

Развертывание центра сертификации на базе Windows Server 2008



Содержание

| 1. | Введение | |
|-----|--|---|
| 1.1 | Центры сертификации | 3 |
| 1.2 | Планирование инфраструктуры | 3 |
| 1.3 | Примеры иерархии РКІ | 4 |
| 2. | Установка ESMART PKI Client | 6 |
| 3. | Установка IIS Сервера | 6 |
| 4. | Добавление контроллера домена в группу CERTSVC_DCOM_ACCESS | 6 |
| 5. | Настройка центра сертификации | 7 |
| 5.1 | Добавление роли | 7 |
| 5.2 | Веб-интерфейс центра сертификации | |
| 5.3 | Использование веб-интерфейса | |
| 5.4 | Установка корневого сертификата вручную | |
| 5.5 | Распространение сертификата через групповые политики | |
| 5.6 | Сертификат контроллера домена | |
| 6. | Сетевой ответчик | |
| 7. | Настройки безопасности | |
| 8. | Шаблоны сертификатов | |
| 8.1 | Создание новых шаблонов сертификатов | |
| 8.2 | Пример создания шаблона | |
| 9. | Запрос сертификата типа Enrollment Agent | |
| 10. | Запрос сертификатов пользователей и запись на смарт-карту | |
| 11. | Подготовка компьютеров пользователей | |
| | | |

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 РКІ 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 | Через web-интерфейс, консоль |
| | или через утилиту командной | ттс или через утилиту |
| | строки certreq.exe | 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;

² перевод термина Certification Authority соответствует текущей локализации OC Windows Server



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

- **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 структура³.

1.3 Примеры иерархии РКІ



Одноуровневая иерархия РКІ

В одноуровневой иерархии РКІ 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 РКІ

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.

| Выбор: "Группы" | ? × |
|---|-----------------------|
| <u>В</u> ыберите тип объекта: | |
| "Группы" или "Встроенные субъекты безопасности" | <u>Т</u> ипы объектов |
| В с <u>л</u> едующем месте: | |
| mycompany.local | <u>Р</u> азмещение |
| Введите <u>и</u> мена выбираемых объектов (<u>примеры)</u> : | |
| Certificate Service DCOM Access | Проверить имена |
| | |
| | |
| Дополнительно ОК | Отмена |



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.

| № Выбор службо ролей Ререда началом работы Ререда началом работы Ролков серера Службо ролей, устанавливаемые для роли сервера "Службы сертификации Астіче Понстолу". Службо ролей Вариант установки Службо регистрации в центре сертификации через Игт Службо регистрации на сетевых устройствах Веб-служба политик регистрации сертификатов | Мастер добавления ролей | × |
|---|--|---|
| Перед началом работы Роли сервера Службы сертификации АD Службы ролей Вариант установки Тил ЦС Закрытый ключ Шифрование Имя ЦС Срок действия Веб-служба регистрации на сетевых устройствах Веб-служба регистрации сертификатов Веб-служба регистрации сертификатов Веб-служба регистрации сертификатов | Выбор служб рол | іей |
| <u>Дополнительные сведения о служbax ролей</u> < <u>Н</u> азад Д <u>а</u> лее > Ус <u>т</u> ановить Отмена | 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 | Выберите службы ролей, устанавливаемые для роли сервера "Службы сертификации Active |

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 РКІ или не корневой ЦС в многоуровневом РКІ;
- Standalone (Автономный) если это корневой ЦС в многоуровневом РКІ.

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 РКІ на сервере muna Enterprise. Возможны другие варианты построения РКІ в зависимости от количества сотрудников, бюджета, кадровой политики и других параметров.

| Мастер добавления ролей | | × |
|--|--|---|
| Задание типа ус | становки | |
| 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 | Центры сертификации могут использовать данные в Active Directory для упрощения выдачи сертификатов и управления ими. Укажите, следует ли установить ЦС предприятия или изолированный ЦС. | |
| | Подробности о различиях между ЦС предприятия и автономным ЦС | |
| | < <u>Н</u> азад Далее > Установить Отмена | |

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).

| Мастер добавления ролей | | | | |
|--|--|--|--|--|
| Установка закрытого ключа | | | | |
| Перед началом работы Роли сервера Службы сертификации АD Службы ролей Вариант установки Тип ЦС Вакрытый ключ Шифрование Иня ЦС Срок действия База данных сертификатов Веб-сервер (IIS) Службы ролей Подтверждение Ход выполнения Результаты | Чтобы создавать и выдавать клиентам сертификаты, ЦС должен иметь закрытый ключ. Укажите, следует ли создать новый закрытый ключ С доздать новый закрытый ключ Ипользуйте этот параметр, если отсутствует закрытый ключ или следует создать новый закрытый ключ. Мазарать и указать длину закрытого ключа. Для выдачи новых сертификатов также инфорозания и указать длину закрытого ключа. Для выдачи новых сертификатов также инфорозания и указать длину закрытого ключа. Для выдачи новых сертификатов также измеротанов выбрать существующий закрытый ключ Используйте этот параметр, чтобы при переустановке ЦС гарантировать непрерывность с ранее выданными сертификат и использовать связанный с ним закрытый ключ Выбрать сертификат и использовать связанный с ним закрытый ключ параметр, если на этом компьютере Выбрать существующий закрытый ключ на этом компьютере Выбрать существующий закрытый ключ и из предыдущей установки или следует использовать закрытый ключ из другого источника. | | | |
| | < <u>Н</u> азад Далее > Установить Отмена | | | |

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

| Мастер добавления ролей | × |
|--|--|
| Настройка шифр | рования для ЦС |
| 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 | Для создания нового закрытого ключа необходимо выбрать поставщика служб шифрования, куш- алгорити и длину ключа в соответствии с назначением выдаваемых сертификатов. Выбор большей длины ключа повышает уровень безопасности, но увеличивает время, необходимое для выполнения операций подписания. Выберите поставщика служб шифрования (CSP): Длина ключа (знаков): RSA#Microsoft Software Key Storage Provider Выберите алгоритм хеширования для подписывания сертификатов, выдаваемых этим ЦС: SHA256 SHA384 SHA512 ↓ ↓ Разрешить взаимодействие с администратором, если центр сертификации обращается к закрытому ключу. |
| | Подробности о параметрах шифрования для ЦС |
| | < <u>Н</u> азад <u>Да</u> лее > Ус <u>т</u> ановить Отмена |

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

Внимание! Изменить параметр соттоп пате 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.



