eSMART®

Развертывание центра сертификации на базе Windows Server 2008

Содержание

1. Введение

В данном руководстве описана настройка службы сертификатов Active Directory на базе Windows Server 2008 и Windows Server 2008 R2 (Standard Edition, Enterprise Edition или Datacenter Edition)[1].

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

1.1 Центры сертификации

Ключевым элементом PKI является центр сертификации (ЦС)[2]. Служба сертификации Active Directory является одной из возможных ролей сервера под управлением операционной системы Windows Server.

Инфраструктура открытых ключей PKI основана на строгой иерархической модели, в которой выделяют:

- Корневой центр сертификации (англ. Root CA). Корневой центр сертификации всегда имеет самоподписанный сертификат.

- Промежуточные центры сертификации (англ. Subordinate CA), которые доверяют соответствующему корневому центру сертификации. Промежуточные центры сертификации могут образовывать многоуровневую иерархию.

На базе Microsoft Windows Server можно организовать центр сертификации одного из двух типов:

	Автономный центр сертификации (Stand-Alone CA)	**Центр сертификации предприятия (Enterprise CA)**
Интеграция с Active Directory	-	+
Запрос сертификатов	*Через web-интерфейс или через утилиту командной строки certreq.exe*	*Через web-интерфейс, консоль mmc или через утилиту командной строки certreq.exe*
Автоматическое получение и обновление сертификатов	-	+
Использование шаблонов	-	+
Данные сертификата	*Должны вводиться вручную*	*Могут браться из Active Directory*
Публикация сертификатов и списка отозванных сертификатов в AD	-	+

1.2 Планирование инфраструктуры

Обратите внимание на настройки групповых политик, представленные в данном руководстве, они позволяют значительно повысить безопасность системы.

При планировании инфраструктуры открытых ключей следует определить количество и иерархию центров сертификации.

При выборе количества уровней следует учитывать:

- ***Количество сотрудников предприятия.** Жестких критериев не существует. Microsoft рекомендует двухуровневую иерархию при количестве сотрудников более 300. Как правило, многоуровневая структура включает от 2 до 4 уровней;*

---

[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*

- ***Количество удаленных филиалов или отделений.*** *При небольшой численности сотрудников, но наличии большого количества филиалов, удаленных друг от друга, можно порекомендовать создание нескольких ЦС;*
- ***Структуру управления предприятием.*** *Отдельный ЦС может понадобиться для каждого филиала, если филиалы имеют собственные органы управления;*
- ***Выделенный бюджет****. Многоуровневая структура подразумевает большое количество оборудования и лицензий для операционных систем.*

Создание службы каталогов Active Directory в данном руководстве не рассматривается.

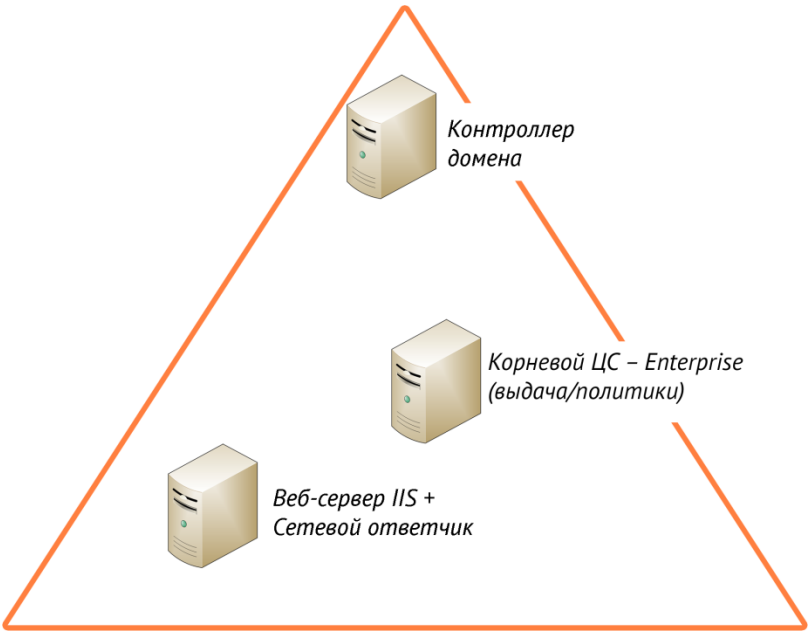
Microsoft не рекомендует размещать контроллер домена и центров сертификации на одном сервере. В противном случае можно столкнуться со следующими проблемами:

- *Домен контроллер, установленный на одном сервере с центром сертификации, невозможно будет ни переименовать, ни понизить. При вызове dcpromo.exe появится сообщение о необходимости сначала удалить центр сертификации;*
- *На домен-контроллере не установить автономный центр сертификации;*
- *Требуется тщательнее продумывать резервное копирование и восстановление из копии;*
- *Совмещение роли корневого центра сертификации с другими ролями считается нежелательным с точки зрения безопасности.*

Для крупных компаний с большим количеством региональных отделений рекомендуются сложная многоуровневая структура[3].

1.3 Примеры иерархии PKI

Одноуровневая иерархия PKI

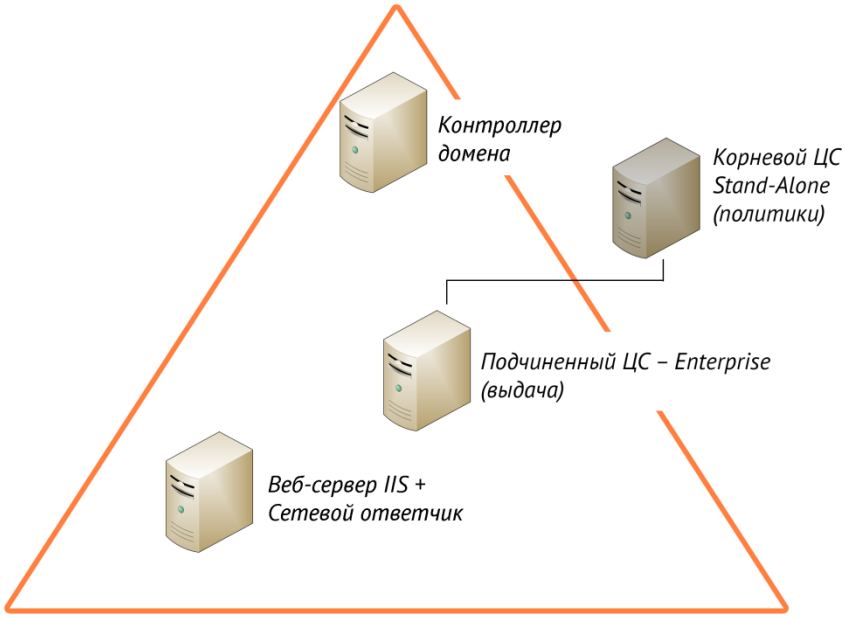


В одноуровневой иерархии PKI центр сертификации обеспечивает весь требуемый функционал. Данный вариант приемлем для небольших компаний. При необходимости веб-сервер с сетевым ответчиком может быть совмещен с сервером центра сертификации.

---

[3] Для дальнейшего изучения возможных типов иерархий PKI рекомендуется книга Windows Server 2008 PKI and Certificate Security, ISBN 13: 9780735625167

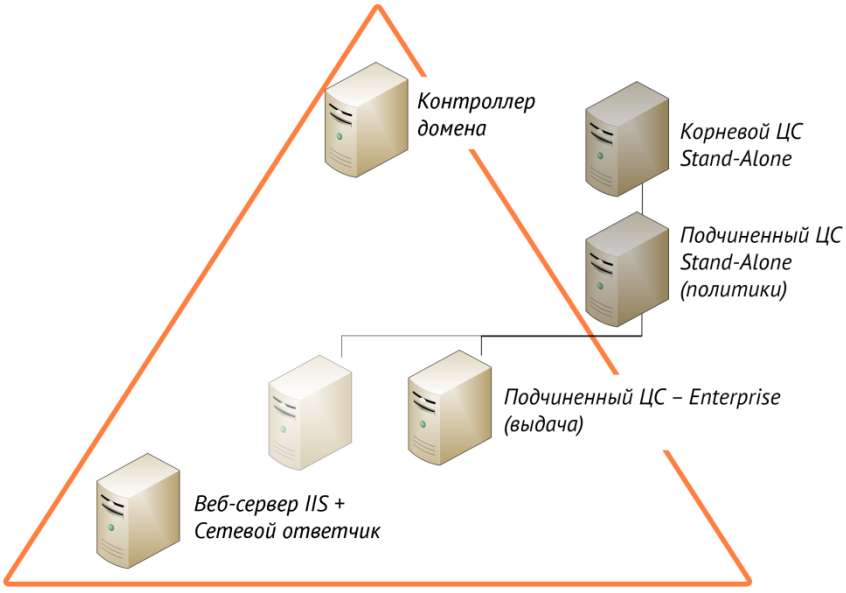
Двухуровневая иерархия PKI



Рекомендуемая конфигурация. Корневой сервер используется только для выдачи сертификатов одному или нескольким промежуточным центрам сертификации. Корневой центр сертификации находится в режиме offline и может не входить в Active Directory.

При необходимости веб-сервер с сетевым ответчиком может быть совмещен с сервером промежуточного центра сертификации.

Трехуровневая иерархия PKI



Трехуровневая иерархия, как правило, используется только в крупных проектах. Для работы с политиками выделен отдельный центр сертификации.

2. Установка ESMART PKI Client

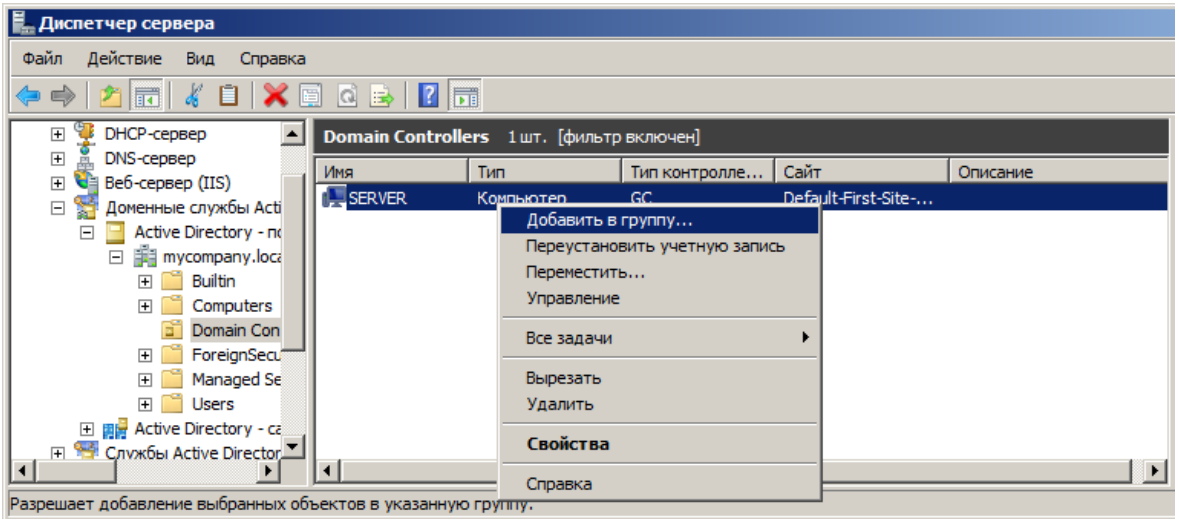
Установите на сервер, который будет выполнять функции ЦС, пакет ESMART PKI Client. Рекомендуется установка с помощью программы-инсталлятора. Подробно установка описана в руководстве администратора ESMART PKI Client.

3. Установка IIS Сервера

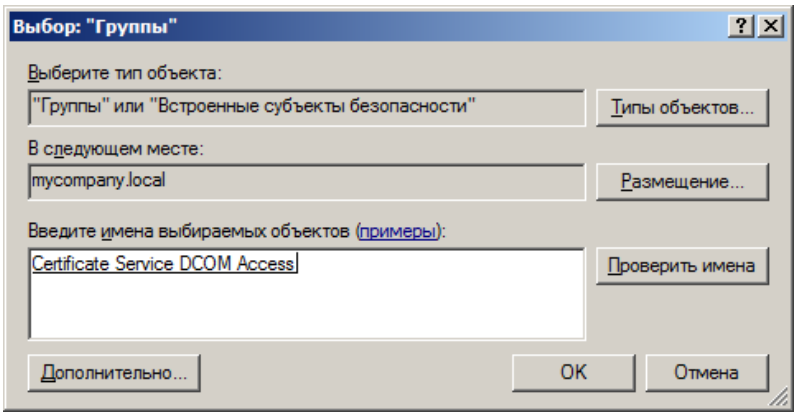
*Зайдите на сервер ЦС как администратор домена. Откройте диспетчер сервера (Server Manager). Нажмите **Добавить роли** (Add Roles), чтобы добавить новую роль. Выберите Web Server (IIS), оставьте значения по умолчанию и завершите установку.*

4. Добавление контроллера домена в группу CERTSVC_DCOM_ACCESS

*Откройте диспетчер сервера на контроллере домена. Чтобы добавить контроллер домена в группу CERTSVC_DCOM_ACCESS, выберите из контекстного меню **Добавить в группу...** (Add to a group...).*



Укажите часть имени группы, например, cert и выберите Certificate Service DCOM Access.



5. Настройка центра сертификации

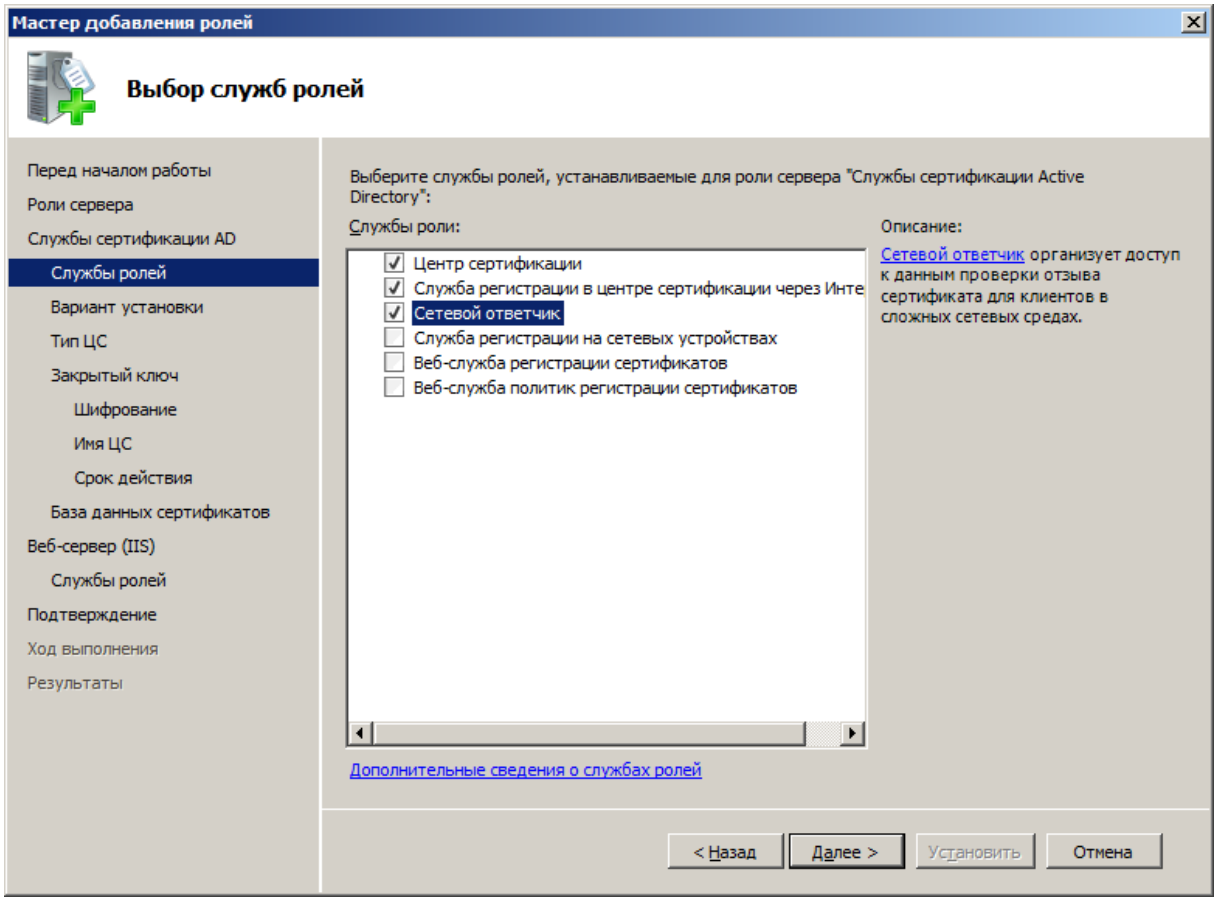
5.1 Добавление роли

Зайдите на сервер ЦС как Администратор домена. Откройте Server Manager. Нажмите ***Добавить роли*** *(Add Roles), чтобы добавить новую роль –* ***Службы сертификации Active Directory*** *(Active Directory Certificate Services).*

В качестве минимально требуемой конфигурации отметьте следующие опции.

- *Центр сертификации (Certification Authority);*
- *Служба регистрации в центре сертификации через интернет (Certification Authority Web Enrollment);*

Отметьте также Сетевой ответчик (Online Responder), если его планируется устанавливать на той же машине, что и центр сертификации.



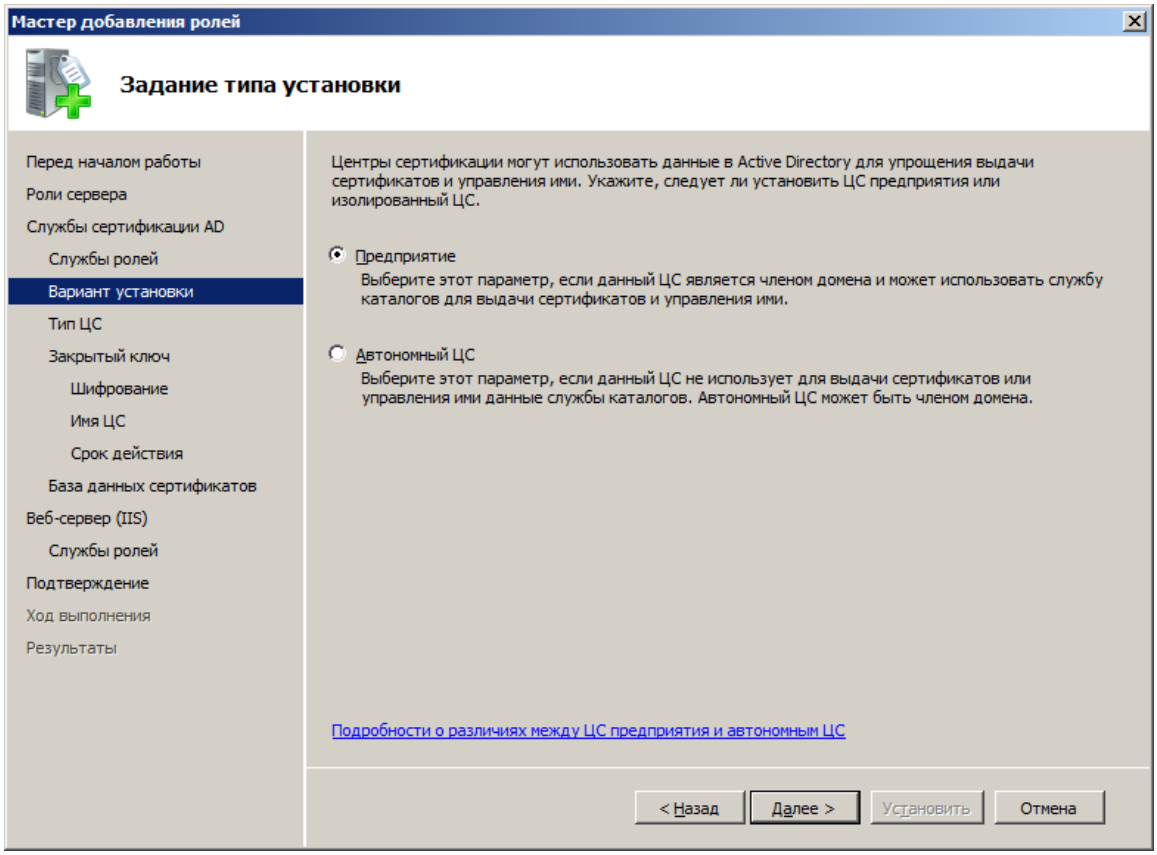
Для службы регистрации через интернет (называемой веб-интерфейсом центра сертификации) и для сетевого ответчика требуются службы IIS-сервера. Подтвердите установку соответствующих служб, нажав ***Добавить требуемые службы*** *(Add Required Role Services).*

Выбрав необходимые опции, нажмите ***Далее****. В следующем окне укажите тип сервера:*

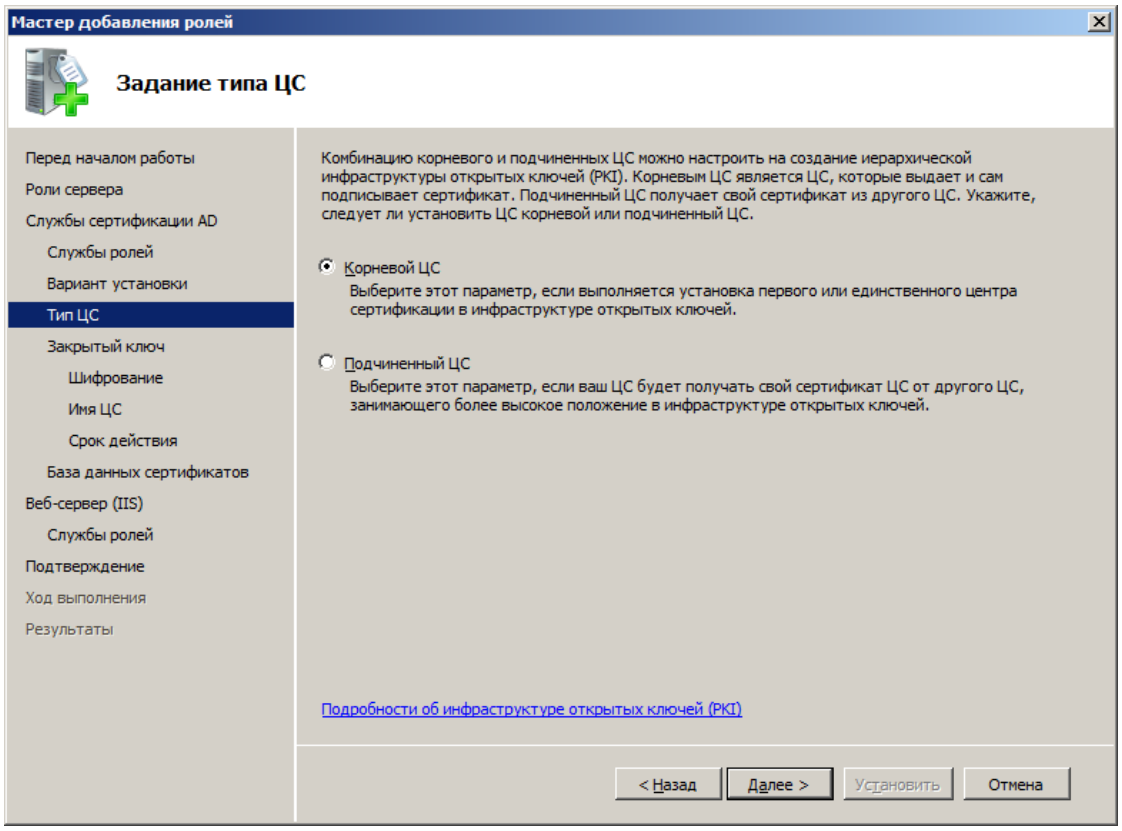
- ***Enterprise*** *(Предприятие) – если это единственный ЦС в одноуровневом PKI или не корневой ЦС в многоуровневом PKI;*
- ***Standalone*** *(Автономный) – если это корневой ЦС в многоуровневом PKI.*

Опция Enterprise может быть недоступна, если ЦС устанавливается не от имени администратора предприятия (Группа Enterprise Admin), или компьютер не входит в домен.

