

Средство защиты информации от несанкционированного доступа
«Блокхост-Сеть 4»

Руководство администратора безопасности
Часть 3. Настройка подсистемы управления токенами, ЦС Microsoft CA

Аннотация

В документе содержатся сведения об установке и настройке подсистемы управления жизненным циклом токенов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4» при взаимодействии с центром сертификации Microsoft CA и сервисом каталогов Active Directory, а также сведения о настройке сертификатов, необходимых для функционирования подсистемы.

Содержание

Введение	5
1 Подсистема жизненного цикла токенов	6
2 Настройки на контроллере домена	8
3 Настройки центра сертификации	12
3.1 Сертификат агента регистрации	12
3.2 Сертификат пользователя	22
4 Настройки на сервере «Блокхост-Сеть»	31
4.1 Выпуск и установка сертификата агента регистрации	31
4.2 Создание профилей в настройках подсистемы	34
4.2.1 Создание профиля Microsoft CA	35
4.2.2 Добавление прокси-клиента для взаимодействия с ЦС	41
5 Особенности при выпуске токена средствами подсистемы	47
6 Настройка прозрачного входа в RDGW	48
7 Настройка входа по сертификатам ЦС Microsoft CA в ОС Linux	49
7.1 Приоритет проверок средств аутентификации при входе	49
7.2 Ввод рабочей станции ОС Linux в домен AD	49
7.2.1 Ввод рабочей станции под управлением ОС Альт в домен Active Directory	49
7.2.2 Ввод рабочей станции под управлением ОС Astra Linux в домен Active Directory	51
7.2.3 Ввод рабочей станции под управлением РЕД ОС в домен Active Directory	53
7.3 Порядок настройки для входа по сертификатам в ОС Linux	55
7.3.1 Экспорт корневого сертификата AD	55
7.3.2 Запуск задачи по настройке входа по сертификату через подсистему разворачивания	57
7.4 Особенности при входе в ОС Альт по сертификатам MS CA	64
7.5 Особенности при входе в ОС Astra Linux с настроенным входом по сертификатам	67
7.6 Удаление сертификата из Active Directory пользователя	67
7.7 Настройка публикации списка отзыва сертификатов в ОС Linux	68
7.7.1 Настройки центра сертификации	68
7.7.2 Настройки на контроллере домена	75

7.7.3	Публикация списка отзывов	87
7.8	Настройка подключения к домену из консоли управления по протоколу <i>ldaps</i> с установкой ssl-сертификатов	88
7.8.1	Настройка контроллера домена AD.....	89
7.8.2	Настройка контроллера домена Samba	97
7.8.3	Настройка контроллера домена FreeIPA.....	99
7.8.4	Настройки на рабочей станции ОС Windows с установленной консолью управления	99
7.8.5	Настройки на рабочей станции ОС Linux с установленной консолью управления	99
7.8.6	Проверка работоспособности подключения	101
7.8.7	Особенности при настройке AD для подключения по <i>ldaps</i> из ОС AstraLinux 1.7 ..	101
	Перечень сокращений	104

Введение

Подсистема управления жизненным циклом токенов предназначена для управления носителями пользователей на протяжении всего жизненного цикла.

Для настройки и установки подсистемы управления жизненным циклом токенов в существующей иерархической структуре уже должны быть развернуты следующие компоненты:

- служба каталога Active Directory;
- центр сертификации (Microsoft Enterprise CA), принадлежащий тому же домену Active Directory, в котором будет развернута подсистема управления жизненным циклом токенов.

Знаки, расположенные на полях руководства, указывают на примечания.

Степени важности примечаний:



Важная информация

Указания, требующие особого внимания.



Дополнительная информация

Указания, позволяющие упростить работу с подсистемой.

1 Подсистема жизненного цикла токенов

Подсистема предназначена для управления устройствами аутентификации пользователей на протяжении всего жизненного цикла и обеспечивает учет токенов в системе, управление токенами и аудит в течении всего жизненного цикла.

Подсистема жизненного цикла токенов поддерживает управление токенами перечисленными в таблице 1.1.

Таблица 1.1 – Поддерживаемые подсистемой токены

Носитель	Производитель	Наименование носителя	
		поддерживаемые ОС Windows	поддерживаемые ОС Linux
eToken	ЗАО «АЛАДДИН Р.Д.»	eToken Pro, eToken Pro (Java), eToken ГОСТ, eToken NG-FLASH, eToken NG-FLASH (Java), eToken NG-OTP, eToken NG-OTP (Java), eToken GT (Java), eToken PRO (Java) SC, eToken PRO SC	
SafeNet eToken	ООО «Сертифицированные информационные системы»	SafeNet eToken 5100, SafeNet eToken 5105, SafeNet eToken 5200, SafeNet eToken 5205, SafeNet eToken 7200, SafeNet eToken 7300, SafeNet eToken 4100	
Рутокен	ЗАО «Актив Софт»	Рутокен, Рутокен S, Рутокен Lite, Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 3.0	Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 3.0
JaCarta	ЗАО «АЛАДДИН Р.Д.»	JaCarta-2, JaCarta PKI, JaCarta PRO	JaCarta-2, JaCarta PKI, JaCarta PRO
eSmart Token	ООО «Интеллектуальные системы управления бизнесом»	eSmart Token	eSmart Token

Для работы с сертификатами на токене в подсистеме жизненного цикла токенов необходимо выполнить определенные настройки на контроллере домена, центре сертификации и в самой подсистеме жизненного цикла токенов.

- Если на клиентских ОС Windows не хватает компонентов для отзыва сертификатов. Для корректного функционирования подсистемы под управлением клиентских ОС необходимо поставить обновление «Remote Server Administration Tools» (установка «Remote Server Administration Tools» необходима только для ОС Windows 7, 8.1, 10 (до версии 1903) и включить компонент **«Средства служб сертификации»**:
- для ОС Windows 7 "Remote Server Administration Tools for Windows 7" (<https://www.microsoft.com/en-us/download/details.aspx?id=7887>);
 - для ОС Windows 8.1 "Remote Server Administration Tools for Windows 8.1" (<https://www.microsoft.com/en-us/download/details.aspx?id=28972>);
 - для ОС Windows 10 до версии 1903 "Remote Server Administration Tools for Windows 10" (<https://www.microsoft.com/en-us/download/details.aspx?id=45520>).¹
- При выдаче токена *Рутокен ЭЦП* для входа по сертификату на сервере под управлением ОС Linux, вход в ОС Windows по такому токену будет невозможен, т.к. производитель не поддерживает данную возможность.

¹ В ОС Windows 10 версии 1903 и выше обновление «Remote Server Administration Tools» уже установлено по умолчанию. Включение компонента **«Средства служб сертификации»** доступно в пункте «Панель управления» → «Программы» → «Включение или отключение компонентов Windows».

2 Настройки на контроллере домена

Для первоначальной настройки подсистемы жизненного цикла токенов необходимо создать сервисную учетную запись, обладающую достаточными правами для создания сертификата и входящую в группу пользователей домена.

- Сервисная учетная запись должна принадлежать тому же домену, что и центр сертификации.

Для создания сервисной учетной записи (например, **serviceCA**) откройте окно оснастки **Active Directory – Пользователи и компьютеры (Active Directory Users and Computers)** (рисунок 2.1).

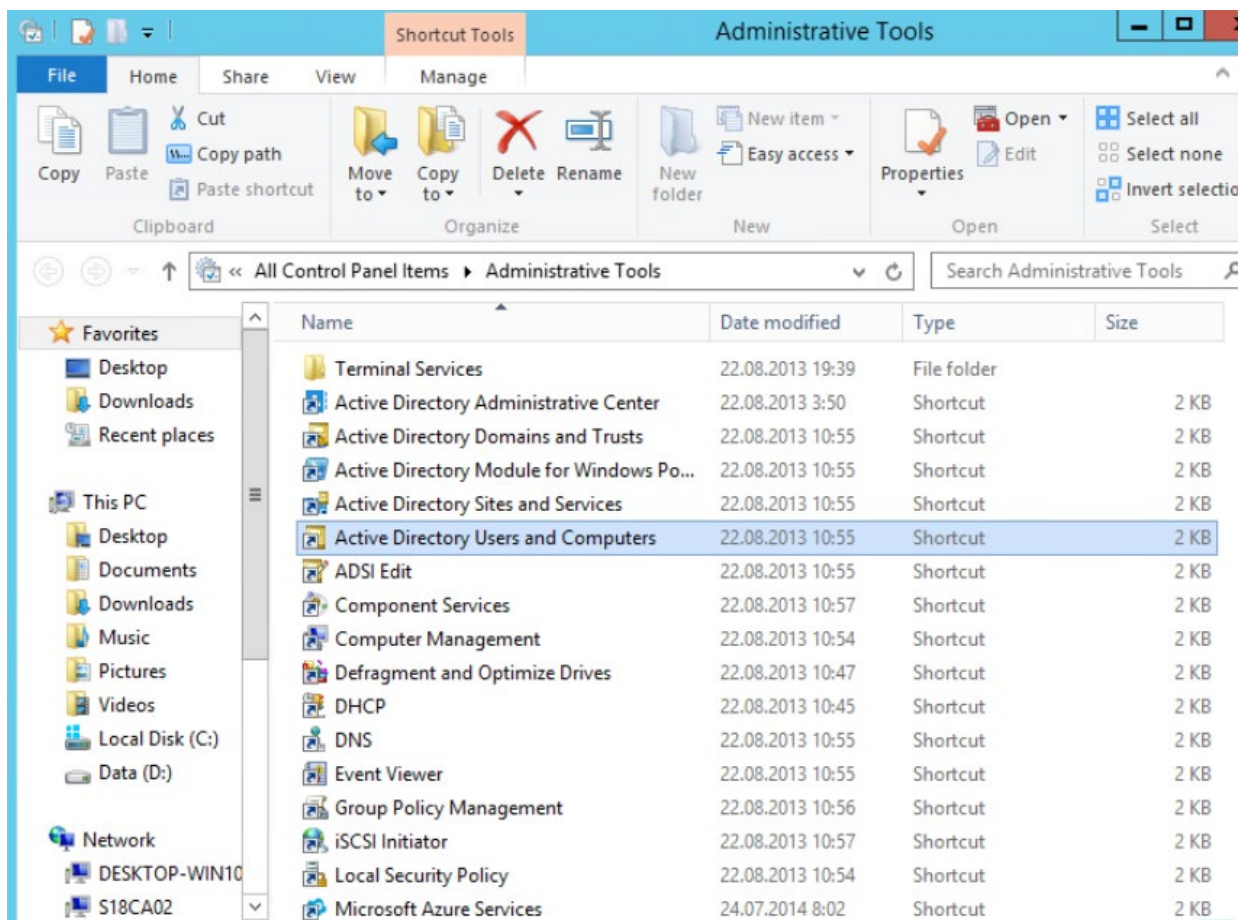


Рисунок 2.1 – Переход к оснастке **Active Directory Users and Computers**

Окно будет иметь следующий вид:

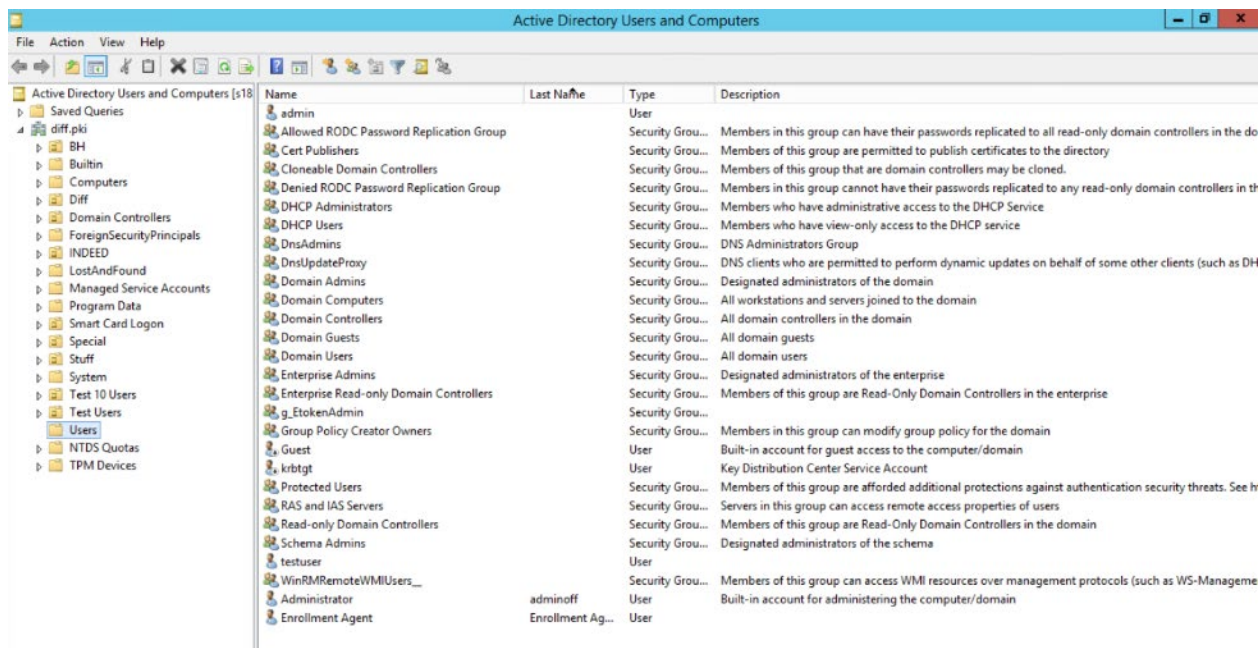


Рисунок 2.2 – Оснастка **Active Directory Users and Computers**

Создайте организационное подразделение (Organizational Unit — OU) издателей сертификатов для работы с выпуском сертификатов подсистемой жизненного цикла токенов (например, на рисунке 2.3 OU **Special**) и создайте группу издателей сертификатов (например, **CertIssuers**) по щелчку правой кнопки мыши **Создать (New)** → **Группа (Group)**.

Создайте сервисную учетную запись по щелчку правой кнопки мыши **Создать (New)** → **Пользователь (User)**. Отобразится окно для ввода данных создаваемой учетной записи пользователя (рисунок 2.3).

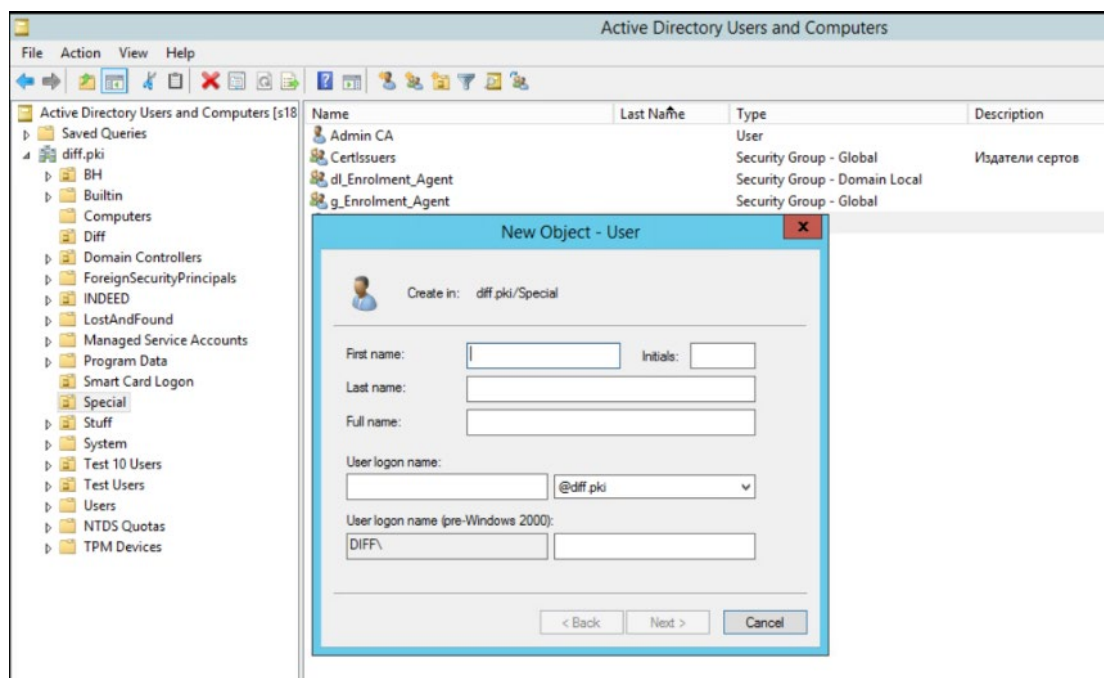


Рисунок 2.3 – Создание сервисной учетной записи

Введите все необходимые данные и нажмите **Далее (Next)**.

В появившемся окне введите пароль создаваемой сервисной учетной записи и подтвердите его в соответствующем поле, и установите параметры **Запретить смену пароля пользователя (User cannot change password)** и **Срок действия пароля не ограничен (Password never expires)** (рисунок 2.4).

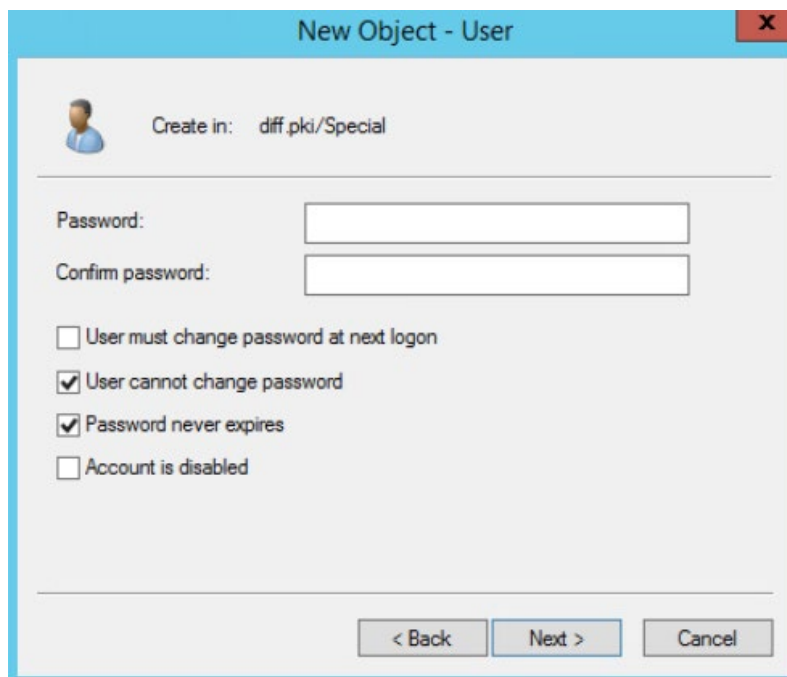


Рисунок 2.4 – Ввод пароля для создаваемой сервисной учетной записи

Нажмите на кнопку **Готово (Finish)** (рисунок 2.5).

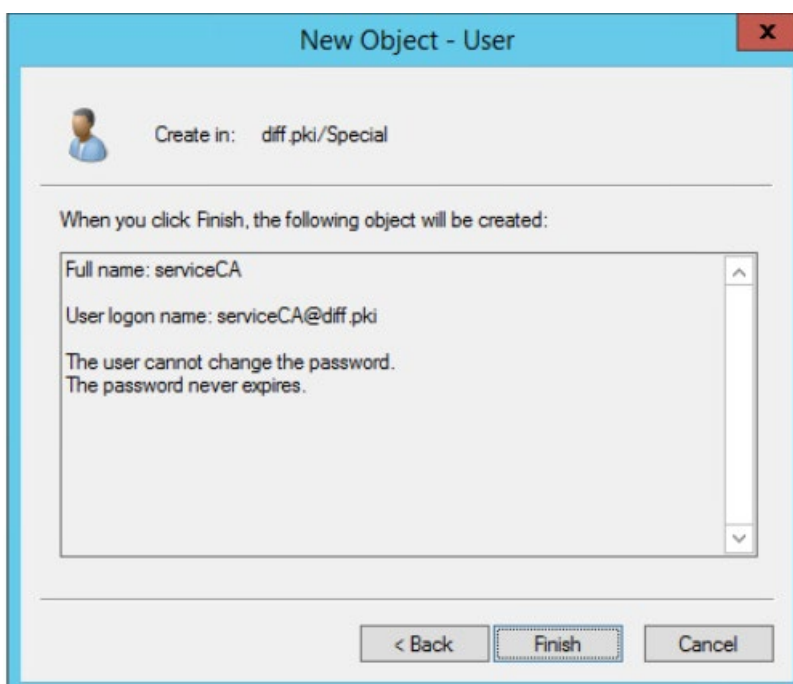


Рисунок 2.5 – Завершение создания сервисной учетной записи

В оснастке **Active Directory – пользователи и компьютеры** щелкните правой кнопкой на имени созданной учетной записи и выберите **Свойства (Properties)**.

Перейдите во вкладку **Член групп (Member of)** и проверьте принадлежность учетной записи группе пользователей домена (**Domain Users**) и созданной группе издателей сертификатов (**CertIssuers**, OU **Special**) в соответствии с рисунком 2.6. При необходимости, добавьте учетную запись в данные группы по кнопке **Добавить (Add)**.

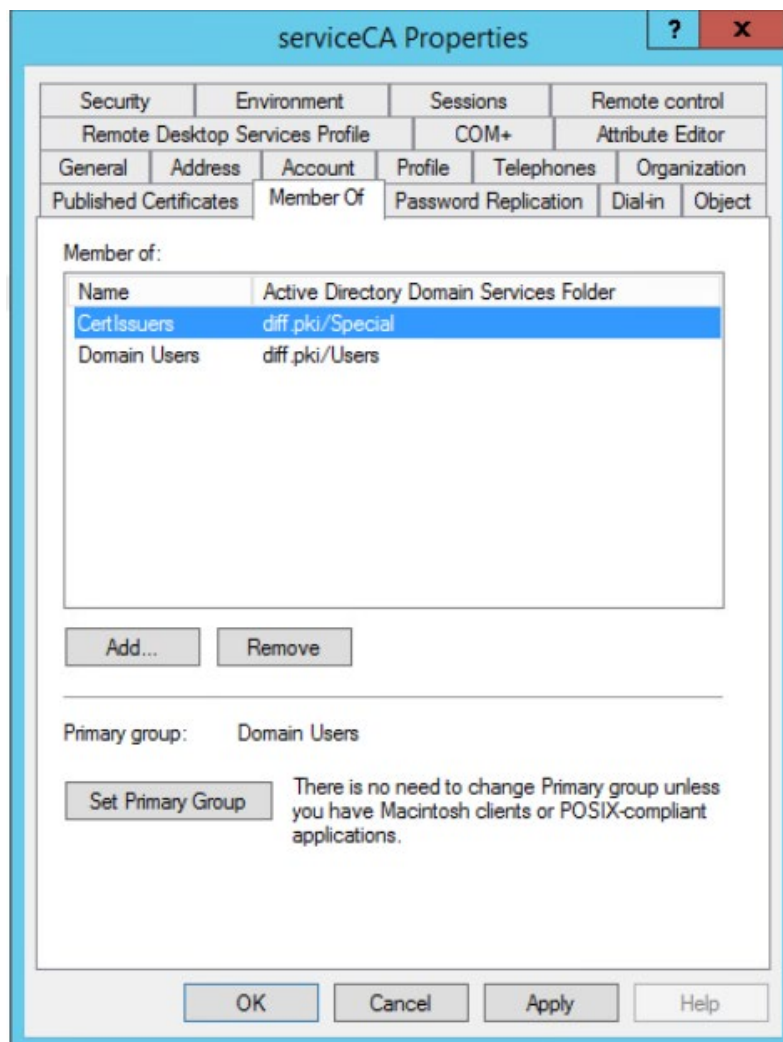


Рисунок 2.6 – Вкладка **Member of**

3 Настройки центра сертификации

3.1 Сертификат агента регистрации

Для выпуска пользовательских сертификатов на токене необходим сертификат, выпущенный по шаблону сертификата агента регистрации. В этом случае администратор может обращаться к центру сертификации для выпуска сертификатов пользователям.

Для создания шаблона запустите консоль центра сертификации с помощью команды **certsrv.msc** в командной строке (рисунок 3.1).

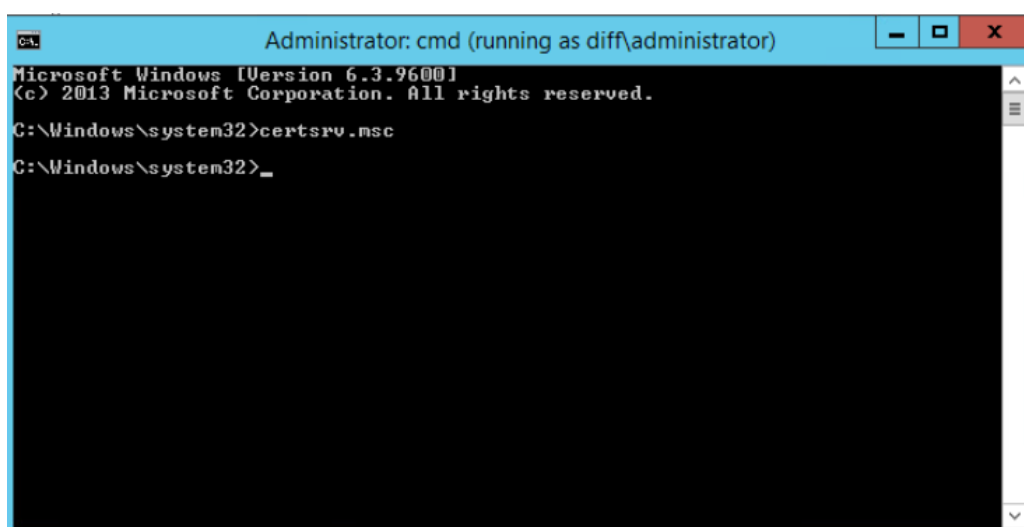


Рисунок 3.1 – Запуск консоли центра сертификации

- i** При возникновении ошибки вида, изображенного на рисунке 3.2, в появившейся консоли центра сертификации по щелчку правой кнопки мыши выберите **Перенацелить центр сертификации (Retarget Certification Authority)** (рисунок 3.3).

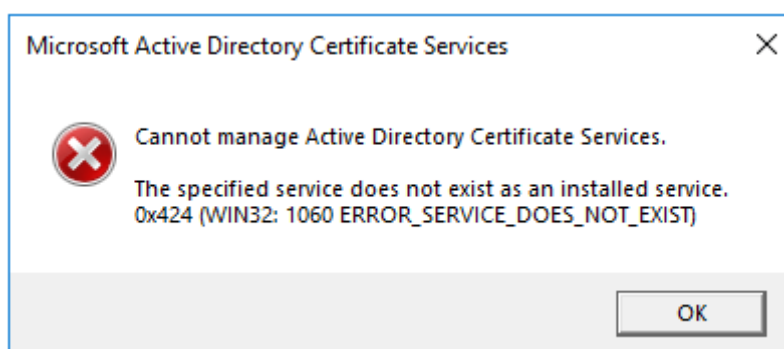


Рисунок 3.2 – Ошибка запуска консоли центра сертификации

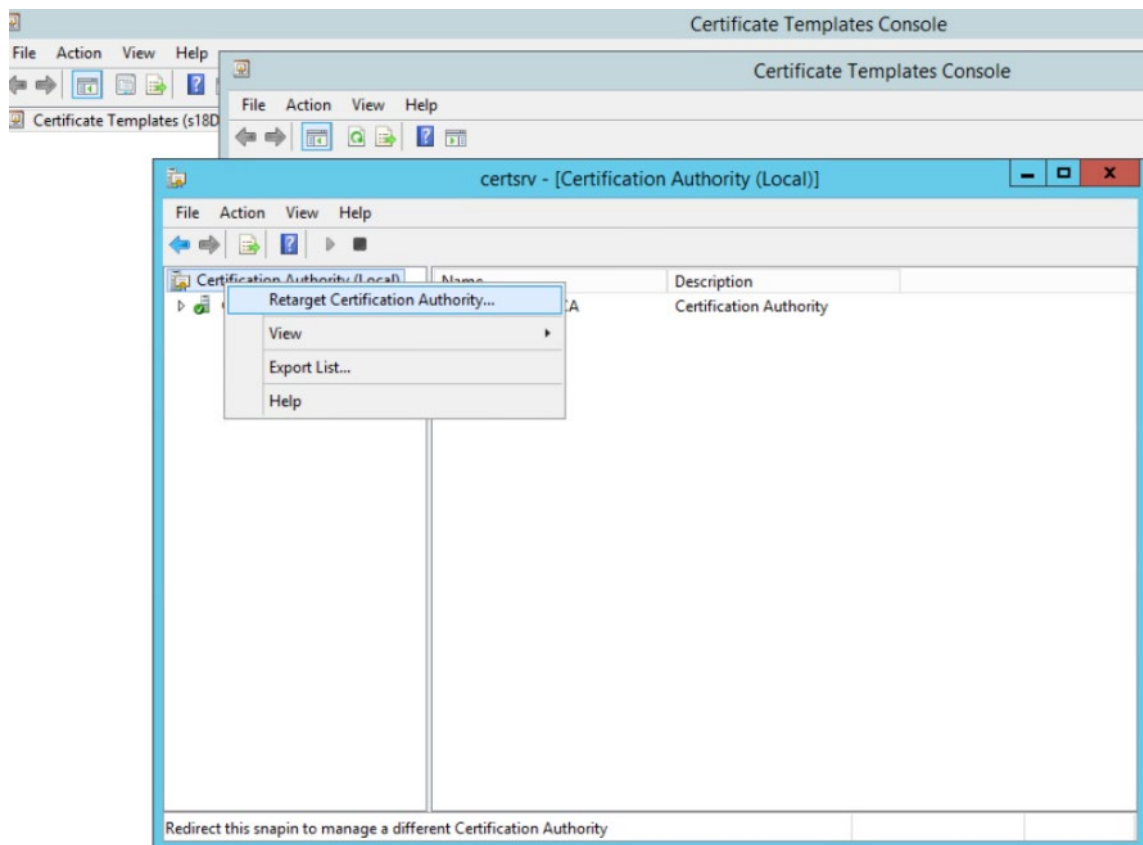


Рисунок 3.3 – Изменение центра сертификации

В появившемся окне установите параметр **Другим компьютером (Another computer)** (рисунок 3.4) и найдите необходимый центр сертификации (рисунок 3.5).

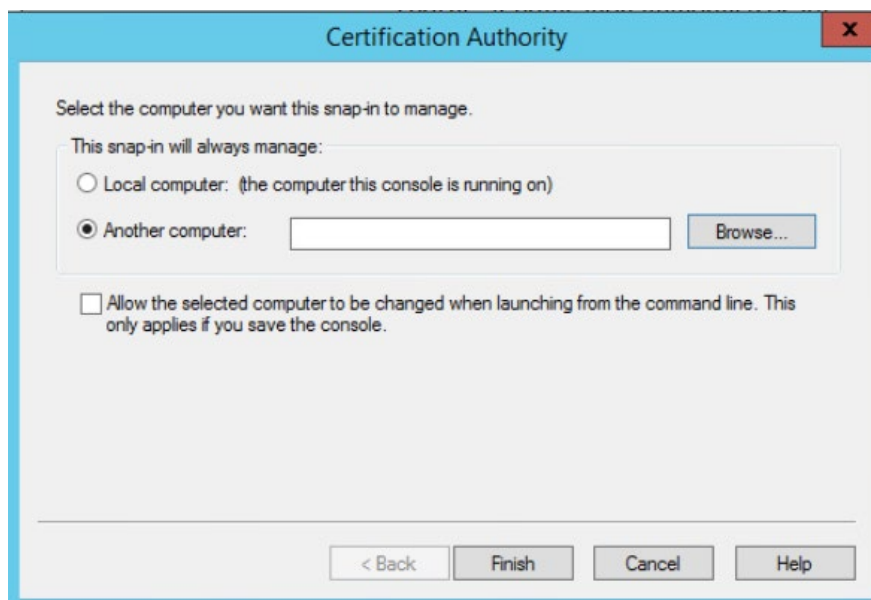


Рисунок 3.4 – Выбор центра сертификации



Рисунок 3.5 – Установка центра сертификации

Окно консоли будет выглядеть следующим образом:

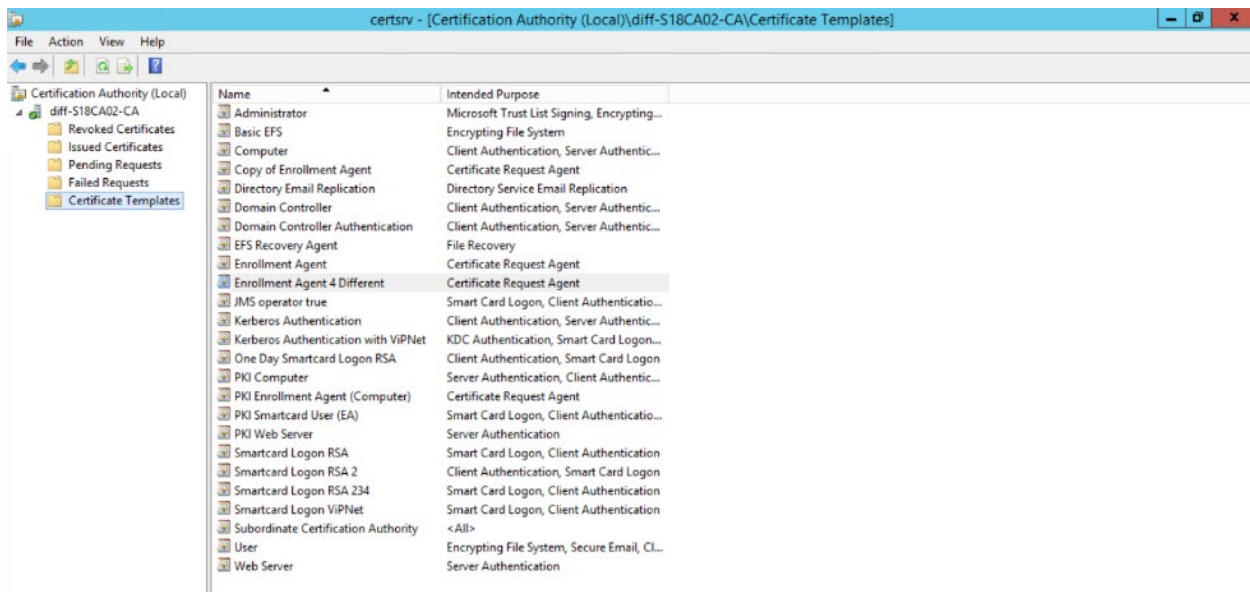


Рисунок 3.6 – Консоль центра сертификации

В левой части окна перейдите в свойства центра сертификации (**Properties**) по щелчке правой кнопки мыши (рисунок 3.7).

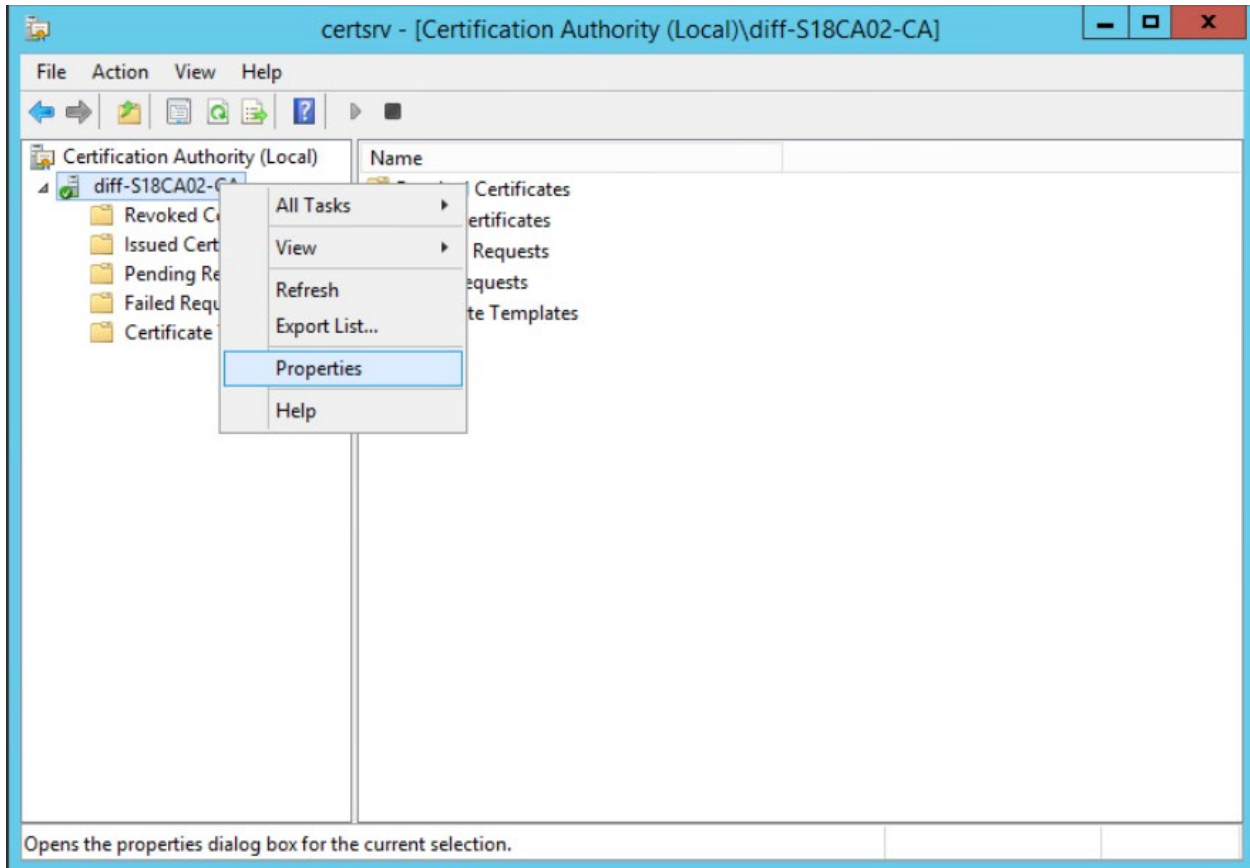


Рисунок 3.7 – Настройка свойств центра сертификации

Перейдите во вкладку **Безопасность (Security)** и по кнопке **Добавить (Add)** добавьте группу издателей сертификатов (рисунок 3.8), в которую входит созданная сервисная учетная запись (в примере, **CertIssuers**).

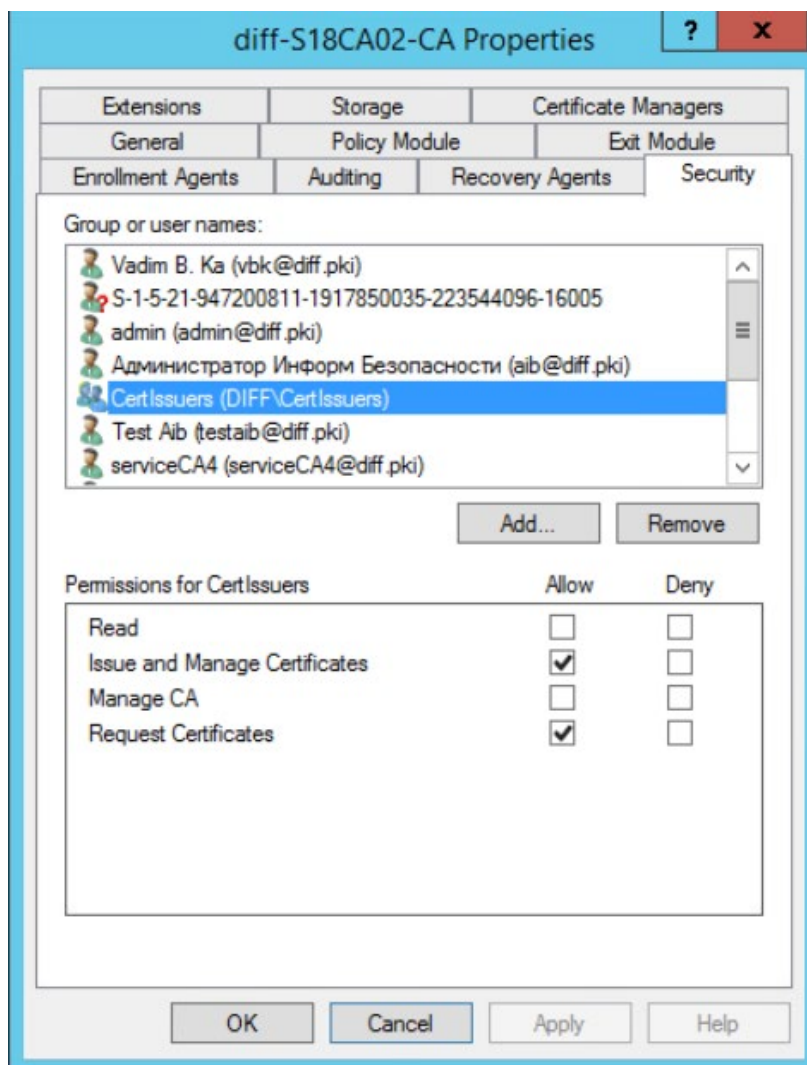


Рисунок 3.8 – Добавление разрешений для группы издателей сертификатов

Установите для группы разрешение **Выпуск и управление сертификатами (Issue and Manage Certificates)** и **Запросить сертификаты (Request Certificates)** и нажмите **ОК** (рисунок 3.8).

В левой части окна перейдите на пункт **Шаблоны сертификатов (Certificate Templates)**, щелкните правой кнопкой мыши и выберите **Управление (Manage)** (рисунок 3.9).

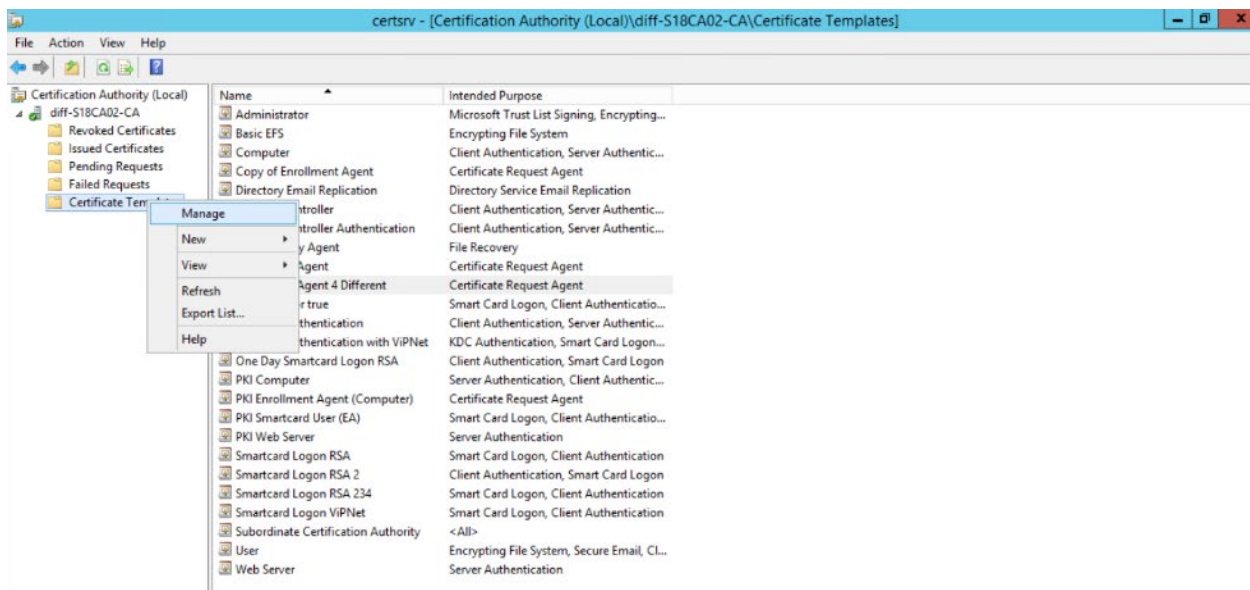


Рисунок 3.9 – Управление шаблонами сертификатов

В появившемся окне выберите пункт **Агент регистрации (Enrollment Agent)** (рисунок 3.10).