| Мастер добавления ролей | | × |
|--|--|---|
| Задание имени L | ĮC | |
| Перед началом работы Роли сервера Службы сертификации AD | Введите общее имя, определяющее ЦС. Это имя добавляется во все сертификаты, выдаваемые данным ЦС. Значения суффикса отличающегося имени генерируются автоматически, но не могут быть изменены. | |
| Службы ролей | Mycompany-Root-Ent-CA | - |
| Вариант установки | | |
| ТипЦС | Суффикс различающегося имени: DC=mycompany_DC=local | - |
| Закрытый ключ | | |
| Шифрование | | |
| Имя ЦС | Предпросмотр различающегося имени: | |
| Срок действия | CN=Mycompany-Root-Ent-CA,DC=mycompany,DC=local | |
| База данных сертификатов | | |
| Веб-сервер (IIS) | | |
| Службы ролей | | |
| Подтверждение | | |
| Ход выполнения | | |
| Результаты | | |
| | | |
| | Подробности о настройке имени ЦС | |
| | < <u>Н</u> азад Далее > Ус <u>т</u> ановить Отмена | |

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



| Мастер добавления ролей | | | |
|--|--|--|--|
| Установить срои | сдействия | | |
| Перед началом работы Роли сервера Службы сертификации AD Службы ролей Вариант установки Тип ЦС Закрытый ключ Шифрование Имя ЦС | 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 АМ Учтите, что сертификаты, выдаваемые ЦС, действительны только до истечения его срока действия. | | |
| Срок действия | | | |
| База данных сертификатов | | | |
| Веб-сервер (IIS) | | | |
| Службы ролей | | | |
| Подтверждение | | | |
| Ход выполнения | | | |
| Результаты | Подробности о настройке срока действия сертификата < <u>Н</u> азад <u>Да</u> лее > Ус <u>т</u> ановить Отмена | | |

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

| Мастер добавления ролей | | | |
|--|---|--|--|
| Настройка базы | данных сертификатов | | |
| Перед началом работы Роли сервера Службы сертификации AD Службы ролей | База данных сертификатов записывает все запросы сертификатов, выданные сертификаты, а также отозванные или просроченные сертификаты. Журнал базы данных можно использовать для отслеживания активности ЦС. <u>Р</u> асположение БД сертификатов: | | |
| Вариант установки Тип ЦС Закрытый ключ Шифрование | C:\Windows\system32\CertLog Обзор Использовать существующую базу данных сертификатов из предыдущей установки в этом расположении Этом Расположение журнала базы данных сертификатов: В этом | | |
| Имя ЦС Срок действия База данных сертификатов | C:\Windows\system32\CertLog O <u>6</u> 3op | | |
| Веб-сервер (IIS) Службы ролей Подтверждение | | | |
| Ход выполнения Результаты | | | |
| | < Назад Далее > Установить Отмена | | |

Настройка веб-сервера. Просмотрите информацию и нажмите далее.



Мастер добавления ролей



Отметьте необходимые опции (можно оставить значения по умолчанию).



14

X



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



| Мастер добавления ролей | | | × |
|---|--|-------------------------------|---|
| Подтверждение | выбранных элементов для | і установки | |
| Подат верикцение выоранных элементов для установки Перед началом работы Роли сервера Службы сертификации АD Службы ролей Вариант установки Тип ЦС Закрытый ключ Шифрование Имя ЦС Срок действия Ваза данных сертификатов Веб-сервер (IIS) Службы ролей Ваза данных сертификатов Веб-сервер (IIS) Службы ролей Службы ролей Службы ролей Службы ролей Службы ролей Службы сертификатов Веб-сервер (IIS) Службы ролей Срок действия Разришть взаимодействие с Отключено После ваяершения : 8/13/2018 6:19 АМ Различающееся имя : CN=Mycompany-Root-Ent-CA,DC=mycompany,DC=local Расположение круньтаты Служба регистрация в центре сертификация через Интернет | | | |
| | Служба регистрации в центр Печать, отправка по электронной по | е сертификации через Интернет | |

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 u 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 <u>http(s)://localhost/certsrv</u> с машины на которой стоит центр сертификации. При обращении с других компьютеров можно указать IP-адрес или FQDN сервера ЦС, например, <u>http(s)://10.1.1.5/certsrv</u> или <u>http(s)://ca.mycompany.local/certsrv</u>. 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 тусотрапу.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.

| Создать сертификат | | ? X | |
|--|---|-----|--|
| Свойства различающегося имени | | | |
| Укажите данные, необход быть указаны полные офи | димые для сертификата. В полях "Область, край" и "Город" должны ициальные названия без сокращений. | | |
| Полное имя: | mycompany.local | | |
| Органи <u>з</u> ация: | MyCompany Inc. | | |
| Подразделение: | dev | | |
| Г <u>о</u> род | Москва | | |
| О <u>б</u> ласть, край: | Московская область | | |
| Страна или регион: | RU | | |
| | | | |
| | | | |
| | <u>Н</u> азад <u>Далее</u> <u>Готово</u> Отме | ена | |

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



| Создать сертификат | <u>? ×</u> |
|--|------------|
| Локальный центр сертификации | |
| Задайте в том же домене центр сертификации, который подпишет сертификат. Рекомендуется легко запоминающееся понятное имя. | |
| <u>Л</u> окальный центр сертификации: | |
| Mycompany-Root-Ent-CA\CA.mycompany.local Выбрать | |
| Пример: ИмяЦентраСертификации ИмяСервера | |
| Понятное имя: | |
| сертификат для certsrv | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| <u>Н</u> азад <u>Да</u> лее <u>Г</u> отово От | мена |

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.



| Привязки | сайта | | | | <u>? x</u> |
|----------|----------|------|-----------|----------|-----------------------------------|
| Тип | Имя узла | Порт | IP-адреса | Сведен | <u>До</u> бавить |
| http | | 80 | * | | |
| https | | 443 | * | | Изменить |
| | | | | | <u>У</u> далить О <u>б</u> зор |
| | | | | <u> </u> | |
| | | | | | <u>З</u> акрыть |

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

| Добавление привя | ізки сайта | <u>? ×</u> |
|-------------------------|---|-------------------------------|
| <u>Т</u> ип: https | IP- <u>ад</u> рес: Все неназначенные | П <u>о</u> рт: 4 43 |
| Имя у <u>з</u> ла: | | 1 |
| Сертификат <u>ы</u> SSL | | |
| сертификат для с | ertsrv 🔽 | <u>В</u> ид |
| | O | С Отмена |

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.