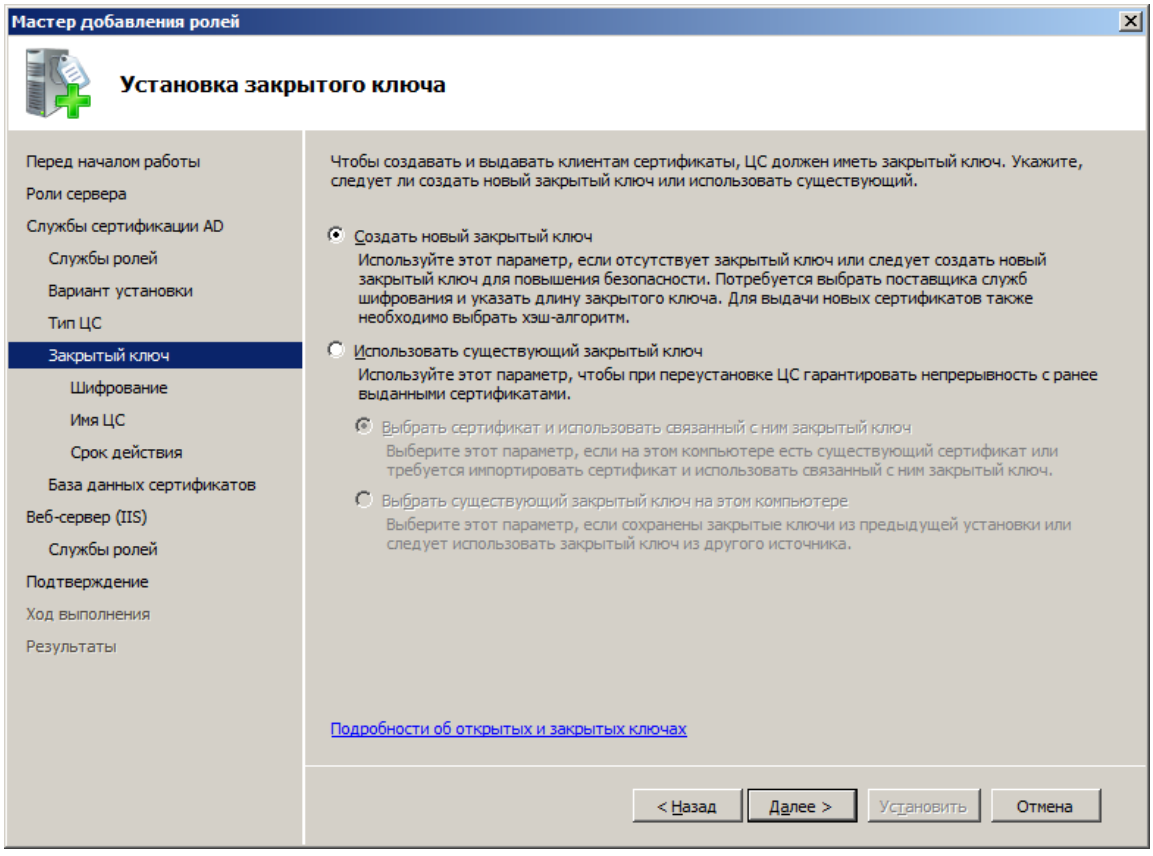
В руководстве описана настройка корневого ЦС одноуровневого PKI на сервере типа Enterprise. Возможны другие варианты построения PKI в зависимости от количества сотрудников, бюджета, кадровой политики и других параметров.



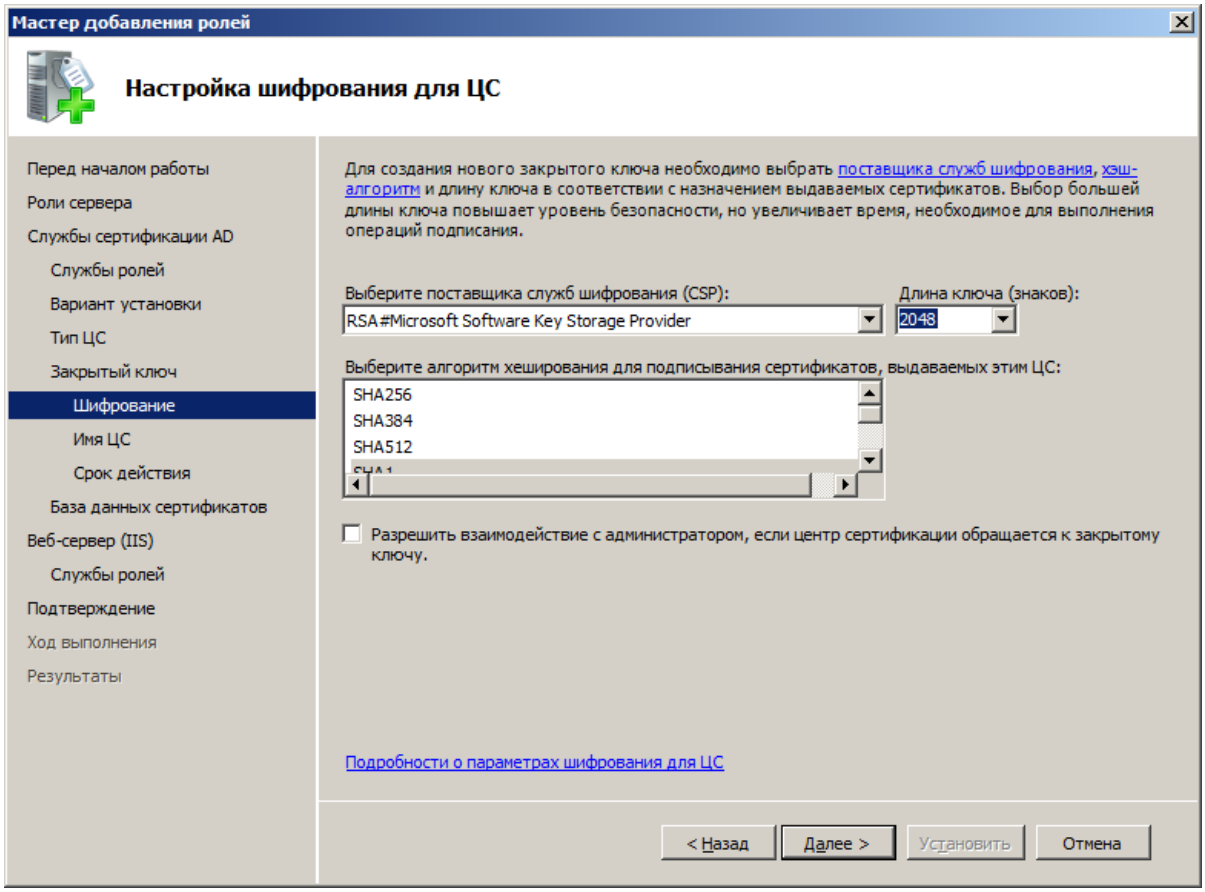
Укажите тип ЦС на данном сервере в зависимости от выбранной архитектуры PKI. Корневой (Root CA) или подчиненный (Subordinate CA).



Создайте новый закрытый ключ (Create a new private key). Если необходимо в рамках проекта, можно использовать существующую ключевую пару, выбрав (Use existing private key).



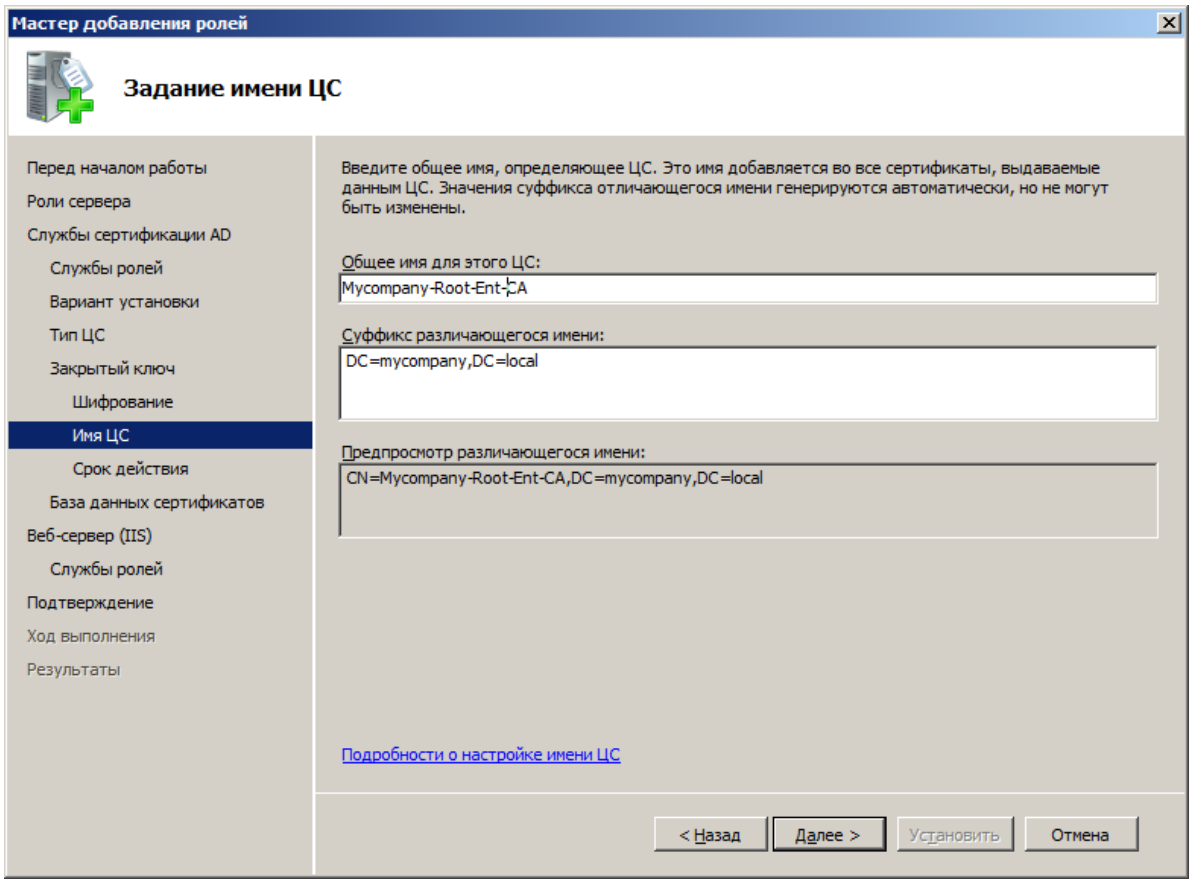
Оставьте значения по умолчанию или задайте другую длину ключа и алгоритм хеширования в соответствии с корпоративными требованиями.



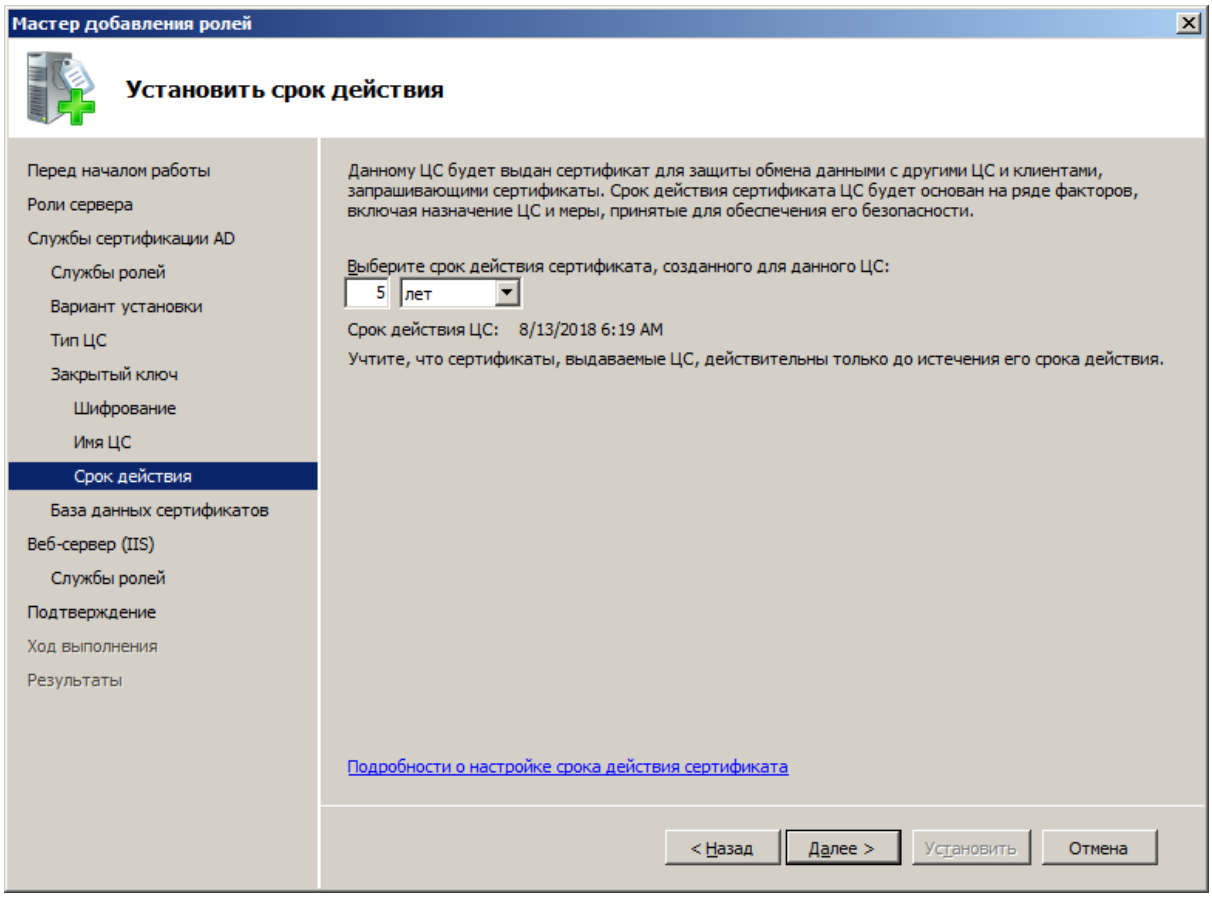
Задайте имена, которые будут отображаться в корневом сертификате (в примере использованы значения по умолчанию).

***Внимание!** Изменить параметр common name и название домена после завершения операции будет невозможно.*

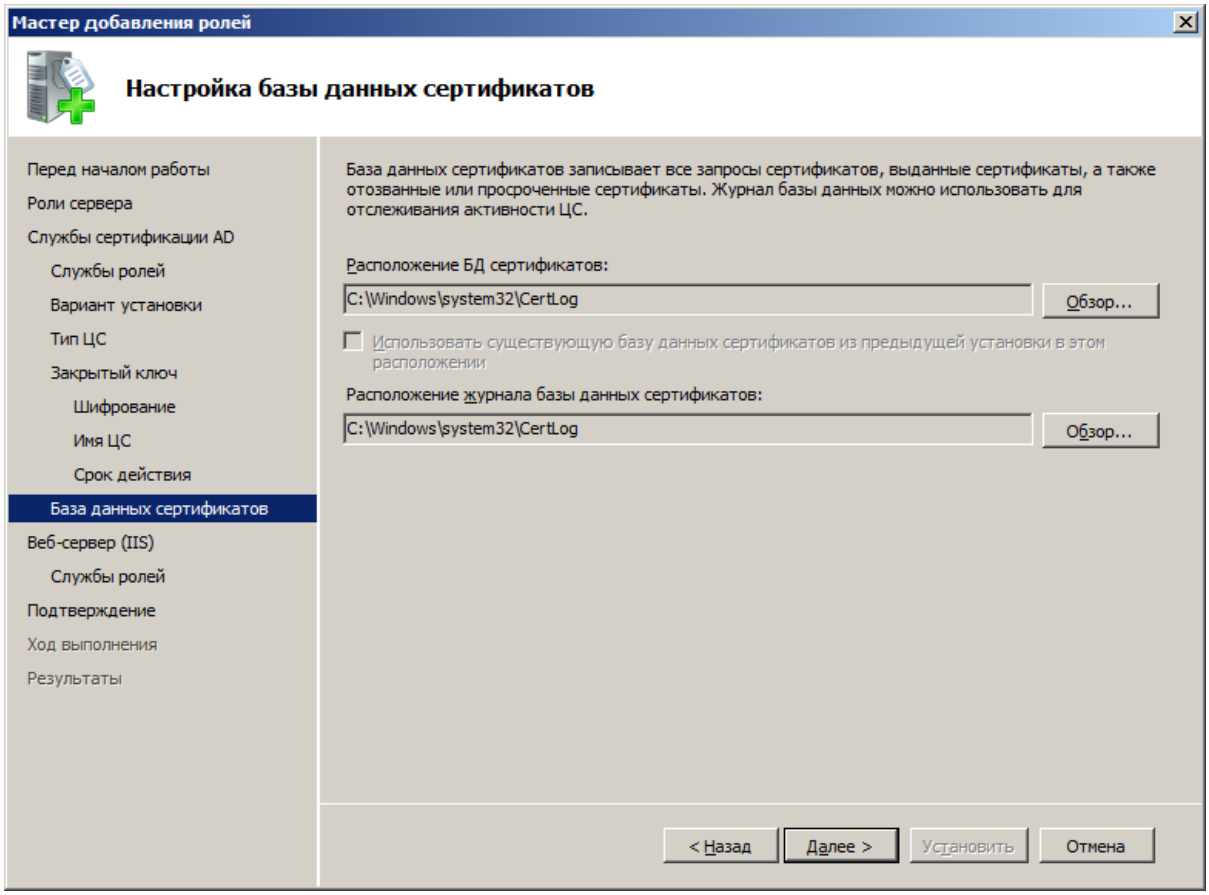
Если центр сертификации установлен на сервере, выполняющем роль контроллера домена, для изменения имени контроллера домена потребуется переустановить центр сертификации.