Настройка свойств шаблона сертификата может осуществляться в уже имеющемся шаблоне, либо в созданной копии имеющегося шаблона.

Для создания копии имеющегося шаблона, щелкните правой кнопкой мыши и выберите **Скопировать шаблон (Duplicate Template)** (рисунок 3.10).

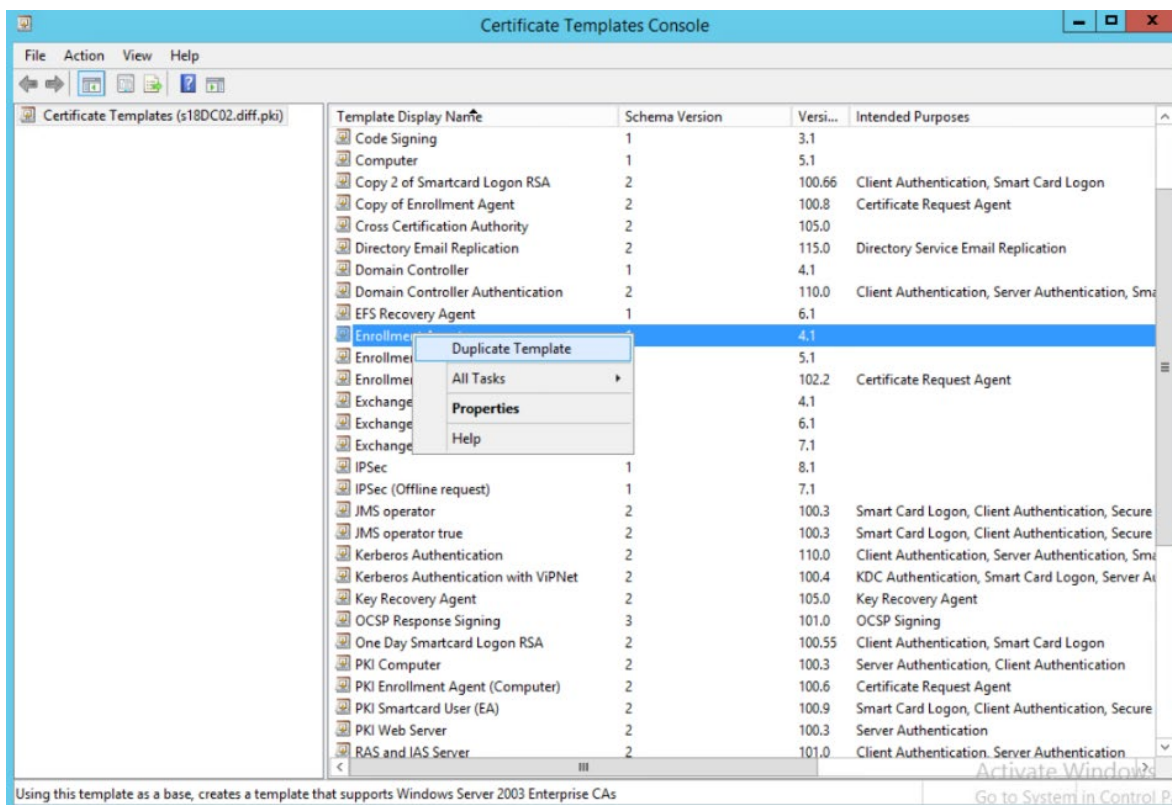


Рисунок 3.10 – Создание копии шаблона

В появившемся окне со свойствами шаблона выполните следующие настройки:

1) Введите имя создаваемого шаблона на вкладке **Общие (General)**. При необходимости настройте **Срок действия сертификата (Validity period)** и **Период обновления (Renewal period)** (рисунок 3.11).

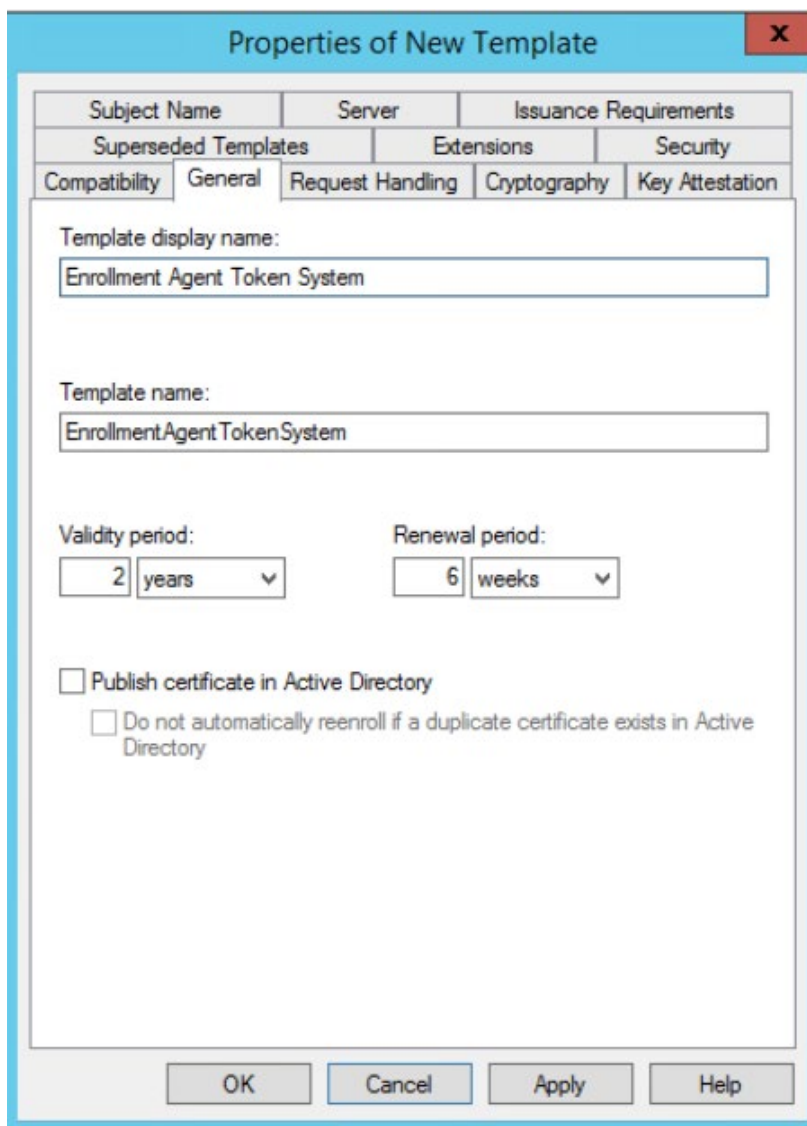
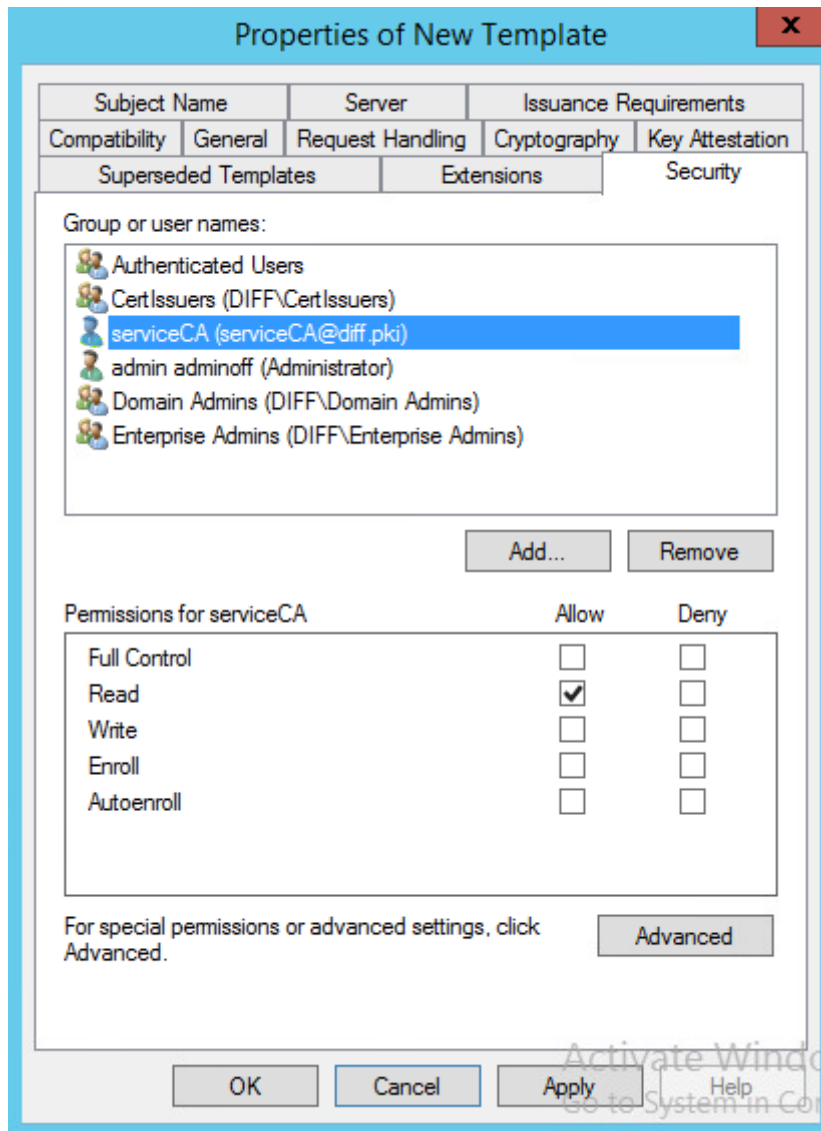
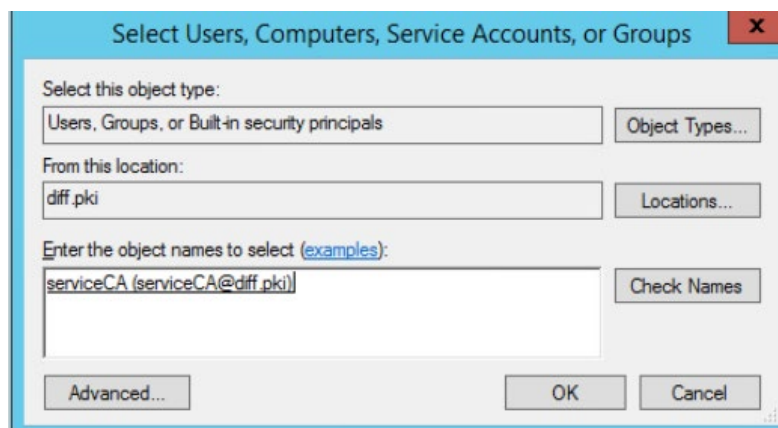


Рисунок 3.11 – Свойства шаблона, вкладка **General**

2) Во вкладке **Безопасность (Security)** добавьте сервисную учетную запись, от имени которой будет запрашиваться выпуск сертификатов для пользователей. Для этого нажмите кнопку **Добавить (Add)** и в появившемся окне найдите созданную учетную запись (в примере, **serviceCA**) (рисунок 3.12 а, б).



а)



б)

Рисунок 3.12 – Свойства шаблона, вкладка **Security**

3) Установите для сервисной учетной записи разрешение **Заявка (Enroll)** (рисунок 3.13).

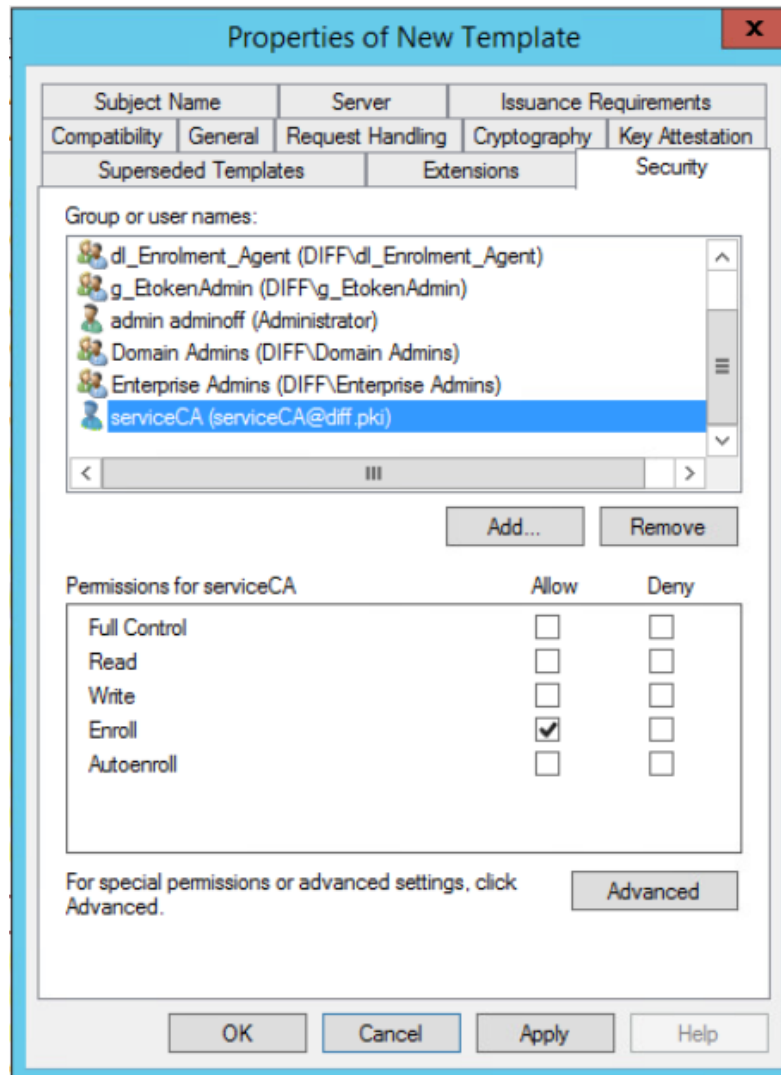


Рисунок 3.13 – Добавление разрешений для сервисной учетной записи

- 4) Во вкладке **Имя субъекта (Subject Name)** установите параметр **Строится на основе данных Active Directory (Build from this Active Directory information)** и нажмите **Применить (Apply)** (рисунок 3.14).

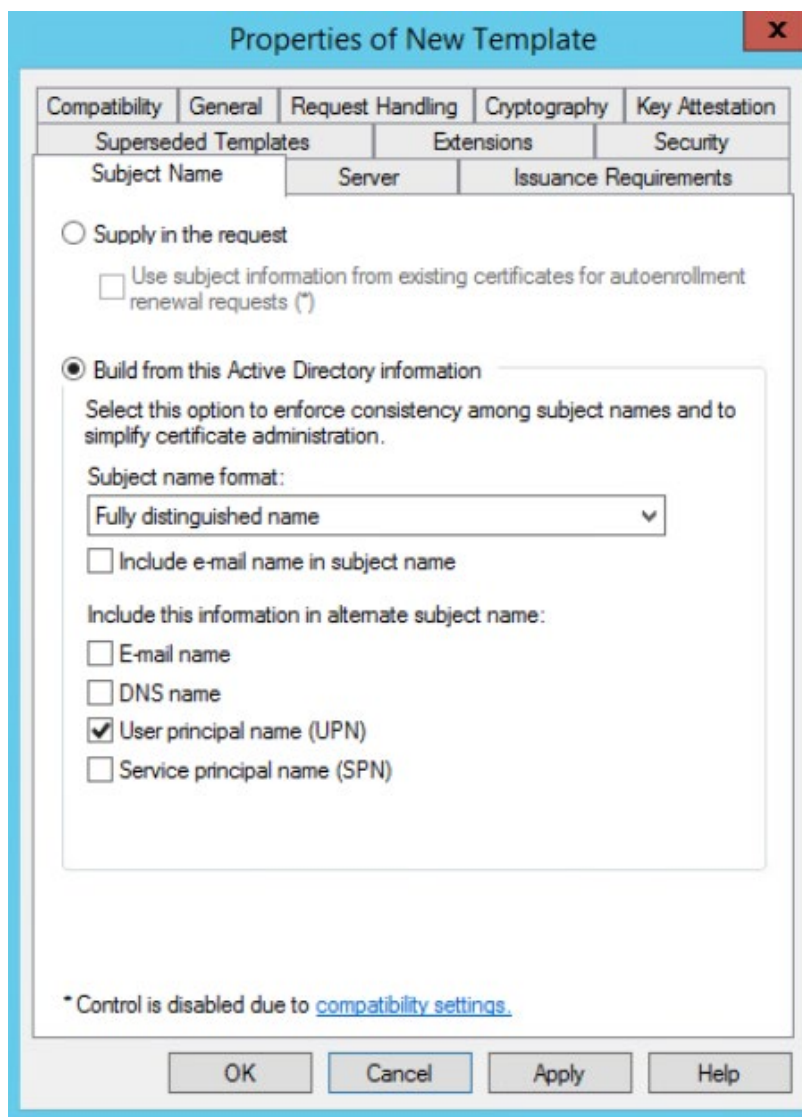


Рисунок 3.14 – Установка параметра *Строится на основе данных Active Directory*

- 5) Для сохранения шаблона нажмите **ОК**.
- 6) Для публикации созданного шаблона, после его настройки, перейдите на пункт **Шаблоны сертификатов (Certificate Templates)**, щелкните правой кнопкой мыши и выберите **Создать (New) → Выдаваемый шаблон сертификата (Certificate Template to Issue)** (рисунок 3.15).

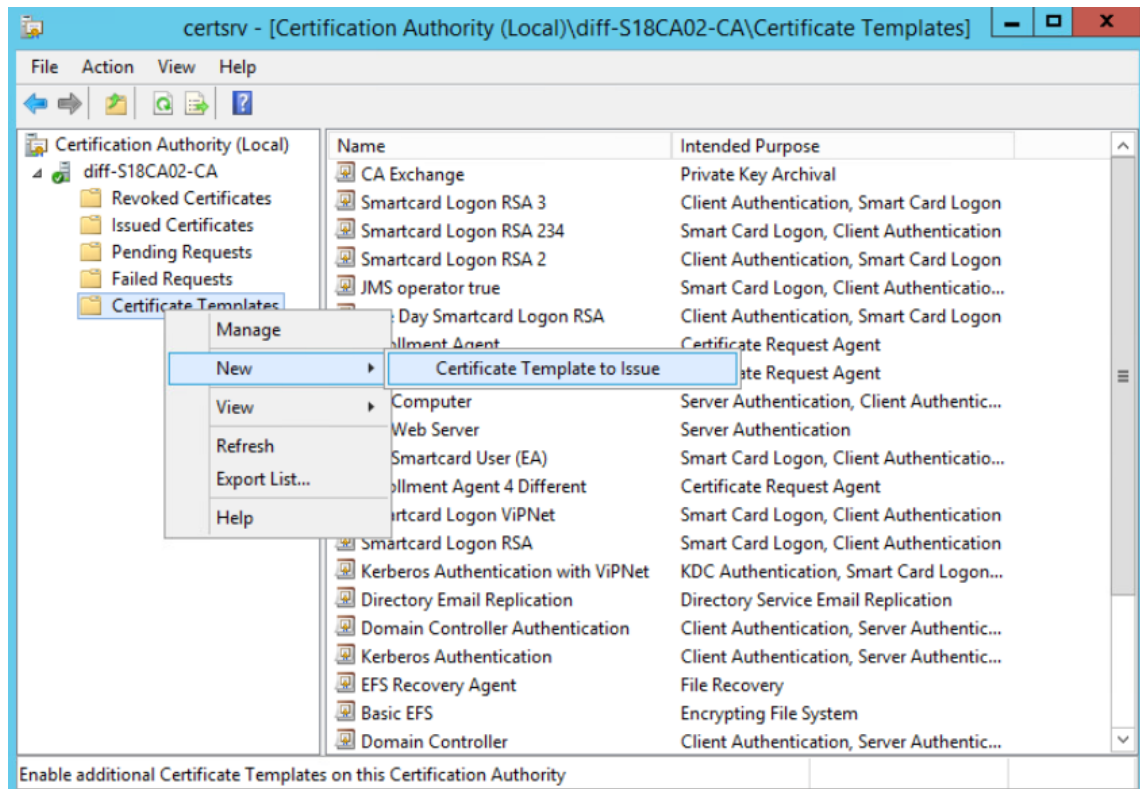


Рисунок 3.15 – Выбор выдаваемого шаблона сертификата

7) В появившемся окне (рисунок 3.16) выберите созданный шаблон сертификата и нажмите **ОК**.

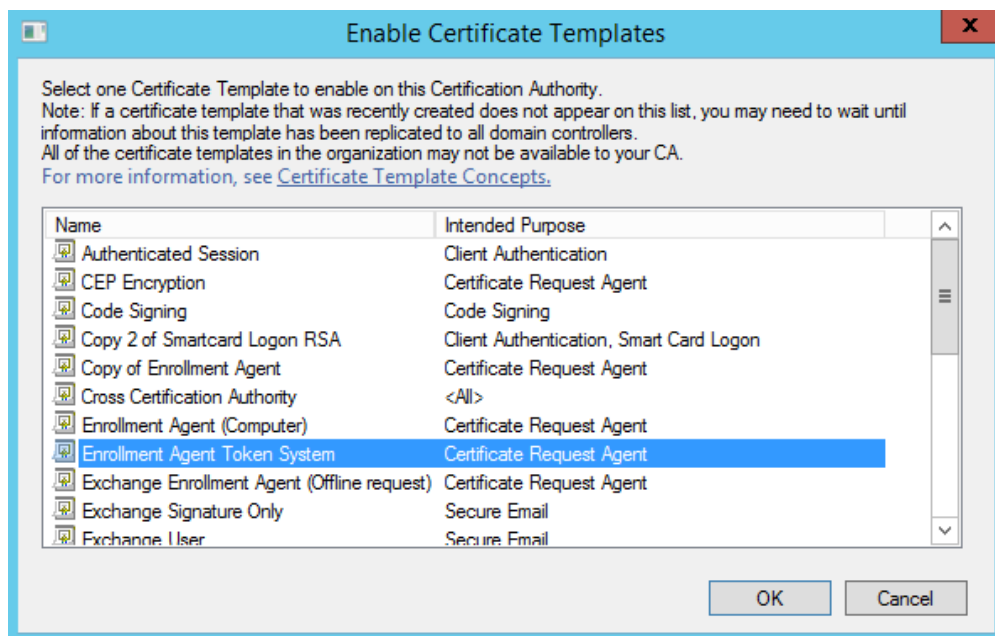


Рисунок 3.16 – Публикация созданного шаблона

3.2 Сертификат пользователя

При выпуске токена с сертификатом, в память токена записывается сертификат, выпущенный по шаблону сертификата пользователя со смарт-картой. Данный

сертификат, позволяет осуществлять пользователю вход в систему.

Для создания шаблона запустите консоль центра сертификации с помощью команды **certsrv.msc** в командной строке (рисунок 3.17).

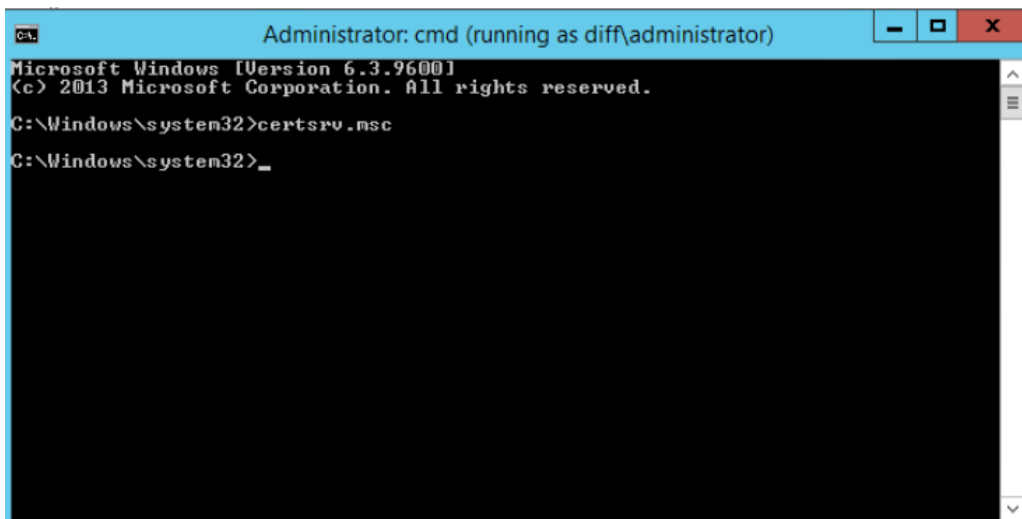


Рисунок 3.17 – Запуск консоли центра сертификации

Окно консоли будет выглядеть следующим образом:

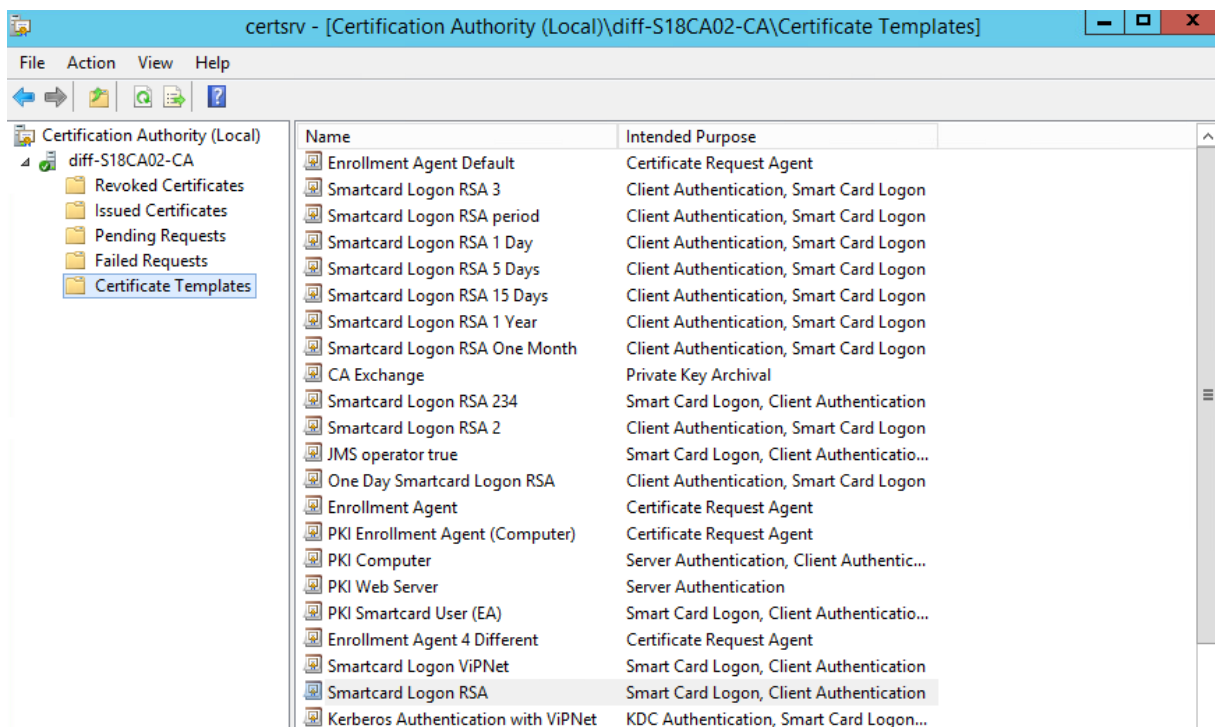


Рисунок 3.18 – Консоль центра сертификации

В левой части окна перейдите на пункт **Шаблоны сертификатов (Certificate Templates)**, щелкните правой кнопкой мыши и выберите **Управление (Manage)** (рисунок 3.19).

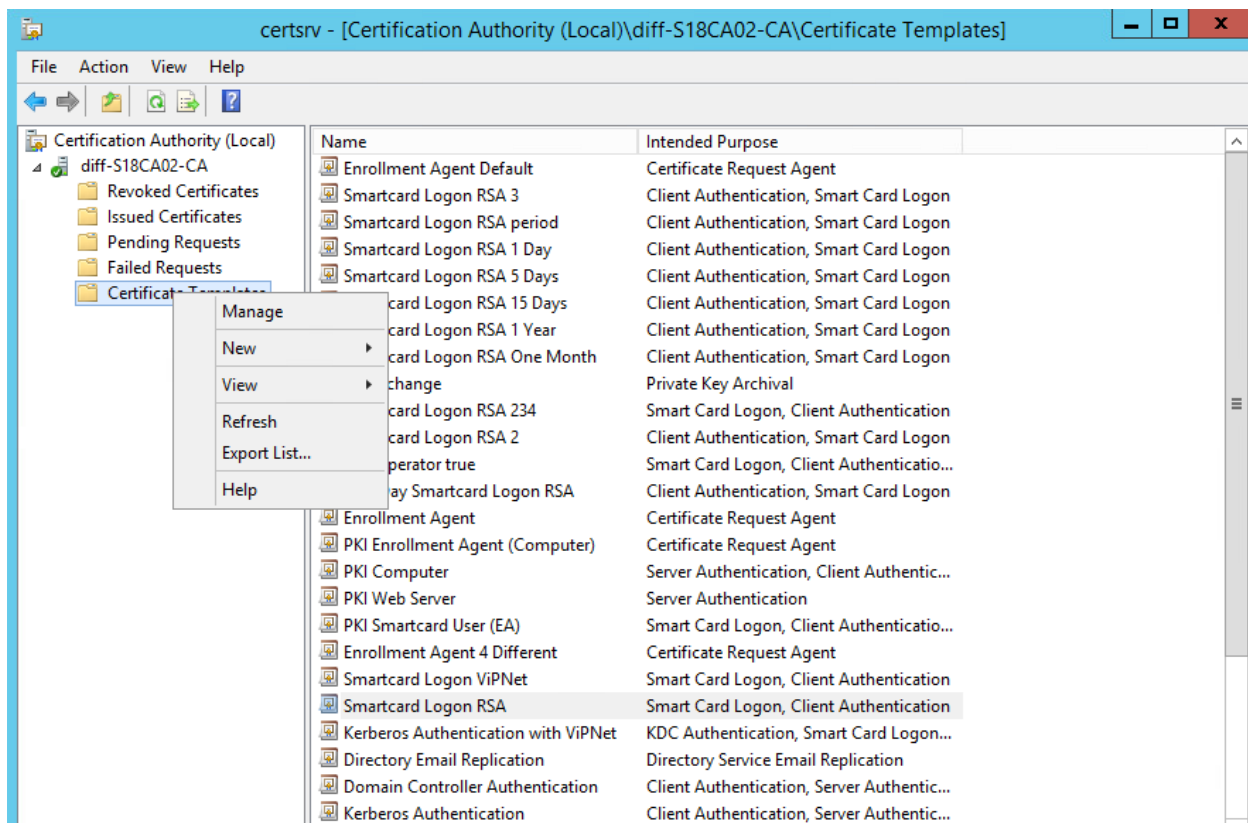


Рисунок 3.19 – Управление шаблонами сертификатов

В появившемся окне выберите пункт **Пользователь со смарт-картой (Smartcard Logon)**, щелкните правой кнопкой мыши и выберите **Скопировать шаблон (Duplicate Template)** (рисунок 3.20).

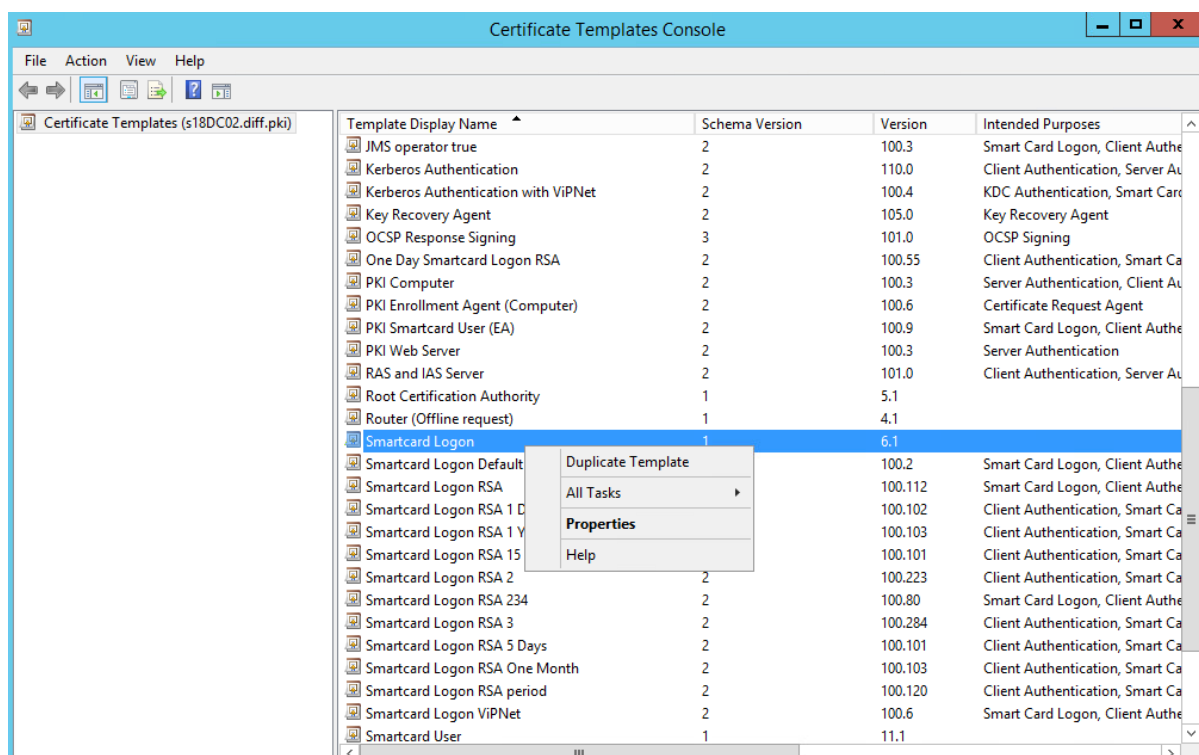
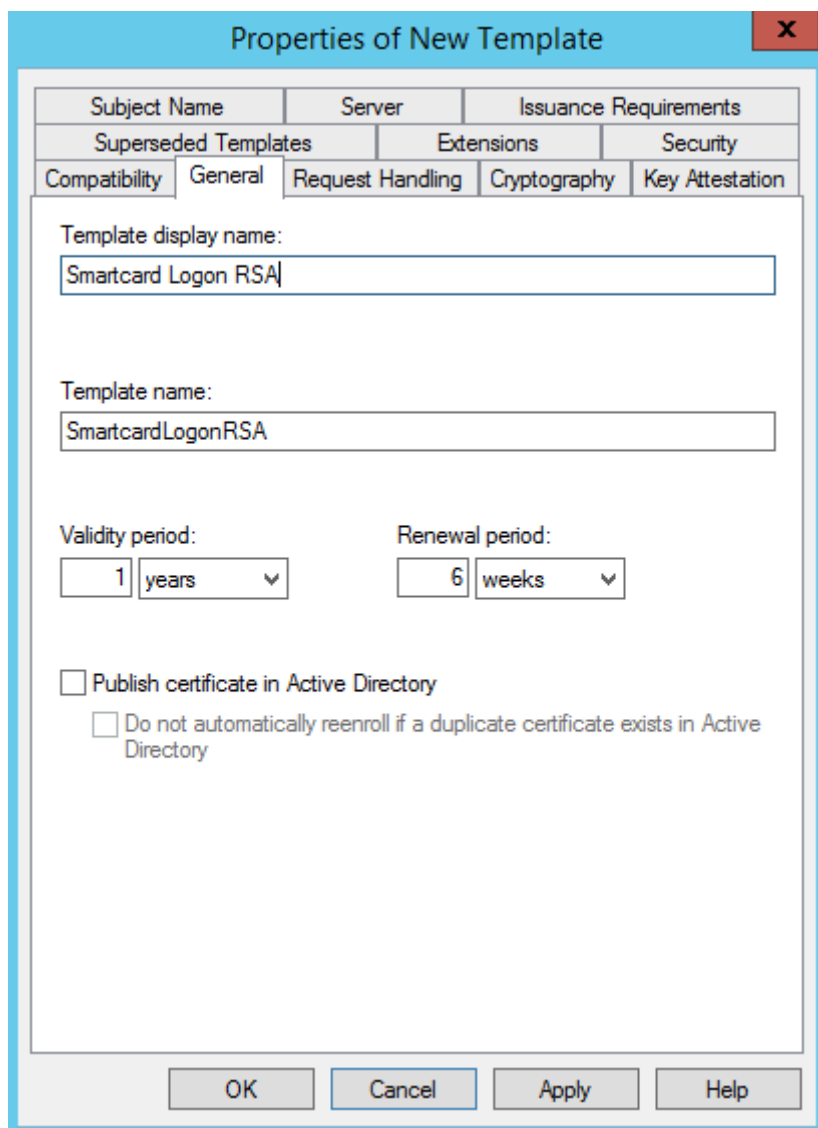


Рисунок 3.20 – Создание копии шаблона

В появившемся окне со свойствами шаблона выполните следующие настройки:

- 1) Введите имя создаваемого шаблона на вкладке **Общие (General)** (рисунок 3.21).



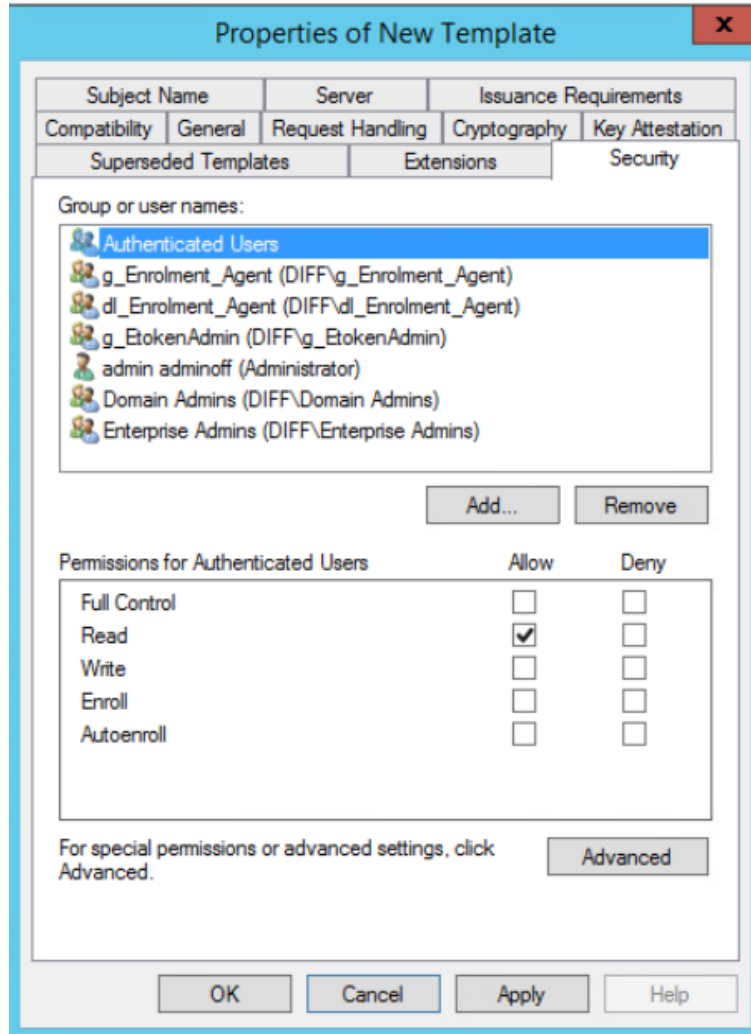
The image shows a Windows-style dialog box titled "Properties of New Template" with a close button (X) in the top right corner. The dialog has a tabbed interface with the following tabs: "Subject Name", "Server", "Issuance Requirements", "Superseded Templates", "Extensions", "Security", "Compatibility", "General", "Request Handling", "Cryptography", and "Key Attestation". The "General" tab is currently selected. Inside the dialog, there are several input fields and controls:

- "Template display name:" with a text box containing "Smartcard Logon RSA".
- "Template name:" with a text box containing "SmartcardLogonRSA".
- "Validity period:" with a dropdown menu showing "1" and "years".
- "Renewal period:" with a dropdown menu showing "6" and "weeks".
- Two checkboxes:
 - Publish certificate in Active Directory
 - Do not automatically reenroll if a duplicate certificate exists in Active Directory

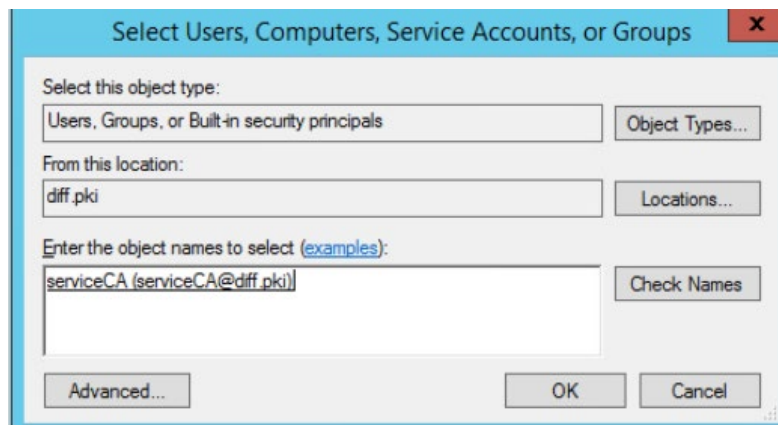
At the bottom of the dialog, there are four buttons: "OK", "Cancel", "Apply", and "Help".

Рисунок 3.21 – Свойства шаблона, вкладка **General**

- 2) Во вкладке **Безопасность (Security)** добавьте сервисную учетную запись, от имени которой будет запрашиваться выпуск сертификатов для пользователей. Для этого нажмите кнопку **Добавить (Add)** и в появившемся окне найдите созданную учетную запись (в примере, **serviceCA**) (рисунок 3.22 а, б).



а)



б)

Рисунок 3.22 – Свойства шаблона, вкладка **Security**

3) Установите для сервисной учетной записи разрешение **Заявка (Enroll)** (рисунок 3.23).

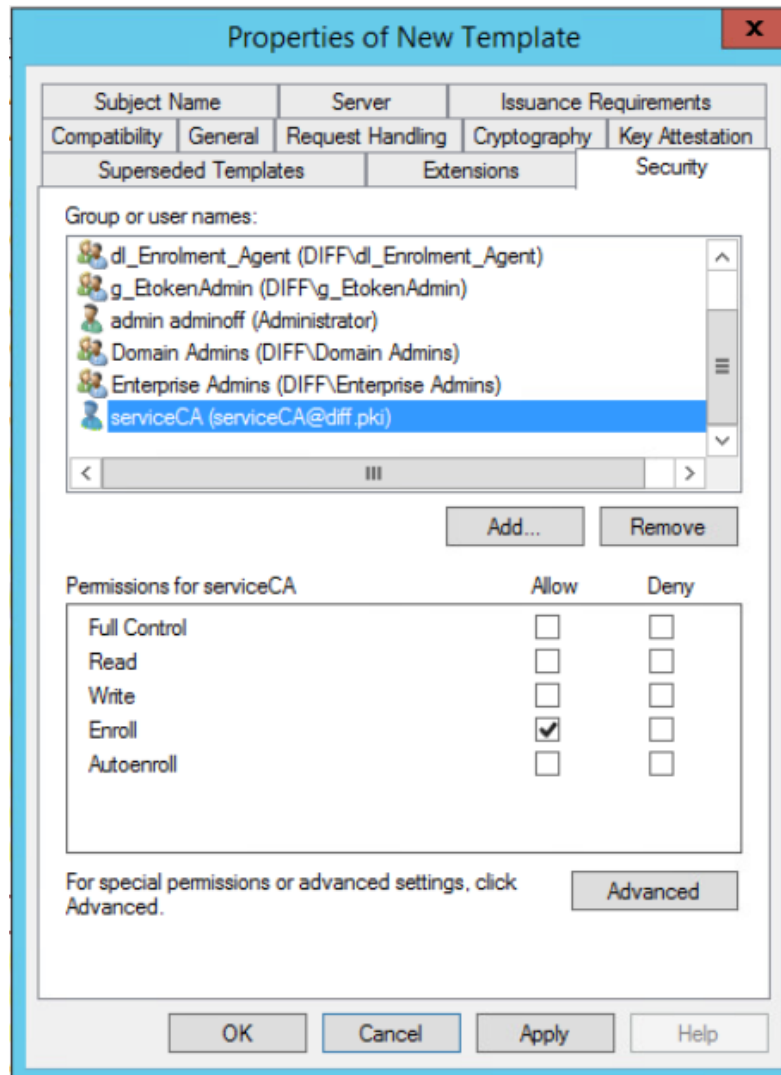


Рисунок 3.23 – Добавление разрешений для сервисной учетной записи

4) Для выпуска сертификата средствами подсистемы управления жизненным циклом токенов, в окне со свойствами шаблона перейдите во вкладку **Имя субъекта (Subject Name)** и установите переключатель на параметр **Предоставляется в запросе (Supply in the request)** (рисунок 3.24).

