Использование «Smart Card Logon» и ЦСК «CryptoKDC»

В Windows Server 2008

Киев 2014

Оглавление

1 Настройка соединения ЦСК «CryptoKDC» с LDAP «Active Directory»

ВНИМАНИЕ: Все действия в этой документации нужно выполнять под пользователем с правами администратора домена и администратора предприятия.

Для входа по смарт-картам нужно настроить соединение ЦСК «CryptoKDC» с LDAP «Active Directory» для публикации списка отозванных сертификатов в среде «Active Directory»

Для этого в «Active Directory» нужно создать доменного пользователя с помощью которого ЦСК «CryptoKDC» будет соединятся с LDAP «Active Directory» и создать пути размещения списка отозванных сертификатов.

1.1 Создание доменного пользователя

1. На стороне контроллера домена откройте управление пользователями «Active Directory» (Пуск-Администрирование-Active Directory-Пользователи и компьютеры);
2. Создайте доменного пользователя с произвольным именем и паролем, который соответствует вашим политикам безопасности. **(Пользователю нужны права администратора для успешного размещения СОС в LDAP)**;
3. На стороне Сервера ЦСК «CryptoKDC» откройте панель настроек подключения к LDAP (Инструменты-Настройка-LDAP);
4. В окне настроек введите полный путь к пользователю в LDAP и пароль пользователя (путь к пользователю можно просмотреть в ADSI Edit, в примере на Рисунок 1 он отображен как: **CN=LDAP,CN=Users,DC=dom,dc=ua**);

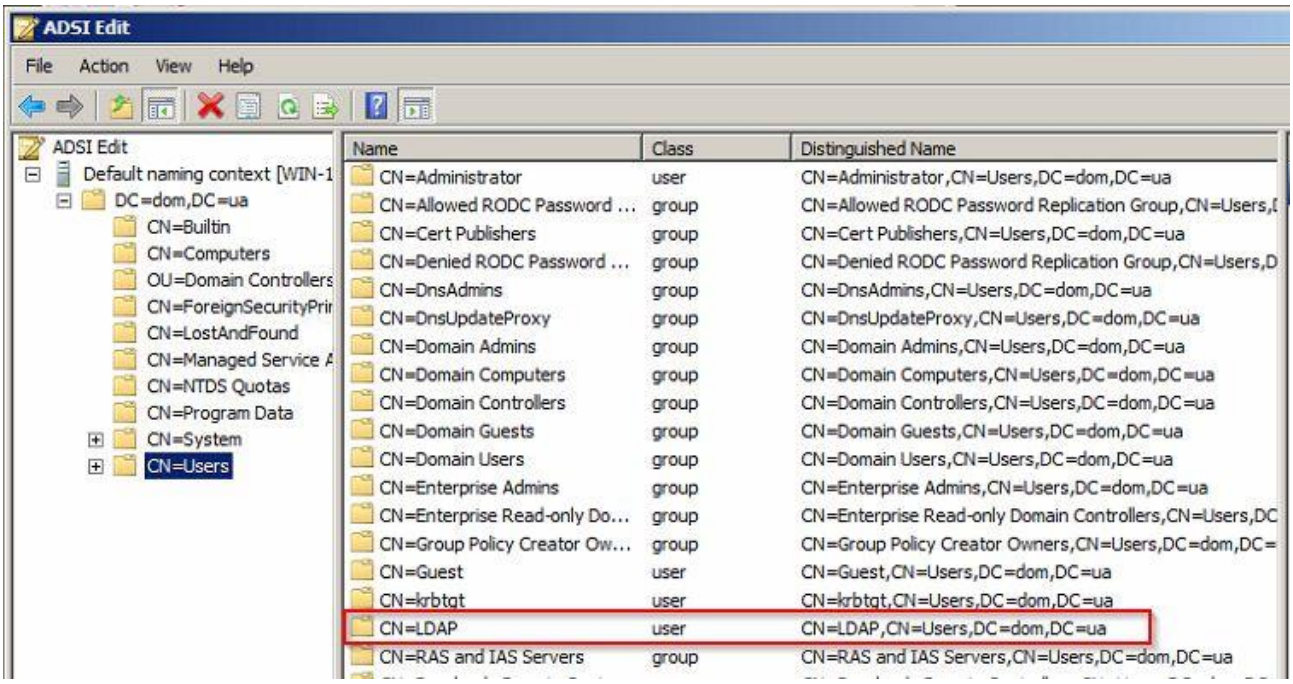

Рисунок 1

5. Введите адрес контроллера домена и порт (по умолчанию 389);
6. Нажмите кнопку «Тест», если настройки заданы верно, проверка будет успешной (Рисунок 2).

