JMS. Типовой сценарий развертывания (MSCA)

Версия ПО: JMS 2.x - 3.x

Токены: Любые

Проблема: Типовой сценарий развертывания для выпуска сертификатов на Microsoft CA

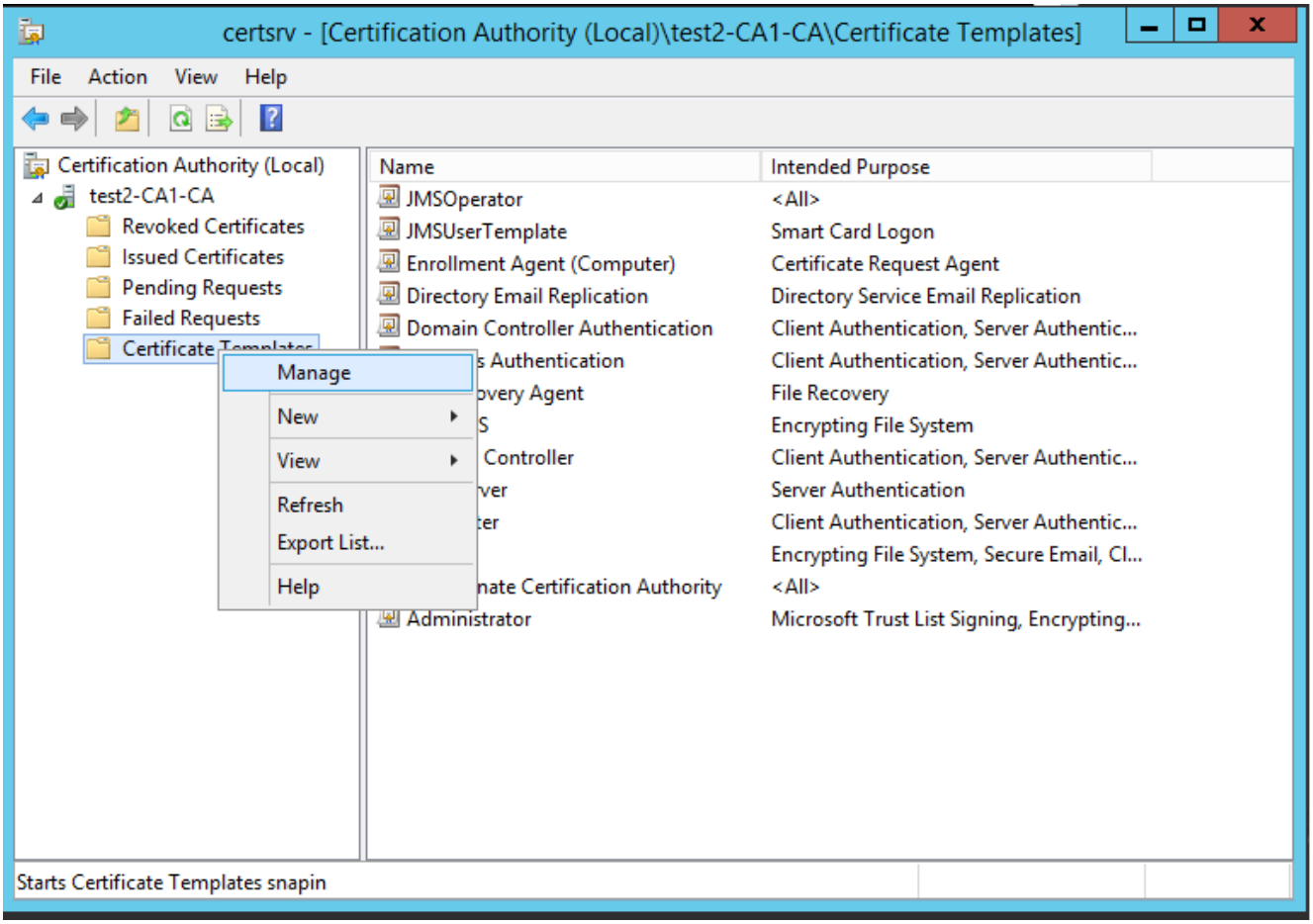
Решение:

1. Настройка УЦ MSCA.

1.1. Шаблон для оператора JMS.

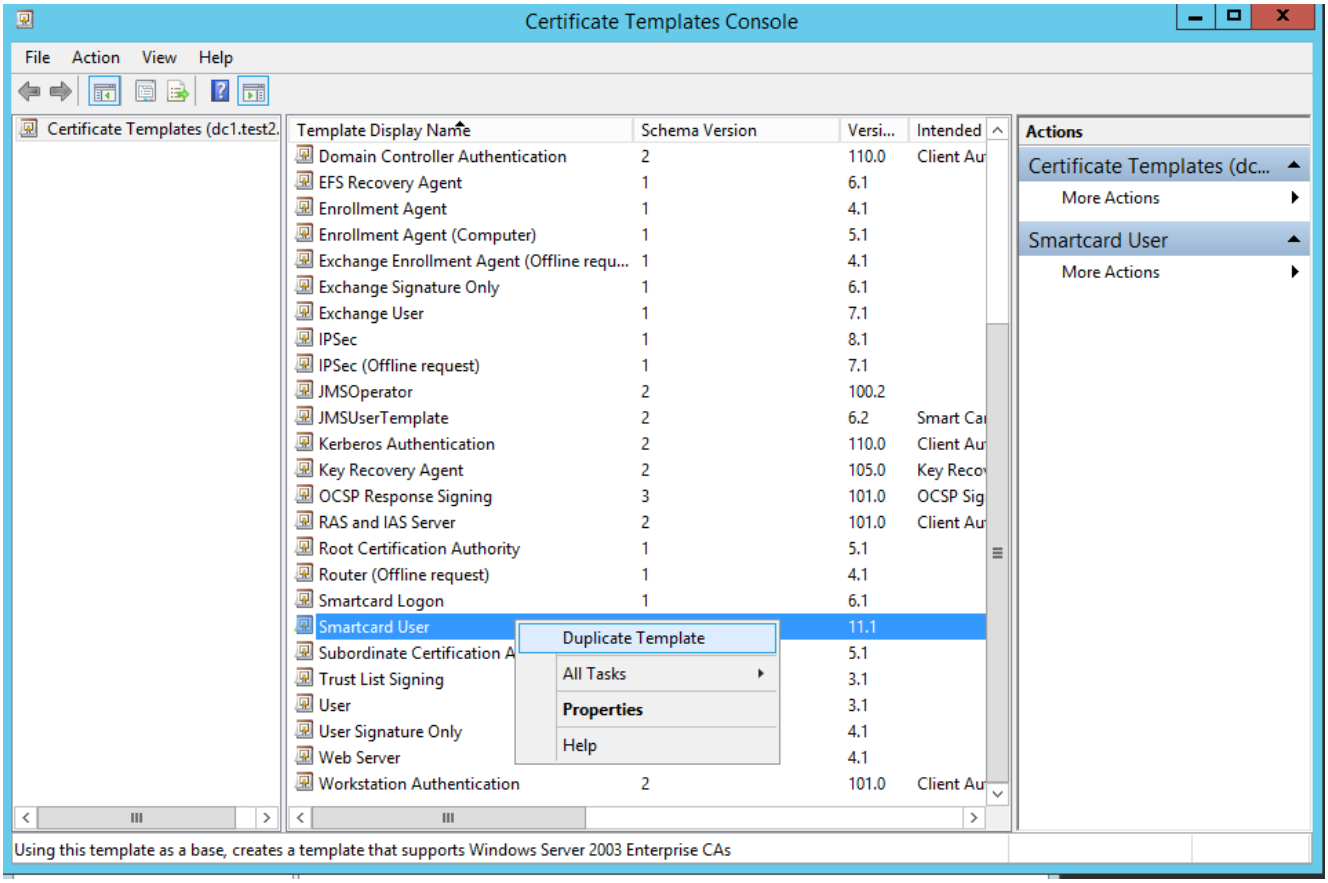
Нажать на клавиатуре Win+R certsrv.msc. Откроется консоль MSCA

Необходимо зайти в управление шаблонами, на папке с шаблонами сертификатов нажать правой кнопкой мыши - "Управление / Manage":

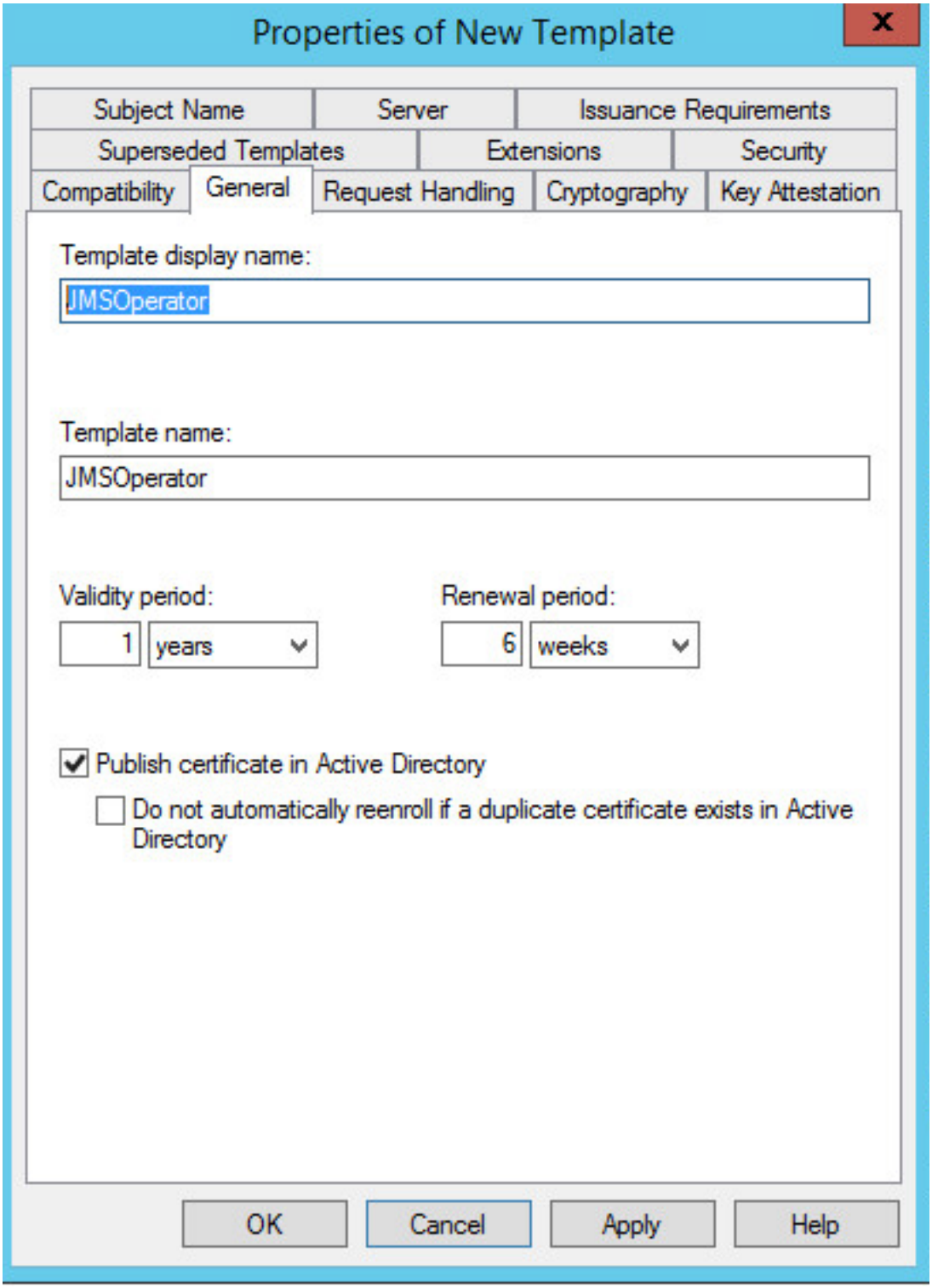


Откроется консоль управления шаблонами.

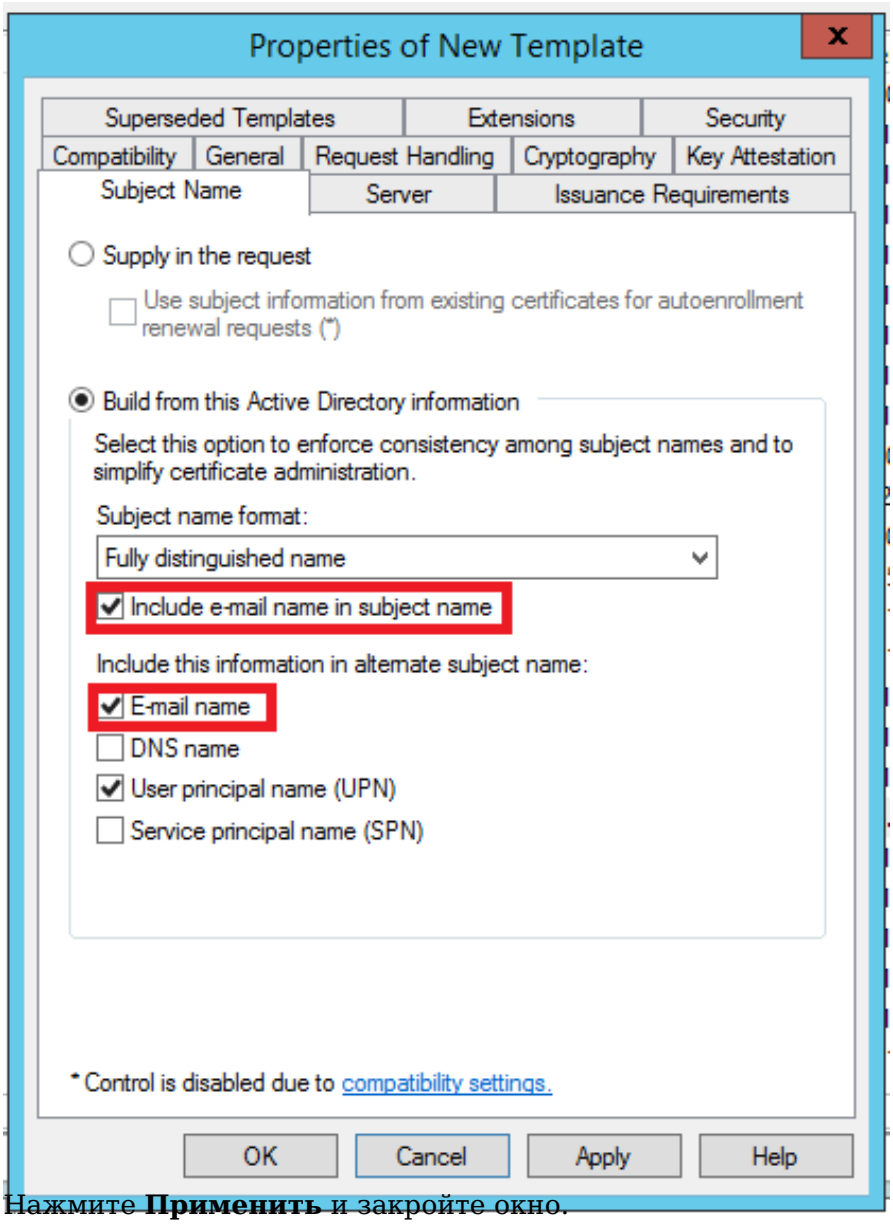
Найдите шаблон "Пользователь со смарт-картой", нажмите правой кнопкой мыши "Скопировать шаблон":



Откроется окно настройки нового шаблона. Перейдите на вкладку **Основные** и задайте имя шаблона:



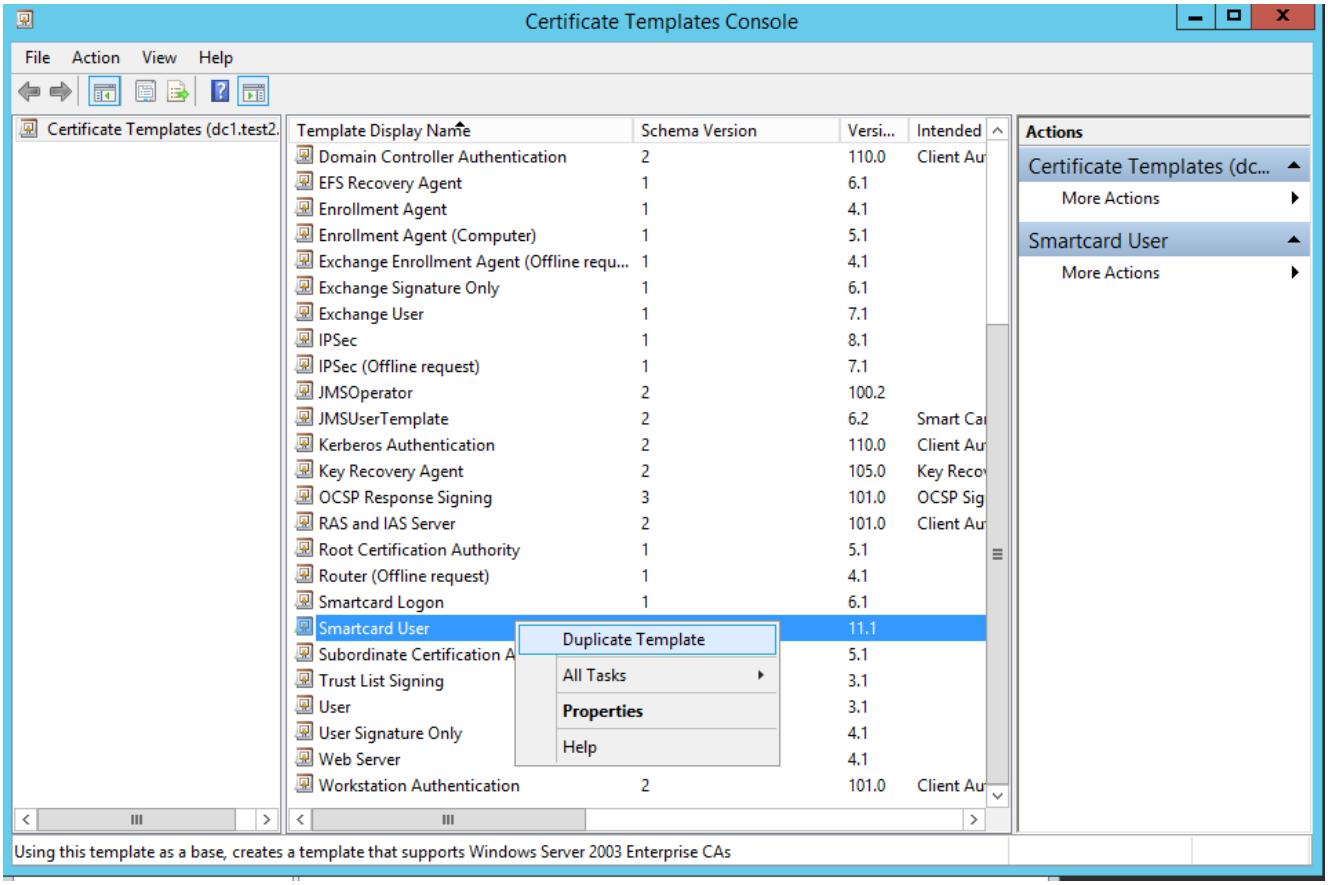
Перейдите на вкладку **Имя субъекта**. Если у пользователя не предполагается наличия адреса Email в AD, уберите опции, указанные ниже:



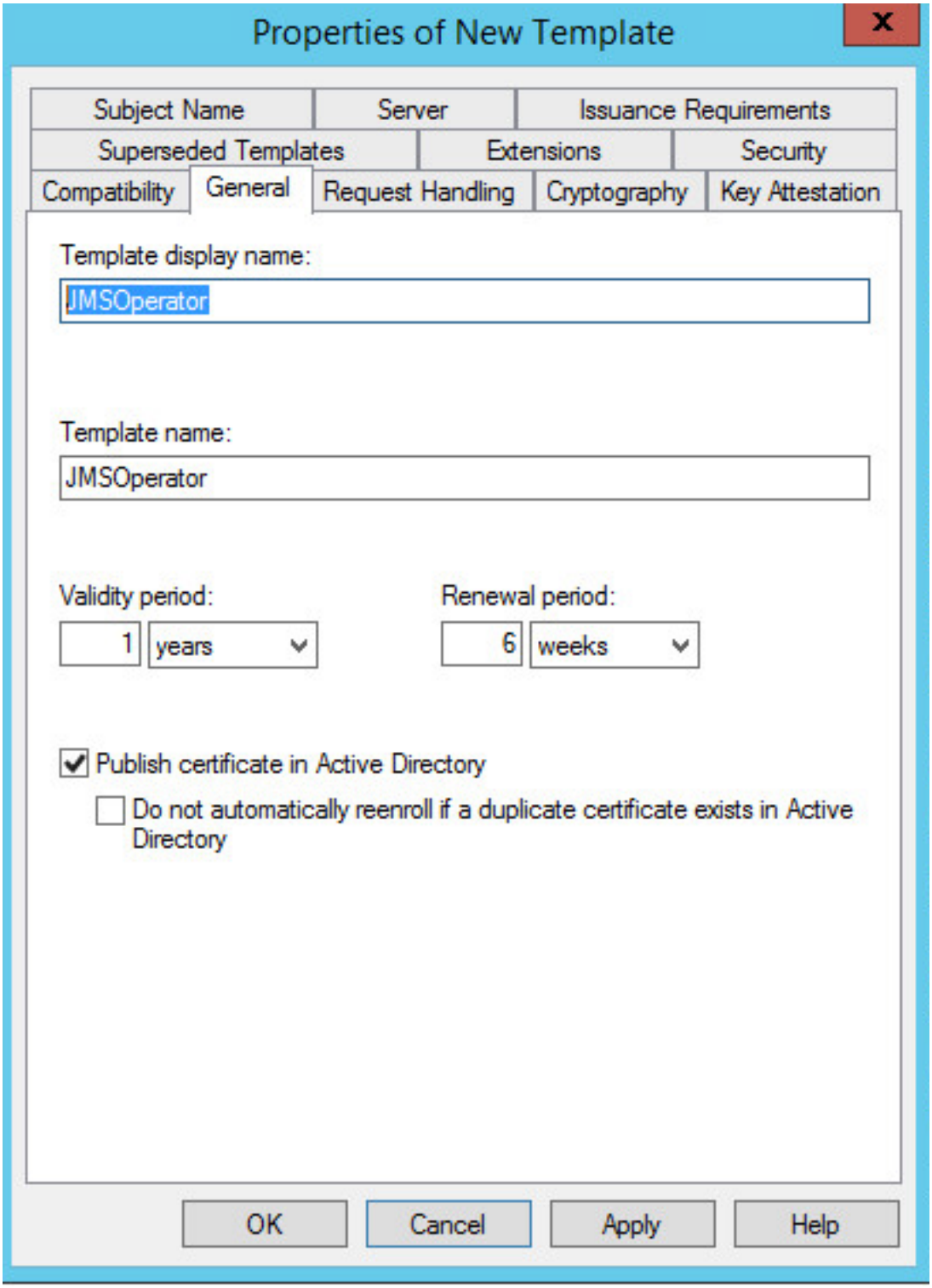
Нажмите **Применить** и закройте окно.

