eSMART®

Развертывание центра сертификации на базе Windows Server 2003

Содержание

1. Общая информация

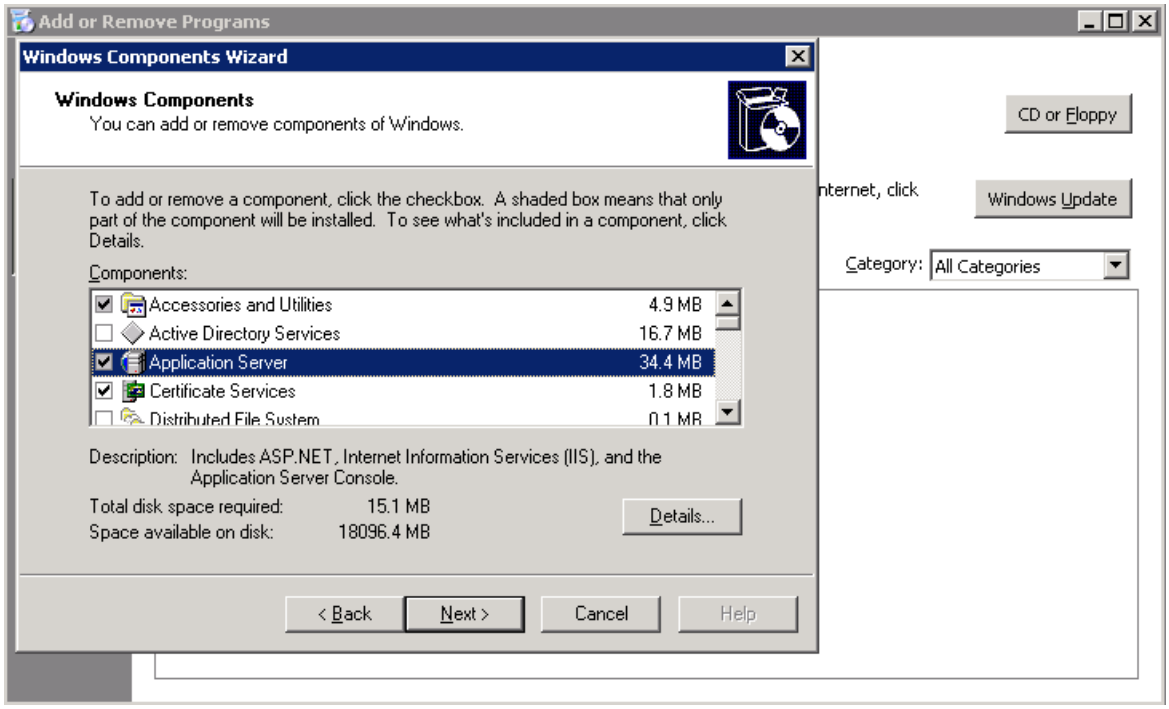
В руководстве описана настройка службы сертификатов Active Directory на базе Windows Server 2003[1].

Настройка служб каталогов Active Directory не рассматривается. Для выполнения описанных процедур требуются права администратора домена (группа Domain Admin) или администратора предприятия (группа Enterprise Admin).

Собственный корпоративный центр сертификации[2] может быть развернут на базе Windows Server 2003. Корпоративный центр сертификации позволяет выпускать сертификаты по шаблонам, используя информацию о пользователях из Active Directory. Центр сертификации на базе Windows Server 2003 имеет веб-интерфейс, который может использоваться для запроса сертификата и записи на смарт-карту или USB-ключ ESMART Token.

Microsoft не рекомендует разворачивать центр сертификации на сервере, являющимся контроллером домена, желательно использовать другую машину.

2. Установка IIS-сервера (Application Server)

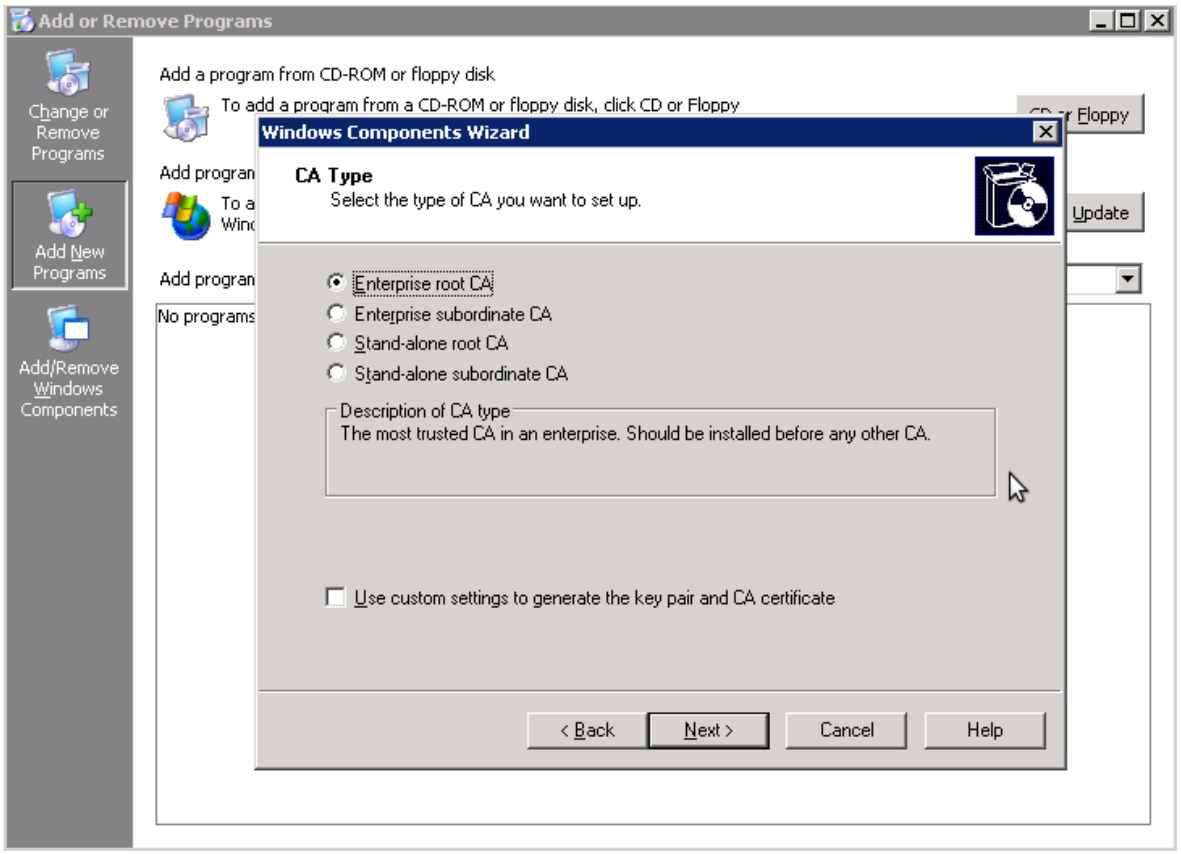


*Убедитесь, что достаточно места для установки и нажмите **Next** (Далее). Дождитесь завершения установки. Закройте программу установщик, нажав **Finish** (Готово).*

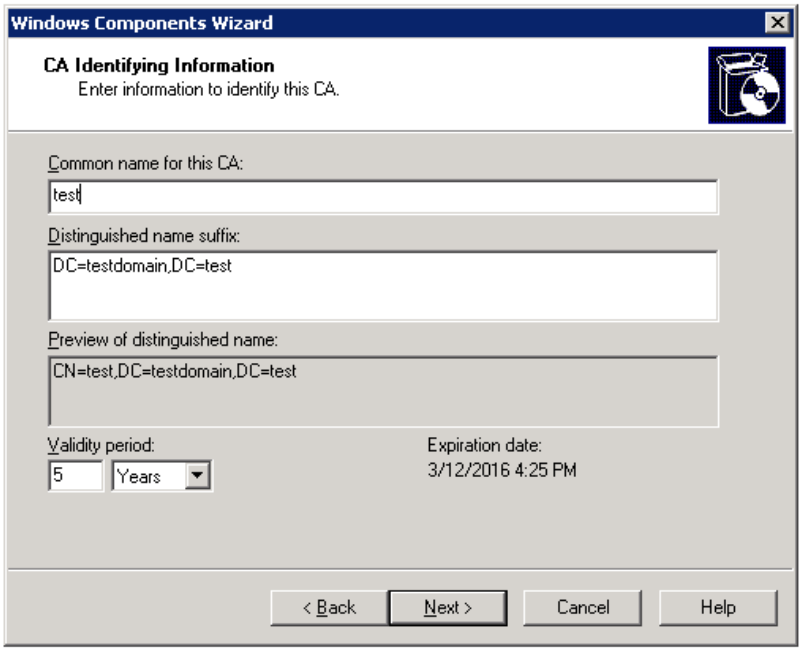
[1] *С особенностями поддержки функций службы сертификатов Active Directory в разных версиях операционной системы Windows Server 2008 можно на сайте Microsoft: http://technet.microsoft.com/ru-ru/library/cc755071.aspx*

[2] *Перевод термина Certification Authority соответствует текущей локализации ОС Windows Server*

3. Установка Certification Authority (CA)

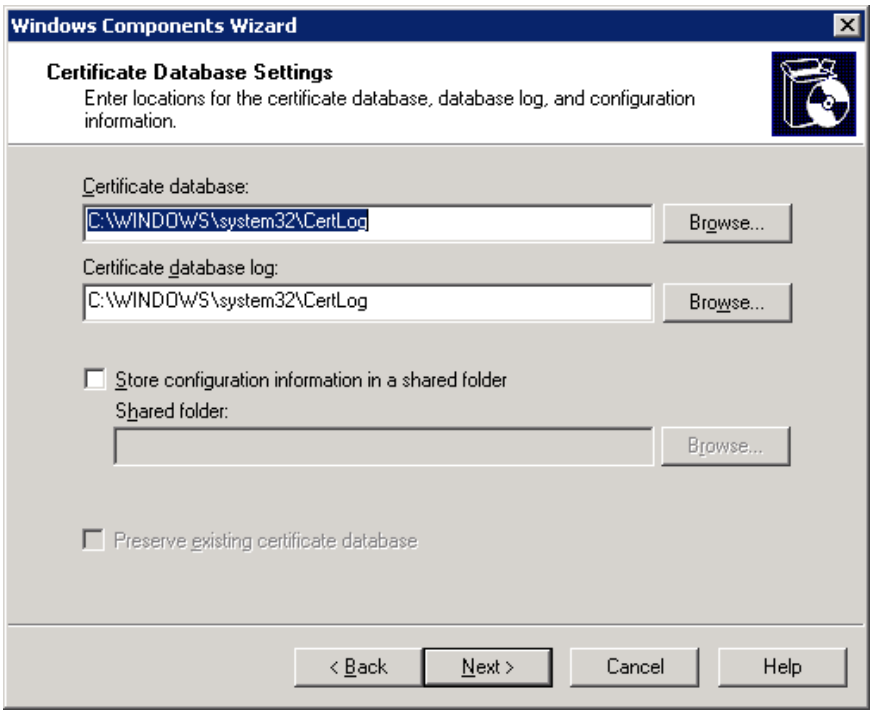


Заполните форму, указав название, суффикс и срок истечения корневого сертификата:



Примерно, срок действия сертификата УЦ должен быть в 2-5 раз больше, чем срок сертификатов, которые будет выписывать данный УЦ.