| Свойства обозревателя | Параметры безопасности - зона надежных узлов |
|---|--|
| Своиства обозревателя Содержание Общие Безопасность Выберите зону для настройки ее параметров безопасности. Выберите зону для настройки ее параметров безопасности. Выберите зону для настройки ее параметров безопасности. | Параметры Параметры Загрузка подписанных элементов ActiveX Включить Отключить Отключить Отключить Эалуск элементов ActiveX и модулей подключения Включить Допущенных администратором Отключить Предлагать Использование элементов управления ActiveX, не помече Включить Отключить Отключить Предлагать Использование элементов управления ActiveX, не помече Включить Отключить Предлагать Поведение двоичного кодов и скриптов Включить Опредлагать Поведение двоичного кодов и скриптов Включить Сорисособых параметров На уровень: Средний (по умолчанию) |
| ОК Отмена Применить | ОК Отмена |

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

| 🖉 Microsoft Active Directory Certificate Services - Windows Internet Explorer | |
|--|---------------------|
| Co Co 🖉 http://localhost/certsrv/certcarc.asp | P - |
| 😪 Избранное 🛛 🍰 🖉 Web Slice Gallery 👻 🖉 Коллекция веб-фрагме 🔻 💽 Рекомендуемые сайты 👻 | |
| 🔠 🔻 🎉 Конфигурация уси 🧭 Новая вкладка 🛛 🎉 Microsoft Active 🗙 🛛 📩 👻 🖾 👻 Страница 👻 Безопасность 👻 Сер | р <u>в</u> ис т 🔞 т |
| () Internet Explorer заблокировал небезопасное использование элементов управления ActiveX на этом веб-узле. Поэтому страница может отображаться неправильно. | × |
| | |
| Microsoft Active Directory Certificate Services Mycompany-Root-Ent-CA | Home |
| Download a CA Certificate, Certificate Chain, or CRI | |
| | — II |
| To trust certificates issued from this certification authority, install this CA certificate chain. | |
| To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method. | |
| CA certificate: | |
| Current [Mycompany-Root-Ent-CA] | |
| | |
| | |
| Encoding mothod: | |
| | |
| O Base 64 | |
| Download CA certificate | |
| Download CA certificate chain | |
| Download latest base CRL | |
| Download latest delta CRL | _ |
| 🕐 Готово 🛛 🔰 🗸 Надежные узлы Защищенный режим: выкл. 🧖 🗸 🔩 | 100% - // |

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**.



| Сертификат | × | |
|--|---|--|
| Общие Состав Путь сертификации | | |
| Сведения о сертификате | | |
| Этот сертификат предназначается для: | | |
| • Все политики выдачи • Все политики применения | | |
| - Dee Hourraidh Ipriteireana | | |
| | | |
| | | |
| Кому выдан: Mycompany-Root-Ent-CA | | |
| Кем выдан: Mycompany-Root-Ent-CA | | |
| Действителен с 8/ 13/ 2013 по 8/ 13/ 2018 | | |
| Установить сертификат Ваявление поставщика Подробнее о <u>сертификатах</u> | | |
| ОК | | |

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.

| Мастер импорта сертификатов Хранилище сертификатов Хранилища сертификатов - это системные области, в которых хранятся сертификаты. | × |
|--|-----|
| Выбор хранилища мож можно указать размец С Автоматически Выберите хранилище сертификатов. | |
| Поместить все кранилище серт Доверенные корневые центры сертиф Доверительные отношения в предпри Доверенные издатели Доверенные издатели Сертификаты, к которым нет ловери Показать физические хранилища |] |
| Подробнее о <u>хранилищах</u> | |
| < Назад Далее > Отме | ена |



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 ММС. 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.

| 🧱 Консоль1 - [Корень консоли\Политика Default Domain Policy [SERVER.mycompany.local]\Конфигура 📃 🔲 🗙 | | | |
|--|---------------------------|------------|--|
| 🚟 Файл Действие Вид Избранное Окно Справка | | _ 8 × | |
| | | | |
| Политики открытого ключа 🔺 Кому выдан 🔺 | Кем выдан | Действия | |
| 📔 Шифрующая файловая система (EFS) 🛛 🗐 Мусотрапу-Root-Ent | -CA Mycompany-Root-Ent-CA | Ловеренн 🔺 | |
| 📔 Шифрование диска BitLocker | | | |
| 📔 Параметры автоматического запроса сертифик | | Допол 🕨 | |
| Доверенные корневые центры сертификации | | | |
| 📔 Доверительные отношения в предприятии | | | |
| Промежуточные центры сертификации | | | |
| 🚰 Доверенные издатели | | | |
| 📔 Сертификаты, к которым нет доверия | | | |
| 📋 Доверенные лица | | | |
| | | | |
| | | | |
| | | | |

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).



| 🙀 Регистрация сертификатов | | |
|--|------------------------------------|-----------------------------|
| 🔄 Регистрация сертификатов | | |
| Запрос сертификатов | | |
| Можно запросить следующие типы сертифи затем нажмите кнопку "Заявка". | катов. Выберите сертификаты, котој | рые необходимо запросить, а |
| Политика регистрации Active Di | rectory | |
| Контроллер домена | () Состояние: Доступно | Подробности 🛞 |
| Почтовая репликация каталога | (1) Состояние: Доступно | Подробности 🛞 |
| Проверка подлинности контроллера домена | Осстояние: Доступно | Подробности 🛞 |
| | | |
| Показать все шаблоны | | |
| Дополнительные сведения о <u>сертификатах</u> | | |
| | | <u>З</u> аявка Отмена |

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).



| 틡 Диспетчер сервера | | |
|--|-----------------------|-----------------------------|
| Файл Действие Вид Справка | | |
| 🗢 🔿 🖄 🖬 📓 🕰 👼 📔 🕨 🔳 | | |
| Службы сертификации Active Directory Стевой ответчик: СА | Mycompany-Root-Ent-CA | Действия |
| 💭 Конфигурация отзыва | Имя | Mycompany-Root-Ent-CA |
| Эконфигурация массива | Выданные сертификаты | Дополнительные действия 🕨 🕨 |
| Ваблоны сертификатов | 🚨 Запросы в ожидании | |
| 🖃 🛃 Mycompany-Root-Ent-(Все задачи | дачные запросы | |
| Отозванные серти Выданные сертис Вид | рлоны сертификатов | |
| Запросы в ожидан | | |
| Неудачные запрос Экспортировать с | писок | |
| Паколоны сертифи Паколоны сертифи Паколоны сертифи Паколоны сертифи Свойства | | |
| Компоненты | | |
| на диагностика Справка | | |
| 🕀 🧱 Хранилище | | |
| 4 P | | |
| Открытие окна свойств выбранного объекта. | | |