1.2. Шаблон для выпуска сертификатов пользователям JMS.

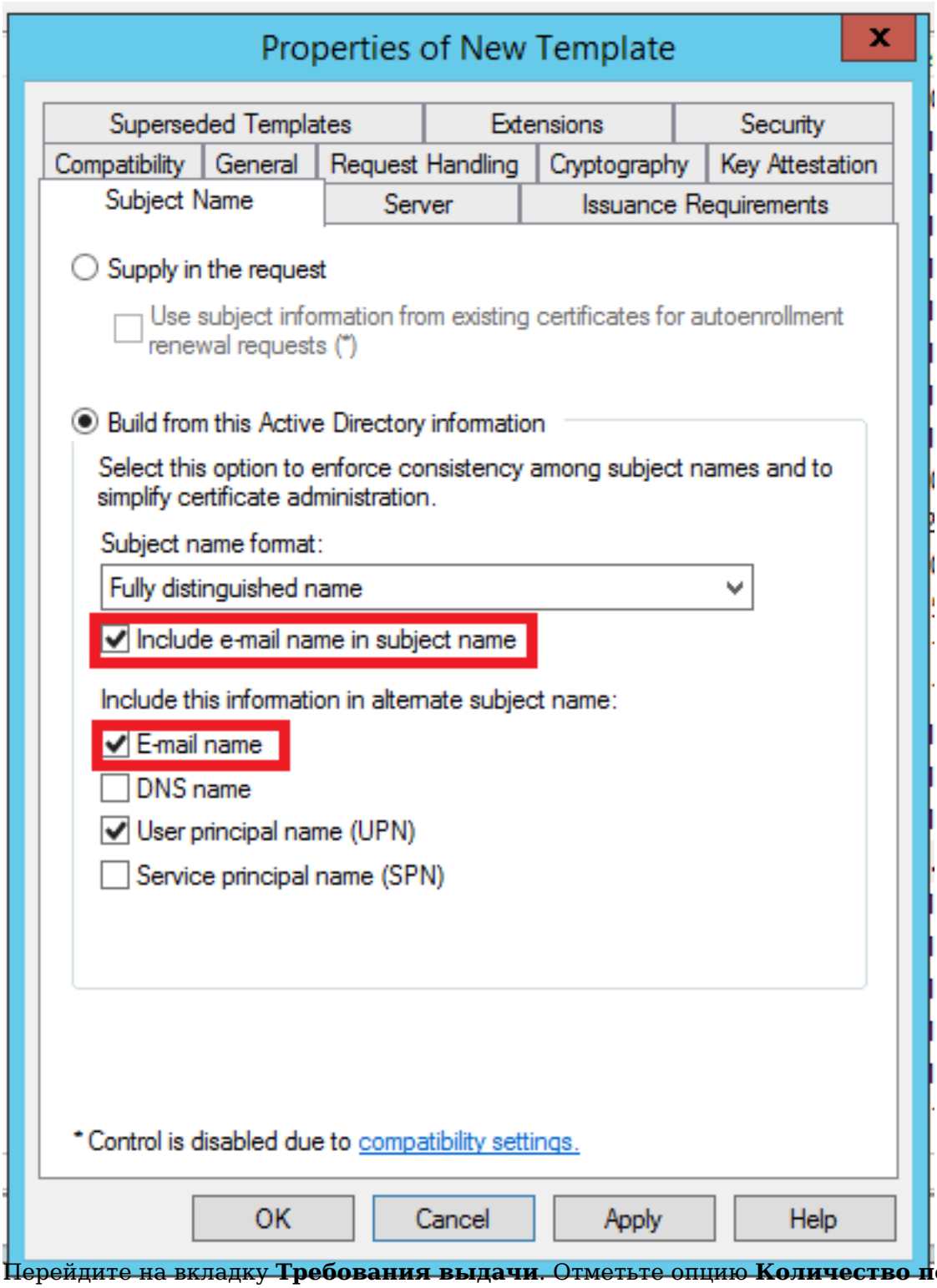
Найдите шаблон "Пользователь со смарт-картой", нажмите правой кнопкой мыши "Скопировать шаблон":



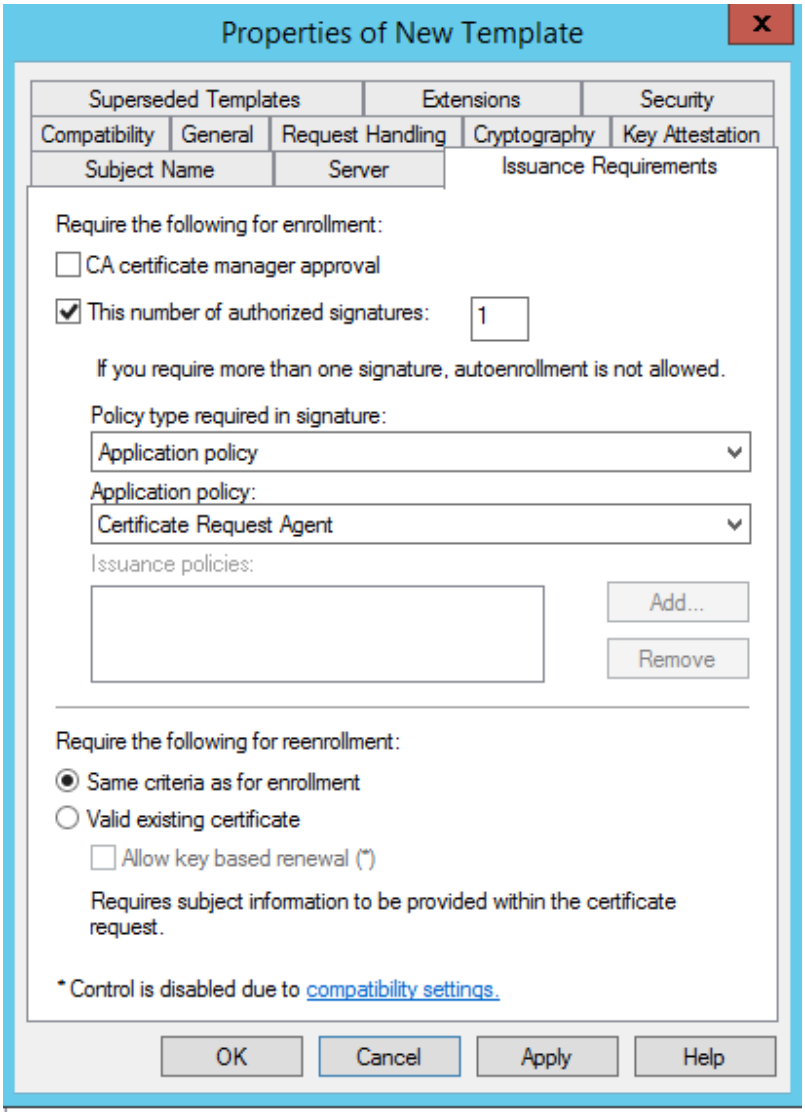
Откроется окно настройки нового шаблона. Перейдите на вкладку **Основные** и задайте имя шаблона:



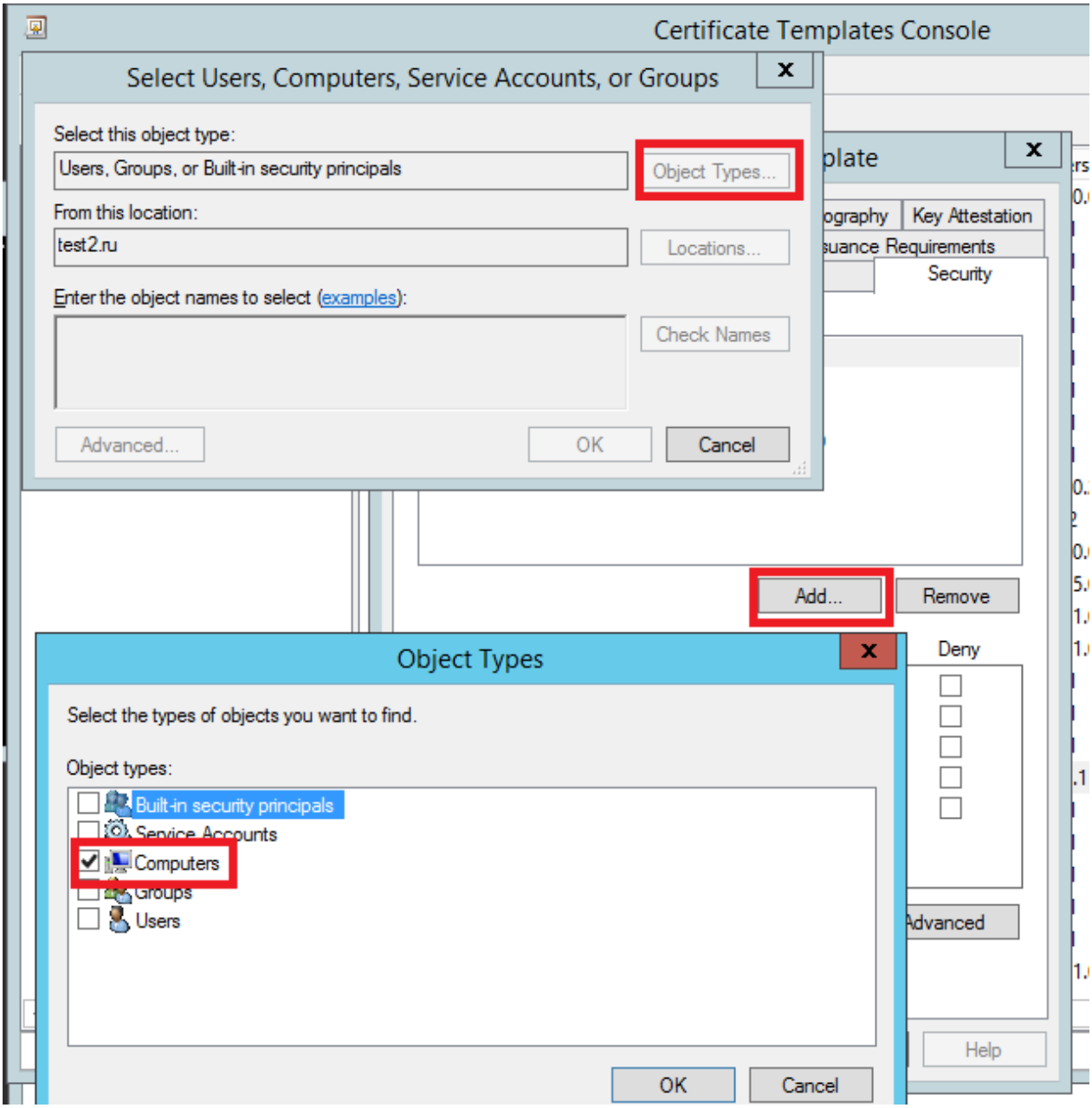
Перейдите на вкладку **Имя субъекта**. Если у пользователя не предполагается наличия адреса Email в AD, уберите опции, указанные ниже:



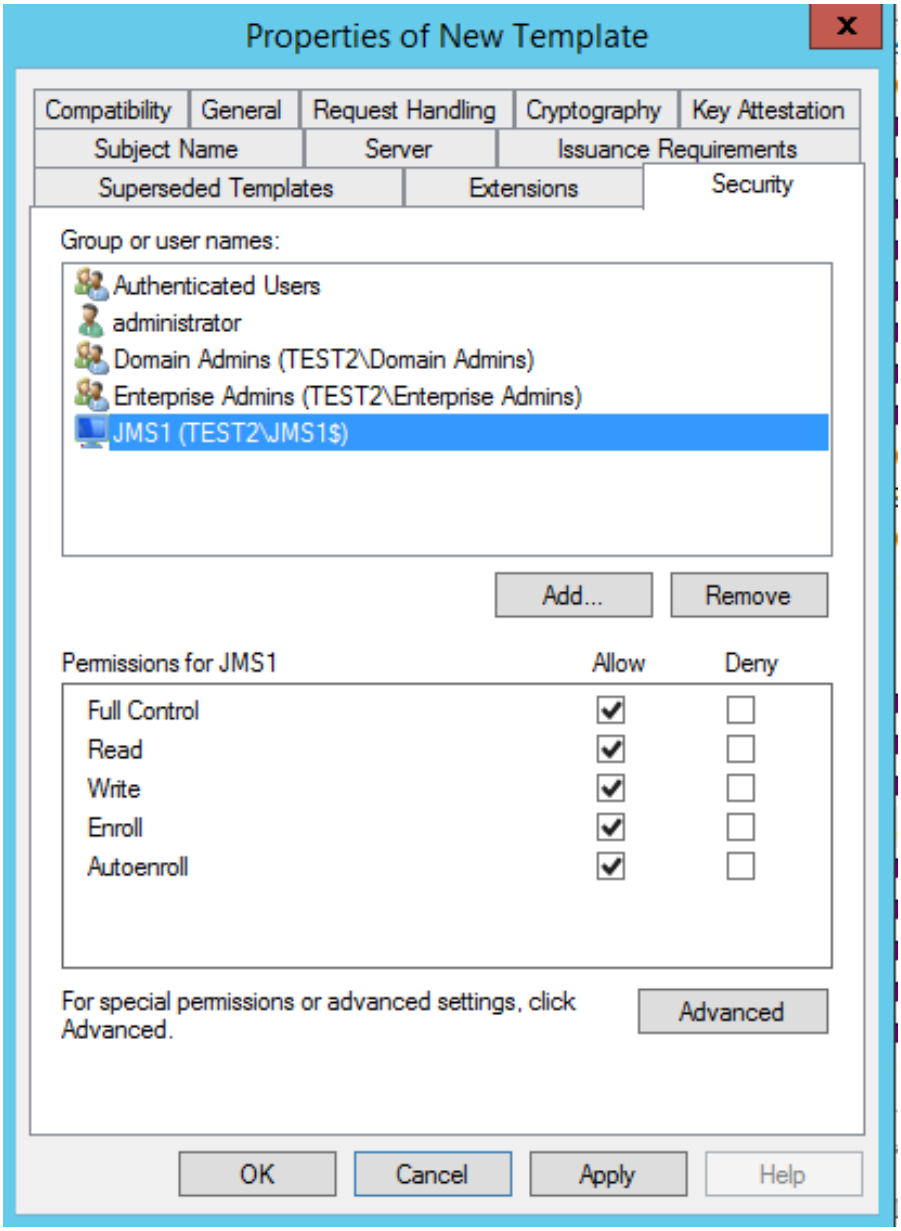
Перейдите на вкладку **Требования выдачи**. Отметьте опцию **Количество подписей**. Ниже выберите из списка **Политика применения** и **Сертификат агента запроса**:



Перейдите на вкладку **Безопасность**, нажмите **Добавить**, далее Типы объектов, оставьте только **Компьютеры**:



Воспользуйтесь кнопкой **Дополнительно** и выберите свой сервер JMS. Установите ему полные права:



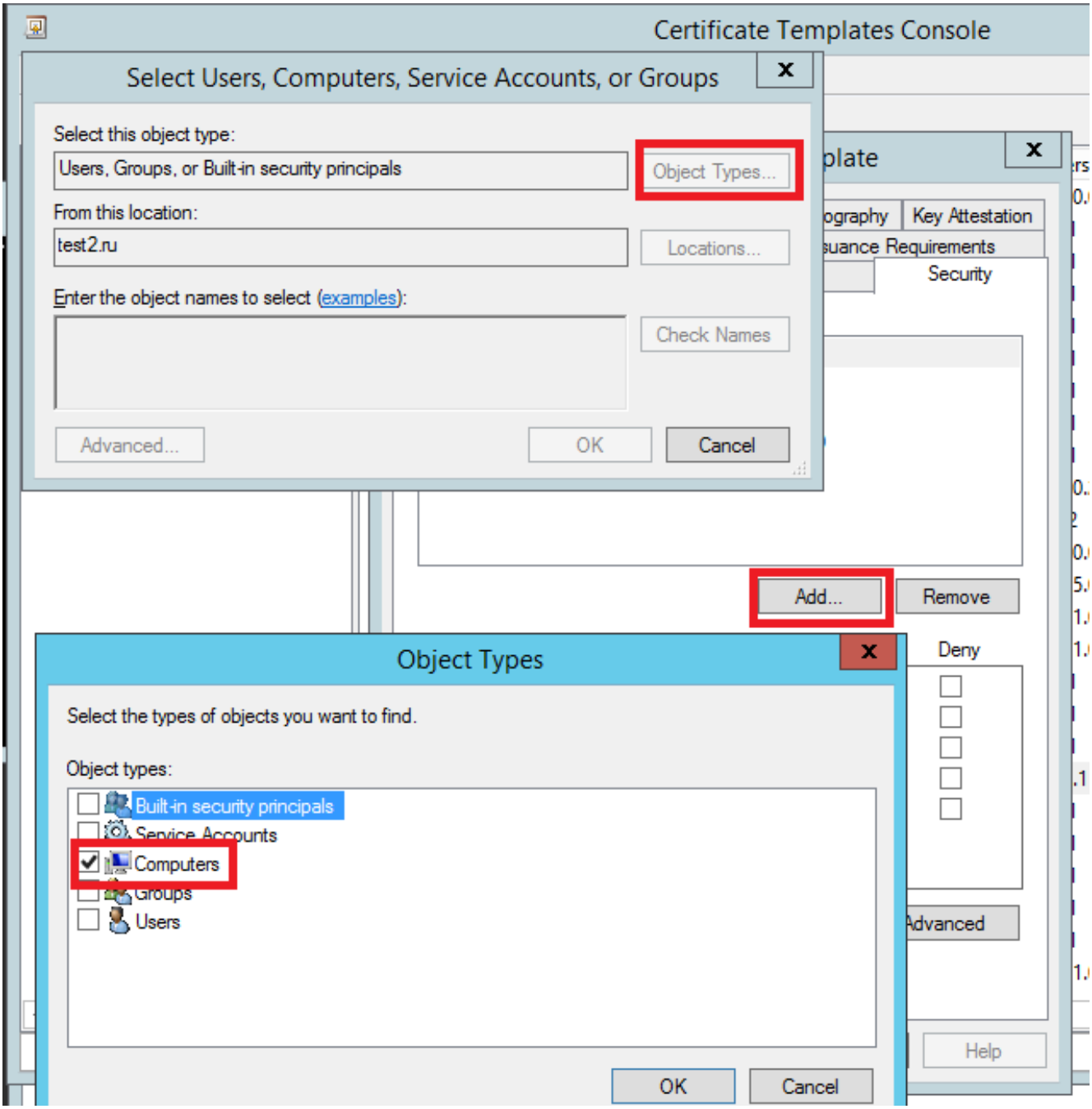
Нажмите **Применить** и закройте окно.

1.3. Шаблон агента выпуска для сервера JMS.