Выберите папку, в которой будет храниться база данных и логи базы:



*Нажмите **Next** (Далее). Подтвердите установку роли.*

Центр сертификации установлен.

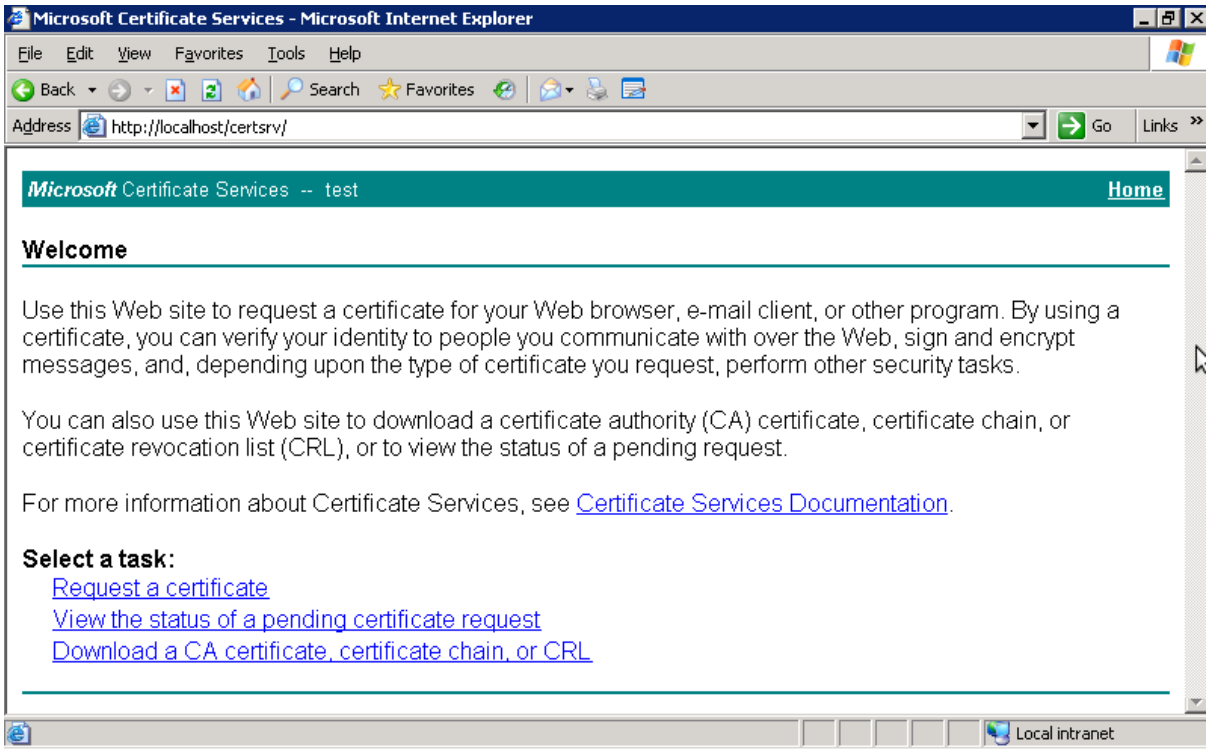
4. Создание и управление сертификатами

Для управления сертификатами через web-интерфейс можно зайти на страницуhttp://serv/certsrv или http://localhost/certsrv на самом сервере.

Доступ для управления сертификатами возможен только из браузера Internet Explorer и ОС Windows XP (или Windows Server на самом сервере). Элементы управления Active X должны быть установлены и активны.

В веб-интерфейсе CA можно:

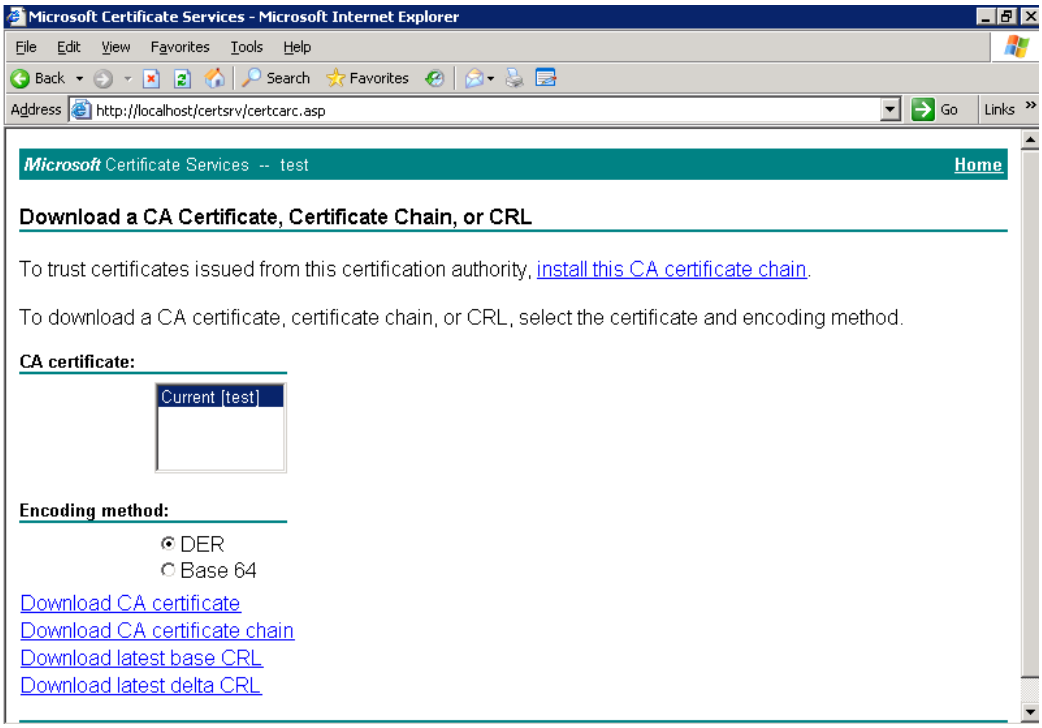
- *Запросить сертификат (**Request a certificate**);*
- *Просмотреть статус запрошенных, но не одобренных сертификатов*
- *(**View the status of a pending certificate request**), используется, только если пользователи могут сами запрашивать сертификаты;*
- *Скачать корневой сертификат CA, серию сертификатов или список отозванных сертификатов (**Download a CA certificate, certificate chain or CRL**).*



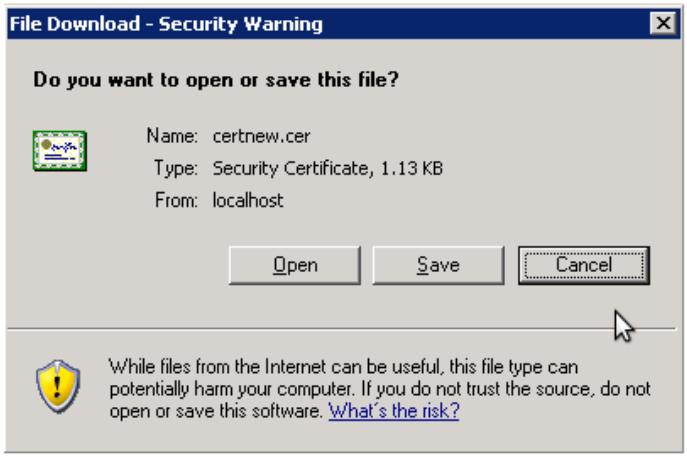
4. Установка корневого сертификата

Для получения корневого сертификата выберите нижнюю ссылку: ***Download a CA certificate, certificate chain or CRL***

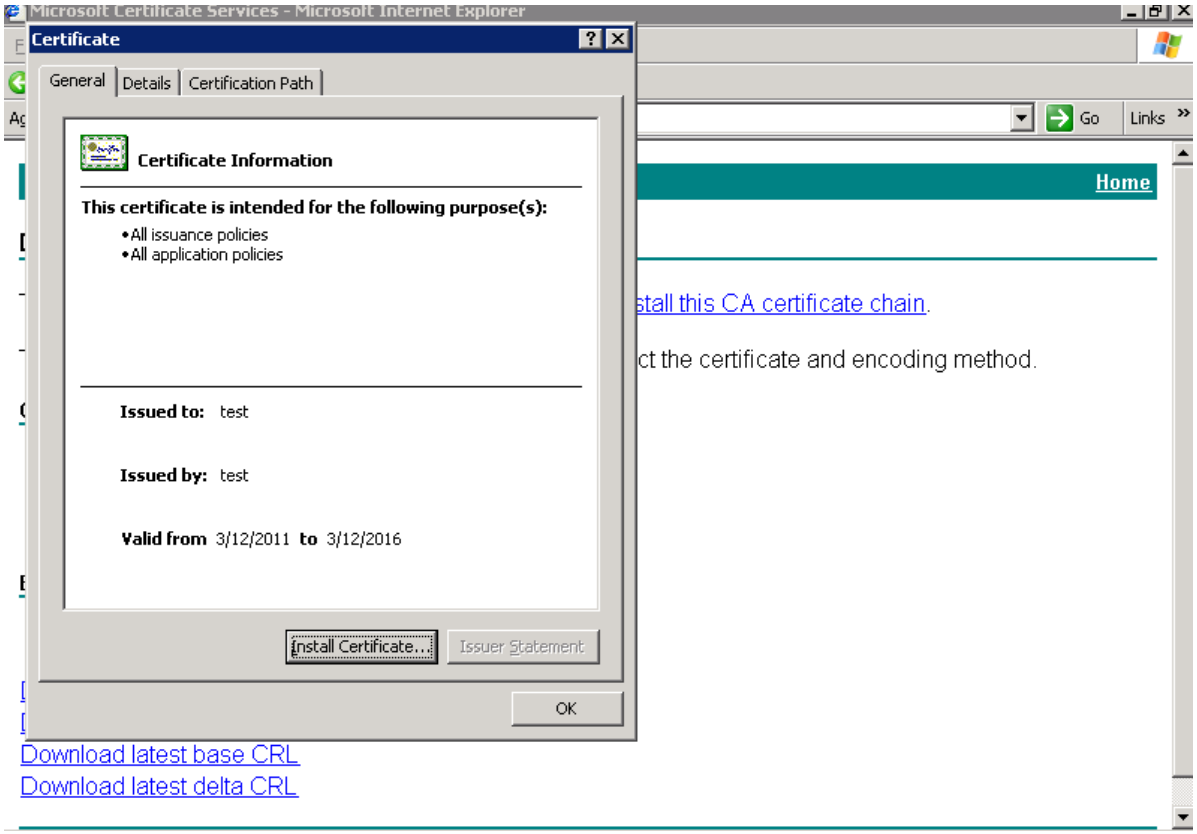
На странице ***certcarc.asp*** *выберите корневой сертификат по названию, заданному в поле* ***Common name*** *на этапе 2. Укажите метод кодирования. DER используется для совместимости с другими ОС, Base64 предназначен для работы с протоколом S/MIME.*