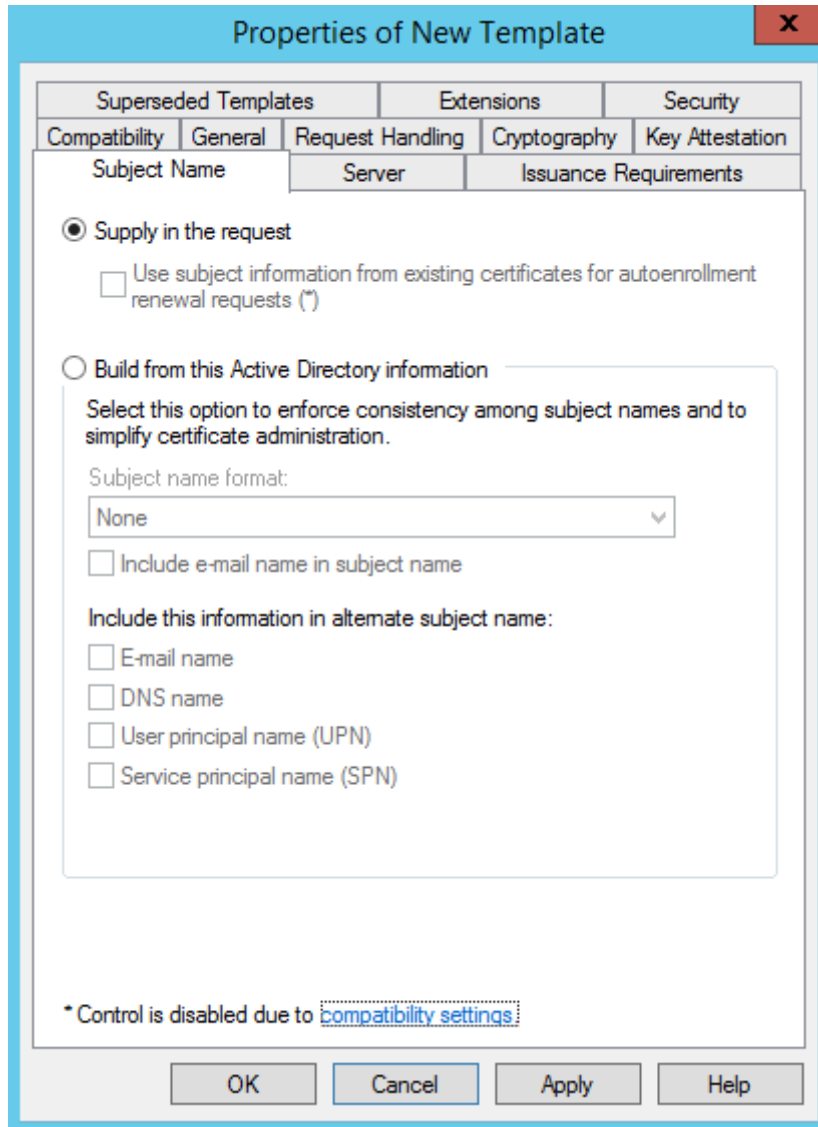


Рисунок 3.24 – Настройка выпуска сертификата пользователя средствами подсистемы

5) Во вкладке **Шифрование (Cryptography)** установите минимальный размер ключа шифрования – 1024 бит (рисунок 3.25).

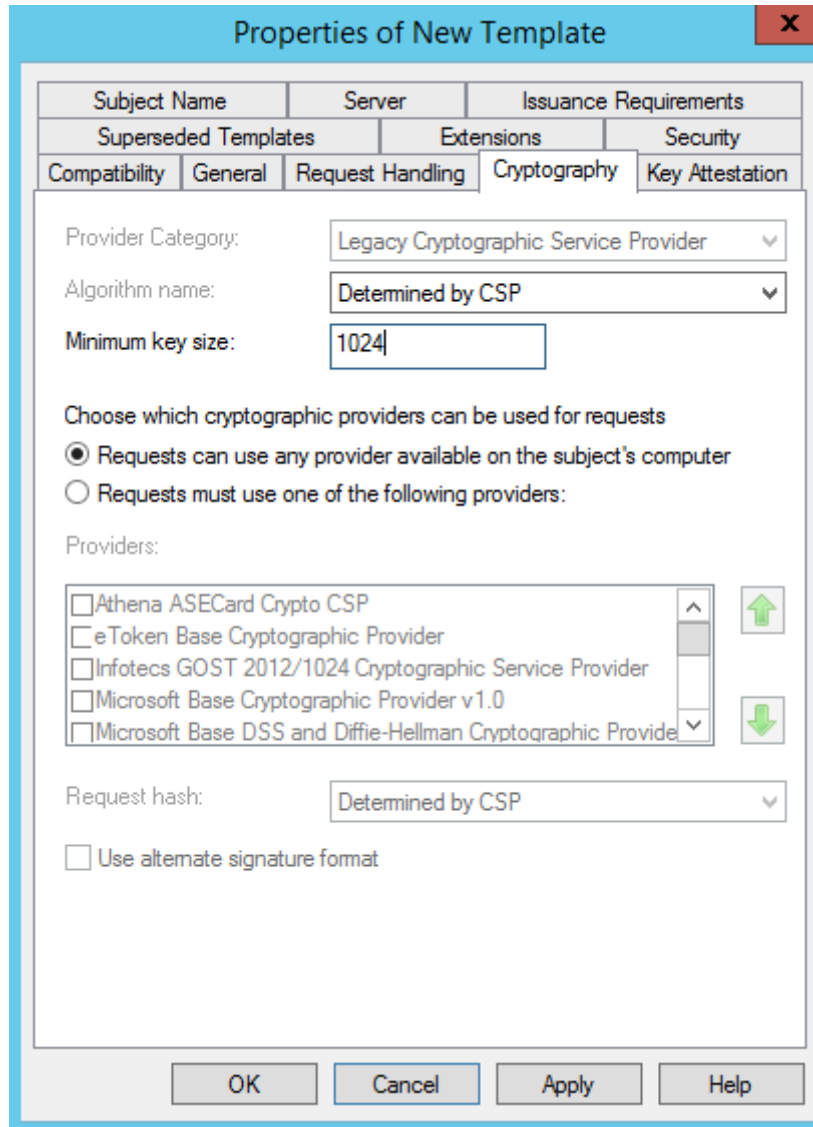


Рисунок 3.25 – Установка минимального размера ключа шифрования

6) Для сохранения шаблона нажмите **OK**.

Для публикации созданного шаблона, после его настройки, перейдите на пункт **Шаблоны сертификатов (Certificate Templates)**, щелкните правой кнопкой мыши и выберите **Создать (New)** → **Выдаваемый шаблон сертификата (Certificate Template to Issue)** (рисунок 3.26).

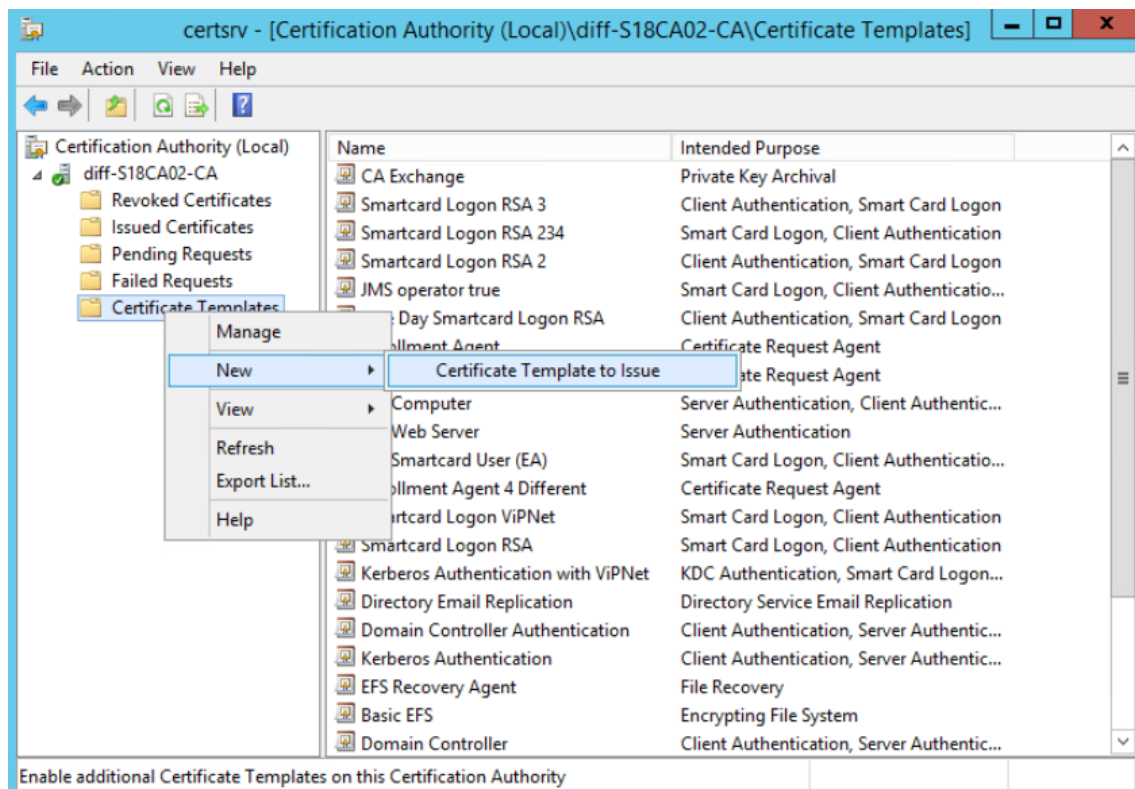


Рисунок 3.26 – Выбор выдаваемого шаблона сертификата

В появившемся окне (рисунок 3.27) выберите созданный шаблон сертификата и нажмите **OK**.

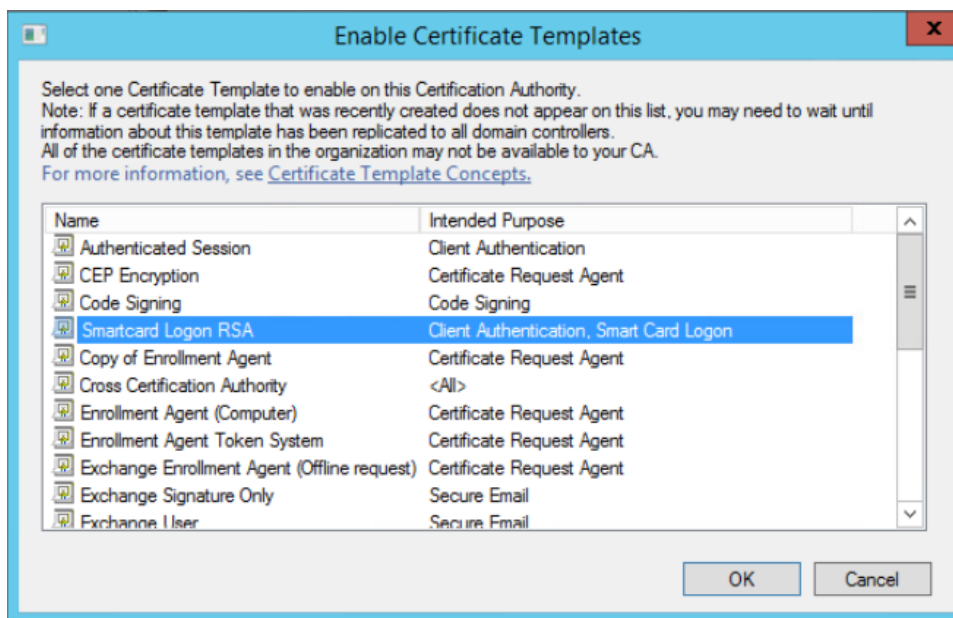


Рисунок 3.27 – Публикация созданного шаблона

4 Настройки на сервере «Блокхост-Сеть»

4.1 Выпуск и установка сертификата агента регистрации

Выпуск и установка сертификата агента регистрации осуществляется на рабочее место администратора безопасности с установленной серверной версией средства защиты от несанкционированного доступа «Блокхост-Сеть 4».

Для возможности выпуска сертификатов пользователей, необходимо наличие в оснастке **Сертификаты (Certificates)** в разделе **Личные (Personal)** установленного сертификата, выпущенного по шаблону сертификата агента регистрации.

Для создания сертификата выполните следующие действия:

- 1) Выполните вход в систему под сервисной учетной записью (**serviceCA**) и перейдите в оснастку сертификатов **certmgr.msc**, либо выполните вход в систему под административной учетной записью и запустите оснастку сертификатов (рисунок 4.1) из-под сервисной учетной записи командой

```
runas /user:<домен\имя пользователя> "cmd /C start /B certmgr.msc"
```

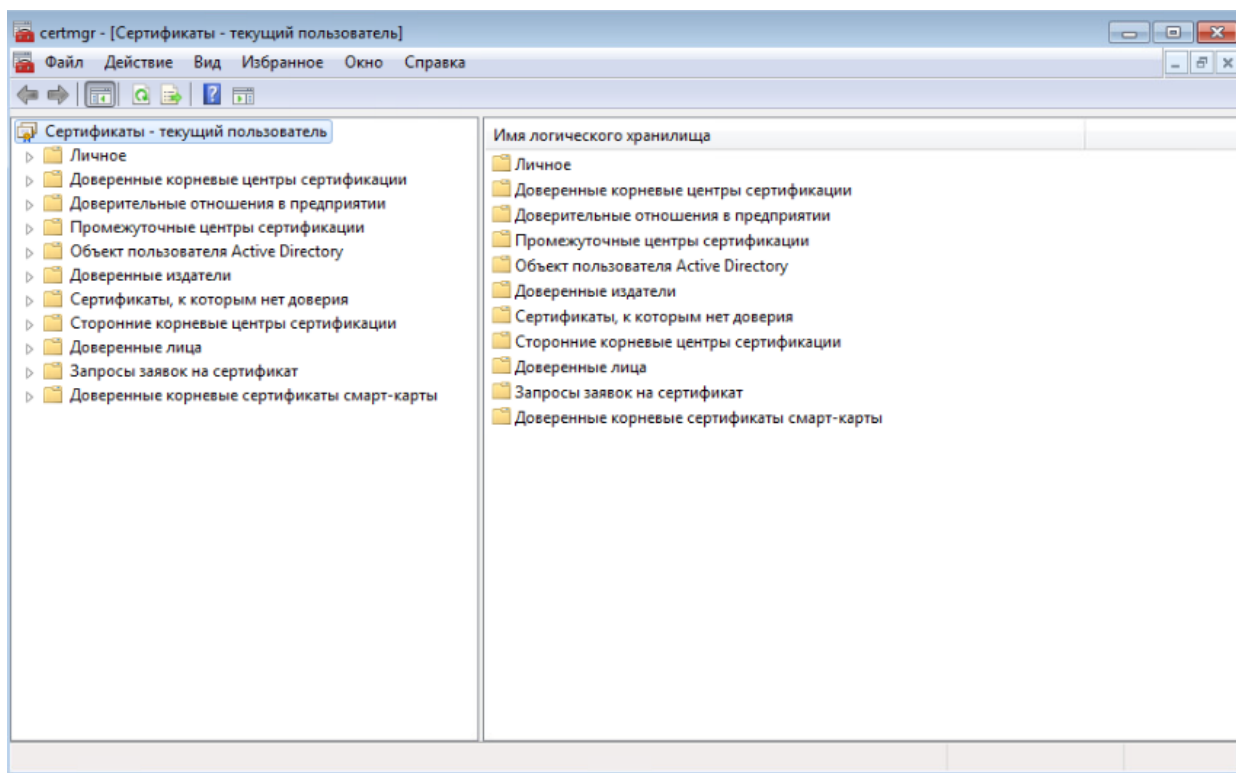


Рисунок 4.1 – Оснастка **Сертификаты (Certificates)**

- 2) В левой части окна перейдите в раздел **Личные (Personal)** и по щелчку правой кнопкой мыши выберите **Все задачи (All Task)** → **Запросить новый сертификат (Request New Certificate)** (рисунок 4.2).

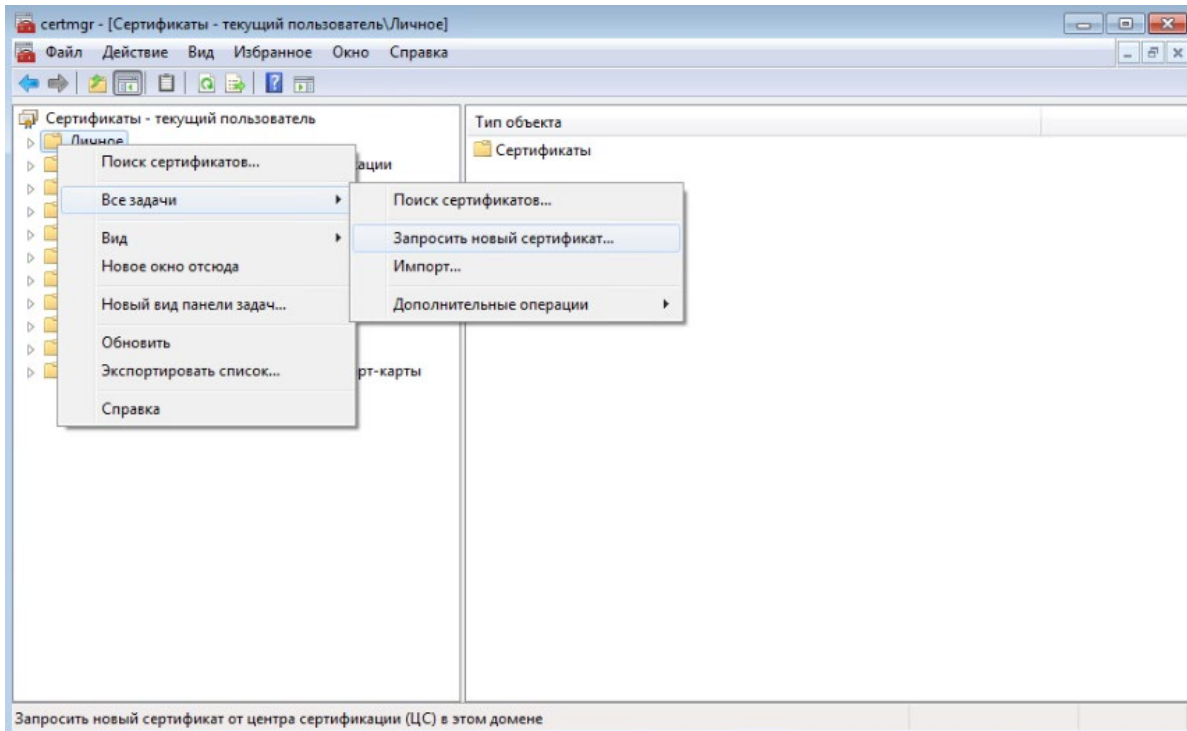


Рисунок 4.2 – Запрос нового личного сертификата

3) В появившемся окне **Регистрация сертификатов** выберите **Политика регистрации Active Directory (Active Directory Enrollment Policy)** и нажмите **Далее** (рисунок 4.3).

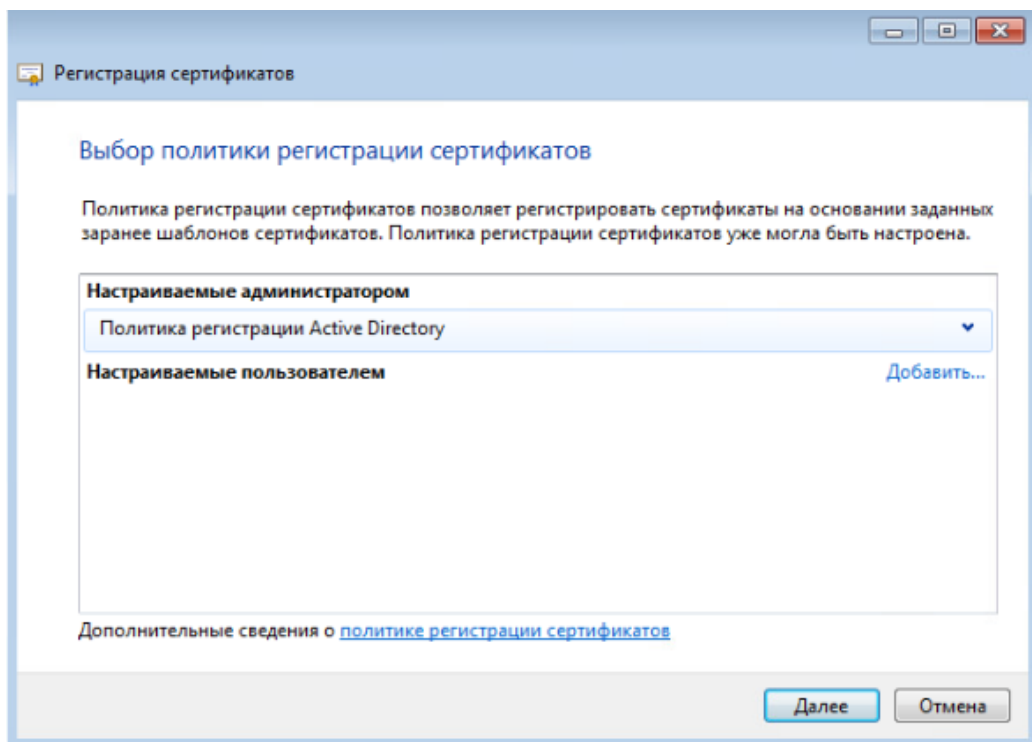


Рисунок 4.3 – Выбор политики регистрации сертификата

4) Выберите шаблон сертификата, созданный в центре сертификации (например,

Enrollment Agent Token System) (рисунок 4.4).

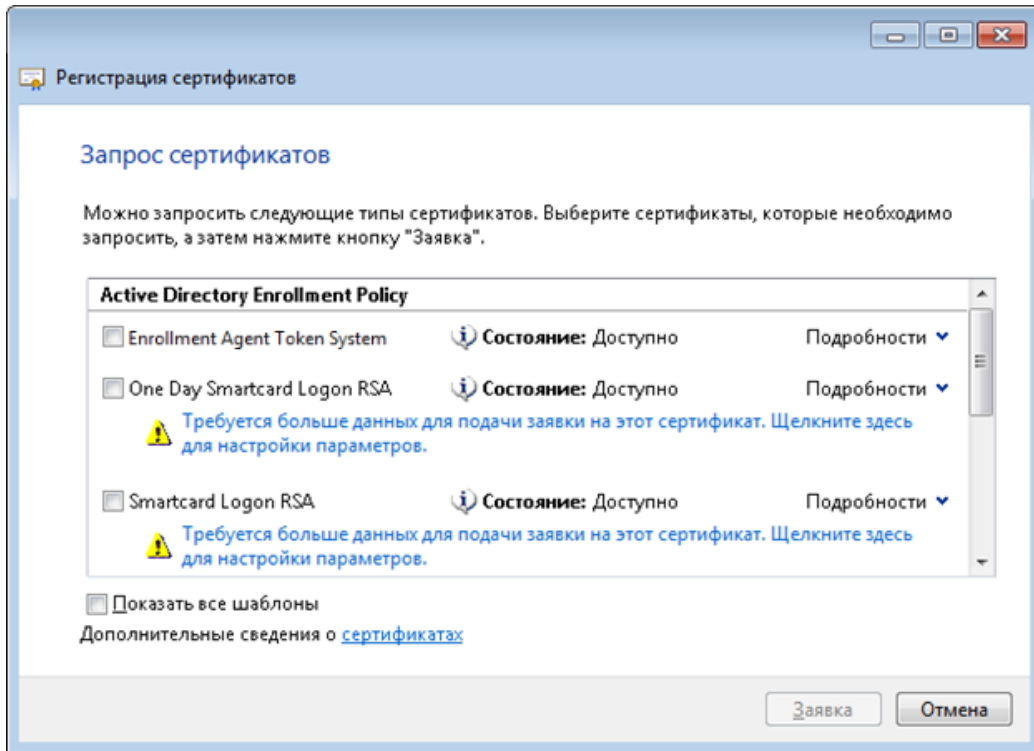
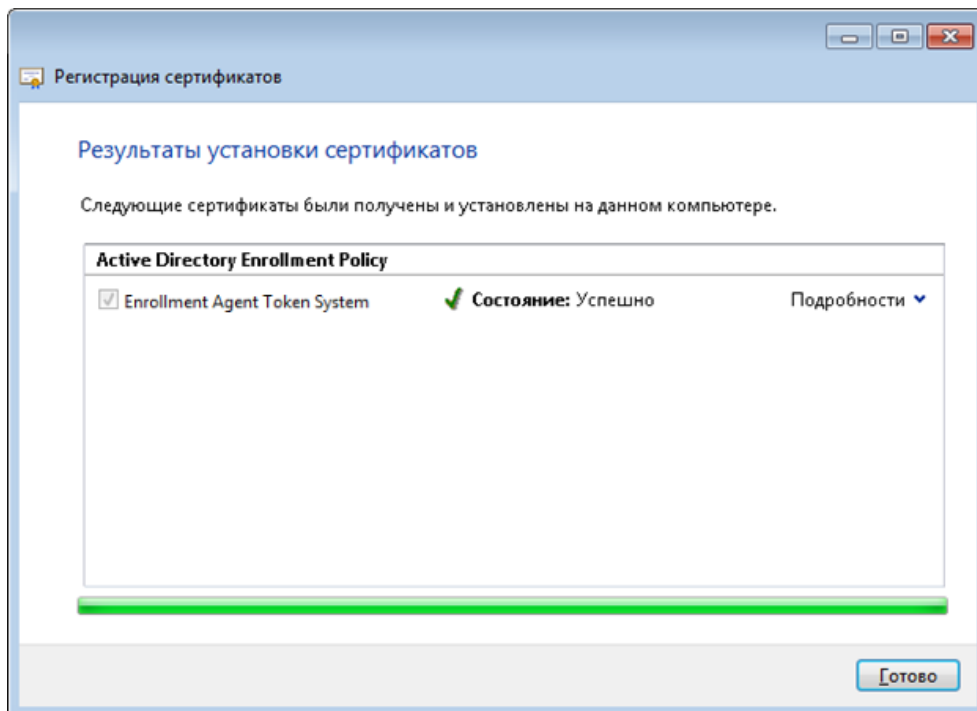
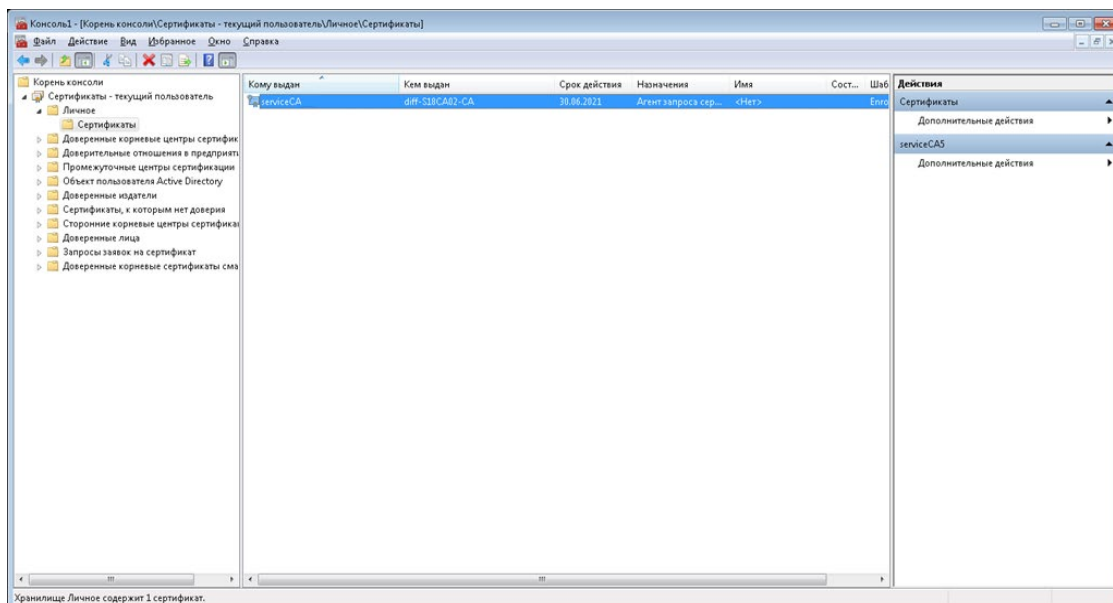


Рисунок 4.4 – Выбор шаблона сертификата

5) Дождитесь выпуска и установки сертификата в хранилище **Личное** (рисунок 4.5 а) и нажмите **Готово** (рисунок 4.5 б).



а)




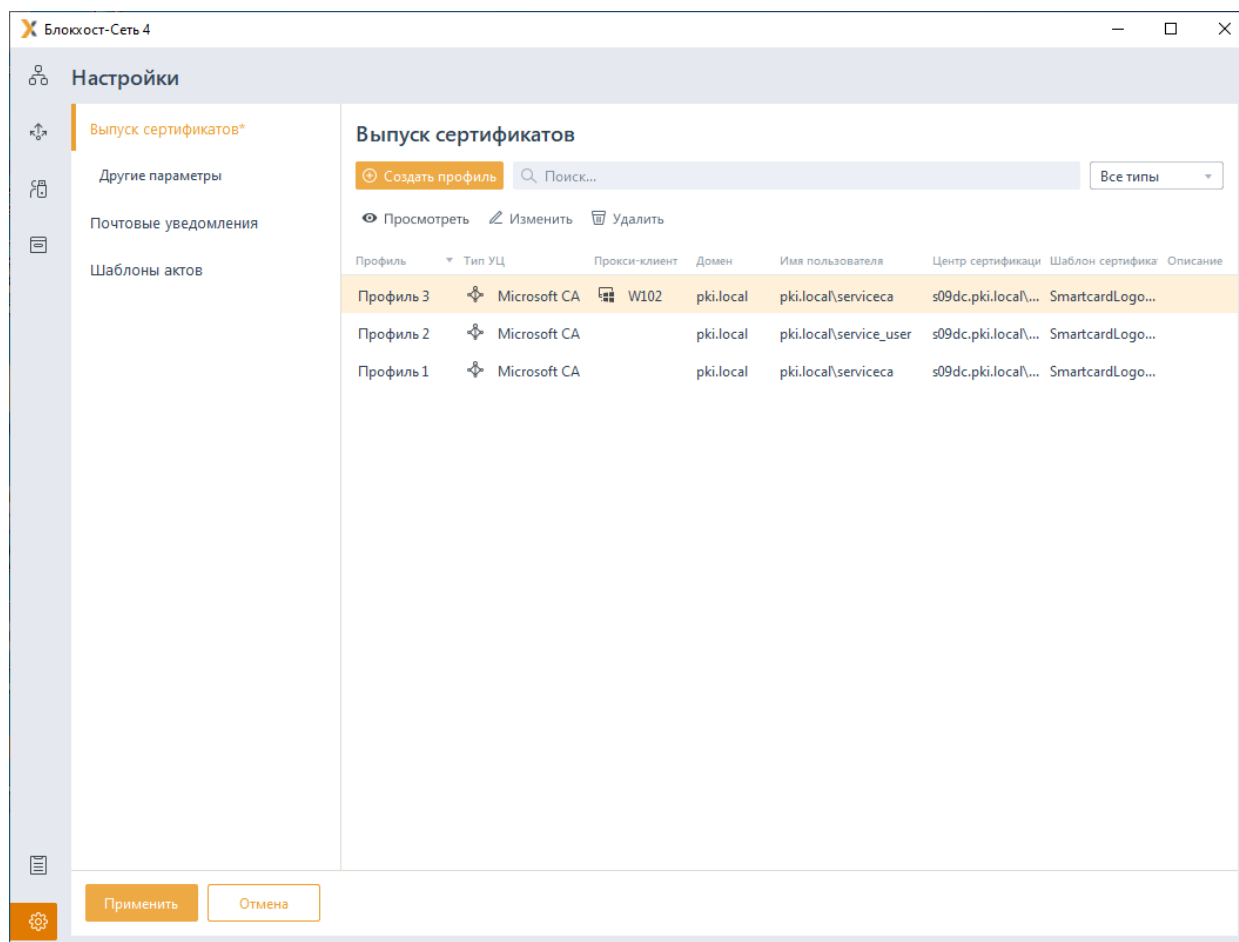
б)

Рисунок 4.5 – Установка сертификата в хранилище *Личное*

4.2 Создание профилей в настройках подсистемы

Для корректной работы подсистемы управления жизненным циклом токенов по выпуску сертификатов необходимо создать профиль для выпуска сертификата в настройках подсистемы управления жизненным циклом токенов.

Откройте консоль администрирования Блокост-Сеть и перейдите в раздел **Настройки** → **Выпуск сертификатов** по кнопке  (рисунок 4.6).

Рисунок 4.6 – Раздел *Настройки*

Для каждого созданного профиля в окне **Выпуск сертификатов** отображается информация:

- *Профиль* – наименование профиля;
- *Тип УЦ* – центр сертификации выпускающий сертификат (Microsoft CA/DogTag);
- *Прокси-клиент* – клиентская рабочая станция, выбранная для взаимодействия с центром сертификации;
- *Домен* – наименование домена;
- *Имя пользователя* – наименование сервисной учетной записи;
- *Центр сертификации* – адрес центра сертификации;
- *Шаблон сертификата* – шаблон сертификата для входа;
- *Описание* – подробное описание профиля.

При необходимости, любой из созданных профилей возможно изменить или удалить с помощью соответствующих кнопок в верхней части вкладки (рисунок 4.6).

4.2.1 Создание профиля Microsoft CA

Для создания профиля по выпуску сертификатов центра сертификации Microsoft CA

нажмите на кнопку  и выберите **Microsoft CA** (рисунок 4.7).

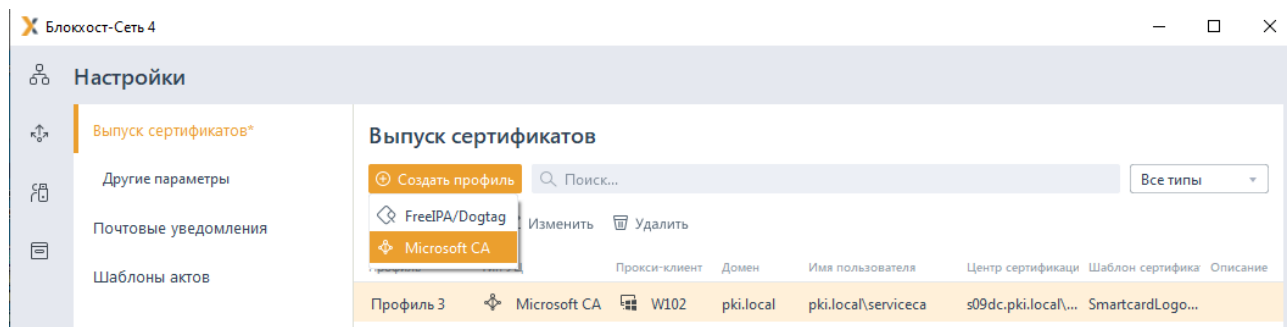


Рисунок 4.7 – Выбор центра сертификации

В появившемся окне (рисунок 4.8) введите наименование профиля, его описание, при необходимости, и параметры сервисной учетной записи (имя пользователя и пароль) в соответствующих полях.

Рисунок 4.8 – Создание профиля AD

Нажмите кнопку **Подключиться** (рисунок 4.8).



При возникновении ошибки при подключении убедитесь, что для вводимой сервисной учетной записи или для группы, в которую учетная запись входит,

правилами клиентской политики безопасности не установлен запрет на аутентификацию Windows (подробное описание приведено в документе «СЗИ от НСД «Блокост-Сеть 4». Руководство администратора безопасности. Часть 1. Управление политиками»).

После успешного подключения произойдет запуск получения списка сертификатов выбранной сервисной учетной записи и в нижней части окна появится информация о подключении (рисунок 4.9).

Создание профиля Active Directory

Имя профиля
Профиль 4

Описание
Введите описание профиля

Указать прокси-клиент для предоставления доступа ⓘ

Каталог учетных записей ⓘ

Active Directory
pki.local

Выпуск сертификатов

Имя пользователя ⓘ serviceca

Пароль
.....

Изменить

Имя центра сертификации Microsoft CA
s09dc.pki.local\pki-S09DC-CA

Сертификат агента регистрации - Enrollment Agent ⓘ ↻
46fcbcb7ebb9525ff819566a343ceb9c53623d02

Шаблон сертификата для входа ↻
Не задано

Таймаут ожидания при выпуске сертификата, сек 30


Размер ключа, бит 1024

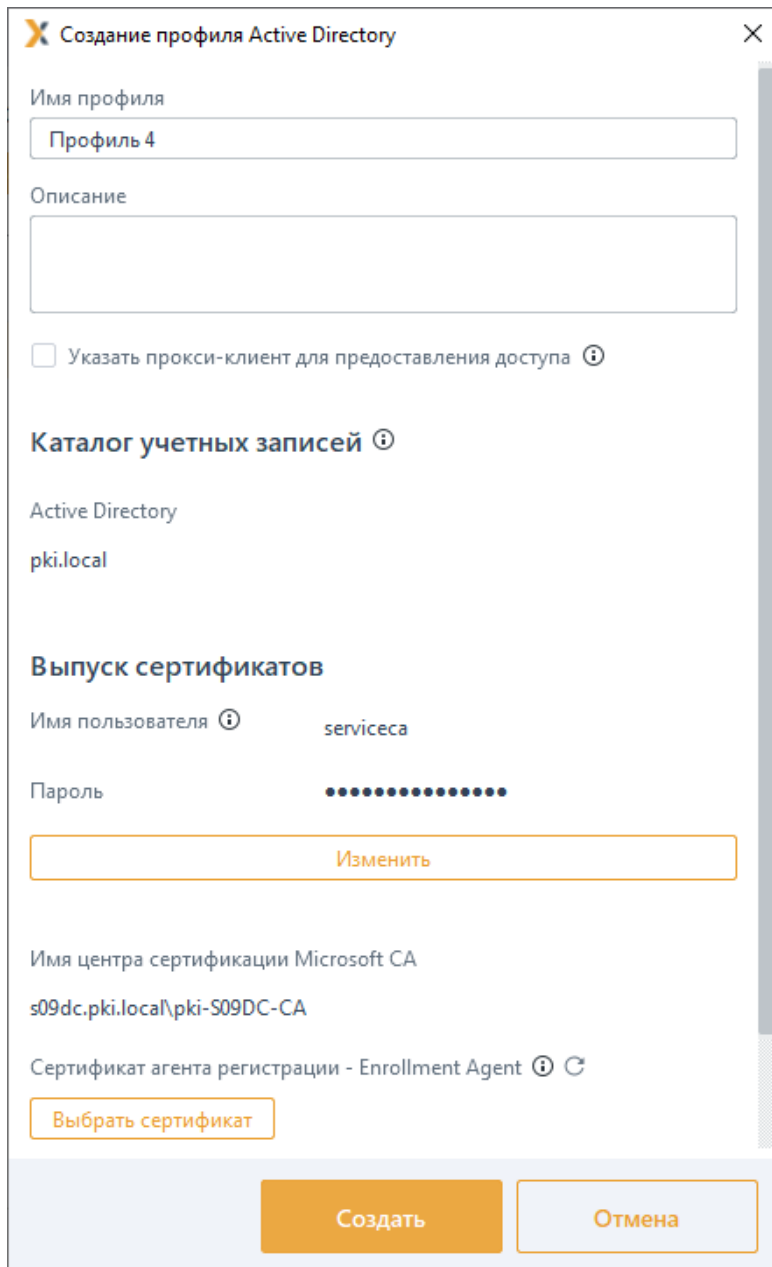
Публиковать выдаваемые сертификаты в ActiveDirectory ⓘ

Создать Отмена

Рисунок 4.9 – Выбор сертификата агента регистрации и шаблона для входа

В поле **Сертификат агента регистрации – Enrollment Agent** отобразится необходимый сертификат агента регистрации, установленный в личное хранилище оснастки **Сертификаты**.

-  Если в личном хранилище выбранной учетной записи несколько сертификатов, в поле **Сертификат агента регистрации – Enrollment Agent** появится возможность выбора необходимого сертификата по кнопке **Выбрать сертификат** (рисунок 4.10 а).



Создание профиля Active Directory

Имя профиля
Профиль 4

Описание

Указать прокси-клиент для предоставления доступа ⓘ

Каталог учетных записей ⓘ

Active Directory
pki.local

Выпуск сертификатов

Имя пользователя ⓘ servicesca

Пароль

Изменить

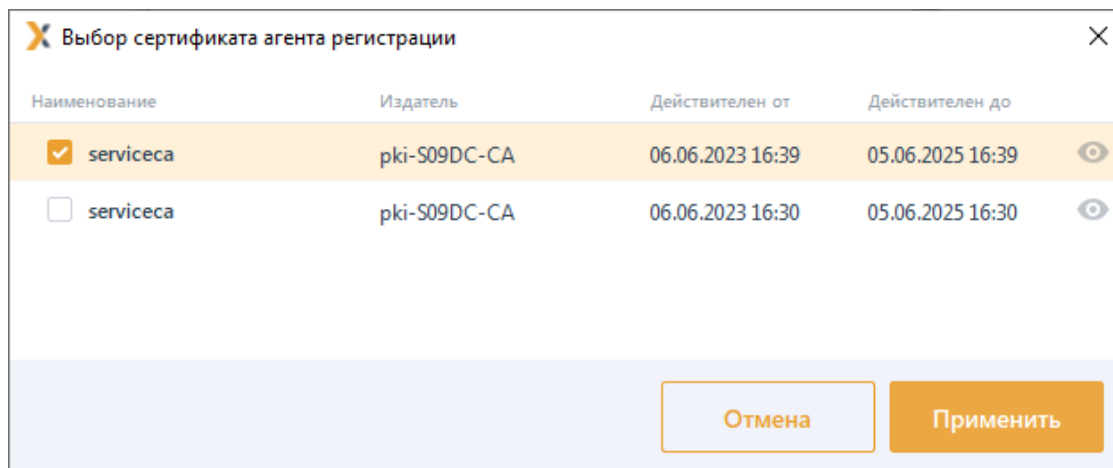
Имя центра сертификации Microsoft CA
s09dc.pki.local\pki-S09DC-CA

Сертификат агента регистрации - Enrollment Agent ⓘ ↻

Выбрать сертификат

Создать Отмена

а)



б)

Рисунок 4.10 – Выбор сертификата агента регистрации из списка



При отсутствии в личном хранилище оснастки **Сертификаты** сертификата агента регистрации выбранной учетной записи, после попытки получения списка сертификатов, в окне настроек появится запись об отсутствии сертификата агента регистрации (рисунок 4.11).