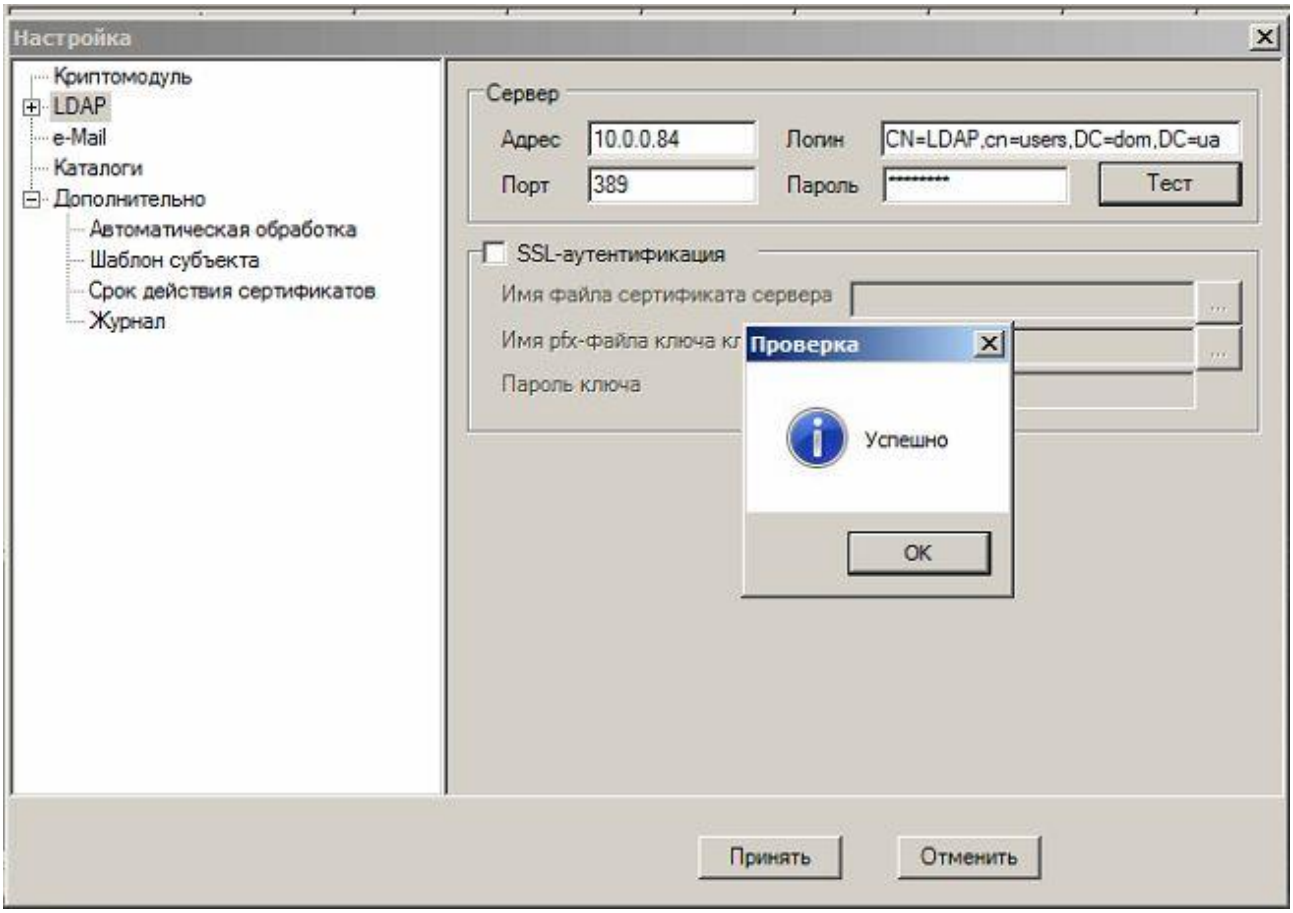

Рисунок 2

1.2 Создание путей размещения списка отозванных сертификатов в среде «Active Directory»

1. Перейдите в настройки обновления LDAP ЦСК «CryptoKDC» (Инструменты-Настройка-LDAP-Обновления);
2. В строке путей размещения COC введите желаемый путь для списка отозванных сертификатов (путь задается по аналогии с путем пользователя для LDAP);
3. Нажмите создать. Если путь и настройки введены верно, будет создан путь размещения для списка отозванных сертификатов (Рисунок 3).