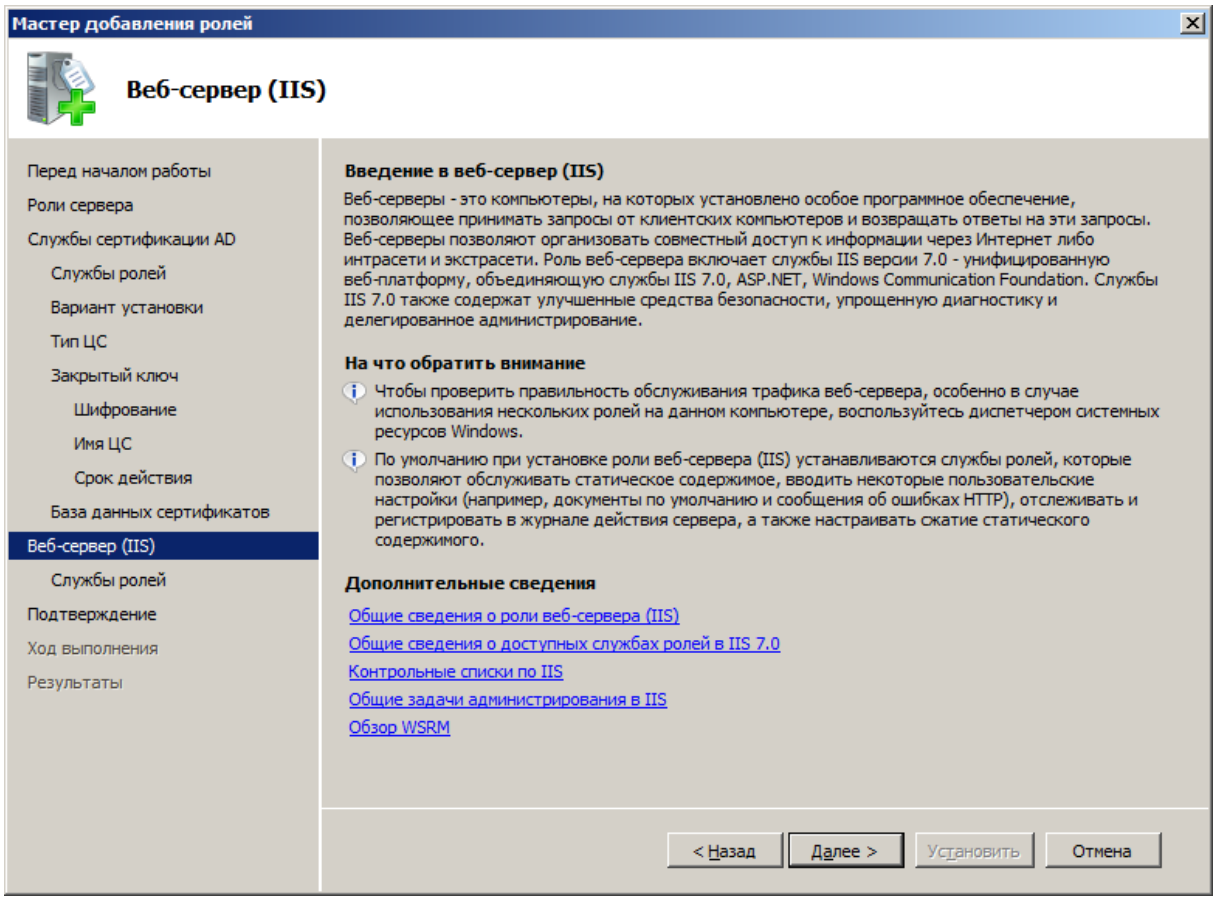
Выберите срок действия. Обычно задают срок минимум в 2 – 5 раз больше, чем планируемый срок действия сертификатов клиентов.


Мастер добавления ролей
Установить срок действия
Перед началом работы
Роли сервера
Службы сертификации AD
Службы ролей
Вариант установки
Тип ЦС
Закрытый ключ
Шифрование
Имя ЦС
Срок действия
База данных сертификатов
Веб-сервер (IIS)
Службы ролей
Подтверждение
Ход выполнения
Результаты
Данному ЦС будет выдан сертификат для защиты обмена данными с другими ЦС и клиентами, запрашивающими сертификаты. Срок действия сертификата ЦС будет основан на ряде факторов, включая назначение ЦС и меры, принятые для обеспечения его безопасности.
Выберите срок действия сертификата, созданного для данного ЦС:
5
лет
Срок действия ЦС: 8/13/2018 6:19 AM
Учтите, что сертификаты, выдаваемые ЦС, действительны только до истечения его срока действия.
Подробности о настройке срока действия сертификата
< Назад
Далее >
Установить
Отмена

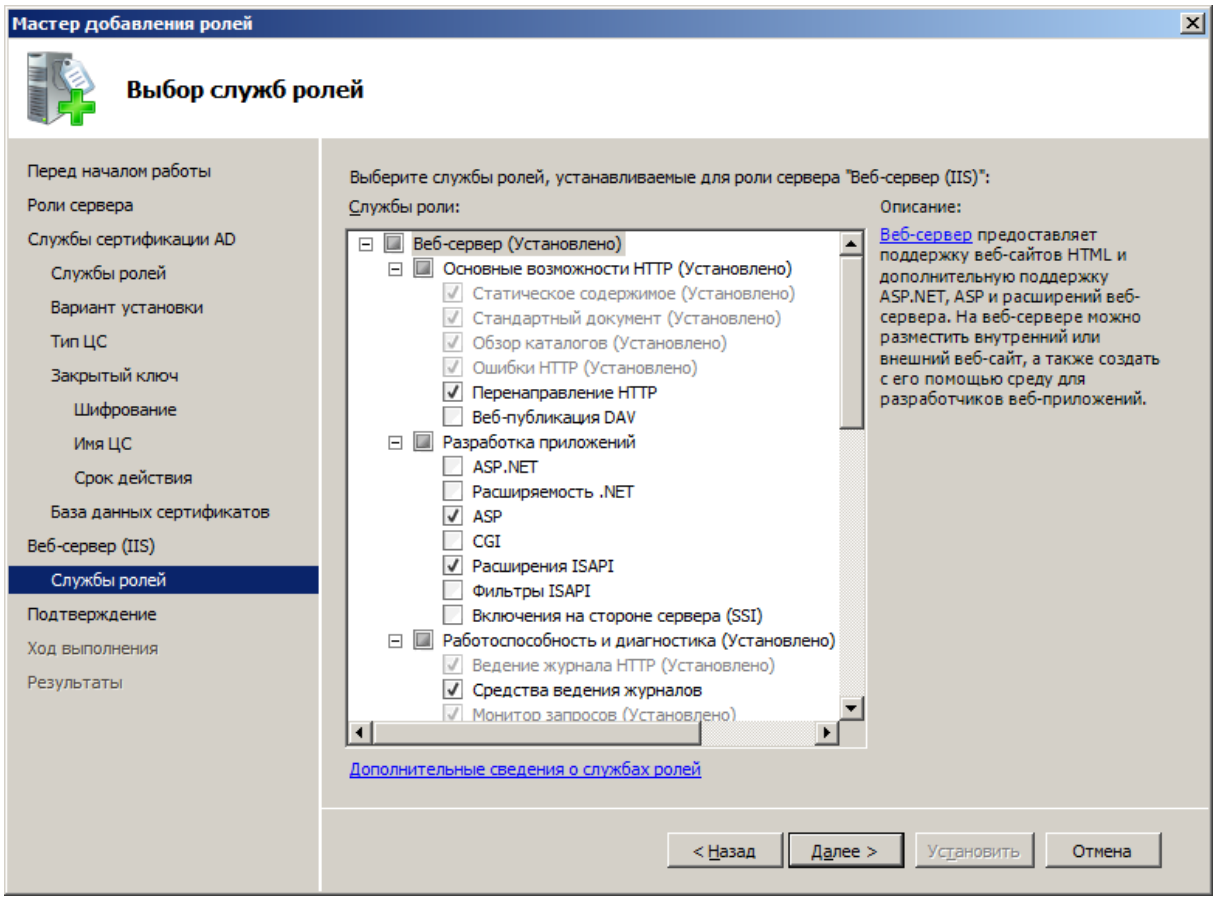
Укажите адреса баз данных и логов. Если оставить адреса по умолчанию, в диспетчере сервера может выдаваться предупреждение.



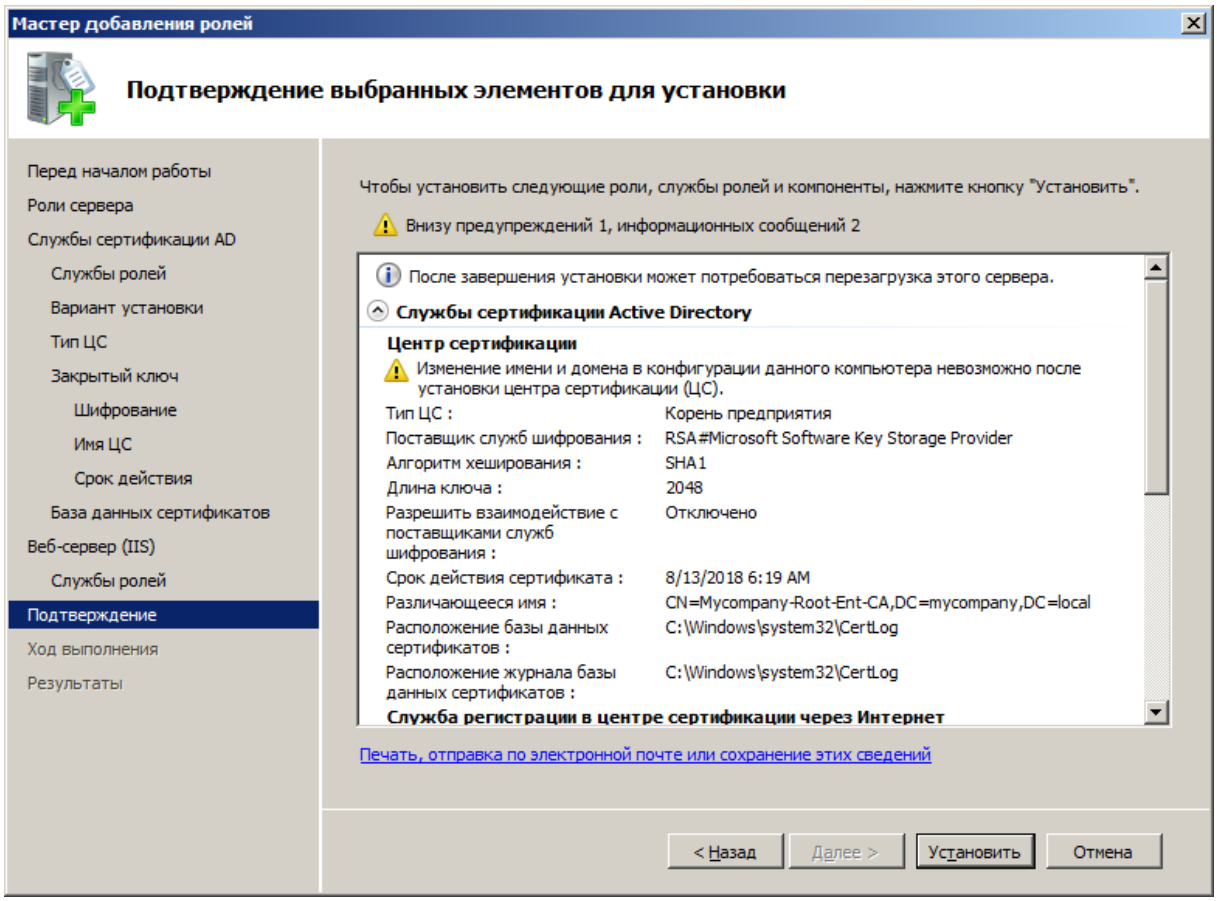
Настройка веб-сервера. Просмотрите информацию и нажмите далее.



Отметьте необходимые опции (можно оставить значения по умолчанию).



*Проверьте параметры. Нажмите **Install** (Установить) и дождитесь, пока выбранные опции будут установлены.*



5.2 Веб-интерфейс центра сертификации

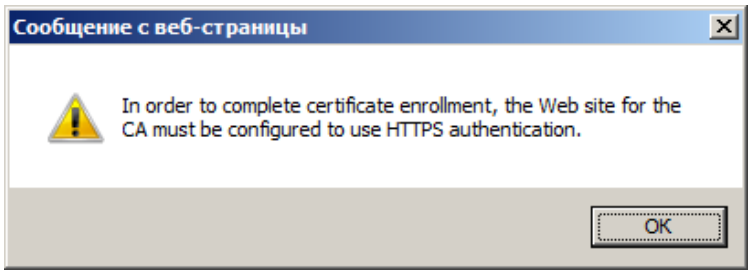
Служба регистрации в службе сертификации через интернет (Certificate Enrollment Web Services) обеспечивает доступ к основным возможностям центра сертификации через интернет-браузер. Для работы с веб-интерфейсом рекомендуется использовать Internet Explorer. В других браузерах некоторые функции могут не поддерживаться. IE 10 не поддерживается.

Таблица совместимости серверов Windows Server и клиентских ПК для доступа к веб-интерфейсу центра сертификации.

	Windows Server 2003 и Windows Server 2003 SP1	*Windows Server 2003 SP2*	*Windows Server 2008*
Windows XP и ранее	*Поддерживается*	*Поддерживается*	*Поддерживается, но не весь функционал*
Windows Vista и позднее	*Не поддерживается. Ошибка «Downloading ActiveX control»*	*Не поддерживается. Появляется сообщение о необходимости обновить Веб-интерфейс*	*Поддерживается*

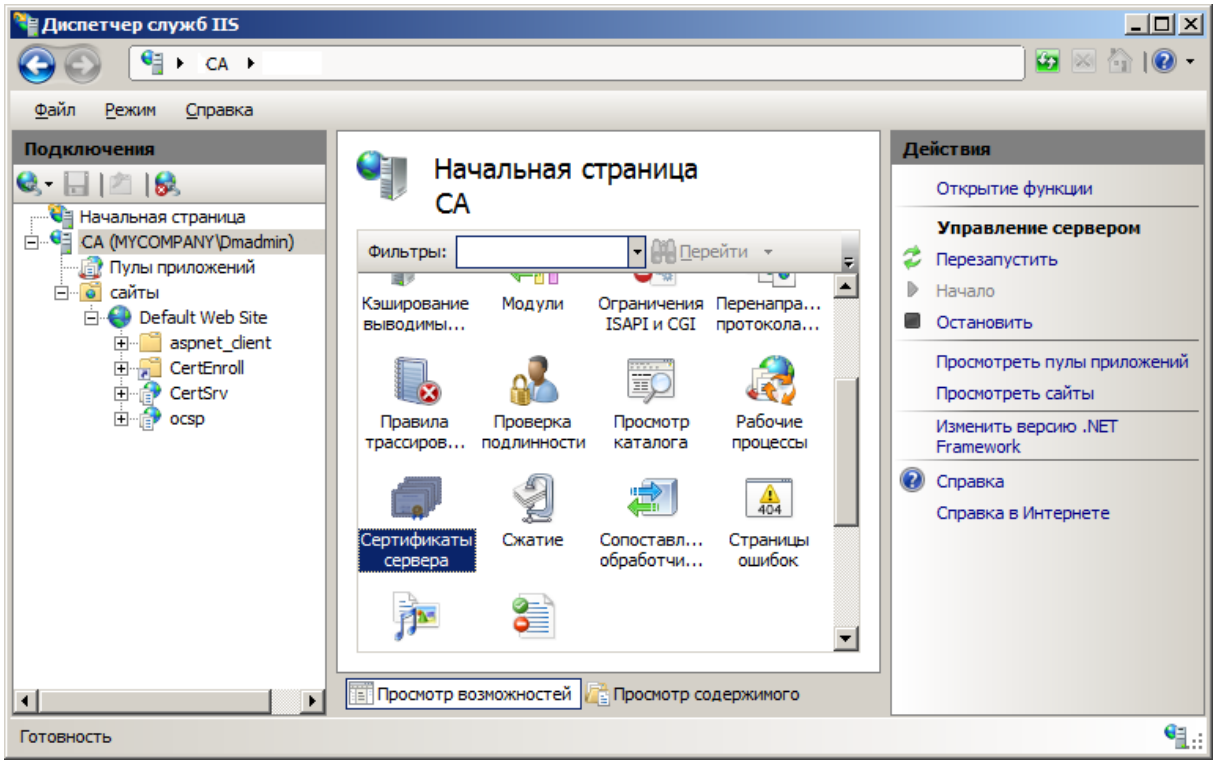
После установки службы регистрации интерфейс доступен по адресу http(s)://localhost/certsrv с машины на которой стоит центр сертификации. При обращении с других компьютеров можно указать IP-адрес или FQDN сервера ЦС, например, http(s)://10.1.1.5/certsrv или http(s)://ca.mycompany.local/certsrv. Адрес следует набирать строчными буквами.

На веб-интерфейс службы сертификации следует заходить по протоколу https. При попытке выписать сертификат по незащищенному http-соединению появится следующая ошибка:

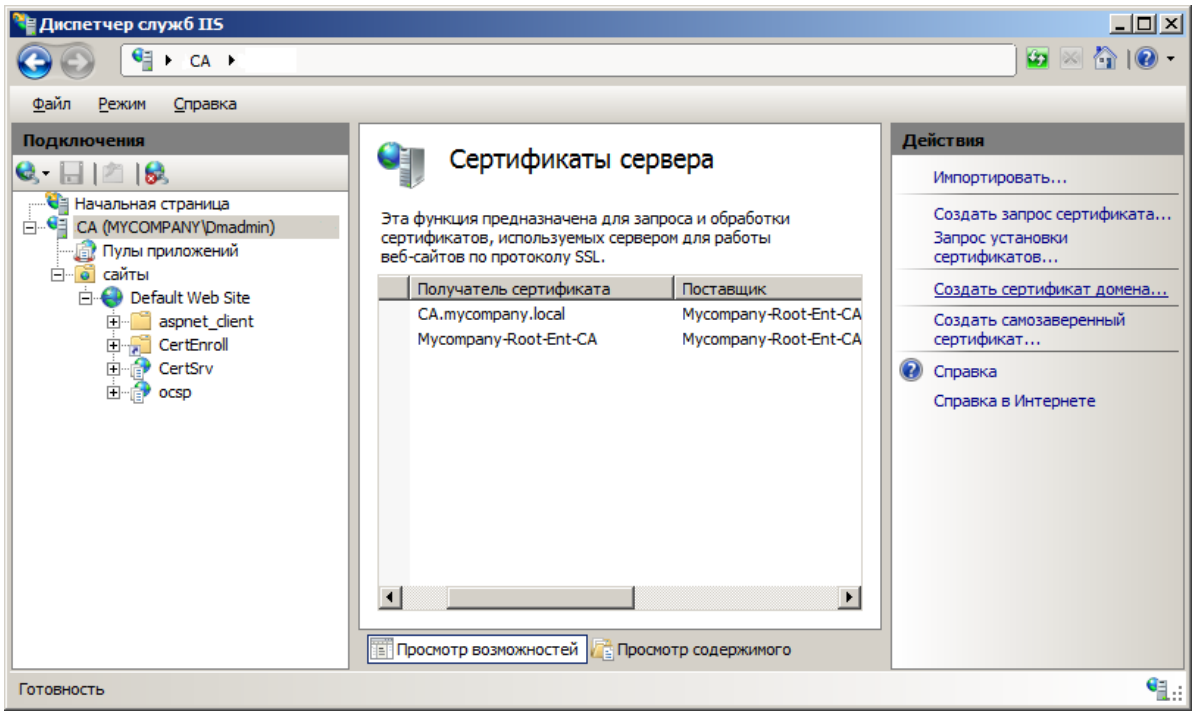


Чтобы получить сертификат для веб-интерфейса центра сертификации, проделайте следующие операции:

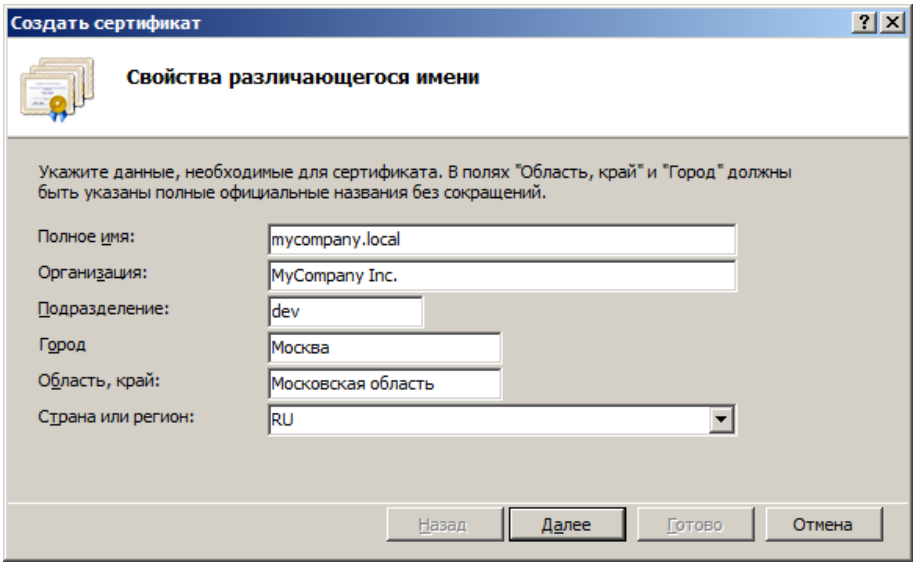
- *Выберите доменное имя, которое будет использоваться для доступа к веб-интерфейсу. В примере выбрано общее доменное имя mycompany.local.*
- *Откройте диспетчер служб IIS и выберите сервер, на котором установлен веб-интерфейс центр сертификации (в данном примере – сервер ЦС). Выберите* ***Сертификаты сервера*** *(****Server Certificates****).*