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

| Свойства: Мусо | ompany-Root-Ent-CA | <u>? ×</u> |
|---|--|--|
| Хранилище Аудит | Диспетчеры сертификатов Агенты восстановления | Агенты подачи заявок Безопасность |
| Общие І | Модуль политики 📗 Модуль і | выхода Расширения |
| Выберите рас | с <u>ш</u> ирение: | |
| Доступ к све | дениям о центрах сертификац | ии (AIA) 💌 |
| Ука <u>ж</u> ите, отку центра сертис | уда пользователи могут получи фикации. | ть сертификат этого |
| C:\Windows\v Idap:///CN=< http:// <server file://<server< td=""><td>system32\CertSrv\CertEnroll\<se CATruncatedName>,CN=AIA,CN rDNSName>/CertEnroll/<serverd DNSName>/CertEnroll/<serverd< td=""><td>rverDNSName>_<caname =Public Key Services,CN=S DNSName>_<caname><ce NSName>_<caname><cert< td=""></cert<></caname></ce </caname></caname </td></serverd<></serverd </se </td></server<></server | system32\CertSrv\CertEnroll\ <se CATruncatedName>,CN=AIA,CN rDNSName>/CertEnroll/<serverd DNSName>/CertEnroll/<serverd< td=""><td>rverDNSName>_<caname =Public Key Services,CN=S DNSName>_<caname><ce NSName>_<caname><cert< td=""></cert<></caname></ce </caname></caname </td></serverd<></serverd </se | rverDNSName>_ <caname =Public Key Services,CN=S DNSName>_<caname><ce NSName>_<caname><cert< td=""></cert<></caname></ce </caname></caname |
| • | | Þ |
| | До | бавить |
| | | |
| | | |
| 🗖 Включать | в AIA-расширение выданных с | ертификатов |
| — П В <u>к</u> лючать | в расширения протокола OCSF | |
| | | |
| | | |
| | ОК Отмена | Применить Справка |
| | | |

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

| Добавление размещения | × |
|--|---|
| Размещение может быть допустимым URL или путем. Введите HTTP, LDAP, адрес файла, или введите UNC или локальный путь. Чтобы вставить переменную в URL или путь, выберите эту переменную в раскрывающемся списке и нажмите кнопку "Вставить". | |
| | |
| Inttp://mycompany.iocal/ocsp | |
| Переменная: | |
| <caname> Вставить</caname> | |
| Описание выбранной переменной: | |
| Используется в URL-адресах и путях Вставляет DNS-имя сервера Пример указания размещения: http:// <dns-имясервера>/CertEnroll/<[или (для OCSP) http://<dns-имясервера>/ocsp</dns-имясервера></dns-имясервера> | |
| ▲ | |
| ОК Отмена | J |

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).

| йства: Подписыван | ие отклика ОЅРС | | ? × |
|---|---|--|--|
| Шифрование | Имя субъекта | Требовани | 1я выдачи |
| Общие | | Обработка запрос | a |
| Устаревшие шаблонь | Расширения | Безопасность | Сервер |
| [руппы или пользоват | ели: | | |
| & Authenticated Use | rs | | |
| 🍇 Domain Admins (M | YCOMPANY\Domain Adm | nins) | |
| 🍇 Enterprise Admins (| (MYCOMPANY\Enterprise | Admins) | |
| NYCOMPANY CA (MYCOMPANY | ∖CA\$) | | |
| | | | Vara |
| | | До <u>б</u> авить | <u>у</u> далить |
| Разрешения для групп | ы "СА" | До <u>б</u> авить | <u>у</u> далить |
| <u>Р</u> азрешения для групг | ы "СА" | <u>Доб</u> авить Разрешить | <u>у</u> далить Запретить |
| <u>Р</u> азрешения для групг Полный доступ | њі "СА" | <u>Доб</u> авить Разрешить | Запретить |
| <u>Р</u> азрешения для групг Полный доступ Чтение | њі "СА" | <u>Доб</u> авить Разрешить Ш | Запретить |
| <u>Р</u> азрешения для групг Полный доступ Чтение Запись | ы "СА" | <u>Доб</u> авить Разрешить | удалить Запретить |
| <u>Р</u> азрешения для групг Полный доступ Чтение Запись Заявка | ы "СА" | <u>Доб</u> авить Разрешить У У У | запретить |
| <u>Р</u> азрешения для групп Полный доступ Чтение Запись Заявка Автоматическая по, | цы "СА" дача заявок | <u>Доб</u> авить Разрешить ☑ ☑ ☑ ☑ ☑ | запретить |
| Разрешения для групп Полный доступ Чтение Запись Заявка Автоматическая по, | њі "СА" дача заявок | <u>Доб</u> авить Разрешить ☑ ☑ ☑ ☑ | удалить Запретить |
| Разрешения для групг Полный доступ Чтение Запись Заявка Автоматическая по, | ъы "СА" дача заявок | <u>Доб</u> авить Разрешить У У О | удалить Запретить |
| Разрешения для групг Полный доступ Чтение Запись Заявка Автоматическая по, Чтобы задать особые нажмите кнопку "Доп | ты "СА" дача заявок разрешения или парами олнительно". | До <u>б</u> авить Разрешить У У С | удалить Запретить ОПО ОПО ОЛНИТЕЛЬНО |
| Разрешения для групг Полный доступ Чтение Запись Заявка Автоматическая по, Чтобы задать особые нажмите кнопку "Доп | ъы "СА" дача заявок разрешения или парами олнительно". | <u>Доб</u> авить Разрешить У У етры, <u>Доп</u> с | удалить Запретить ОПО ОПНИТЕЛЬНО |
| Разрешения для групг Полный доступ Чтение Запись Заявка Автоматическая по, Чтобы задать особые нажмите кнопку "Доп | вы "СА" дача заявок разрешения или парами олнительно". ании доступом и разреш | <u>Доб</u> авить Разрешить ☑ ☑ ☑ етры, <u>Доп</u> с | удалить Запретить ОПО ОПО ОЛНИТЕЛЬНО |