*В появившемся окне нажмите **Open** (Открыть):*



*Сертификат откроется в новом окне. Нажмите **Install Certificate** (Установить сертификат):*

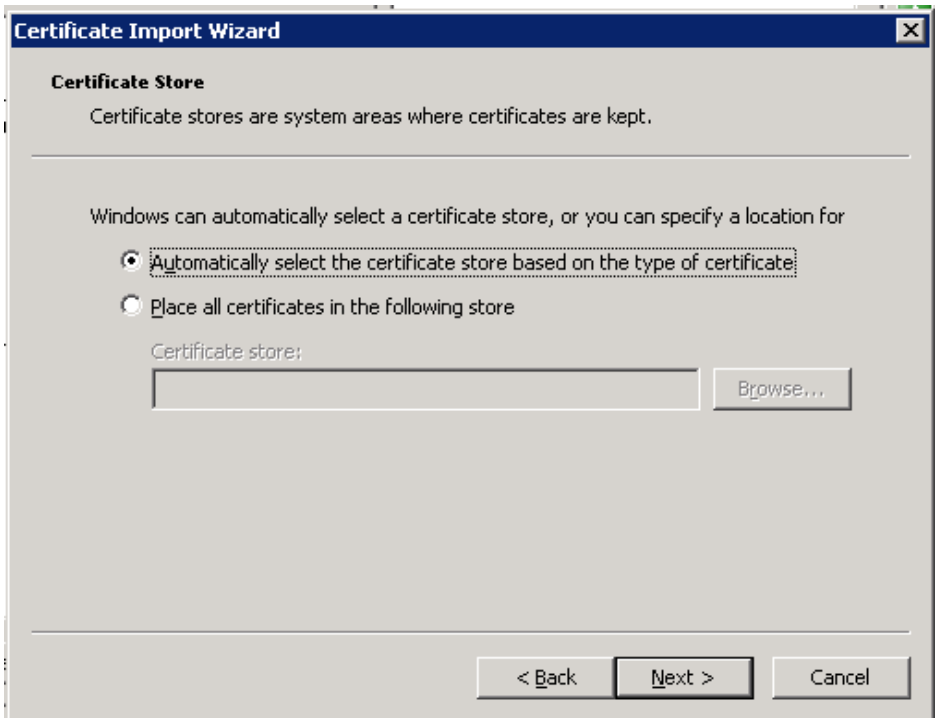


Появится окно помощника для импорта сертификата:

Выберите место хранения сертификата:

- *Автоматически выбрать хранилище в зависимости от типа сертификата (Рекомендуется)*
- *Помещать все сертификаты в определенную папку (для опытных пользователей)*

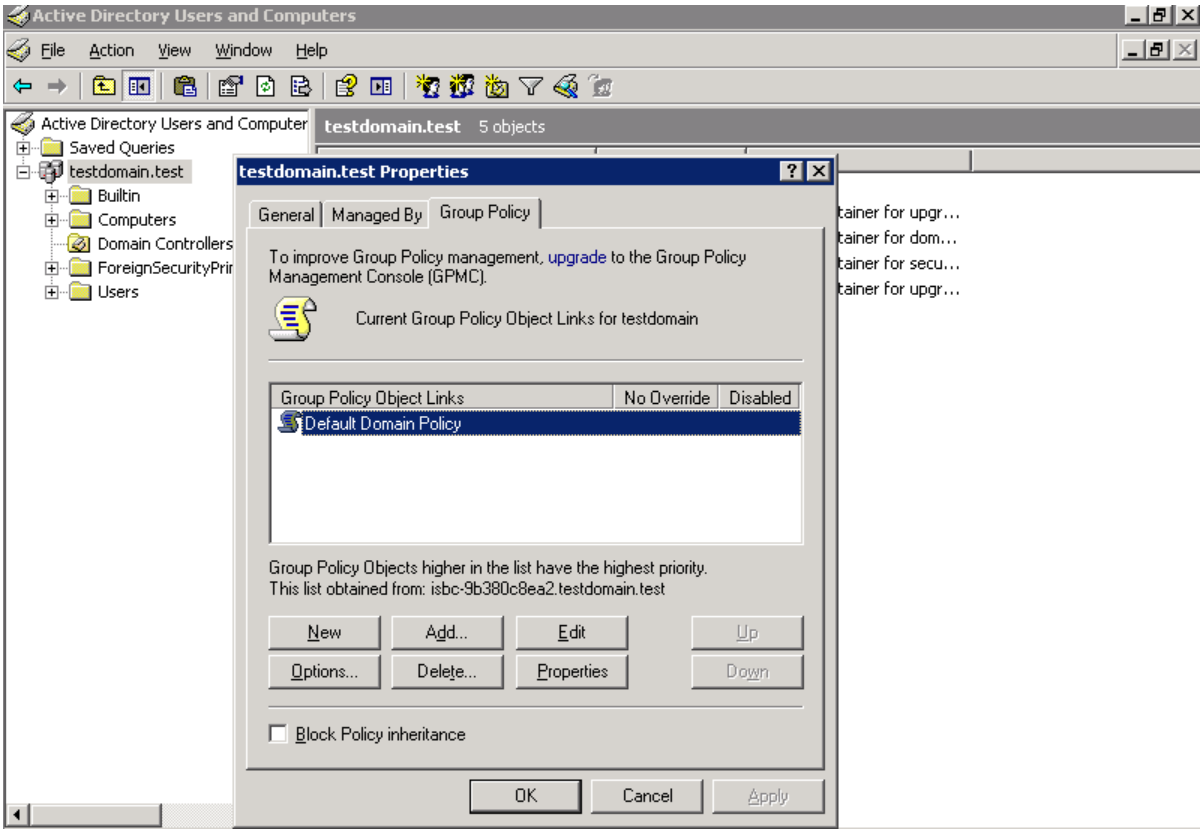
*Нажмите **Next** (Далее).*



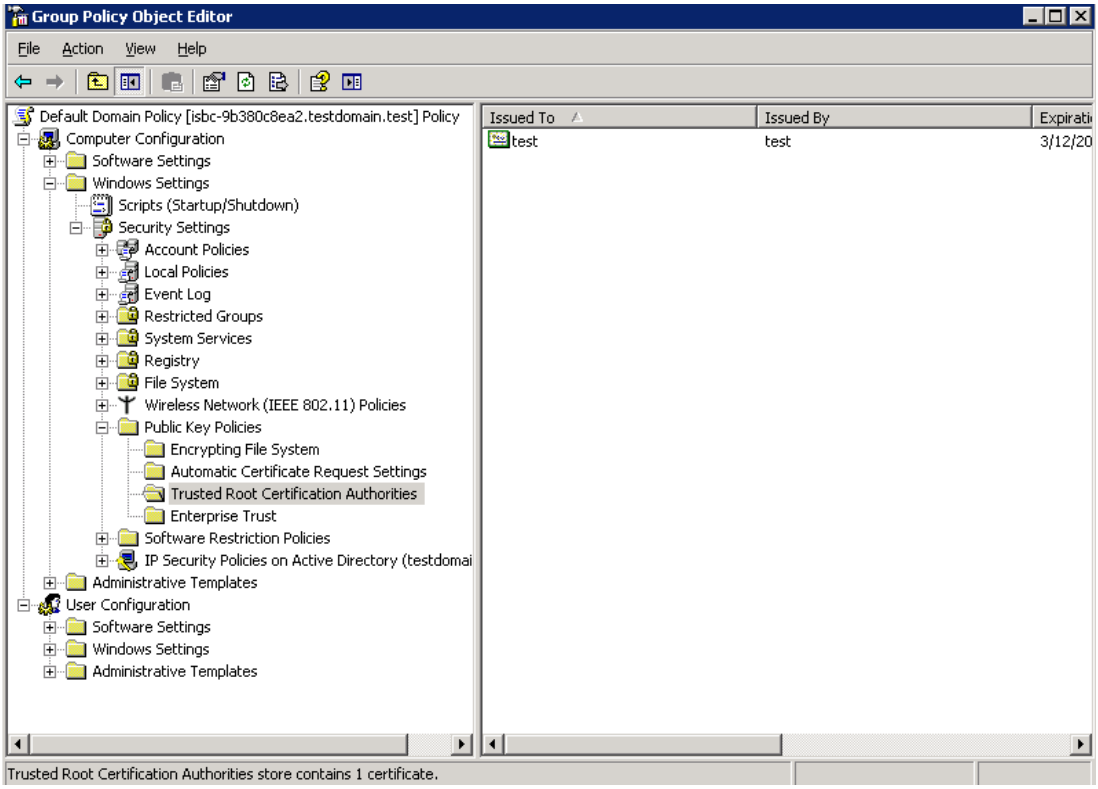
При установке корневого сертификата требуется выбрать хранилище «Доверенные корневые сертификаты вручную.