Необходимо установить сертификат в личное хранилище, последовательно выполняя действия, описанные в разделе **Установка сертификата агента регистрации в хранилище**, и нажать кнопку

Имя центра сертификации Microsoft CA

s09dc.pki.local\pki-S09DC-CA

Сертификат агента регистрации - Enrollment Agent

Отсутствует

Рисунок 4.11 – Отсутствие сертификата агента регистрации

После добавления сервисной учетной записи нажмите кнопку **Применить** для перезапуска службы **GIS.ServerTokenSystem**.

В поле **Шаблон сертификата для входа** (рисунок 4.12) необходимо выбрать из списка шаблон сертификата пользователя, созданный в центре регистрации (например, **SmartcardLogonCA**).

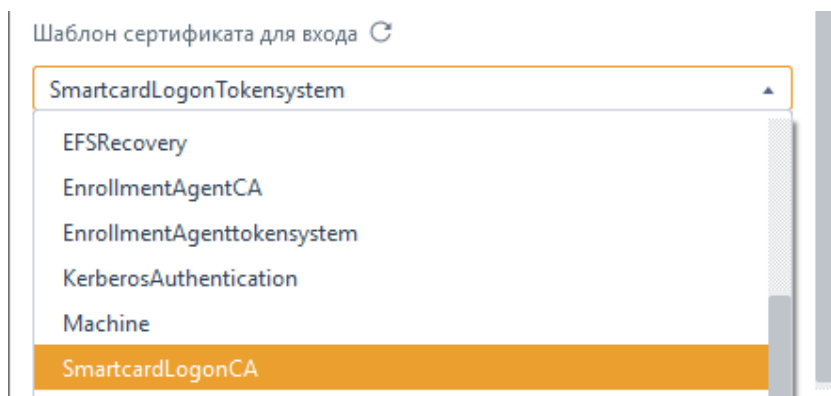


Рисунок 4.12 – Выбор шаблона сертификата для входа



Имя шаблона сертификата пользователя в поле **Шаблон сертификата для входа** соответствует имени, заданному при создании шаблона в центре сертификации на вкладке **Общие (General)** в параметре **Имя шаблона (Template name)** (рисунок 4.13).

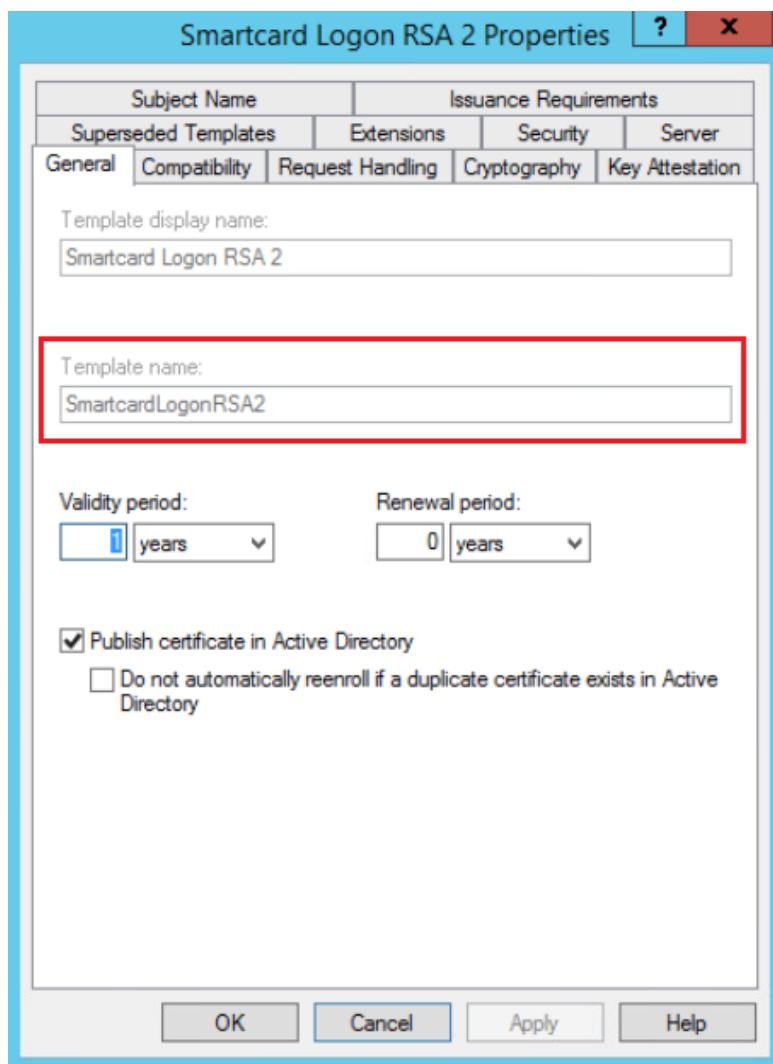


Рисунок 4.13 – Шаблон сертификата для входа

После нажатия кнопки **Создать** профиль отобразится в списке и будет доступен к

выбору при выпуске токена пользователю для входа по сертификату (рисунок 4.14).

Выпуск токена для входа по управляемому сертификату

ruToken, S/N 0951209993

Пользователь **Иванов Иван Иванович** ✎ 🗑

Домен **Active Directory**

Профиль выпуска **Профиль 1** 👁

Имя токена **Rutoken ECP <no label>**

Инвентарный номер

Комментарий

Инициализировать

Отмена Применить

Рисунок 4.14 – Отображение профиля при выпуске токена

4.2.2 Добавление прокси-клиента для взаимодействия с ЦС

При эксплуатации серверной части «СЗИ от НСД «Блокхост-Сеть 4» под управлением ОС семейств Linux не предусматривается возможность взаимодействия с центром сертификации Microsoft CA напрямую.

Для возможности обращения к центру сертификации Microsoft CA серверной части «СЗИ от НСД «Блокхост-Сеть 4» под управлением ОС Linux с целью выпуска сертификатов Microsoft CA необходимо выбрать одну из клиентских рабочих станций под управлением ОС Windows и назначить ее прокси-клиентом, через который будет происходить взаимодействие с центром сертификации Microsoft CA.

Установка флага **Указать прокси-клиент для представления доступа** (рисунок 4.15) позволяет выбрать клиентскую рабочую станцию Блокхост-Сеть под управлением ОС Windows для взаимодействием с центром сертификации Microsoft CA.



При обращении к центру сертификации Microsoft CA серверной части «СЗИ от НСД «Блокхост-Сеть 4» под управлением ОС Windows установка флага является опциональной.

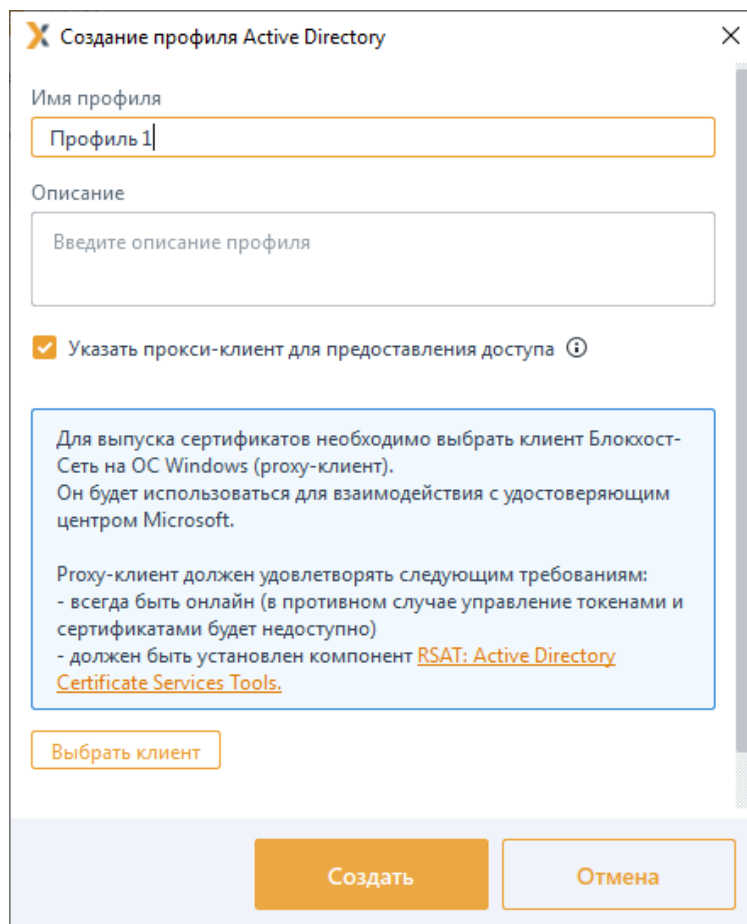


Рисунок 4.15 – Добавление прокси-клиента

При этом прокси-клиент должен удовлетворять следующим требованиям:

- всегда быть в состоянии онлайн (для возможности выпуска сертификатов);
- на клиенте должен быть установлен компонент **RSAT Active Directory Certificate Services (AD CS) tools** (<https://learn.microsoft.com/en-us/troubleshoot/windows-server/system-management-components/remote-server-administration-tools>).

Выбрать клиент

По кнопке **Выбрать клиент** добавьте клиентскую рабочую станцию Блокхост-Сеть под управлением ОС Windows, которая будет использоваться для взаимодействия с центром сертификации Microsoft CA (рисунок 4.16).

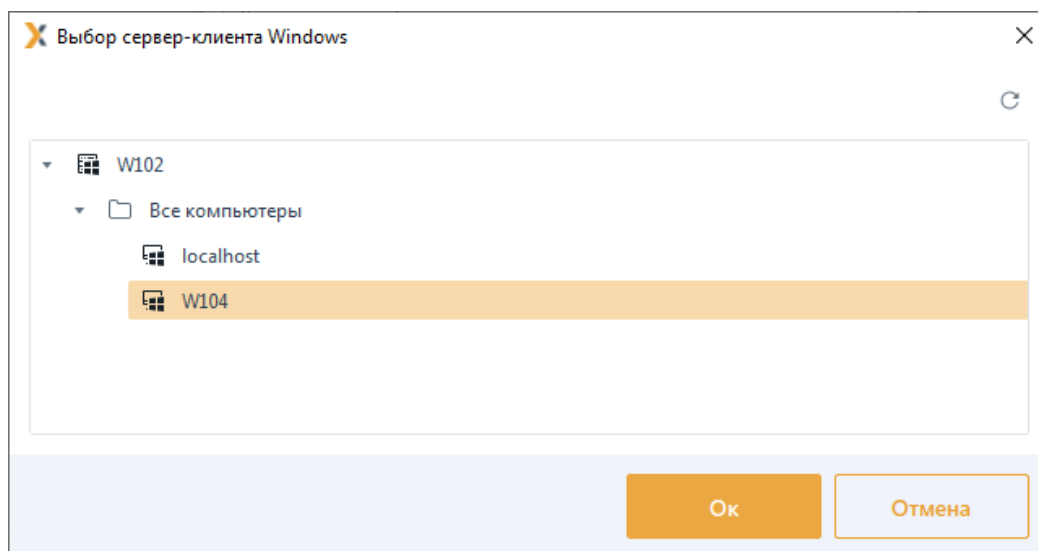


Рисунок 4.16 – Выбор прокси-клиента

Введите наименование профиля, его описание и параметры сервисной учетной записи (имя пользователя и пароль) в соответствующих полях (рисунок 4.17).

Создание профиля Active Directory

Имя профиля
Профиль 1

Описание
Введите описание профиля

Указать прокси-клиент для предоставления доступа ⓘ

Прокси-клиент Windows W104

Каталог учетных записей ⓘ

Active Directory
pki.local

Выпуск сертификатов

Имя пользователя ⓘ servicesca

Пароль
.....

Изменить

Имя центра сертификации Microsoft CA
s09dc.pki.local\pki-S09DC-CA

Сертификат агента регистрации - Enrollment Agent ⓘ ↻
4ee2b7711c6db5e1c4b5878af618ffff8aa90fc8

Шаблон сертификата для входа ↻
SmartcardLogonTokenSystem

Таймаут ожидания при выпуске сертификата, сек 30

Размер ключа, бит 1024

Публиковать выдаваемые сертификаты в ActiveDirectory ⓘ

Создать Отмена

Рисунок 4.17 – Ввод данных для создания профиля

Дальнейшие действия по созданию профиля выпуска сертификата аналогичны описанным в разделе **Создание профиля Microsoft CA**.

- i** Необходимо обратить внимание, что все шаги по выпуску и установке сертификата агента регистрации, описанные в разделе **Создание профиля Microsoft CA** выполняются на клиентской рабочей станции, выбранной в качестве прокси-клиента.

При необходимости, прокси-клиента возможно изменить или удалить с помощью контекстного меню (рисунок 4.18).

- i** При удалении или изменении прокси-клиента все его настройки будут утеряны.

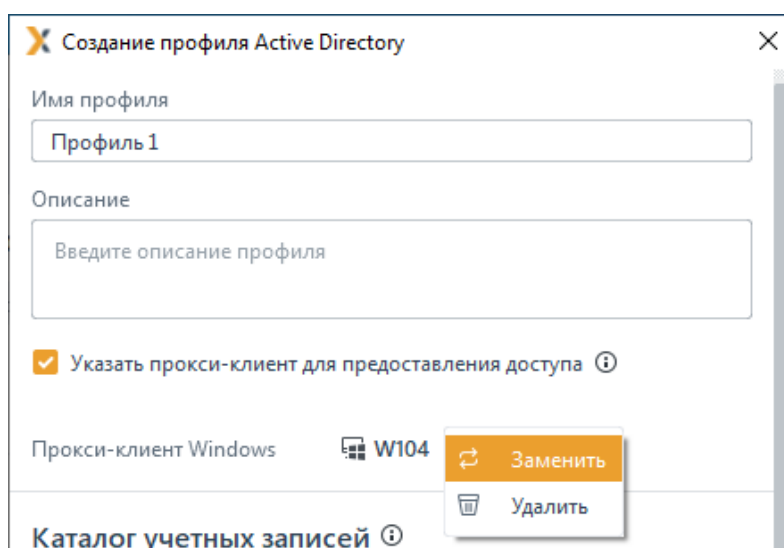


Рисунок 4.18 – Изменение прокси-клиента

Флаг **Публиковать выдаваемые сертификаты в Active Directory** (рисунок 4.19) необходим для того, чтобы все выпускаемые сертификаты публиковались в Active Directory пользователя, который был указан при выпуске токена. Посмотреть их можно на домен-контроллере: **Active Directory Users and Computers** → **Свойства пользователя** → **Published Certificates**.

При отзыве токена через подсистему управления токенами, выпущенный сертификат автоматически удаляется из Active Directory пользователя (при отзыве через оснастку Windows этого не произойдет).

Создание профиля Active Directory

Имя профиля
Профиль 1

Описание
Введите описание профиля

Указать прокси-клиент для предоставления доступа ⓘ

Прокси-клиент Windows W104 ⋮

Каталог учетных записей ⓘ

Active Directory
pki.local

Выпуск сертификатов

Имя пользователя ⓘ servicesca

Пароль
●●●●●●●●

Изменить

Имя центра сертификации Microsoft CA
s09dc.pki.local\pki-S09DC-CA

Сертификат агента регистрации - Enrollment Agent ⓘ ↻
4ee2b7711c6db5e1c4b5878af618ffff8aa90fc8

Шаблон сертификата для входа ↻
SmartcardLogonTokenSystem

Таймаут ожидания при выпуске сертификата, сек 30

Размер ключа, бит 1024

Публиковать выдаваемые сертификаты в ActiveDirectory ⓘ

Создать Отмена

Рисунок 4.19 – Публиковать выдаваемые сертификаты в AD

5 Особенности при выпуске токена средствами подсистемы

При выпуске токена средствами подсистемы жизненного цикла токенов, с записью на него сертификата для входа пользователя или при использовании токена для входа по паролю, на токен записывается информация служебного характера (рисунок 5.1).

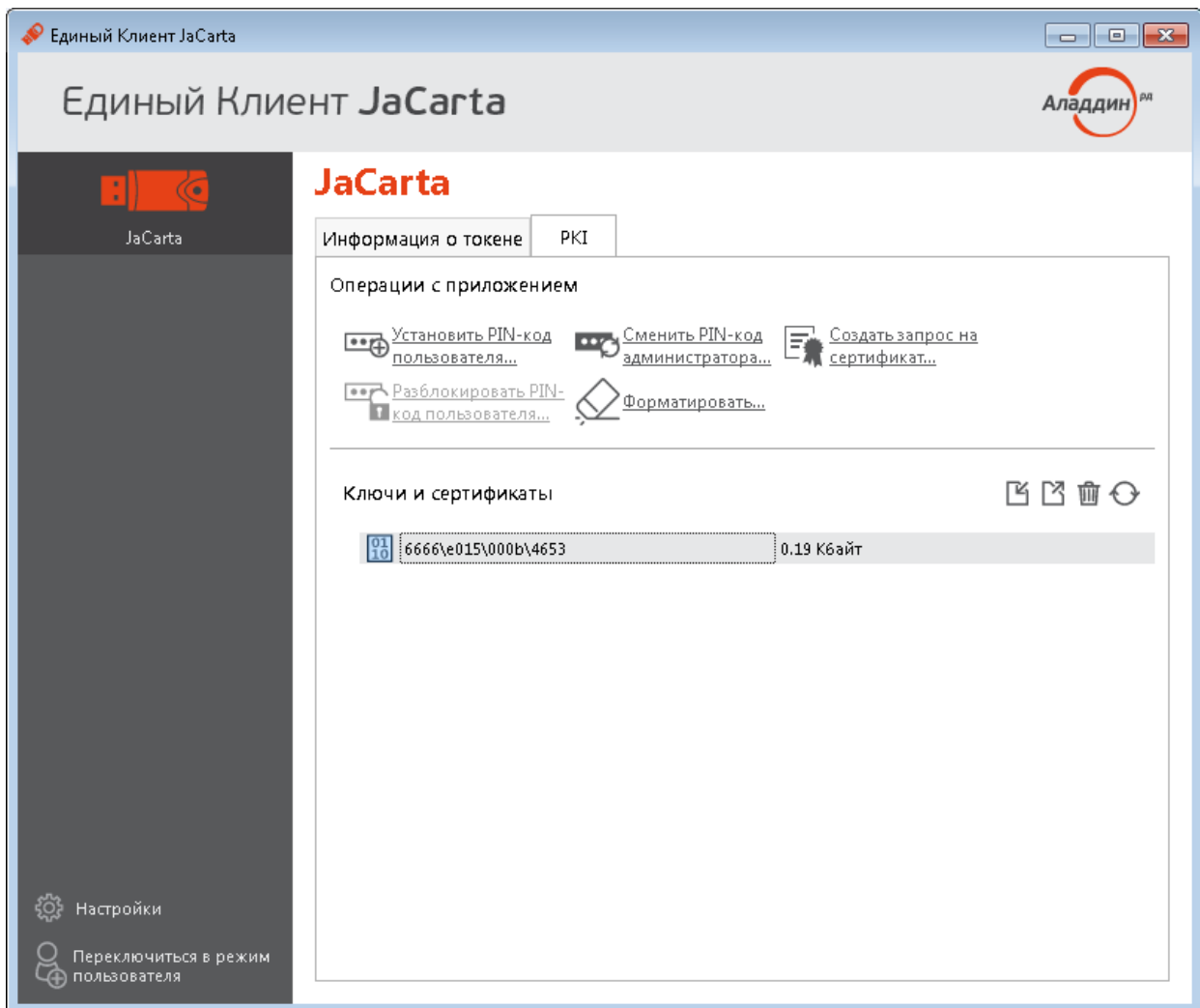


Рисунок 5.1 – Запись служебной информации при выпуске токена

- i** Служебная информация на токене не подлежит удалению или редактированию. Указанные действия приведут к некорректной работе подсистемы с используемым токеном, и ошибкам при выполнении операций с ним.

Дальнейшие действия администратора по работе с подсистемой управления жизненным циклом токенов описаны в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 5. Управление токенами».

6 Настройка прозрачного входа в RDGW

Удалённое подключение к рабочей станции осуществляется через RDGW (защищённый RDP), используется аутентификация на шлюзе удалённых рабочих столов по сертификату, сохранённому на токене.



Прозрачный вход возможен только в случае разрешённого для пользователя типа входа **«Аутентификация Windows»** в разделе клиентской политики **«Управление входом в ОС»** (подробное описание приведено в документе «СЗИ от НСД «Блокост-Сеть 4». Руководство администратора безопасности. Часть 1. Управление политиками»).

Для настройки прозрачного входа необходимо выполнить следующие действия:

- 1) Выполнить запуск *mstsc* и настроить RDGW вход.
- 2) Сохранить настройки в отдельный файл, например, *rdgw.rdp*.
- 3) Проверить возможность подключения по RDGW.
- 4) Открыть сохранённый файл *rdgw.rdp* в блокноте и добавить параметры:

```
promptcredentialonce:i:0  
prompt for credentials on client:i:0  
prompt for credentials:i:0
```

где:

promptcredentialonce:i:0 – соответствует снятию флага «использовать мои учётные данные шлюза для удалённого компьютера»;

prompt for credentials on client:i:0

prompt for credentials:i:0

– отключают запрос данных локальной станции, заставляя искать сохранённые credentials.

- 5) Сохранить файл *rdgw.rdp*.
- 6) Сохранить credentials входа через с указанием полного имени рабочей станции, включая суффикс домена (например, *gis.lan* или *da.lan*):

```
cmdkey /add:targetname /user:username /pass:password
```

Например:

```
cmdkey /add:test.da.lan /user:testuser /pass:TestPassw0rd
```

В результате данной настройки пользователь вводит ПИН-код от смарт-карты для аутентификации на шлюзе рабочих столов по сертификату и подключается к удалённой рабочей станции без дополнительного ввода логина и пароля.

7 Настройка входа по сертификатам ЦС Microsoft CA в ОС Linux

Перед настройкой входа по сертификатам на рабочие станции под управлением ОС семейства Linux необходимо убедиться в том, что на рабочих станциях установлены все последние обновления ОС и что на рабочей станции установлена клиентская часть СЗИ от НСД «Блокхост-Сеть 4».

- ① Установка клиентской части СЗИ на рабочие станции под управлением ОС семейства Linux описана в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux».

7.1 Приоритет проверок средств аутентификации при входе

При входе пользователя в ОС семейства Linux действует следующая очередность проверок предъявляемых пользователем средств аутентификации по убыванию приоритета: вход по сертификату, вход по БВПП, вход по паролю:

- 1) При предъявлении пользователем токена, в первую очередь выполняется проверка на наличие на устройстве сертификата для входа:

если сертификат для входа присутствует на токене (вне зависимости от истечения срока действия сертификата, наличия возможности безопасного входа по паролю), будет осуществлена попытка входа по сертификату.

- 2) При отсутствии на предъявляемом токене сертификата для входа, выполняется проверка на наличие на устройстве возможности безопасного входа по паролю:

если безопасный вход по паролю возможен для пользователя, будет осуществлена попытка входа по паролю на токене.

- 3) В случае невозможности входа по сертификату и по паролю на токене, пользователь может воспользоваться входом по паролю без предъявления токена, при этом предъявляемое для входа устройство необходимо извлечь.

7.2 Ввод рабочей станции ОС Linux в домен AD

7.2.1 Ввод рабочей станции под управлением ОС Альт в домен Active Directory

- ① Перед вводом рабочей станции в домен, необходимо предварительно убедиться в **правильности настроек сети** (домен и все вводимые в него рабочие станции находятся в одной виртуальной подсети) и в **отсутствии расхождения по времени** между доменом и рабочей станцией, которая вводится в домен.

Ввод рабочей станции под управлением ОС Альт в домен Active Directory может быть выполнен только одним способом с использованием инструментария sssd.

Подробное описание ввода в домен Active Directory рабочей станции под управлением ОС Альт доступно на сайте справочного центра Альт <https://www.altlinux.org/ActiveDirectory/Login>.

Для ввода в домен рабочей станции в ОС Альт необходимо последовательно выполнить следующие действия:

- 1) Скачать и установить все необходимые для работы пакеты:

```
sudo apt-get install task-auth-ad-sssd samba-client sssd-ad
```

- 2) Если используется домен, оканчивающийся на «.local», выполнить следующую команду:

```
sudo chkconfig avahi-daemon off  
sudo reboot
```

- 3) В *Центре управления системой* перейти в раздел **Пользователи** → **Аутентификация**, выбрать пункт **Домен Active Directory** и заполнить поля (рисунок 7.1).

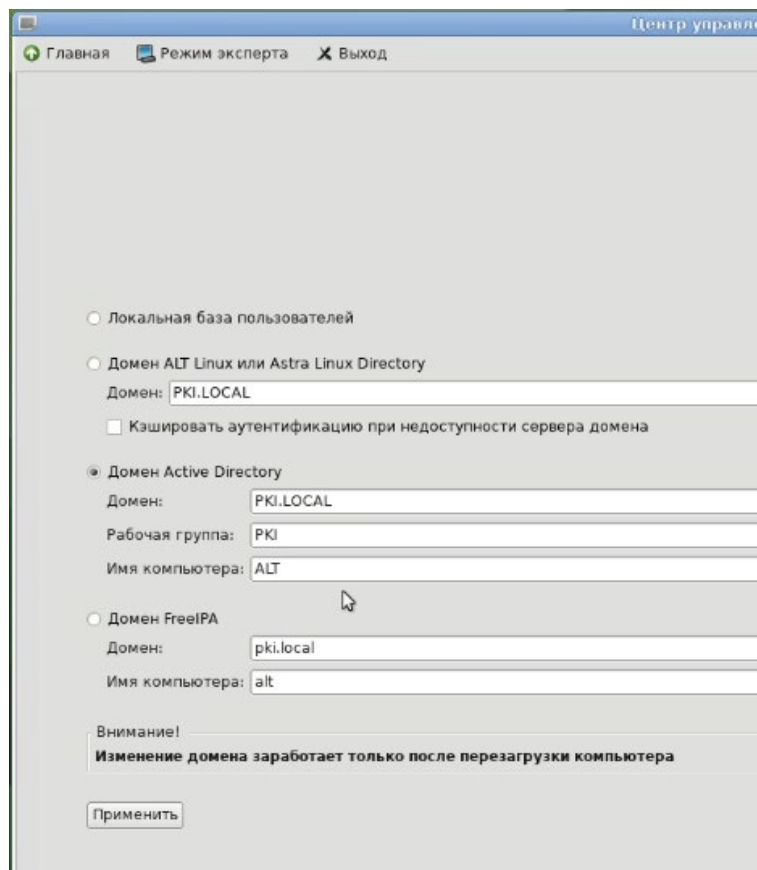


Рисунок 7.1 – Заполнение полей для ввода в домен AD

- 4) Нажать кнопку **Применить**.

7.2.2 Ввод рабочей станции под управлением ОС Astra Linux в домен Active Directory



Перед вводом рабочей станции в домен, необходимо предварительно убедиться в **правильности настроек сети** (домен и все вводимые в него рабочие станции находятся в одной виртуальной подсети) и в **отсутствии расхождения по времени** между доменом и рабочей станцией, которая вводится в домен.

Ввод рабочей станции под управлением Astra Linux в домен Active Directory может быть выполнен с использованием инструментария winbind.

Подробное описание ввода в домен Active Directory рабочей станции под управлением ОС Astra Linux каждым из способов доступно на сайте справочного центра Astra Linux <https://wiki.astralinux.ru/pages/viewpage.action?pageId=27361515>.

Для ввода в домен рабочей станции в ОС Astra Linux необходимо последовательно выполнить следующие действия:

- 1) Скачать и установить все необходимые для работы пакеты:

```
sudo apt install fly-admin-ad-client
```

- 2) Открыть **Панель управления**:

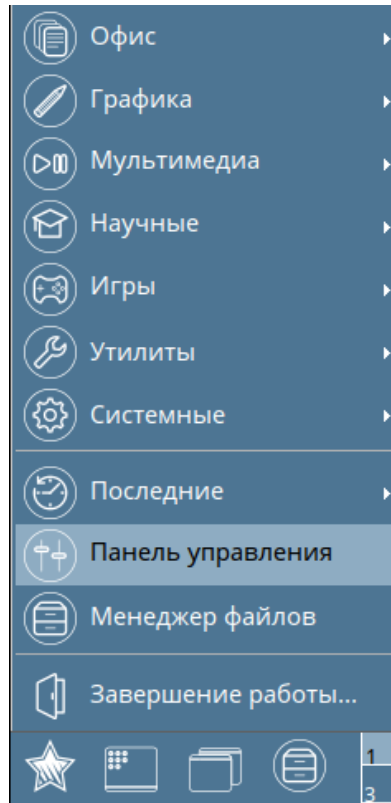


Рисунок 7.2 – Открытие панели управления

3) Выбрать раздел **Сеть** → **Настройка клиента Active Directory**:

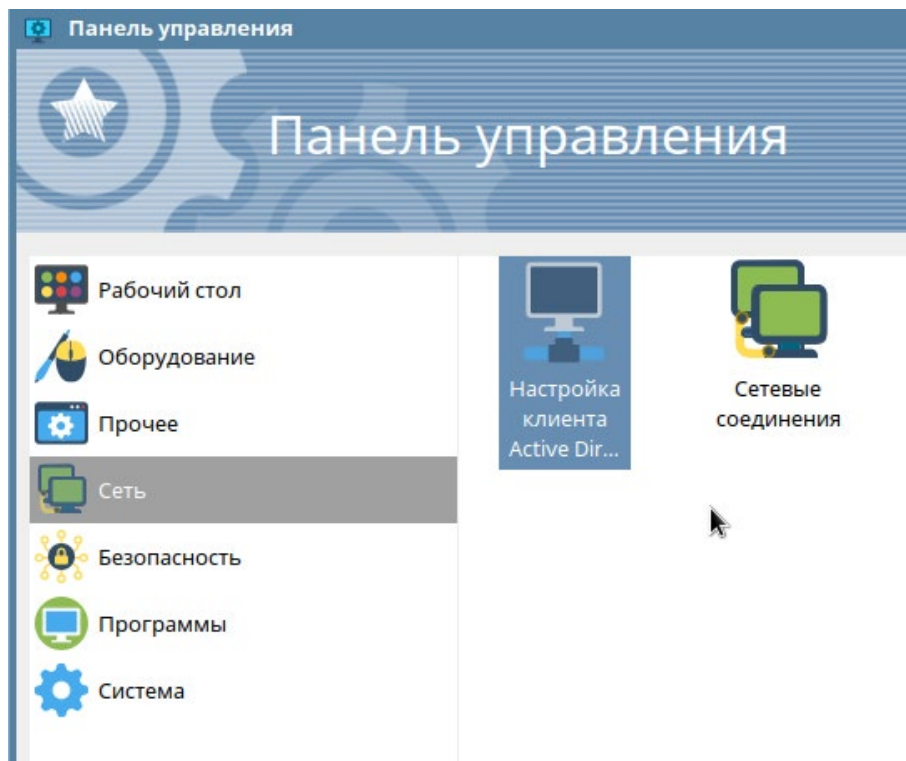
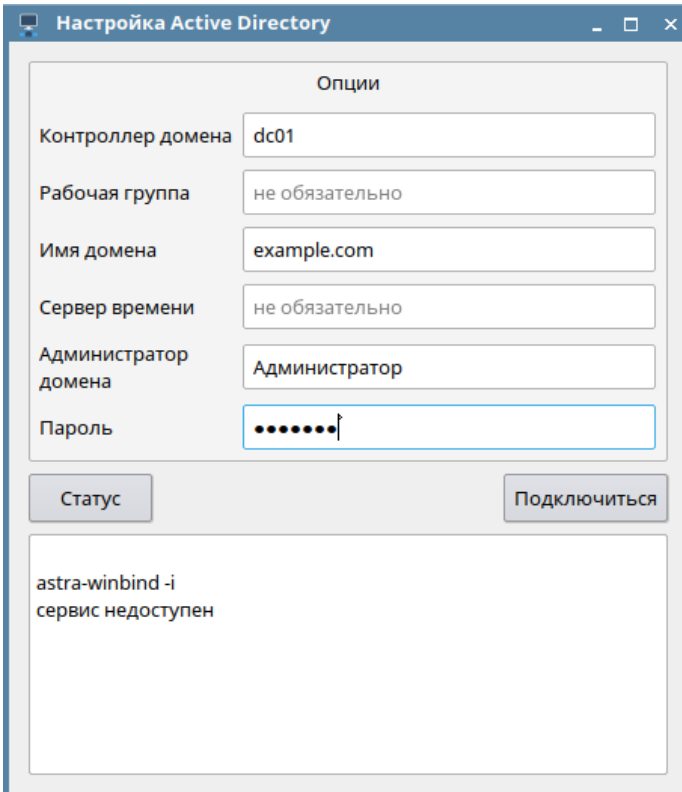


Рисунок 7.3 – Настройка клиента Active Directory

- 4) Заполнить все поля и нажать кнопку **Подключиться**:



Настройка Active Directory

Опции

Контроллер домена dc01

Рабочая группа не обязательно

Имя домена example.com

Сервер времени не обязательно

Администратор домена Администратор

Пароль

Статус Подключиться

astra-winbind -i
сервис недоступен

Рисунок 7.4 – Заполнение полей и подключение

7.2.3 Ввод рабочей станции под управлением РЕД ОС в домен Active Directory

- i** Перед вводом рабочей станции в домен, необходимо предварительно убедиться в **правильности настроек сети** (домен и все вводимые в него рабочие станции находятся в одной виртуальной подсети) и в **отсутствии расхождения по времени** между доменом и рабочей станцией, которая вводится в домен.

Подробное описание ввода в домен Active Directory рабочей станции под управлением РЕД ОС доступно на сайте справочного центра РЕД ОС <https://redos.red-soft.ru/base/arm/arm-domen/arm-msad/>.

Для ввода в домен рабочей станции в РЕД ОС необходимо последовательно выполнить следующие действия:

- 1) Задать имя клиентского компьютера следующей командой:

```
hostnamectl set-hostname <Имя компьютера>.<домен>
```

при этом, имя клиентского компьютера обязательно должно содержать **win.redos**.

2) В файле `/etc/hosts` указать:

```
127.0.0.1 <Имя компьютера>.<домен> <Имя компьютера>
```

3) Проверить доступность клиентского компьютера командой:

```
ping <Имя компьютера>.<домен>
```

4) Установить графический инструмент **join-to-domain** для ввода рабочей станции в домен:

```
dnf update join-to-domain
```

5) После установки пакет будет доступен в графическом меню **Главное меню** → **Системные** → **Ввод ПК в домен**.

6) Для ввода рабочей станции в РЕД ОС в домен Active Directory необходимо выполнить запуск инструмента, введя пароль от пользователя **root**.

7) После успешной аутентификации откроется окно выбора типа домена, выберите пункт **Домен Windows/Samba**:

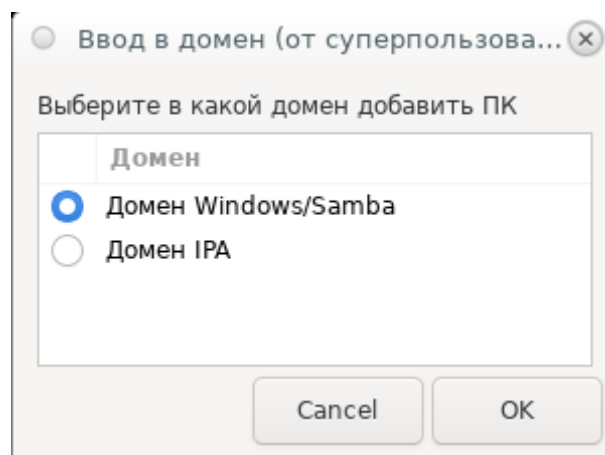


Рисунок 7.5 – Выбор домена

8) После успешной аутентификации откроется основное окно, в котором необходимо указать имя домена, имя и пароль администратора и нажать кнопку **Да**:

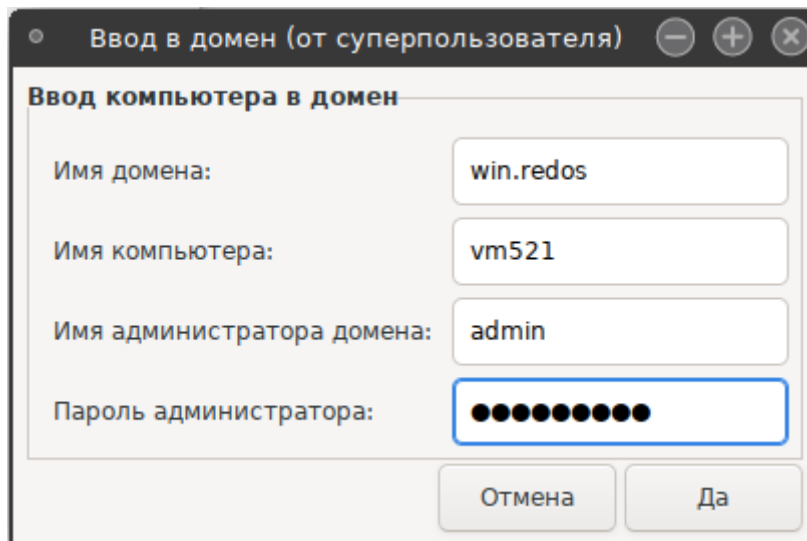


Рисунок 7.6 – Ввод компьютера в домен

7.3 Порядок настройки для входа по сертификатам в ОС Linux

Для возможности аутентификации пользователя на клиентской рабочей станции под управлением СЗИ от НСД «Блокхост-Сеть 4» с использованием цифрового сертификата в ОС Linux необходимо выполнить следующие действия на клиентской рабочей станции:

- 1) Установить корневые сертификаты домена Active Directory.
- 2) Запустить задачу по настройке входа по сертификату через подсистему развертывания.

7.3.1 Экспорт корневого сертификата AD

Для установки корневого сертификата домена Active Directory необходимо перейти к настройкам центра сертификации и выполнить следующие действия:

- 1) В командной строке выполнить команду *mmc*.
- 2) Добавить оснастку **Сертификаты** для локального компьютера (**Файл** → **Добавить или удалить оснастку...**):

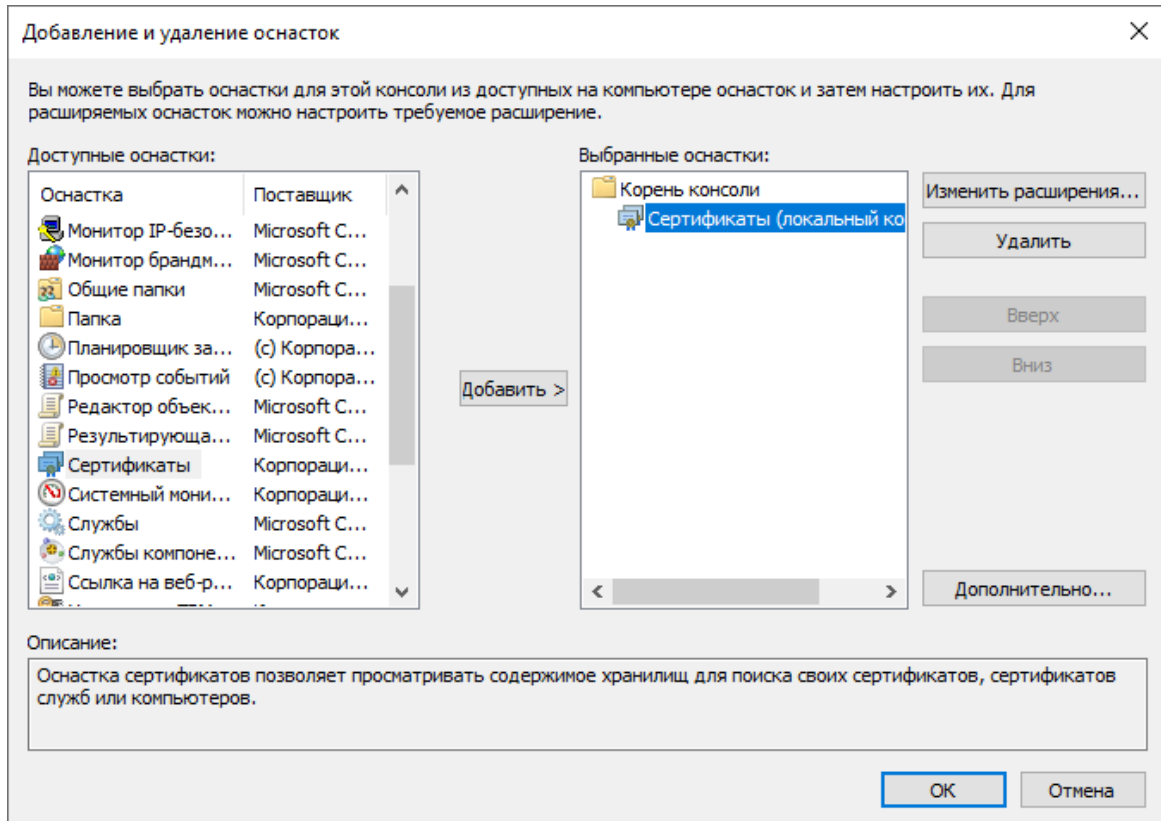
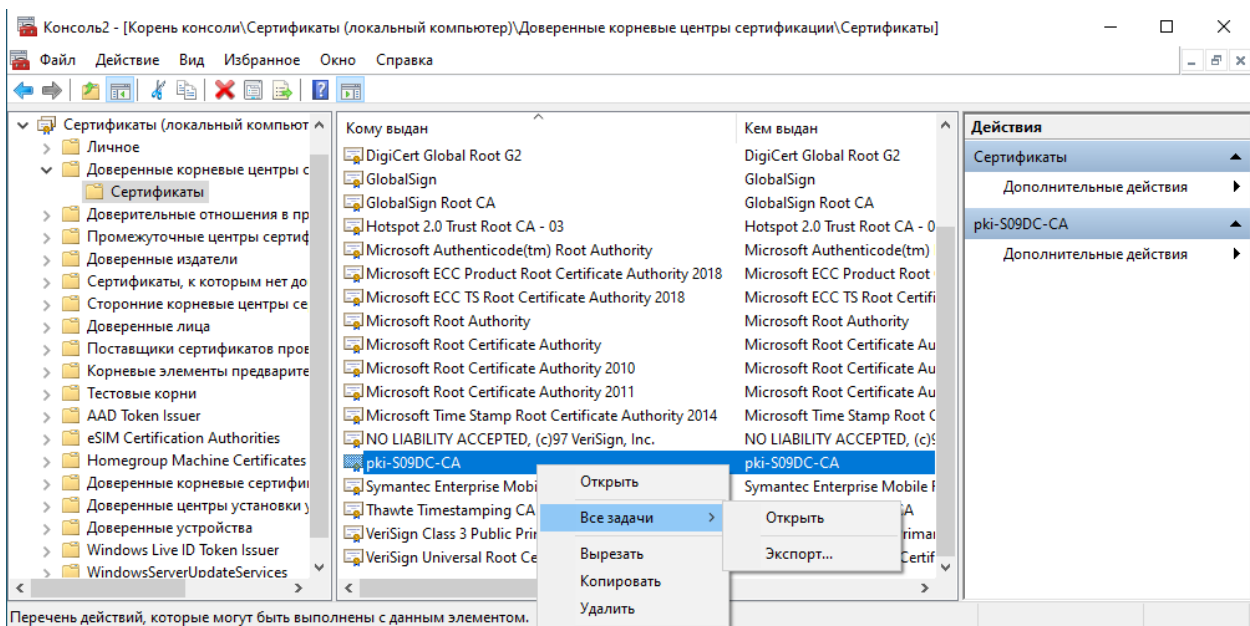
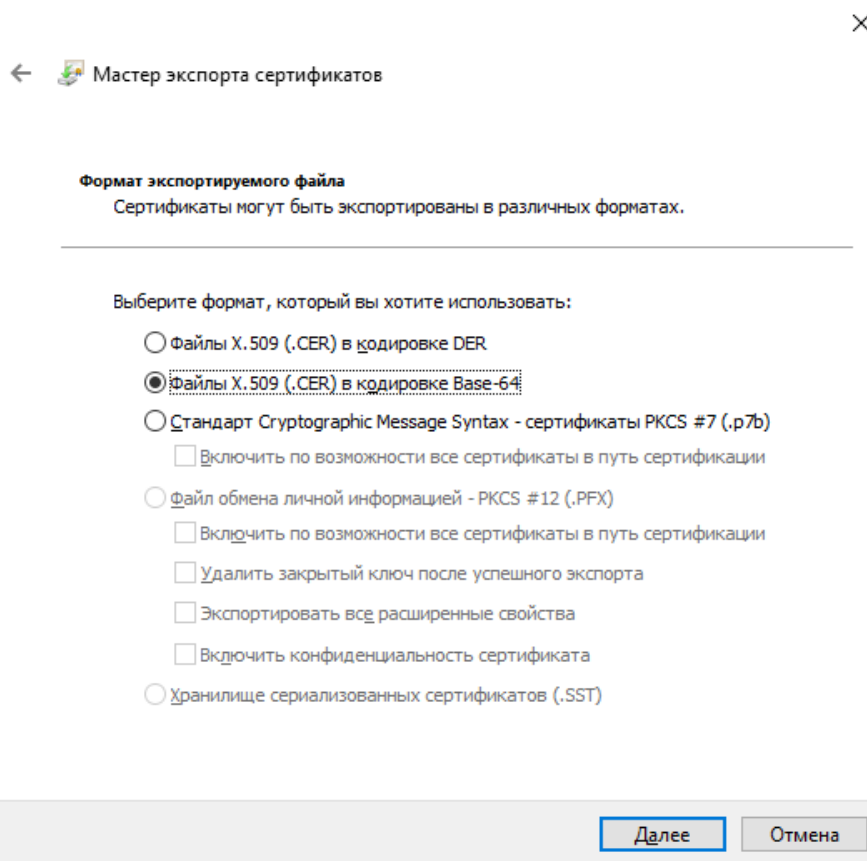


Рисунок 7.7 – Добавление оснастки «Сертификаты»

- 3) Перейти в **Доверенные корневые центры сертификации**, найти корневой сертификат центра сертификации и экспортировать его в Base64 (**контекстное меню** → **Все задачи** → **Экспорт**).