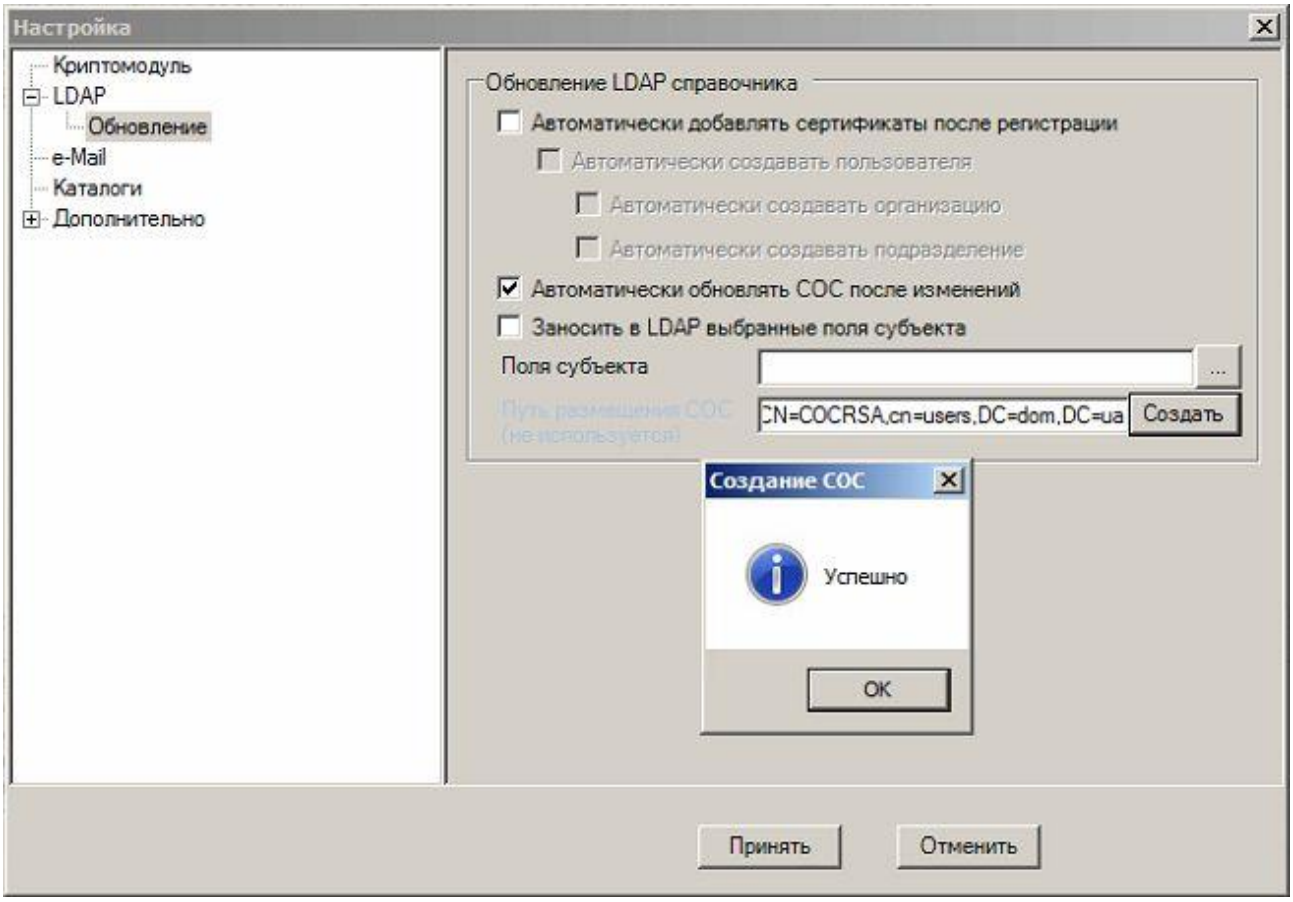

Рисунок 3

1.3 Публикация списка отозванных сертификатов в LDAP «Active Directory»

Также для того чтобы ЦСК «CryptoKDC» начал публиковать COC в LDAP «Active Directory» и записывать эти пути в сертификат, нужно указать соответствующий путь в конфигурационном файле «CryptoProviders.xml».

1. Закройте ПО ЦСК «CryptoKDC» и остановите службу «CA Logic Core»;
2. Откройте папку с серверной частью ПО ЦСК «CryptoKDC»;
3. Найдите конфигурационный файл «CryptoProviders.xml» и нажмите изменить;
4. Добавьте пути для публикации COC в Active Directory (путь аналогичен тому, который был задан на этапе создания путей для COC в настройках LDAP (см. п. 1.2.2), Рисунок 4);

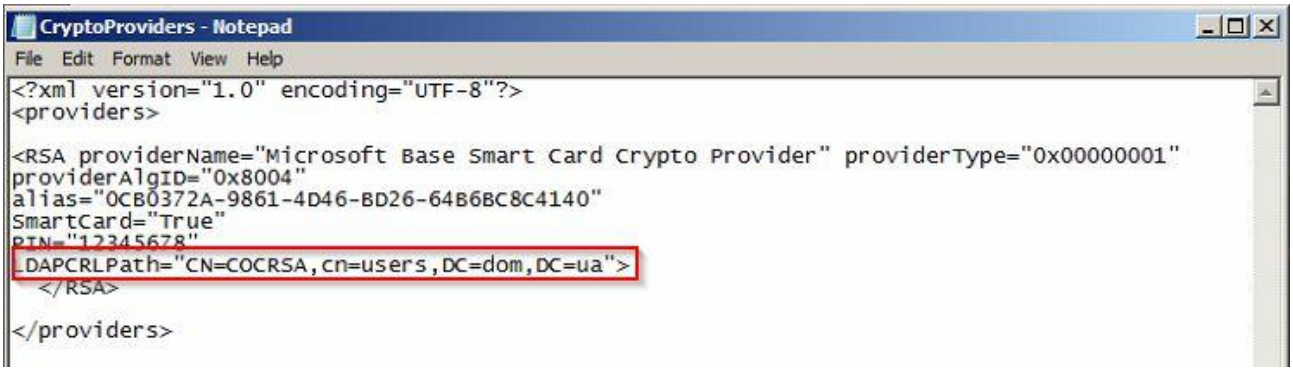

Рисунок 4

5. Добавьте пути СОС для записи их в выдаваемые сертификаты (Рисунок 5) – запись вида:

<CRLPoint>ldap:///CN=COCSA,cn=users,DC=dom,DC=ua?certificateRevocationList?base?objectClass=cRLDistributionPoint</CRLPoint>

Рисунок 5

6. Сохраните изменения и запустите службу «CA Logic Core»;
7. Если все сделано правильно, то при обновлении СОС ПО ЦСК «CryptoKDC» будет публиковать СОС в LDAP «Active Directory», а в выдаваемых шаблонах будут указаны пути к СОС.