*Проверьте выбранные опции хранилища и тип содержимого. Нажмите **Finish** (Готово).*

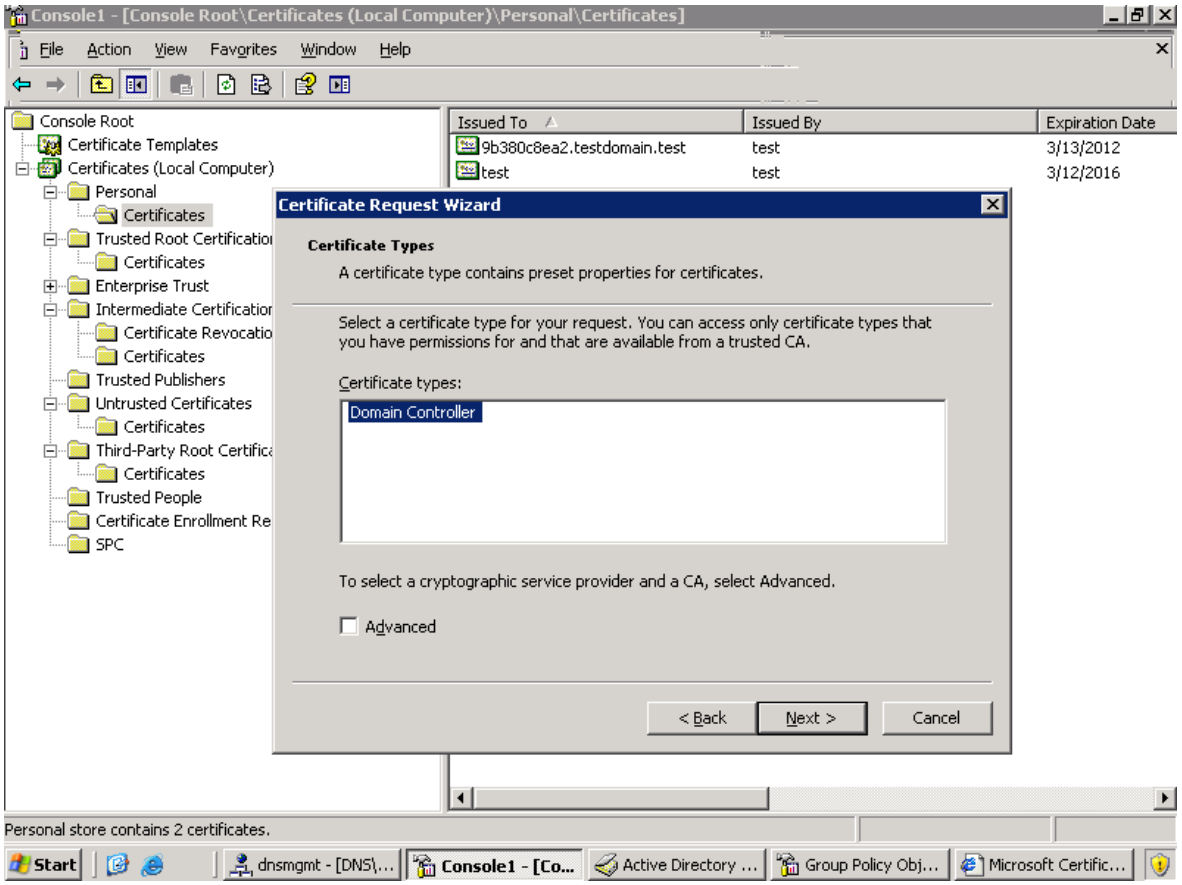
5. Настройка групповых политик



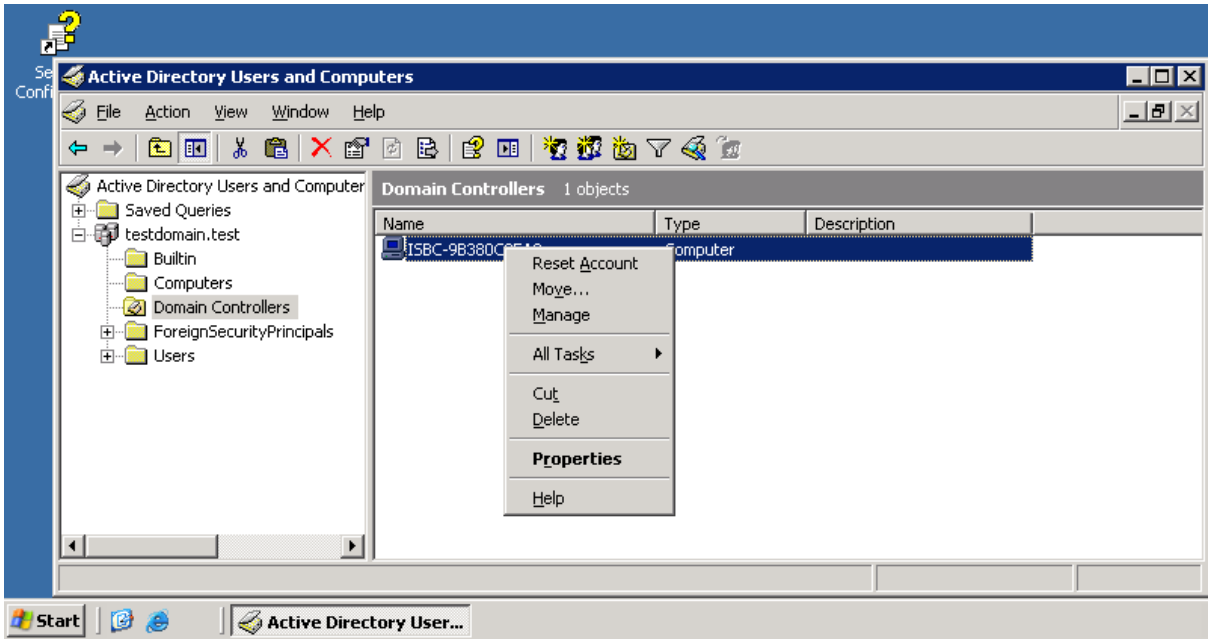
Необходимо импортировать доменный сертификат, если его нет в хранилище.