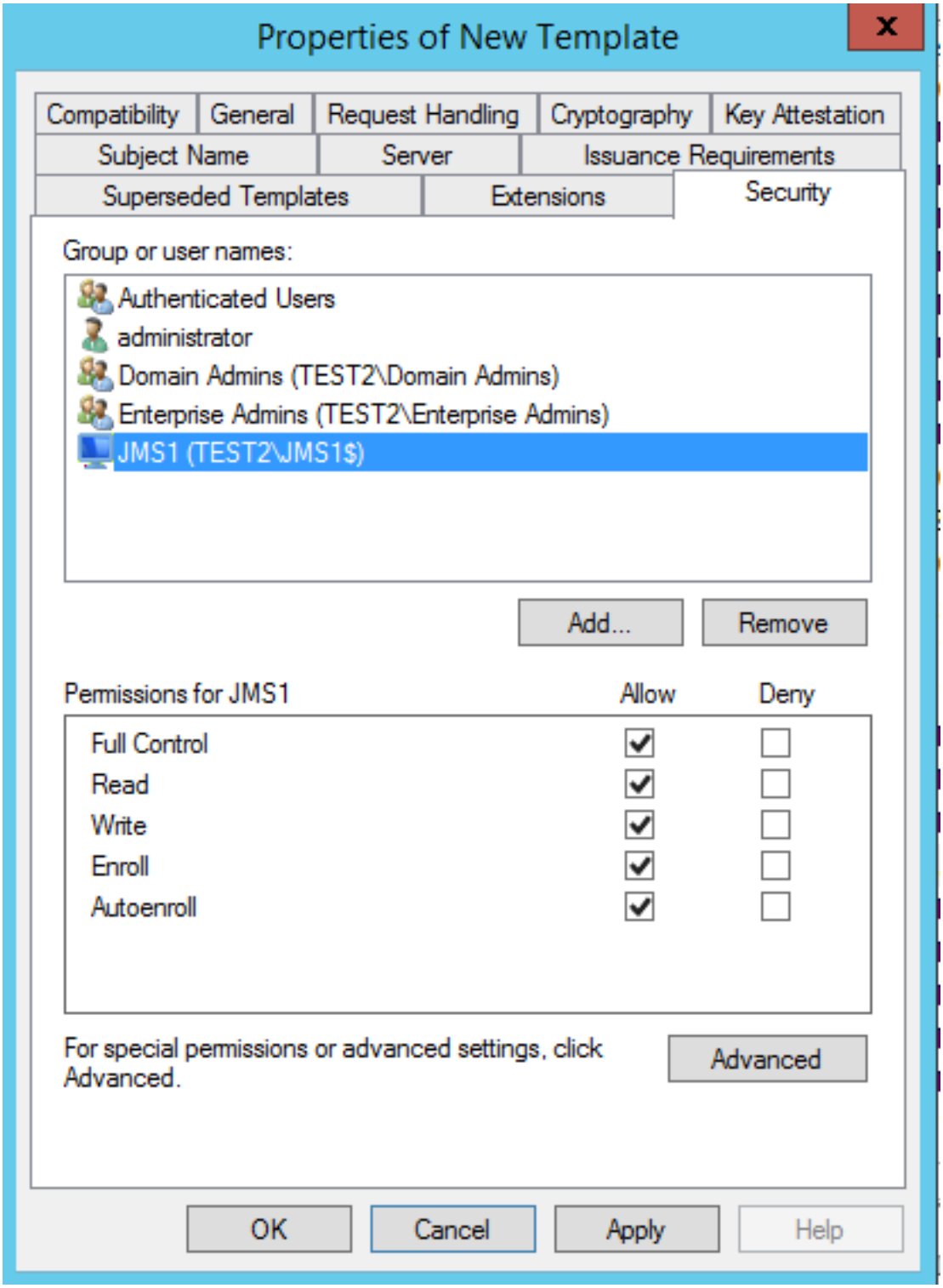
Найдите шаблон "Агент регистрации (компьютер)", нажмите правой кнопкой мыши "Скопировать шаблон".

Откроется окно настройки нового шаблона. Перейдите на вкладку **Основные** и задайте имя шаблона.

Перейдите на вкладку **Безопасность**, нажмите **Добавить**, далее — Типы объектов, оставьте только **Компьютеры**:



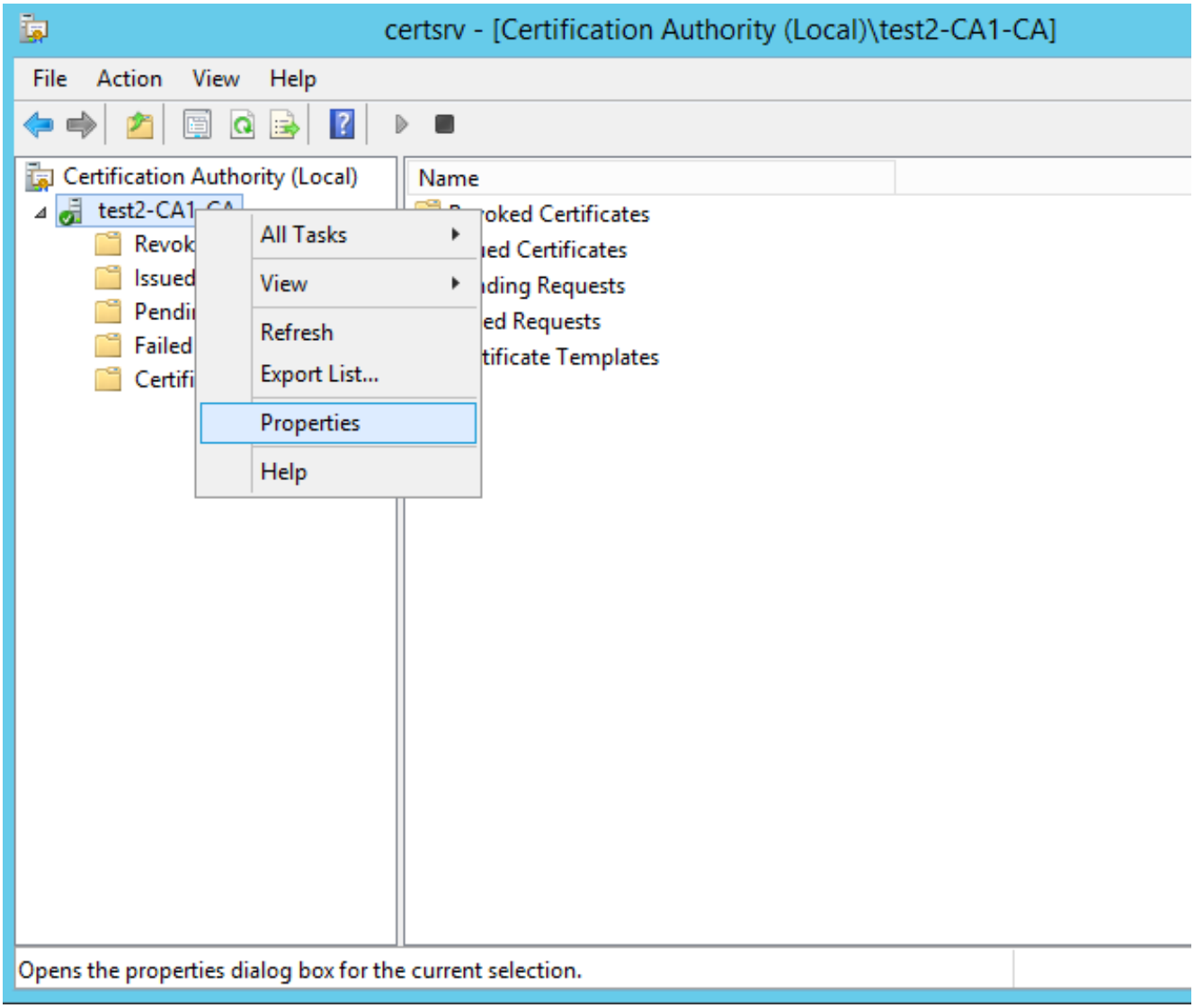
Воспользуйтесь кнопкой **Дополнительно** и выберите свой сервер JMS. Установите ему полные права:



Нажмите **Применить** и закройте окно.

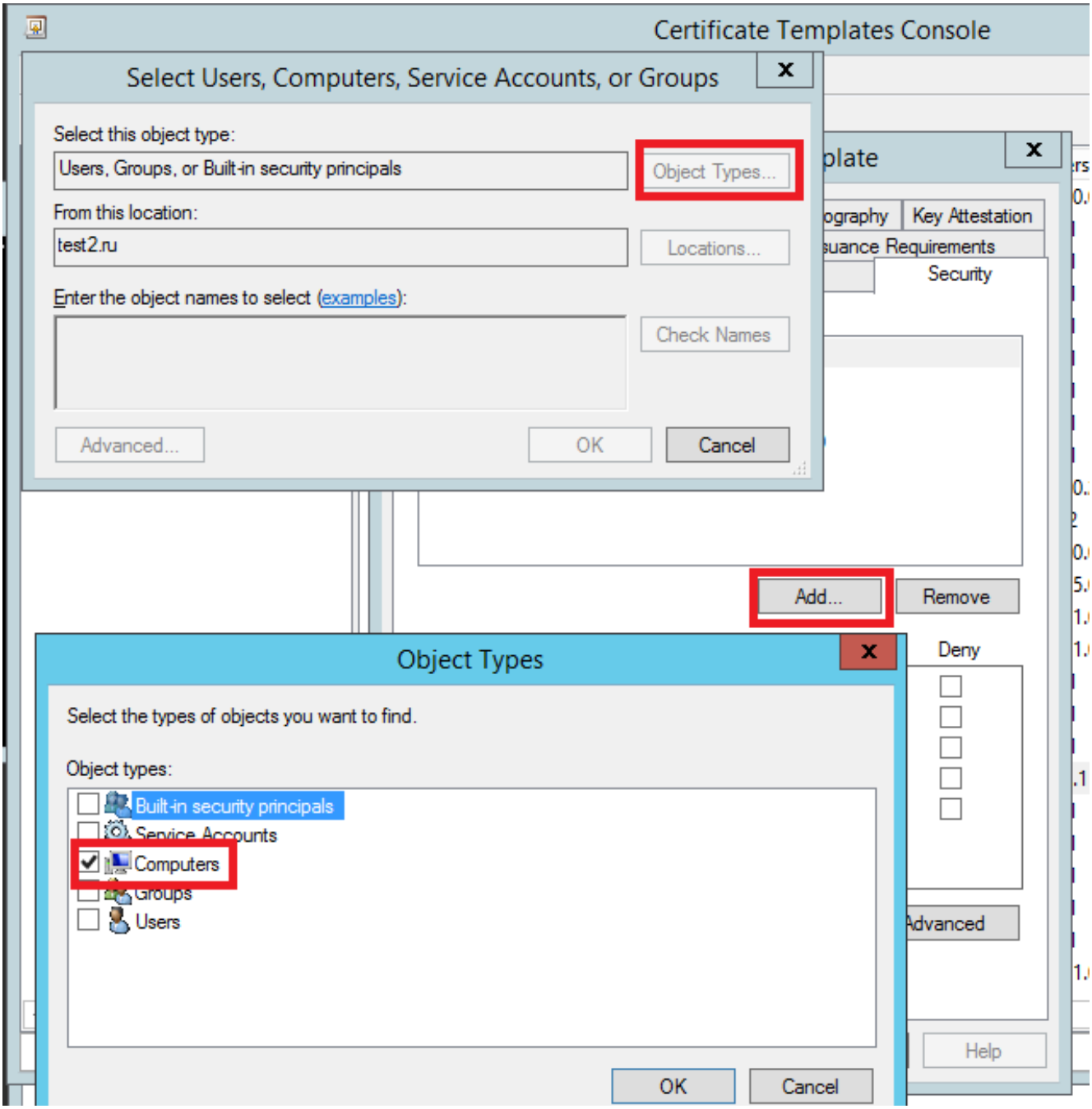
1.4. Настройка доступа к MSCA.

В консоли MSCA поместите курсор на имя сервера, нажмите правой кнопкой мыши "Свойства":

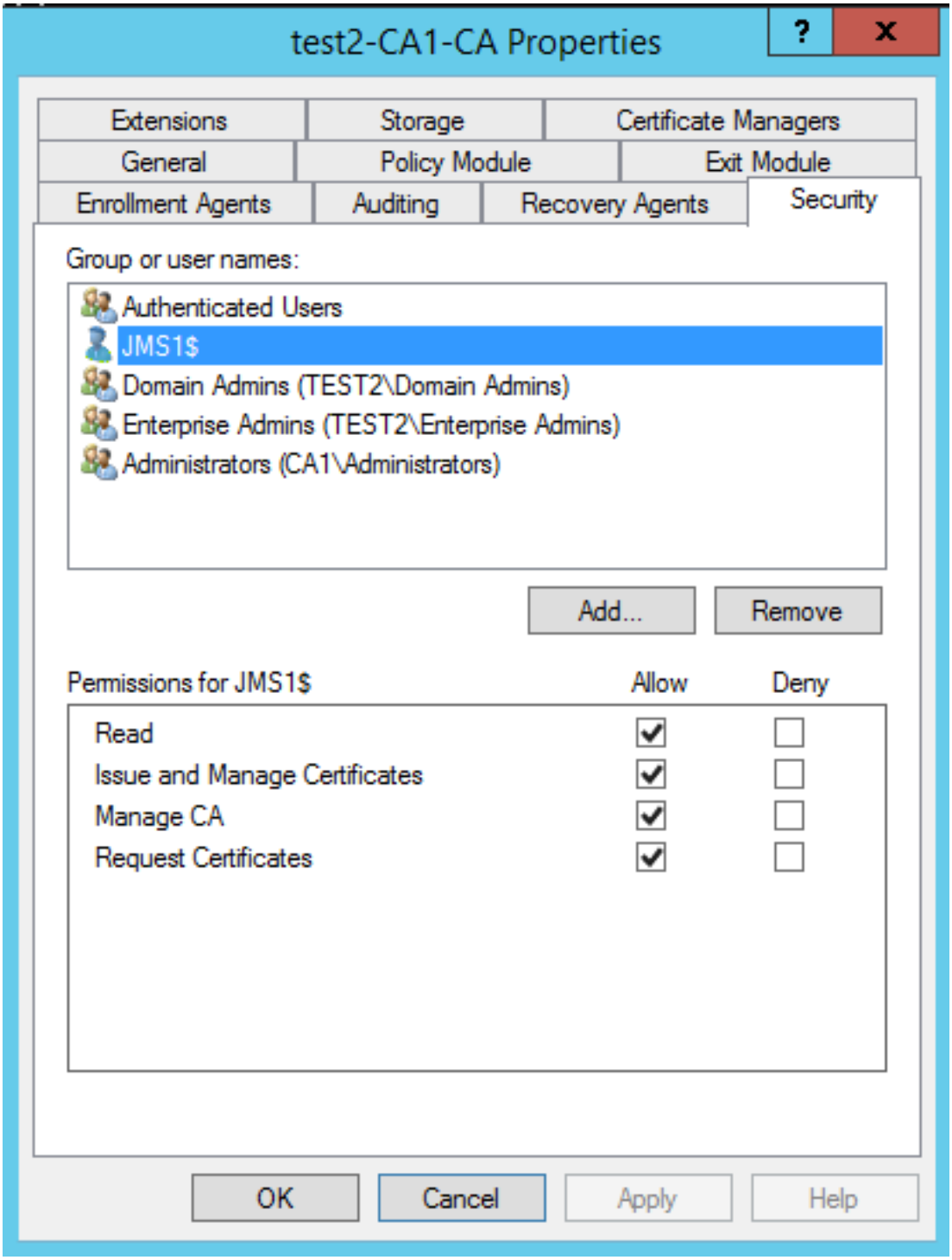


В открывшемся окне перейдите на вкладку **Безопасность**. Нажмите **Добавить** и выберите ваш сервер JMS.

Далее — Типы объектов, оставьте только **Компьютеры**:



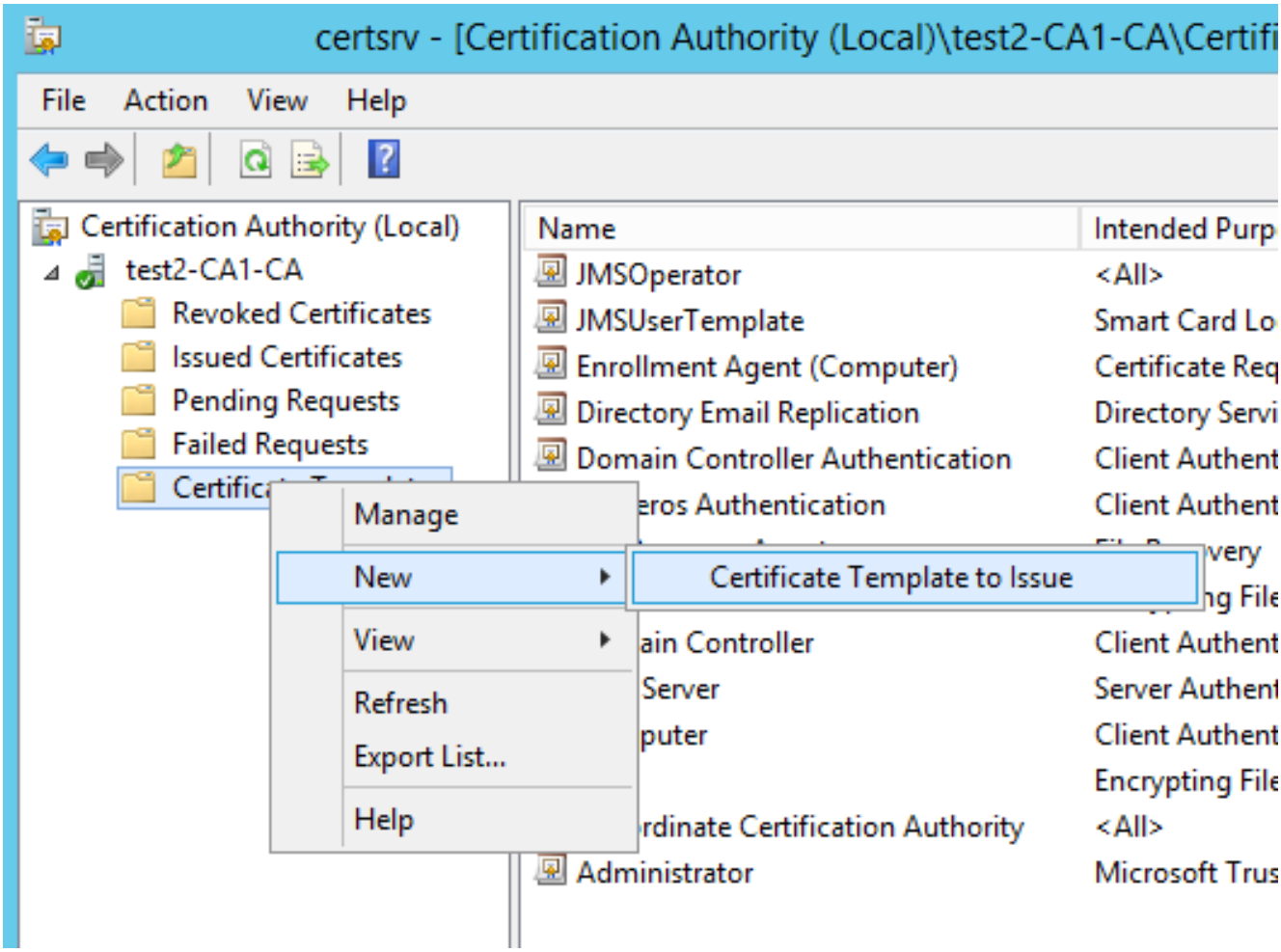
Дайте полные права серверу JMS:



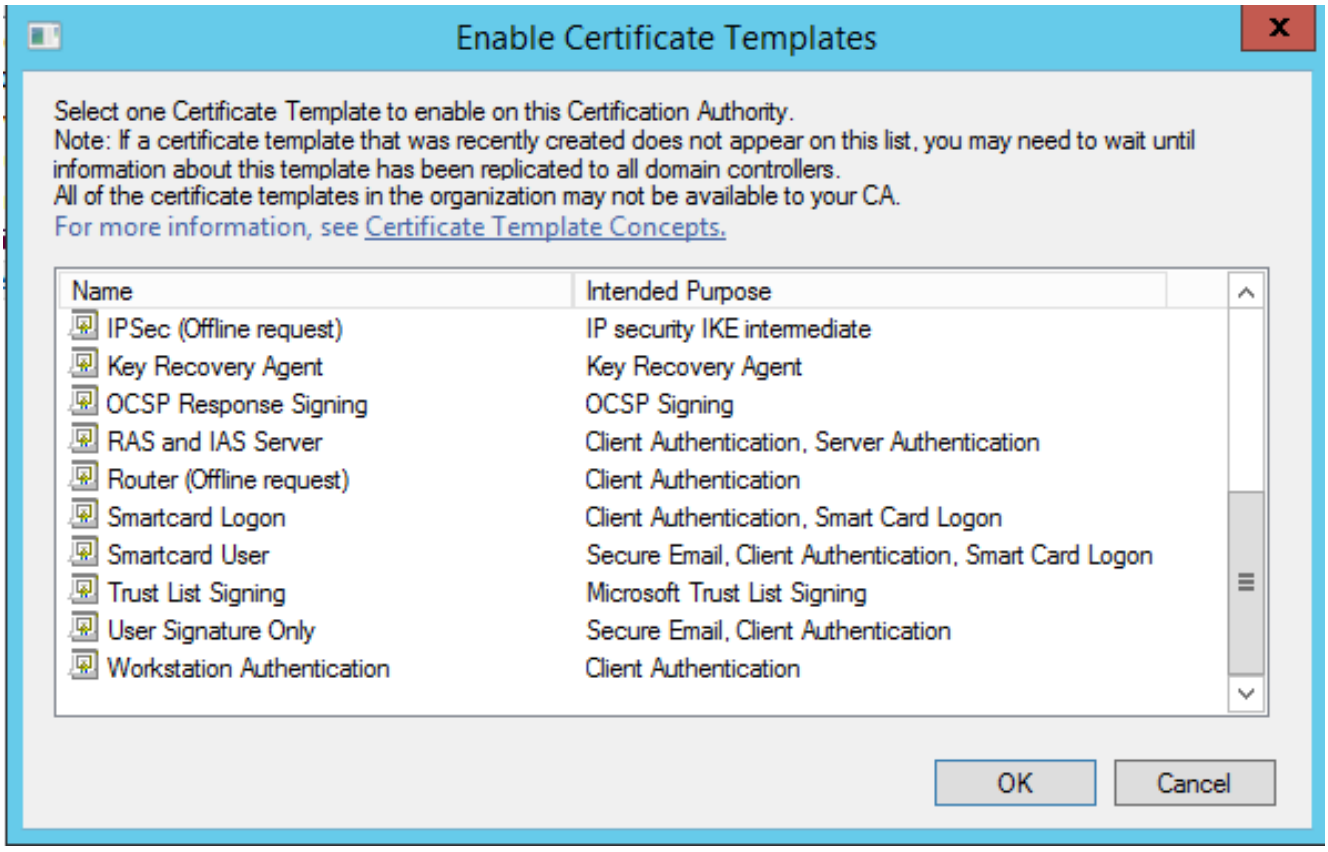
Нажмите **Применить** и закройте окно.

1.5. Добавление шаблонов в список выдаваемых.

В консоли сервера MSCA на папке шаблонов нажмите правой кнопкой мыши — "Новый" — "Выдаваемые шаблоны сертификатов".



