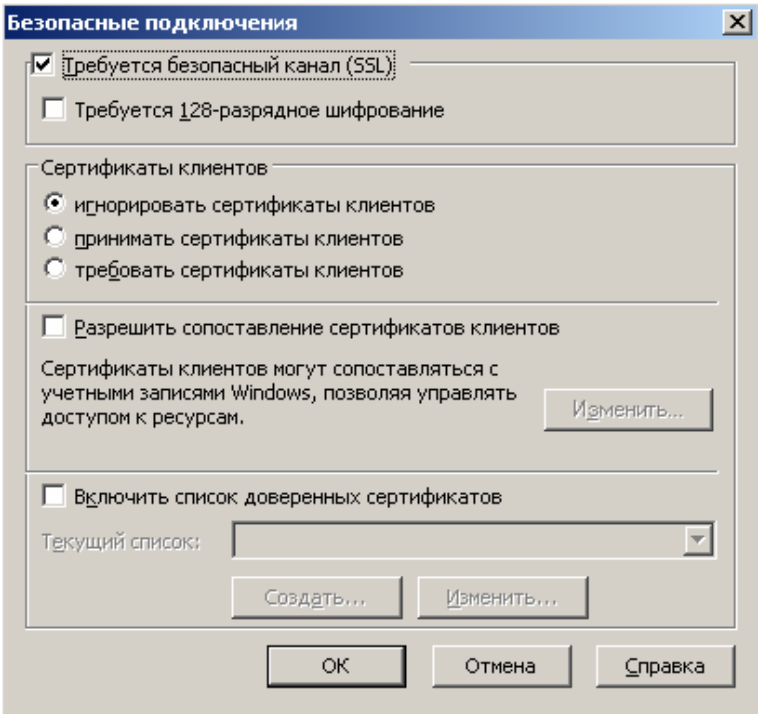

Рис. 21 Настройка параметров аутентификации на Web-сервере

Для двусторонней аутентификации сервера и клиента необходимо создание ключевой пары и сертификата открытого ключа для клиента. Для этого необходимо при помощи web интерфейса службы сертификации выдать сертификатов открытых ключей Web-клиентов, и установить его для текущего пользователя.

Заключительным этапом тестирования является попытка произвести доступ к защищенному Web-сайту. Необходимо в свойствах обозревателя web браузера разрешить использовать SSL. В web-браузере на клиентском рабочем месте набрать следующую

строку https://<имя компьютера web сервера>. После этого на экране у пользователя должно будет открыться окно Рис 22 и после нажатия Да, открыться ваша страничка по протоколу https.

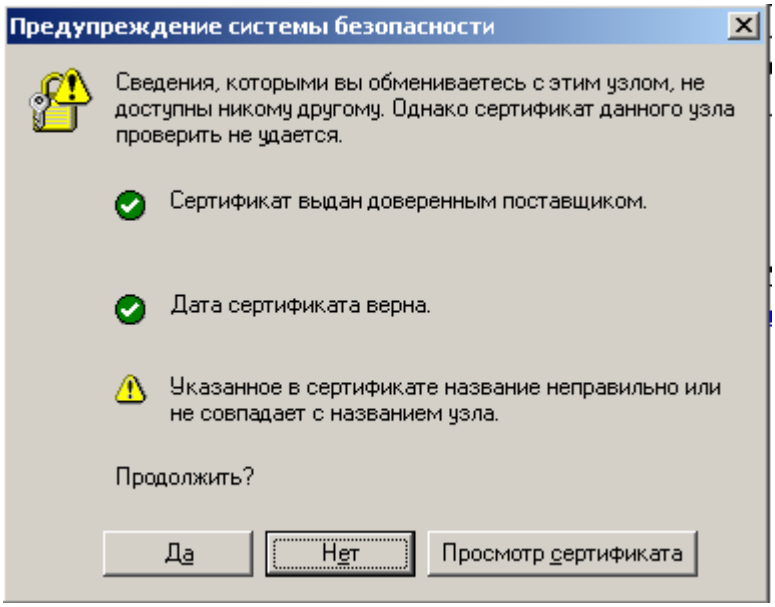

Рис. 22 Окно предупреждения о начале безопасного просмотра web узла

В зависимости от настроек безопасного подключения (Рис. 21) пользователю будет предложено выбрать сертификат аутентификации клиента для доступа к web-сайту (Рис.23) . В результате пользователь получит доступ к защищенному Web-сайту с установлением SSL соединения.

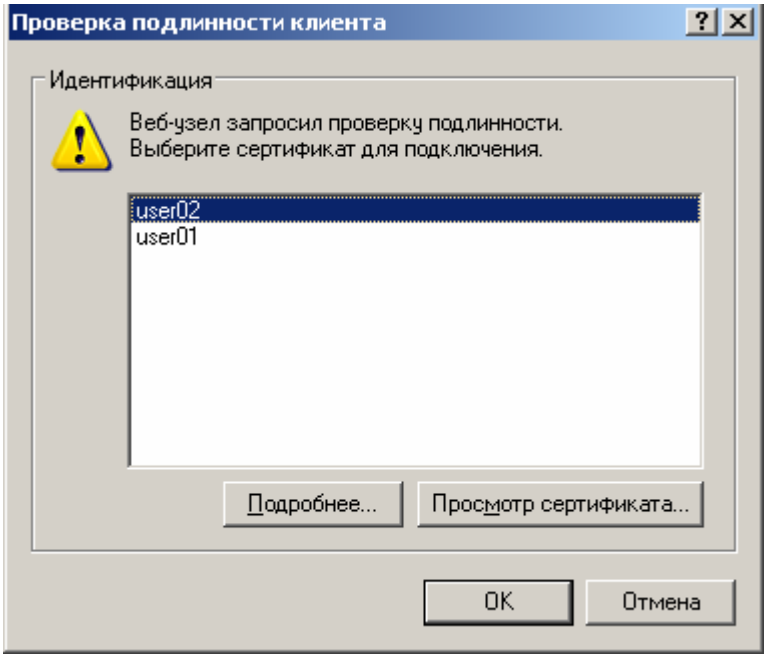

Рис. 23 Окно проверки подлинности клиента web узла

Задание *– Настройте защищенное соединение с web сайтом по протоколу https с проверкой подлинности клиента. Убедитесь что соединение устанавливается. Отзовите сертификат клиента. Опубликуйте новый список отзыва CRL и попробуйте заново подключиться к web узлу с отозванным сертификатом клиента.*

Рекомендуемая литература

1. Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure. Training kit (exam 70-291) /J. C. Mackin, Ian McLean, Microsoft Press 2004
2. Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure. Training Kit (Exam 70-293) / Craig Zacker. Microsoft Press, 2004
3. Справочная система ОС Microsoft "Windows Server 2008/2003 "