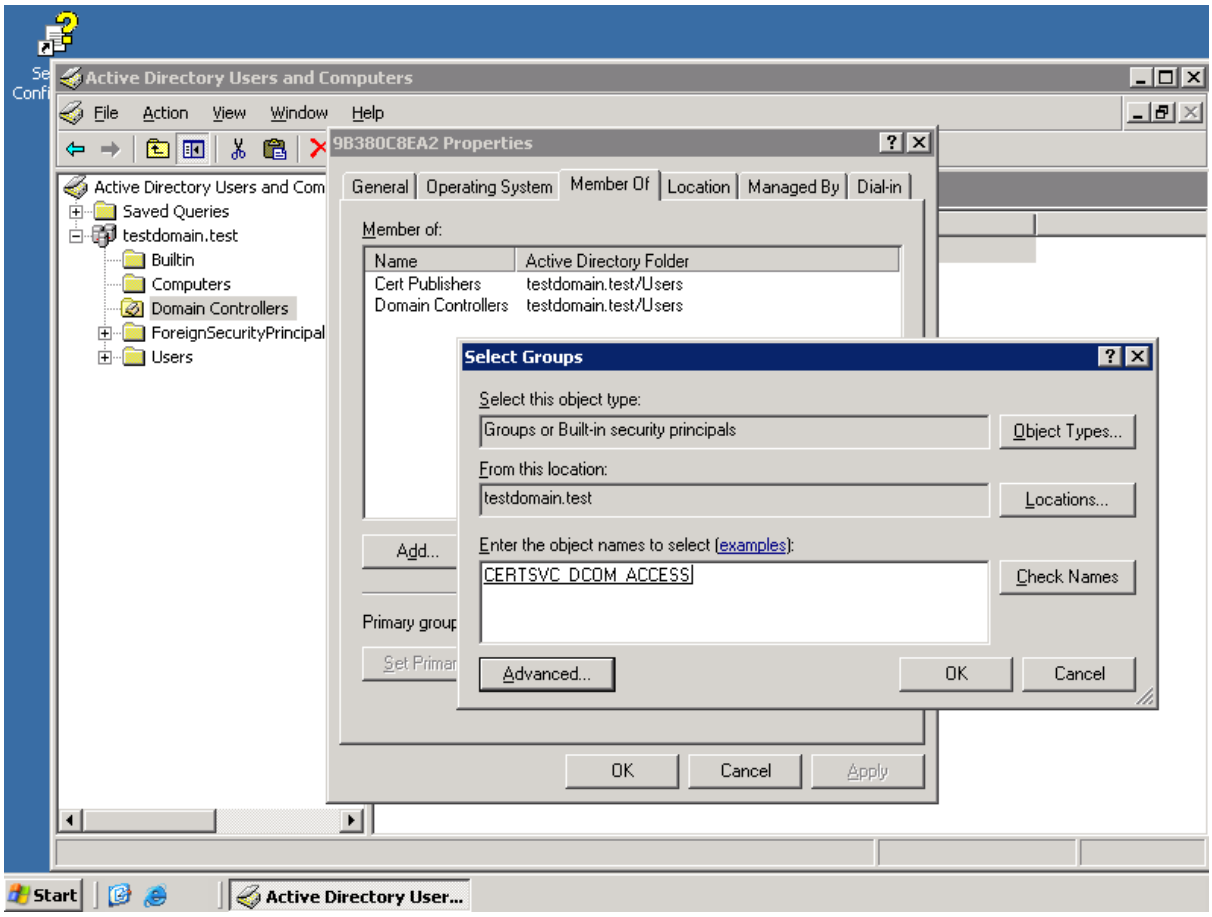


5. Запрос сертификата контроллера домена



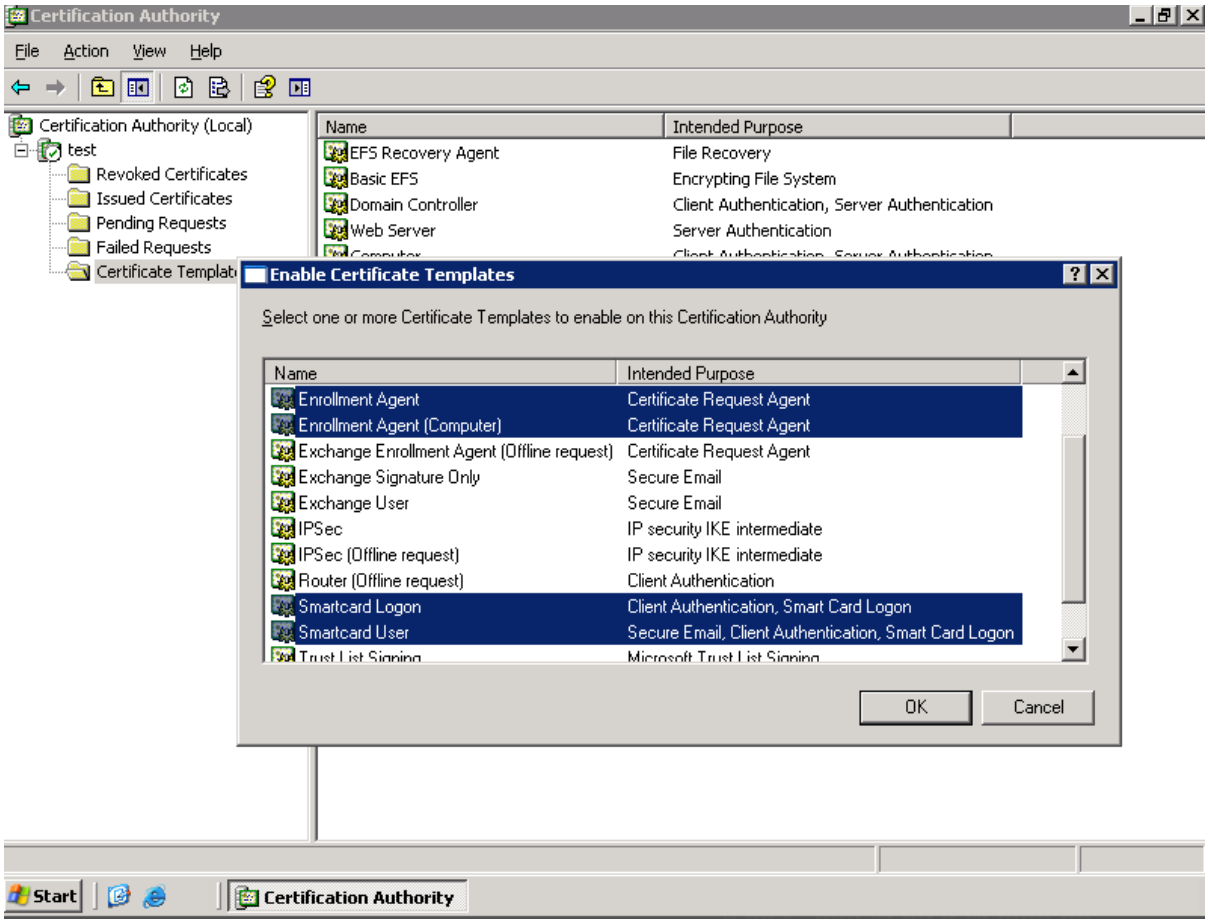
6. Включение контроллера домена в группу CERTSVC_DCOM_ACCESS





Также обязательно нужно добавить нужные шаблоны
в оснастке ***Certification Authority****:*

- *Authentificated Session*
- *Enrollment Agent (Агент подачи заявок)*
- *Enrollment Agent (Computer)*
- *Smartcard Logon (Логин по смарт-карте)*
- *Smartcard User (Пользователь со смарт-картой)*



После всех проведенных операций нужно принудительно обновить политики:

```
cmd->gpupdate /force
```

Перезагрузите сервер.

7. Настройки безопасности

Доменные групповые политики позволяют повысить уровень информационной безопасности системы с использованием ESMART Token при помощи двух основных механизмов:

- *Вход в систему только при предъявлении ESMART Token;*
- *Принудительная блокировка рабочей станции или завершение сеанса при извлечении ESMART Token.*

Использовать данные механизмы надежнее всего на уровне доменной групповой политики. Возможности изменения локальных настроек на рабочих станциях описаны в руководстве ESMART Token – Авторизация в домене Windows. Правила, заданные доменной групповой политикой имеют наибольший приоритет и потому рекомендуется использовать именно этот метод.

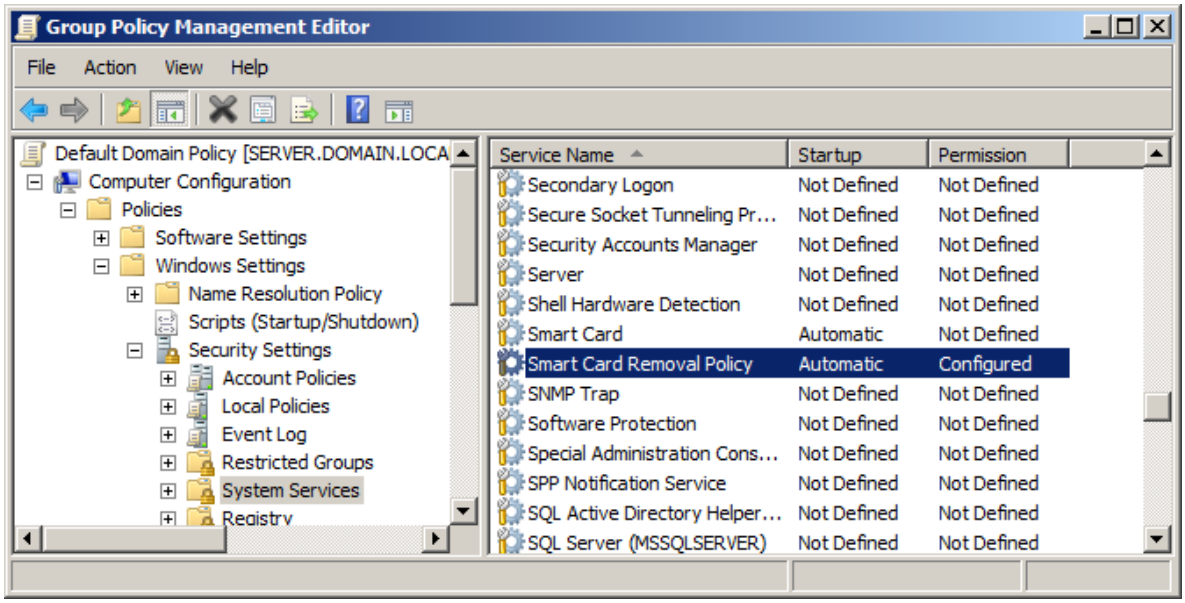
*Если решено ввести вход по обязательному предъявлению ESMART Token, необходимо предусмотреть процедуру выдачи временных сертификатов. Для временного отзыва постоянного сертификата используется опция**Certificate Hold**, т.к. только эта причина позволяет впоследствии вернуть статус действующего сертификату, который был отозван.*

*Чтобы операционная система могла заблокировать рабочую станцию при извлечении ESMART token, необходимо запустить службу **Smartcard Removal Policy – Политика удаления смарт-карт** (**SCPolicySVC**). В ОС Windows XP служба запущена по умолчанию, а в ОС Windows Vista и выше служба по умолчанию отключена. Если служба не запущена, при извлечении ESMART Token не произойдет никаких изменений при любых настройках.*

На контроллере домена откройте консоль MMC. Добавьте оснастку Group Policy Management Editor › Default Domain Policy (или текущую доменную политику). Чтобы служба запускалась автоматически на всех рабочих станциях в домене, откройте в редакторе доменной групповой политики:

> *Computer Configuration › Windows Settings › Security Settings › System Services*
>
> *Конфигурация компьютера › Конфигурация Windows › Параметры безопасности › Системные службы*

*Выставите значение для **Smart Card Removal Policy – Automatic**.*



В той же консоли перейдите к разделу:

Local Policies › Security Options

Локальные политики › Параметры безопасности

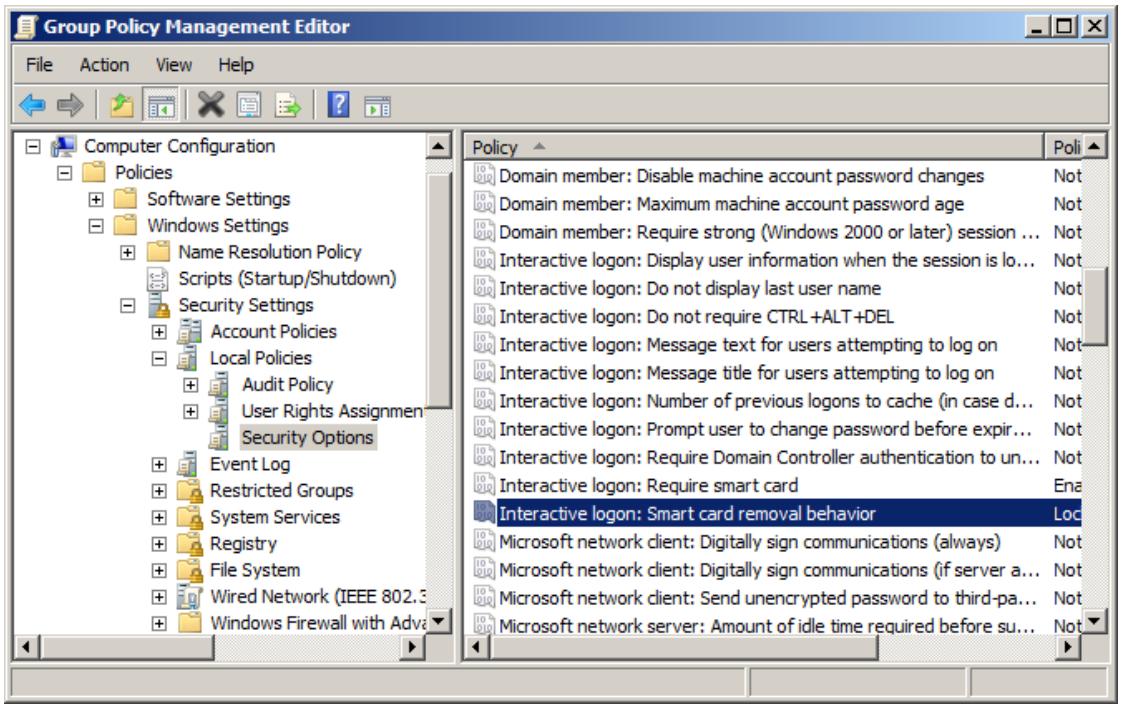
В соответствии с корпоративными требованиями задайте значения для параметров:

Interactive Logon: Require smartcard
(Интерактивный вход в систему: Требовать смарт-карту)

Interactive Logon: Smartcard removal behavior
(Интерактивный вход в систему: Поведение при извлечении смарт-карты)

ВНИМАНИЕ! *Перед перезагрузкой убедитесь, что администратор предприятия или администраторы домена не потеряют возможность входа в систему из-за настройки, требующей обязательного предъявления смарт-карты. Рекомендуется предварительно создать смарт-карту администратора предприятия или администратора домена, имеющего доступ к управлению групповыми политиками*

.