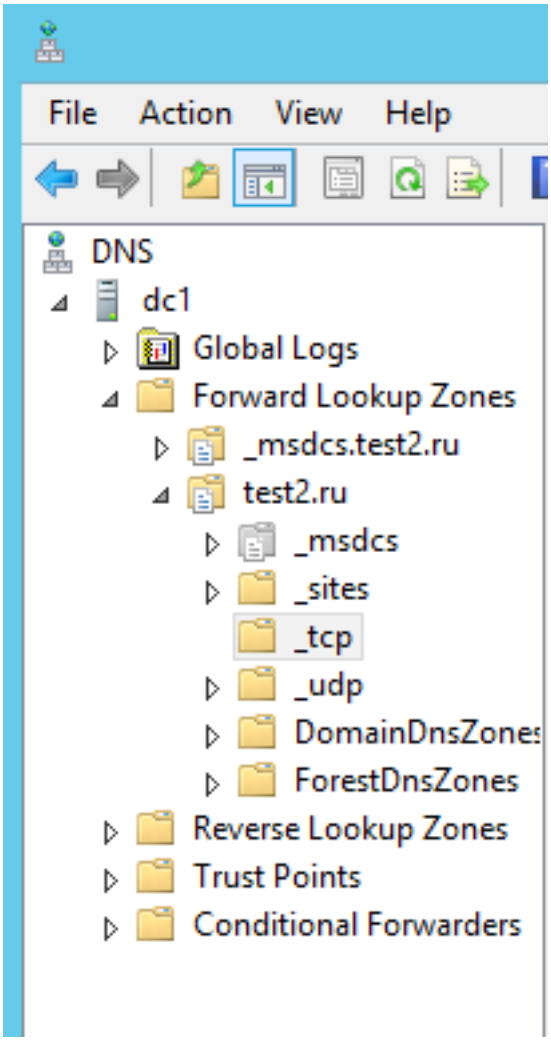
Откроется окно с доступными шаблонами:



Отметьте созданные нами шаблоны и нажмите OK.

2. Настройка записей на сервере DNS.

Запустите консоль управления сервером DNS: `dnsmgmt.msc`. Перейдите в папку Зоны прямого просмотра\<Имя вашего домена>_tcp.



Нажмите правой кнопкой мыши на папке _tcp: "Другая новая запись". В появившемся окне найдите Расположение службы (**SRV**) и нажмите "Создать запись". В открывшемся окне введите данные:

Аналогично создайте также записи для служб **_eap_client**, порт 9009 и **_eap_sts**, порт 9011.

В свойствах созданных записей на вкладке **Безопасность** дайте следующие права на чтение:

- для всех группе Authenticated users, для **_eap_client** и **_eap_sts** добавьте еще группу "Компьютеры домена";

- для проверки корректности записей DNS используйте команду:

```
nslookup -type=srv _eap_server._tcp.<?????? ??? ??????>
```

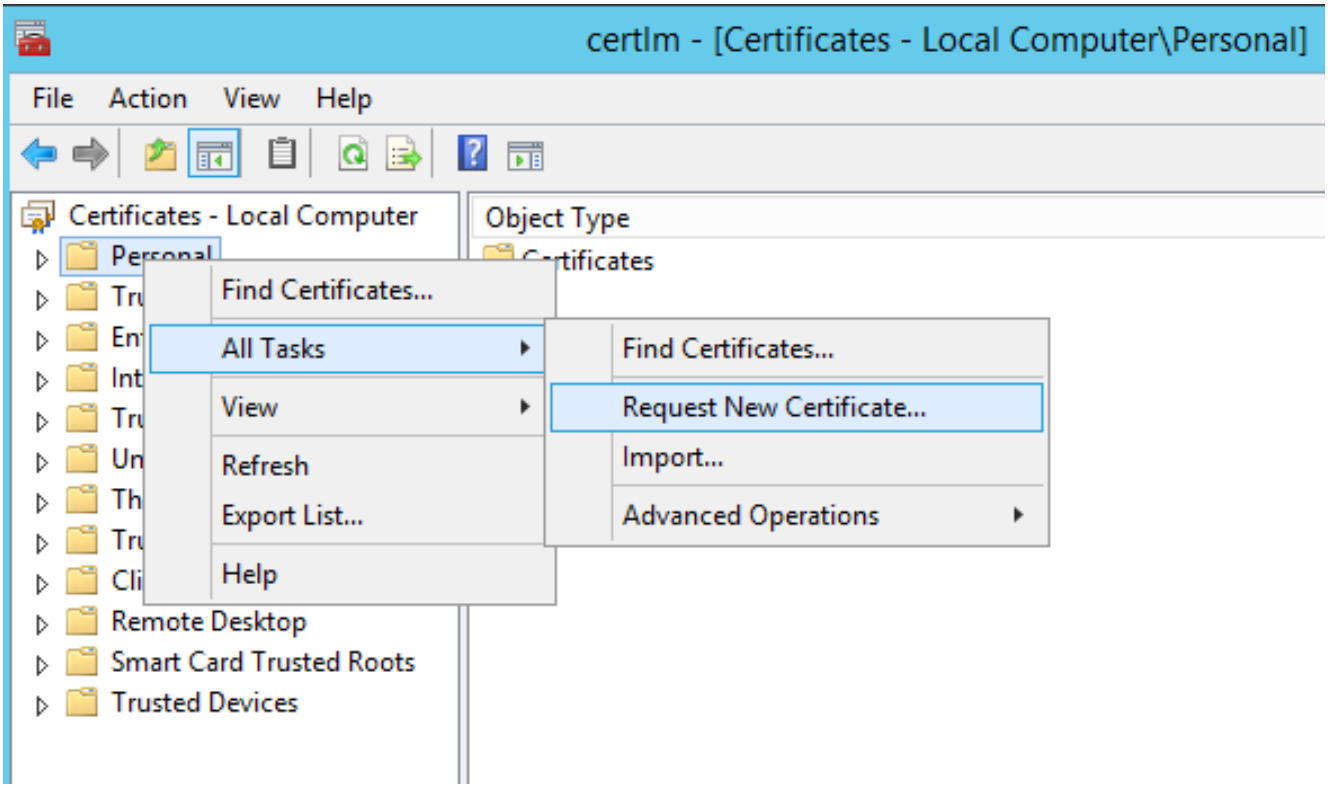
3. Подготовка сервера и установка JMS.

Действия производятся на сервере JMS.

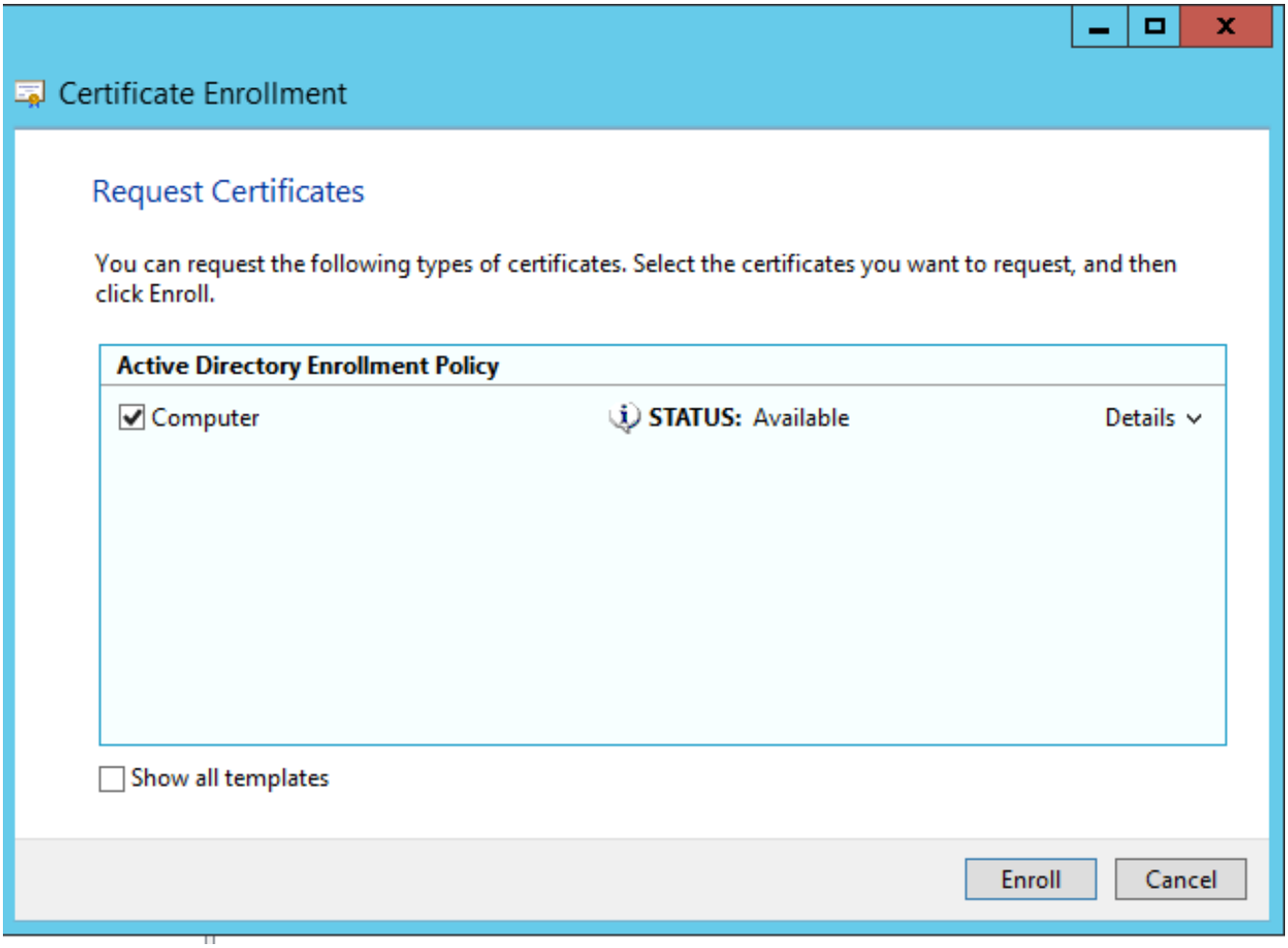
3.1. Установка сертификата аутентификации.

Откройте консоль сертификатов локального компьютера: `certlm.msc`.

На папке "**Личные**" нажать правой кнопкой мыши — "**Все задачи**" — "**Запросить новый сертификат**":



Откроется мастер запроса сертификатов. Два раза нажимаем "**Далее**" и выбираем шаблон **Компьютер**. Нажимаем **Выпустить** и дожидаемся сообщения об успешном выпуске.

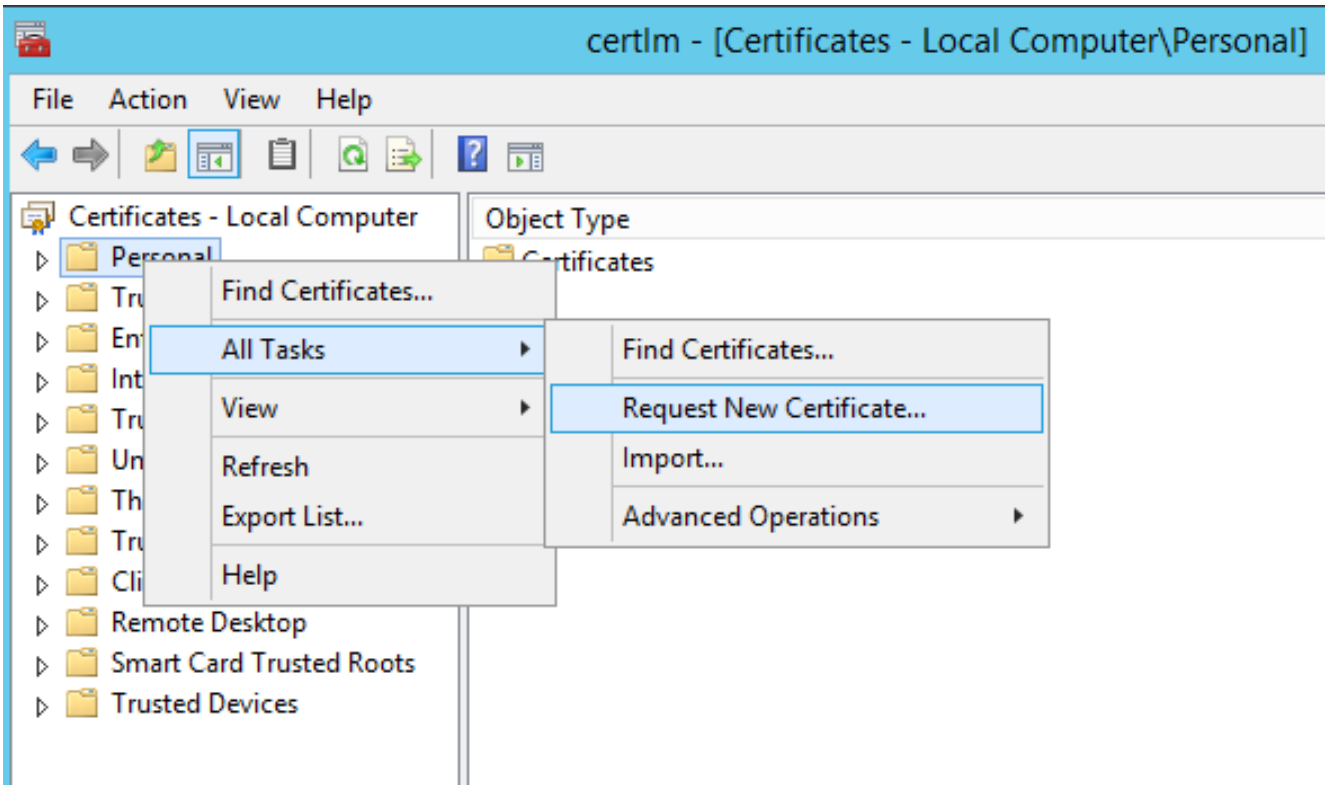


3.2. Выпуск сертификата агента запроса.

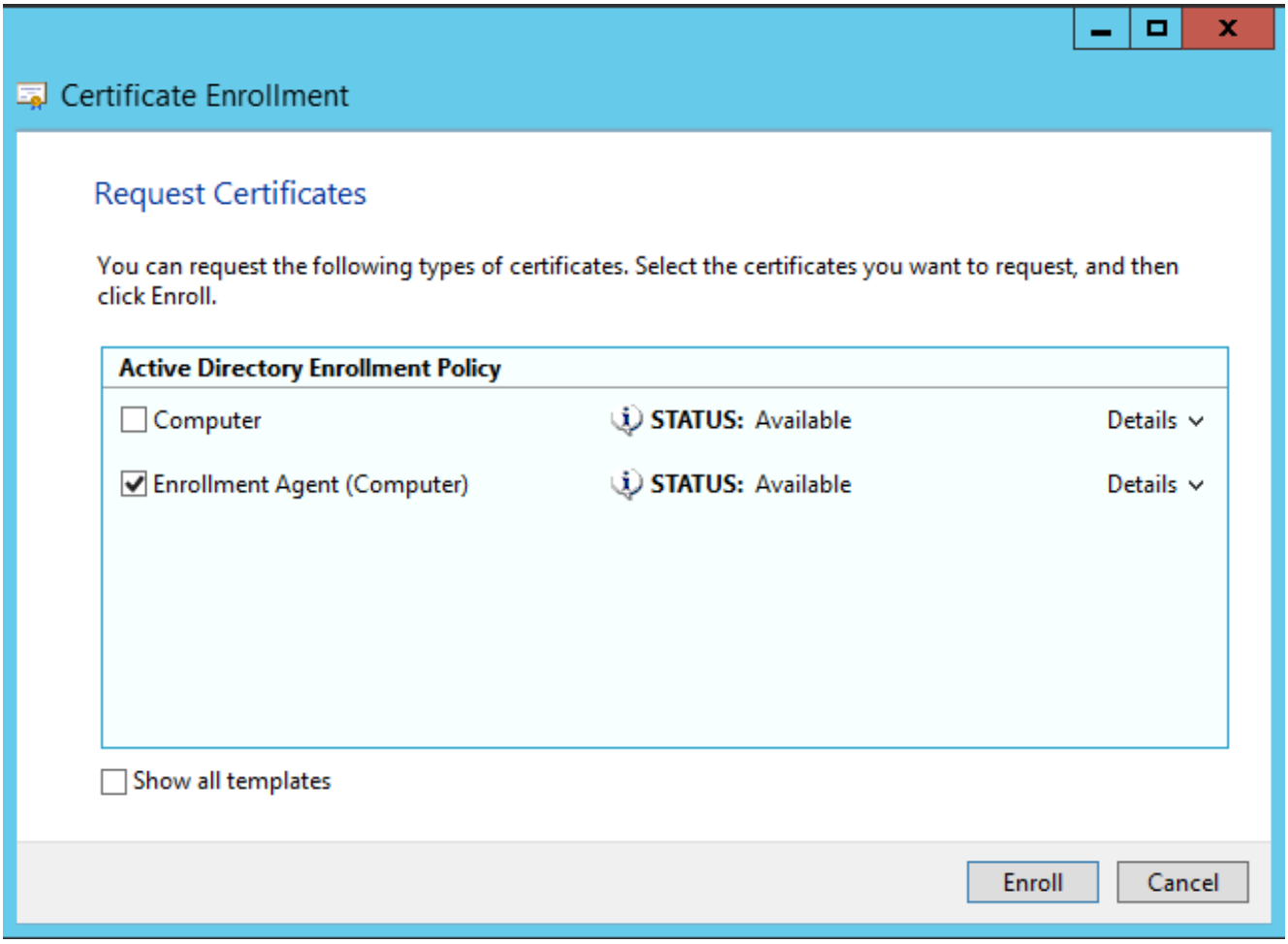
Откройте консоль сертификатов локального компьютера: `certlm.msc`.

На папке "**Личные**" нажать правой кнопкой мыши — "**Все задачи**" — "**Запросить новый**

сертификат":



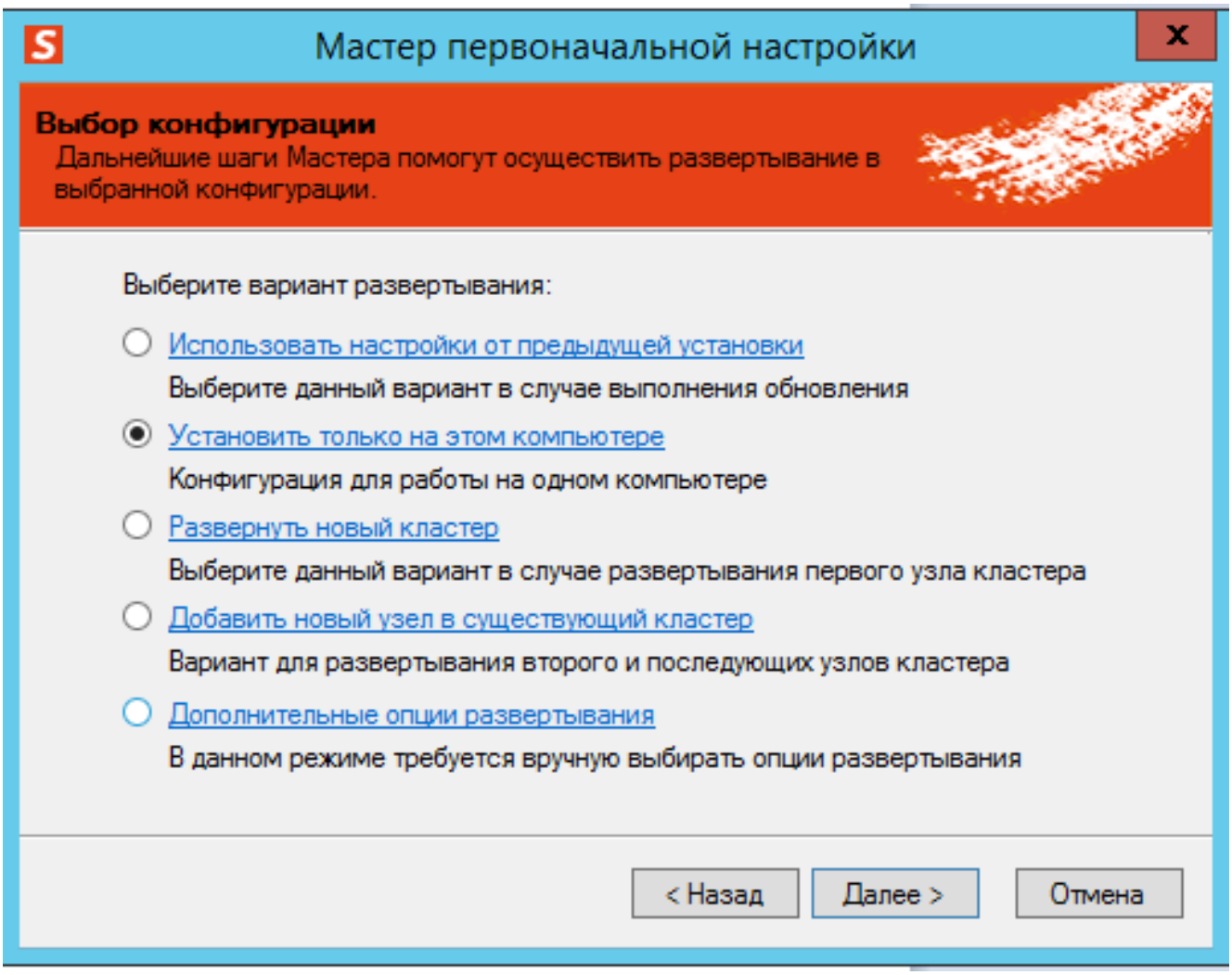
Откроется мастер запроса сертификатов. Два раза нажимаем "Далее" и выбираем шаблон агента запроса сертификатов.