а)



б)

Рисунок 7.8 – Экспорт корневого сертификата центра сертификации



- 4) Записать экспортируемый сертификат на переносное устройство для установки на клиентской рабочей станции.
- 5) На клиентской рабочей станции под управлением СЗИ от НСД «Блокхост-Сеть 4» для сохранения сертификата центра сертификации создать каталог `/etc/certs/`:

```
sudo mkdir /etc/certs
```

- 6) Скопировать в каталог `/etc/certs/` сертификат центра сертификации (`root_base64.cer`):

```
sudo cp /<директория хранения сертификата> /etc/certs
```

7.3.2 Запуск задачи по настройке входа по сертификату через подсистему развертывания

Для создания задачи по настройке входа по сертификату на клиентских рабочих станциях откройте консоль управления Блокхост-Сеть перейдите по кнопке  во вкладку **Задачи**, раскройте меню создания задач по кнопке  и выберите пункт **Настройка входа по сертификатам** (рисунок 7.9).

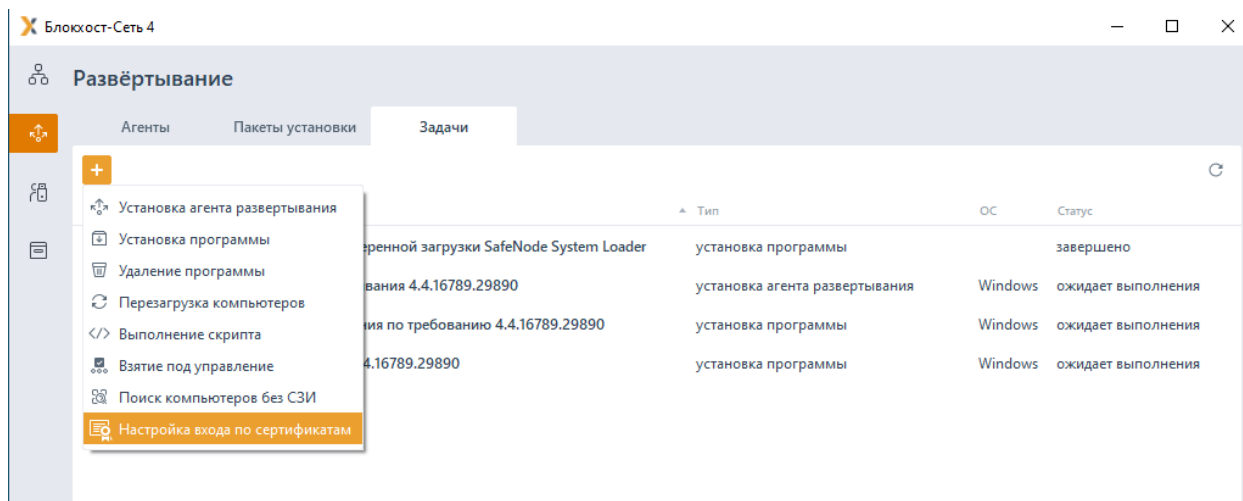


Рисунок 7.9 – Выбор задачи настройки входа по сертификатам

В открывшемся окне создания задачи настройки входа по сертификатам (рисунок 7.10) нажмите кнопку **Выбрать** для перехода к окну выбора домена.

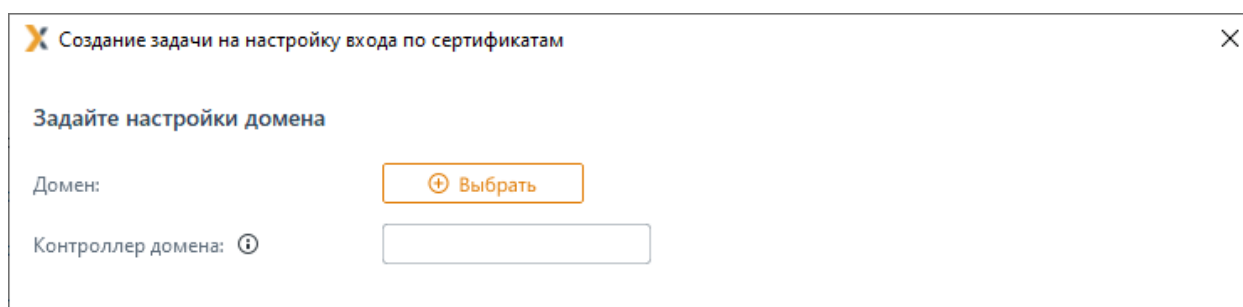
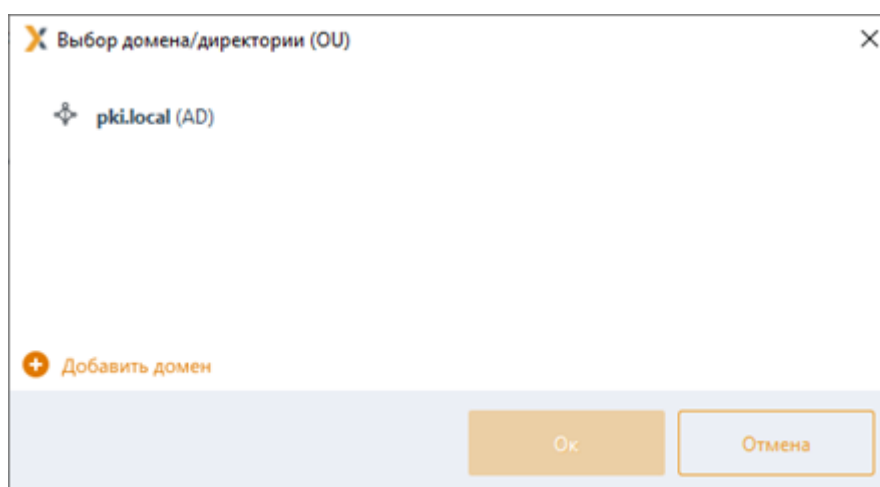
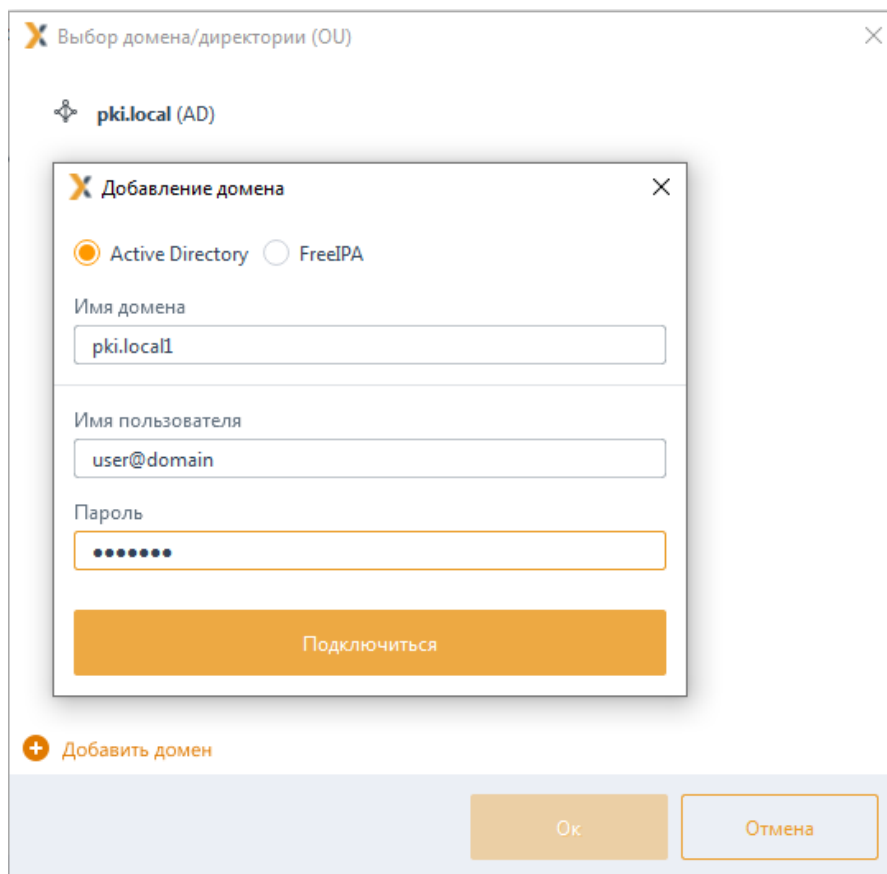


Рисунок 7.10 – Задание настроек домена

Выберите нужный домен (рисунок 7.11 а) или, при отсутствии необходимого домена в списке, добавьте его по ссылке **Добавить домен** (рисунок 7.11 б) и нажмите **ОК**.



а)



б)

Рисунок 7.11 – Выбор домена

Домены во вкладке **Домены** подразделяются на:

- *системные* домены, которые добавляются в список доменов автоматически. Подключение к системному домену (при раскрытии дерева или по двойному щелчку) происходит из-под текущей учетной записи или, в случае неудачи, запрашивается логин/пароль для подключения.
- *пользовательские* домены, которые добавляются по кнопке **+ Добавить домен**. При подключении к пользовательскому домену всегда запрашивается логин/пароль для подключения (попытка подключения из-под текущей учетной записи не выполняется).

После выбора домена нажмите кнопку **Далее** (рисунок 7.12).

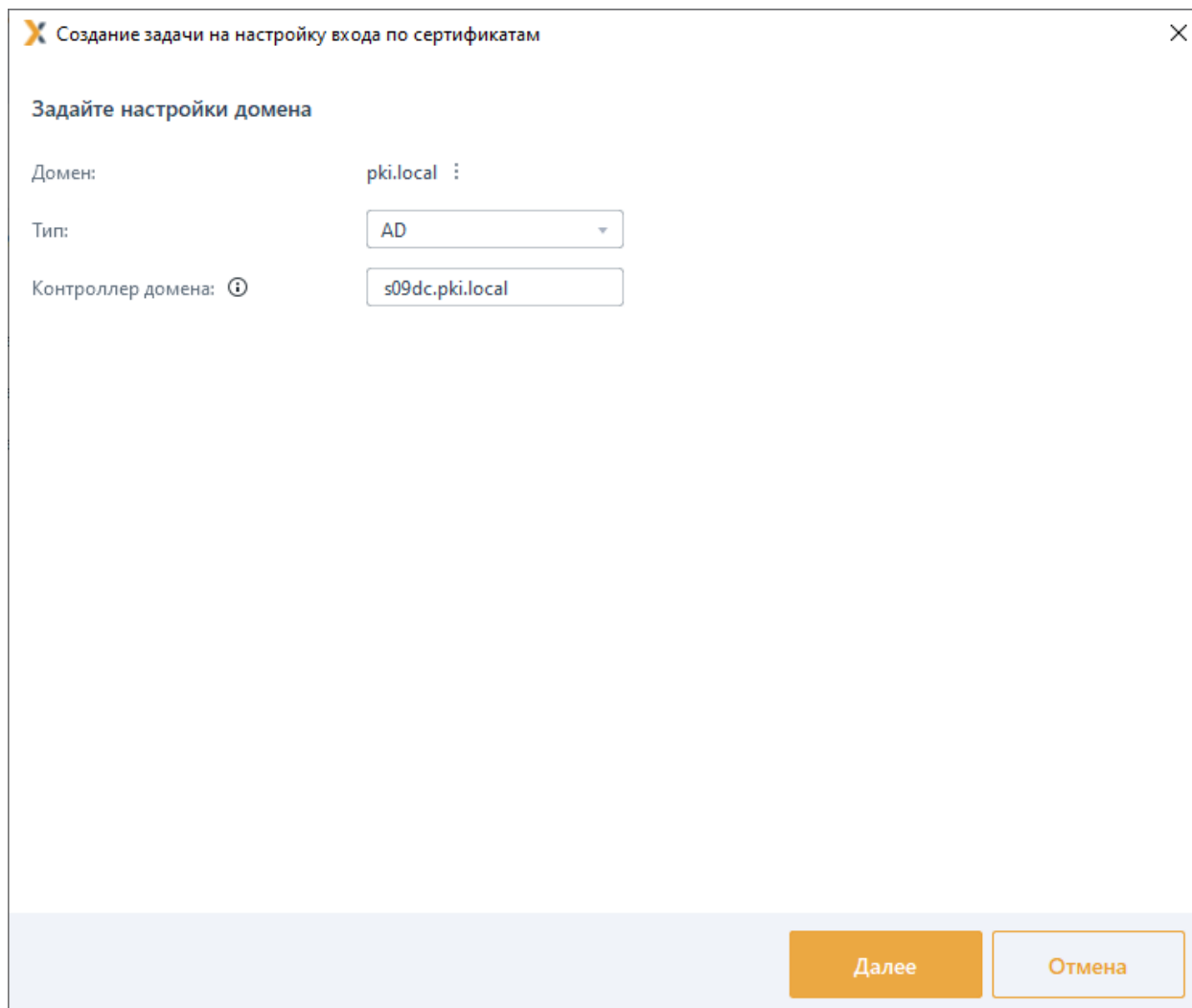


Рисунок 7.12 – Отображение выбранного домена

Выберите в списке те рабочие станции, на которых необходимо выполнить настройку входа по сертификатам, и нажмите кнопку **Далее** (рисунок 7.13).

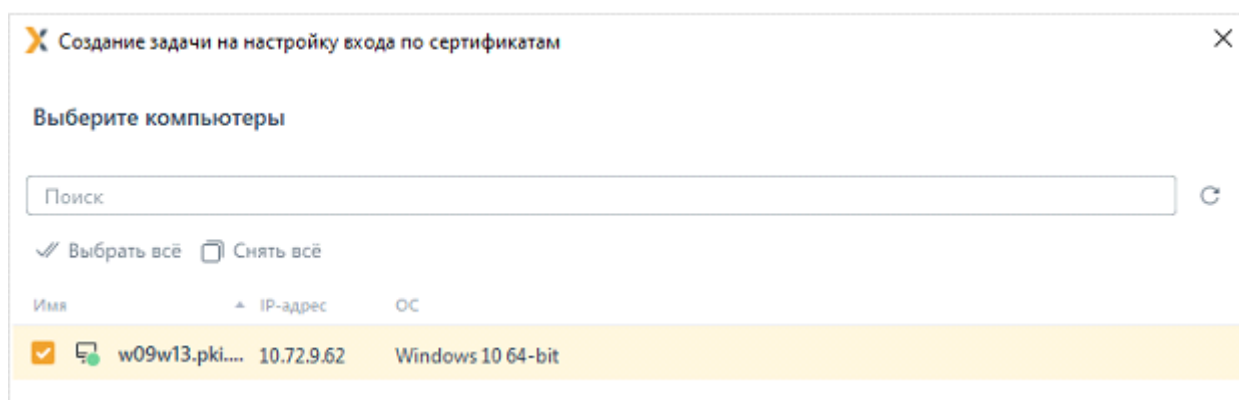
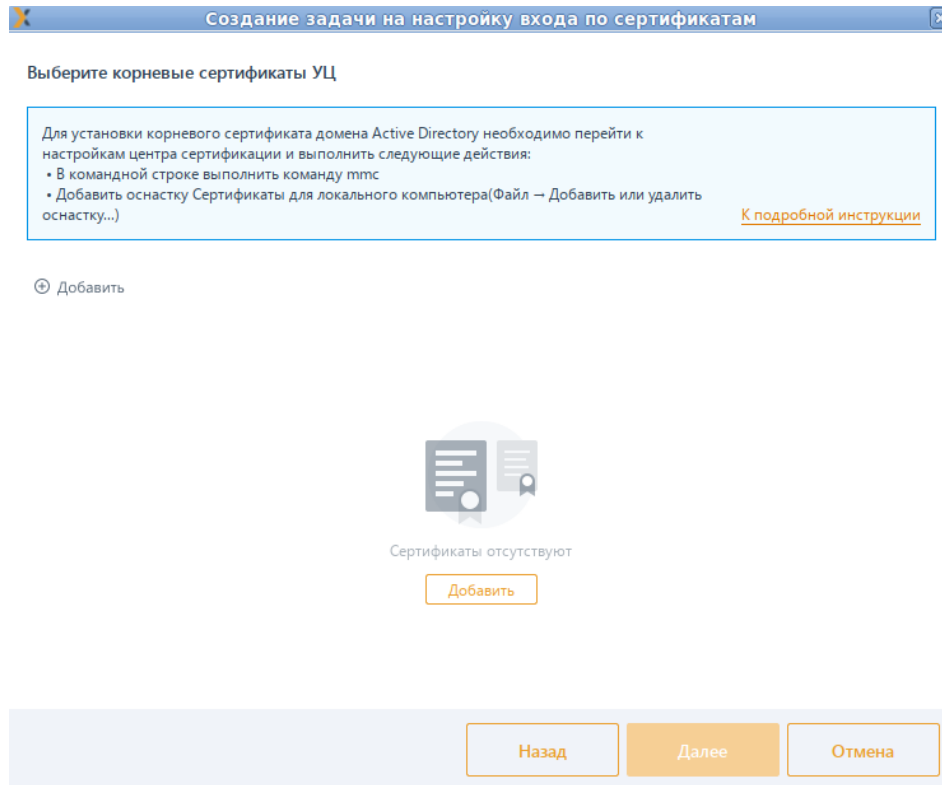


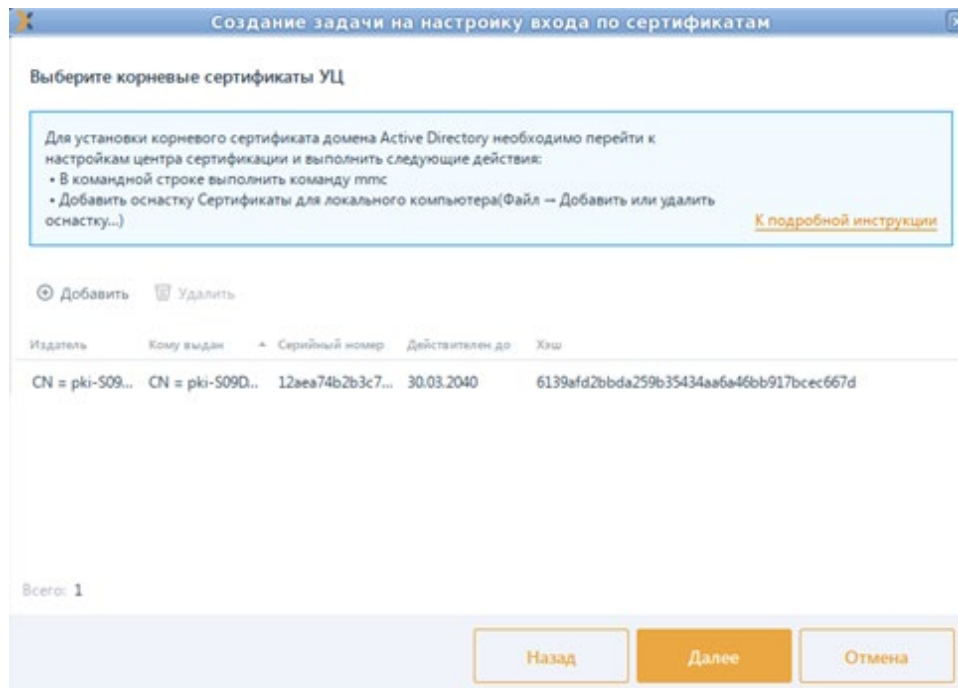
Рисунок 7.13 – Выбор рабочих станций

В следующем окне (рисунок 7.14 а) по кнопке **Добавить** добавьте корневой сертификат домена Active Directory (экспорт подробно описан в разделе **«Экспорт корневого**

сертификата AD»). При необходимости воспользуйтесь инструкцией по установке корневого сертификата доступной по кнопке *К подробной инструкции* (рисунок 7.14 б).



а)

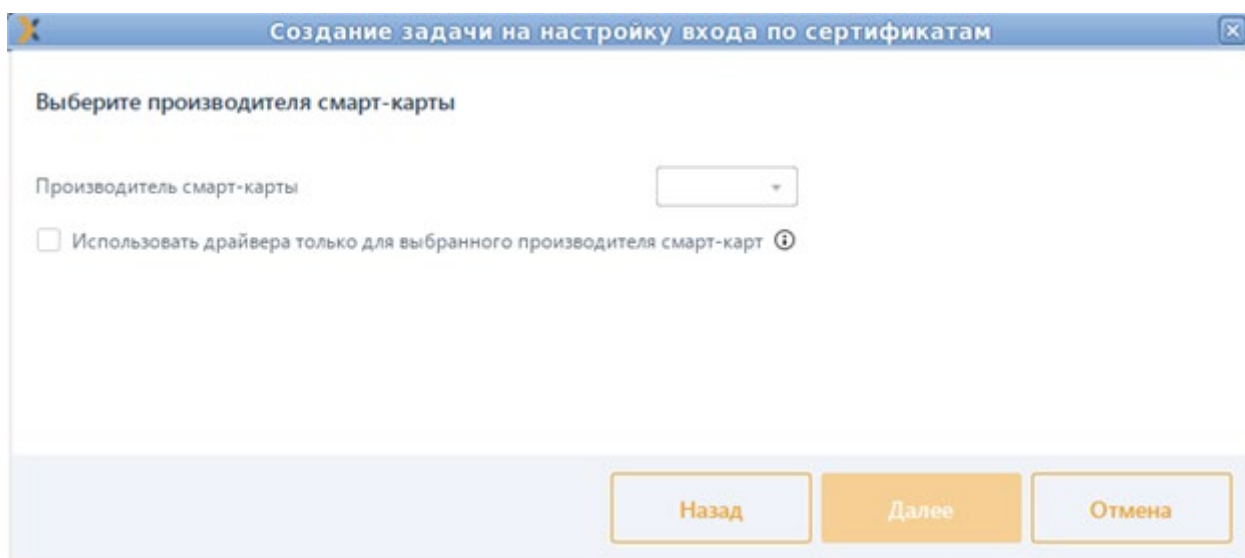


б)

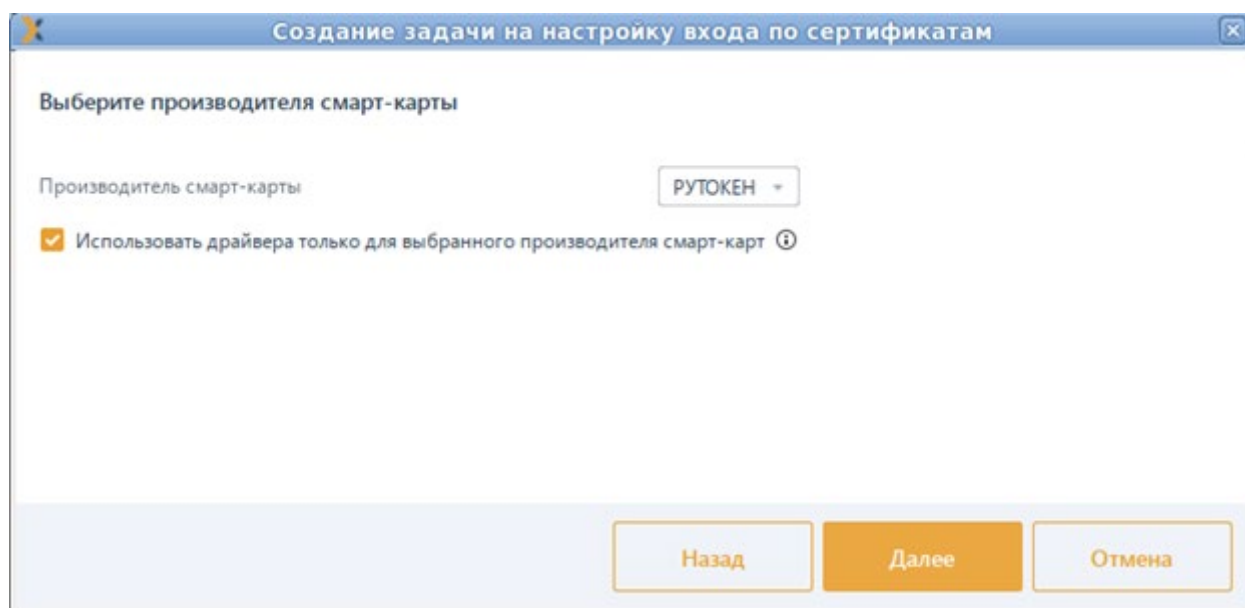
Рисунок 7.14 – Добавление корневого сертификата

В следующем окне выберите из списка производителя смарт-карты для которого будет выполняться настройка входа по сертификатам (рисунок 7.15).

- i** При настройке двухфакторной аутентификации драйвера смарт-карты могут конфликтовать с драйверами других производителей в том числе и системными. Это может привести к невозможности входа с использованием сертификата. Рекомендуется выполнять настройку с установленным параметром **Использовать драйвера только для выбранного производителя смарт-карты** (рисунок 7.15 б).



а)



б)

Рисунок 7.15 – Выбор производителя смарт-карты

Задайте параметры планировщика запуска задачи (подробнее в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 2. Развертывание и аудит» в пункте **«Указание параметров планировщика задачи по установке агента»**), определите интервалы времени выполнения задачи (рисунок 7.16) и нажмите кнопку **Далее** для продолжения создания задачи по настройке входа по сертификатам.

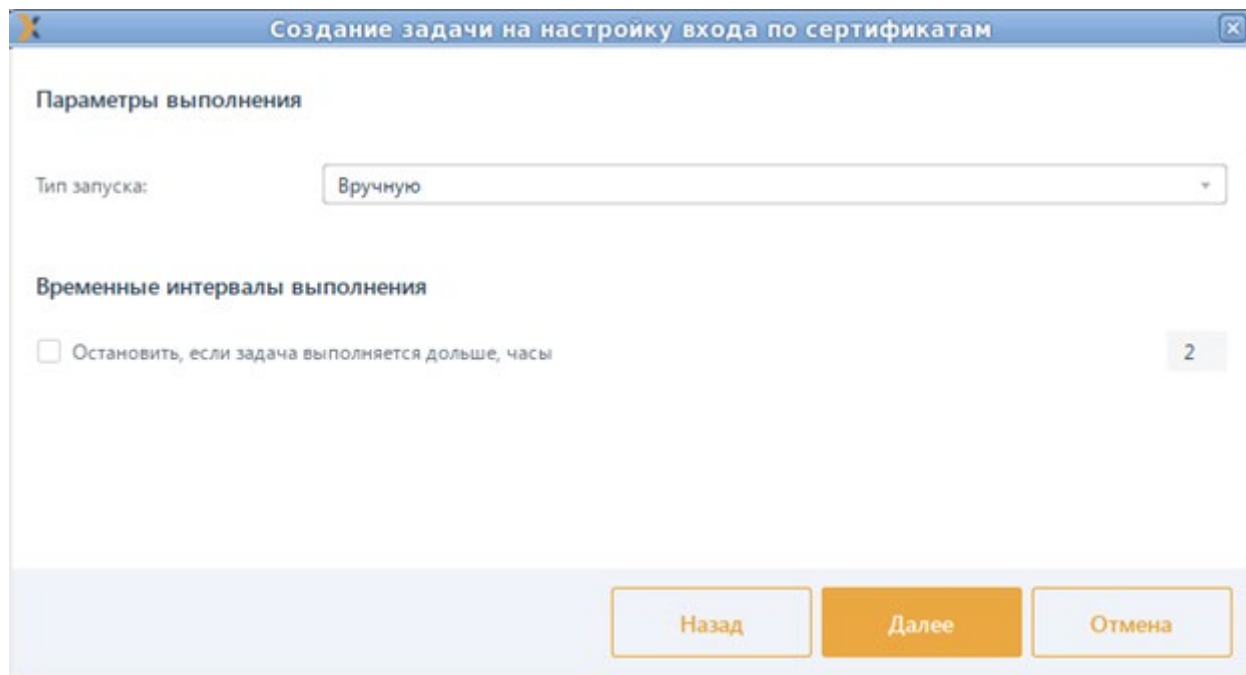


Рисунок 7.16 – Определение параметров планировщика и временных интервалов выполнения задачи

Введите имя создаваемой задачи и нажмите кнопку **Создать**.

В результате во вкладке **Задачи** будет создана новая задача по настройке входа по сертификатам с заданными в ходе работы мастера создания задачи параметрами.

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную.

Для запуска задачи вручную выделите нужную задачу в списке и нажмите в меню кнопку **▶ Запустить** или нажмите кнопку **Запустить** в открывшейся панели справа (подробнее в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 2. Развертывание и аудит» в пункте **«Запуск задачи»**).

В результате выполнения задачи по настройке входа по сертификатам на всех указанных в списке рабочих станциях будет настроен вход по сертификатам для выбранного производителя смарт-карт.

7.4 Особенности при входе в ОС Альт по сертификатам MS CA

Для корректной работы входа в ОС Альт по сертификатам MS CA, выпущенными средствами СЗИ от НСД «Блокхост-Сеть 4», необходимо произвести следующие настройки:

- 1) Добавить служебную учетную запись Enrollment-агента в группу Cert Publishers через оснастку контроллера домена: **Active Directory Users and Computers** → **Свойства пользователя** → вкладка **Member Of**.

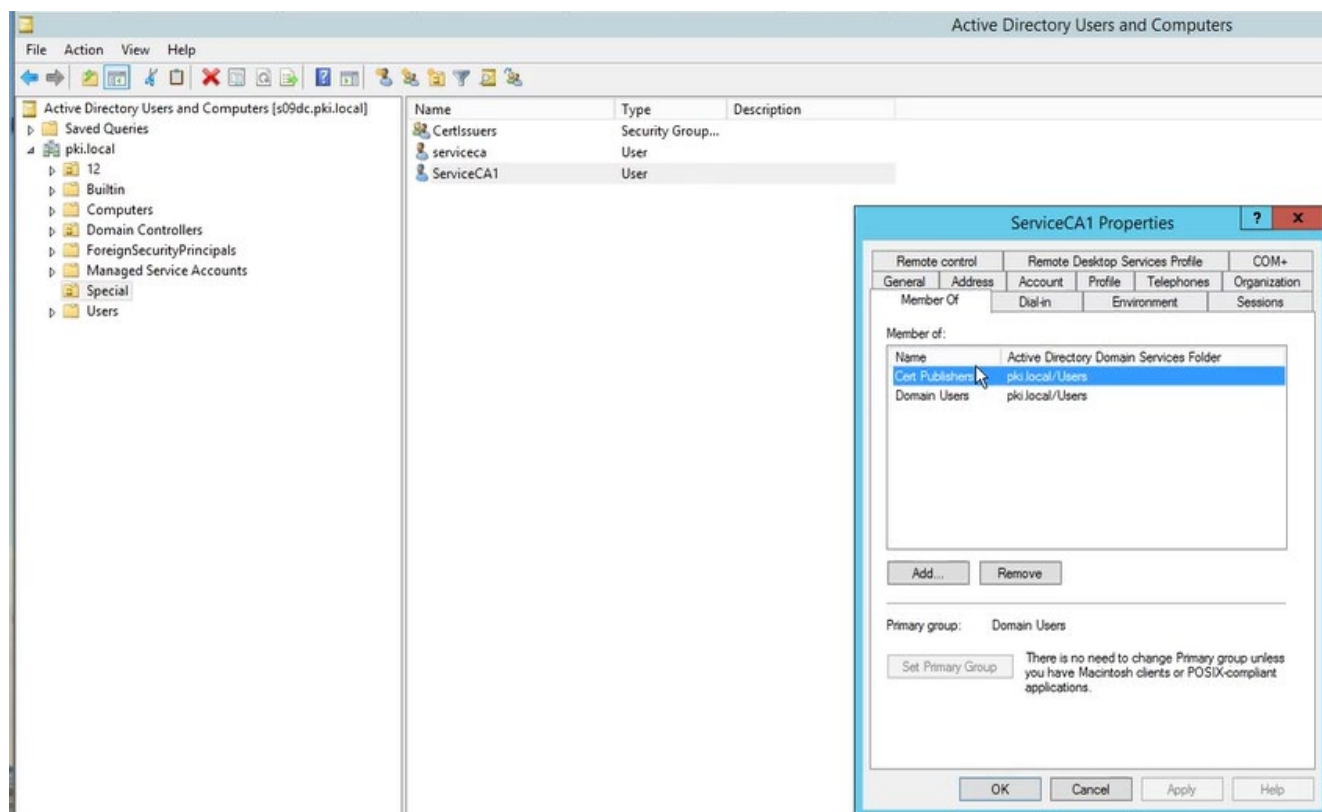


Рисунок 7.17 – Добавление служебной учетной записи в группу *Cert Publishers*


- 2) Установить флаг **Публиковать выдаваемые сертификаты в Active Directory** в настройках выпуска сертификатов консоли управления Блокхост-Сеть при создании профиля: **Настройки**  → **Выпуск сертификатов** → создание профиля **Microsoft CA** (рисунок 7.18).

Рисунок 7.18 – Установка флага **Публиковать выдаваемые сертификаты в Active Directory**

3) Выдать токен для входа по управляемому сертификату с помощью консоли управления (см. документ «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 5. Управление токенами»).

Все выпущенные сертификаты будут публиковаться в Active Directory пользователя, указанного при выпуске токена.

Просмотреть сертификаты можно на контроллере домена: в оснастке **Active Directory Users and Computers** выбрать **View** → **Advanced Features**, затем перейти в оснастке к **Свойства пользователя** → вкладка **Published Certificates** (рисунок 7.19).

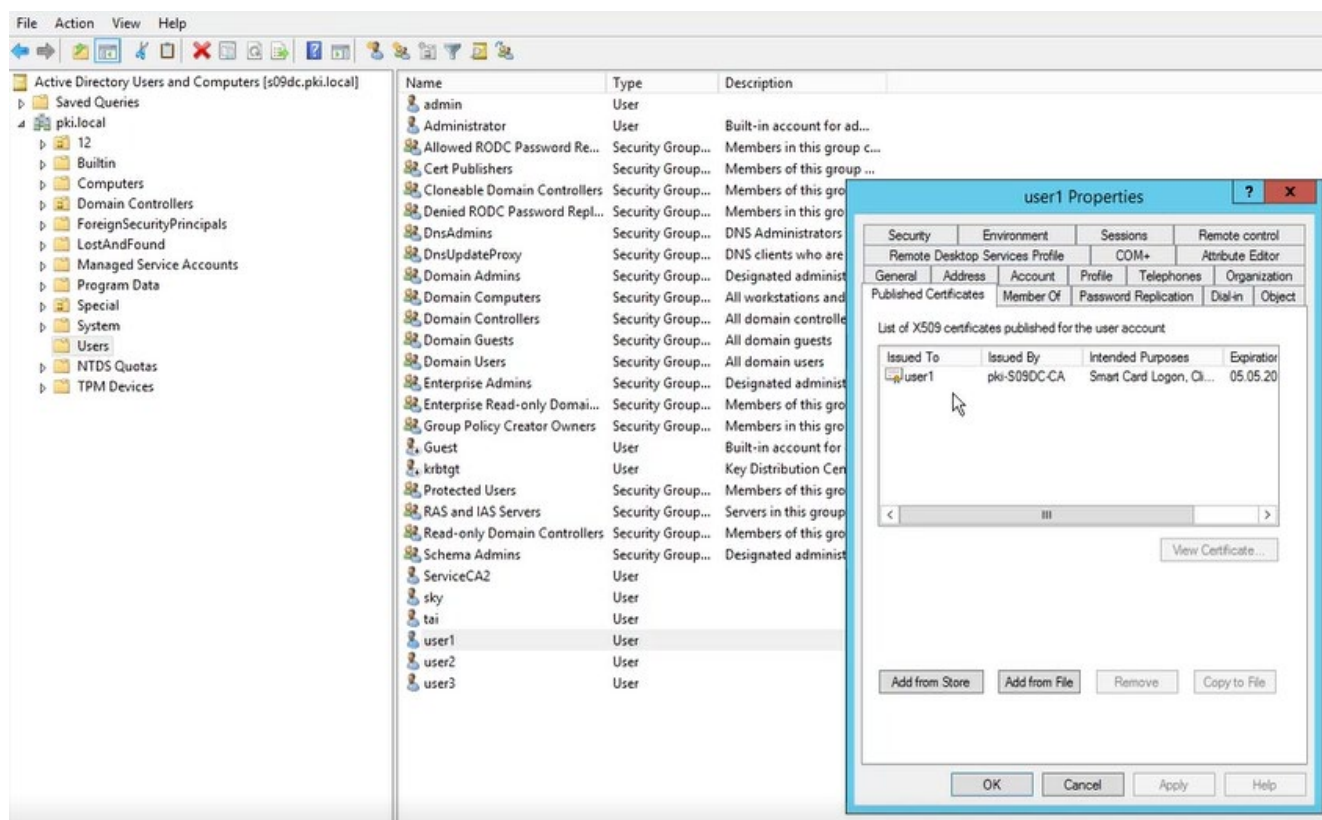


Рисунок 7.19 – Публикация сертификата в **Active Directory**

Также, список сертификатов можно получить через LDAP-запрос (для этого следует включить в список запрашиваемых атрибутов **userCertificate**).



После проведения настроек вход по ранее выданным токенам в ОС Альт будет невозможен. Для входа по ранее выданным токенам необходимо заново выпустить все токены, с помощью которых планируется аутентификация в ОС Альт или добавить выпущенный сертификат в **Published Certificates** вручную на контроллере домена или отправив соответствующий LDAP-запрос.

7.5 Особенности при входе в ОС Astra Linux с настроенным входом по сертификатам

Если рабочая станция под управлением ОС Astra Linux введена в домен с использованием инструментария sssd и на рабочей станции настроен вход по сертификатам, при попытке входа по БВПП ОС будет запрашивать ввод ПИН-кода повторно, так как токен настроен в `/etc/krb5.conf`.


Если вход по сертификатам больше планируется использовать, можно отключить токен, закомментировав в `/etc/krb5.conf` строку:

```
pkinit_identities = PKCS11:module_name=/usr/lib/librtpkcs11ecp.so
```

где:

`pkinit_identities` – библиотека используемого токена.

В дальнейшем, при входе пользователя по БВПП, ПИН-код не будет запрашиваться повторно.

-  Необходимо учитывать, что данное действие приведет к невозможности входа пользователя по сертификату.


7.6 Удаление сертификата из Active Directory пользователя

Для удаления сертификата из Active Directory пользователя можно воспользоваться двумя способами:

- 1) Отозвать токен через консоль управления Блокхост-Сеть. При этом выпущенный ранее сертификат автоматически удаляется из Active Directory пользователя.

-  При отзыве через оснастку Windows сертификат не удаляется.

- 2) Удалить сертификат вручную на контроллере домена: **Active Directory Users and Computers** → **Свойства пользователя** → вкладка **Published Certificates**.

-  Если служебная учетная запись enrollment-агента будет исключена из **Cert Publishers**, при этом сохранен установленный флаг **Публиковать выдаваемые сертификаты в Active Directory**, то система при каждом выпуске/отзыве токена будет выдавать соответствующее предупреждение о невозможности опубликовать/удалить сертификат в Active Directory.

7.7 Настройка публикации списка отзыва сертификатов в ОС Linux

При установке серверной части СЗИ от НСД «Блокхост-Сеть 4» на рабочей станции под управлением ОС Linux при выпуске токена для входа по управляемому сертификату, в результате того, что в ОС Linux списки отзыва сертификатов распространяются по протоколу *ldap*, может возникнуть ошибка вида:

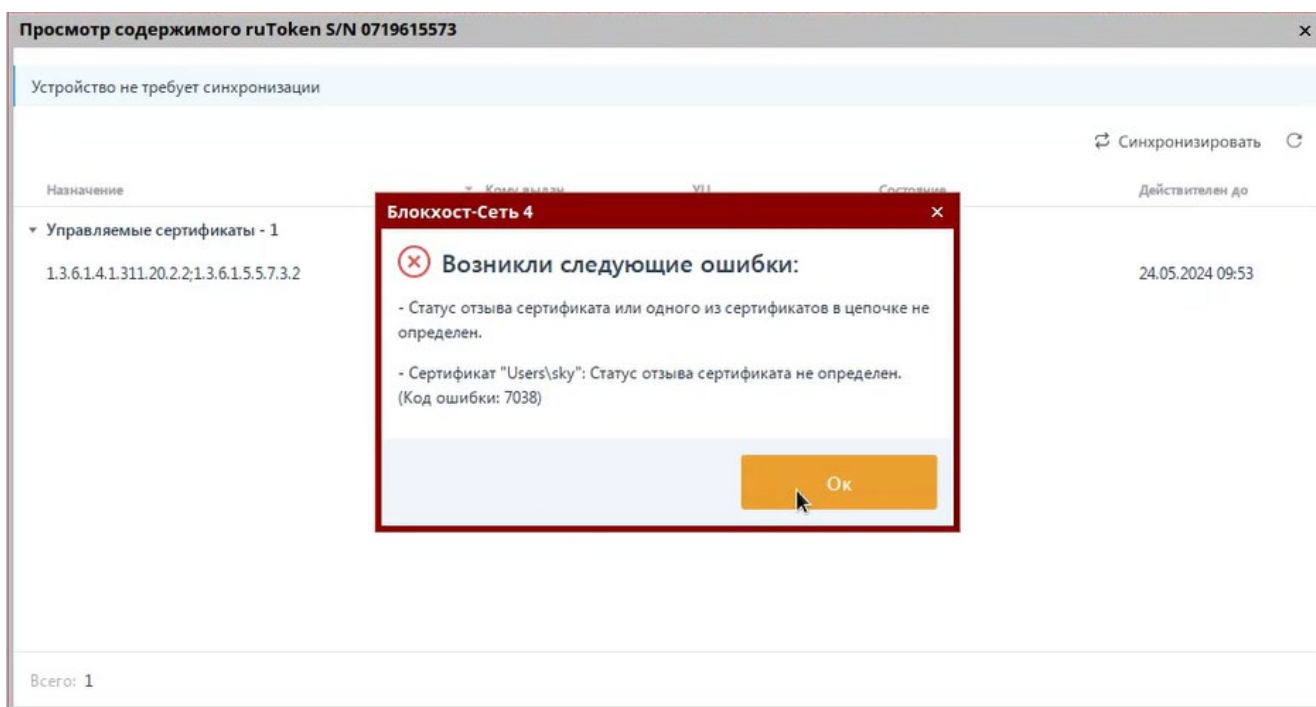


Рисунок 7.20 – Ошибка определения статуса отзыва сертификата

В этом случае, необходимо выполнить настройку публикации списка отзыва сертификатов по протоколу *http*.