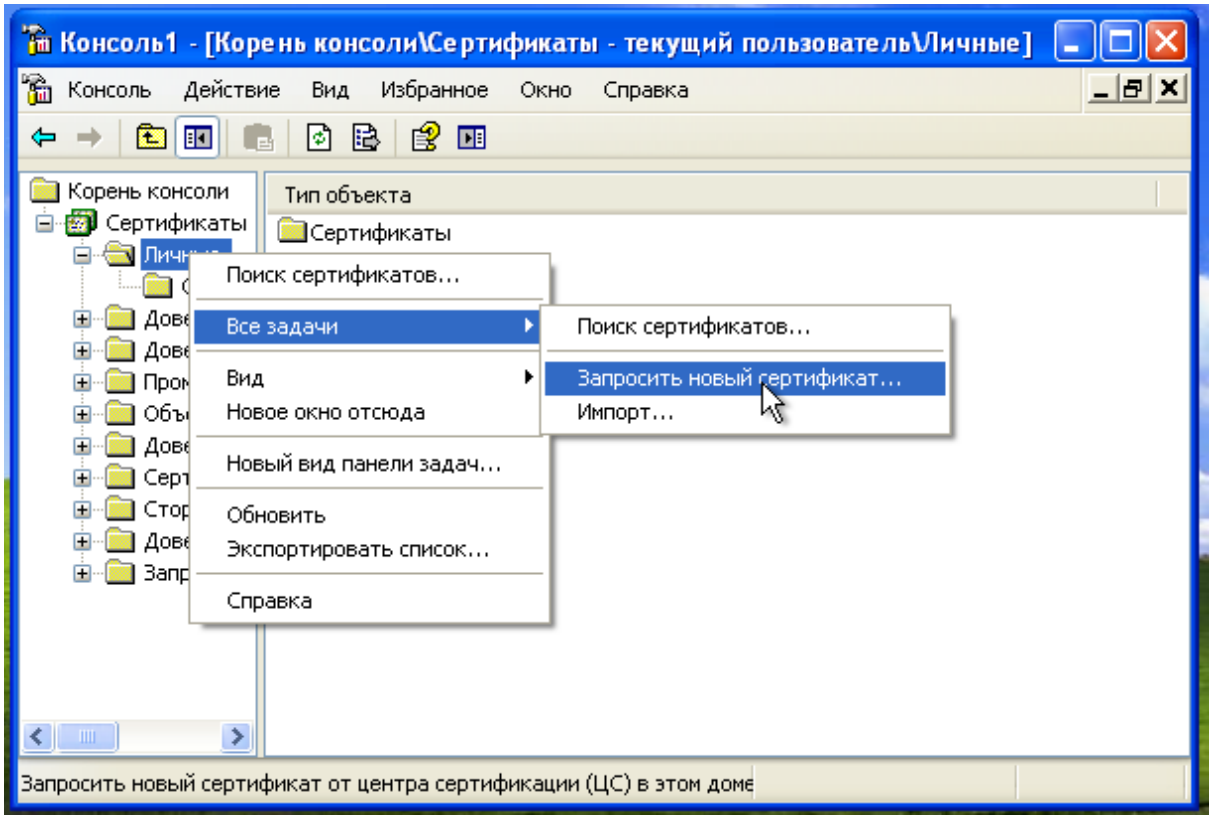


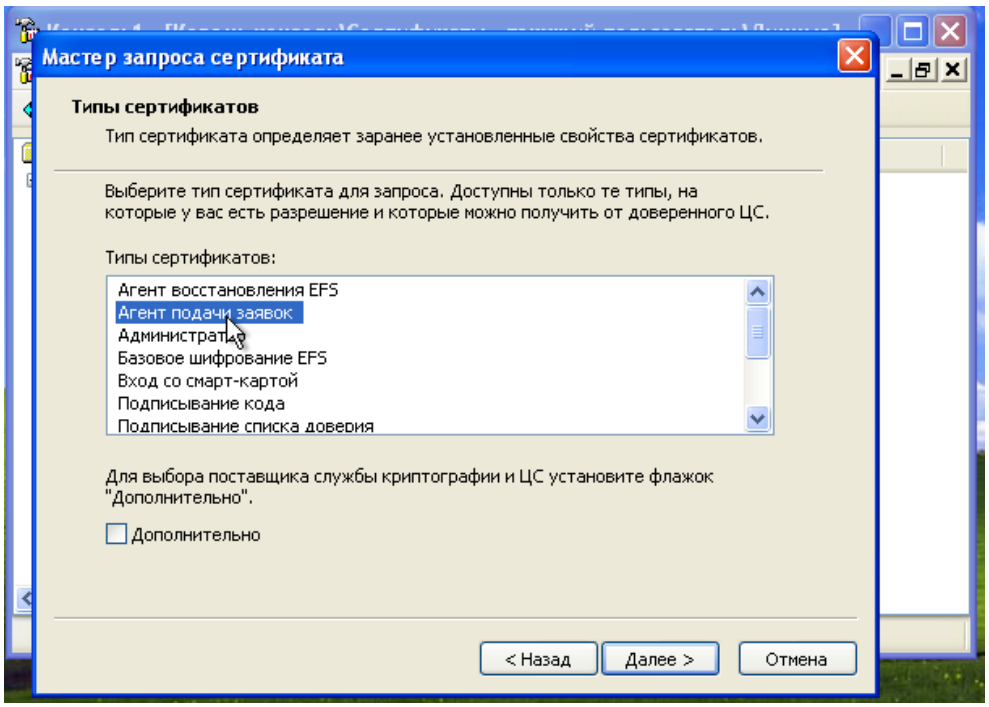
Проверьте настройки. Обновите групповые политики в принудительном режиме и перезагрузите сервер.

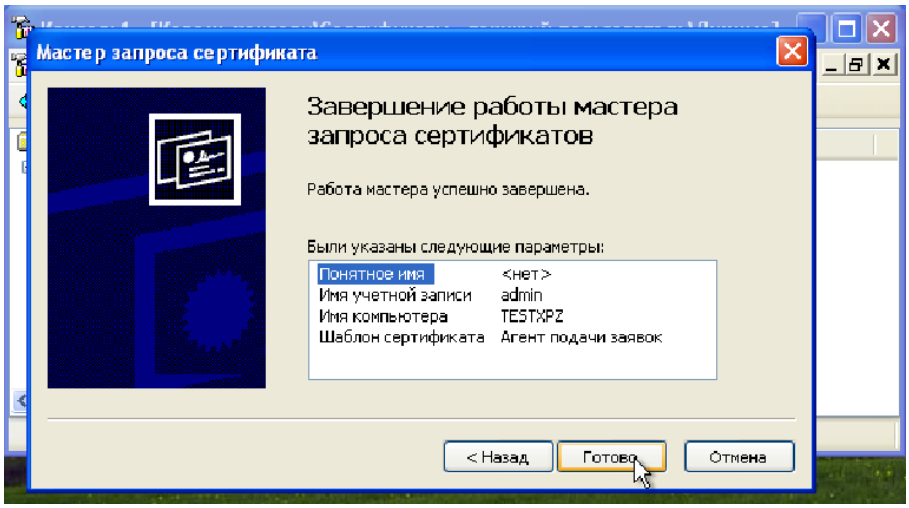
8. Разрешение на запрос сертификатов

*Разрешите текущему пользователю (администратору) запрашивать сертификаты для других пользователей (через консоль – команда **mmc** в командной строке **Win+R**):*

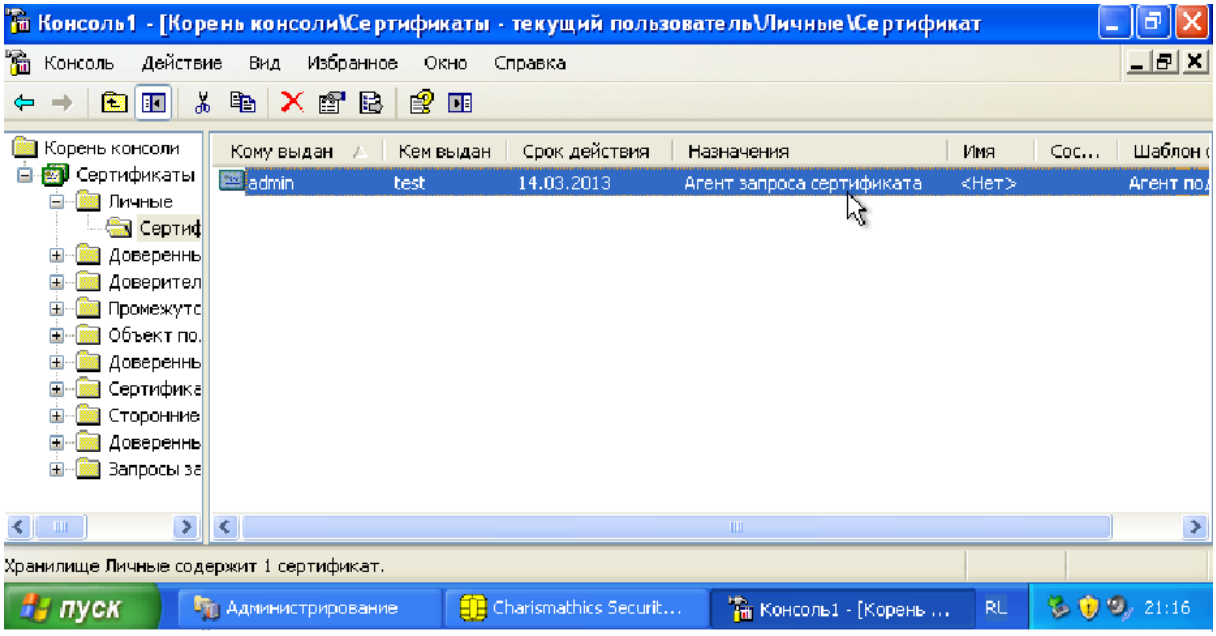
Запросите новый сертификат:







В результате сертификат администратора, позволяющий ему выписывать сертификаты от имени других пользователей, попадет в хранилище.