2 Внедрение корневого сертификата ПО ЦСК «CryptoKDC» в домен

Для входа в систему по смарт-картам нужно добавить корневой сертификат центра сертификации к доверенным корневым центрам в объект групповой политики службы «Active Directory» и добавить сторонние выпускающие центры сертификации в хранилище «NTAuth» службы «Active Directory».

2.1 Добавление корневого сертификата центра сертификации в «Active Directory»

1. На контроллере домена: нажмите кнопку **Пуск**, выберите последовательно пункты **Administrative Tools**, а затем **Group Policy Management**;
2. На левой панели найдите домен, к которому относится политика, требующая изменения;
3. Нажмите правой кнопкой мышки по «**Default Domain Policy**» и нажмите «**Edit» (**Рисунок 6**);**

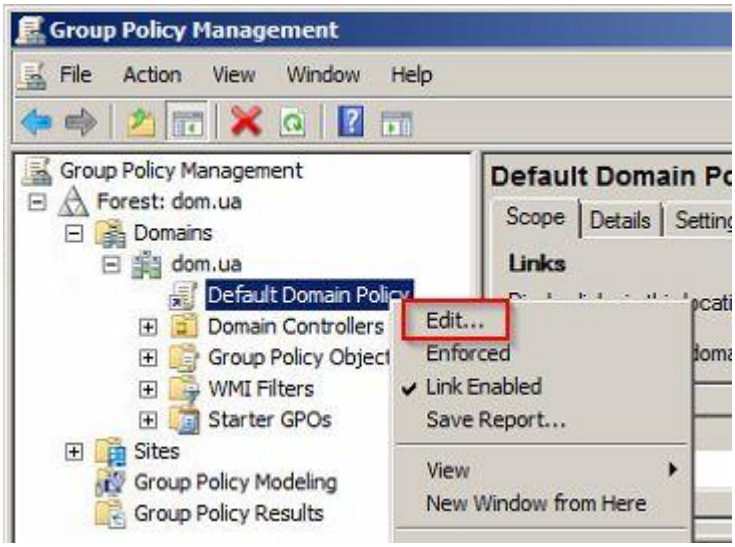

Рисунок 6

4. В левой области в **Computer Configuration** разверните следующие пункты:
   - Policies;
   - Windows setting;
   - Security setting;
   - Public Key Policies.
5. Нажмите правой кнопкой мышки по меню «**Trusted Root Certification Authorities»** и нажмите «**import»**;
6. Импортируйте корневой сертификат ПО ЦСК «CryptoKDC» (сертификат должен быть заранее перенесен на контроллер домена любым удобным способом), следуя указаниям мастера;
7. Закройте окно **Group Policy Management**.

2.2 Добавление сертификата центра сертификации в хранилище «NTAuth «службы «Active Directory»

Запустите командную строку и выполните команду: **certutil -dspublish -f C:\CAroot.crt NTAuthCA**

Где C:\CAroot.crt путь к корневому сертификату ЦСК и его название (для успешного выполнения команды администратор должен входить в группу администраторов предприятия). Если команда выполнена верно, появится соответствующее сообщение (Рисунок 7).

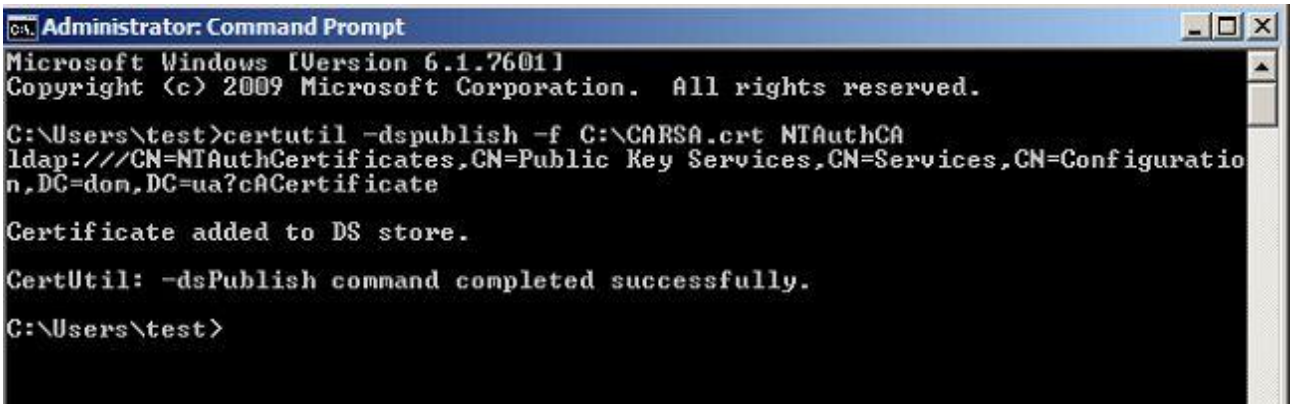

Рисунок 7

3 Создание сертификата для контроллера домена

Для создания сертификата контроллера домена, нужно выдать на контроллере запрос на сертификат и удостоверить его в ЦСК, по шаблону «DomainController».

3.1 Создание запроса на сертификат по шаблону «DomainController»

Для того чтобы при генерации запроса на сертификат в списке шаблонов отображался шаблон «DomainController», нужно на контроллере домена в разделе «Feature(компоненты)» добавить средства служб сертификации Active Directory.