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



| войства: Подписыван | ие отклика ОЅРС | | <u>? ×</u> | | |
|--|--|-----------------------------------|------------|--|--|
| Шифрование | Имя субъекта | Требования | выдачи | | |
| Устаревшие шаблоны | Расширения | Безопасность | Сервер | | |
| Общие | | Обработка запроса | | | |
| Цель: Подли | сь | | • | | |
| ⊏ <u>У</u> да сер | лять отозванные или г тификаты, не архивиру | просроченные я | | | |
| ⊏ <u>В</u> кл раз ⊏ Аох | ючить симметричные ; решенные субъектом ивировать закрытый к | алгоритмы, люч счбъекта | | | |
| | 1спользовать расшире алгоритм для отправки | нный симметричный ключа в Ц.С. | | | |
| ✓ Авторизация дополнительных учетных записей служб для доступа к закрытому ключу Газрещения для ключа Газрешить экспортировать закрытый ключ При подаче заявки для субъекта и использовании закрытого ключа | | | | | |
| Подавать заявку д. | от. ля субъекта, не требуя | ввода данных | | | |
| C Secolutions control | | UCTOBILIU | | | |
| Запрашивать пользователя и требовать ответа при использовании закрытого ключа | | | | | |
| | ОК Отмена | Применить | Справка | | |

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

| Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или " <u>?</u> 🗙 | | | | |
|--|-----------------------|--|--|--|
| <u>В</u> ыберите тип объекта: | | | | |
| "Пользователи", "Группы" или "Встроенные субъекты безопасно | <u>Т</u> ипы объектов | | | |
| В с <u>л</u> едующем месте: | | | | |
| mycompany.local | <u>Р</u> азмещение | | | |
| Введите <u>и</u> мена выбираемых объектов (<u>примеры</u>): | | | | |
| NETWORK SERVICE | Проверить имена | | | |
| | | | | |
| | | | | |
| Дополнительно ОК | Отмена | | | |
| | | | | |



| [Разрешения для группы | "Подписывание о | тклика 05 🗴 |
|--|---------------------|--------------------|
| Безопасность | | |
| і Группы или пользователи: | | |
| SYSTEM Administrators (MYCOMP) | ANY\Administrators) | |
| & NETWORK SERVICE | | |
| & OcspSvc | | |
| | | |
| | | × 1 |
| | Додавить | <u>у</u> далить |
| <u>Разрешения для группы "NE</u> SERVICE" | TWORK Paspeuurt | ь Запретить |
| Чтение | | |
| Полный доступ | | |
| | _ | _ |
| | | |
| | | |
| | | |
| | | |
| Подробнее об управлении до | оступом и разрешени | IRX |
| | | |
| OK | Отмена | При <u>м</u> енить |

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





| 🔜 Включение шаблонов сертификатов | × | | | |
|---|--------------|--|--|--|
| Выберите один шаблон сертификата для использован центре сертификации (ЦС). | ИЯ В ЭТОМ | | | |
| Примечание. Если созданный шаблон сертификата не отображается в списке, подождите некоторое время, пока информация о шаблоне не будет реплицирована на все контроллеры домена. | | | | |
| Не все шаблоны сертификатов в организации могут б для вашего ЦС. | ыть доступны | | | |
| Дополнительную информацию см. в разделе <u>Основны</u> <u>шаблонах сертификатов.</u> | е сведения о | | | |
| Имя | Назначе 🔺 | | | |
| 🗵 Перекрестный центр сертификации | <bce></bce> | | | |
| 🗵 Подписывание кода | Подпись | | | |
| Подписывание отклика OSPC Подписа | | | | |
| 🖳 Подлисывание списка доверия Подлисы | | | | |
| 🖳 Пользователь Exchange Защище | | | | |
| 🖳 Проверенный сеанс Провер | | | | |
| | • | | | |
| ОК | Отмена | | | |

На сервере сетевого ответчика выпишите сертификат через консоль ттс с оснасткой **Сертификаты - Локальный компьютер**.

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

| 📕 Диспетчер сервера | | |
|---|-------------------------------|-----------------------------------|
| <u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>С</u> правка | | |
| 🗢 🔿 🖄 💼 🖬 | | |
| E 🚏 Службы сертификации Active Directory | CA | Действия |
| 🔊 Конфигурация отзыва | Имя конфигурации отзыва | CA 🔺 |
| 🖃 🌮 Конфигурация массива | | Установить как контроллер массива |
| 🛱 РКІ предприятия | | Вид 🕨 |
| 🚇 Шаблоны сертификатов | | 🗙 Удалить |
| Mycompany-Root-Ent-CA | | О Обновить |
| Выданные сертификаты | | Справка |
| Запросы в ожидании | | - |
| Пеудачные запросы Шаблоны сертификатов | Состояние конфигурации отзыва | |
| 🕀 🛅 Файловые службы | | |
| на Компоненты на Лиагностика | | |
| 🗄 📊 Конфигурация | Просмотр сертификата подлиси | |
| 🛨 🚰 Хранилище | Состояние поставщика отзыва: | |
| Назначить контроллером массива | | I |
| nasio in promponingentiace/bu | | |

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.



| 🔚 Диспетчер сервера | |
|---|------------|
| Файл Действие Вид Справка | |
| | |
| Службы сертификации Active Directory 🗾 Конфигурация отзыва | Действия |
| р 😨 сетевой ответчик: SERVER-CA Имя Выбор сертиd | Конфигур 🔺 |
| Конфигурация отзыва Конфигурация массие Добавить конфигурацию отзыва Нет элементов для отображения в этом виде. | Добав |
| Вид № Вид Вид • Вид | Вид 🕨 |
| а Шолонан сертификатов а Мусотрапу-Root-Ent-CA Обновить | Обнов |
| Отозванные сертифи Экспортировать список | 🔒 Экспо |
| Выданные сертифика Запросы в ожидании Справка | 🛛 Справка |
| 🗎 Неудачные запросы | - |
| 🚰 Шаблоны сертификатов | |
| В Файловые службы | |
| рмпоненты | |
| иагностика | |
| | |
| Добавить конфигурацию отзыва | |

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

| Добавить конфигурацию | отзыва | ? × |
|-----------------------|--|-----|
| Введите и | имя конфигурации отзыва | |
| Основные сведения п, | Имя конфигурации отзыва помогает идентифицировать конфигурацию | |
| Введите имя конфигу | отзыва. Рекомендуется использовать имя, способное идентифицировать | |
| Выберите расположе | це, который будет солоставлет этой конфигурации отзыва. | |
| Выбрать сертификат | <u>Имя:</u> OCSP Mycompany | |
| Выбрать сертификат | | |
| Поставщик отзыва | | |
| | | |
| | | |
| | < <u>Н</u> азад Далее >отово Отмена | • |

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.