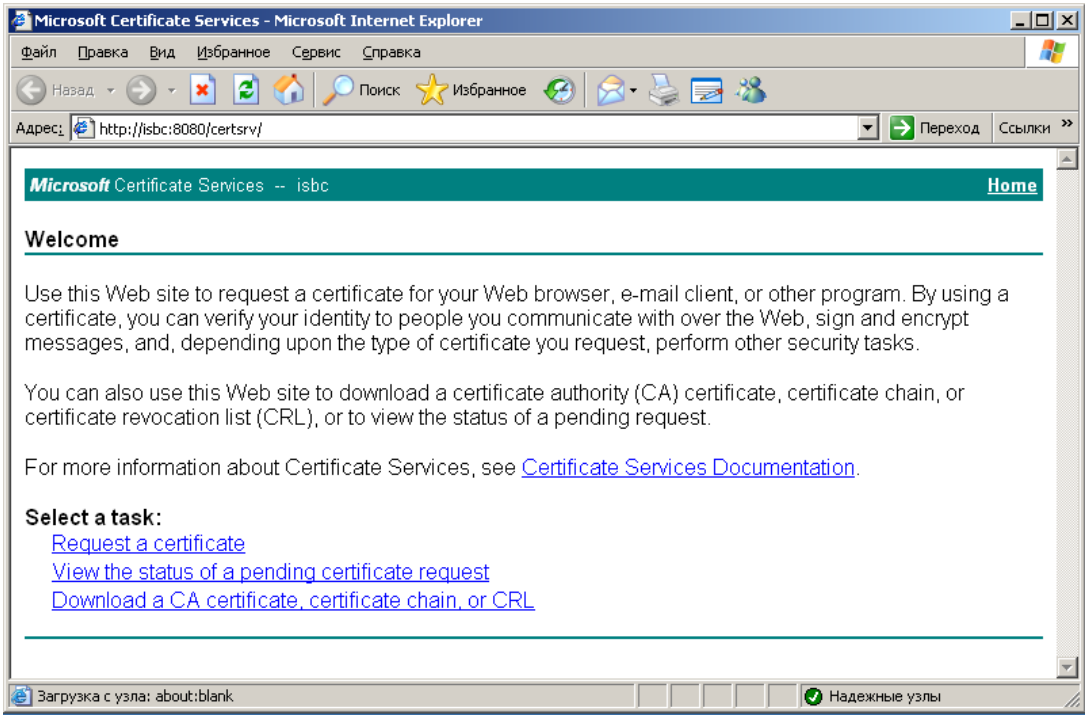


9. Процесс выдачи сертификата пользователя

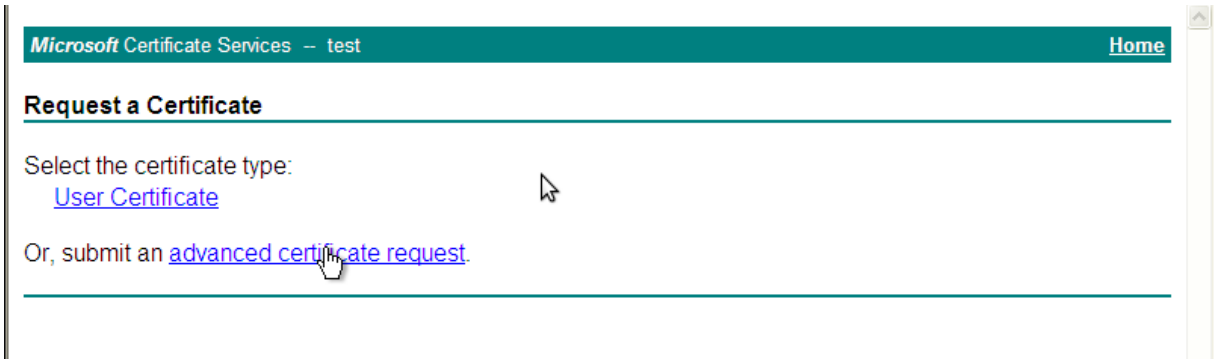
Только для Windows Server 2003. Windows сервер 2008 и выше не имеют веб-интерфейса для выдачи сертификатов, необходимо использовать консоль. См. руководство Развертывание центра сертификации Windows Server 2008.

Зайдите в WEB-интерфейс CA (http://serv/certsrv или http://localhost/certsrv на самом сервере) с ПК, на котором установлена Windows XP и Internet Explorer. Проверьте, не отключено ли выполнение элементов управления Active X в браузере
(см. руководство к установленной версии браузера Internet Explorer).

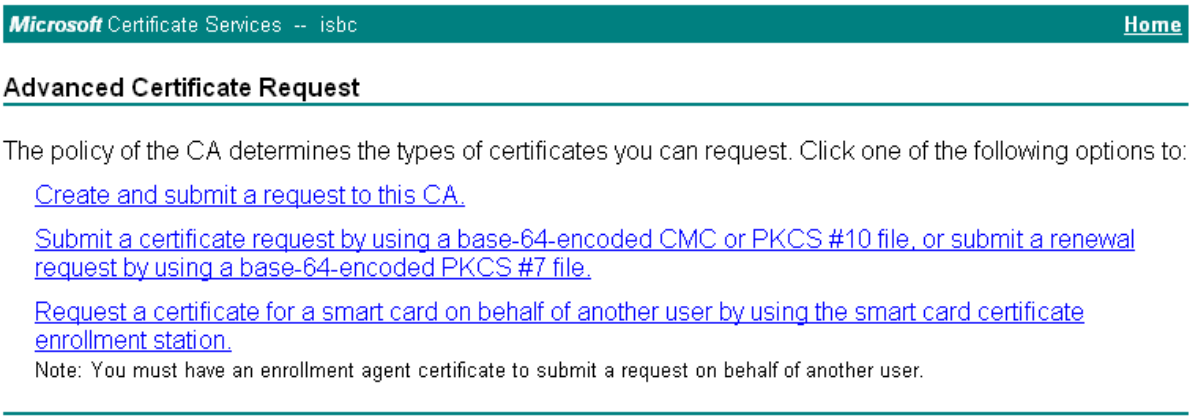
*Нажмите **Request a certificate** (Запросить сертификат):*



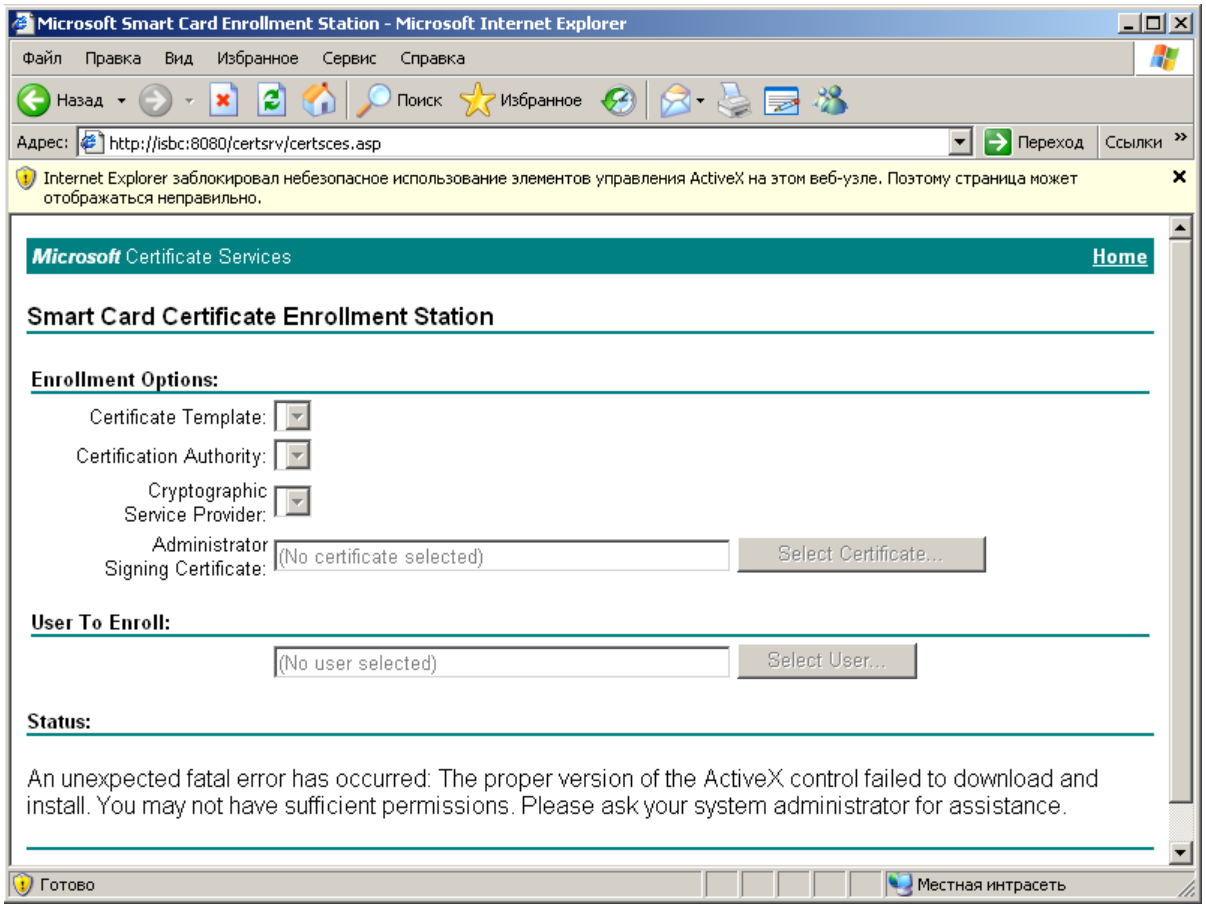
*Выберите **advanced certificate request** (Расширенный запрос сертификата):*



*Выберите нижнюю ссылку **Запросить сертификат от имени другого пользователя, используя станцию выдачи сертификатов**:*