3.1.1 Добавление средств сертификации Active Directory.

1. На контроллере домена откройте **Server Manager;**
2. Перейдите на вкладку **«features»** и нажмите **«Add Features»;**
3. Откройте вкладку «**Remote Server Administration Tools»** и найдите и установите «**Certification Authority Tools»(**Рисунок 8**) .**

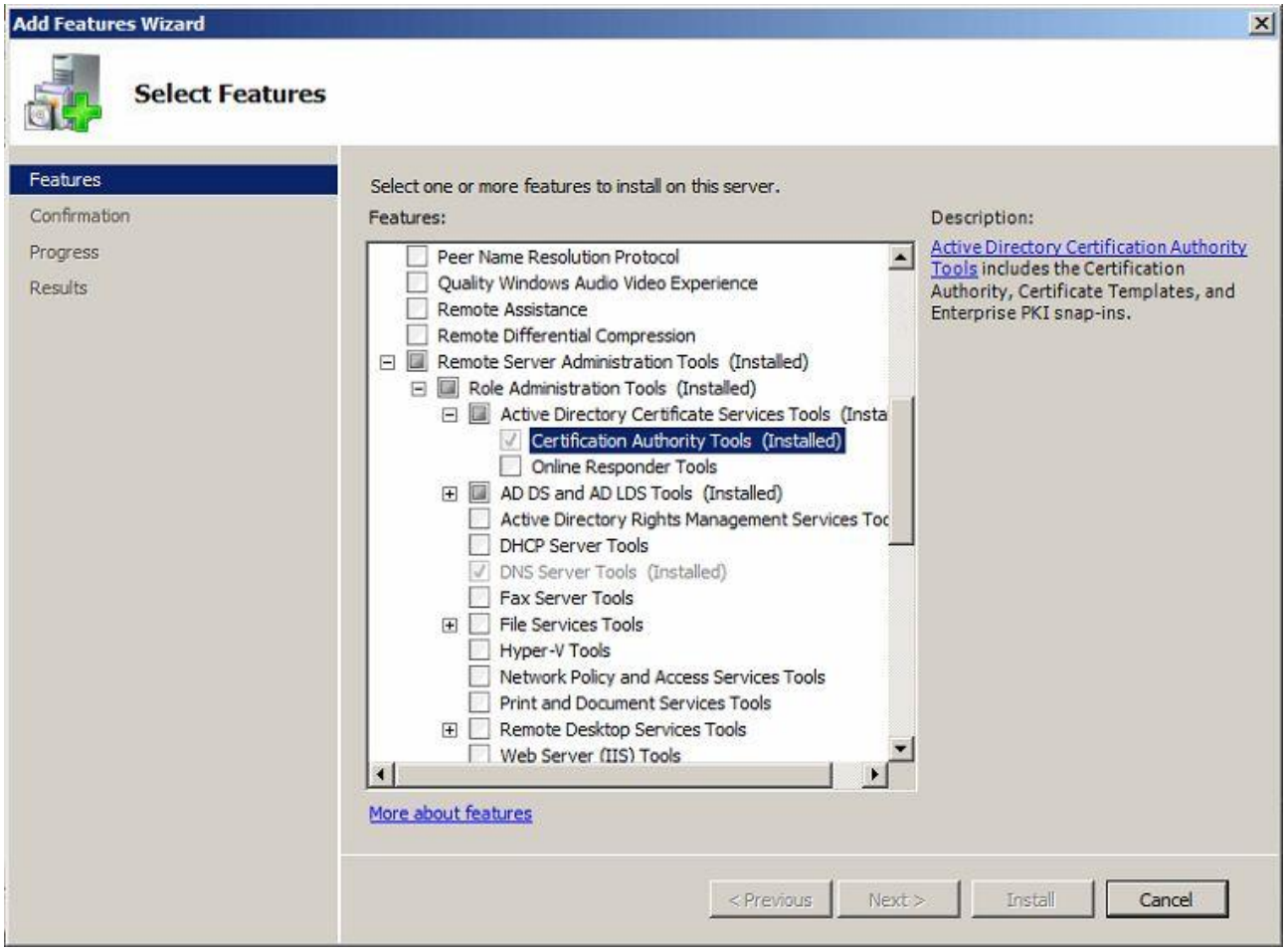

Рисунок 8

3.1.2 Создание запроса на сертификат, по шаблону «DomainController»

Для успешного выполнения данного пункта администратор должен входить в группу администраторов предприятия.

1. На контроллере домена, в меню пуск нажмите **«выполнить»(Run)** и введите команду **«mmc»;**
2. В появившемся окне нажмите **«File»** и выберите **«Add/Remove snap-in»;**
3. Найдите оснастку **«Certificate»** и нажмите **«Add»;**
4. Установите чек бокс на пункт «Computer account» и нажмите **«Next»;**
5. В следующем окне нажмите **«Finish»;**
6. В следующем окне нажмите **«OK»;**
7. В появившейся оснастке последовательно перейдите в **«Certificates»-«Personal,** нажав правой кнопкой мышки, последовательно выберите **«All Task»-«Advanced Operations»-«Create Custom Request…» (**Рисунок 9**);**