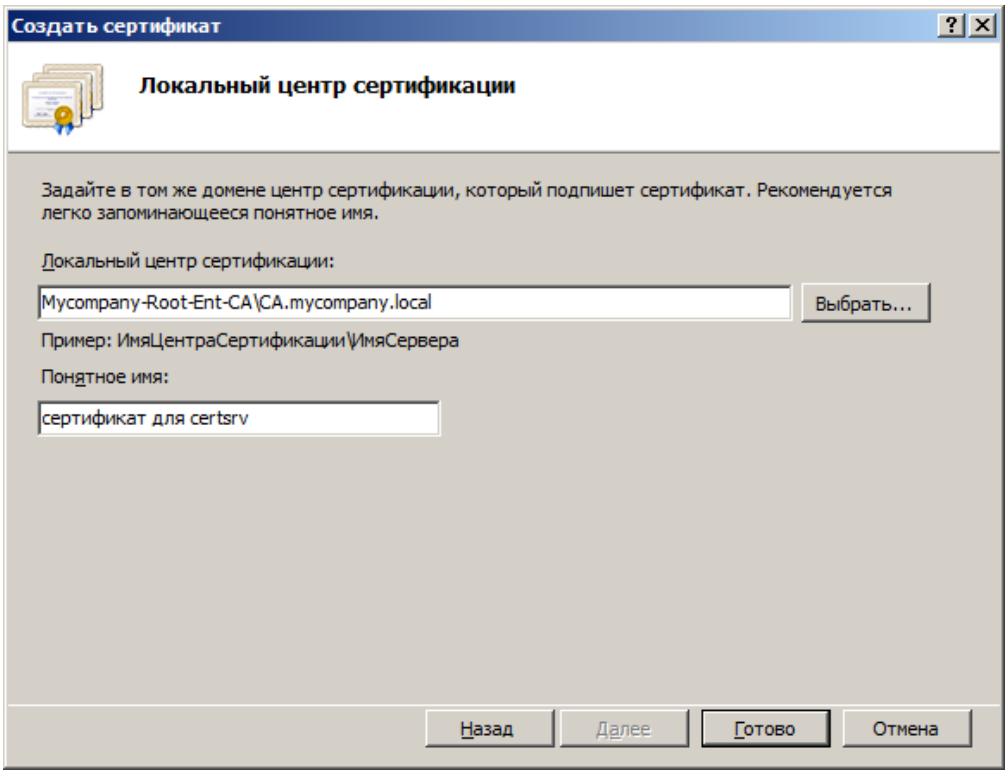
В открывшемся разделе будут опубликованы сертификаты данного сервера. В меню справа выберите ***Создать сертификат домена*** *(****Create Domain Certificate****).*



*Заполните форму. В поле **Полное имя** необходимо ввести планируемое доменное имя.*

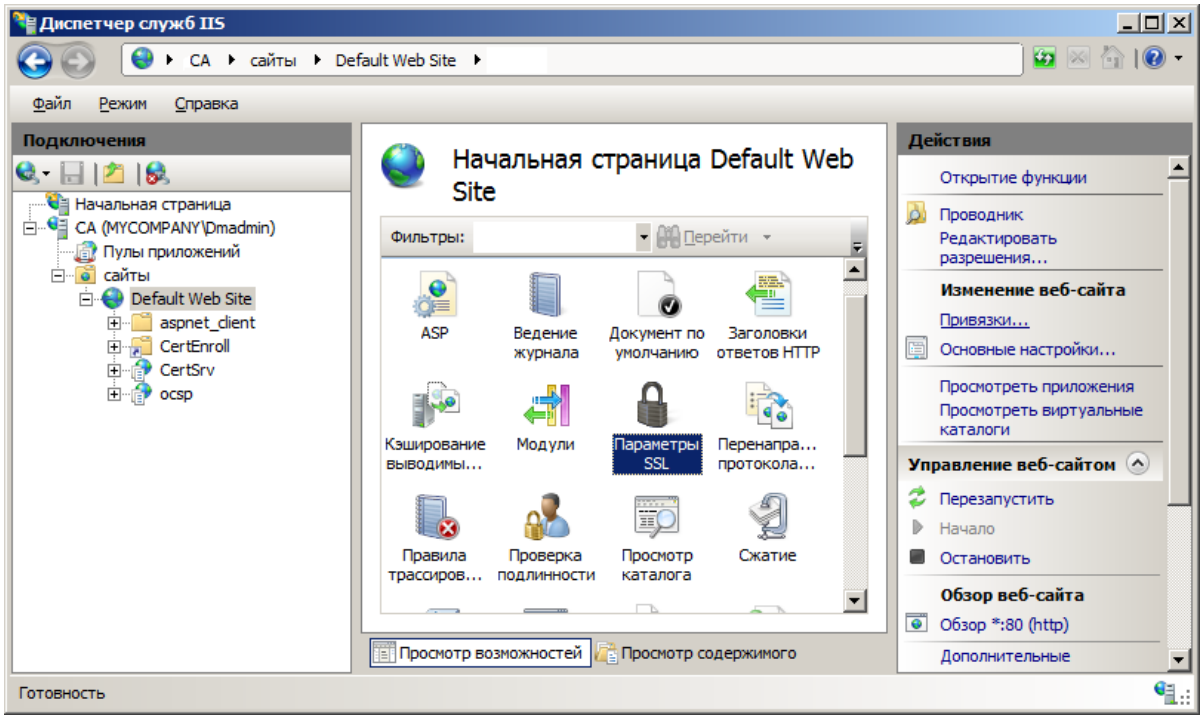


Укажите центр сертификации, который будет подписывать данный сертификат и введите понятное имя.

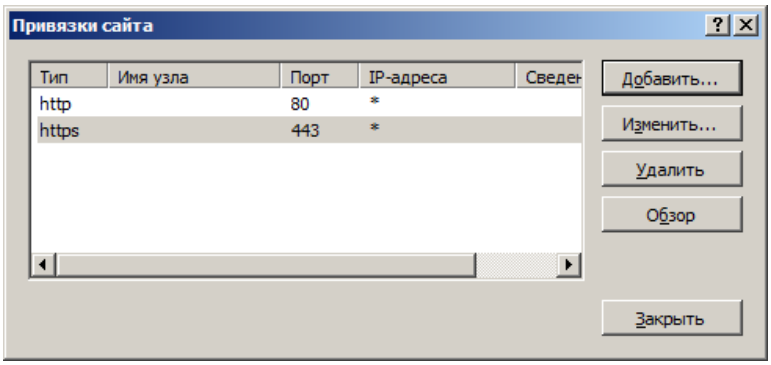


Выписанный сертификат появится в списке сертификатов сервера.

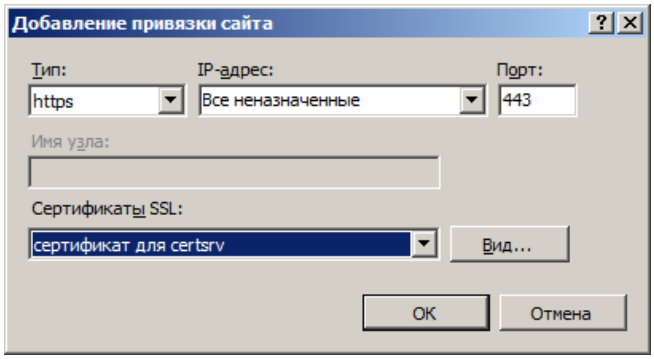
Перейдите в диспетчере служб IIS к разделу сайтов.



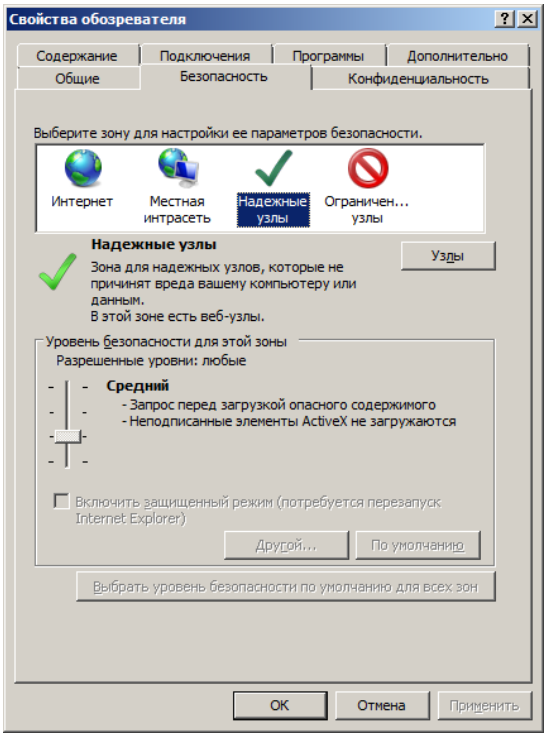
*Выберите сайт и в меню справа откройте пункт **Привязки** (Bindings). Добавьте привязку по https на порт 443, если ее нет в списке.*

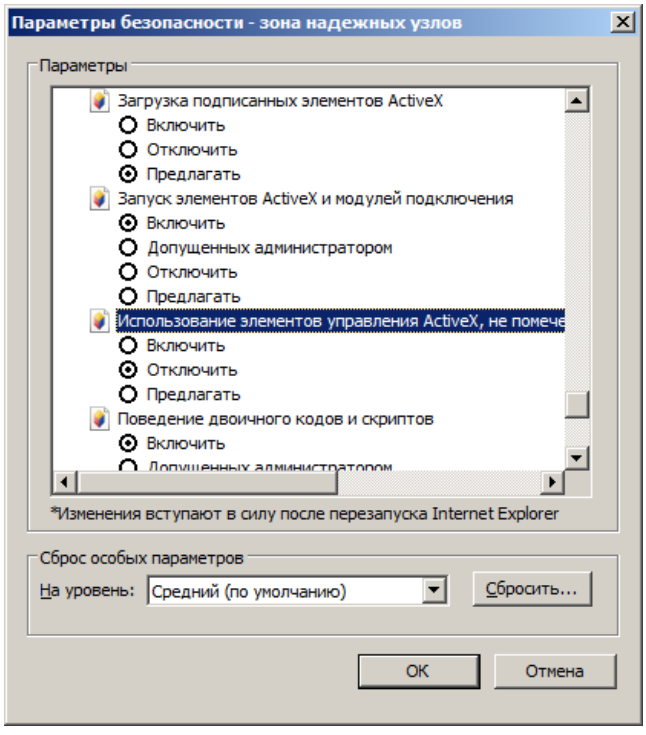


В настройках привязки по https укажите созданный на предыдущем этапе сертификат веб-сервера.



Веб-интерфейс центра сертификации использует технологии Active X, которые по умолчанию отключены в настройках браузера. Для использования веб-интерфейса необходимо внести сайт в доверенную зону, где по умолчанию разрешено выполнение Active X.



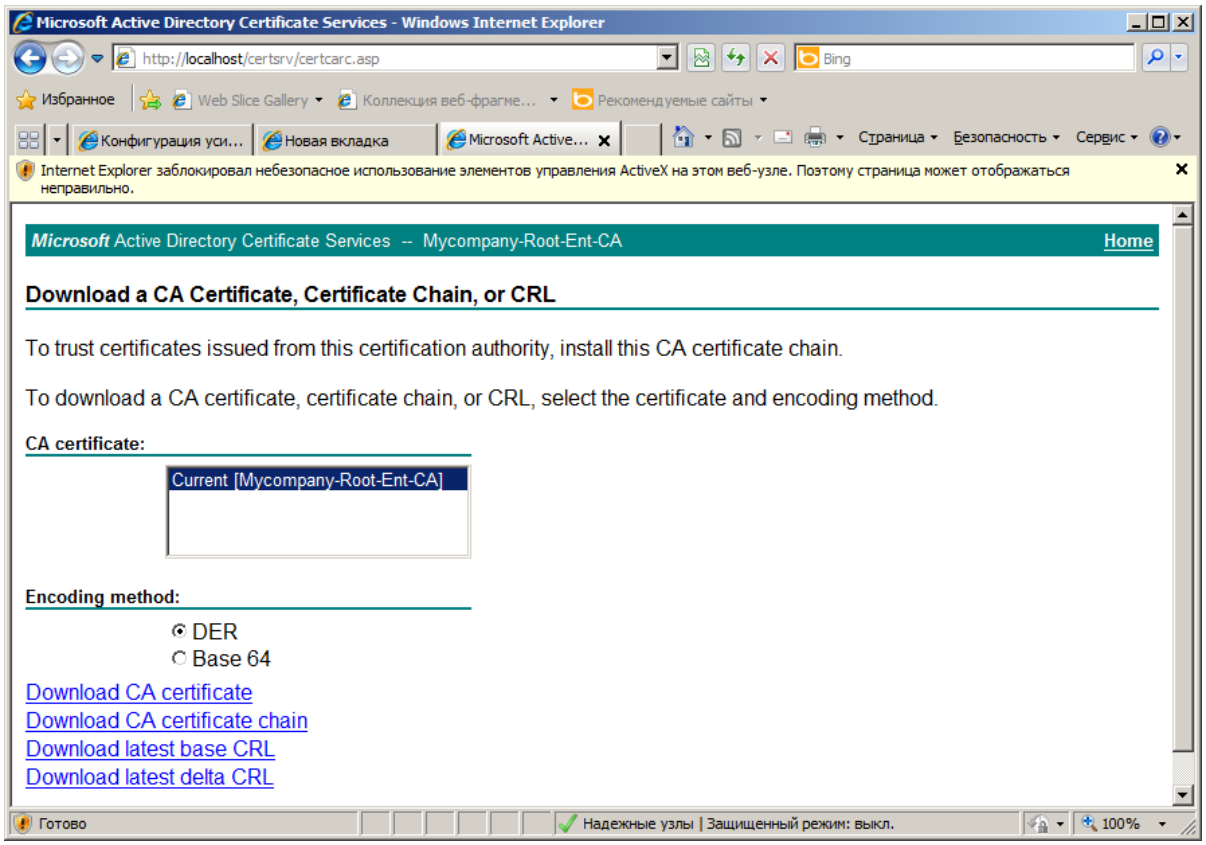


Если в настройках Internet Explorer не доступно изменение уровня безопасности, отключите Конфигурацию усиленной безопасности Internet Explorer (Enhanced Security Configuration).

Если после добавления сайта в доверенную зону ошибка не пропадает, в параметрах безопасности измените ***Использование элементов управления Active X, не помеченных как безопасные для использования*** *(Initialize and script ActiveX controls not marked as safe for scripting) на* ***Включить*** *или* ***Предлагать****.*

Веб-интерфейс готов к использованию.

5.3 Использование веб-интерфейса



Веб-интерфейс позволяет скачать в виде файлов в двоичном виде (DER) или в кодировке Base64:

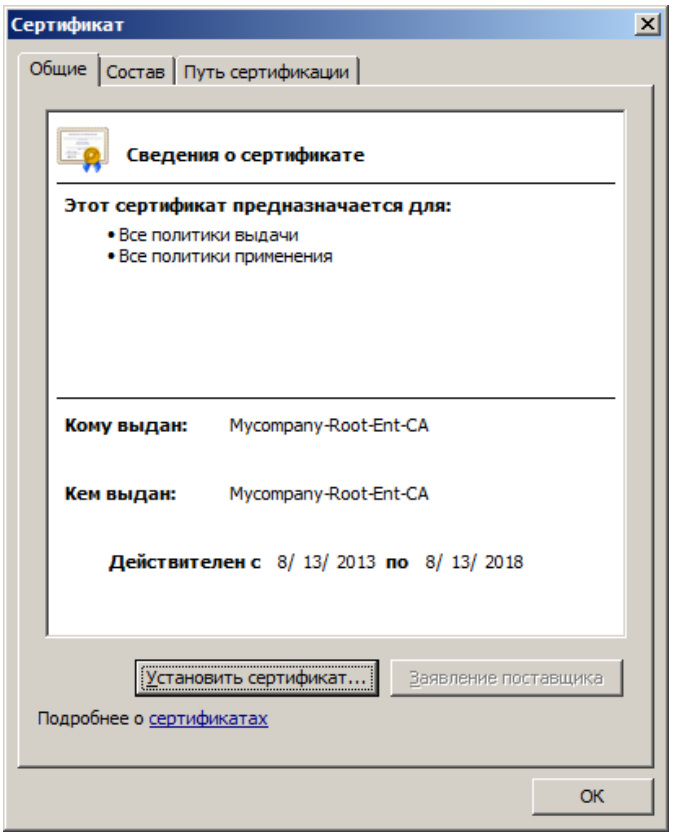
Download CA certificate	*Корневой сертификат центра сертификации в файле .cer*
Download CA certificate chain	*Цепочку сертификатов в файле .p7b*
Download latest base CRL	*Последнюю версию базового списка отозванных сертификатов*
Download latest delta CRL	*Последнюю версию разностного списка отозванных сертификатов*

В бинарном виде данные файлы хранятся в C:\Windows\System32\certsrv\CertEnroll.

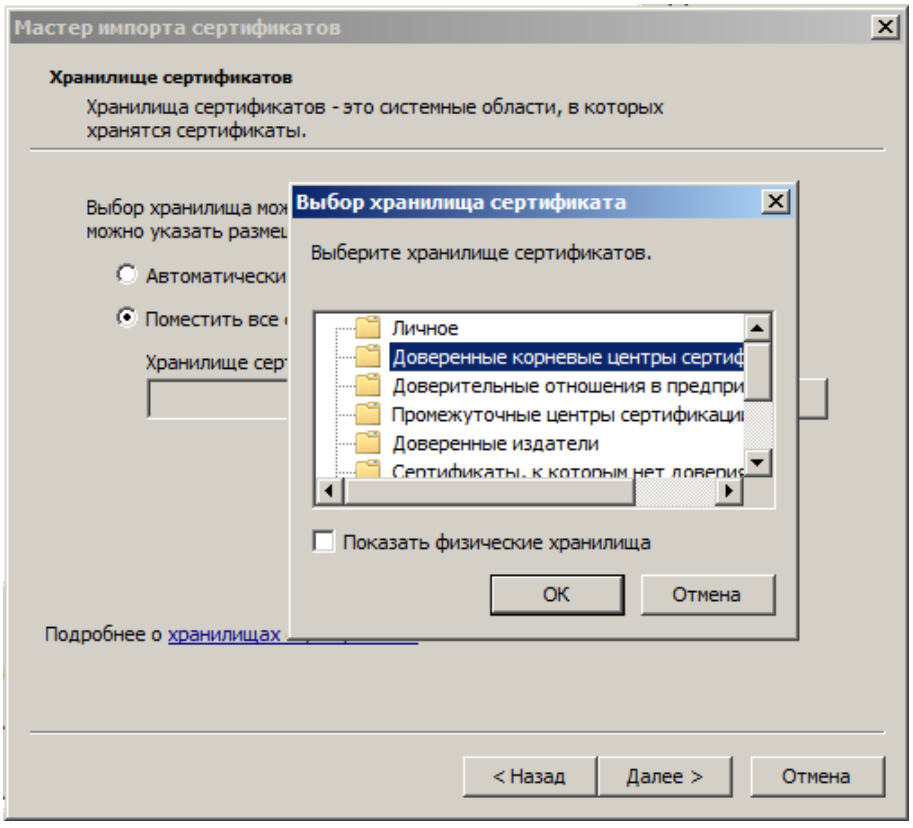
5.4 Установка корневого сертификата вручную

Ручная установка корневого сертификата может потребоваться для машин, которые не входят в Active Directory.

Перенесите файл сертификата (без закрытого ключа) при помощи съемного носителя или скачайте его через веб-интерфейс центра сертификации (если возможно) и нажмите ***Установить сертификат****.*



Рекомендуется вручную выбрать раздел хранилища ***Доверенные корневые центры сертификации (Trusted Root Certification Authorities)*** *или* ***Промежуточные центры сертификации (Intermediate Certificate Authorities)*** *в зависимости от типа сертификата.*



5.5 Распространение сертификата через групповые политики

При установке центра сертификации типа Enterprise корневой сертификат автоматически публикуется в Active Directory. После установки центра сертификации выполните в командной строке сервера центра сертификации

```
certutil -pulse
```

Сертификат будет помещен в хранилище после перезагрузки клиентских машин.

Описанная ниже процедура позволяет распространить на все ПК в домене корневой сертификат центра сертификации автономного типа, не входящего в домен (типа Stand-Alone). Также данная процедура может применяться для распространения сторонних сертификатов.

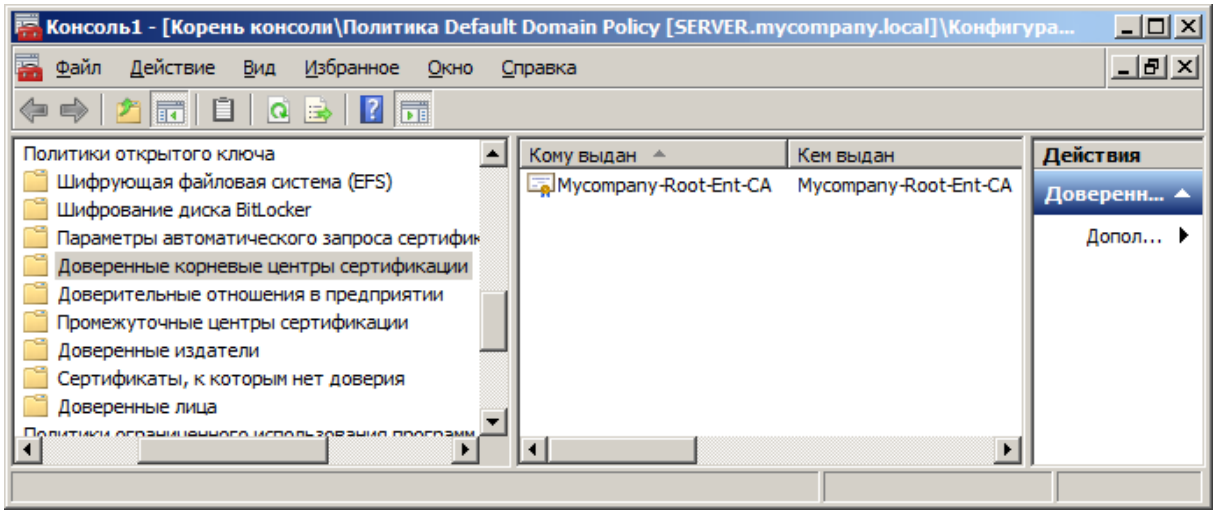
Использование групповых политик позволяет поместить сертификаты корневого и/или промежуточных ЦС в соответствующее хранилище компьютеров, входящих в домен, автоматически, не повторяя импорт на каждой машине.

На контроллере домена откройте консоль MMC. Добавьте оснастку ***Редактор управления групповыми политиками (Group Policy Management Editor)****. Выберите политику* ***Default Domain Policy*** *или другую используемую.*

Раскройте дерево:

Конфигурация компьютера › Политики › Конфигурация Windows › Параметры безопасности › Политики открытого ключа › Доверенные корневые центры сертификации.