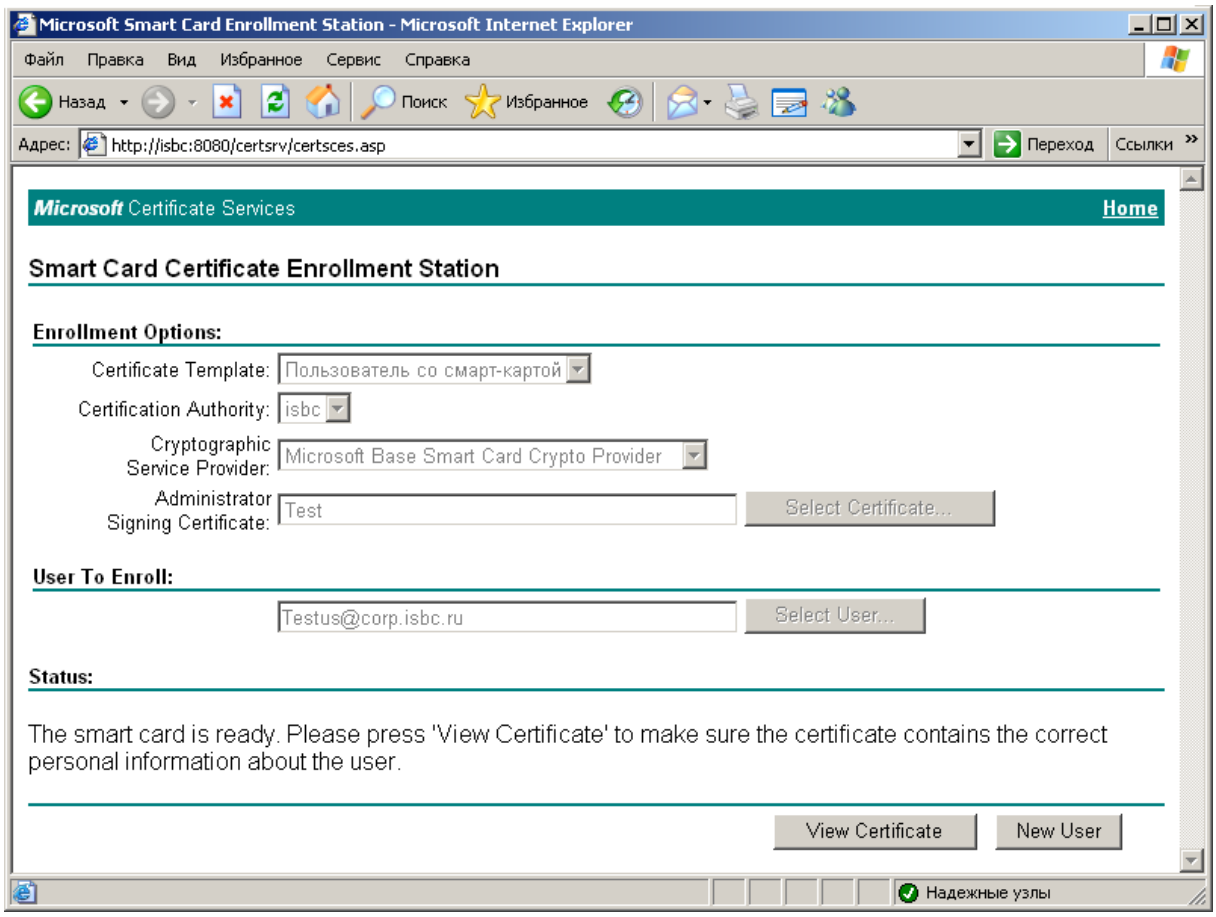
Также IE запросит разрешение на установку надстройки для выписки сертификата. Подтвердите установку настройки.



Выберите необходимые значения для полей:

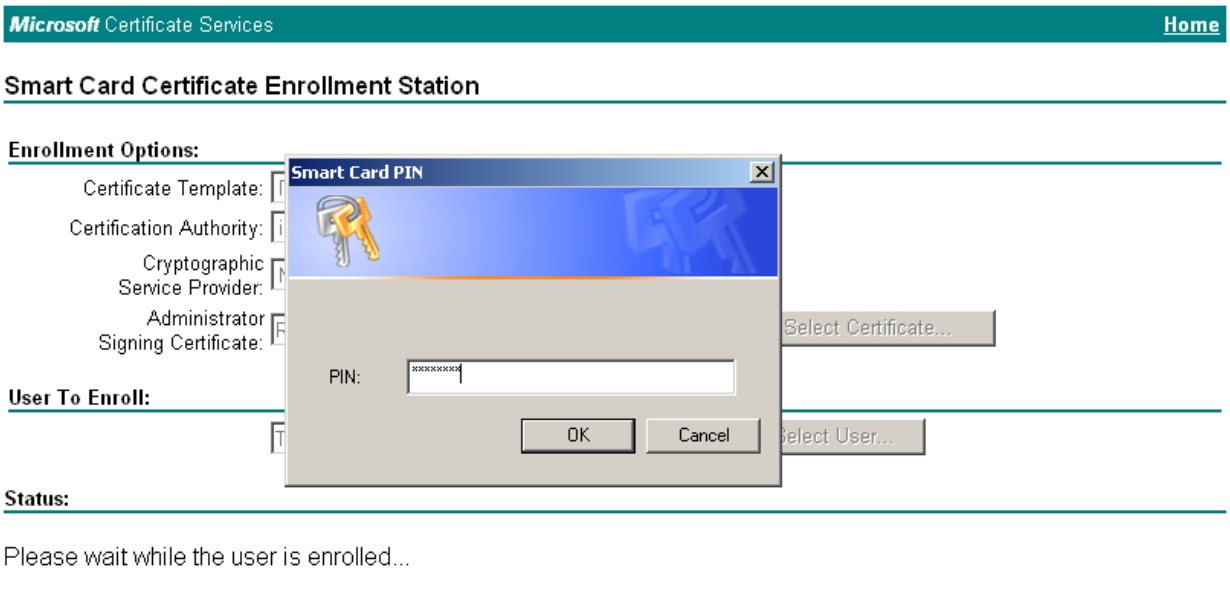
- *Шаблон сертификата (**Certificate template**);*
- *Сертифицирующий центр (**Certificate authority**);*
- *Криптопровайдер (**Cryptographic Service Provider**)[3];*
- *Сертификат администратора, от имени которого будет выписан сертификат (**Administrator Signing Certificate**).*

[3] *ESMART Token использует надстройку над криптопровайдером Microsoft Base Cryptographic Provider.*

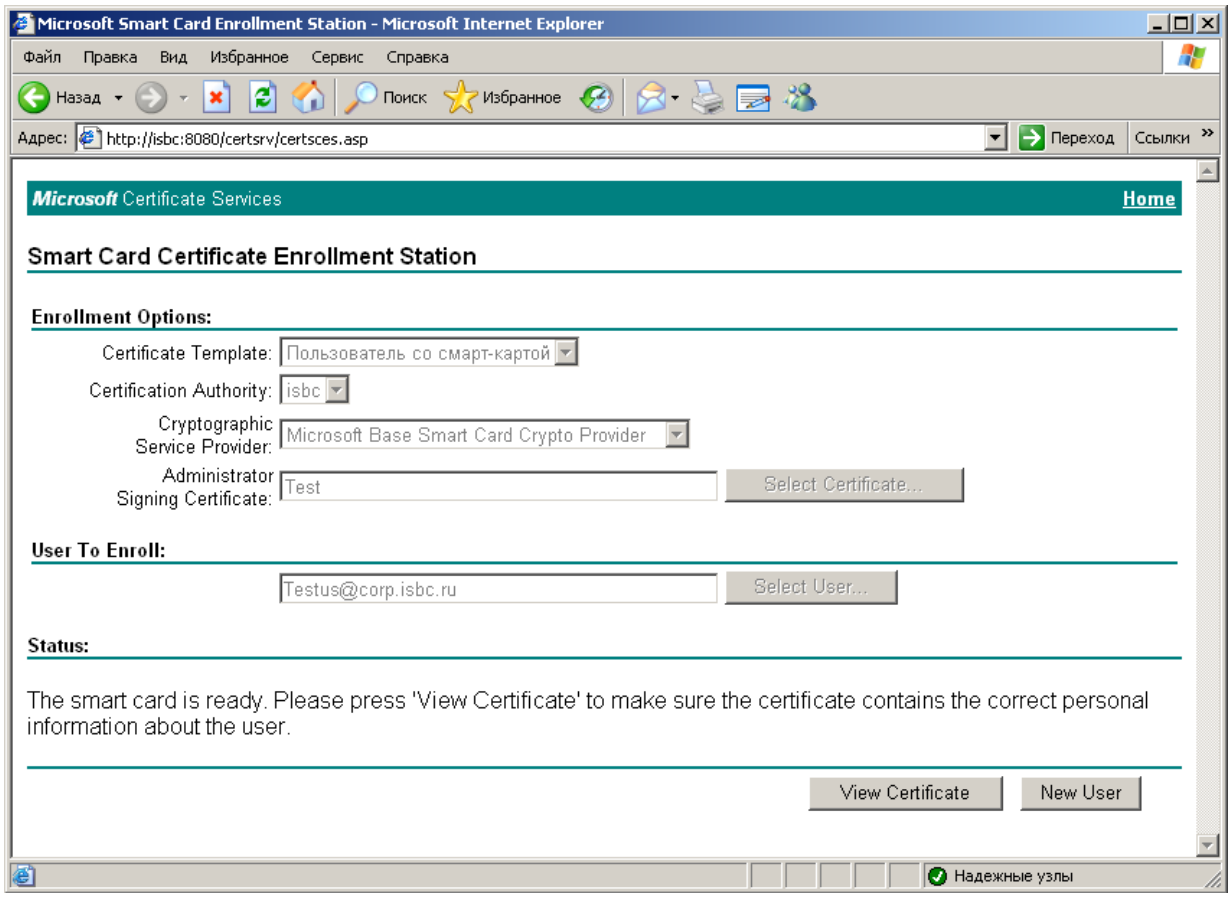


*Нажмите **Select User** и выберите пользователя смарт-карты. Убедитесь, что считыватель подключен к ПК и в него вставлена карта. Нажмите **Enroll** (Подать заявку).*

*В появившемся окне введите ПИН-код пользователя, который был задан при создании профиля на карте и нажмите **Вход в систему**.*



Дождитесь подтверждения:



*Нажмите **View Certificate** для просмотра сертификата или **New User** для запроса сертификата для следующего пользователя.*

Сертификат получен и записан на карту. Теперь пользователь может использовать сертификат для авторизации в Windows. При авторизации по сертификату вводить необходимо ПИН-код карты, а не пароль пользователя на ПК.

6. Установка ESMART PKI Client

*Рекомендуется установить пользователям бесплатное приложение ESMART PKI Client. При установке ESMART PKI Client через групповые политики необходимо заранее установить для всех пользователей сертификат ISBC в хранилище **Доверенные издатели**. Сертификат можно скопировать из инсталлятора приложения.*