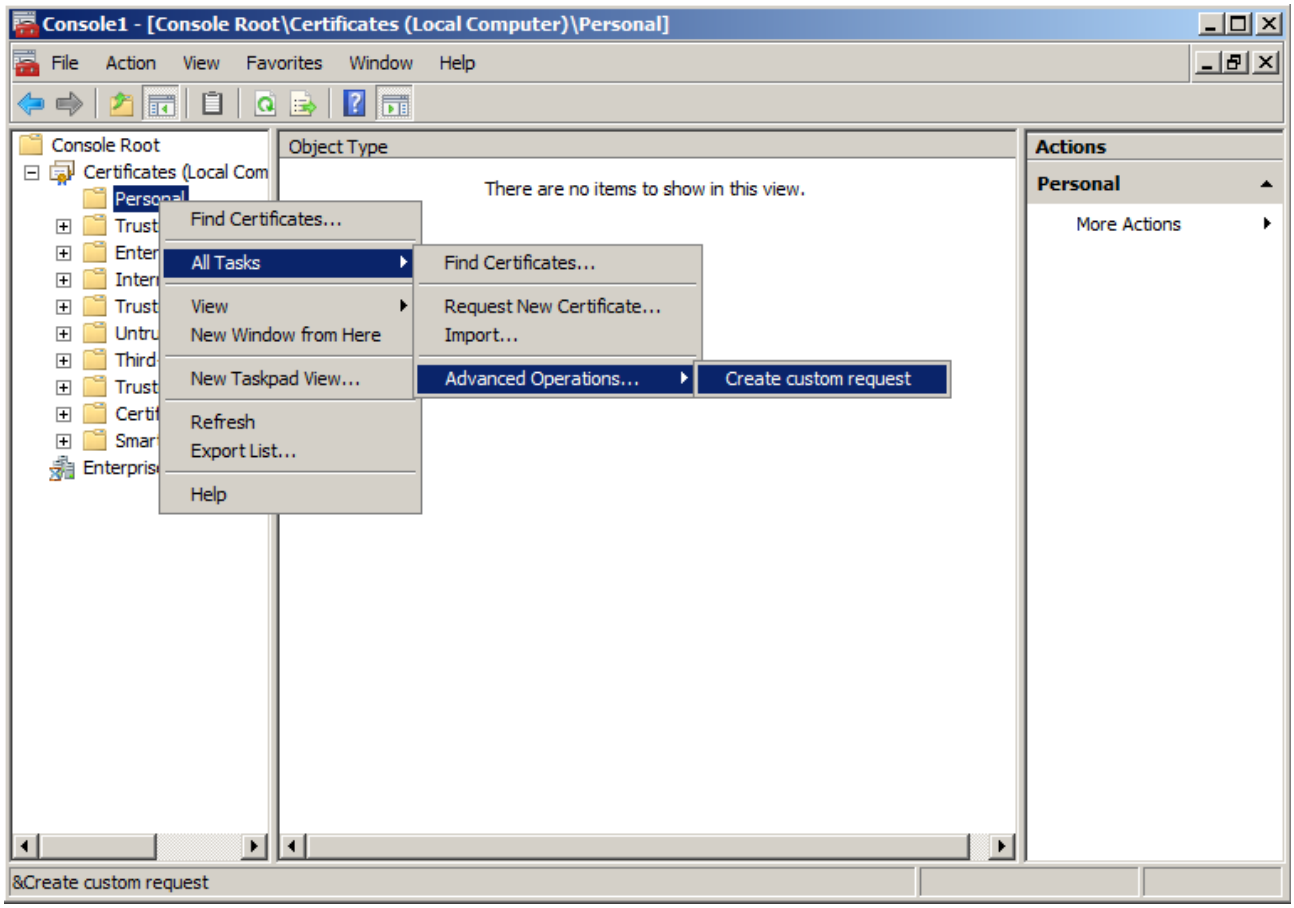

Рисунок 9

8. В появившемся окне **«Certificate Enrollment»** нажмите **«Next»;**
9. В следующем окне нажмите **«Next»;**
10. В следующем окне выберите из списка шаблонов **«Domain Controller»** , в качестве формата выберите **«PKCS #10»** и нажмите **«Next»;**
11. В следующем окне нажмите **«Next»;**
12. В окне сохранения выберите файл формата «Base 64» и укажите путь сохранения и название запроса. Нажмите кнопку «Finish»;

13. Найдите сохраненный запрос и измените ему разрешение на «р.10»;
14. Перенесите запрос любым удобным способом на машину с ПТК ЦСК.

3.2 Создание сертификата для контроллера домена из созданного запроса

В зависимости от регламента работы ЦСК, администратору регистрации и/или администратору безопасности и/или администратору сертификации ЦСК необходимо выполнить следующие действия:

1. В Центре сертификации создать пользователя для контроллера домена;
   Для пользователя добавить параметр DNSName и указать ему значение имени контроллера домена вида «ComputerName.domain». Для этого необходимо на вкладке «ФИО» окна «Данные пользователя» нажать кнопку «Дополнительно…» и в появившемся окне ввести необходимые данные (Рисунок 10). Нажать кнопку «Добавить», затем кнопку «Принять»;