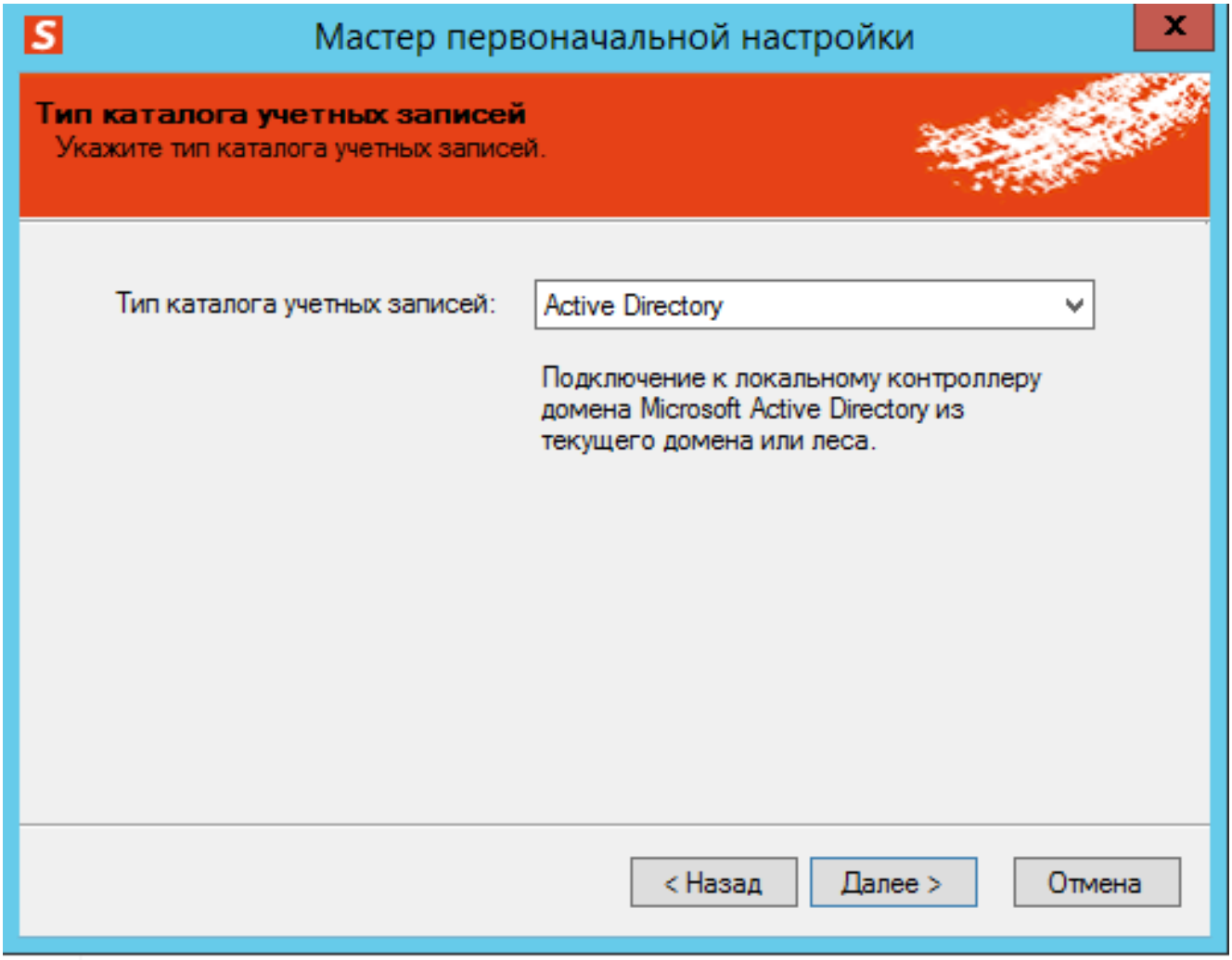
Нажмите "Выпустить" и дождитесь сообщение об успешном выпуске.

3.3. Установка и конфигурация сервера JMS.

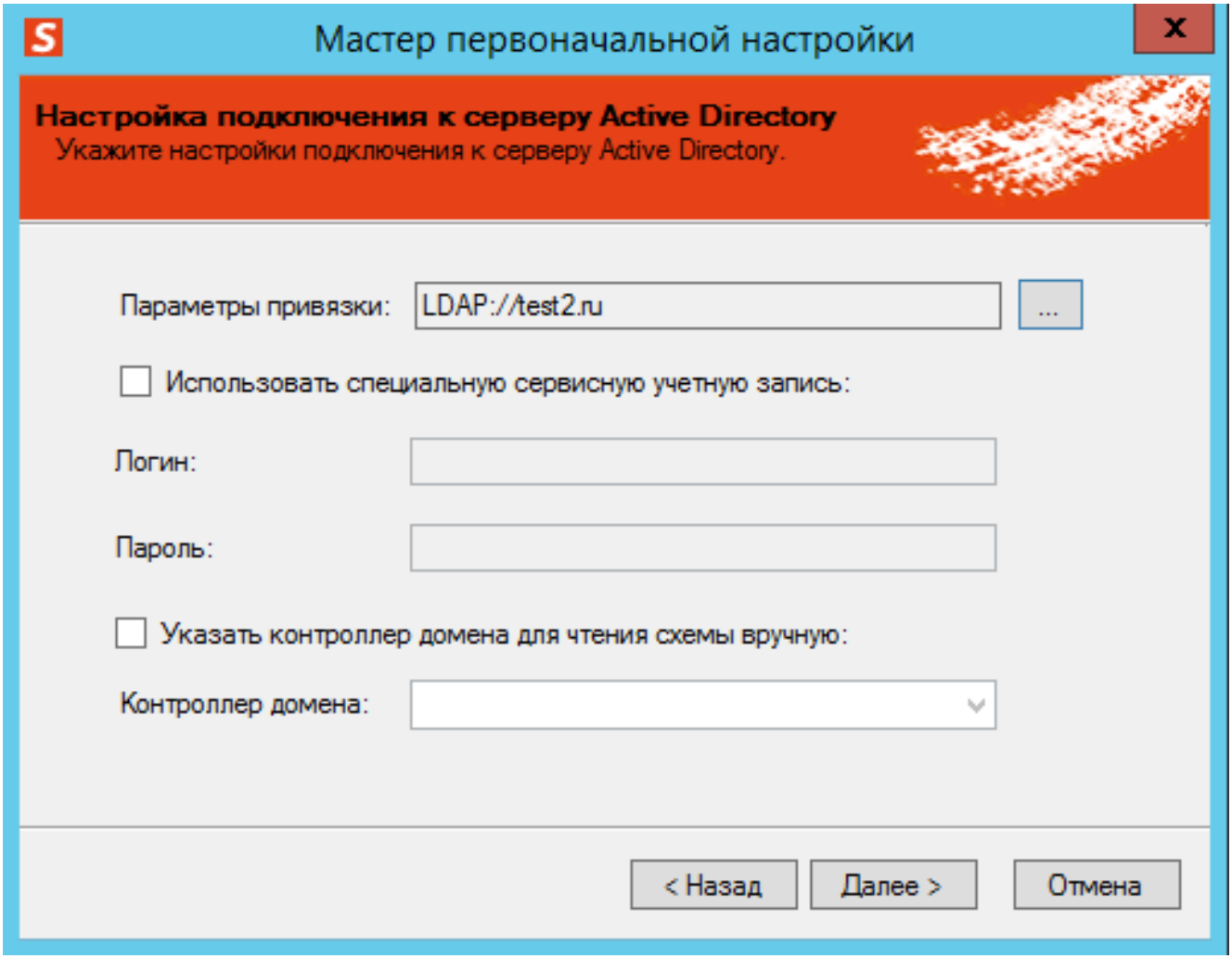
Запустите установку серверной части JMS. После установки запустится мастер начальной конфигурации. Выберите "Установить только на этом компьютере":



Тип каталога — Active Directory:

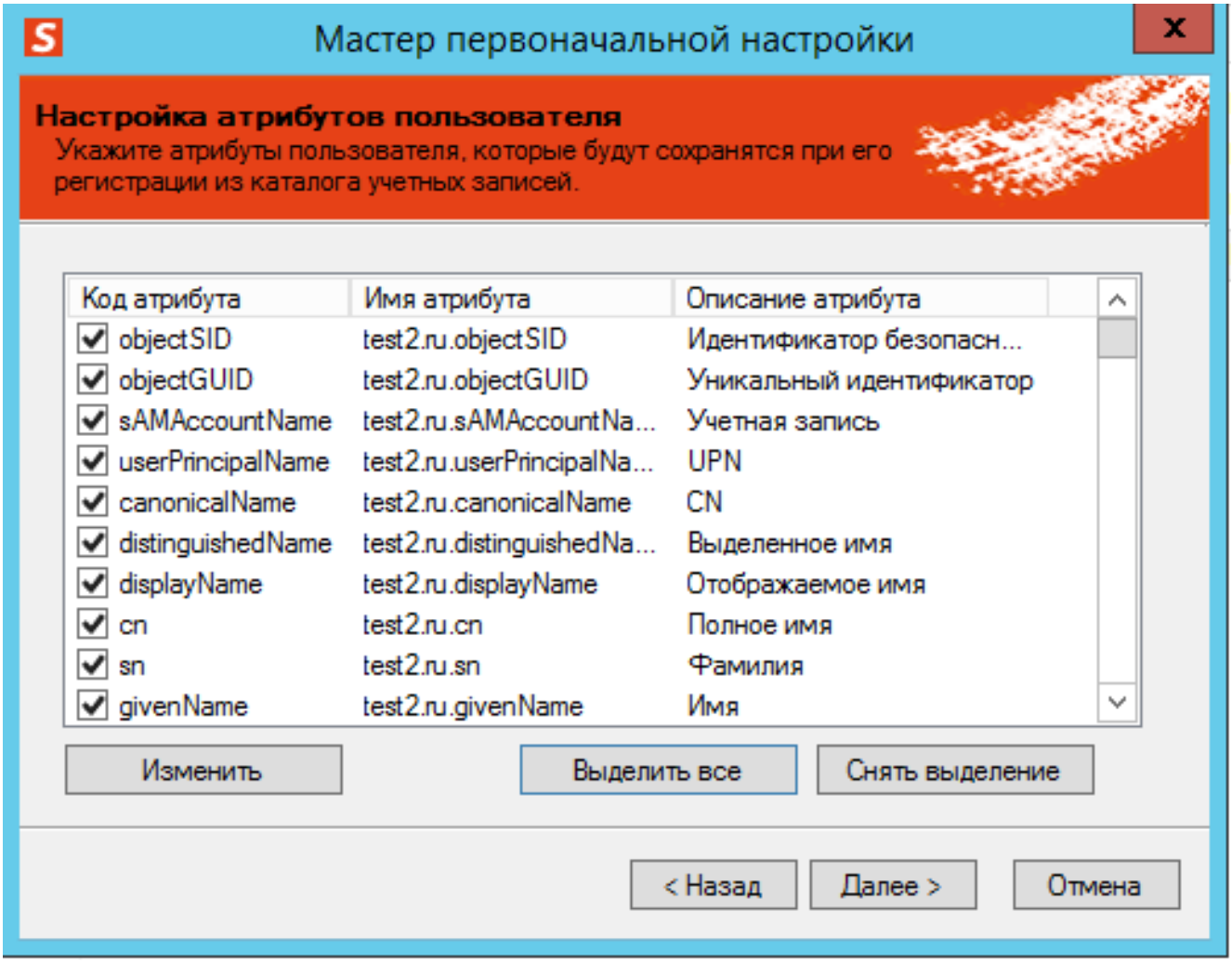


Параметры привязки — выберите свой домен:

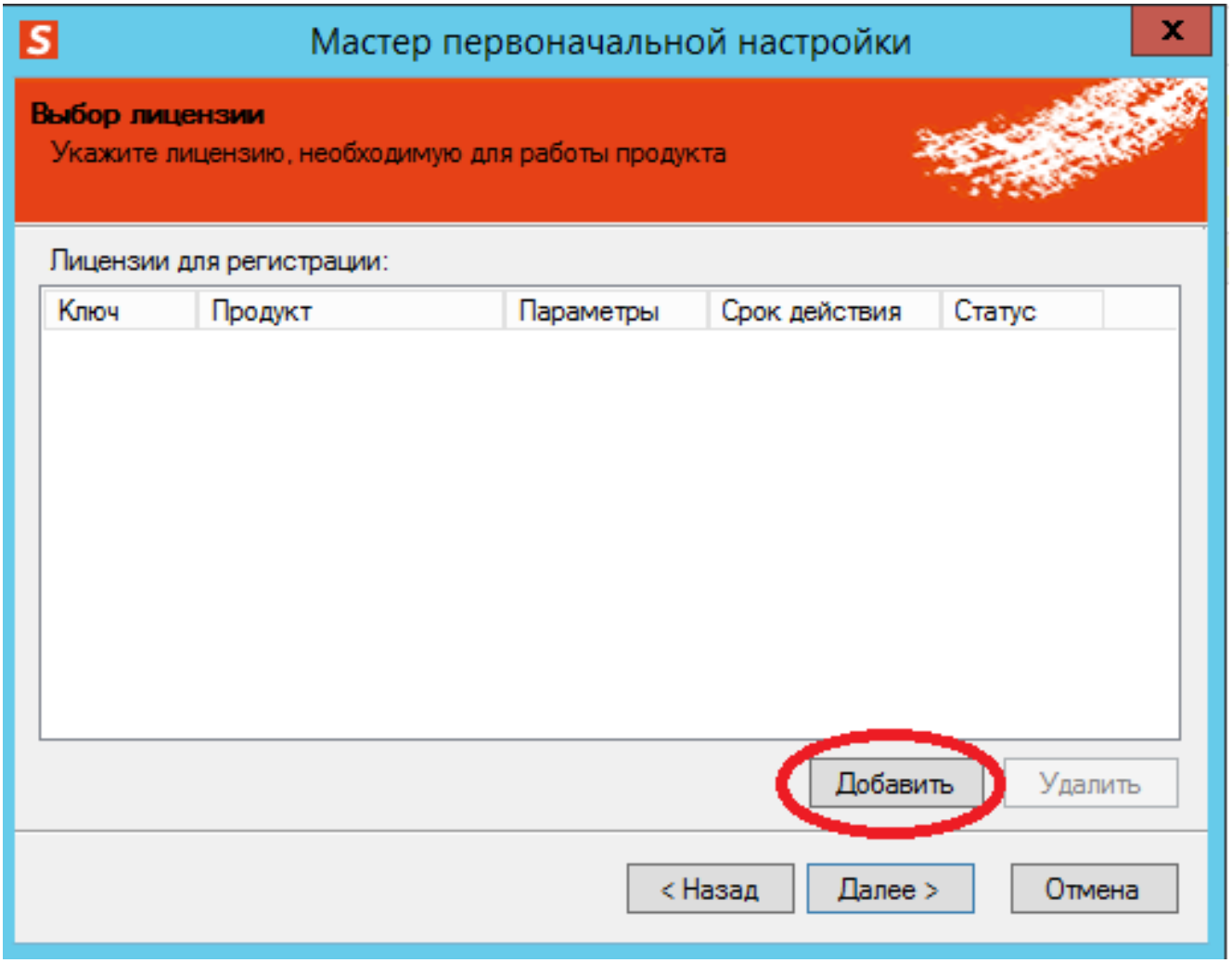


Следующий экран оставьте без изменений.

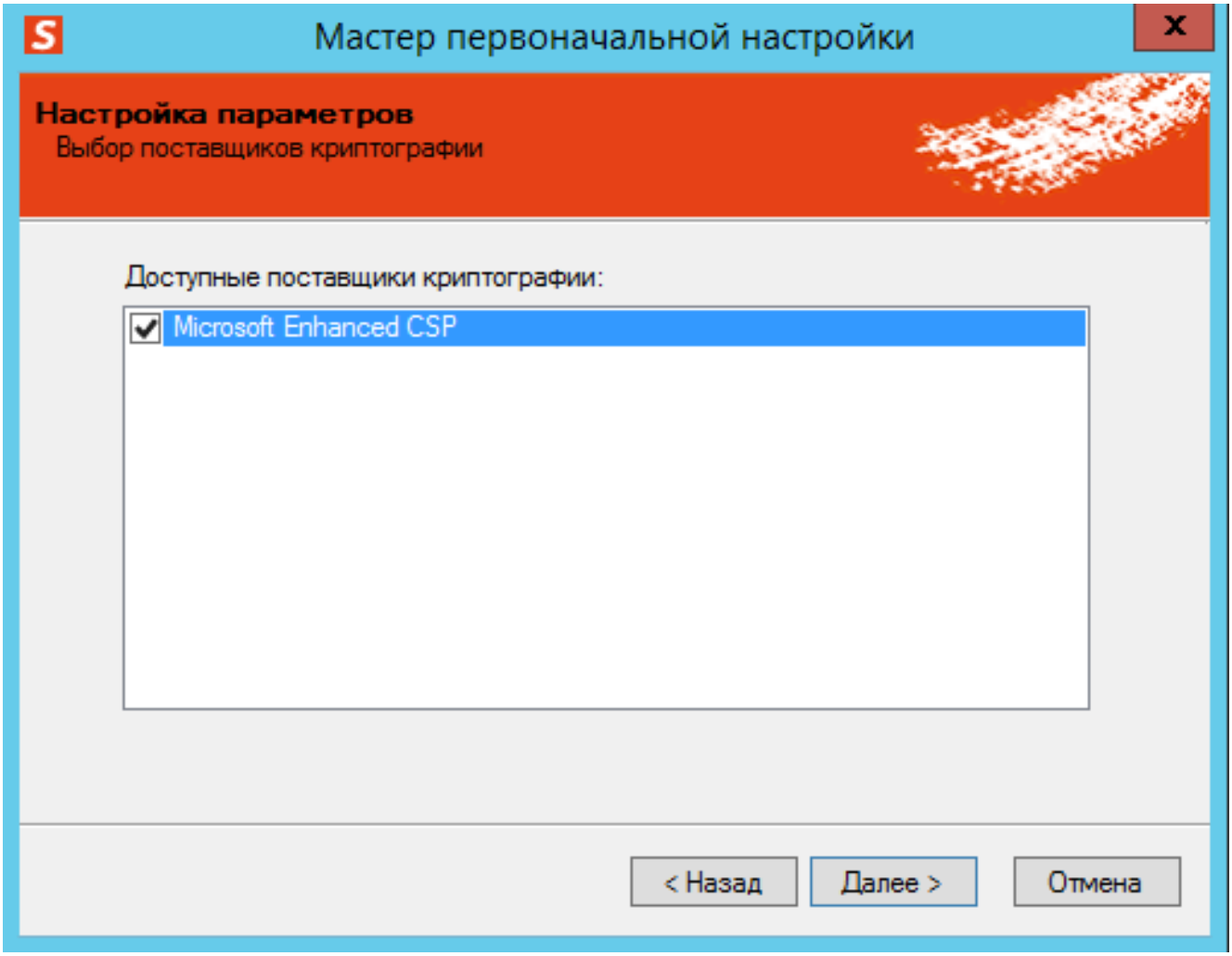
Далее выберите атрибуты пользователя. Если сомневаетесь, выберите все:



Добавьте вашу лицензию JMS:

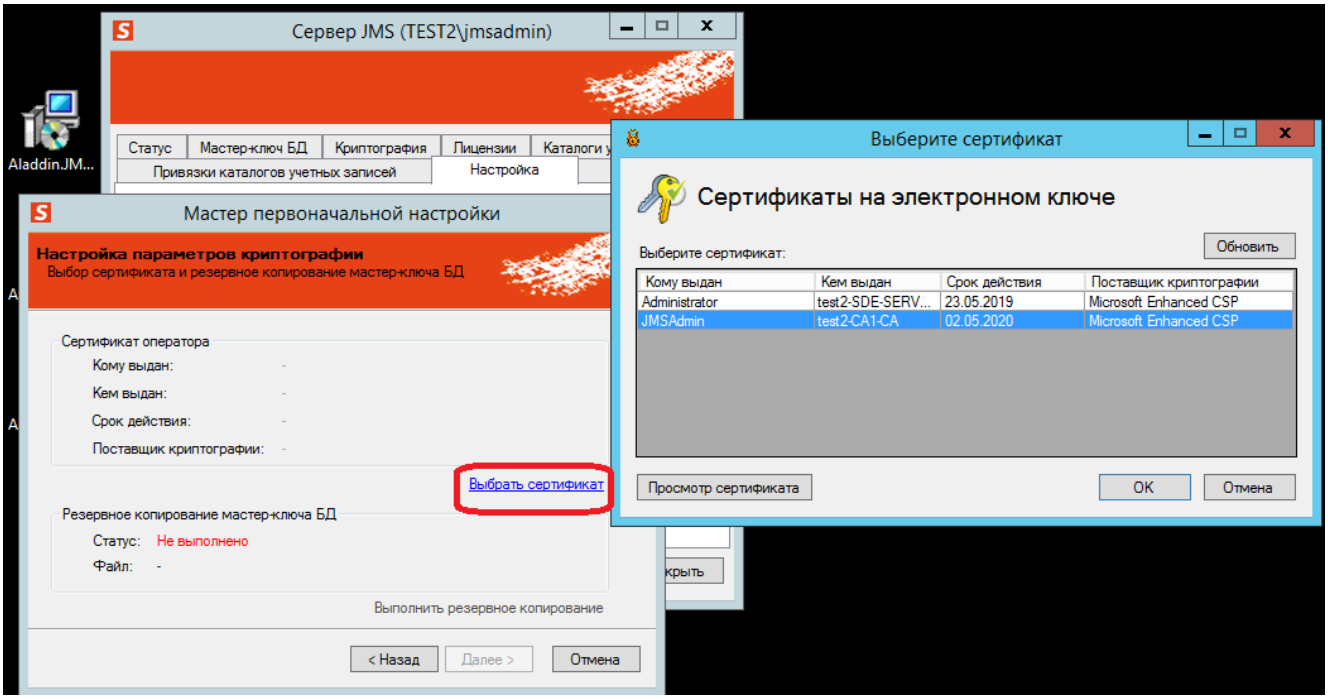


Выберите поставщика криптографии:

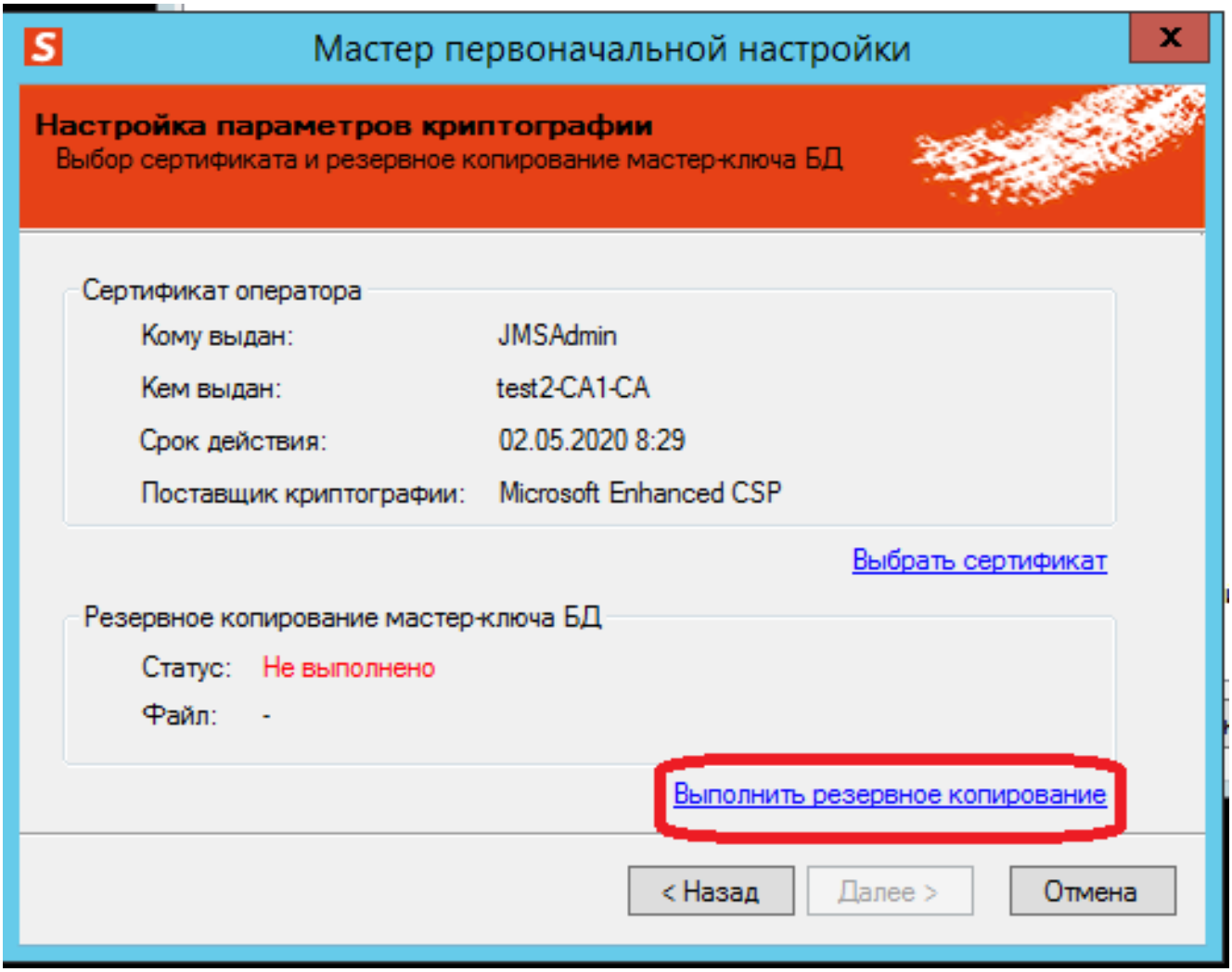


В следующем экране ничего не менять.

Выбрать сертификат оператора. Указать сертификат на токене, шаблон для которого подготовили в п.1.1.

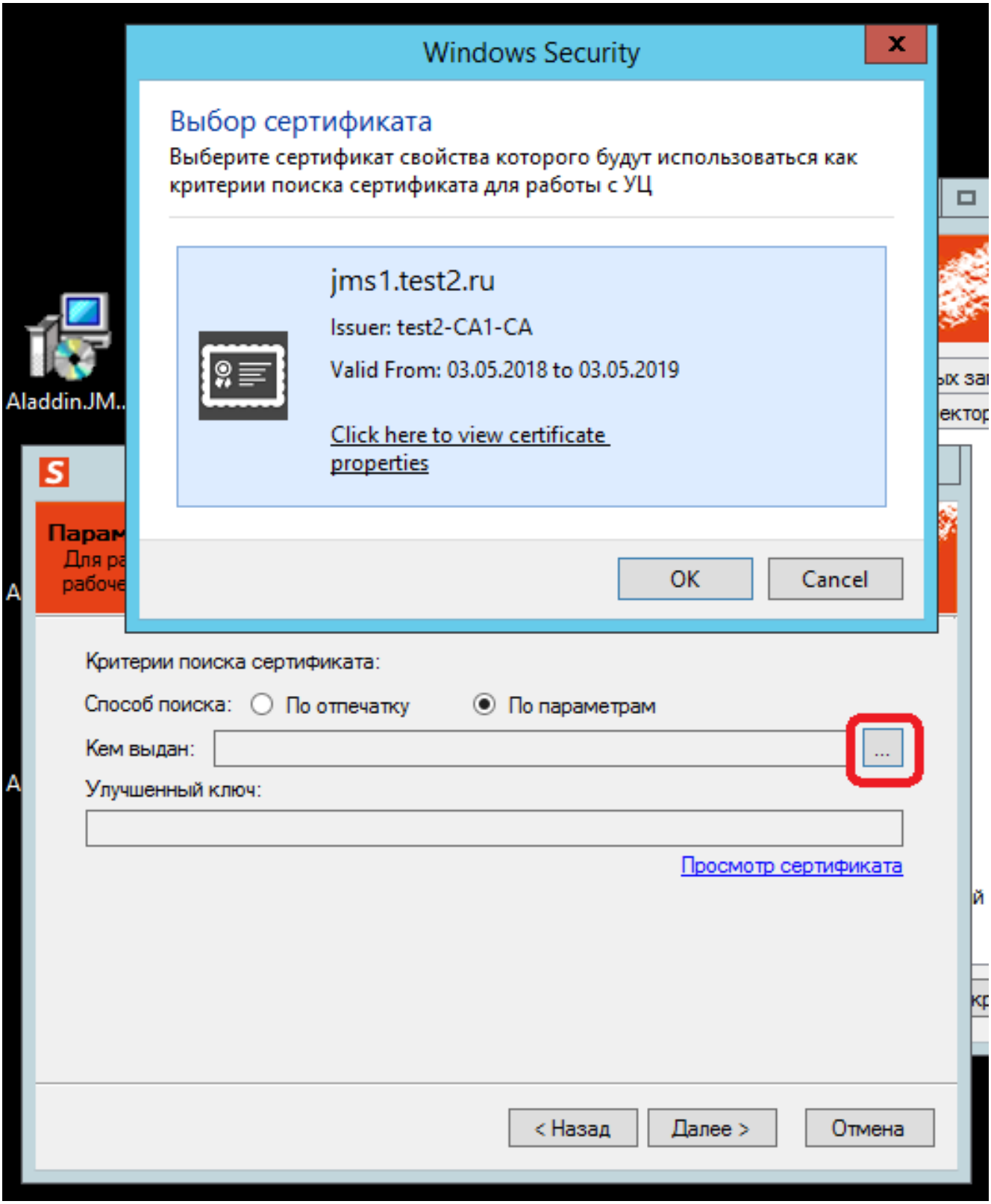


Выполните резервное копирование ключа шифрования:

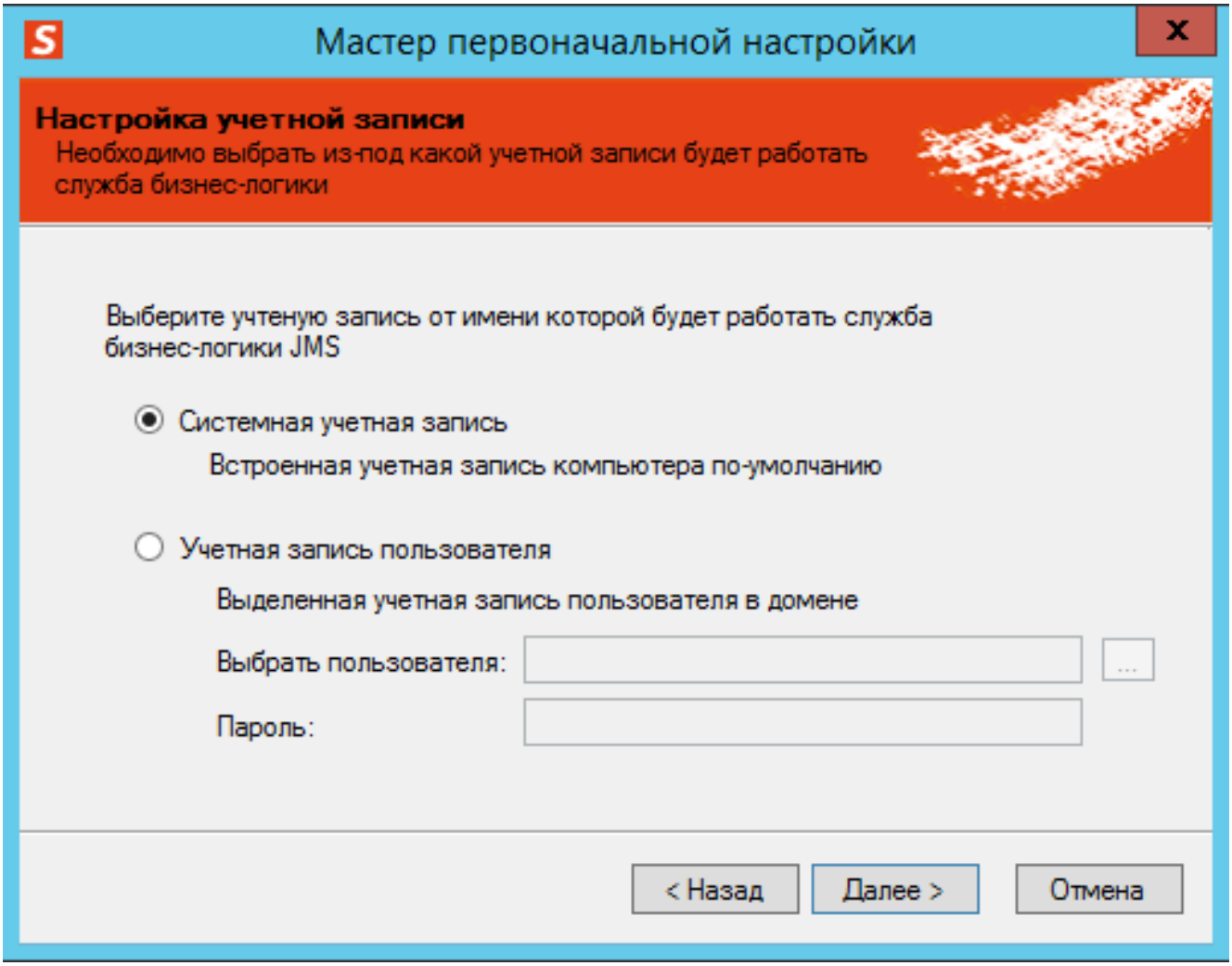


После этого будет доступна кнопка "Далее".

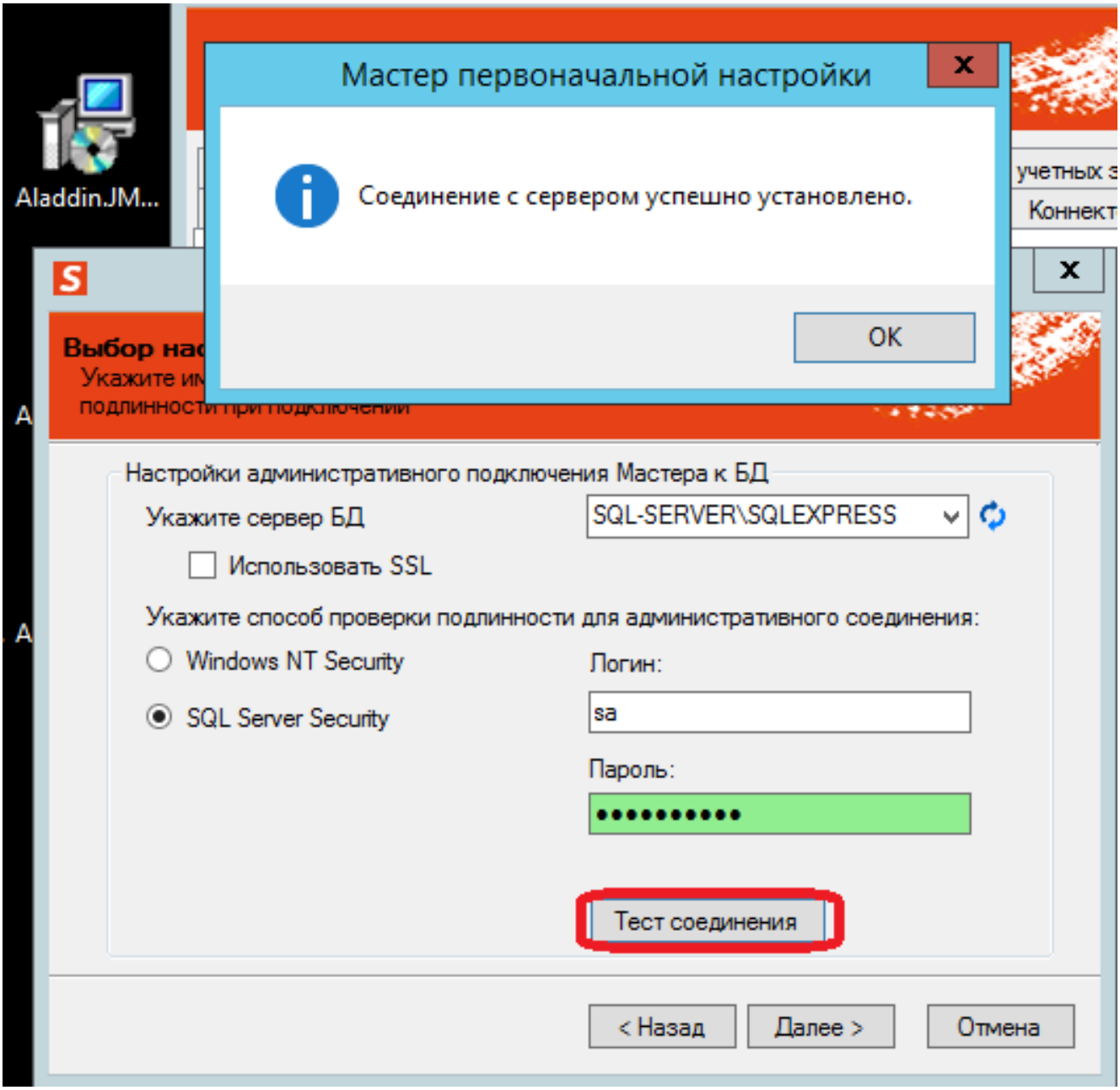
Укажите сертификат для аутентификации сервера, выпущенный согласно п.3.1.



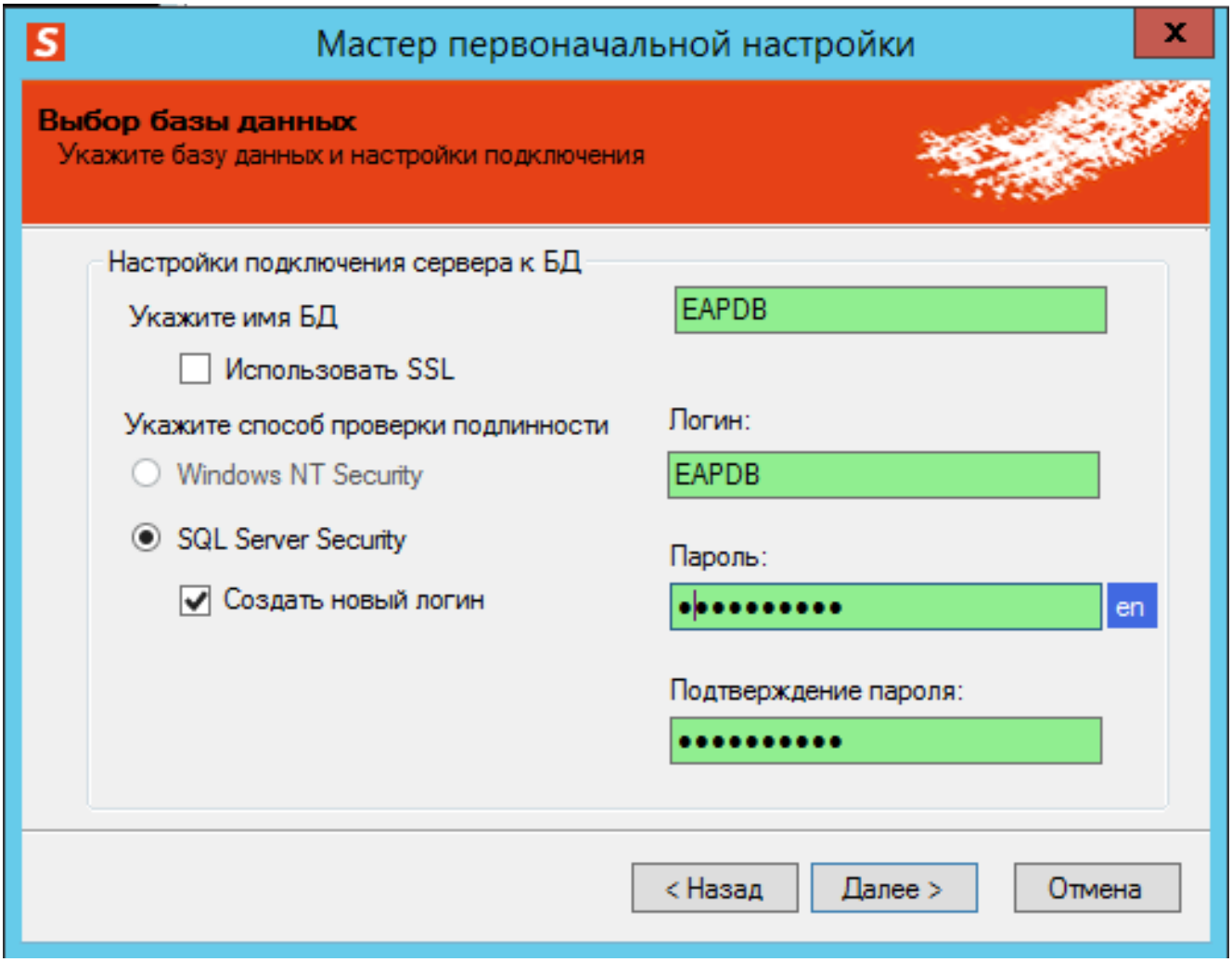
Укажите учётную запись службы, оставив "Системную учётную запись":



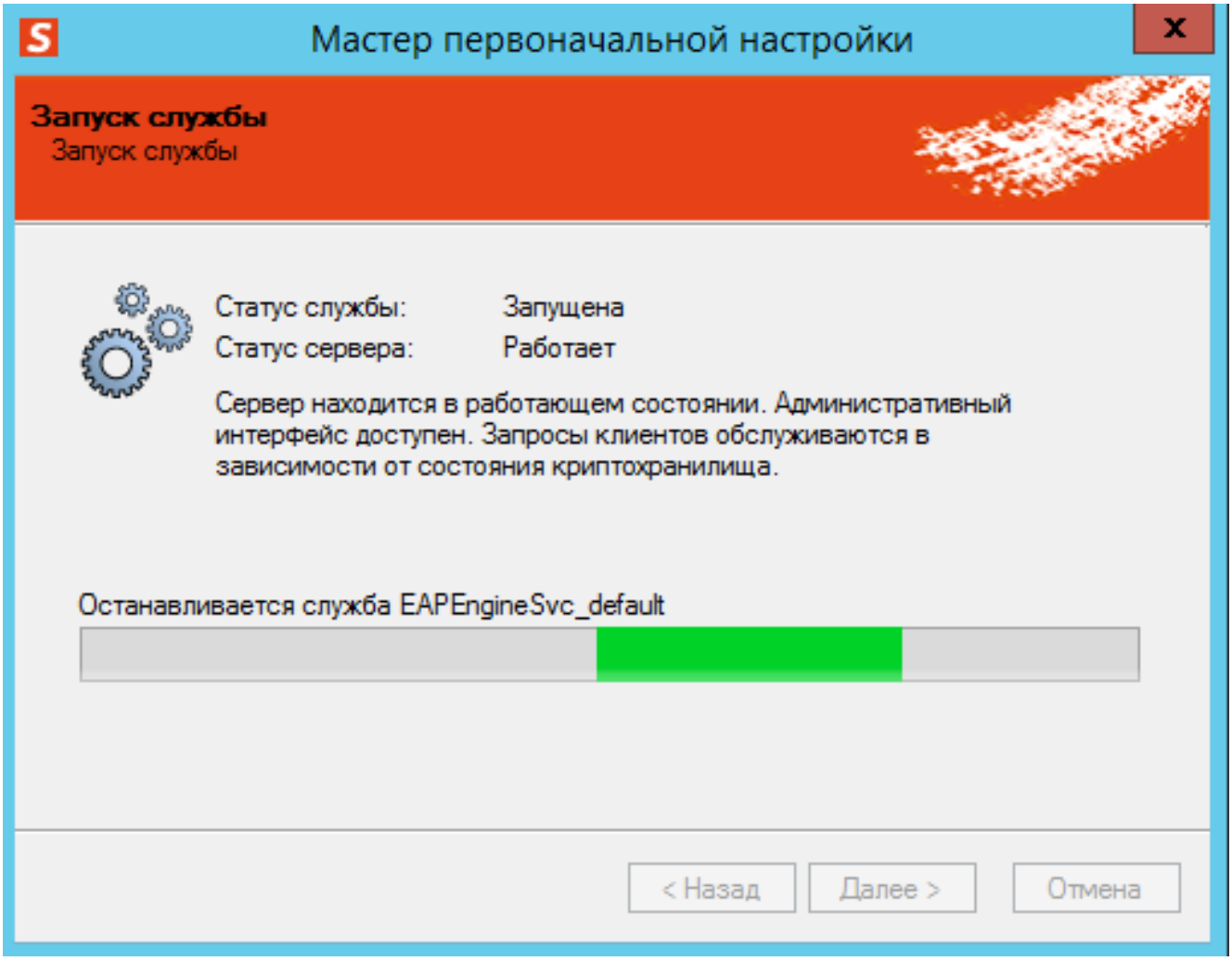
Укажите сервер БД и учётные данные для него. Нажмите "Тест соединения", убедитесь, что соединение успешно:



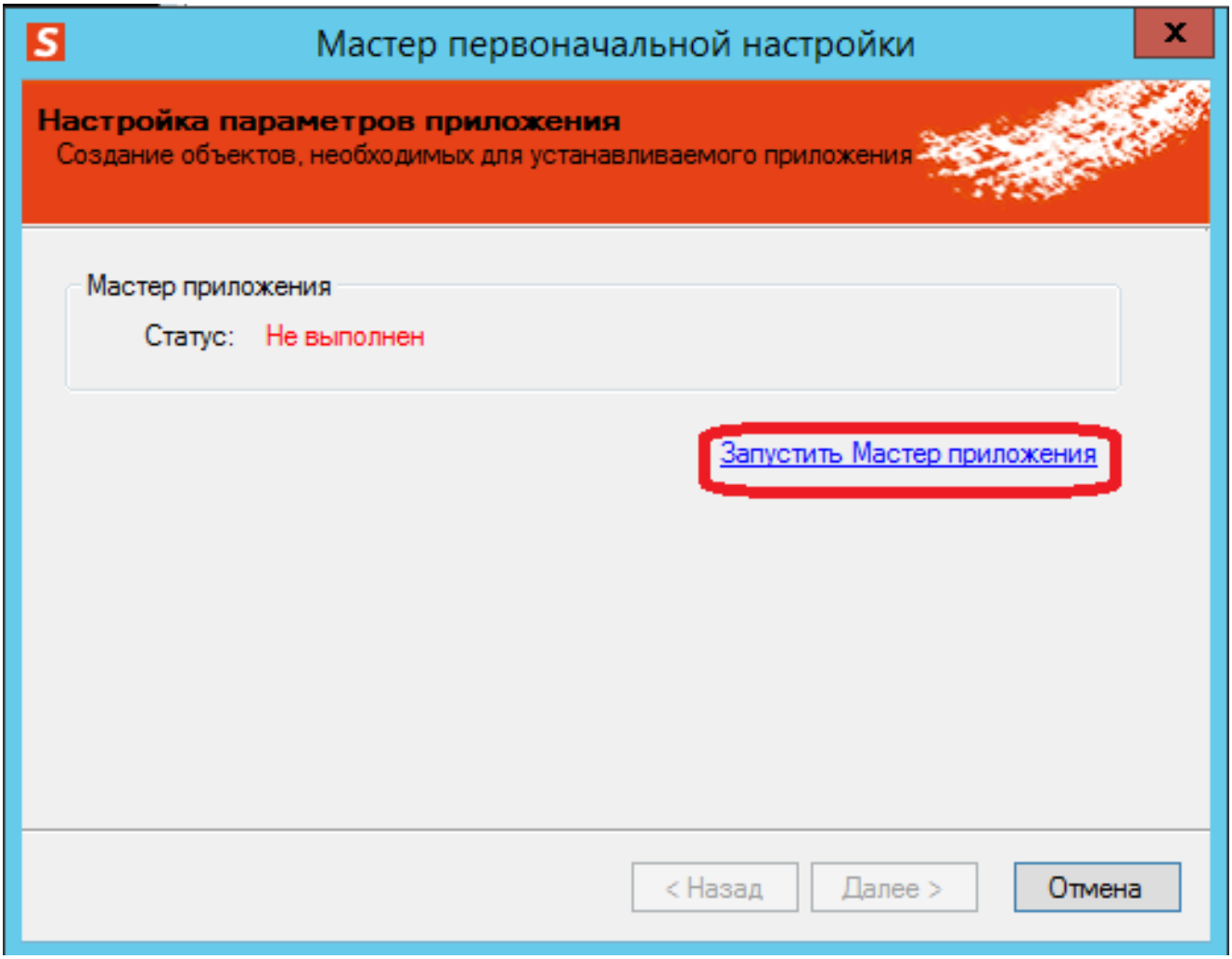
Укажите имя БД и учётные данные при необходимости:



Дождитесь запуска службы:



Запустите мастер приложения и дождитесь его завершения:



Далее будет предложено смонтировать криптохранилище и работа мастера завершится.

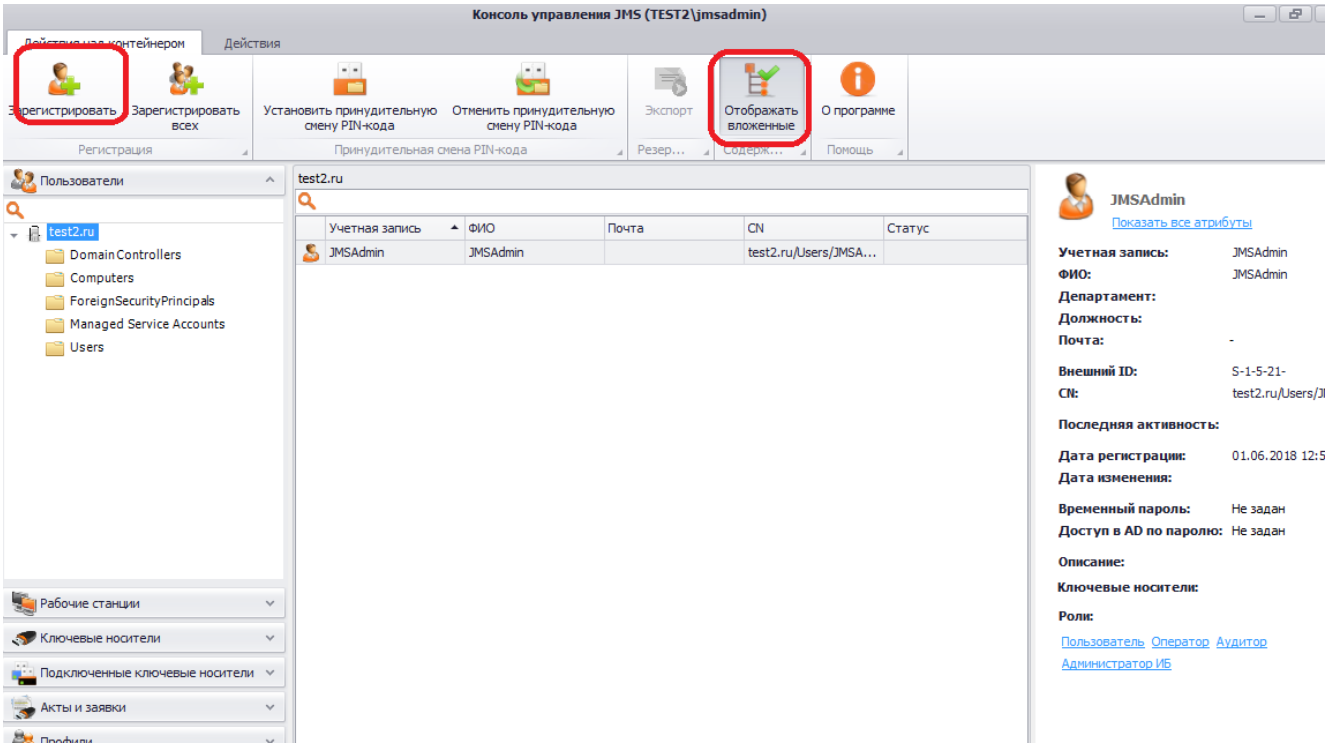
4. Настройка и выпуск сертификата в JMS.

4.1. Подготовка системы к выпуску.

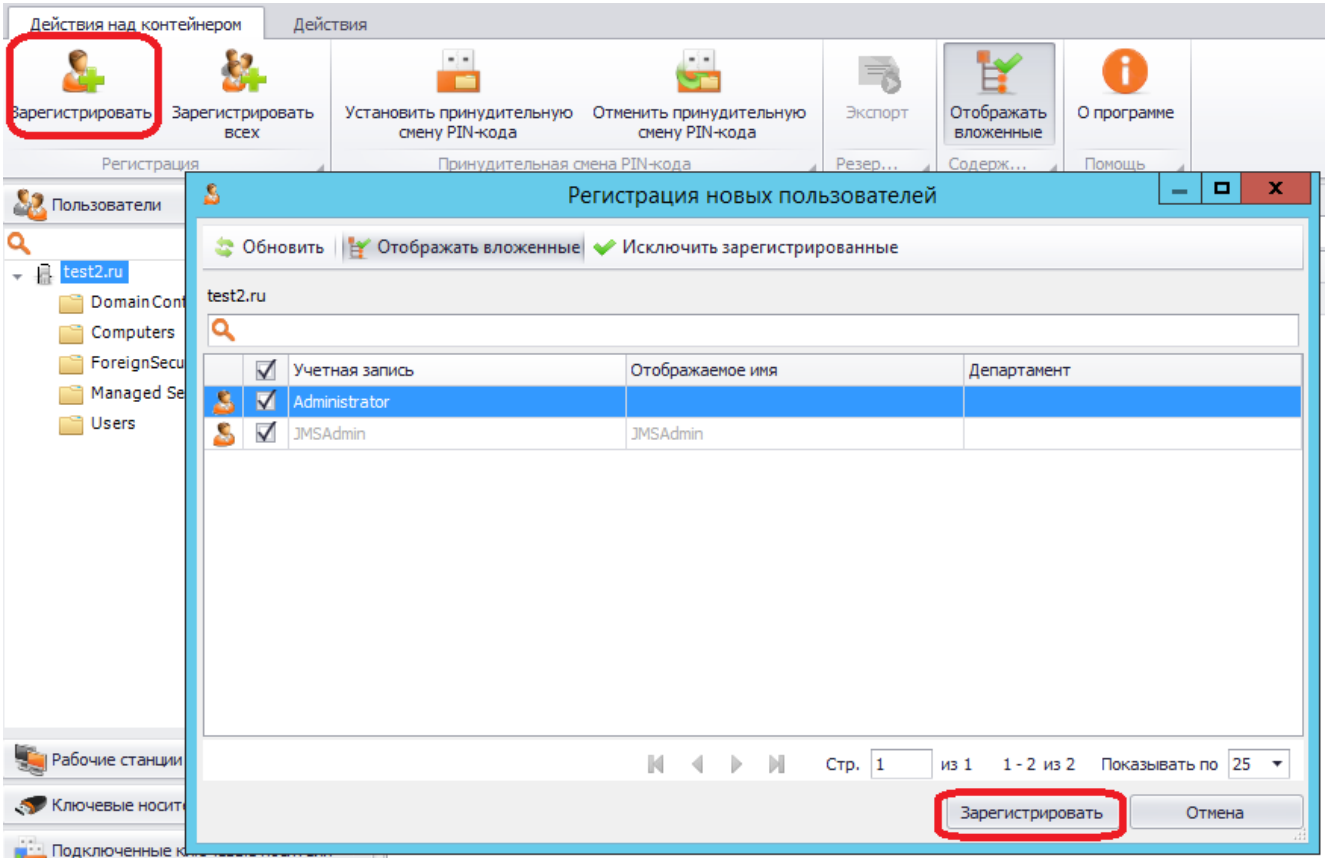
Для работы с JMS установите консоль JMS из файла вида Aladdin.JMS.Admin-*.msi

Запустите консоль управления JMS.

Перейдите на вкладку (в левой части окна) "Пользователи". Сверху перейдите на вкладку "Действия над контейнером", включите вид "Отображать вложенные". Нажмите кнопку "Зарегистрировать".

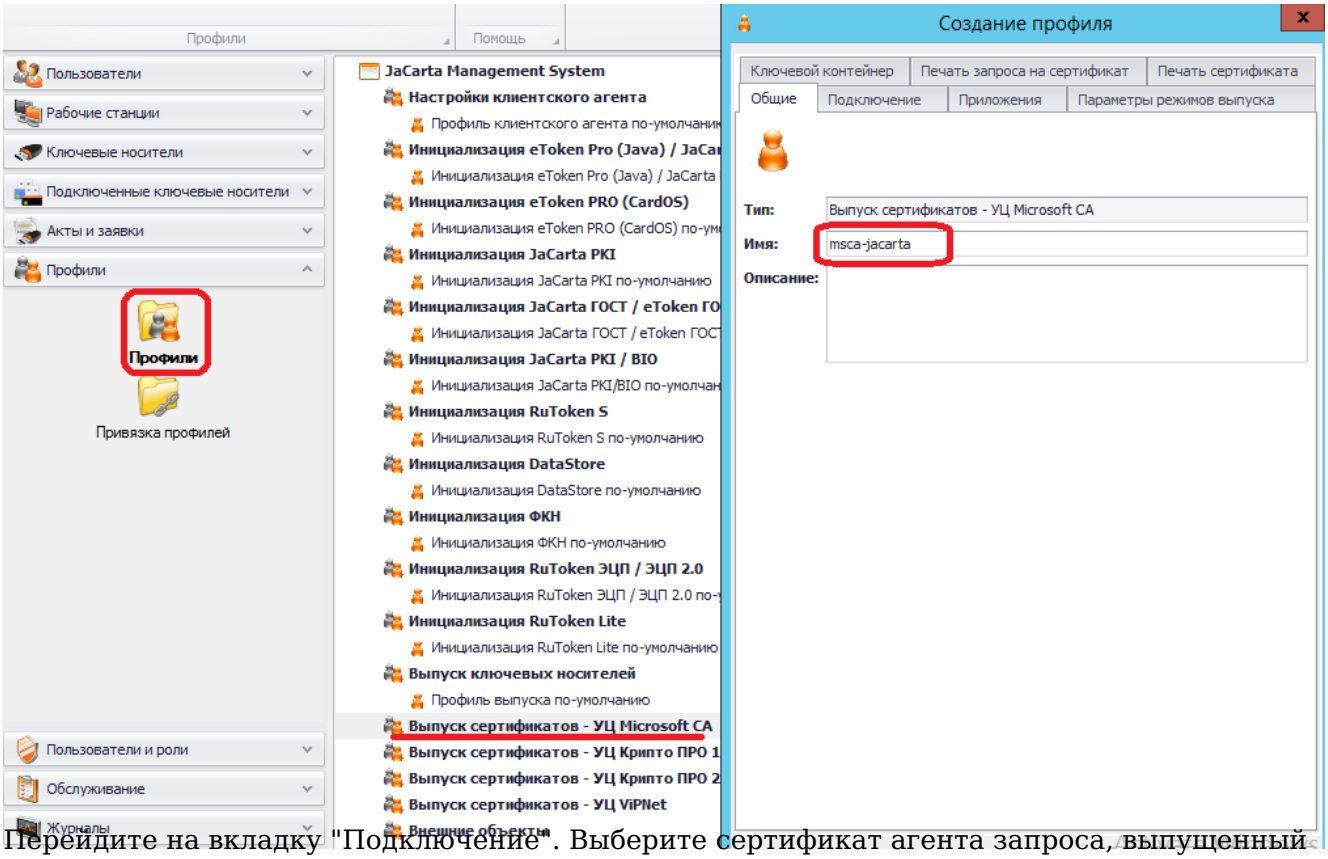


В появившемся окне отметьте необходимых пользователей и нажмите «Зарегистрировать»:

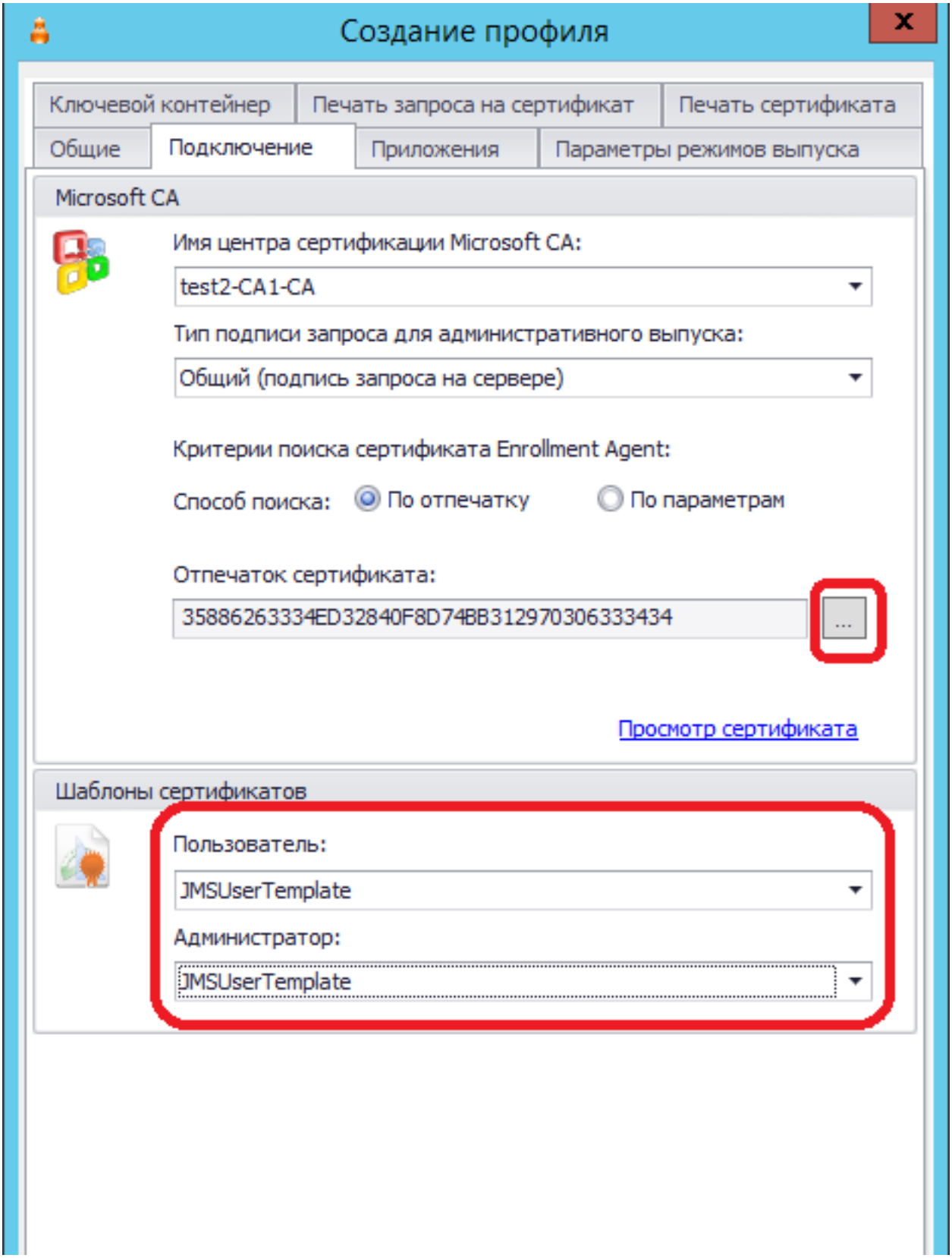


Эти пользователи будут отображаться в основном окне.