- ❗ После выполнения настроек для публикации списка отзывов сертификатов по протоколу *http*, чтобы корректно определялся статус сертификата на токене, все выданные токены для входа по управляемому сертификату необходимо перевыпустить!

7.7.1 Настройки центра сертификации

Для настройки публикации списка отзыва сертификатов по протоколу *http* перейдите к настройкам центра сертификации и откройте оснастку **Certification Authority** (рисунок 7.21).

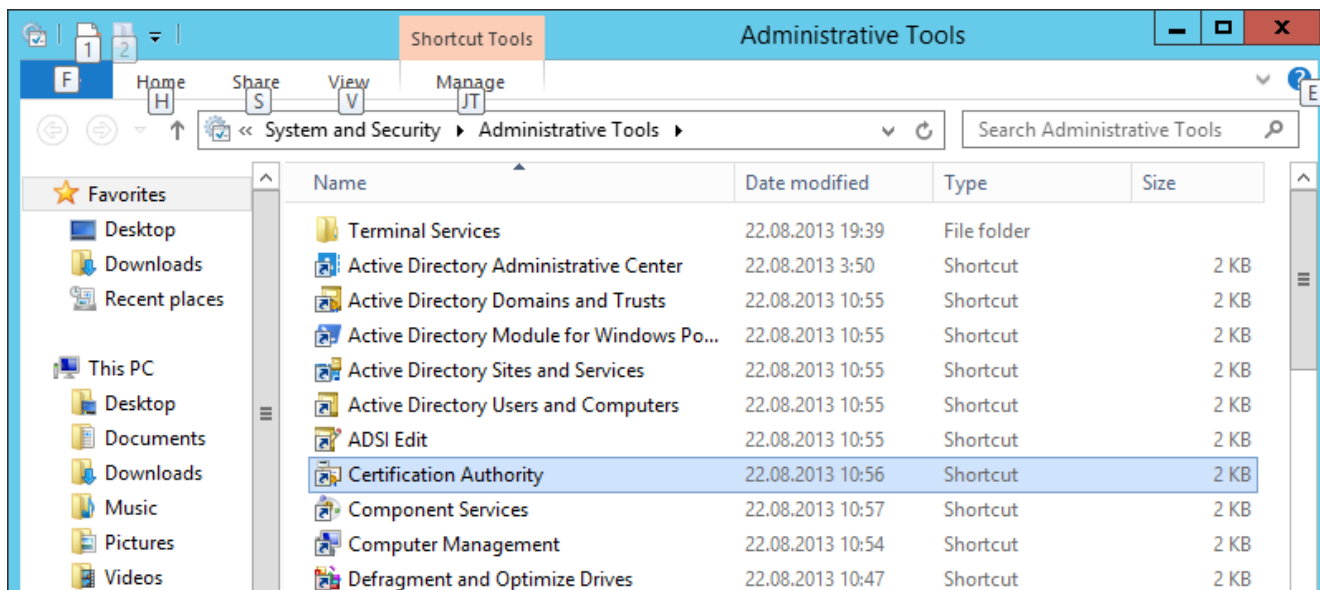


Рисунок 7.21 – Выбор оснастки **Certification Authority**

Окно консоли будет выглядеть следующим образом:

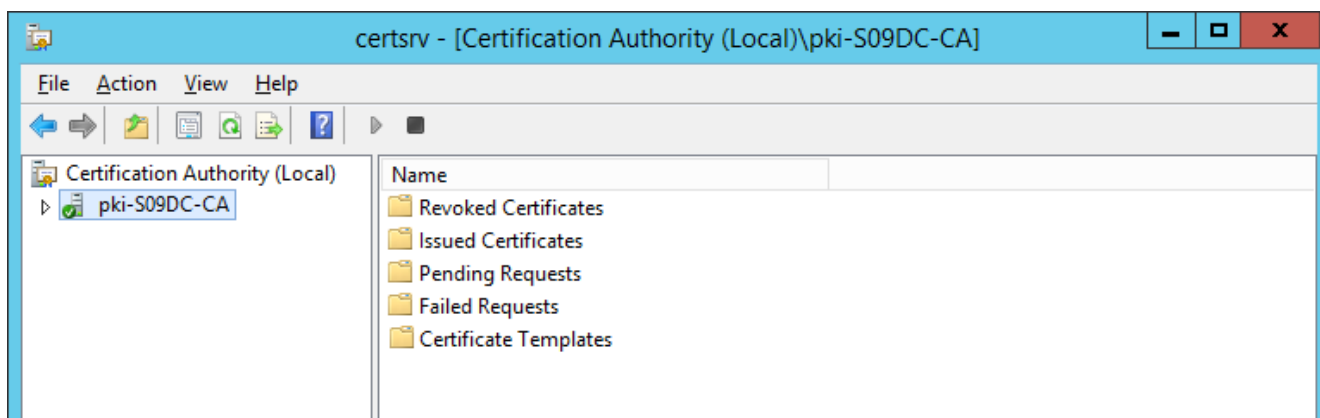


Рисунок 7.22 – Консоль центра сертификации

В левой части окна перейдите в свойства центра сертификации (**Properties**) по щелчку правой кнопки мыши (рисунок 7.23).

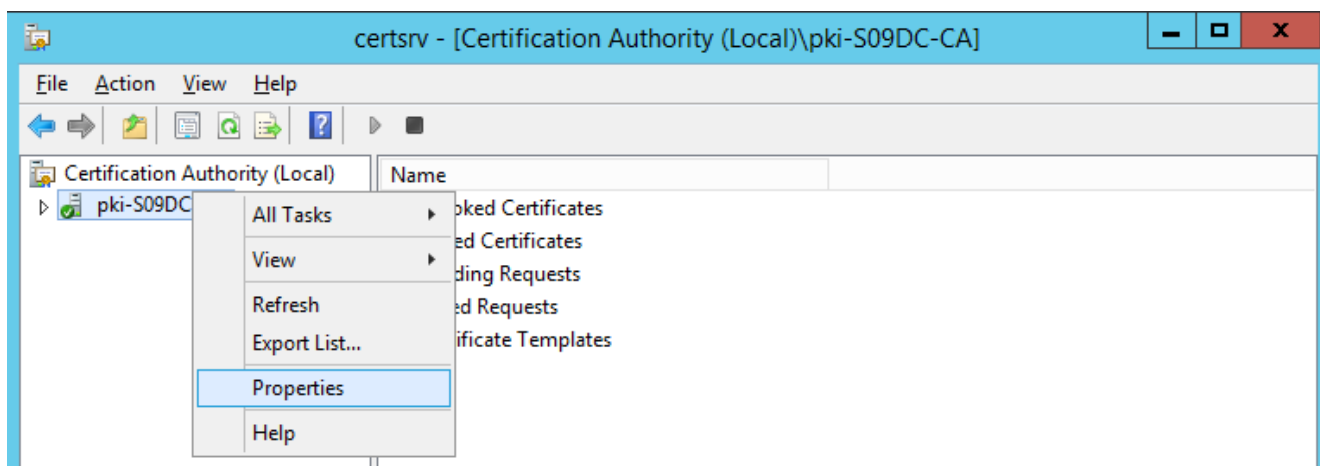


Рисунок 7.23 – Настройка свойств центра сертификации

Перейдите во вкладку **Extensions** (рисунок 7.24), выберите расширение **CRL Distribution Point (CDP)**.

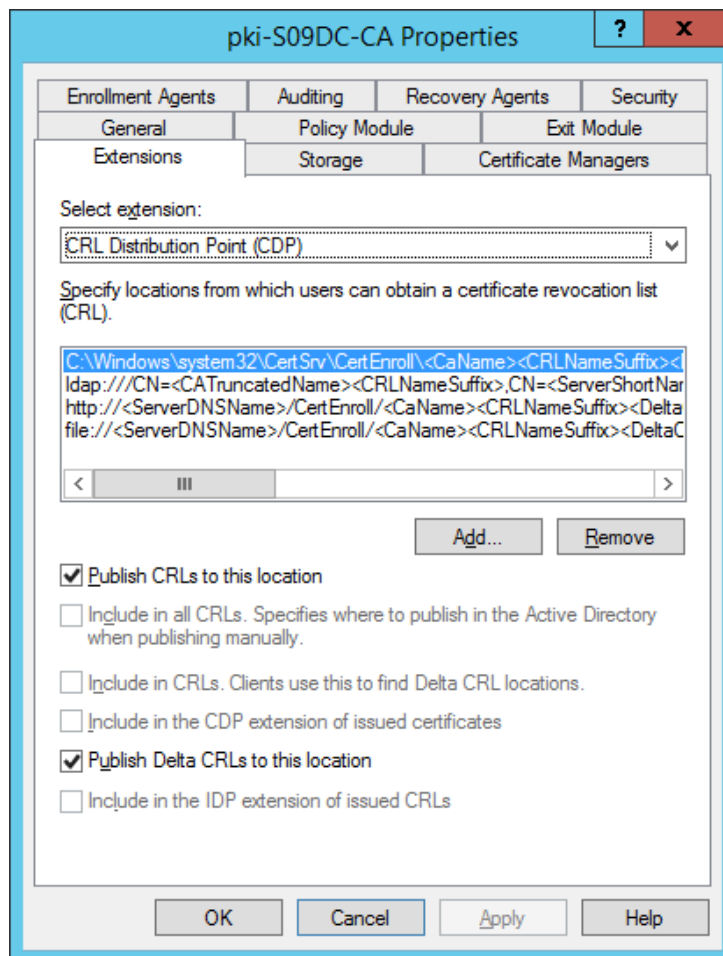
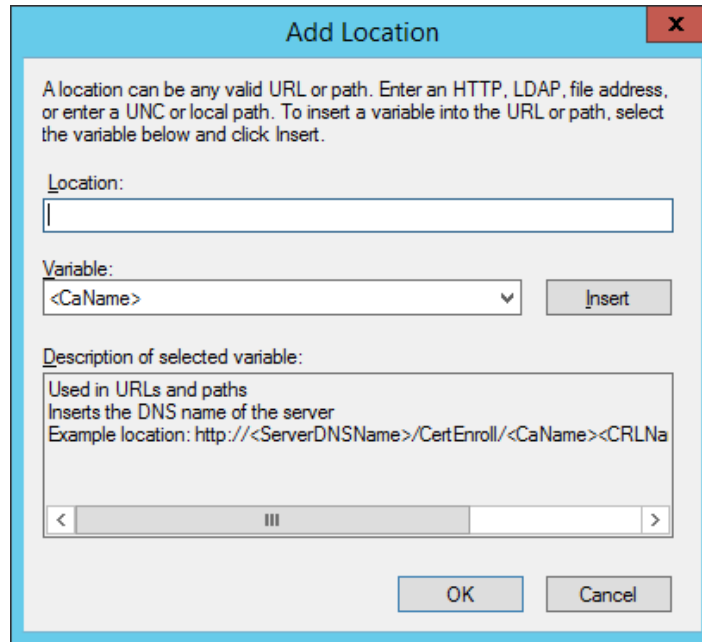


Рисунок 7.24 – Переход во вкладку **Extensions**

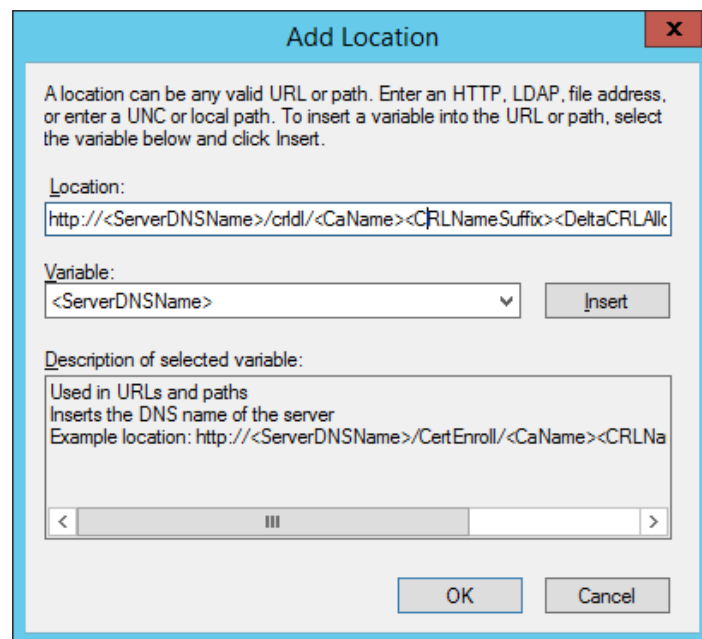
Нажмите кнопку **Добавить (Add)** для добавления настроек (рисунок 7.25), в поле **Location** введите строку:

`http://<ServerDNSName>/crl/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`

и нажмите **OK**.



а)



б)

Рисунок 7.25 – Добавление места публикации списка отзывов

Установите флаги (рисунок 7.26) для включения созданной записи в выдаваемые сертификаты.

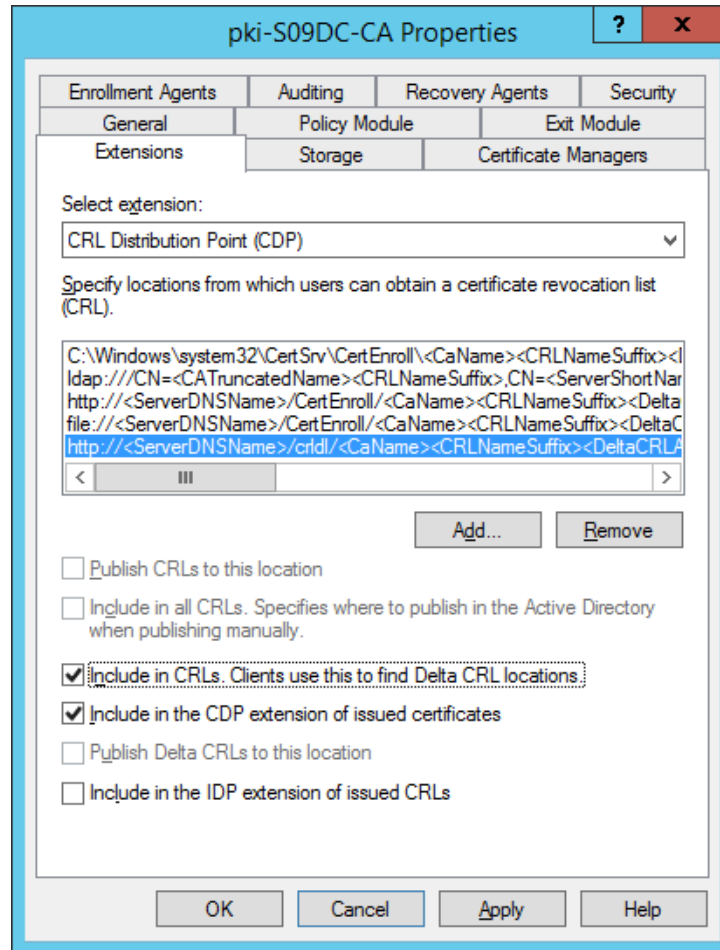


Рисунок 7.26 – Включение созданной записи в выдаваемые сертификаты
Отключите те же флаги для *ldap* протокола (рисунок 7.27).

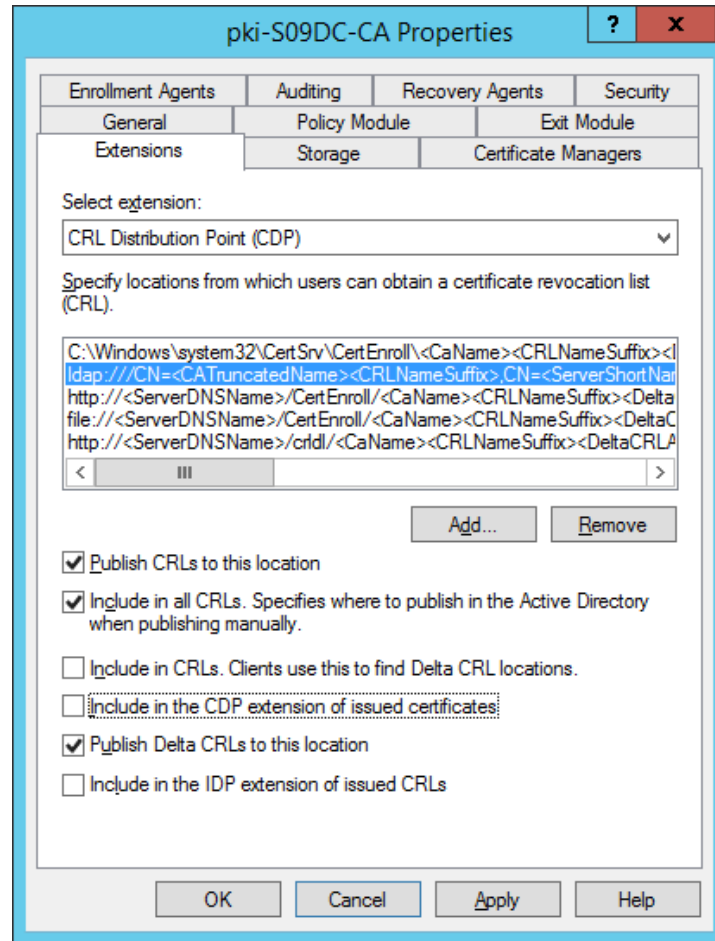


Рисунок 7.27 – Отключение в протоколе ldap

Нажмите кнопку **Добавить (Add)** для добавления места хранения выпускаемого списка отзывов (рисунок 7.28) и укажите в поле **Location** адрес:

`\\s09dc\crl\dist$\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`

и нажмите **OK**.

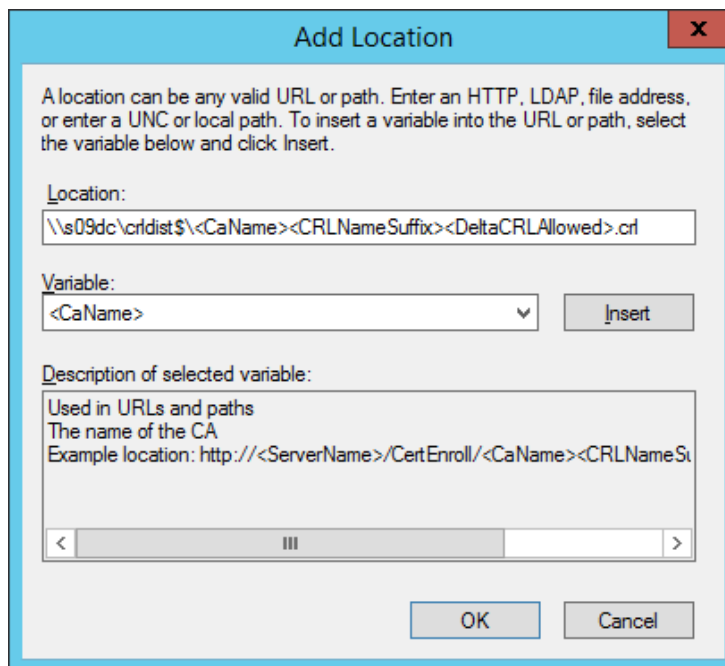


Рисунок 7.28 – Добавление места хранения выпускаемого списка отзывов

Для добавленной записи установите следующие флаги (рисунок 7.29):

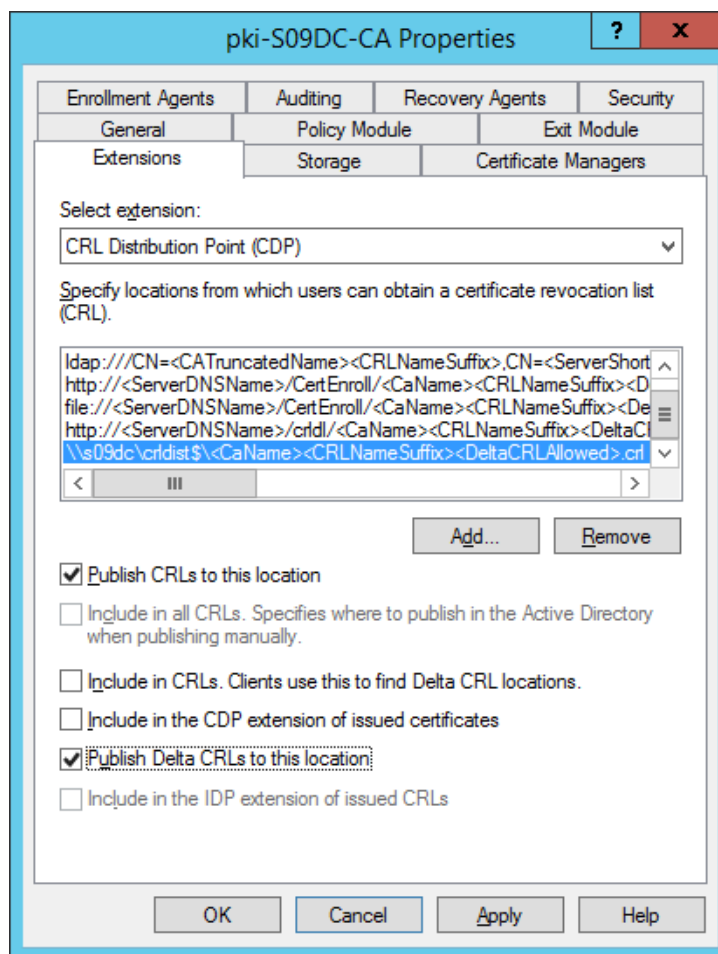


Рисунок 7.29 – Установка публикации в выбранной локации

Нажмите **Применить (Apply)**.

7.7.2 Настройки на контроллере домена

Перейдите к настройкам контроллера домена и откройте оснастку **DNS** (рисунок 7.30).

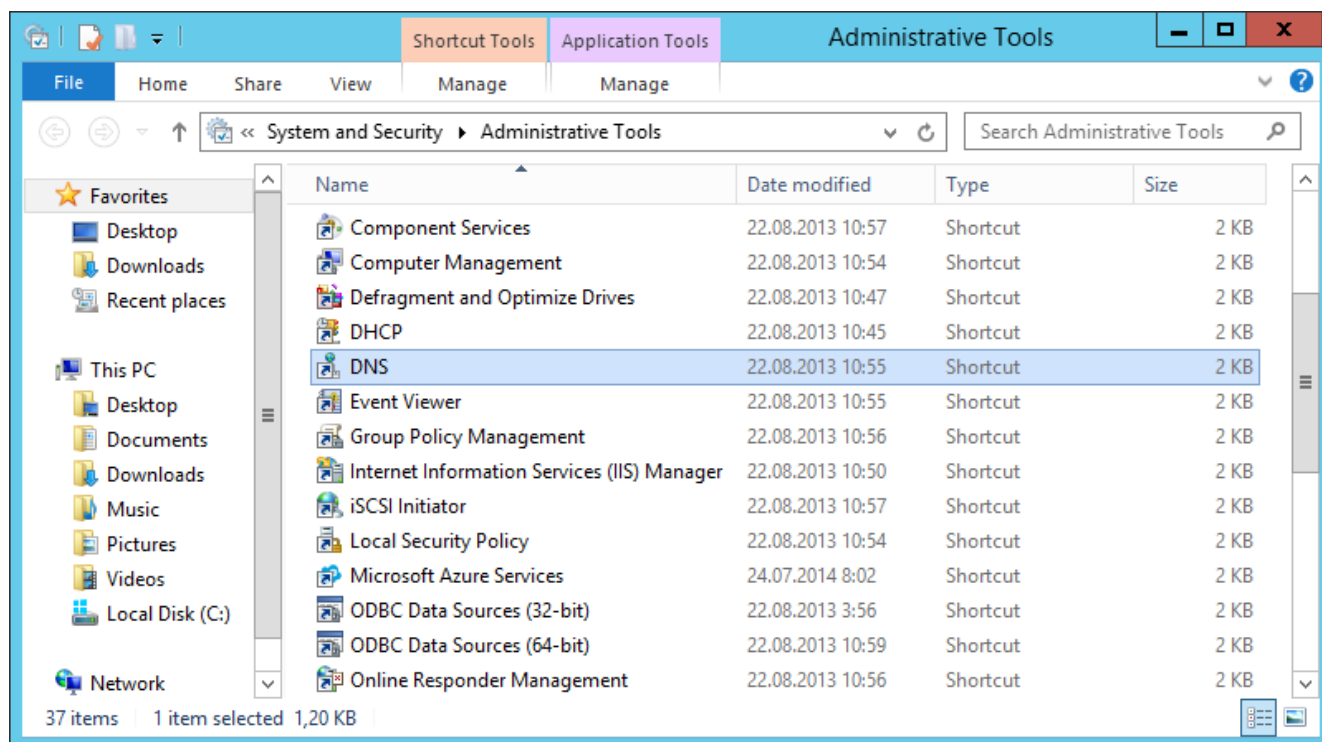


Рисунок 7.30 – Выбор оснастки **DNS**

Окно консоли будет выглядеть следующим образом:

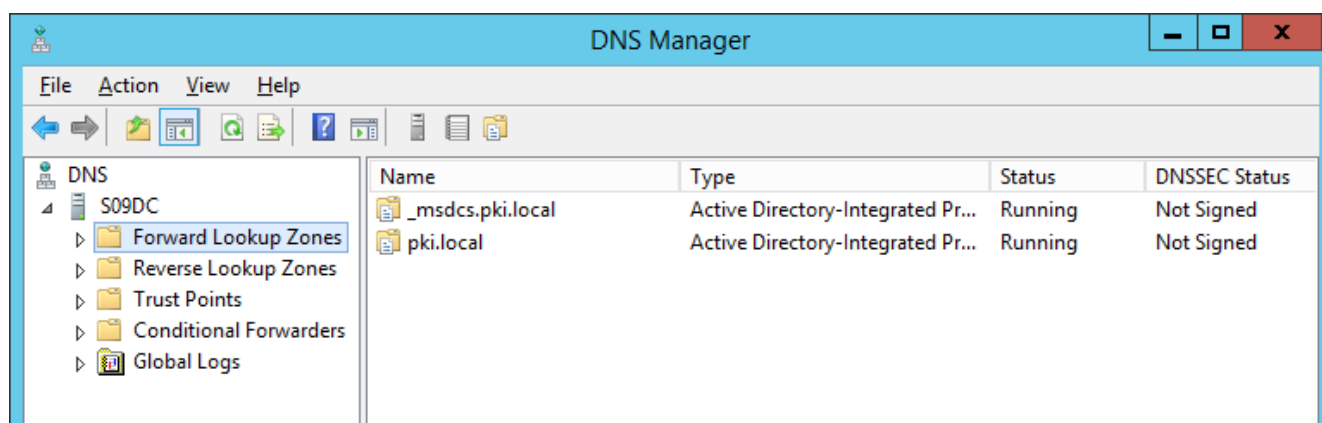


Рисунок 7.31 – Консоль контроллера домена **DNS**

В левой части окна перейдите раскройте пункт **Forward Lookup Zones**, перейдите к домену и по щелчку правой кнопки мыши выберите **New Host** (рисунок 7.32).

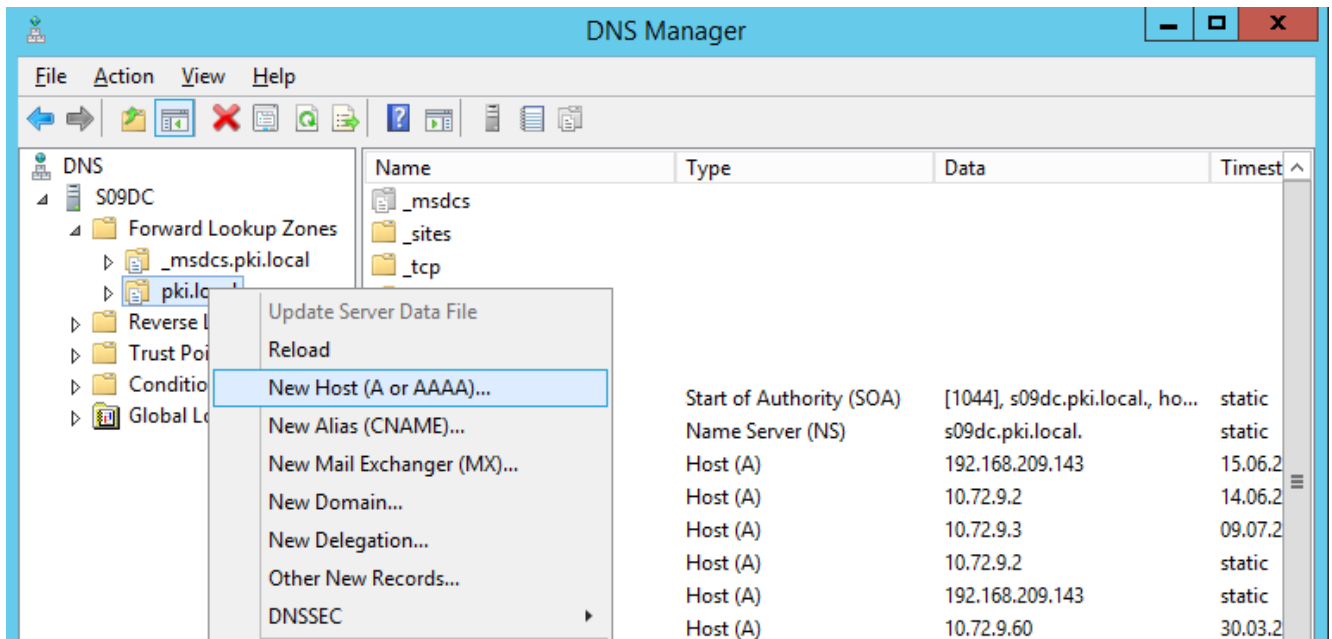


Рисунок 7.32 – Переход к меню домена

В открывшемся окне (рисунок 7.33) введите наименование в поле **Name** и укажите адрес сервера Блокост-Сеть в поле **IP address**.

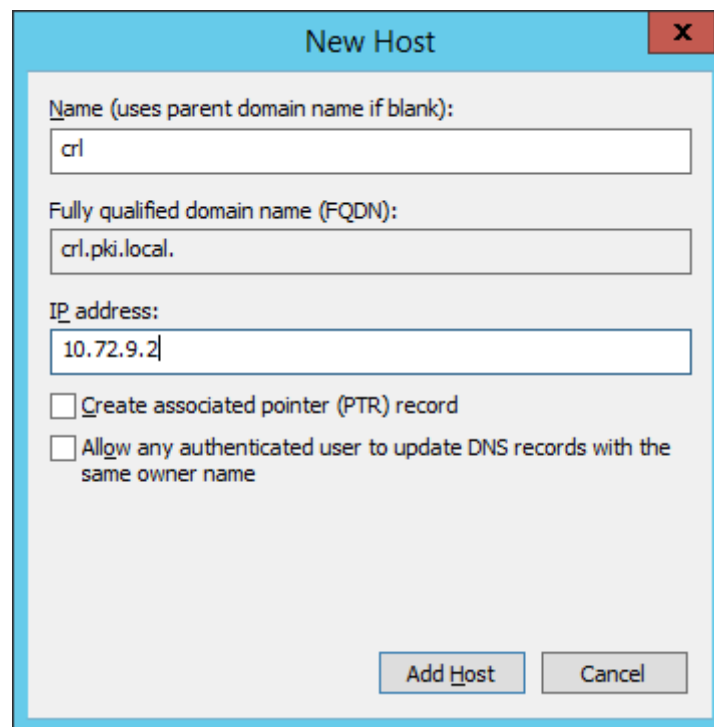


Рисунок 7.33 – Создание нового хоста

Перейдите в оснастку **IIS** (рисунок 7.34).

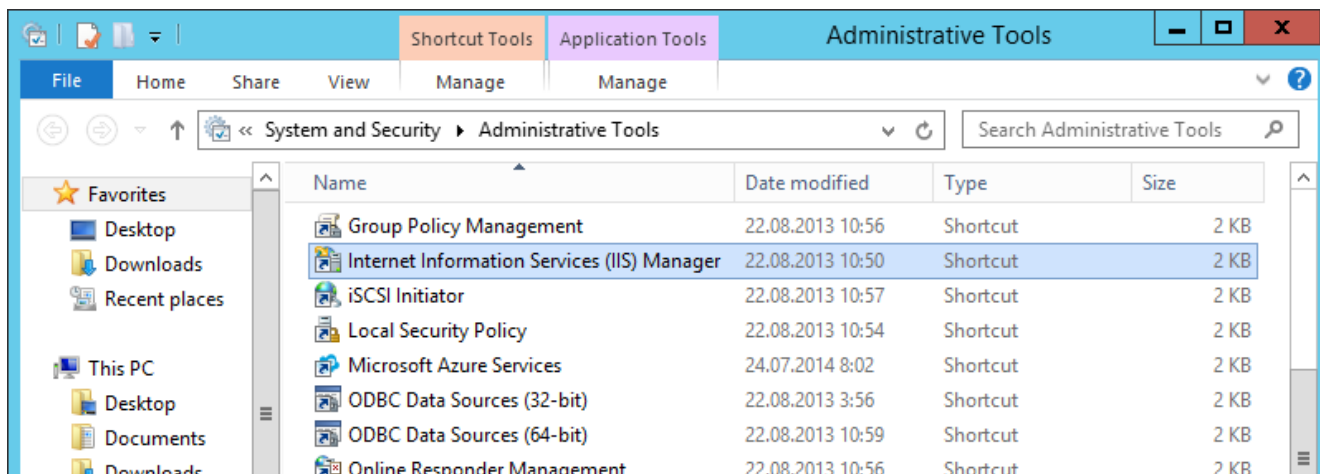


Рисунок 7.34 – Выбор оснастки **IIS**

Окно консоли будет выглядеть следующим образом:

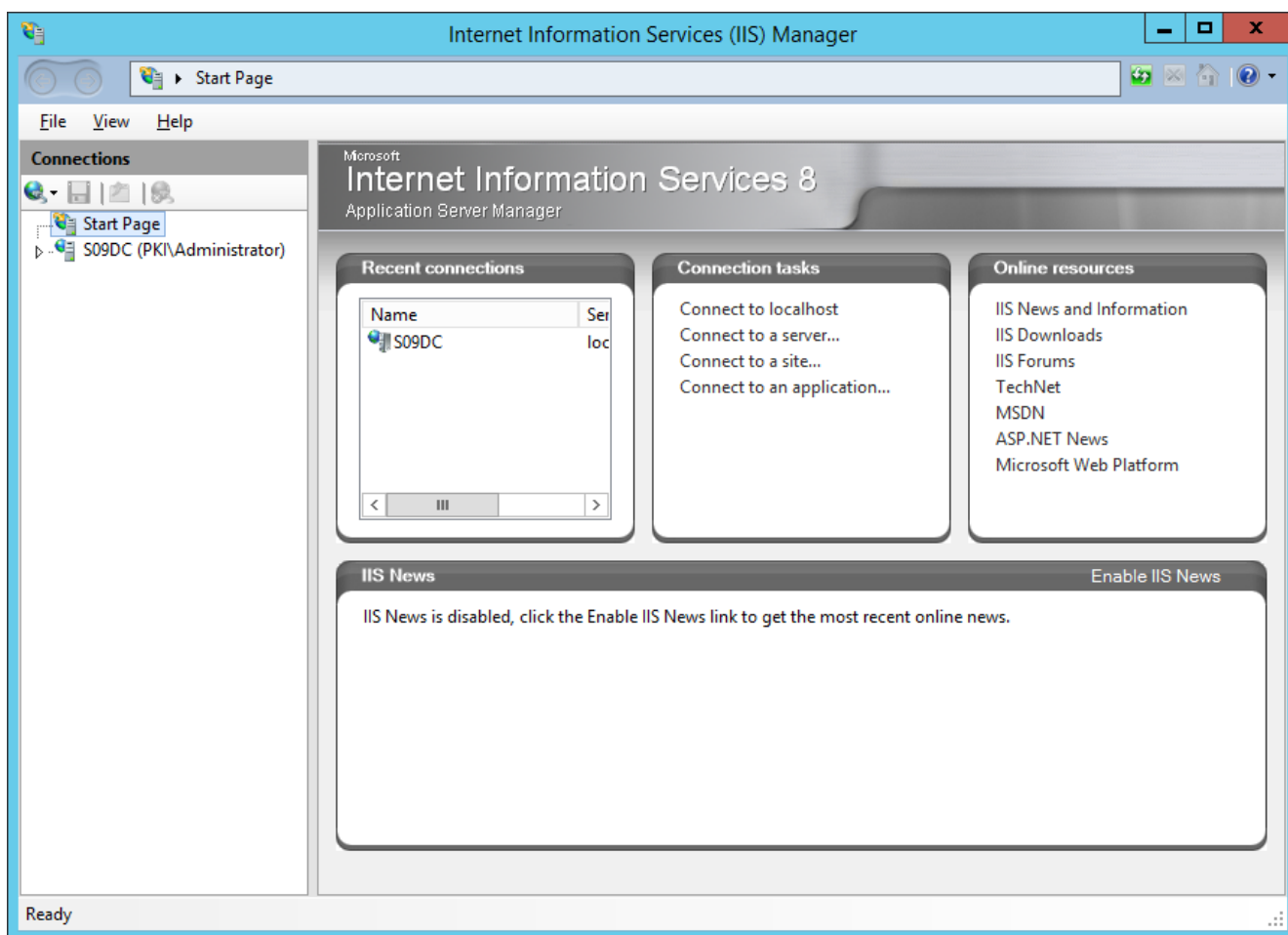


Рисунок 7.35 – Консоль контроллера домена **IIS**

В левой части окна раскройте контроллер домена, перейдите к пункту **Sites** → **Default Web Site** и по щелчку правой кнопки мыши выберите **Add Virtual Directory** (рисунок 7.36).

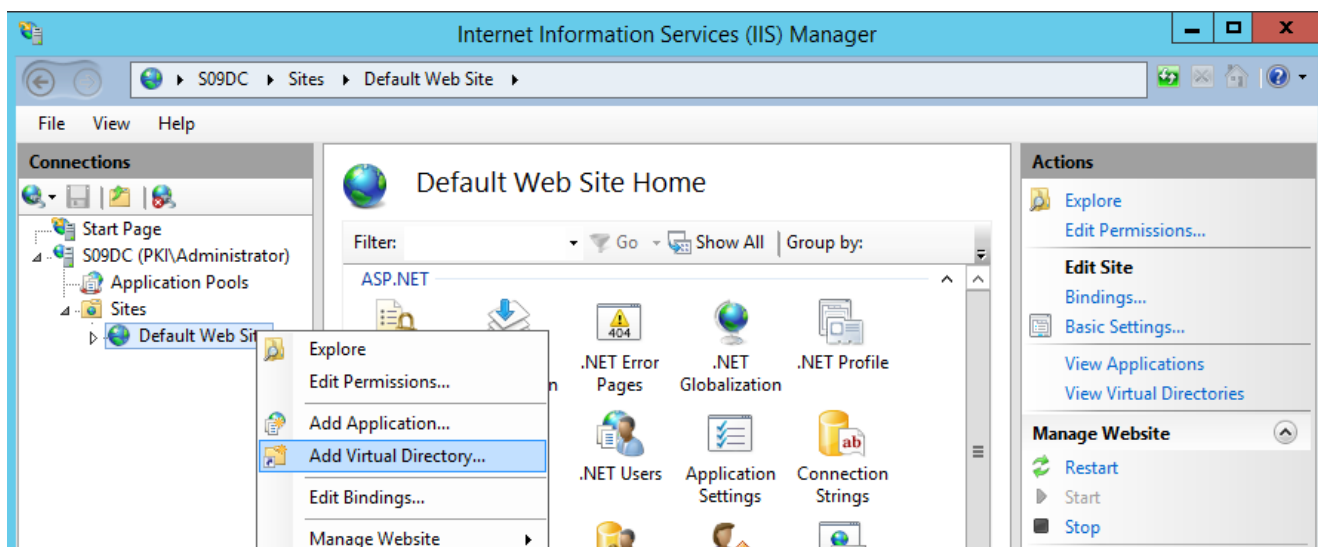


Рисунок 7.36 – Переход к меню создания виртуальной директории

В открывшемся окне (рисунок 7.37) введите наименование в поле **Alias** и укажите путь для каталога в поле **Physical path**.

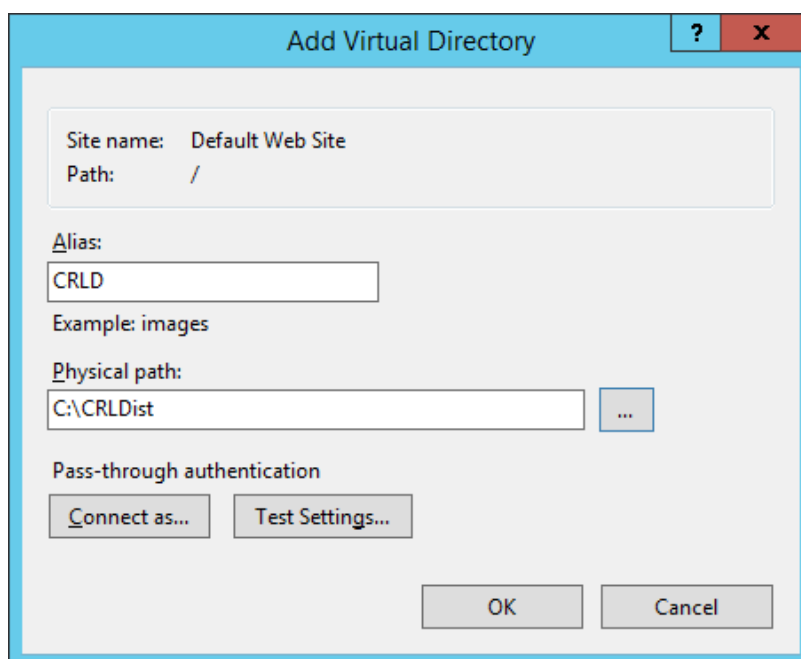


Рисунок 7.37 – Создание виртуальной директории

После нажатия кнопки **OK** перейдите в левой части окна к созданной виртуальной директории и откройте пункт **Directory Browsing** (рисунок 7.38).

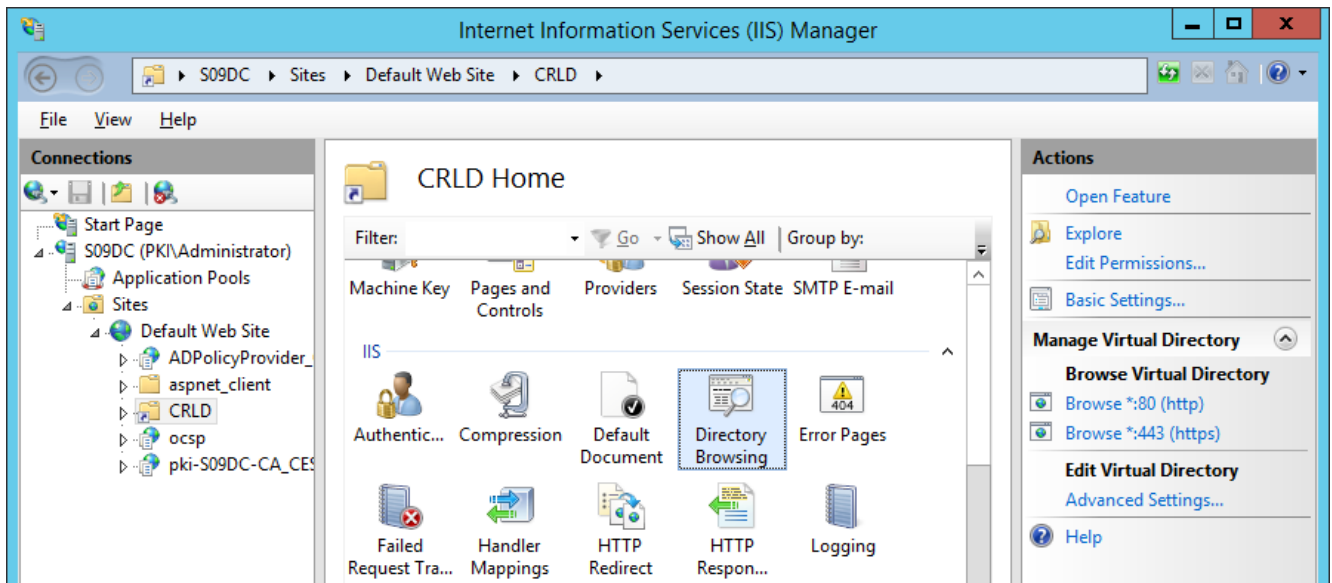


Рисунок 7.38 – Переход к просмотру каталогов

В следующем окне (рисунок 7.39) в правой части меню окна, нажмите на кнопку **Enable** для включения просмотра каталогов.