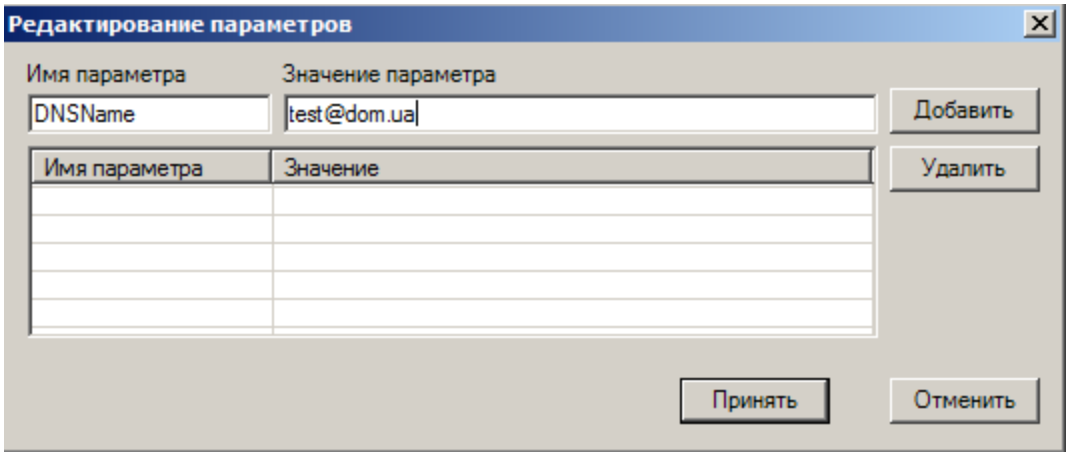

Рисунок 10

2. Создать шаблон сертификата (DomainController.xml), который будет отвечать требованиям политик домена;

Пример шаблона:

```
<?xml version="1.0" encoding="UTF-8"?>
<template name="DomainController" visibleName="DomainController"
visible="True" priority="10">
  <subject usePrevious="False">
  </subject>
  <extensions usePrevious="False">
    <IssuerKeyIdentifier usePrevious="False" critical="False" />
    <SubjectKeyIdentifier usePrevious="False" critical="False"
typeGenerate="0" />
    <KeyUsages usePrevious="False" critical="True"
mandatory="KeyUsages!">
      <value>160</value>
    </KeyUsages>
```

```
    <ExtendedKeyUsage usePrevious="False" critical="False"
mandatory="ExtendedKeyUsage!">
       <oid>1.3.6.1.5.5.7.3.1</oid>
       <oid>1.3.6.1.5.5.7.3.2</oid>
    </ExtendedKeyUsage>
    <Custom oid="1.3.6.1.4.1.311.20.2" usePrevious="False"
critical="False" mandatory="!">
      <x1E><sunicode>DomainController</sunicode></x1E>
    </Custom>
    <Custom oid="1.2.840.113549.1.9.15" usePrevious="False"
critical="False" mandatory="!">
      <x30><x>30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 00 80 30 0E
06 08 2A 86 48 86 F7 0D 03 04 02 02 00 80 30 0B 06 09 60 86 48 01
65 03 04 01 2A 30 0B 06 09 60 86 48 01 65 03 04 01 2D 30 0B 06 09
60 86 48 01 65 03 04 01 02 30 0B 06 09 60 86 48 01 65 03 04 01 05
30 07 06 05 2B 0E 03 02 07 30 0A 06 08 2A 86 48 86 F7 0D 03
07</x></x30>
    </Custom>
    <Custom oid="2.5.29.31" usePrevious="False" critical="False"
mandatory="!">
          <x30>
               <x30>
                    <xA0>
                         <xA0>
                              <x86>
                                   <p>CRLPoint</p>
                              </x86>
                         </xA0>
                    </xA0>
               </x30>
          </x30>
    </Custom>
    <Custom oid="2.5.29.17" usePrevious="False" critical="False"
mandatory="!">
      <x30>
          <x82><p>DNSName</p></x82>
       </x30>
    </Custom>
 </extensions>
 </template>
```

3. Разместить СОС средствами ЦСК в Active Directory (LDAP-каталог);
4. Положить созданный шаблон в каталог «Templates», путь по умолчанию на сервере ЦСК «C:\Program Files\Author\Центр Сертификации\Templates»;
5. Выбрать созданного пользователя и создать ему заказ на сертификат, по шаблону «ControllerDomain»;

6. Перейти на вкладку **«Заказы»,** выбрать созданный заказ, открыть его контекстное меню правой кнопкой мыши и выбрать пункт **«Зарегистрировать запрос из файла»;**
7. В качестве запроса выбрать запрос, который был создан на предыдущем этапе (см. п.3.1.2, шаг 14);
8. Перейти в меню «запросов» и удостоверить созданный на предыдущем этапе запрос;
9. Перейти на вкладку **«Сертификаты»** и сохранить созданный сертификат в любое удобное место;
10. Перенести созданный сертификат на контроллер домена любым удобным способом;
11. На контроллере домена, в меню пуск нажмите **«Выполнить»(Run)** и введите команду **«mmc»;**
12. В появившемся окне нажмите **«File»** и выберите **«Add/Remove snap-in»;**
13. Найдите оснастку **«Certificate»** и нажмите **«Add»;**
14. Установите флажок на пункт «Computer account» и нажмите **«Next»;**
15. В следующем окне нажмите **«Finish»;**
16. В следующем окне нажмите **«ОК»;**
17. В появившейся оснастке последовательно перейдите в «Certificates»-«Personal», нажав правой кнопкой мышки, последовательно выберите **«All Task»-«Import»;**
18. Импортируйте созданный сертификат контроллера домена, следуя указаниям мастера.