Computer Configuration › Policies › Windows Settings › Security Settings › Public Key Policies › Trusted Root Certification Authorities.

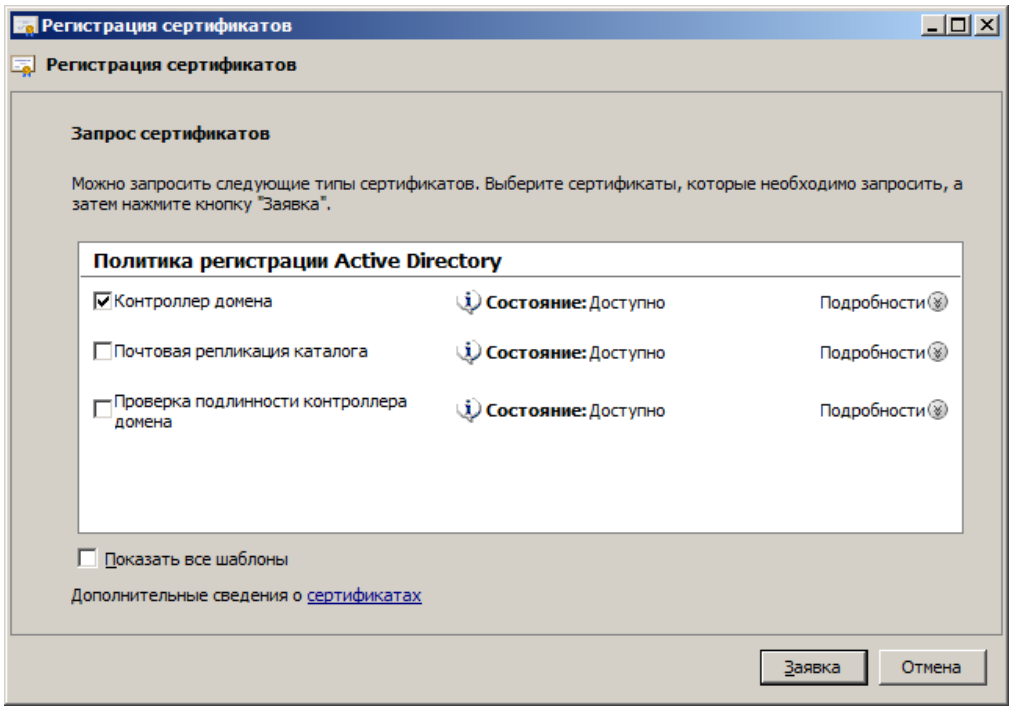


Обновите групповые политики и перезагрузите сервер.

```
gpupdate /force
```

5.6 Сертификат контроллера домена

Выпишите сертификат для каждого контроллера домена. На контроллере домена запустите консоль mmc. Добавьте оснастку Сертификаты для локального компьютера. Откройте хранилище сертификатов Личное. Выберите: Все задачи › Запросить новый сертификат. Укажите шаблон ***Контроллер домена*** *(Domain Controller) и нажмите Заявка (Enroll).*



Сертификат контроллера домена будет помещен в хранилище сертификатов локального компьютера в папку Личное.

6. Сетевой ответчик

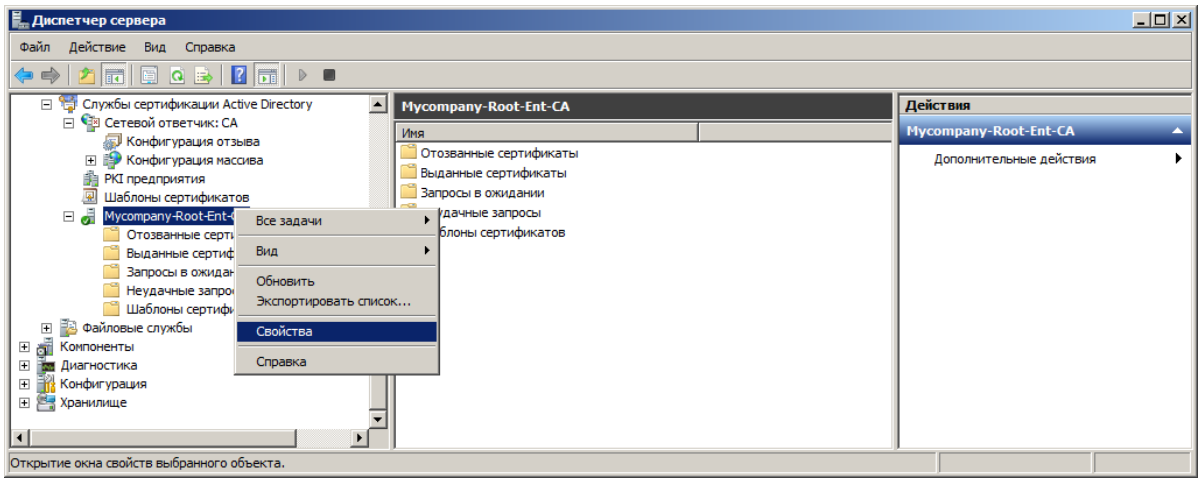
Для проверки действительности сертификатов помимо базового и разностного списка отозванных сертификатов (Base и Delta CRL соответственно) может использоваться проверка по протоколу OCSP (RFC 2560). Проверка сертификатов по протоколу OSCP реализована в Windows, начиная с Windows Server 2008 (для серверной части, называемой Online Responder , т.е. сетевой ответчик) и Windows Vista (для клиентской части).

Для проверки сертификата клиент по протоколу http или https передает специально сформированный запрос на соответствующий сервер – сетевой ответчик. Адрес для передачи запроса указан в сертификате там же, где адрес публикации списков отозванных сертификатов. Сетевой ответчик получает запрос и передает подписанный ответ клиенту по http или https.

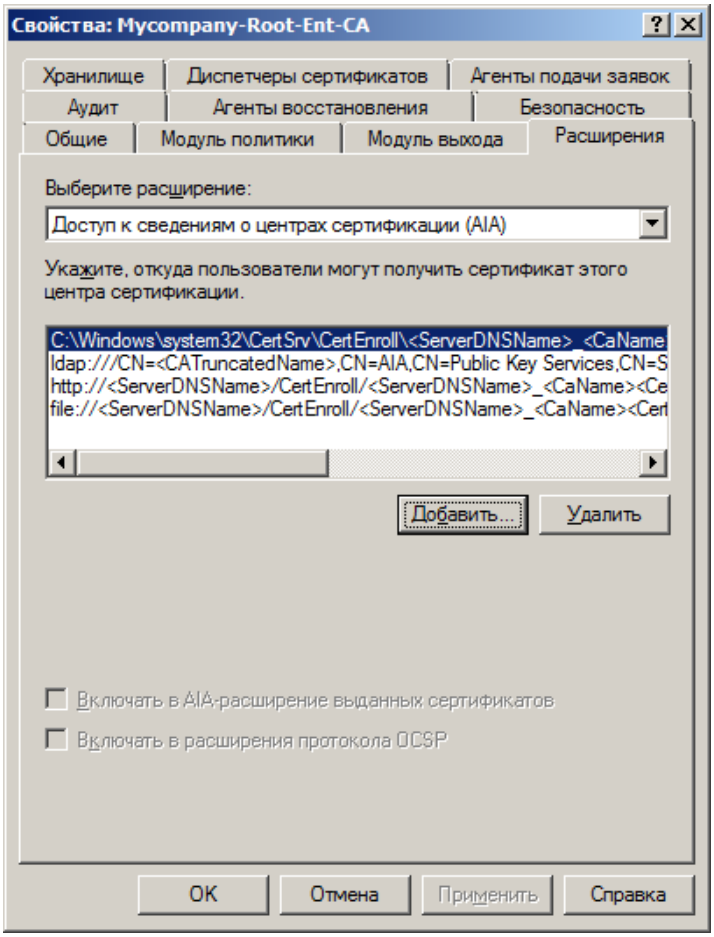
В отличие от списков отозванных сертификатов клиентская операционная система не скачивает файл со списком всех сертификатов, которые когда-либо были отозваны, а делает только один конкретный запрос.

Установите службу роли центра сертификации Сетевой ответчик (Online Responder) на одном из серверов. В данном примере роль была установлена одновременно с центром сертификации. Однако, Microsoft не рекомендует устанавливать сетевой ответчик на сервер центра сертификации.

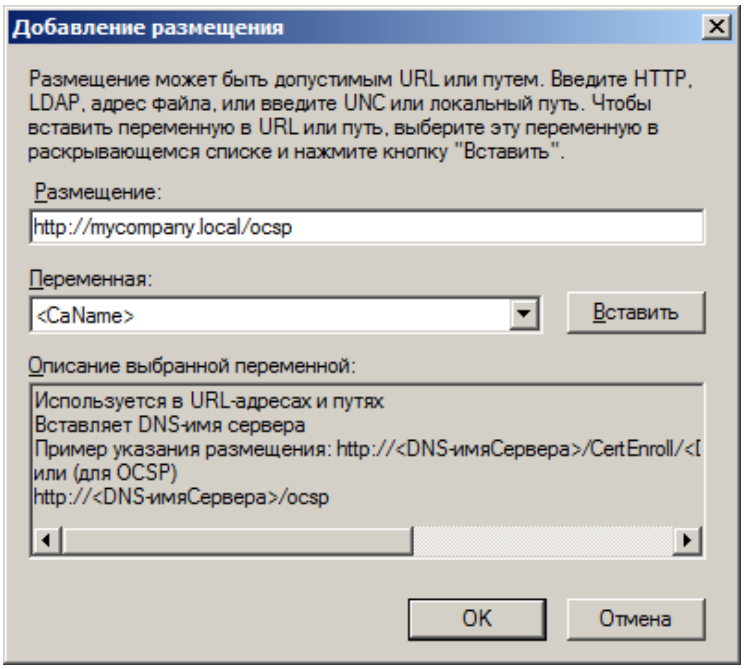
*Чтобы адрес URL службы Online Responder включался в сертификаты, его необходимо добавить в раздел AIA На сервере ЦС в диспетчере сервера откройте **Службы сертификации Active Directory** (Active Directory Certificate Services) и в контекстном меню сервера ЦС выберите **Свойства** (Properties).*



Адрес службы Сетевого ответчика (Online Responder) включают в раздел AIA во вкладке Расширения (Extensions).

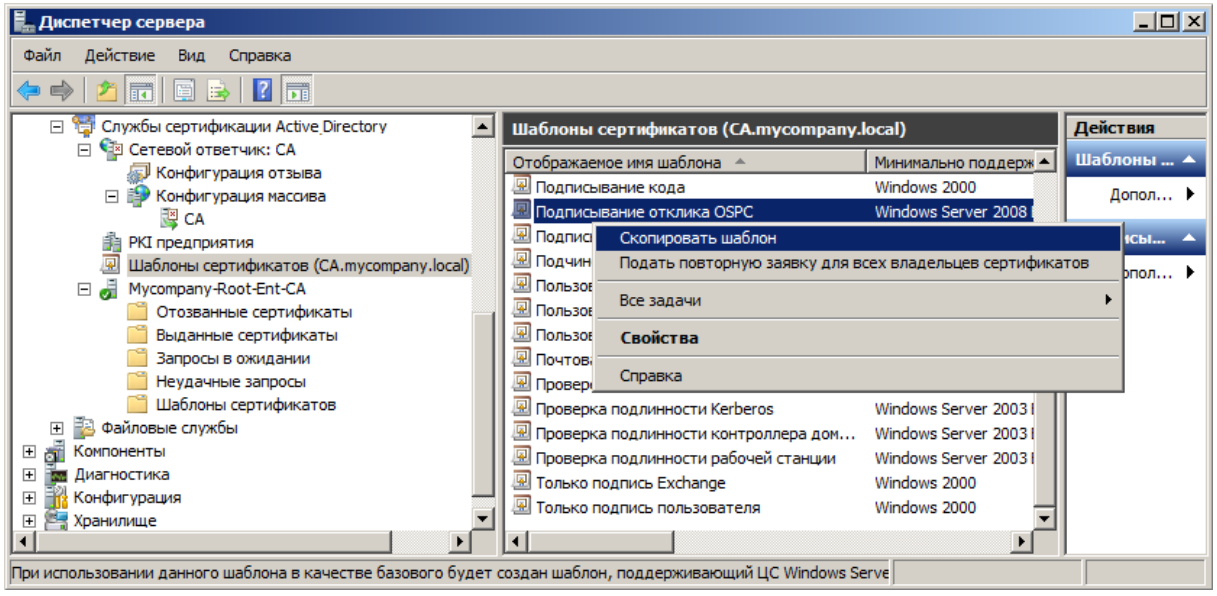


Добавляем адрес планируемого сетевого ответчика. В данном случае сетевой ответчик находится на том же сервере, что и веб-интерфейс центра сертификации.

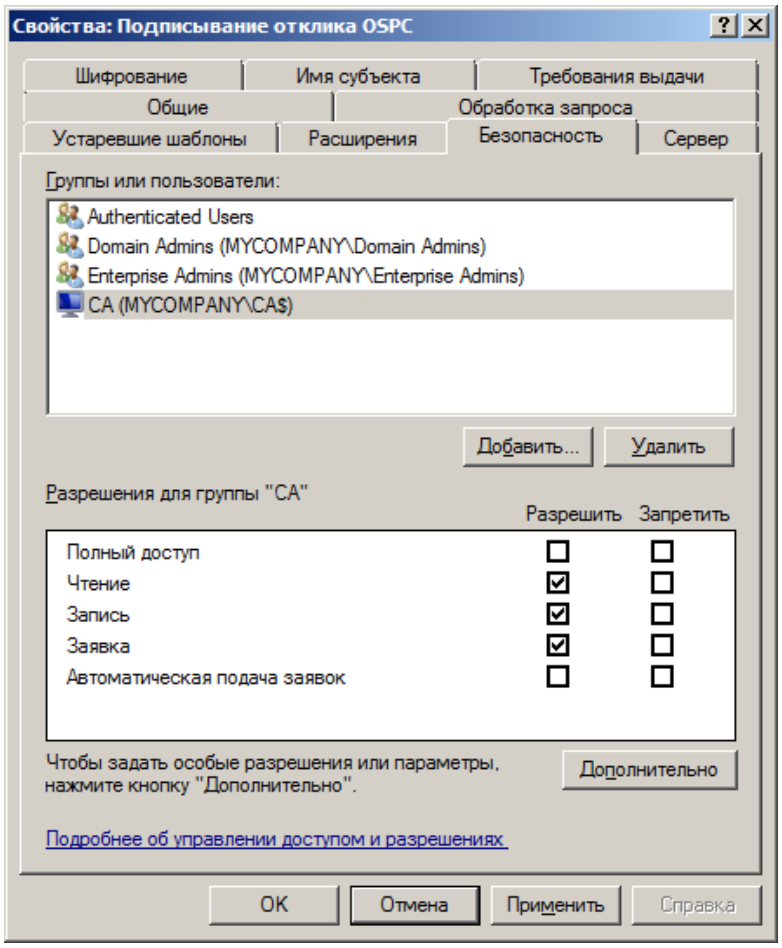


Для добавленного адреса отметьте: ***Включать в расширения протокола OCSP***

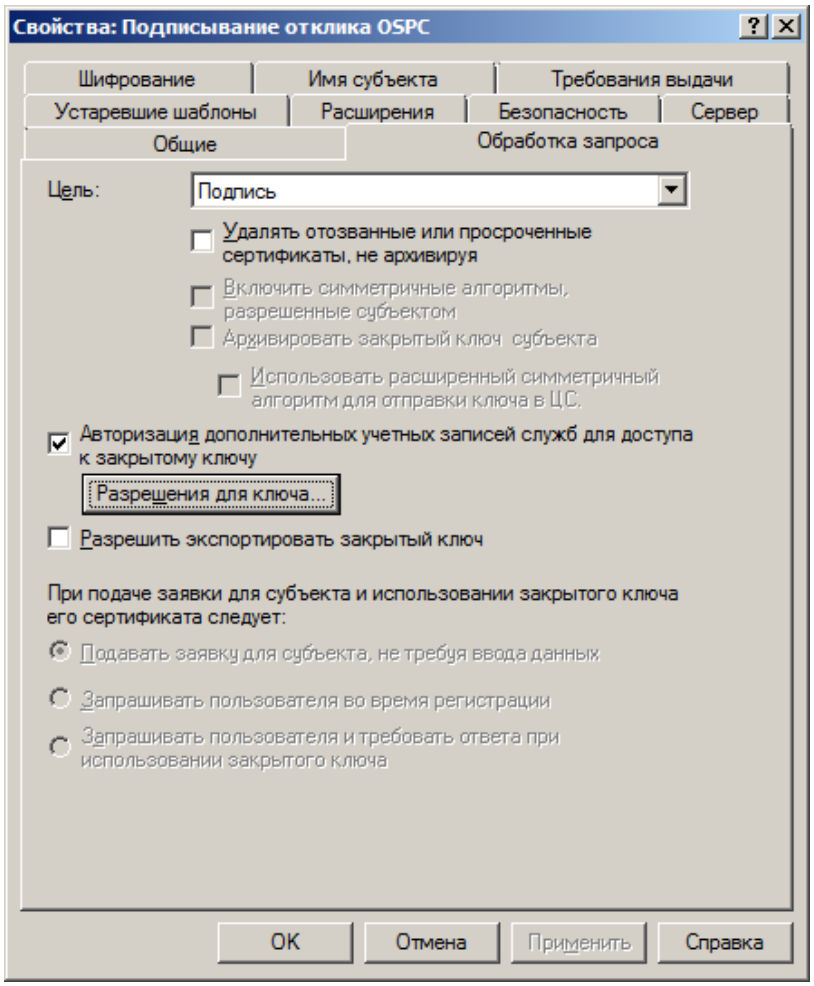
На сервере ЦС выпишите сертификат по шаблону ***Подписывание отклика OCSP*** *(OCSP Response Signing). Создайте новый шаблон, нажав* ***Скопировать шаблон*** *(Duplicate template) в списке шаблонов сервера или измените параметры самого шаблона, выбрав в контекстном меню* ***Свойства*** *(Properties).*



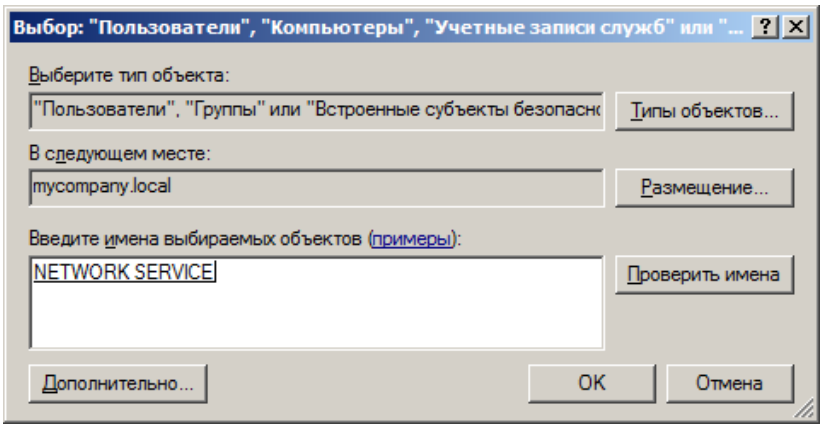
Во вкладке безопасность выдайте права на работу с шаблоном учетной записи сервера, на котором находится сетевой ответчик. Отметьте опции: ***чтение, запись, заявка*** *(Read, Write, Enroll). Не отмечайте* ***Автоматическая подача заявок*** *(Autoenrollment).*

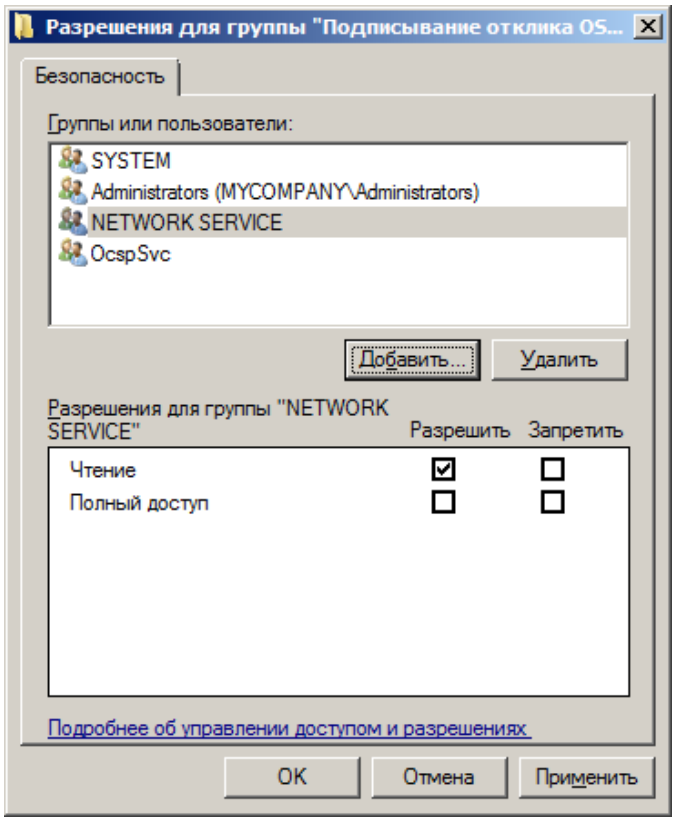


*Во вкладке **Обработка запроса** (Request Handling) Выберите **Разрешения для ключа** (Key Permissions).*