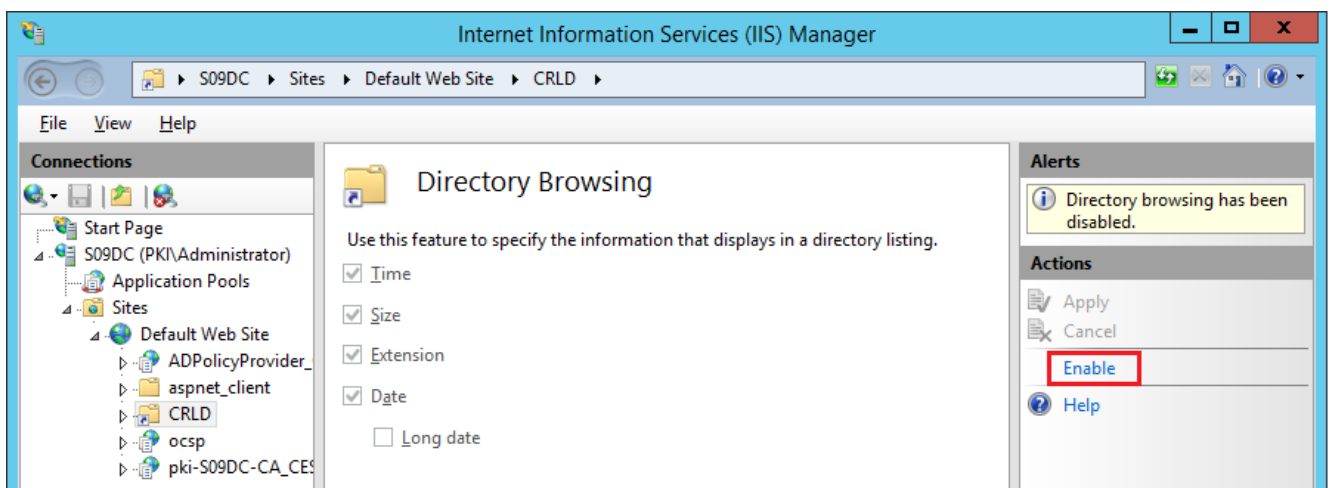


Рисунок 7.39 – Включение просмотра каталогов

Перейдите в левой части окна к созданной виртуальной директории и откройте пункт **Configuration Editor** (рисунок 7.40).

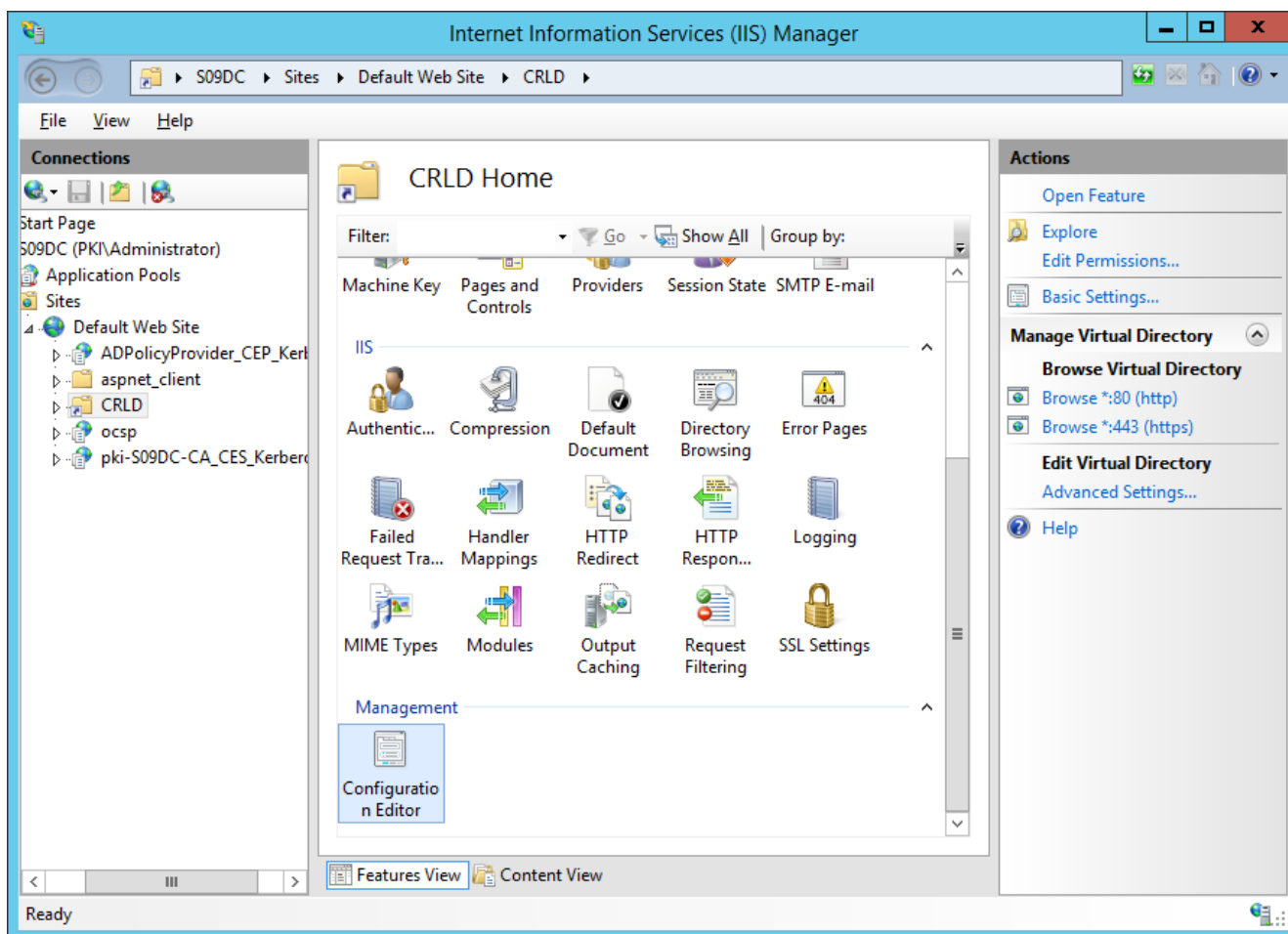


Рисунок 7.40 – Переход к редактору конфигураций

В открывшемся окне (рисунок 7.41) в поле **Section** выберите в раскрывающемся списке **system.webServer** → **security** → **requestFiltering**.

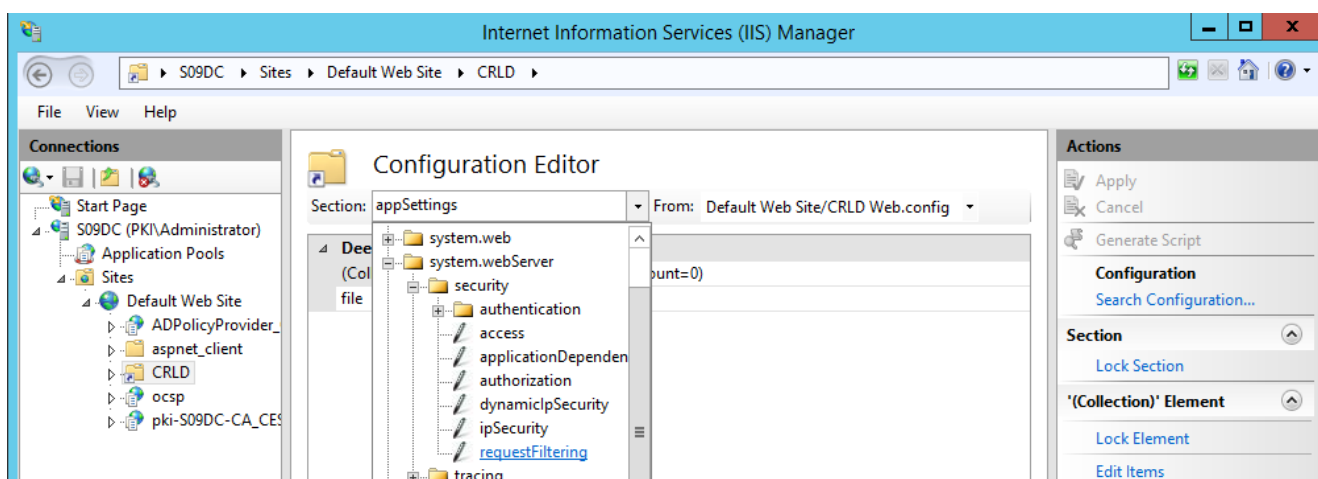


Рисунок 7.41 – Выбор раздела редактора конфигураций

Для параметра **allowDoubleEscaping** установите значение **True** (рисунок 7.42) и нажмите кнопку **Apply** в правой части окна.

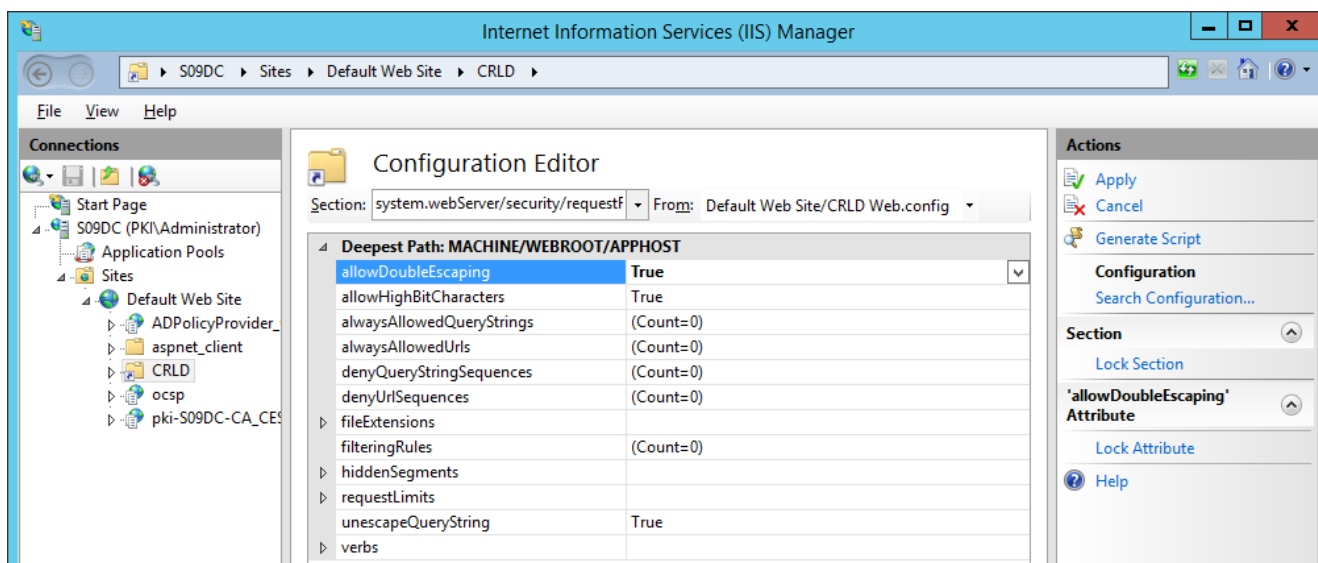


Рисунок 7.42 – Настройка раздела редактора конфигураций

Перейдите к созданному каталогу (рисунок 7.43), в котором будут размещены списки отзывает (в примере **C:\CRLDist**) и откройте свойства каталога по щелчку правой кнопки мыши на каталоге.

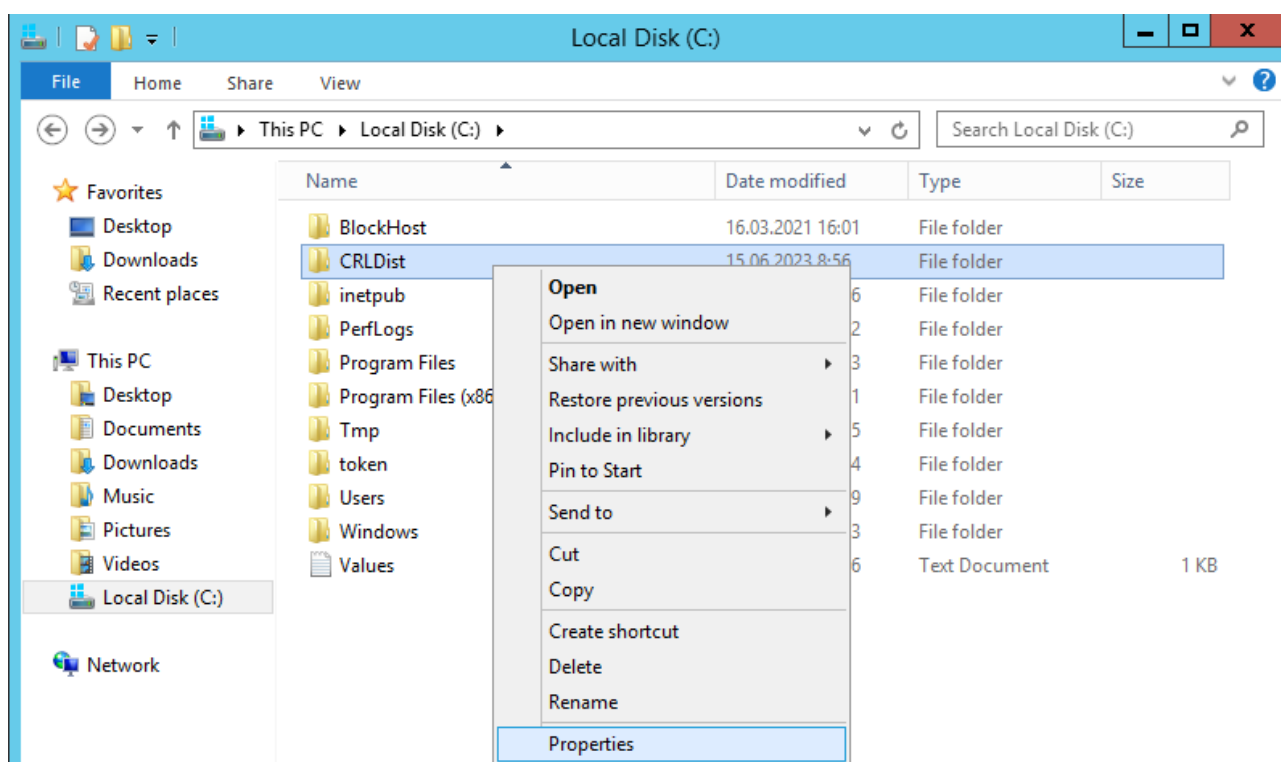
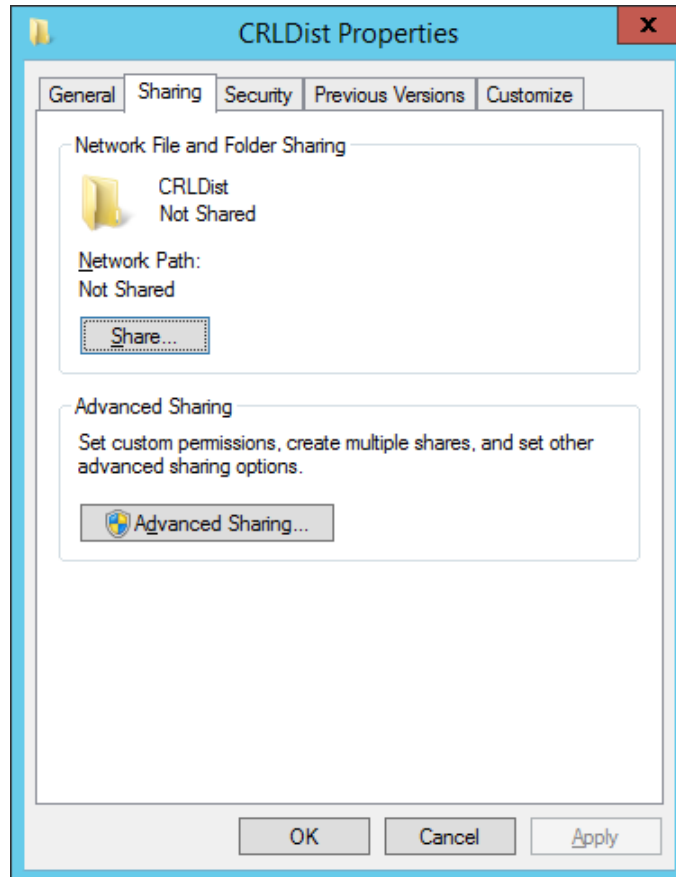


Рисунок 7.43 – Переход в свойства каталога

Перейдите во вкладку **Sharing** (рисунок 7.44) и нажмите кнопку **Advanced Sharing** для предоставления общего доступа к директории.

Рисунок 7.44 – Вкладка **Sharing**

В появившемся окне установите флаг **Share this folder**, в поле **Share name** укажите «CRLDist\$» (рисунок 7.45).

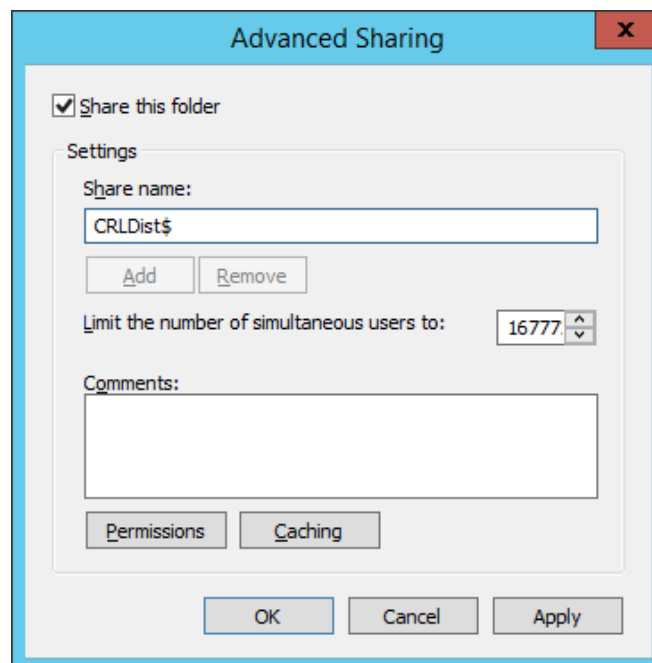


Рисунок 7.45 – Установка расширенного доступа

Нажмите на кнопку **Permissions** (рисунок 7.46) и в появившемся окне нажмите **Add** для

предоставления разрешений контроллеру домена (рисунок 7.47).

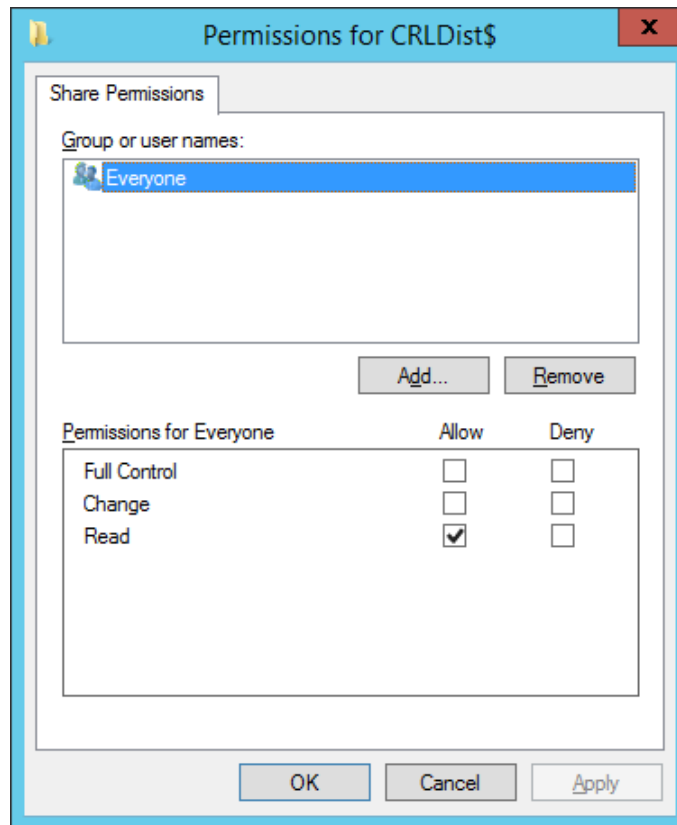


Рисунок 7.46 – Установка разрешений

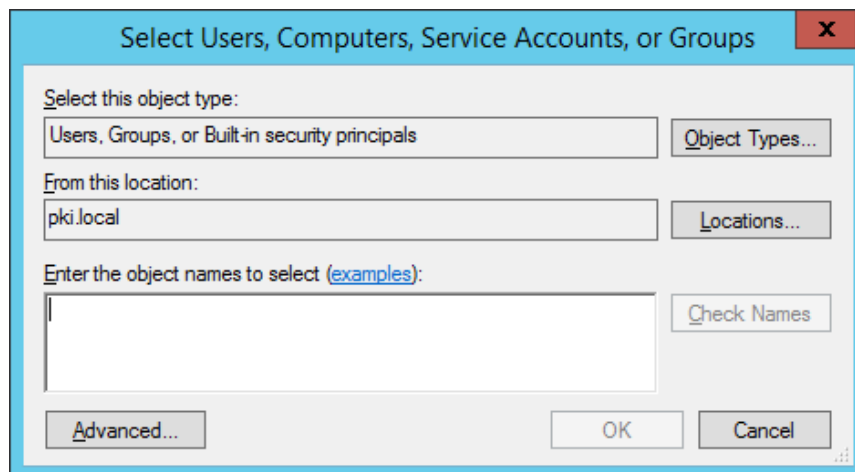


Рисунок 7.47 – Выбор типа для установки разрешений

По кнопке **Object types** (рисунок 7.48) установите флаг **Computers** и в поле **Enter the object names to select** введите имя контроллера домена (рисунок 7.49).

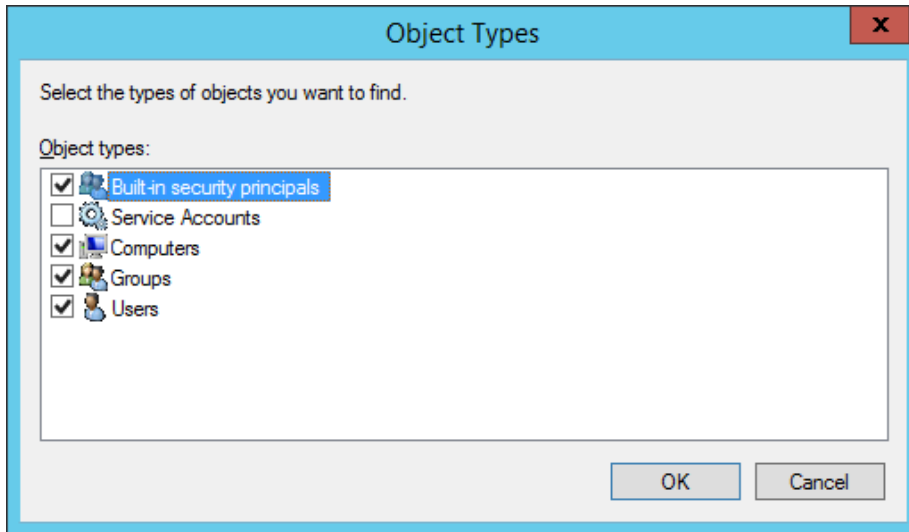


Рисунок 7.48 – Выбор типа **Компьютеры**

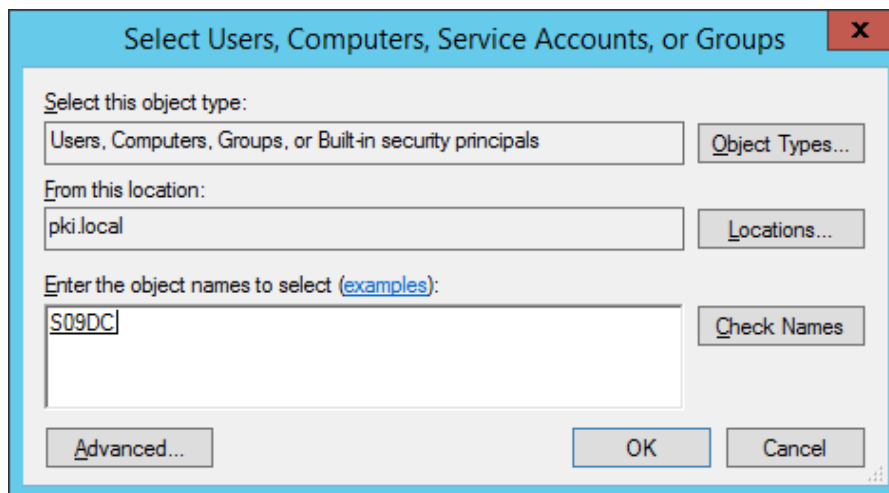


Рисунок 7.49 – Выбор контроллера домена

Установите полный доступ для контроллера домена (рисунок 7.50).

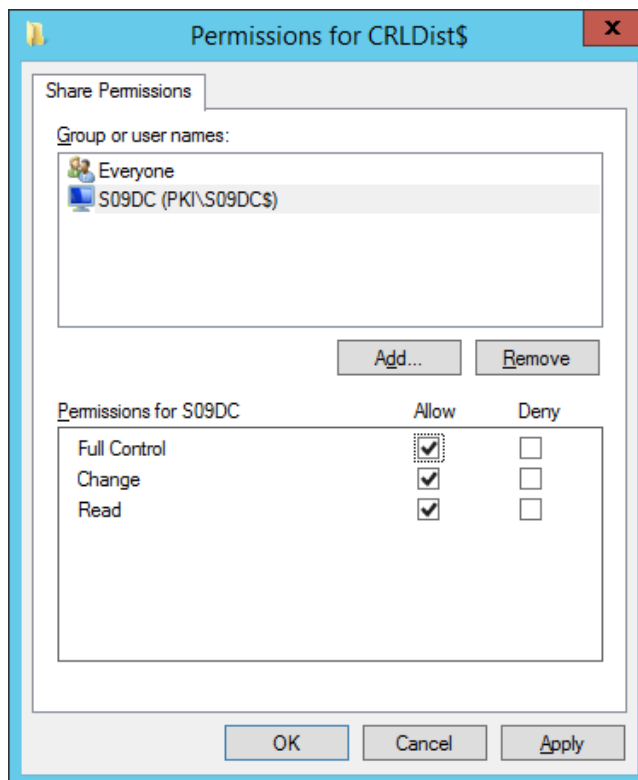


Рисунок 7.50 – Установка разрешений для контроллера домена

Перейдите во вкладку **Security** (рисунок 7.51) и нажмите кнопку **Edit** для добавления в разрешения контроллера домена.

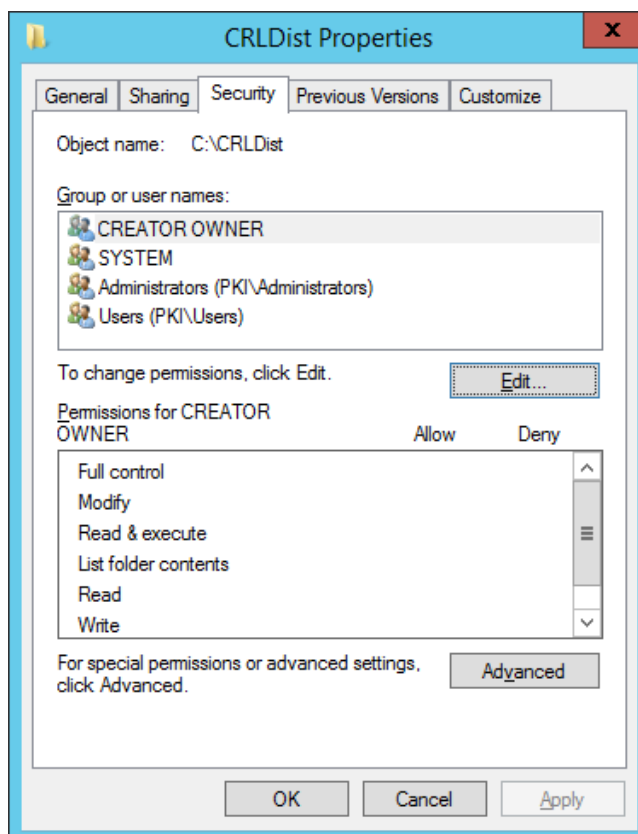


Рисунок 7.51 – Вкладка **Security**

В появившемся окне нажмите **Add** для предоставления разрешений контроллеру домена (рисунок 7.52).

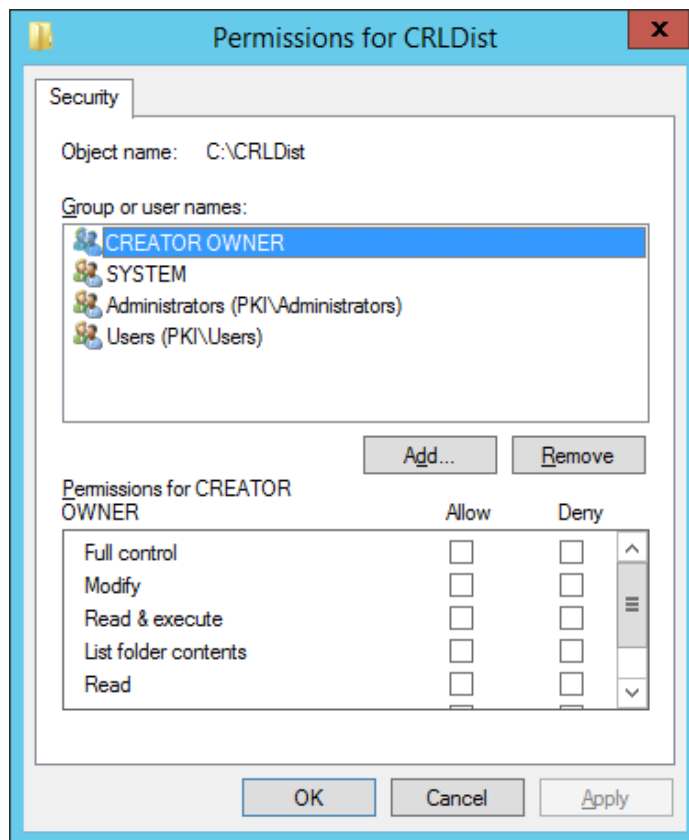


Рисунок 7.52 – Установка разрешений

По кнопке **Object types** (рисунок 7.48) установите флаг **Computers** и в поле **Enter the object names to select** введите имя контроллера домена (рисунок 7.49).

Установите полный доступ для контроллера домена (рисунок 7.53).

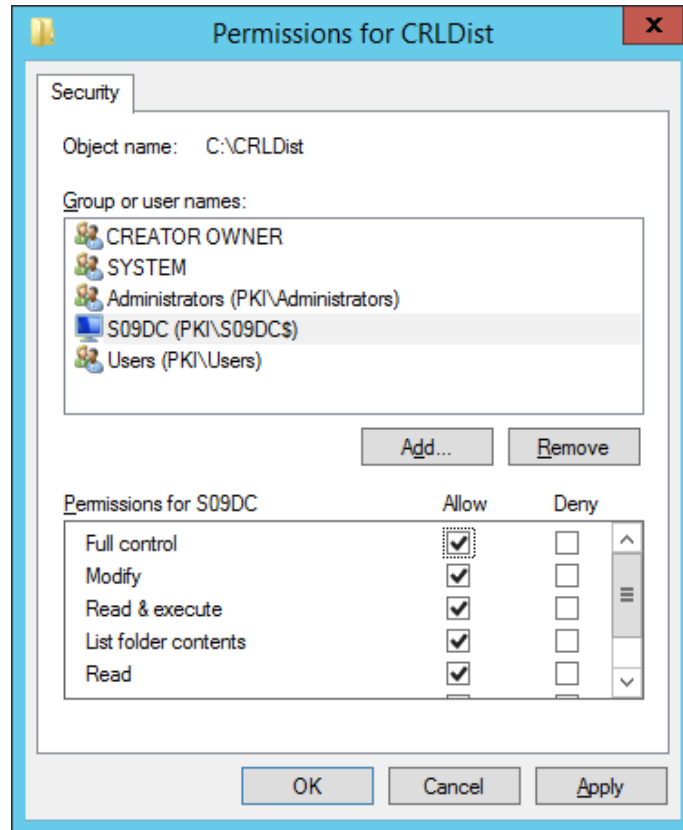


Рисунок 7.53 – Установка разрешений для контроллера домена

7.7.3 Публикация списка отзывов

Перейдите к настройкам центра сертификации и откройте оснастку **Certification Authority** (рисунок 7.21).

В левой части окна перейдите в пункт **Revoked Certificates** и по щелчку правой кнопки мыши выберите **All Tasks** → **Publish** для публикации списка отзывов (рисунок 7.54).

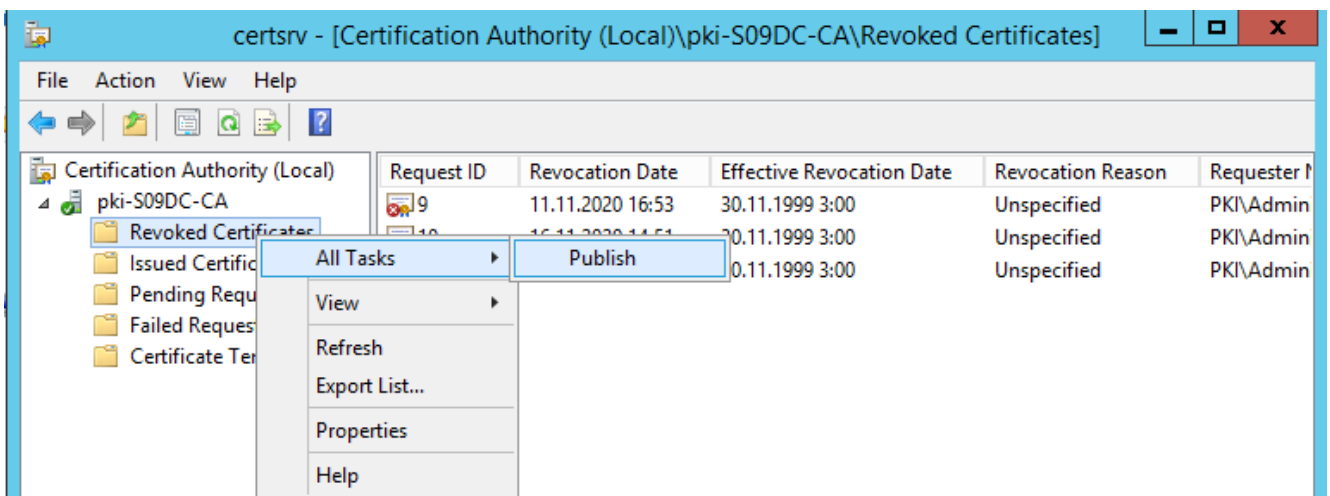


Рисунок 7.54 – Переход к публикации списка отзывов

В появившемся окне выберите тип публикации **New CRL** и нажмите **OK** (рисунок 7.55).

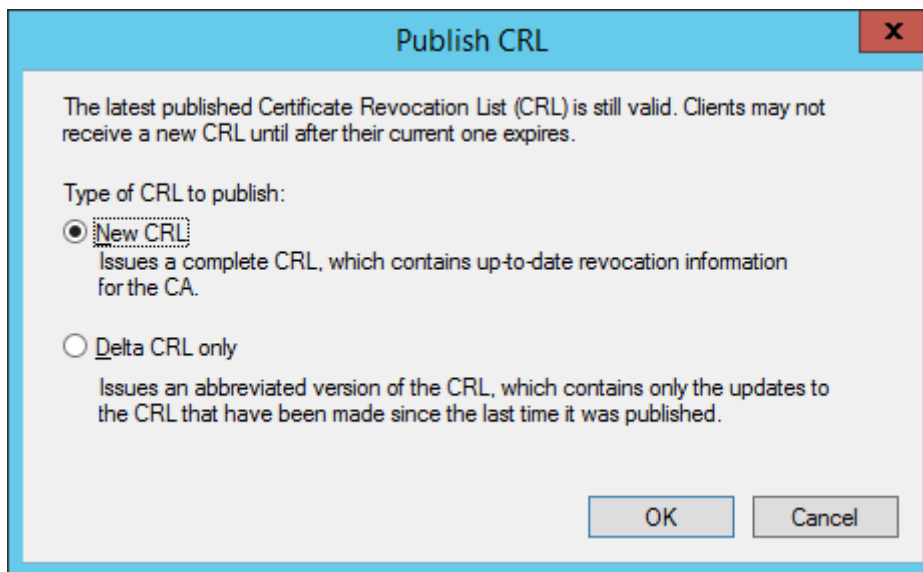


Рисунок 7.55 – Публикация нового списка отзывов

В результате в выбранной директории будут опубликованы списки отзывов (рисунок 7.56).

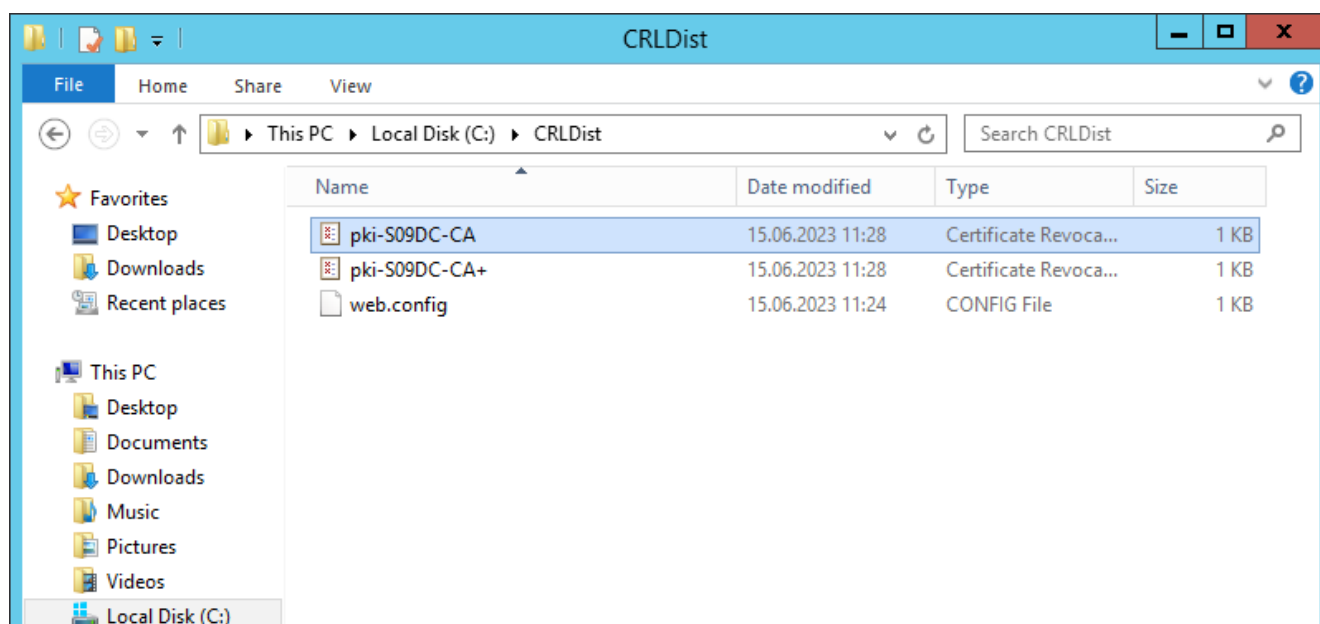


Рисунок 7.56 – Опубликованный список отзывов сертификатов

7.8 Настройка подключения к домену из консоли управления по протоколу *Idaps* с установкой *ssl*-сертификатов

Подключение к домену из консоли управления СЗИ от НСД «Блокост-Сеть 4» может осуществляться:

- **без пароля** – подключение по протоколу *ldap* с использованием билета *kerberos* (используется механизм *gssapi*);
- **по имени пользователя и паролю** – подключение по протоколу *ldaps*, который

обеспечивает безопасность передачи пароля пользователя при подключении (подключение по *ldaps* выполняется с установкой ssl-сертификатов и требует дополнительных настроек).

7.8.1 Настройка контроллера домена AD

Для подключения к домену AD по протоколу *ldaps* с установкой ssl-сертификатов на рабочей станции с ролью центра сертификации (Certification Authority) запустите консоль центра сертификации с помощью команды **certsrv.msc** в командной строке (рисунок 7.57).

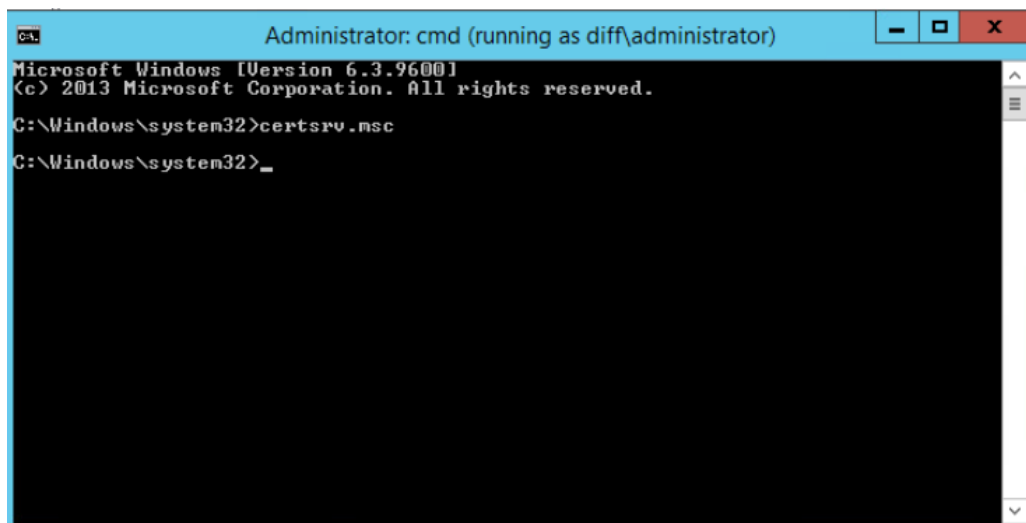


Рисунок 7.57 – Запуск консоли центра сертификации

В левой части окна перейдите на пункт **Шаблоны сертификатов (Certificate Templates)**, щелкните правой кнопкой мыши и выберите **Управление (Manage)** (рисунок 7.58).