4 Выдача сертификата для входа по смарт-картам пользователю в домене

1. Создать шаблон сертификата (UserDomainShablon.xml), который будет отвечать требованиям политик домена;

Пример шаблона:

```
<?xml version="1.0" encoding="UTF-8"?>
<template name="UserDomain" visibleName="UserDomain" visible="True"
priority="10">
  <extensions usePrevious="False">
   <IssuerKeyIdentifier usePrevious="False" critical="False" />
    <SubjectKeyIdentifier usePrevious="False" critical="False"
typeGenerate="0" />
    <KeyUsages usePrevious="False" critical="True"
mandatory="KeyUsages!">
      <value>160</value>
   </KeyUsages>
    <ExtendedKeyUsage usePrevious="False" critical="True"
mandatory="ExtendedKeyUsage!">
      <oid>1.3.6.1.5.5.7.3.4</oid>
      <oid>1.3.6.1.5.5.7.3.2</oid>
       <oid>1.3.6.1.4.1.311.20.2.2</oid>
    </ExtendedKeyUsage>
    <Custom oid="1.2.840.113549.1.9.15" usePrevious="False"
critical="False" mandatory="!">
```

```
      <x30><x>30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 00 80 30 0E
06 08 2A 86 48 86 F7 0D 03 04 02 02 00 80 30 07 06 05 2B 0E 03 02
07 30 0A 06 08 2A 86 48 86 F7 0D 03 07</x></x30>
    </Custom>
    <Custom oid="1.3.6.1.4.1.311.20.2" usePrevious="False"
critical="False" mandatory="!">
      <x1E><sunicode>SmartcardUser</sunicode></x1E>
    </Custom>
    <Custom oid="2.5.29.31" usePrevious="False" critical="False"
mandatory="!">
          <x30>
               <x30>

               <xA0>

                         <xA0>
                              <x86>
                                   <p>CRLPoint</p>
                              </x86>
                         </xA0>
                    </xA0>
               </x30>
          </x30>
    </Custom>
    <Custom oid="1.3.6.1.5.5.7.1.1" usePrevious="False"
critical="False" mandatory="!">
      <x30>
          <x30>
            <o>1.3.6.1.5.5.7.48.2</o>
            <x86>
                 <p>CAPoint</p>
            </x86>
          </x30>
       </x30>
   </Custom>
    <Custom oid="2.5.29.17" usePrevious="False" critical="False"
mandatory="!">
      <x30>
         <xA0>
            <o>1.3.6.1.4.1.311.20.2.3</o>
            <xA0>
              <x0C><p>name</p></x0C>
            </xA0>
          </xA0>
       </x30>
    </Custom>
 </extensions>
 </template>
```

2. Разместить СОС средствами ЦСК в Active Directory (LDAP-каталог);
3. Положить созданный шаблон в каталог «Templates», путь по умолчанию на сервере ЦСК «C:\Program Files\Author\Центр Сертификации\Templates»;
4. На контроллере домена в «Пуск» - «Администрирование» - «Active Directory – пользователи и компьютеры» создать пользователя, которому будет выдан сертификат на НКИ;
5. В Центре сертификации создать пользователя с такими же параметрами (Рисунок 11). Обязательным является заполнение дополнительного параметра «Name» («Данные пользователя» – «Дополнительно…») в формате авторизации в домен (логин@домен);

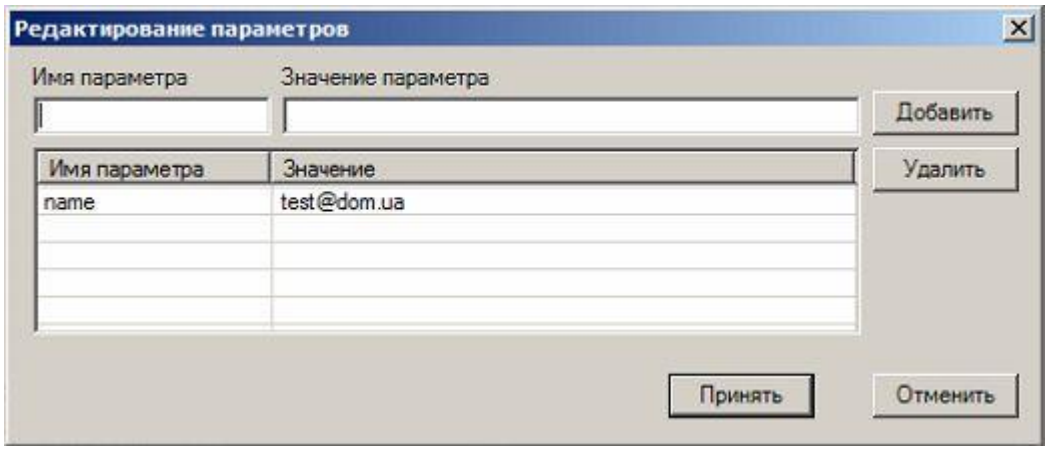

Рисунок 11

6. Выдать пользователю на НКИ сертификат по шаблону «UserDomainShablon.xml»;
7. Перезагрузить контроллер домена и рабочее место пользователя;
8. Войти в систему с помощью смарт-карты.