| Свойства | поставщика отзыва | × | | |
|--|--|----------------|--|--|
| Этот поставщик доступа определяет состояние отзыва сертификатов на основании списков отзыва, которые выдает ЦС. Определите расположение для списков отзыва сертификатов. | | | | |
| <u>Б</u> азовые (| CRL: | | | |
| ldap:///C | N=Mycompany-Root-Ent-CA,CN=CA,CN=CDP, | Вверх | | |
| | - | Внив | | |
| 4 | | DUID | | |
| | Добавить Изменить Удалить | | | |
| Р <u>а</u> зностн | ые CRL: | | | |
| | <u> </u> | Вв <u>е</u> рх | | |
| • | | Вни <u>в</u> | | |
| | <u>До</u> бавить Из <u>м</u> енить Уда <u>л</u> ить | | | |
| Обное | зл <u>я</u> ть CRL на основании их периодов действия | | | |
| Обновля <u>т</u> | ть CRL с указанным интервалом обновления (мин): | | | |
| | OK | Отмена | | |

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.

| 🎼 pkiview - [PKI предприятия\Мус | ompany-Root-Ent-CA (V0.0)] | | | | <u> </u> |
|---|----------------------------|------|----------------|------------------------------------|------------|
| <u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>С</u> правка | | | | | |
| 🗢 🔿 🙇 🖪 | | | | | |
| 🏥 PKI предприятия | Имя | Сост | Срок действия | Размещение | Действия |
| 🙀 Mycompany-Root-Ent-CA (V0.0) | 🙀 Сертификат ЦС | ОК | 8/13/2018 8:34 | | Mycompan 🔺 |
| | 🗐 Расположение AIA #1 | OK | 8/13/2018 8:34 | ldap:///CN=Mycompany-Root-Ent-CA,C | |
| | 🖹 Расположение CDP #1 | OK | 8/27/2013 8:44 | ldap:///CN=Mycompany-Root-Ent-CA,C | Дополн 🕨 |
| | 🗵 Расположение DeltaCRL #1 | OK | 8/23/2013 11:3 | ldap:///CN=Mycompany-Root-Ent-CA,C | |
| | Расположение OCSP #1 | OK | | http://mycompany.local/ocsp | Расположе |
| | | | | Þ | Дополн 🕨 |
| | | | | | |

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 OC Windows XP служба запущена по умолчанию, а в OC 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 ММС. 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)



| 🧱 Консоль1 - [Корень консоли\Политика Default Domain Policy [SERVER.mycompany.local]\Конфигурация компьютера\Политик 🛛 | | | |
|--|-----------------------|--|--|
| 🚟 <u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>И</u> збранное <u>О</u> кно <u>С</u> правка | _ 8 × | | |
| | | | |
| 🖃 🛅 Конфигурация Windows 🔺 Политика 🔺 Парамет | гр политик 🔺 Действия | | |
| 🗄 🛅 Политика разрешения и! 🛛 🔯 Завершение работы: разрешить завершение работы системы Не опре, | делено Параметр 🔺 | | |
| 😫 Сценарии (запуск/завер 🔰 🌒 Интерактивный вход в систему: поведение при извлечении с Не опре | делено | | |
| 🖃 🛅 Параметры безопасност 🔤 💹 Интерактивный вход в систему: заголовок сообщения для пол Не опре, | делено Допол 🕨 | | |
| 🕀 📑 Политики учетных з 🛛 📓 Интерактивный вход в систему: количество предыдущих под Не опре, | делено Интеракт | | |
| 🖃 🧃 Люкальные политика 🛛 🐘 Интерактивный вход в систему: напоминать пользователям о Не опред | делено | | |
| 🔲 🔲 политика аудита 🗌 🐘 Интерактивный вход в систему: не отображать последнее им Не опред | делено Допол 🕨 | | |
| назначение прав Пазмачение прав Мнтерактивный вход в систему: не требовать нажатия CTRL+ Не опред | делено | | |
| Шанаристри останции Интерактивный вход в систему: отображать сведения о польз Не опред | делено | | |
| Портипы с ограничени Интерактивный вход в систему: текст сообщения для пользов Не опред | делено | | |
| Системные службы 🛛 🖏 Интерактивный вход в систему: требовать проверки на контр Не опред | делено | | |
| 🗄 🔂 Реестр 💦 🔛 Интерактивный вход в систему: требовать смарт-карту Не опред | делено | | |
| | | | |
| | | | |

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:

| 🧱 Консоль1 - [Корень консоли\Центр сертификации (Локальный)\Mycompany-Root-Ent-CA\Шаблоны сертификатов] 💶 🗵 | | | |
|---|------------------------------------|------------------------|---------------|
| 🚟 <u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>И</u> збранное <u>О</u> кни | о <u>С</u> правка | | _ & × |
| 🗢 🔿 🖄 🖬 🗙 😖 🔽 🗊 | | | |
| 🧮 Корень консоли | Имя | Назначение | Действия |
| 🖃 🚋 Центр сертификации (Локальный) | 🚇 Агент регистрации (компьютер) | Агент запроса сертифик | Шаблоны сер 🔺 |
| E 🚽 Mycompany-Root-Ent-CA | 🚇 Агент регистрации | Агент запроса сертифик | |
| Отозванные сертификаты | 🚇 Пользователь со смарт-картой | Защищенная электронна | Дополнит 🕨 |
| Выданные сертификаты | 🚇 Вход со смарт-картой | Проверка подлинности к | Выбланные а |
| Запросы в ожидании | 🚇 Почтовая репликация каталога | Почтовая репликация сл | |
| | 🚇 Проверка подлинности контроллера | Проверка подлинности к | Дополнит 🕨 |
| шаолоны сертификатов | 🚇 Агент восстановления EFS | Восстановление файлов | |
| | 🚇 Базовое шифрование EFS | Шифрующая файловая с | |
| | 🚇 Контроллер домена | Проверка подлинности к | |
| | 🚇 Веб-сервер | Проверка подлинности с | |
| | 🚇 Компьютер | Проверка подлинности к | |
| | 🗵 Пользователь | Шифрующая файловая с | |
| | 🚇 Подчиненный центр сертификации | <bce></bce> | |
| | 🚇 Администратор | Подписывание списка до | |
| | • | ► I | |
| | | | |

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 Server⁴, 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.