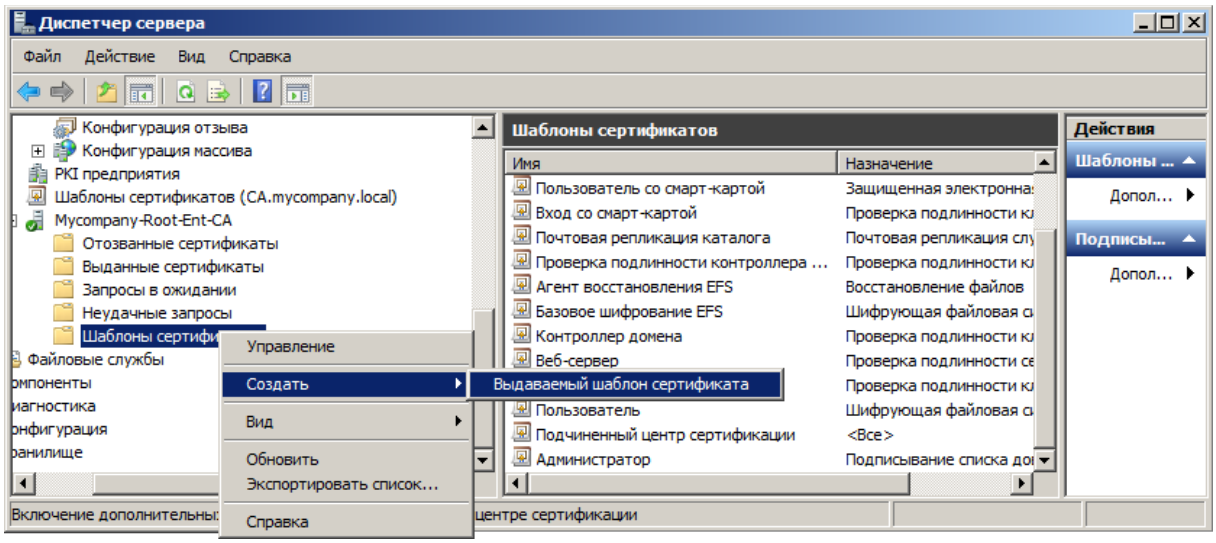


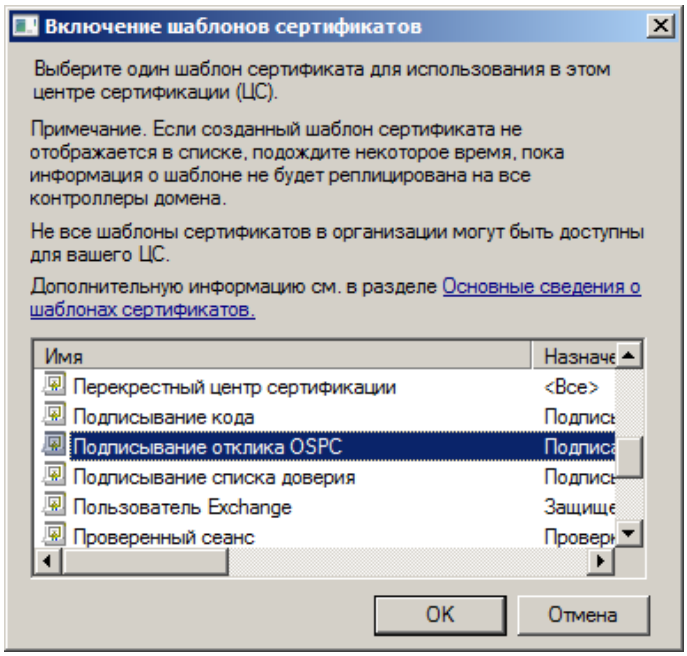
Добавьте права на чтение закрытого ключа службе Network Service, под которой запускается служба сетевого ответчика.





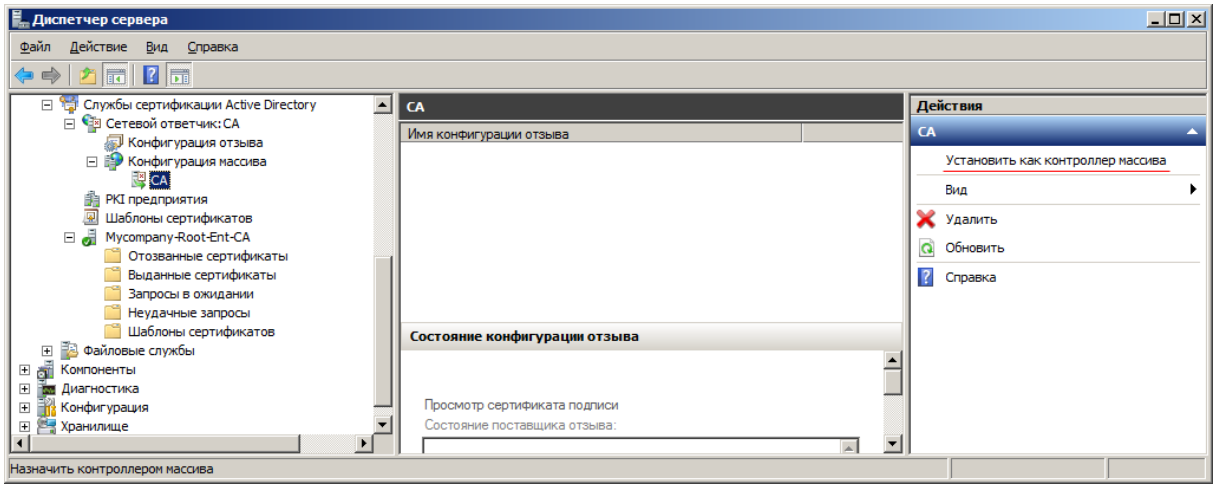
Работа с шаблоном завершена. Выпишите шаблон для использования в выбранном центре сертификации.





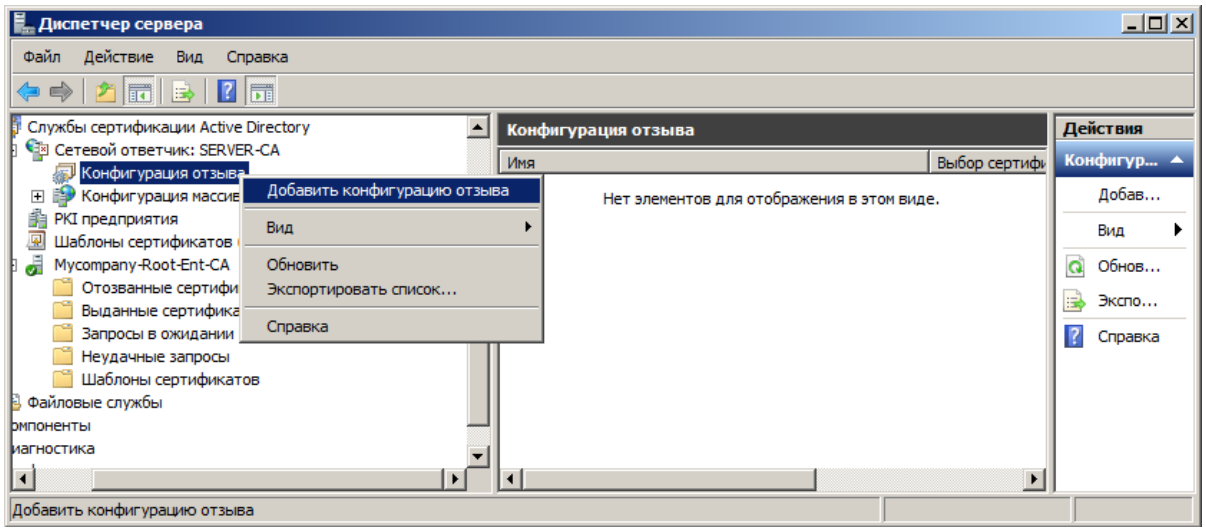
На сервере сетевого ответчика выпишите сертификат через консоль mmc с оснасткой ***Сертификаты › Локальный компьютер****.*

Назначьте один из сетевых ответчиков контроллером массива, даже если предусмотрен только один сетевой ответчик.

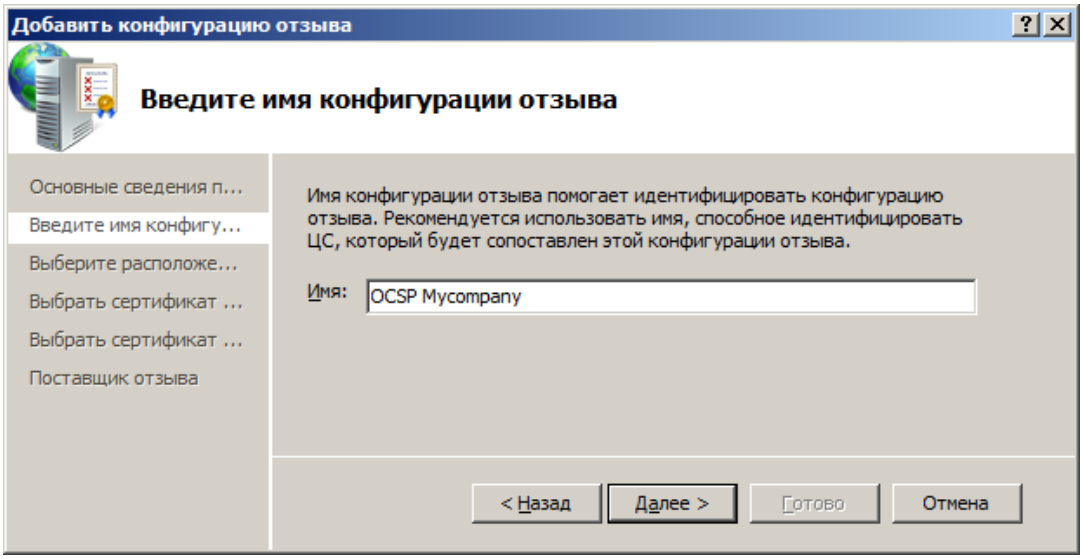


Выберите сервер и нажмите в меню справа или в контекстном меню ***Установить как контроллер массива*** *(Assign as Array Controller).*

Создайте конфигурацию отзыва, т.е. набор параметров, определяющих работу сетевого ответчика.

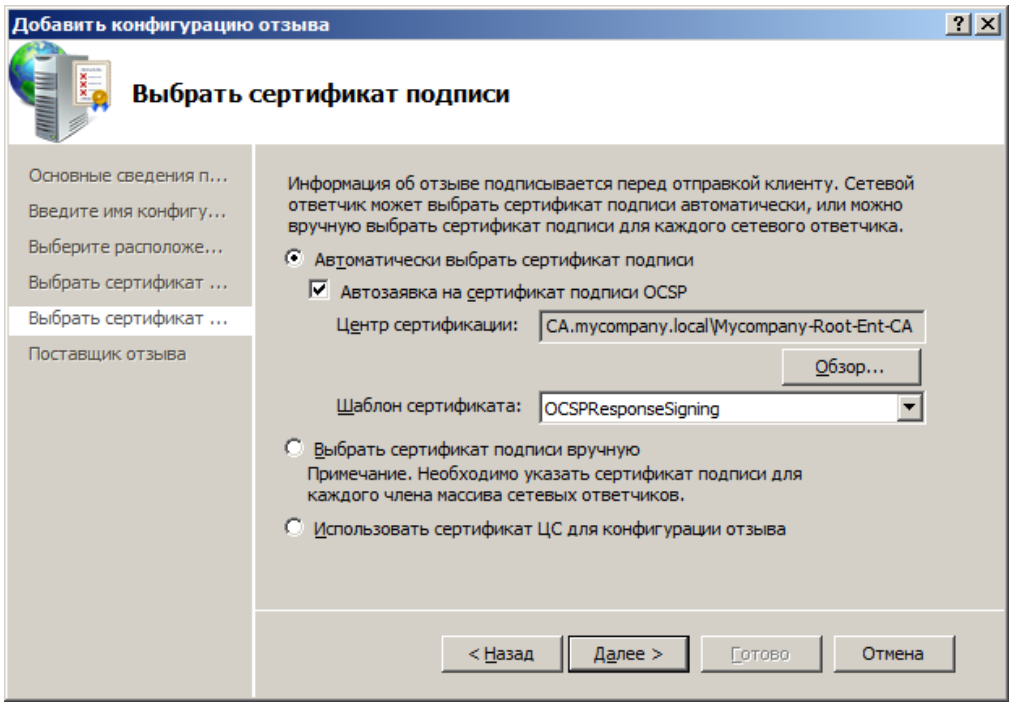


Заполните поля, требуемые мастером создания конфигурации. Введите имя конфигурации.

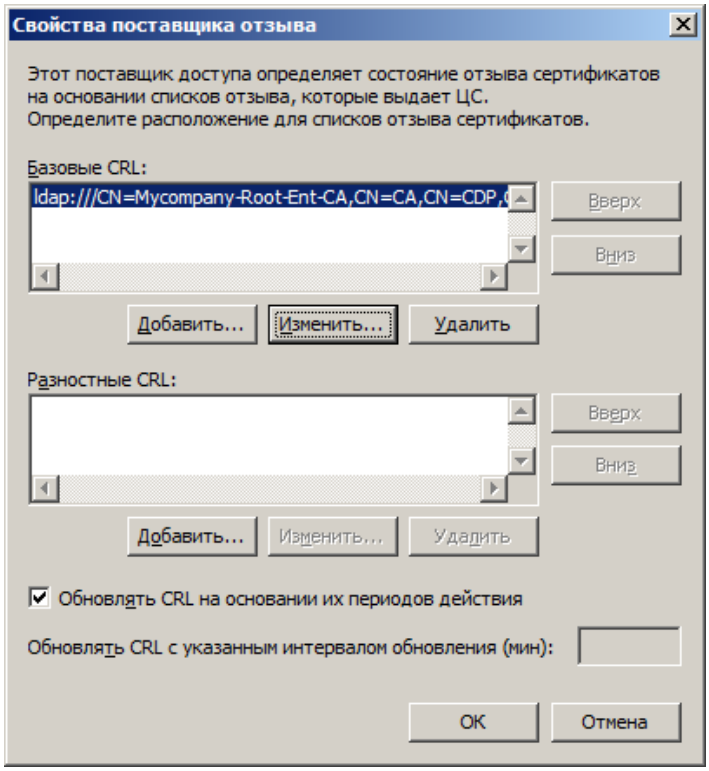


Укажите сертификат центра сертификации и сертификат подписи отклика OCSP.

*Рекомендуется отметить опцию **Автозаявка** на сертификат подписи OCSP, т.к. данный тип сертификата имеет достаточно короткий период действия и обновлять его вручную нецелесообразно.*

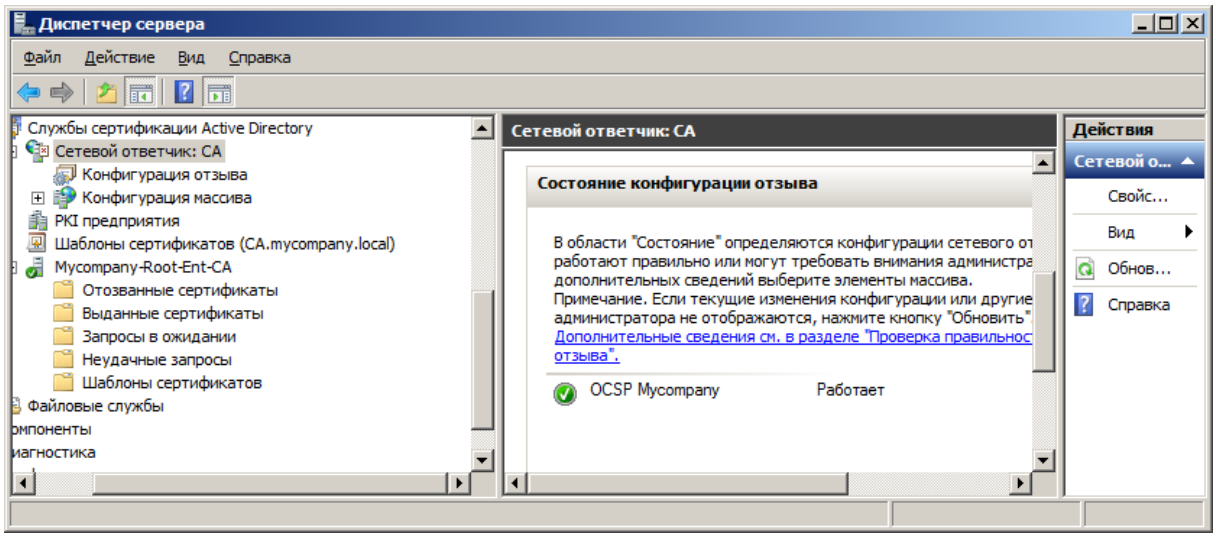


При выборе поставщика отзыва указываются файлы базового и разностного списков отозванных сертификатов (Base и Delta CRL). Данные берутся из настроек центра сертификации. При необходимости добавьте дополнительные адреса.



Завершите работу мастера создания конфигурации.

Проверьте состояние конфигурации в диспетчере сервера.

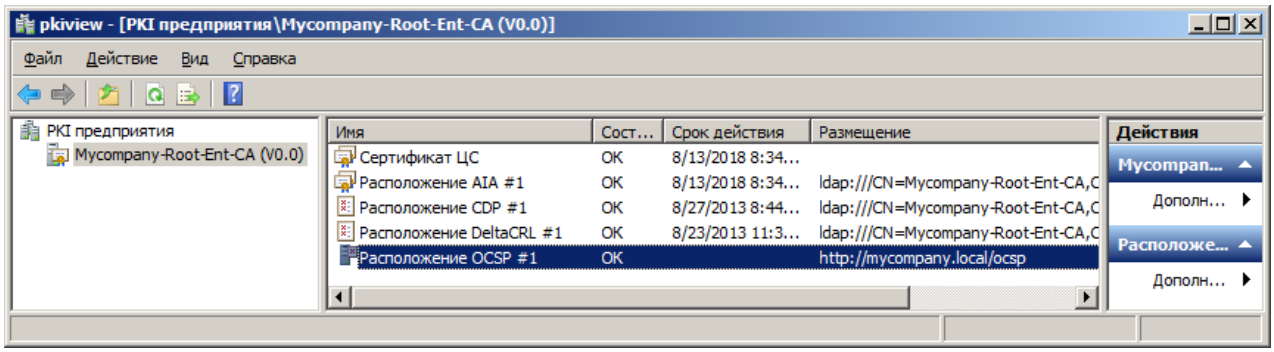


От администратора выполните в командной строке:

```
certutil -pulse
```

Перезагрузите сервер ЦС и сервер сетевого ответчика.

Для дополнительной проверки работоспособности сетевого ответчика откройте консоль pkiview.msc.



Если расположение сетевого ответчика OCSP в информации AIA менялось, отзовите сертификат или сертификаты Обмен ЦС (CA Exchange) и перезагрузите сервер центра сертификации. Новый сертификат Обмен ЦС (CA Exchange) будет выписан автоматически. Повторите проверку.