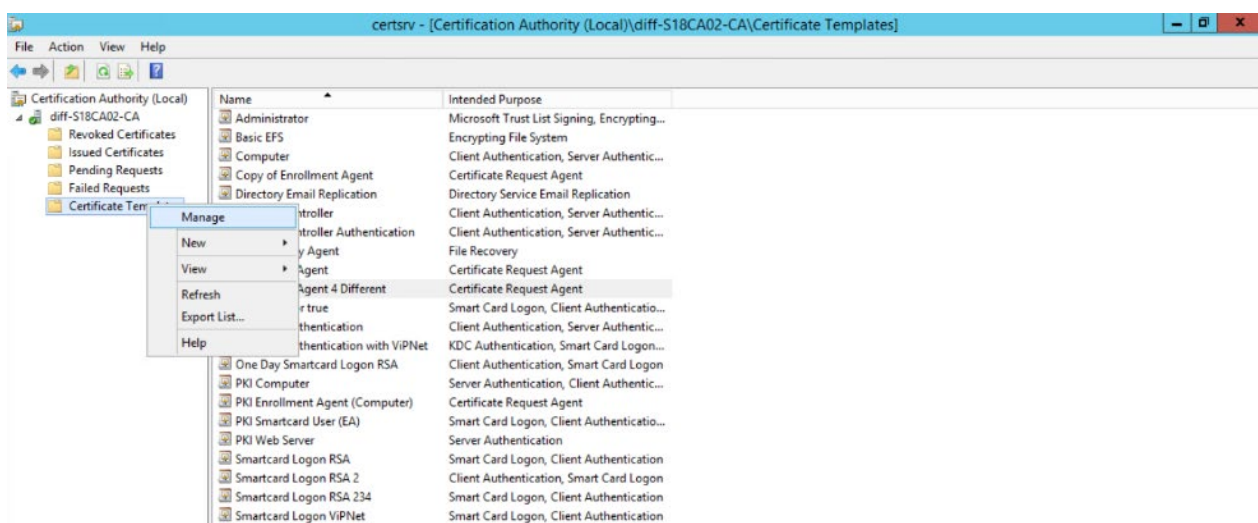


Рисунок 7.58 – Управление шаблонами сертификатов

В появившемся окне выберите пункт **Kerberos Authentication** (рисунок 7.59).

Для создания копии имеющегося шаблона, щелкните правой кнопкой мыши и выберите **Скопировать шаблон (Duplicate Template)** (рисунок 7.59).

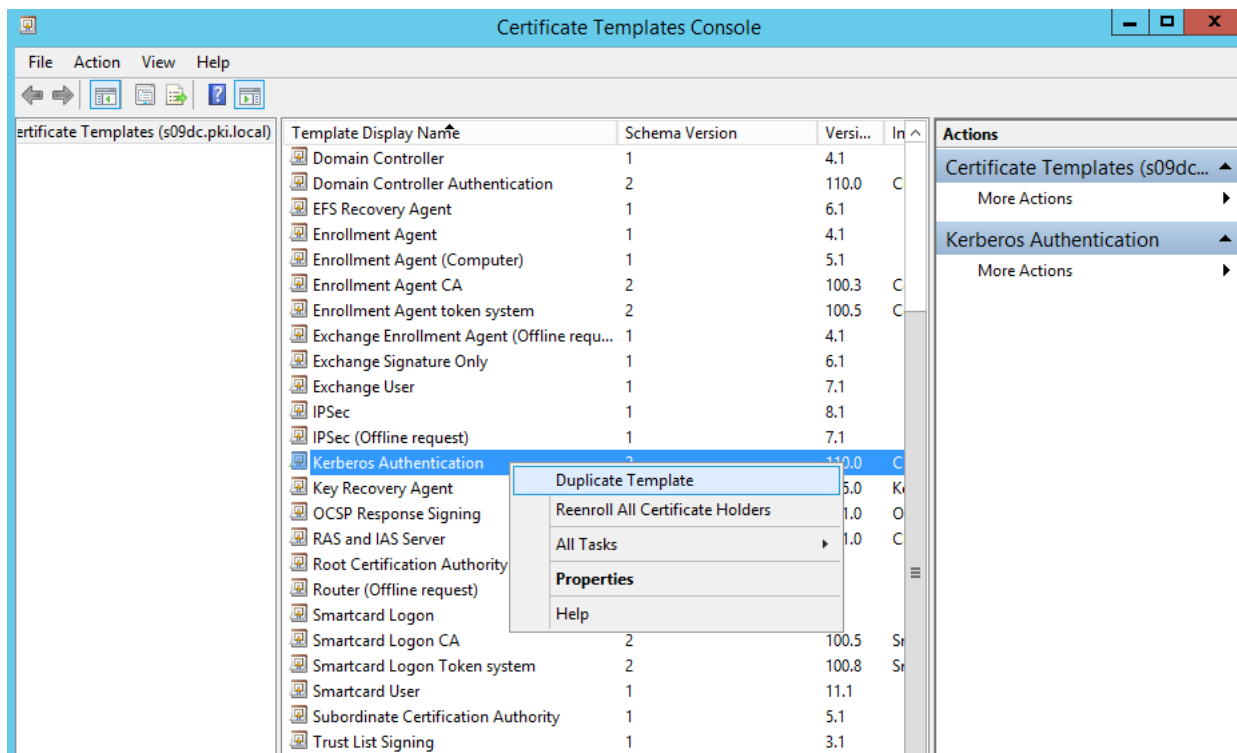


Рисунок 7.59 – Создание копии шаблона

В появившемся окне со свойствами шаблона выполните следующие настройки:

- 1) Введите имя создаваемого шаблона на вкладке **Общие (General)**. Например, **LDAPoverSSL**. При необходимости настройте **Срок действия сертификата (Validity period)** и **Период обновления (Renewal period)** и опубликуйте его в AD (**Publish certificate in Active Directory**) (рисунок 7.60).

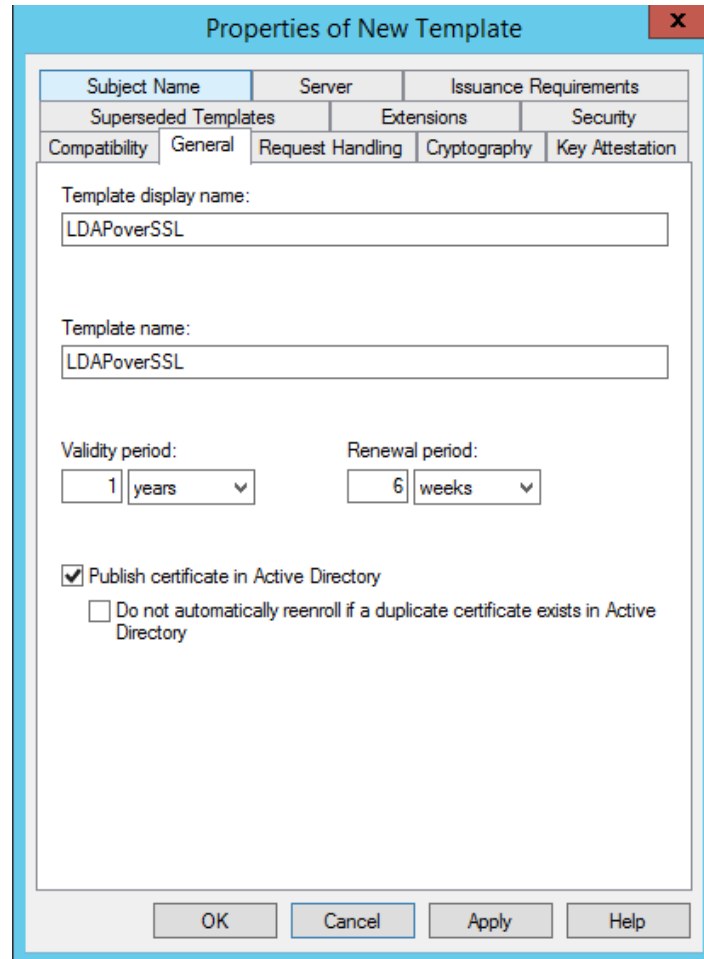


Рисунок 7.60 – Свойства шаблона, вкладка **General**

2) Во вкладке **Обработчик запросов (Request Handling)** установите параметр **Разрешить экспорт закрытых ключей (Allow private key to be exported)** и нажмите **OK** для сохранения шаблона (рисунок 7.61).

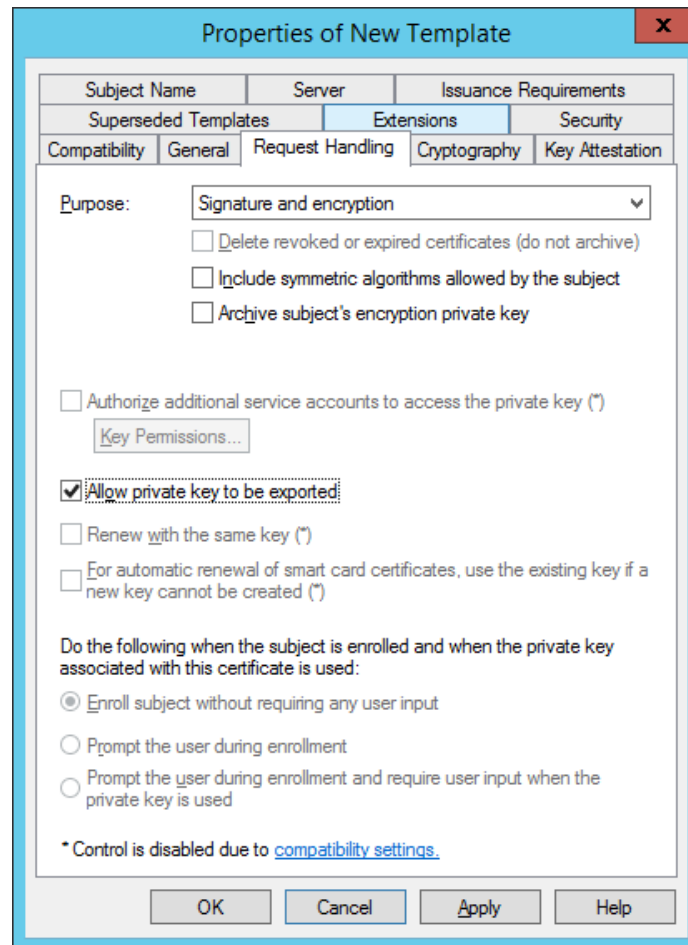


Рисунок 7.61 – Свойства шаблона, вкладка **Request Handling**

Для публикации созданного шаблона, после его настройки, перейдите на пункт **Шаблоны сертификатов (Certificate Templates)**, щелкните правой кнопкой мыши и выберите **Создать (New)** → **Выдаваемый шаблон сертификата (Certificate Template to Issue)** (рисунок 7.62).

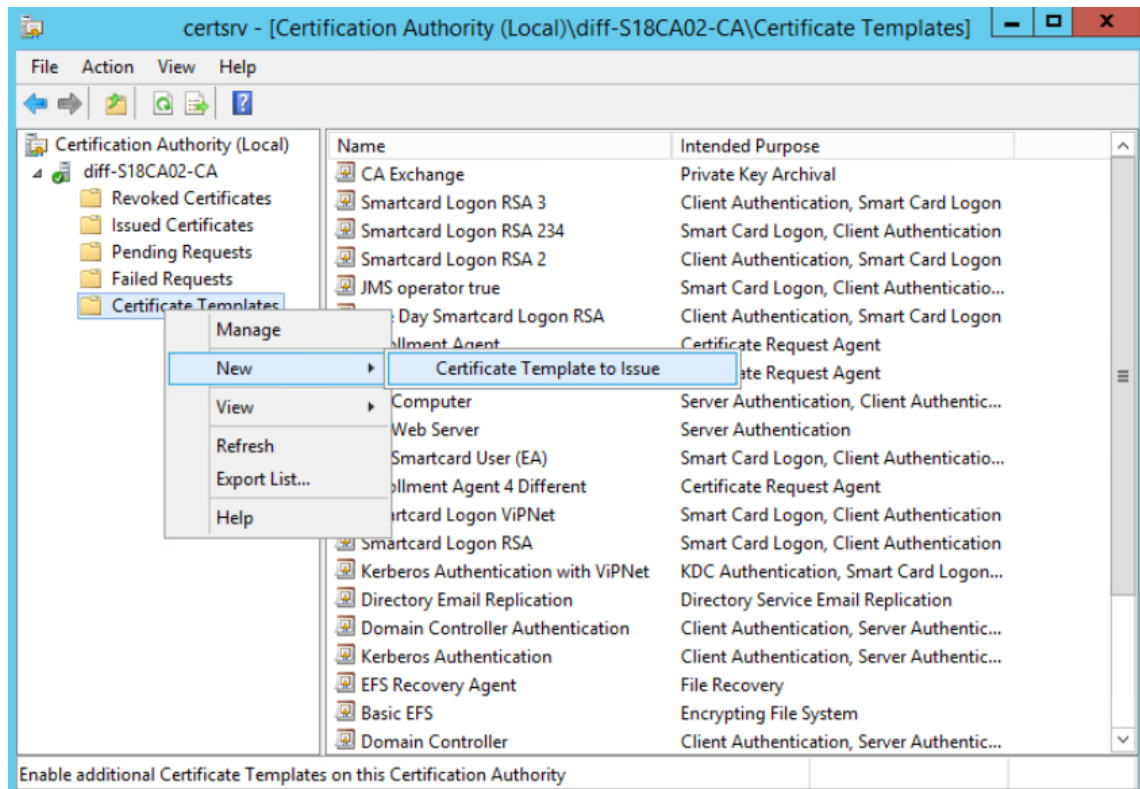


Рисунок 7.62 – Выбор выдаваемого шаблона сертификата

В появившемся окне (рисунок 7.63) выберите созданный шаблон сертификата и нажмите **OK**.

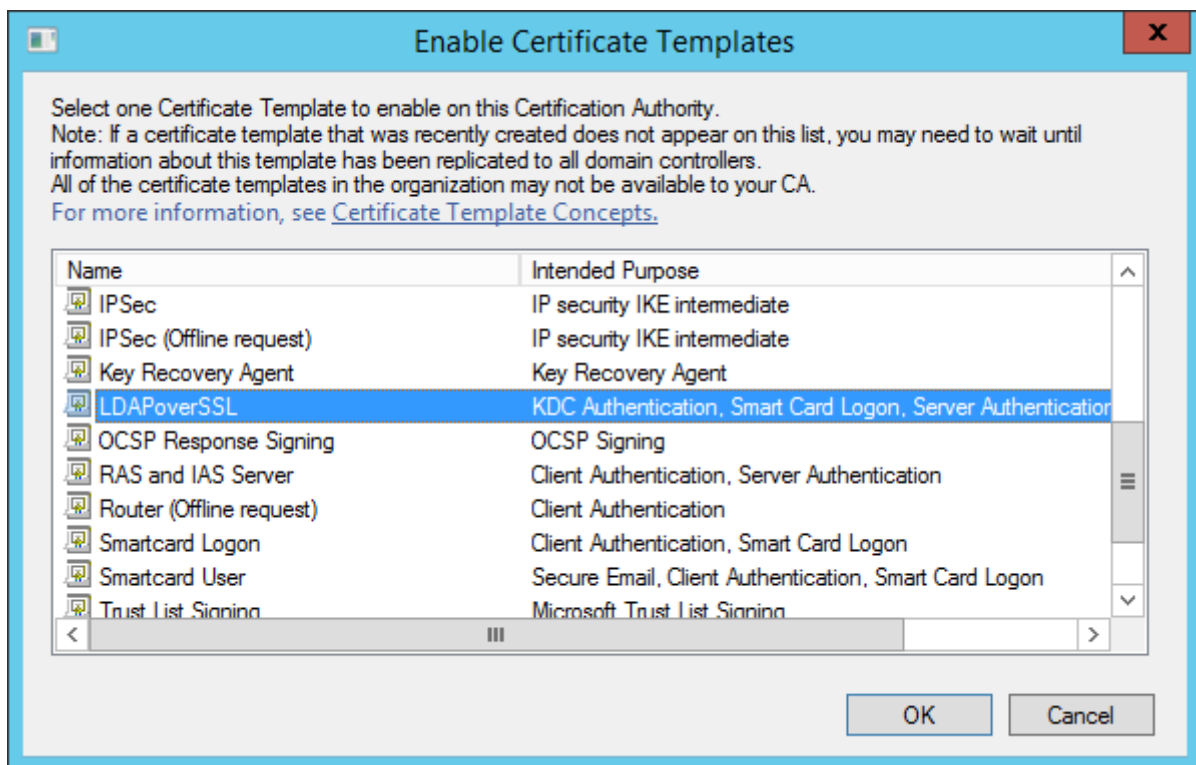


Рисунок 7.63 – Публикация созданного шаблона

На контроллере домена, для которого планируется задействовать *LDAPS*, необходимо

наличие в оснастке **Сертификаты (Certificates)** в разделе **Личные (Personal)** установленного сертификата, выпущенного по шаблону созданного сертификата.

Для создания сертификата выполните следующие действия:

- 1) Перейдите в оснастку сертификатов **certmgr.msc** (рисунок 7.64).

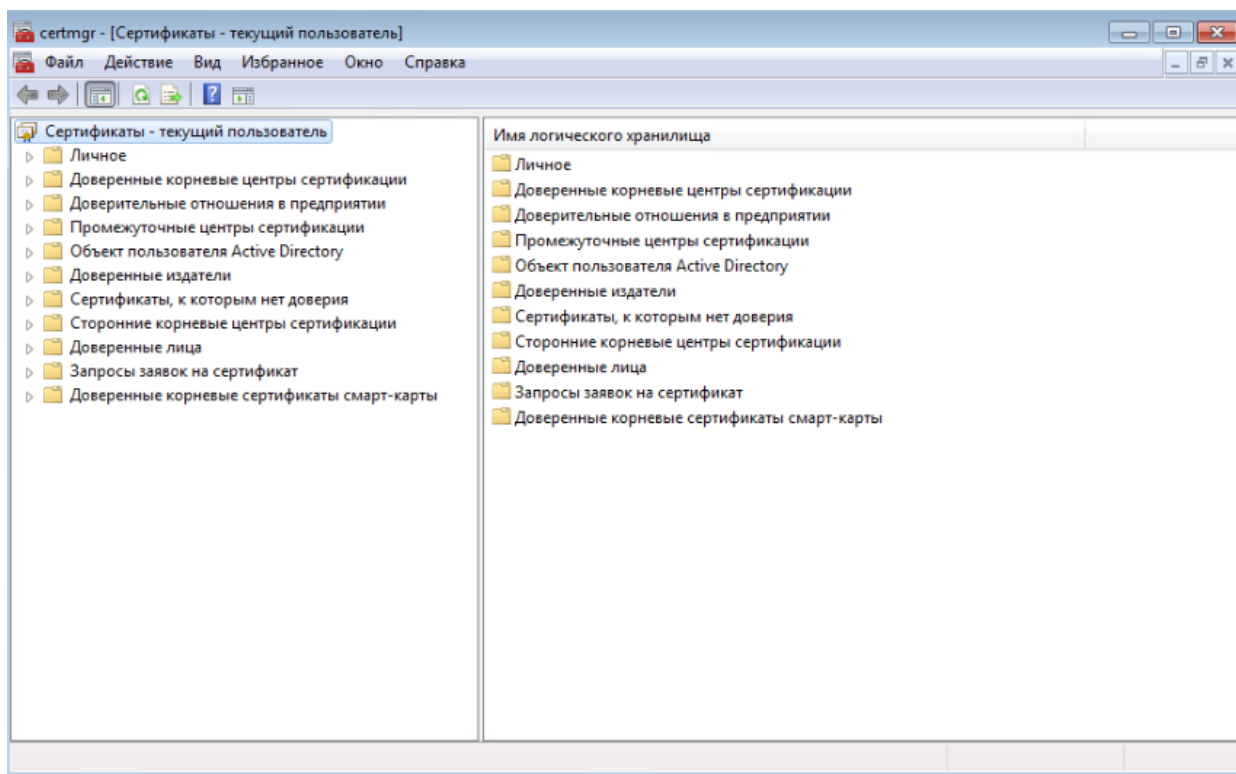


Рисунок 7.64 – Оснастка **Сертификаты (Certificates)**

- 2) В левой части окна перейдите в раздел **Личные (Personal)** и по щелчку правой кнопкой мыши выберите **Все задачи (All Task) → Запросить новый сертификат (Request New Certificate)** (рисунок 7.65).

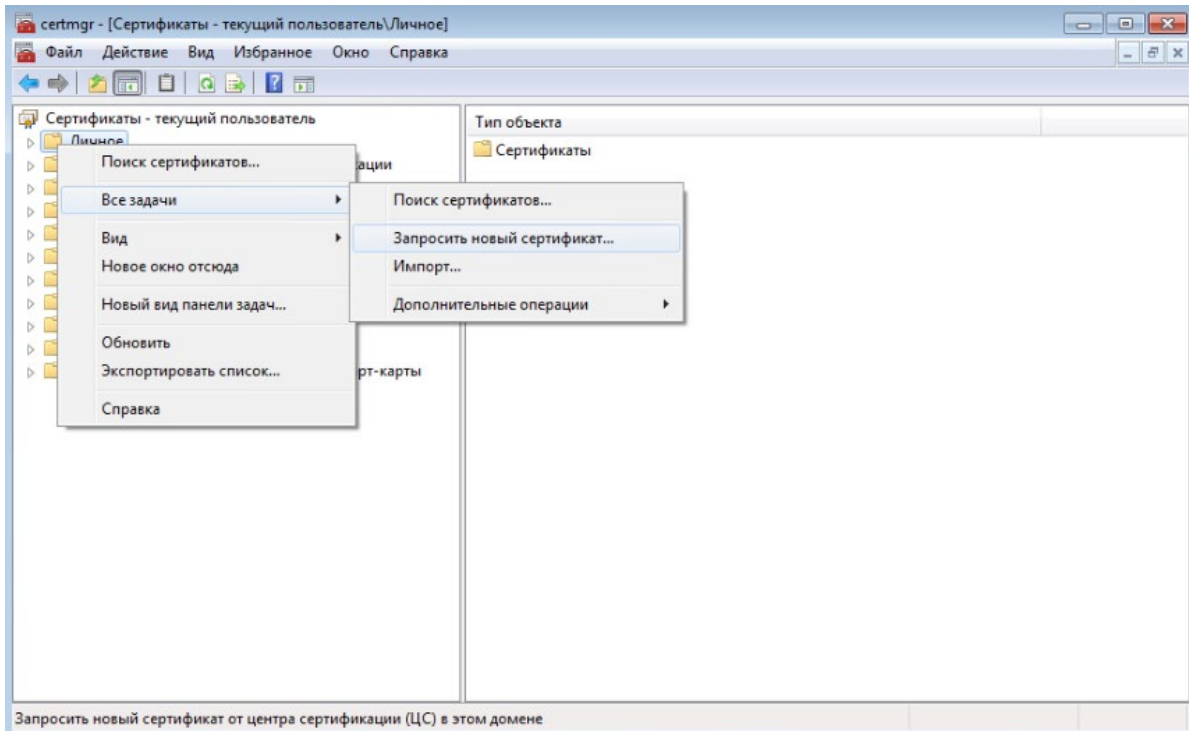


Рисунок 7.65 – Запрос нового личного сертификата

3) В появившемся окне **Регистрация сертификатов** выберите **Политика регистрации Active Directory (Active Directory Enrollment Policy)** и нажмите **Далее** (рисунок 7.66).

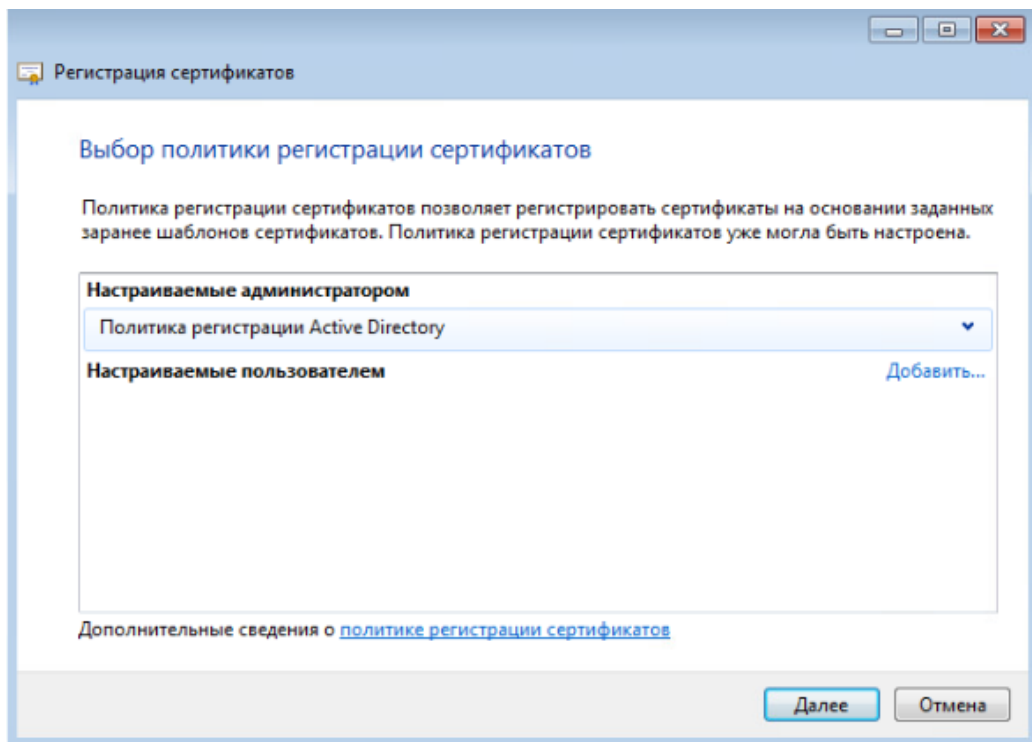


Рисунок 7.66 – Выбор политики регистрации сертификата

- 4) Выберите шаблон сертификата, созданный в центре сертификации (например, **LDAPoverSSL**) (рисунок 7.67).

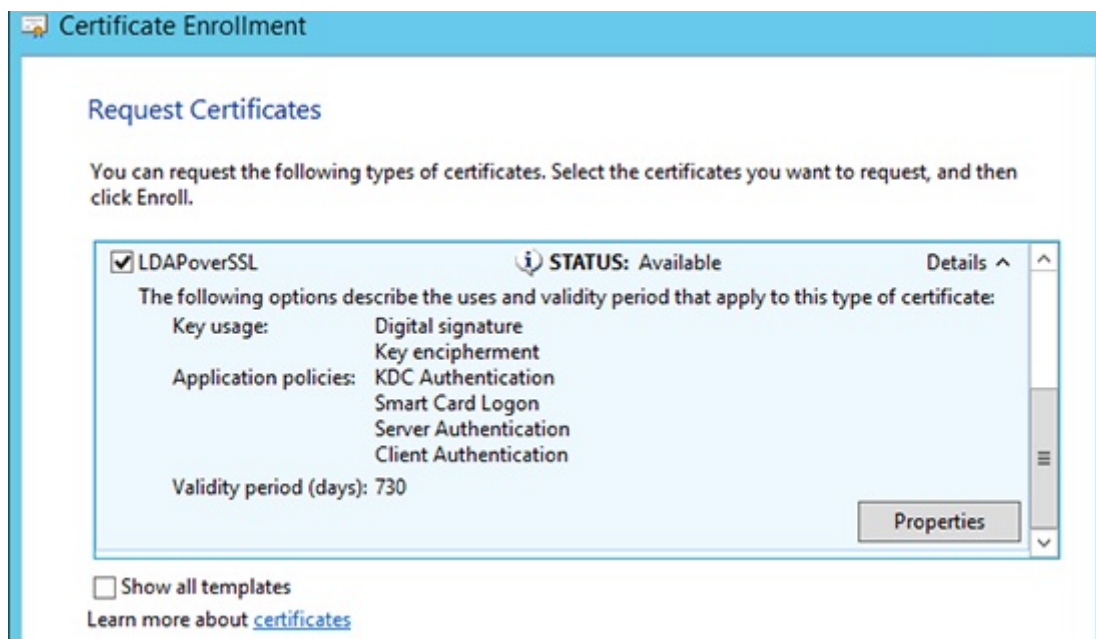


Рисунок 7.67 – Выбор шаблона сертификата

- 5) Дождитесь выпуска и установки сертификата в хранилище **Личное** и нажмите **Готово**.

Для взаимодействия контроллера домена и рабочей станции с установленной консолью управления через **LDAPS** необходимо установить доверие удостоверяющему центру (CA), который выдал сертификат для контроллера домена:

- 1) На рабочей станции с ролью центра сертификации (Certification Authority) выполните экспорт корневого сертификата удостоверяющего центра в файл с помощью команды:

```
certutil -ca.cert ca_name.cer
```



Файл сертификата сохранится в профиле текущего пользователя с именем **ca_name.cer**.

- 2) Добавьте экспортированный сертификат в хранилище сертификатов **Trusted Root Certification Authorities** на рабочей станции с установленной консолью управления и контроллере домена вручную через оснастку управления сертификатами или из командной строки:

```
certutil -addstore -f "ROOT" <path_to_certificate>
```

- 3) Перезапустите службы Active Directory на контроллере домена, либо перезагрузите контроллер домена.

7.8.2 Настройка контроллера домена Samba

Для подключения к домену Samba по протоколу *ldaps* с установкой ssl-сертификатов установите пакет *openssl*.

На контроллере домена, для которого планируется задействовать *ldaps* выполните генерацию корневой пары ключ-сертификат:

```
openssl genrsa -out rootCA.key 2048  
openssl req -x509 -new -key rootCA.key -days 10000 -out rootCA.crt
```

Выполните генерацию приватного ключа и сертификата, подписанного корневым сертификатом:

```
openssl genrsa -out lnxdc11.alt.test.key 2048  
openssl req -new -key lnxdc11.alt.test.key -out lnxdc11.alt.test.csr
```

Ответьте на вопросы.



При ответах на вопросы важно учитывать следующее:

- 1) в поле **Common Name** важно указать FQDN имя хоста, для которого генерируется сертификат;
- 2) можно заполнить только поле **Common Name**;
- 3) ответы на вопросы для первого или второго сертификата не должны совпадать, иначе рабочая станция с установленной консолью управления считает такой сертификат невалидным (самоподписанным) и подключение не удастся.

При подключении к домену с проверкой сертификатов, подключение будет успешно, когда подключение осуществляется по имени, указанному в поле **Common name** или в поле **Дополнительное имя субъекта** (рисунок 7.68).

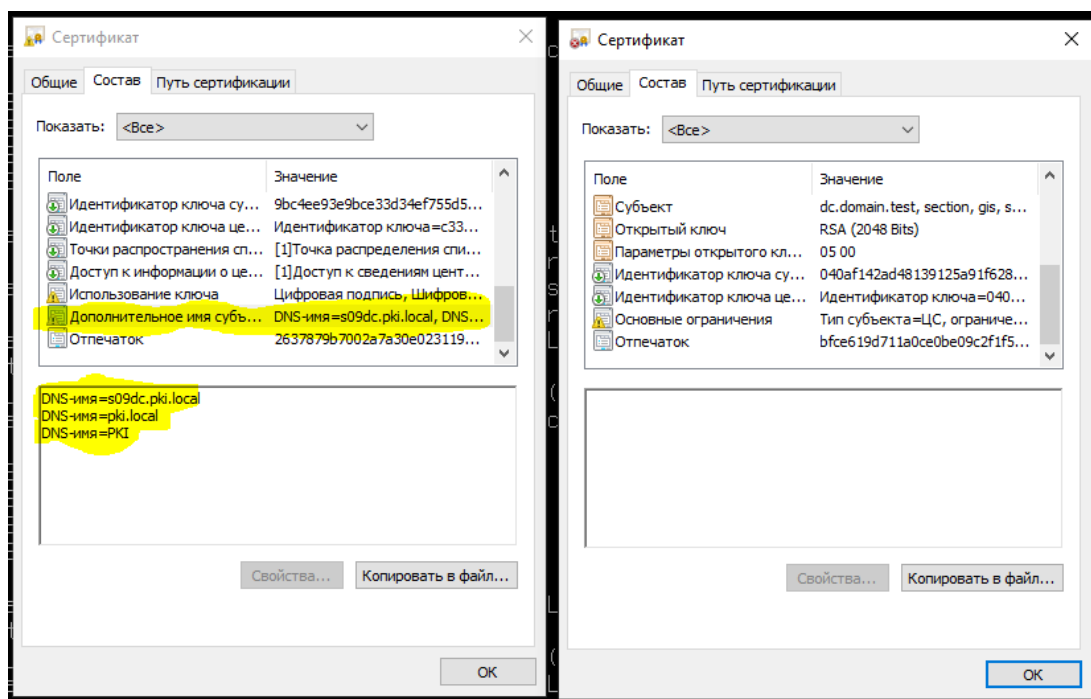


Рисунок 7.68 – Подключение по имени в поле **Дополнительное имя субъекта**

i В openssl поле **Дополнительное имя субъекта** по умолчанию не задается, для его включения следует обратиться к дополнительным инструкциям, например, <https://r-notes.ru/administrirovanie/poleznosti/164-openssl-sozdanie-multidomennogo-sertifikata.html>.

```
openssl x509 -req -in lnx-dc11.alt.test.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial  
-out lnx-dc11.alt.test.crt -days 5000
```

В итоге получаем комплект:

```
Cert: lnx-dc11.alt.test.crt  
Key: lnx-dc11.alt.test.key  
CA: rootCA.crt
```

Выполните настройку SSL/TLS на контроллере домена Samba:

1) Сгенерированные ключи скопируйте в рабочий каталог Samba (от имени суперпользователя):

```
# cp lnx-dc11.alt.test.crt /var/lib/samba/private/tls/  
# cp lnx-dc11.alt.test.key /var/lib/samba/private/tls/  
# cp rootCA.crt /var/lib/samba/private/tls/
```

2) В секцию *Global* в */etc/samba/smb.conf* добавьте следующие параметры:

```
ldap server require strong auth = yes  
tls enabled = yes  
tls keyfile = tls/lnx-dc11.alt.test.key
```

```
tls certfile = tls/lnx-dc11.alt.test.crt
```

3) Перезапустите сервис Samba:

```
# systemctl restart samba
```

7.8.3 Настройка контроллера домена FreeIPA

Для подключения к домену FreeIPA по протоколу *ldaps* с установкой ssl-сертификатов нет необходимости устанавливать сертификаты, т.к. они уже присутствуют на домене FreeIPA.

Для выполнения настройки подключения к домену FreeIPA требуется только экспортировать цепочку корневых сертификатов с сервера и установить их на рабочие станции с установленной консолью управления.

7.8.4 Настройки на рабочей станции ОС Windows с установленной консолью управления

Для подключения к домену по протоколу *ldaps* с установкой ssl-сертификатов необходимо на рабочей станции под управлением ОС Windows с установленной консолью управления выполнить следующие действия:

- 1) Экспортировать корневой сертификат удостоверяющего центра на рабочую станцию.
- 2) Добавить корневой сертификат в хранилище сертификатов **Trusted Root Certification Authorities** вручную через оснастку управления сертификатами или из командной строки:

```
certutil -addstore -f "ROOT" <path_to_certificate>
```

где *<path_to_certificate>* - путь к файлу с экспортированным корневым сертификатом.

- 3) Для добавления цепочки корневых сертификатов повторите приведенные действия для всех сертификатов цепочки.

7.8.5 Настройки на рабочей станции ОС Linux с установленной консолью управления

Подключение к домену по протоколу *ldaps* с установкой ssl-сертификатов на рабочей станции под управлением ОС Linux с установленной консолью управления возможно несколькими способами:

Вариант 1 (рекомендуемый):

При необходимости выполните преобразование файла в формате *.cer* в файл в формате *.crt* с помощью команды:

```
openssl x509 -inform der -in certificate.cer -out certificate.crt
```

где *certificate.cer* – файл в формате .cer, *certificate.crt* – файл в формате .crt.

В конфигурационном файле *ldap* (путь к файлу */etc/openldap/ldap.conf* в ОС Альт, РЕД ОС или */etc/ldap/ldap.conf* в ОС AstraLinux) на рабочей станции под управлением ОС Linux с установленной консолью управления задайте параметр *TLS_CACERT* и укажите путь к файлу, в котором приведены все необходимые сертификаты:

```
TLS_CACERT /etc/ssl/certs/ca-certificates.crt
```

- ❗ Файл *ca-certificates.crt* может содержать несколько сертификатов, каждый из которых начинается с *-----BEGIN CERTIFICATE-----* и заканчивается на *-----END CERTIFICATE-----*. Администратору нужно добавить в файл все необходимые сертификаты для организации безопасного подключения.

Для добавления цепочки корневых сертификатов повторите приведенные действия для всех сертификатов цепочки.

- ❗ Если параметр *TLS_CACERT* задан, то сертификаты, добавленные другими способами, будут проигнорированы при подключении.

Вариант 2:

Для добавления корневого сертификата необходимо выполнить следующие шаги:

- 1) На рабочую станцию под управлением ОС Linux с установленной консолью управления экспортируйте необходимый корневой сертификат.
- 2) В терминале выполните команду

```
sudo trust anchor --store <path_to_certificate>
```

где *path_to_certificate* – путь к файлу с экспортируемым корневым сертификатом.

- 3) Нажмите *Enter* и введите пароль администратора, если потребуется.
- 4) Для добавления цепочки корневых сертификатов повторите приведенные действия для всех сертификатов цепочки.

- ❗ Сертификаты, заданные таким образом, игнорируются, если в config-файле задан параметр *TLS_CACERT*.

Вариант 3:

Для добавления корневого сертификата необходимо выполнить следующие шаги:

- 1) На рабочую станцию под управлением ОС Linux с установленной консолью управления в системный репозиторий сертификатов от имени суперпользователя добавьте корневой сертификат:

```
# cp <path_to_certificate> /etc/pki/ca-trust/source/anchors/  
# update-ca-trust
```

2) Для добавления цепочки корневых сертификатов повторите приведенные действия для всех сертификатов цепочки.

- ❗ Сертификаты, заданные таким образом, игнорируются, если в config-файле задан параметр `TLS_CACERT`.

7.8.6 Проверка работоспособности подключения

На рабочей станции под управлением ОС Linux для проверки работоспособности подключения можно использовать следующую команду:

```
ldapsearch -h "<[полное] имя домена>" -Z -x -LLL -b "" -s base supportedSASLMechanisms -d0
```

параметр `Z` – устанавливает ssl-соединение;
параметр `d` со значением «0» определяет минимальный уровень отладки (уровень отладки регулируется значением от 0 до 3).

- ❗ При правильно настроенных сертификатах команда выводит список поддерживаемых алгоритмов, в противном случае – ошибку.

Для успешного подключения должны выполняться следующие условия:

- домен доступен и настроен в части работы с сертификатами;
- сертификат установлен;
- `<[полное] имя домена>` соответствует значению поля **Common name** установленного сертификата;
- в файле конфигурации отсутствует/закомментирован параметр `TLS_CACERT`.

На рабочей станции под управлением ОС Windows для проверки работоспособности подключения можно использовать утилиту `ldp.exe`.

Для проверки в окне подключения к домену указывается домен, порт (636 для ldaps) и выбирается поддержка ssl.

7.8.7 Особенности при настройке AD для подключения по ldaps из ОС AstraLinux 1.7

На сервере центра сертификации (Certification Authority) при выпуске сертификата может использоваться алгоритм SHA1, считающийся устаревшим (рисунок 7.69).

В ОС AstraLinux версии 1.7 с настройками по умолчанию такой сертификат будет считаться ненадежным и подключение к AD по такому сертификату работать не будет.

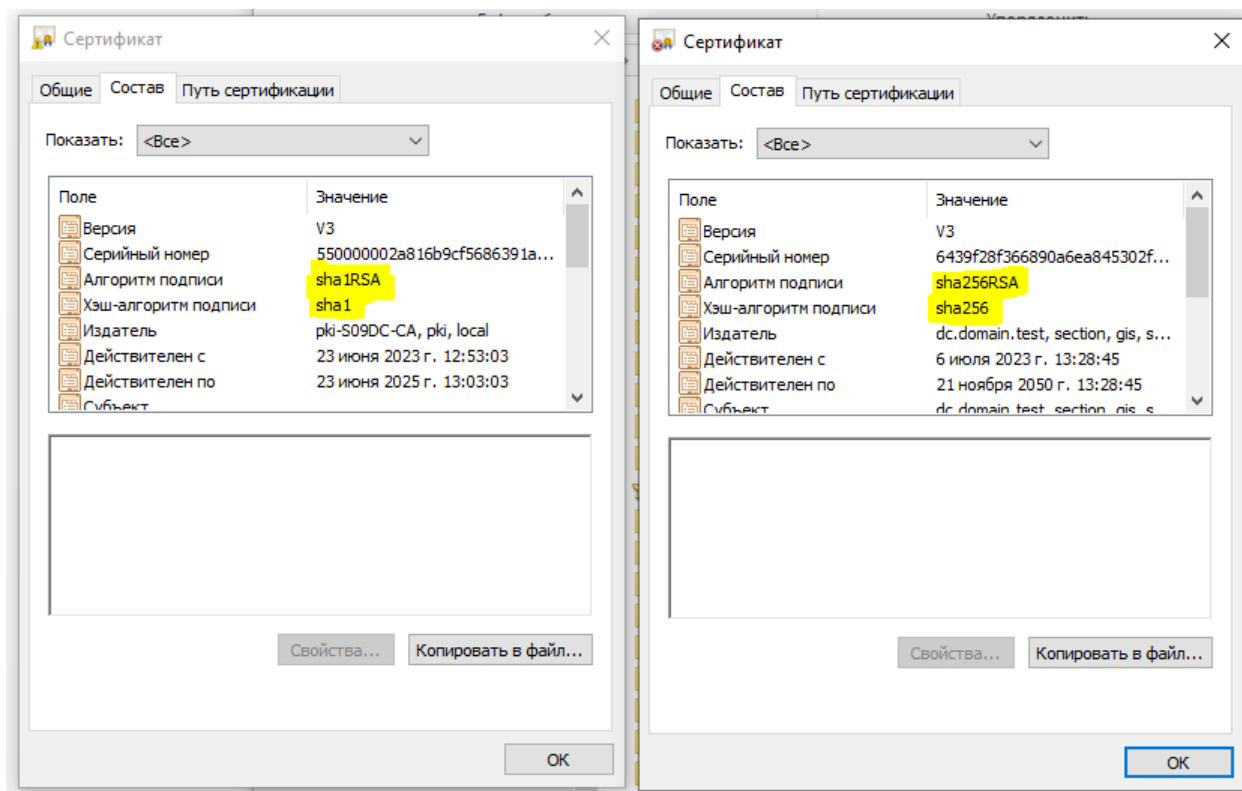


Рисунок 7.69 – Сертификат, использующий sha1 (слева) и sha256 (справа)

Просмотреть используемый сертификат можно командой:

```
openssl x509 -in certificate.crt -text -noout
```

где *certificate.crt* – файл сертификата.

Для изменения алгоритма SHA1 на SHA256 в центре сертификации Windows CA воспользуйтесь инструкцией <https://www.bulygin.su/2016/04/sha1-sha256-windows-ca.html> и выполните следующие действия:

1) На сервере с ролью CA (Certification Authority) проверьте текущий используемый алгоритм командой:

```
certutil -getreg ca\csp\CNGHashAlgorithm
```

Если результат выполнения команды SHA256, перейдите к шагу 4.

2) Если результат выполнения команды **SHA1**, для перенастройки центра сертификации на использование SHA256 необходимо выполнить команду:

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
```

3) Перезапустите *Certificate Services* с помощью команды:

```
net stop CertSvc && net start CertSvc
```

4) Перевыпустите корневой сертификат:


```
certutil -renewCert ReuseKeys
```

5) Перезапустите службу *Certificate Services*:

```
net stop CertSvc && net start CertSvc
```

В результате указанных действий будет создан новый корневой сертификат центра сертификации с использованием SHA256 в качестве алгоритма подписи, который необходимо экспортировать на клиентские рабочие станции.

Перечень сокращений

CA	–	Certification Authority (удостоверяющий центр)
OU	–	Organizational Unit (организационное подразделение)
RSA	–	Аббревиатура от фамилий Rivest, Shamir и Adleman (криптографический алгоритм с открытым ключом)
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
СЗИ	–	Средство защиты информации