| 🚆 Server Manager | | | <u>_ ×</u> |
|---|--------------------------------------|-----------|----------------|
| File Action View Help | | | |
| 🗢 🔿 🙍 🖬 🗙 🖬 🔒 | | | |
| Server Manager (SERVER) | Certificate Templates (SERVER.DOMAIN | I.LOCAL) | Actions |
| Roles Active Directory Certificate Service | Template Display Name 🔺 | Minimun 🔺 | Certificate 🔺 |
| Active Directory Certificate Service T I I I I I I I I I I I I I I I I | Administrator | Window | More 🕨 |
| | Ruthenticated Session | Window | |
| Certificate Templates (SERVER | Basic EFS | Window | Copy of S 🔺 |
| 🗆 🚽 DOMAIN-SERVER-CA | Reference CA Exchange | Window | More |
| 📄 Revoked Certificates | CEP Encryption | Window | More |
| Issued Certificates | 🚇 Code Signing | Window | |
| Pending Requests | Computer | Window | |
| Failed Requests | Copy of Smartcard User | Window | |
| Certificate Templates | Record Cross Certification Authority | Window | |
| Active Directory Domain Services | Directory Email Replication | Window | |
| 🖃 📄 Active Directory Users and Cor 💌 | | Window | |
| | | ► I | |
| | | | |

Откройте свойства нового шаблона (в примере рассмотрены не все опции шаблона). Во вкладке General (Общие) можно изменить срок, на который выдается сертификат.

| Cryptography Subject Name Issuance Requirements Superseded Templates Extensions Security Serv General Request Handling Template display name: Copy of Smatcard User Minimum Supported CAs: Windows Server 2008 Enterprise Template name: Copy of Smatcard User Validity period: Renewal period: Image: Validity period: Image: Copy of Smatcard User Validity period: Renewal period: Image: Validity period: Image: Copy of Smatcard User Validity period: Renewal period: Image: Validity period: Image: Copy of Smatcard User Validity period: Image: Copy of Smatcard User Image: Validity period: Image: Copy of Smatca | operties | f Smartcard User I |
|--|---|---|
| Superseded Templates Extensions Security Server General Request Handling Template display name: Copy of Smattcard User Minimum Supported CAs: Windows Server 2008 Enterprise Template name: Copy of Smattcard User Validity period: Renewal period: Image: Image: Validity period: Image: Validity period: Image: Image: Image: Validity period: Image: Image: Image: Validity period: Image: Image: Image: Image: <td< th=""><th>ubject Name 📔 Issuance Requirements</th><th>yptography</th></td<> | ubject Name 📔 Issuance Requirements | yptography |
| General Request Handling Template display name: Copy of Smatcard User Minimum Supported CAs: Windows Server 2008 Enterprise Template name: Copy of Smatcard User Validity period: Renewal period: Image: Image: Validity period: Image: Validity period: Image: Image: Image: Validity period: Image: Image: Image: | Extensions Security Server | perseded Templates |
| Template display name: Copy of Smatcard User Minimum Supported CAs: Windows Server 2008 Enterprise Template name: Copy of Smatcard User Validity period: Renewal period: Validity period: 6 weeks ▼ Publish certificate in Active Directory Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory For automatic renewal of smart card certificates, use the existing key if a new key cannot be created | Request Handling | General |
| Copy of Smartcard User Minimum Supported CAs: Windows Server 2008 Enterprise Template name: Copy of Smartcard User Validity period: Renewal period: years 6 weeks Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory For automatic renewal of smart card certificates, use the existing key if a new key cannot be created | | nplate display name: |
| Minimum Supported CAs: Windows Server 2008 Enterprise Template name: Copy of Smartcard User Validity period: | | y of Smartcard User |
| Copy of Smartcard User Validity period: Image: state of the st | Nindows Server 2008 Enterprise | mum Supported CAs: |
| Validity period: Validity per | | v of Smartcard User |
| Validity period: Renewal period: Image: Second state of the second state of the second state state of the second state state of the second state stat | | y or officiated oper |
| Directory For automatic renewal of smart card certificates, use the existing key if a new key cannot be created | Renewal period: | dity period: |
| For automatic renewal of smart card certificates, use the existing key if a new key cannot be created | Renewal period: 6 weeks itive Directory reenroll if a duplicate certificate exists in Active | dity period: Image: second control of the s |
| | Renewal period: 6 weeks tive Directory reenroll if a duplicate certificate exists in Active | dity period: years Publish certificate in A Do not automatical Directory |
| | Renewal period: 6 weeks tive Directory reenroll if a duplicate certificate exists in Active f smart card certificates, use the existing key created | dity period: years Publish certificate in A Do not automatica Directory For automatic renewal f a new key cannot b |
| | Renewal period: 6 weeks tive Directory reenroll if a duplicate certificate exists in Active f smart card certificates, use the existing key created | dity period: years Publish certificate in A Do not automatica Directory For automatic renewal f a new key cannot be |
| | Renewal period: 6 weeks tive Directory reenroll if a duplicate certificate exists in Active fi smart card certificates, use the existing key created | dity period: years Publish certificate in A Do not automatica Directory For automatic renewal f a new key cannot be |
| OK Cancel Andur Heir | Renewal period: 6 weeks tive Directory reenroll if a duplicate certificate exists in Active f smart card certificates, use the existing key created | dity period: years Publish certificate in A Do not automatica Directory For automatic renewal f a new key cannot bu |

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.

| | Copy of Smartcard User Properties | ? × |
|---|---|---|
| | Cryptography Subject Name Issuance Re General Request Handl | equirements |
| | Superseded Templates Extensions Security | Server |
| Edit Application Policies Extension | x ptensions included in this template: | |
| An application policy defines how a certificate can be used. Application policies: Client Authentication Secure Email Smart Card Logon | Application Policies Basic Constraints Certificate Template Information Issuance Policies | |
| Add Edit Remove | escription of Application Policies: Dient Authentication Encrypting File System Secure Email Email | Edit |
| Make this extension critical | | <u> </u> |
| | OK Cancel Apply | Help |
| Application Policies Extension application policy defines how a certificate can be ed. | X Add Application Policy An application policy (called enhanced key usage in defines how a certificate can be used. Select the app for valid signatures of certificates issued by this templated | Windows 2000) Ilication policy requi ate. |
| ient Authentication ecure Email mart Card Logon | Application policies: Any Purpose Certificate Request Agent Code Signing CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Signing Domain Name System (DNS) Server Trust Embedded Windows System Component Verification | |
| Add Edit Remove | File Recovery IP security end system | |
| Make this extension critical | | New |
| OK Cancel | | New |