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.*

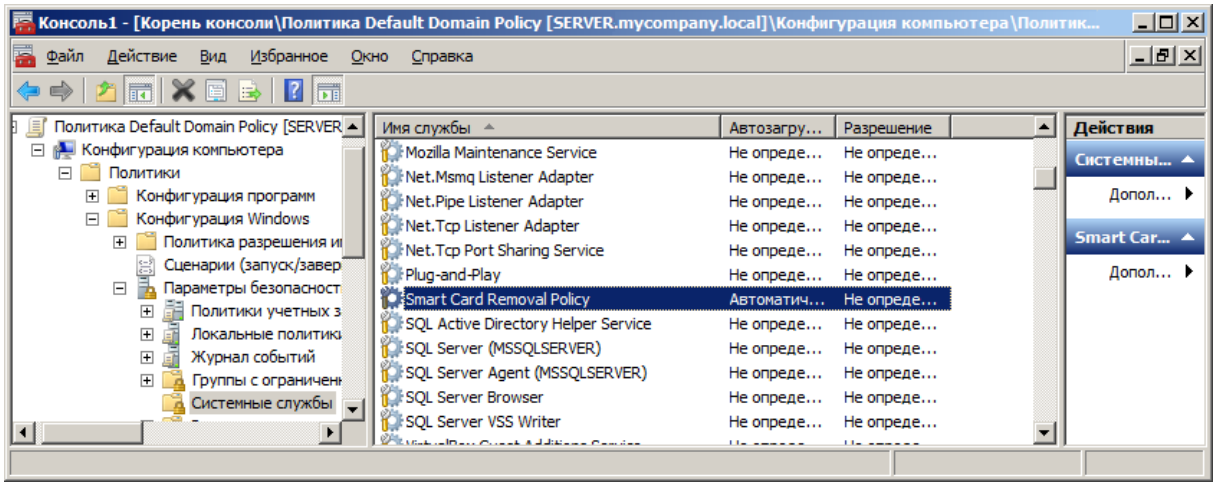
*Чтобы операционная система могла заблокировать рабочую станцию при извлечении ESMART token, необходимо запустить службу **Smartcard Removal Policy** – Политика удаления смарт-карт (SCPolicySVC). В ОС Windows XP служба запущена по умолчанию, а в ОС Windows Vista и выше служба по умолчанию отключена.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

*На контроллере домена откройте консоль MMC. Добавьте оснастку **Редактор управления групповыми политиками** (Group Policy Management Editor) › **Default Domain Policy** (или собственную доменную политику).*

Чтобы служба запускалась автоматически на всех рабочих станциях в домене, откройте в редакторе доменной групповой политики:

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

*Выставите значение **Политика удаления смарт-карты – автоматически** (Smart Card Removal Policy – Automatic).*

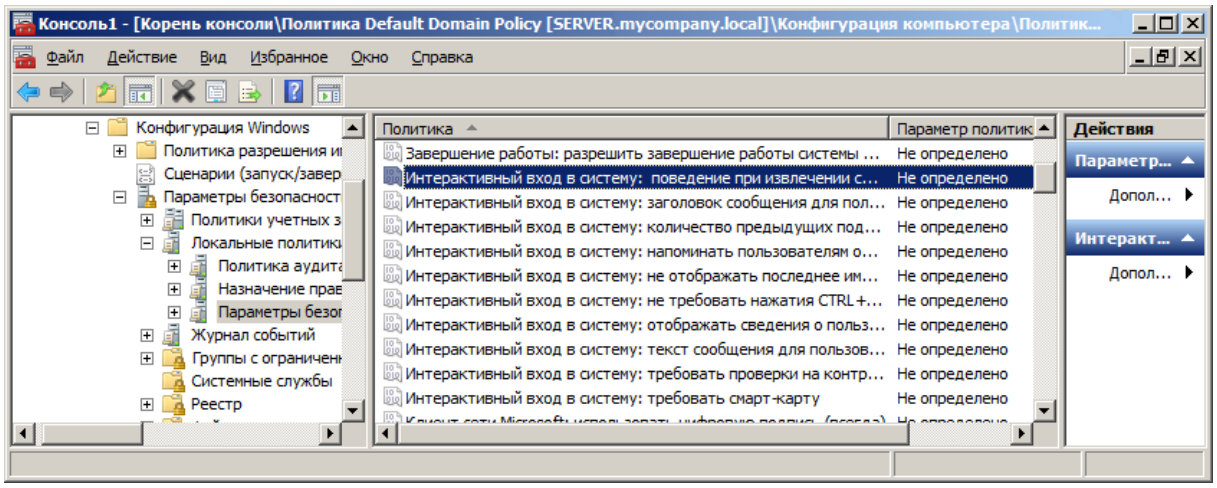


В той же консоли перейдите к разделу:

> *Локальные политики › Параметры безопасности*
>
> *Local Policies › Security Options*

В соответствии с корпоративными требованиями задайте значения для параметров:

> ***Интерактивный вход в систему: Требовать смарт-карту***
>
> *(Interactive Logon: Require smartcard)*
>
> ***Интерактивный вход в систему: Поведение при извлечении смарт-карты***
>
> *(Interactive Logon: Smartcard removal behavior)*



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.*

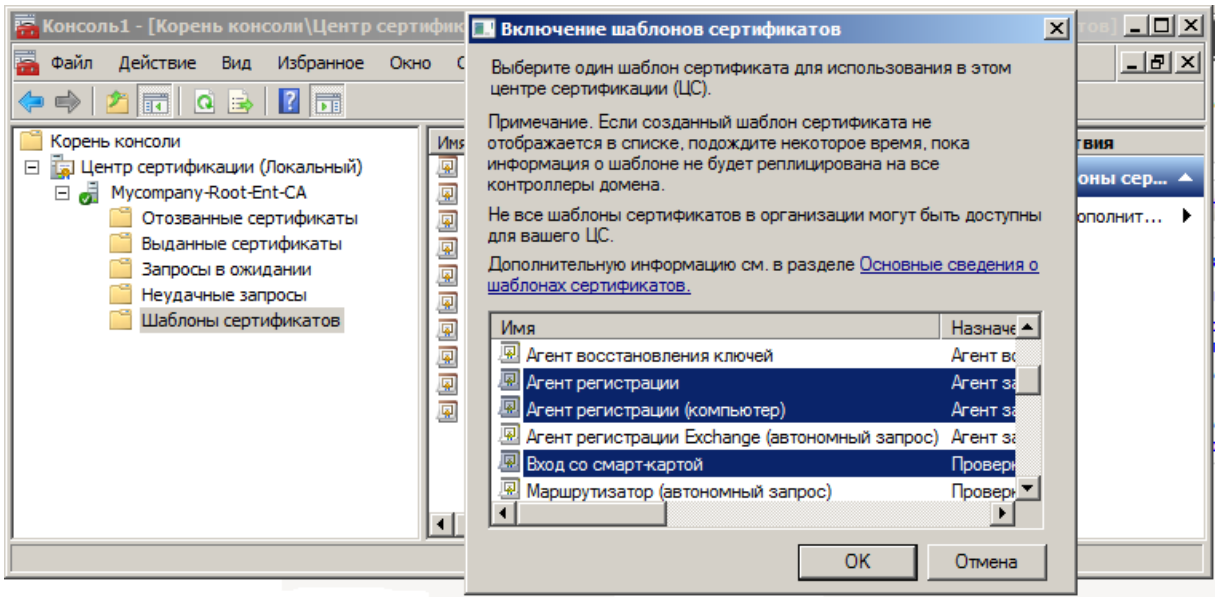
Проверьте настройки. Обновите групповые политики и перезагрузите сервер.

8. Шаблоны сертификатов

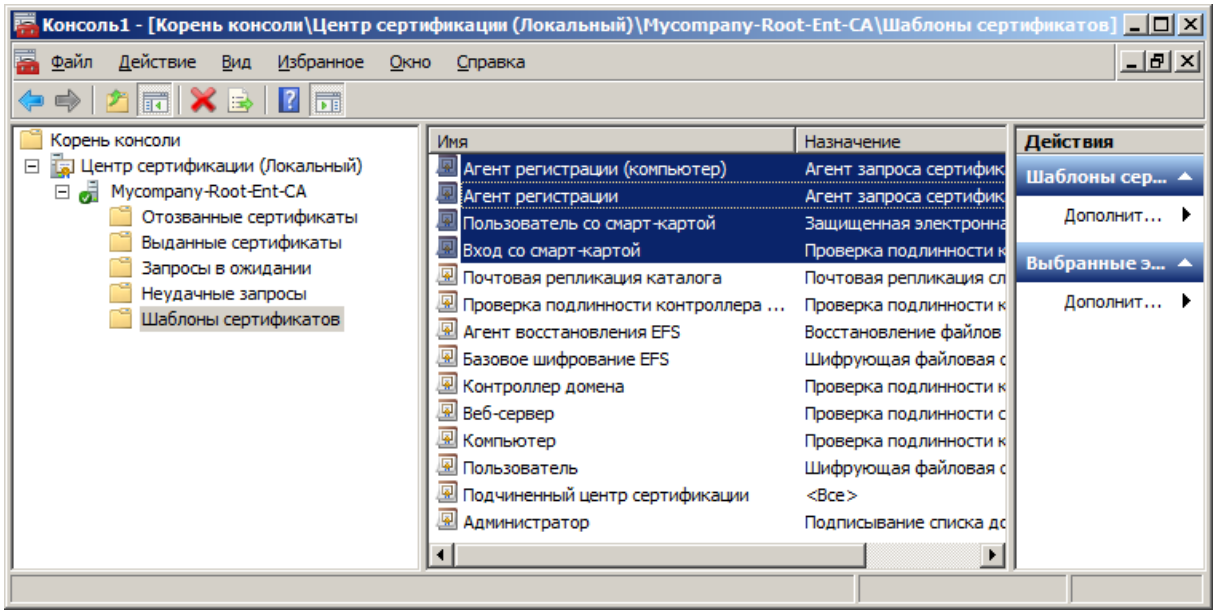
Для работы со смарт-картами требуются сертификаты на базе шаблонов, не доступных по умолчанию. На сервере центра сертификации добавьте оснастку – ***Certificate Authority (Local)****. В домене выберите раздел* ***Certificate templates****. В контекстном меню раздела выберите* ***Certificate templates to issue****.*

Удерживая CTRL, выделите:

- ***Агент регистрации*** *– Enrollment agent);*
- ***Агент регистрации (компьютер)*** *– Enrollment agent (Computer);*
- ***Пользователь со смарт-картой*** *– Smart Card User;*
- ***Вход со смарт-картой*** *– Smart Card Logon.*



В списке появятся добавленные роли:



Расширить функционал возможностей корпоративного центра сертификации помогают также нестандартные шаблоны сертификатов.

8.1 Создание новых шаблонов сертификатов

Преимуществом использование сертификатов, выпущенных собственным корпоративным ЦС на Windows Server[4], является их гибкость и возможность вносить модификации в стандартные шаблоны. Шаблоны сертификатов позволяют не вводить данные пользователя и опции в виде запроса CSR для каждого отдельного сертификата, а использовать предварительно настроенные шаблоны и данные пользователей из Active Directory.

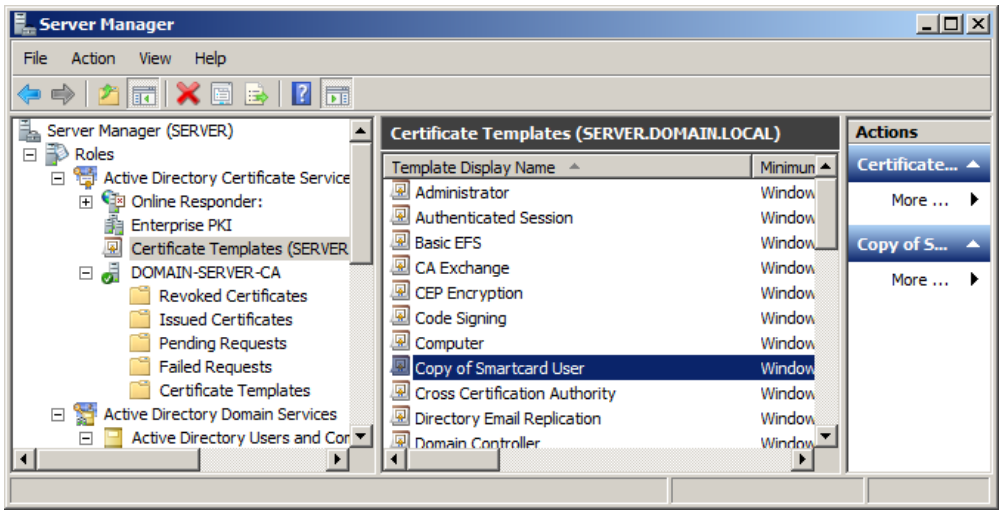
*В приведенном ниже примере мы добавляем в стандартный шаблон **Пользователь со смарт-картой** (Smartcard User) дополнительную опцию – EFS шифрование. Таким образом, пользователь сможет шифровать файлы EFS тем же сертификатом (закрытым ключом), что и осуществлять вход в систему.*

Данный пример не является рекомендуемым, а приведен исключительно для демонстрации возможностей изменения шаблонов сертификатов.

8.2 Пример создания шаблона

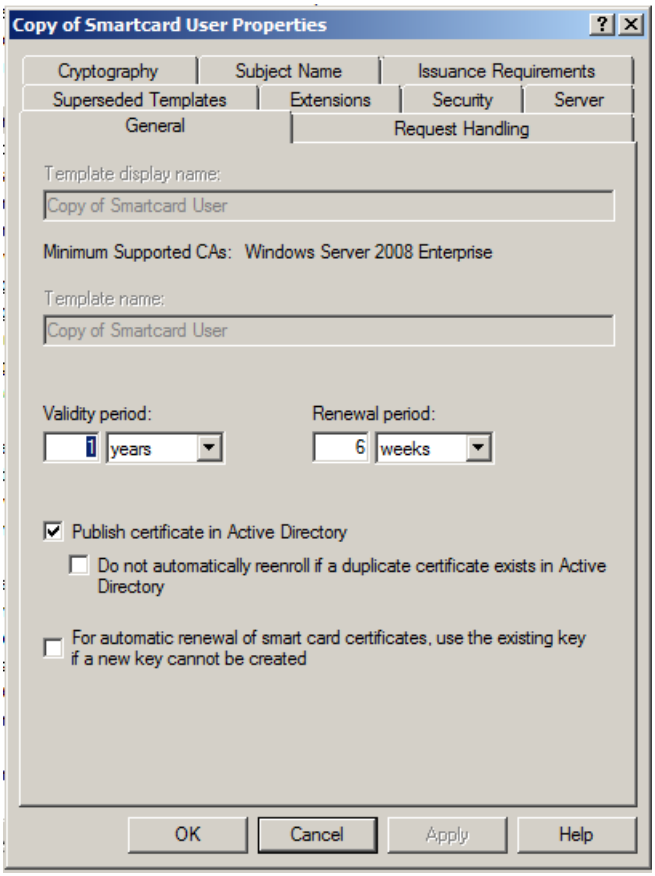
*Зайдите на сервер, на котором установлен ЦС, под учетной записью администратора. Раскройте раздел **Certificate Templates** для всего ЦС. В контекстном меню нужного шаблона выберите **Duplicate Template** (Дублировать шаблон). Исходные шаблоны редактировать не рекомендуется.*

4 Шаблоны используются только для ЦС типа Enterprise. ЦС типа Standalone не используют шаблоны и данные из Active Directory.



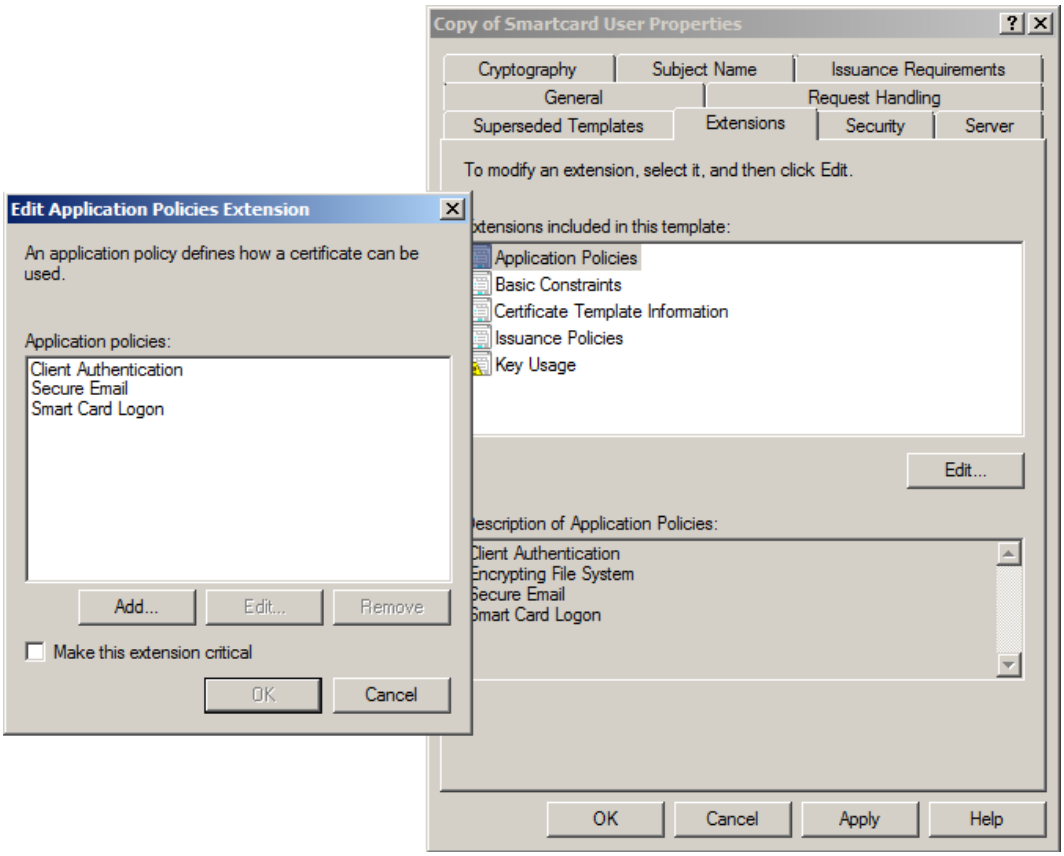
Откройте свойства нового шаблона (в примере рассмотрены не все опции шаблона).

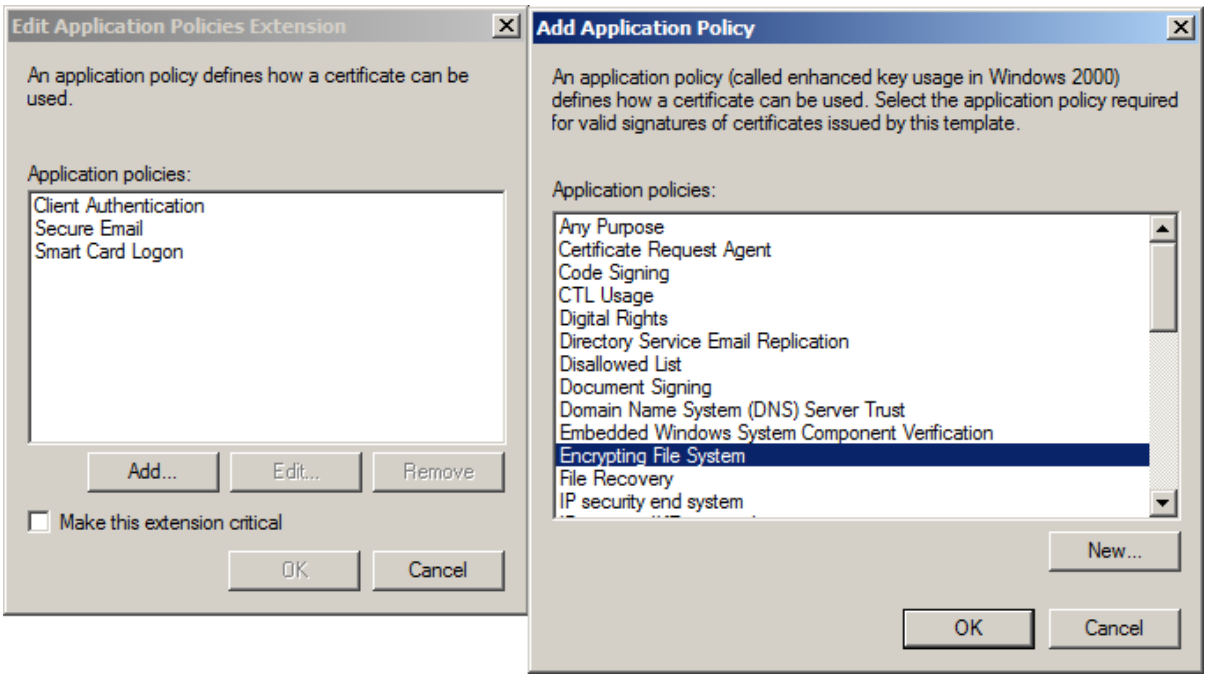
Во вкладке General (Общие) можно изменить срок, на который выдается сертификат.



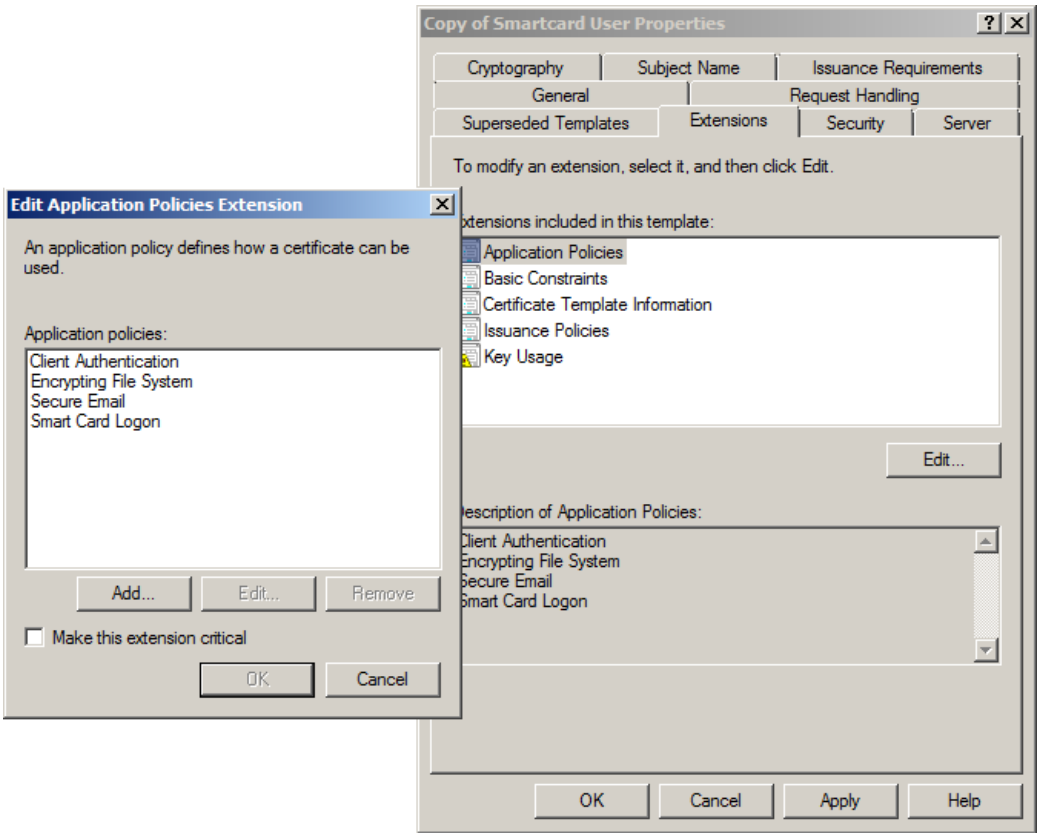
Перейдите на вкладку Extensions (Расширения), чтобы изменить способы использования сертификата. В качестве примера добавлена возможность EFS-шифрования. Выберите в окне Application policies и нажмите ***Edit*** *(Редактировать).*

В первом окне нажмите ***Add*** *(Добавить) и укажите требуемые опции из списка или создайте новые.*



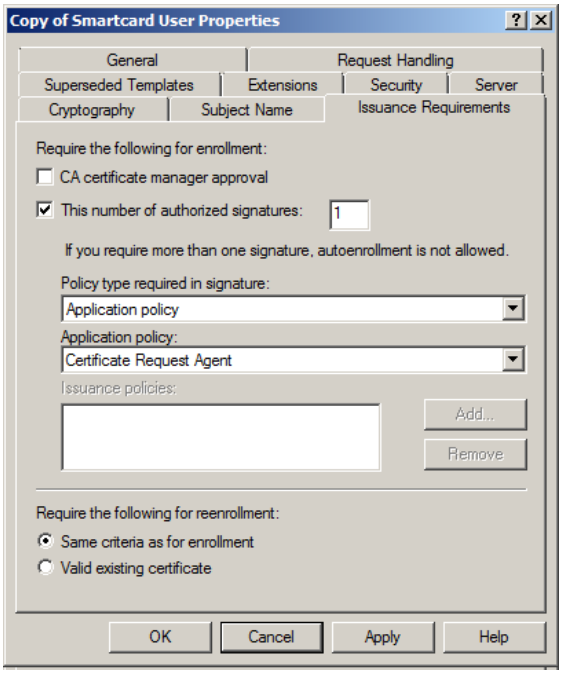


Сохраните изменения. В списке Application Policies появилась опция Encrypting File System.