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

| | Copy of Smartcard User Properties |
|--|--|
| | Cryptography Subject Name Issuance Requirements General Request Handling |
| | To modify an extension, select it, and then click Edit. |
| Edit Application Policies Extension An application policy defines how a certificate can be used. | xtensions included in this template: Application Policies Basic Constraints Certificate Template Information |
| Application policies: Client Authentication Encrypting File System Secure Email Smart Card Logon | Issuance Policies |
| | Edit |
| Add Edit Remove | Lient Authentication Automatication Incrypting File System Secure Email Smart Card Logon |
| OK Cancel | |
| | OK Cancel Apply Help |

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.

| Copy of Smartcard User Properties | ? × |
|--|-----|
| General Request Handling Superseded Templates Extensions Security Serve | er |
| Cryptography Subject Name Issuance Requirements | |
| Require the following for enrollment: | |
| CA certificate manager approval | |
| This number of authorized signatures: | |
| If you require more than one signature, autoenrollment is not allowed. | |
| Policy type required in signature: | |
| Application policy | - |
| Application policy: | |
| Certificate Request Agent | - |
| Issuance policies: | . |
| Add Remove | |
| Require the following for reenrollment: Same criteria as for enrollment Valid existing certificate | |
| OK Cancel Apply Help | |

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 ОК. Шаблон появится в списке.



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

9. 3anpoc cepmuфukama muna 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).



| 🙀 Certificate Enrollment | | |
|--|---|-------------------------------|
| 🚽 Certificate Enrollment | | |
| Request Certificates | | |
| You can request the following types of c | ertificates. Select the certificates you want to re | quest, and then click Enroll. |
| Basic EFS | (i) STATUS: Available | Details 🛞 🛋 |
| EFS Recovery Agent | 🤃 STATUS: Available | Details 🛞 |
| Enrollment Agent | 🤃 STATUS: Available | Details® |
| Smartcard Logon | 🤃 STATUS: Available | Details 🛞 |
| Smartcard User | 🤃 STATUS: Available | Details 🛞 |
| □User | 🤃 STATUS: Available | Details 🛞 🔔 |
| Show <u>a</u> ll templates | | |
| Learn more about certificates | | |
| | | Enroll Cancel |

У администратора появился новый сертификат Enrollment Agent.

| 🧧 certmgr - [Certificates - Current | User\Personal\Certificates] | | | | | | | |
|--------------------------------------|-----------------------------|------------------|-----------------|------------------------|---------------|--------|------------------|--|
| File Action View Help | | | | | | | | |
| 🗢 🔿 🙍 📅 📋 🧔 📑 | ? 🖬 | | | | | | | |
| 🙀 Certificates - Current User | Issued To 🔺 | Issued By | Expiration Date | Intended Purposes | Friendly Name | Status | Certificate Tem | |
| 🖃 🧮 Personal | Administrator | Administrator | 12/30/2112 | File Recovery | <none></none> | | | |
| Certificates | Administrator | domain-SERVER-CA | 1/24/2015 | Certificate Request Ag | <none></none> | | Enrollment Agent | |
| Trusted Root Certification Authority | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

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.



| rtificate Enrollment | | <u>_ 0 ×</u> |
|--|--|-----------------------------|
| ertificate Enrollment | | |
| Request Certificates | | |
| You can request the following | types of certificates. Select the certificates you want to re | quest, and then click Next. |
| C Smartcard Logon | i STATUS: Available | Details 🛞 🔺 |
| ⊙ Smartcard User | i) STATUS: Available | Details 🛞 |
| The following options des Key usage: Application policies: Validity period (days) | cribe the uses and validity period that apply to this type of Digital signature Key encipherment Secure Email Client Authentication Smart Card Logon : 365 | f certificate: |
| OUser | 🛈 STATUS: Available | |
| Show <u>a</u> ll templates Learn more about <u>certificates</u> | | |
| | | <u>N</u> ext Cancel |

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 ОК.

| 🖀 certmgr - [Certificates - Current User\Per | 🙀 Certificate Enrollment | |
|--|---|-----------------------------------|
| File Action View Help | 📮 Certificate Enrollment | |
| File Action View Help File Action View Help Image: Second | Certificate Enrollment Certificate Enrollment Certificate Enrollment Certificate Enrollment Certificate Properties Private Key Certification Authority Yo Cryptographic Service Provider A CSP is a program that generates a public and private key pair used in many certificate-related processes. Select cryptographic service provider (Encryption) Microsoft Strong Cryptographic Provider (Encryption) Microsoft Base DSS and Diffie-Hellman Cryptographic Provider (Encryption) Microsoft Base Smart Card Crypto Provider (Encryption) Microsoft DH SChannel Cryptographic Provider (Encryption) Show all CSPs Let | k Next. is @ A is @ is @ |
| Personal store contains 2 certificates. | | Cancel |
| | Learn more about <u>private key</u> OK Cancel Apply | |

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.

| 🚡 certmgr - [Certificates - Current User\Per | Certificate Enrollment | _ 🗆 🗵 |
|---|---|-------------------|
| File Action View Help | 🙀 Certificate Enrollment | |
| Certificates - Current User Personal Certificates Trusted Root Certification Autho Enterprise Trust Intermediate Certification Autho Active Directory User Object | Select a user To request a certificate on behalf of another user, enter the formal name or domain name of that u Firstname Lastname, username, or domain\username. User name or alias: | ser. For example, |
| Trusted Publishers Untrusted Certificates Third-Party Root Certification AL Trusted People Certificate Enrollment Requests Smart Card Trusted Roots | Select User | Browse |
| | User Object Types From this location: | |
| Personal store contains 2 certificates. | Advanced OK Cancel | Cancel |

Нажмите ОК, 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.

| 🚰 certmgr - [Certificates - Current User\Per | Certificate Enrollment | |
|--|---|--------|
| File Action View Help | 🙀 Certificate Enrollment | |
| Certificates - Current User Personal Certificates Trusted Root Certification Author Certificates Trusted Root Certification Author Certificates Trusted Personal Trusted Publishers Untrusted Certificates Trusted People Certificate Enrollment Requests Smart Card Trusted Roots | Requesting certificates. Please wait The enrollment server is being contacted to obtain the certificates you have requested. Active Directory Enrollment Policy © Smartcard User Vindows Security Enter PIN. Enrolling for the user certificate. Please enter your PIN. Please enter your PIN. Discrete for more information OK Cancel | |
| Personal store contains 2 certificates. | | Cancel |

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 СА 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 ММС с оснасткой – Сертификаты (Локальный компьютер) – Доверительные корневые центры сертификации.

Можно завершить сеанс текущего пользователя и авторизоваться по сертификату.