*Во вкладке **Cryptography** настраивается тип и длина ключей, а также криптопровайдер, используемый по умолчанию. Задайте алгоритм RSA и выберите длину ключевой пары в соответствии с корпоративными требованиями.*

В качестве провайдера по умолчанию укажите Microsoft Base Smart Card Cryptoprovider. Таким образом, для ESMART Token не нужно будет каждый раз указывать криптопровайдер при выдаче сертификата по данному шаблону.

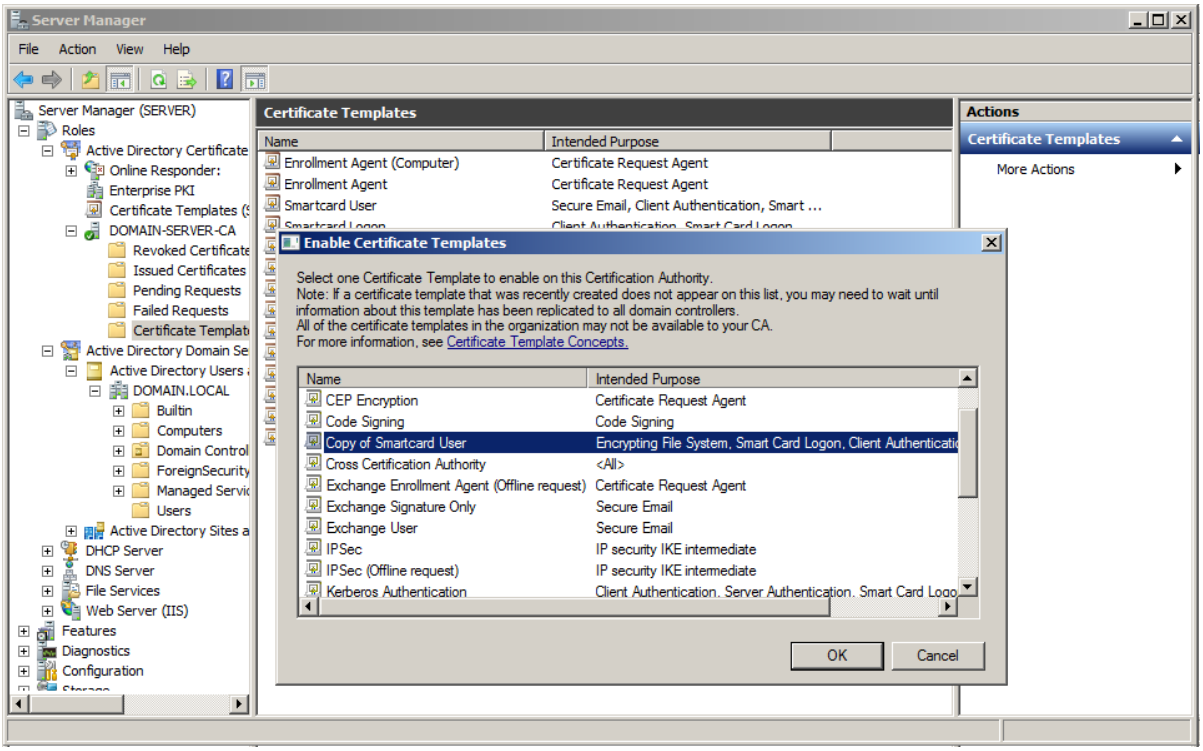


*Следующая настройка очень важна. Чтобы администратор (Enrollment Agent) мог запрашивать сертификаты для других пользователей, необходимо убедиться, что в новом шаблоне во вкладке **Issuance Requirements** (Требования к выдаче) были выставлены следующие настройки:*

*The number of requested signatures = **1** (значение по умолчанию 0)*
Policy type, required in signature = Application Policy.
*Application Policy = **Certificate request Agent**.*

В противном случае, новый шаблон может быть недоступен при запросе сертификата администратором.

*Шаблон сертификата теперь нужно опубликовать в данном домене. Для этого в Server Manager перейдите в раздел Certificate Templates для выбранного домена. В контекстном меню раздела выберите **New › Certificates Template to Issue** (Новые › Выписать шаблон сертификата). Выберите отредактированный на предыдущем этапе шаблон и нажмите OK. Шаблон появится в списке.*

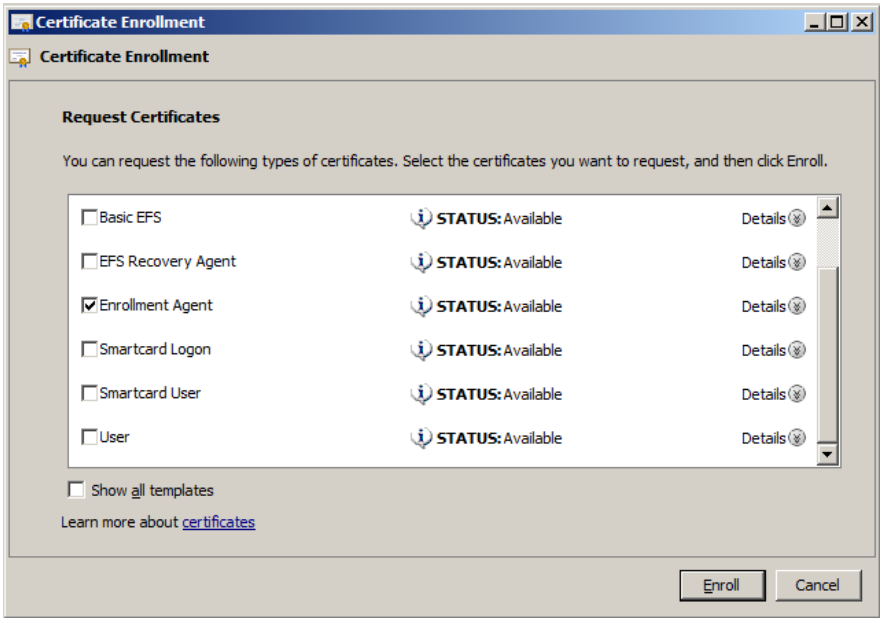


*Выдайте сертификаты пользователям, как показано в разделе **10 Запрос сертификатов пользователей и запись на смарт-карту**.*

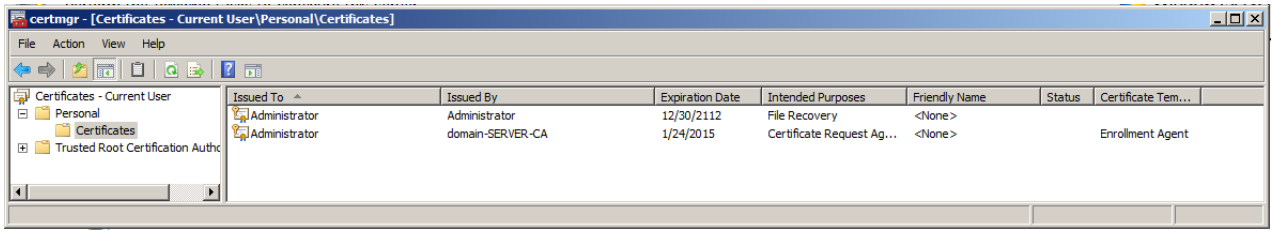
9. Запрос сертификата типа Enrollment Agent

*Войдите на сервер с ЦС как Администратор домена. Откройте оснастку сертификатов **certmgr.msc** для локального пользователя, раздел **Personal** (Личные).*

*В контекстном меню выберите **All tasks – Request new certificate** (Все задачи – Запросить новый сертификат). Оставьте значение для Enrollment Policy по умолчанию, нажмите **Next**. На следующем экране отметьте Enrollment Agent и нажмите **Enroll** (Запросить).*



У администратора появился новый сертификат Enrollment Agent.



10. Запрос сертификатов пользователей и запись на смарт-карту

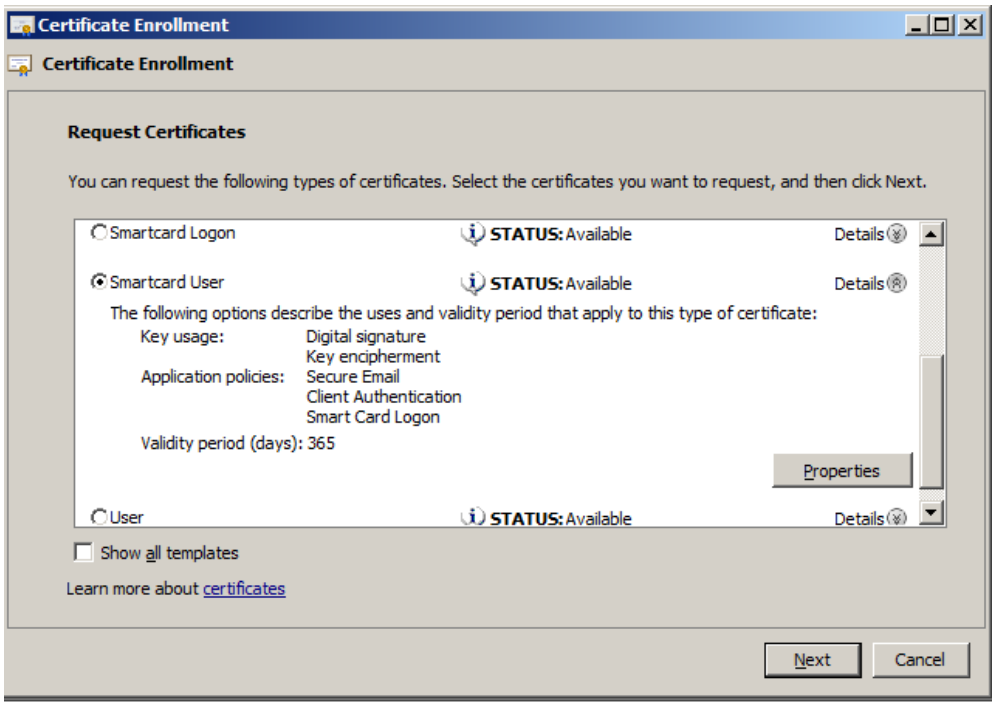
Запрос сертификатов пользователей в Windows Server 2003 выполняется через Internet Explorer. Подробно процедура описана в руководстве Развертывание центра сертификации Windows Server 2003.

Войдите на сервер с ЦС как Администратор домена, для которого на предыдущем этапе был выписан сертификат Enrollment Agent.

*В консоли **certmgr.msc** в разделе Personal в контекстном меню выберите: **All tasks – Advanced operations – Enroll on behalf of...** Нажмите **Next** (Далее) в окне приветствия. Оставьте по умолчанию значение в следующем окне (Enrollment Policy). Нажмите **Next**.*

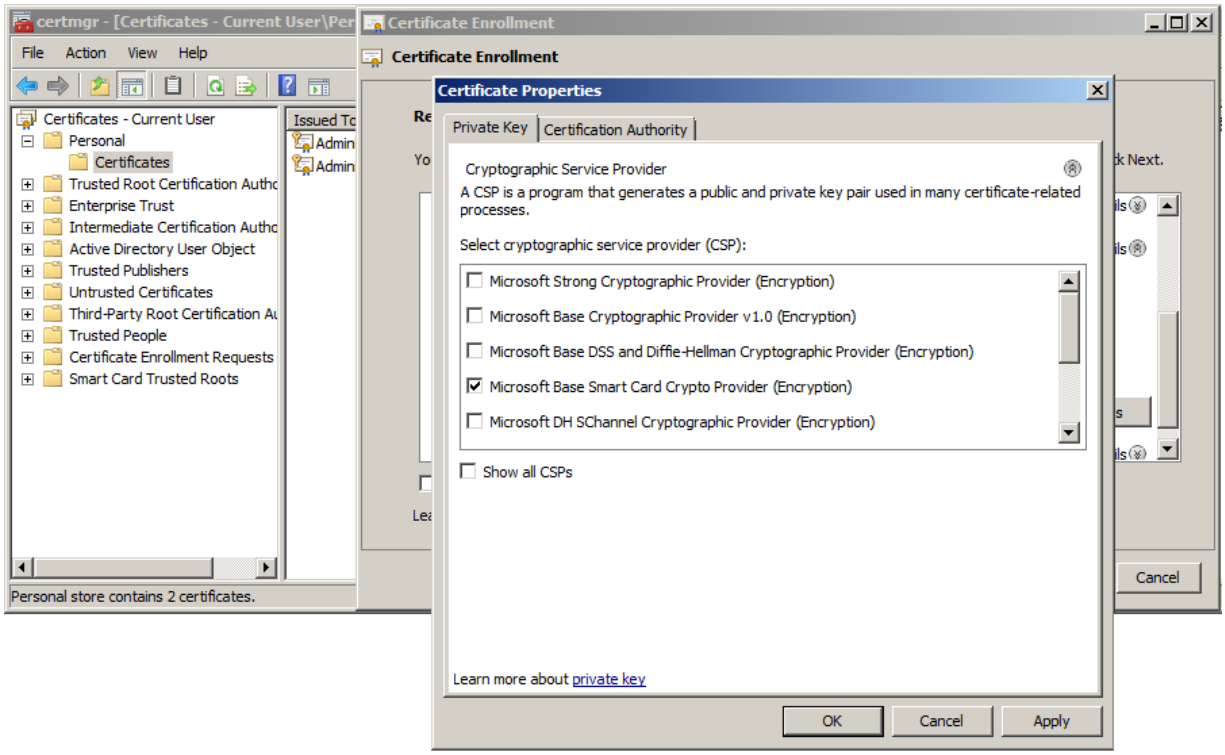
*Нажмите **Browse** (Обзор) и выберите сертификат администратора с функцией Enrollment agent. Нажмите **Next** (Далее).*

*В следующем окне выберите шаблона сертификата, который будет выписан для пользователя, например, **Smart Card User** (Пользователь со смарт-картой). В списке также могут появиться новые шаблоны, созданные специально для данного ЦС. См. раздел Создание новых шаблонов. Нажмите на стрелочку рядом со словом **Details** (Подробно), чтобы развернуть опции шаблона. Нажмите кнопку **Properties** (Свойства) справа.*



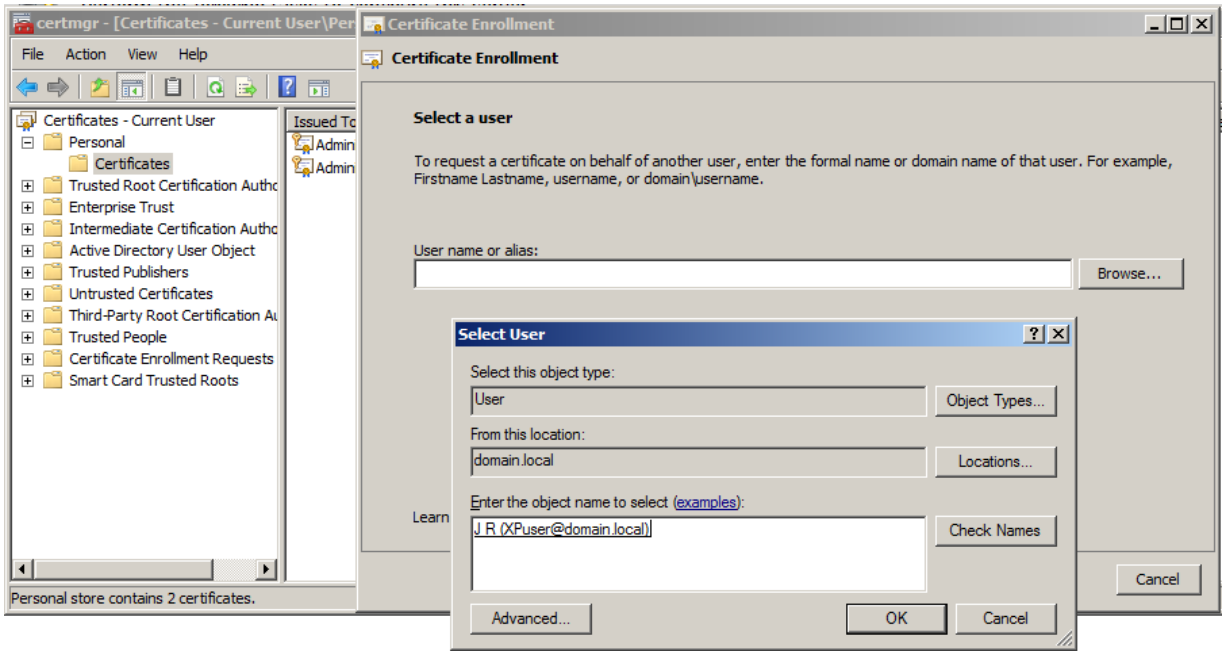
*Во вкладке **Private key** (Закрытый ключ) разверните Cryptographic Service Provider, нажав на двойную стрелочку справа.*

В списке отметьте – Microsoft Base Smart Card Cryptoprovider (Encryption). Нажмите OK.



*Окно со свойствами закроется. Нажмите **Next** в окне выбора шаблона сертификата клиента.*

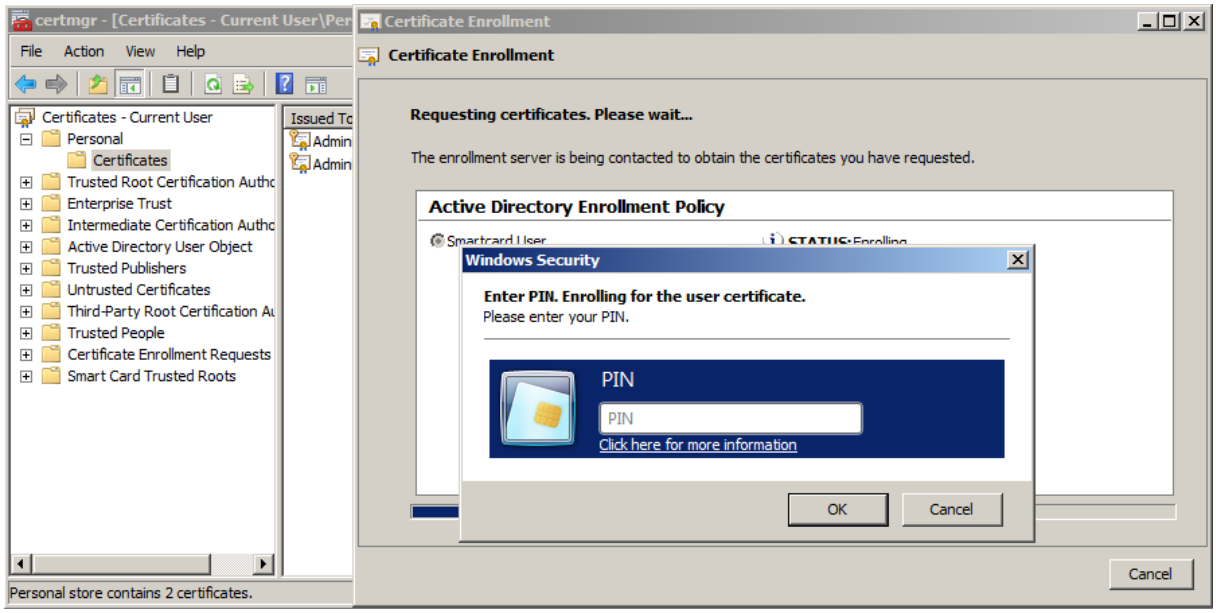
*Выберите пользователя, для которого будет выписан сертификат. Для этого, нажмите **Browse** (Обзор), затем введите часть имени пользователя и нажмите **Check names** (Проверить имена). Выберите нужного пользователя.*



*Нажмите OK, потом **Enroll** (Подать заявку).*

Вставьте смарт-карту. Если карта была вставлена раньше, возможно придется вынуть ее и вставить еще раз, когда появится сообщение, что карта не вставлена.

Введите ПИН-код пользователя карты. Не вынимайте карту до того, как появится сообщение об успешном завершении операции.



*Сертификат и ключевая пара записаны на карту. Чтобы выдать сертификат следующему пользователю, нажмите **Another User.***

11. Подготовка компьютеров пользователей

Установите на каждый компьютер клиента пакет ESMART PKI Client. Рекомендуется установка с помощью программы-инсталлятора. Подробно установка описана в руководстве администратора ESMART PKI Client. При установке ESMART PKI Client через групповые политики необходимо добавить сертификат ISBC, которым подписан дистрибутив, в раздел ***Доверенные издатели*** *в хранилище сертификатов.*

Компьютеры пользователей должны быть введены в домен. Создайте пользователей и заполните данные в их учетных карточках в соответствии с корпоративными требованиями.

Если не использовались доменные групповые политики, настройте локальные групповые политики или параметры реестра. См. руководство ***ESMART Token – Авторизация в домене Windows****.*

Если не использовались доменные групповые политики, добавьте корневой сертификат CA в хранилище сертификатов Windows. Для этого откройте консоль ***certmgr.msc*** *– Доверительные корневые центры сертификации. Дополнительно, можно добавить корневой сертификат в хранилище для локального компьютера (если на одном ПК используются несколько учетных записей пользователей) – консоль MMC с оснасткой – Сертификаты (Локальный компьютер) – Доверительные корневые центры сертификации.*

Можно завершить сеанс текущего пользователя и авторизоваться по сертификату.