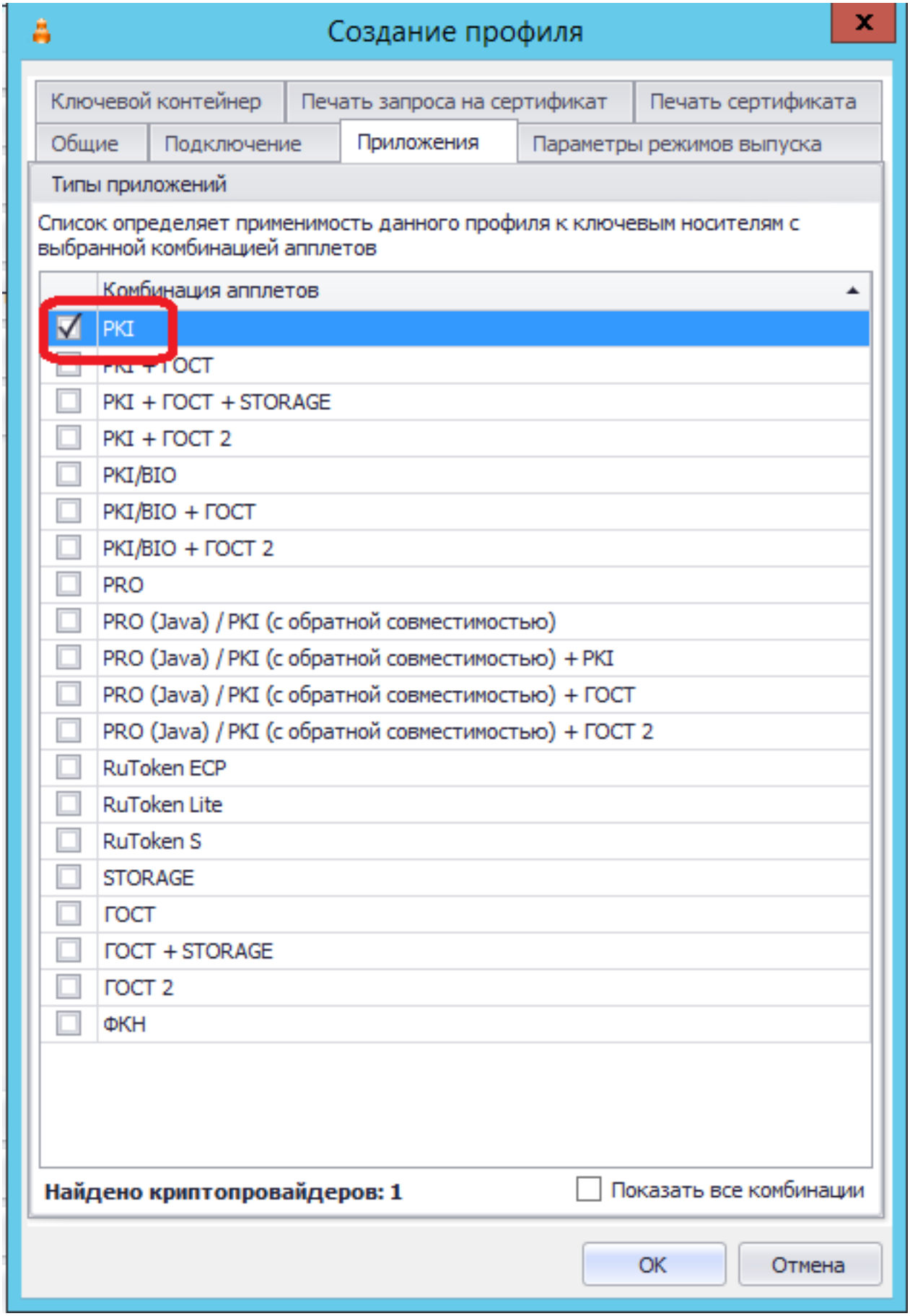
Перейдите на вкладку "Профили", выберите пункт "Профили". Установите указатель на "Выпуск сертификатов — УЦ Microsoft CA". На верхней панели нажмите "Создать". Откроется окно нового профиля. Введите имя профиля.



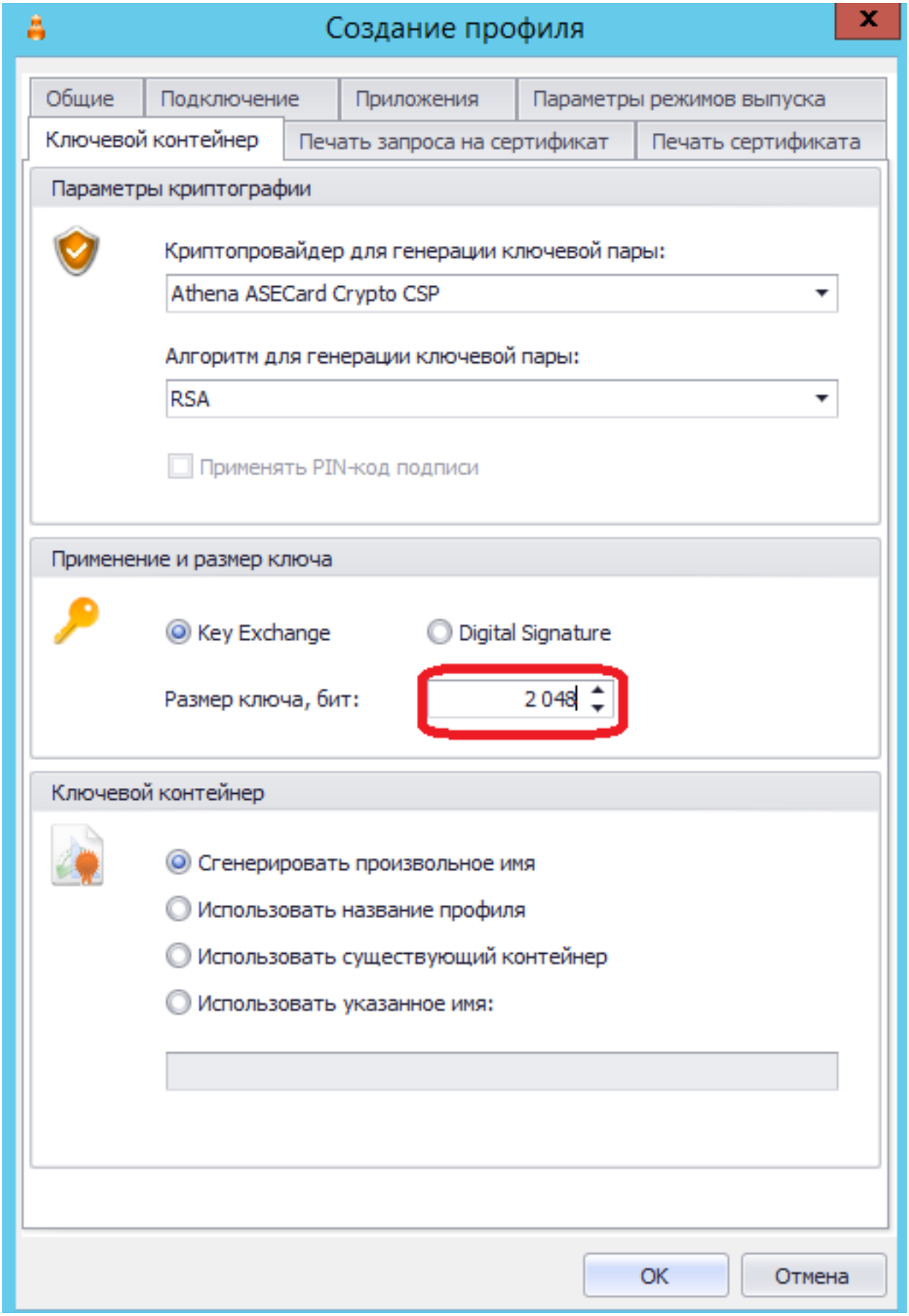
Перейдите на вкладку "Подключение". Выберите сертификат агента запроса, выпущенный согласно п.3.2. В обоих полях шаблонов сертификатов укажите шаблон, созданный согласно п.1.2.



Перейдите на вкладку "Приложения". Отметьте апплет PKI.

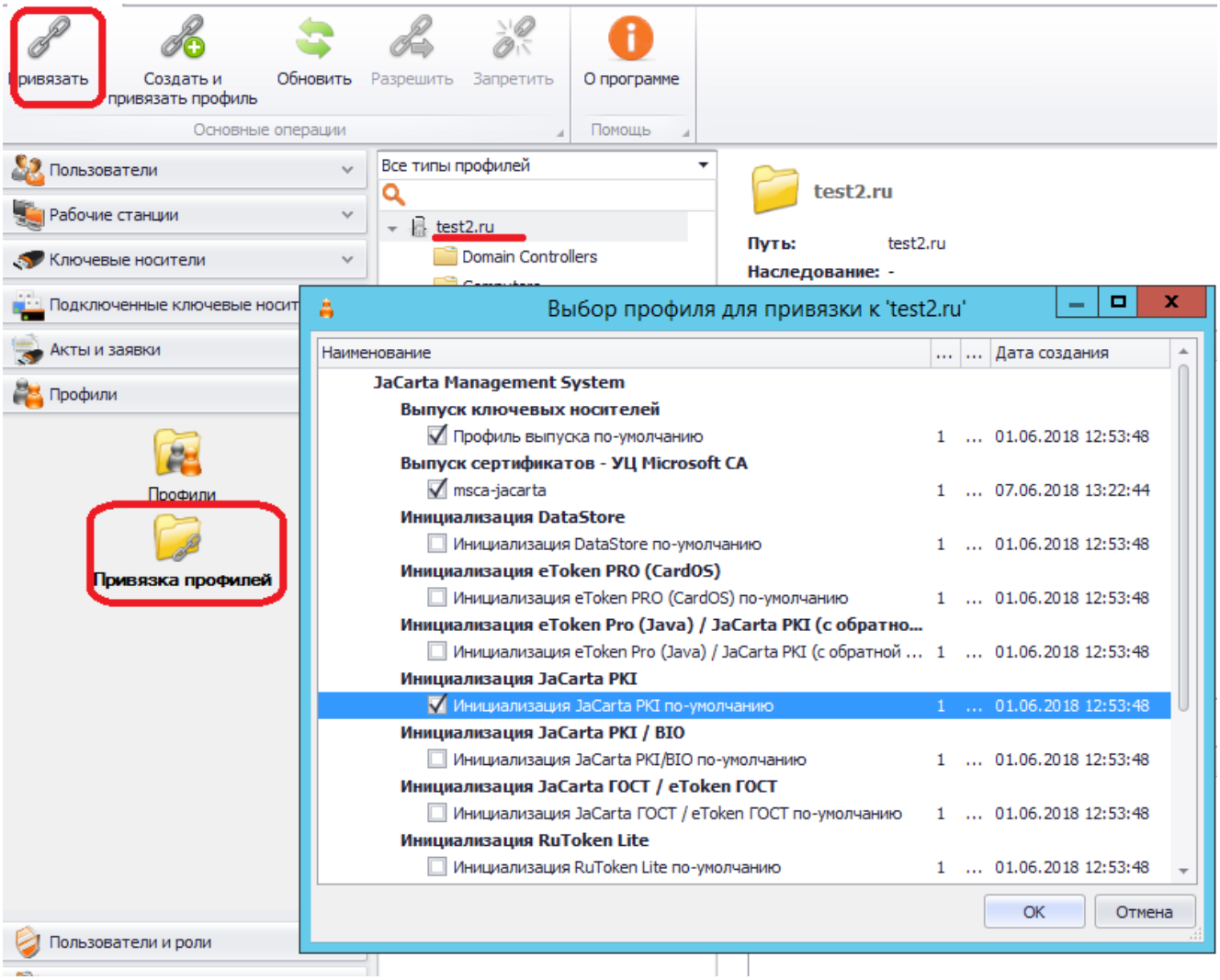


Перейдите на вкладку "Ключевой контейнер". При необходимости измените размер ключа. Он должен совпадать с размером в шаблоне согласно п.1.2.



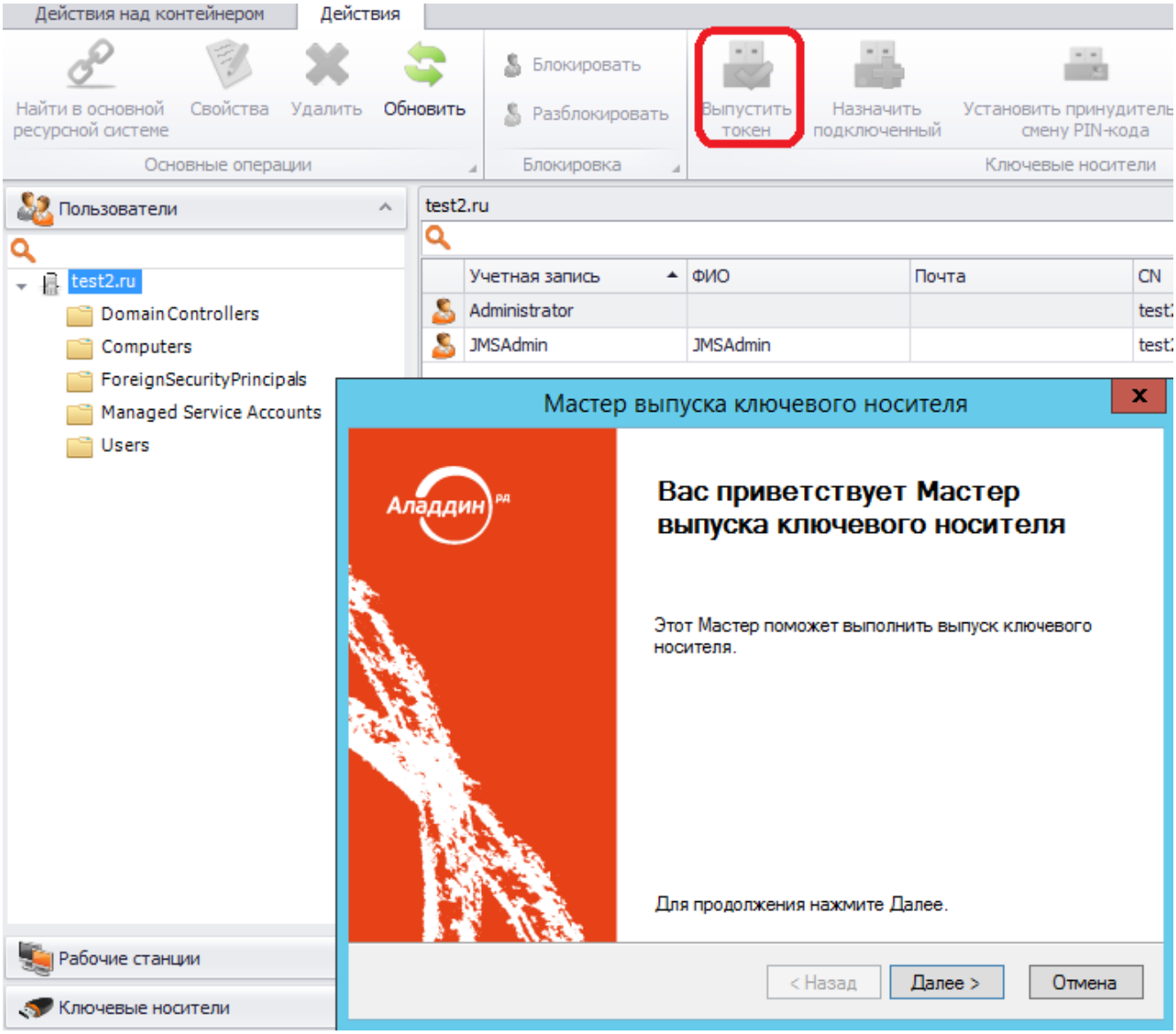
Нажмите "OK".

Перейдите к пункту "Привязка профилей". Выберите нужный контейнер в AD и нажмите "Привязать". Откроется окно профилей. Выберите профиль выпуска сертификатов, профиль выпуска по умолчанию, профиль инициализации и нажмите OK.

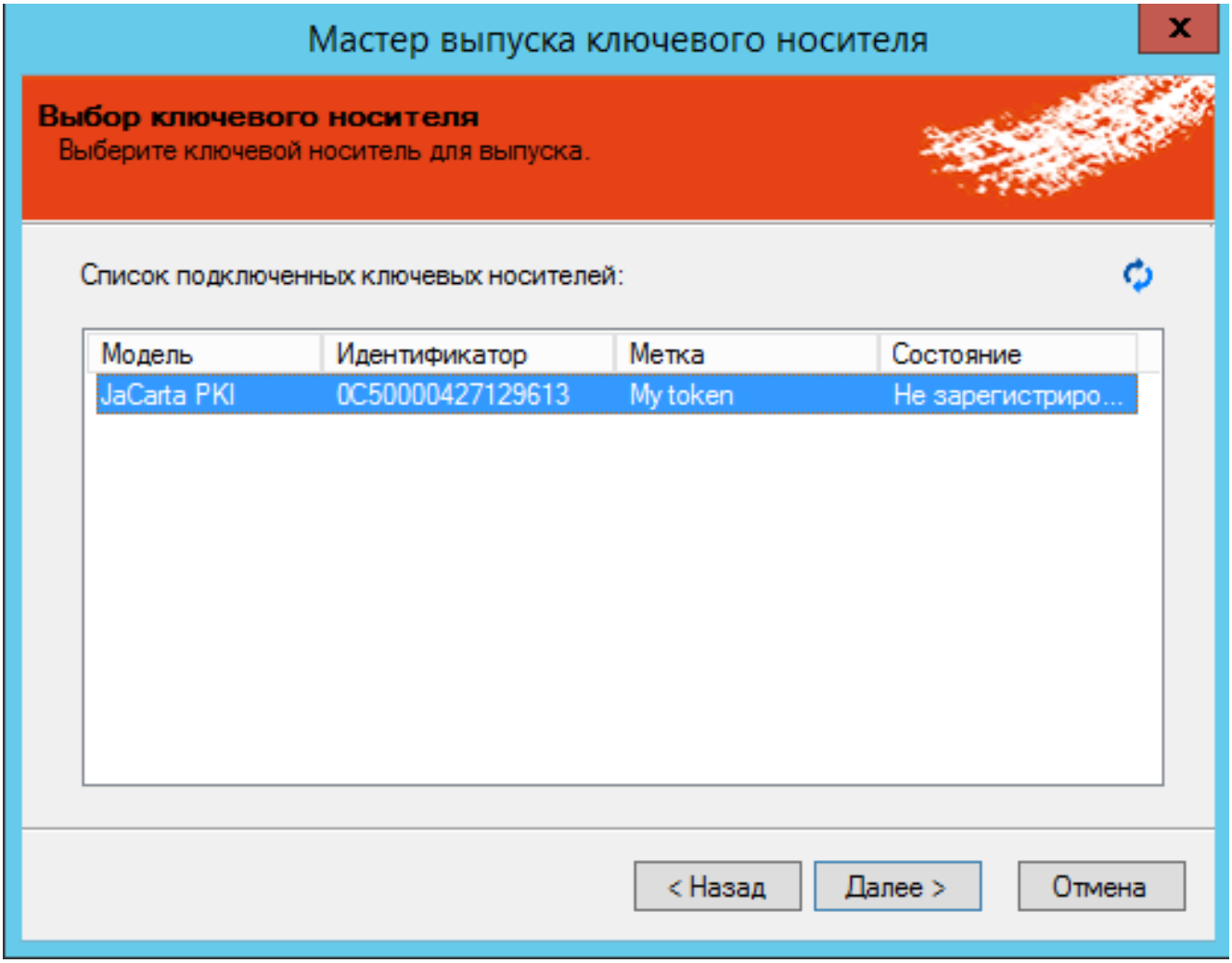


4.2. Выпуск сертификата на токен.

Перейдите в раздел **Пользователи**. Подключите чистый токен, который будем привязывать и выпускать для этого пользователя. Найдите нужного пользователя, кликните на него. В верхней панели нажмите кнопку "Выпустить токен". Откроется мастер выпуска:

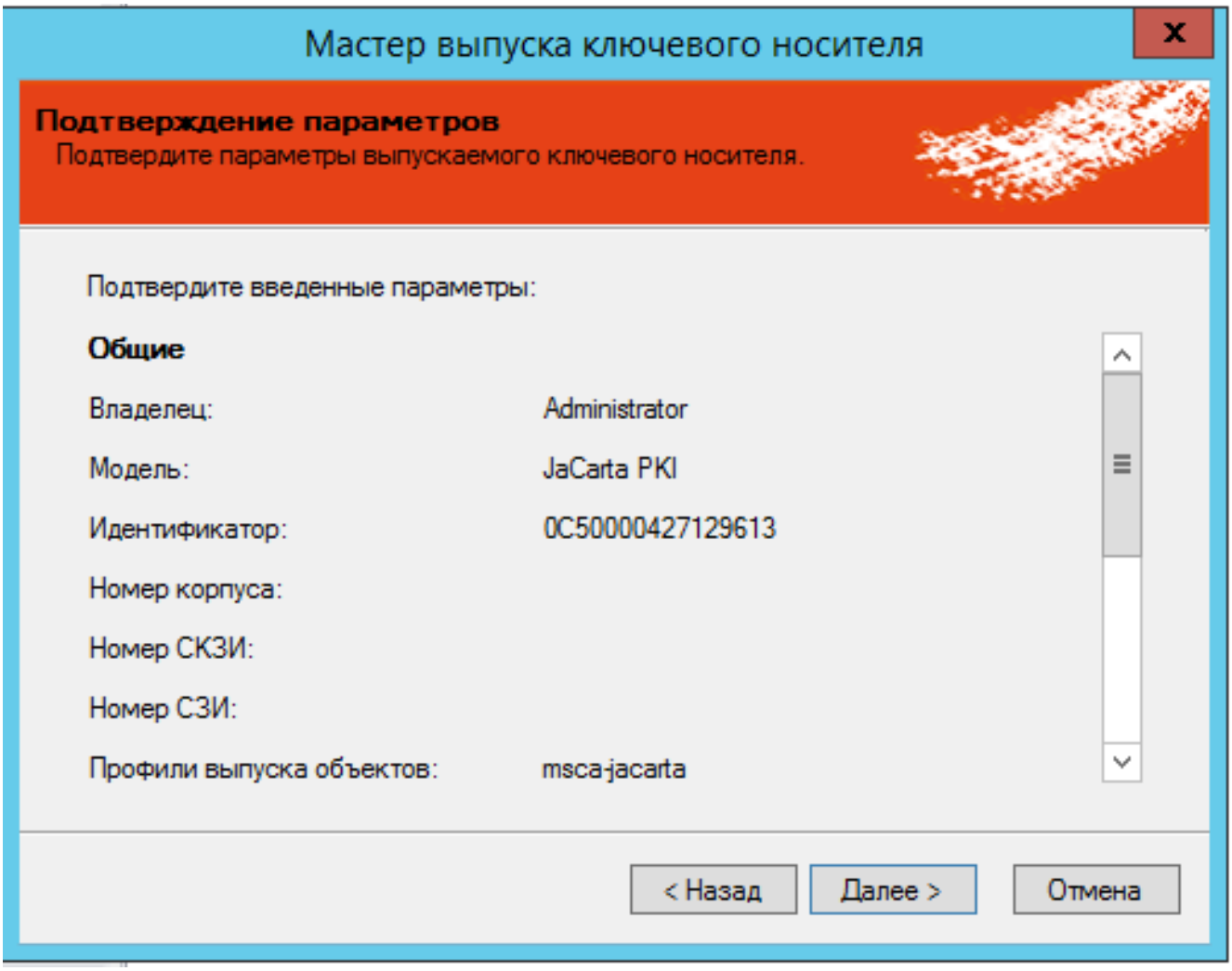


На следующем этапе дождитесь, когда отобразится ваш токен. Кликните на него и нажмите "Далее".

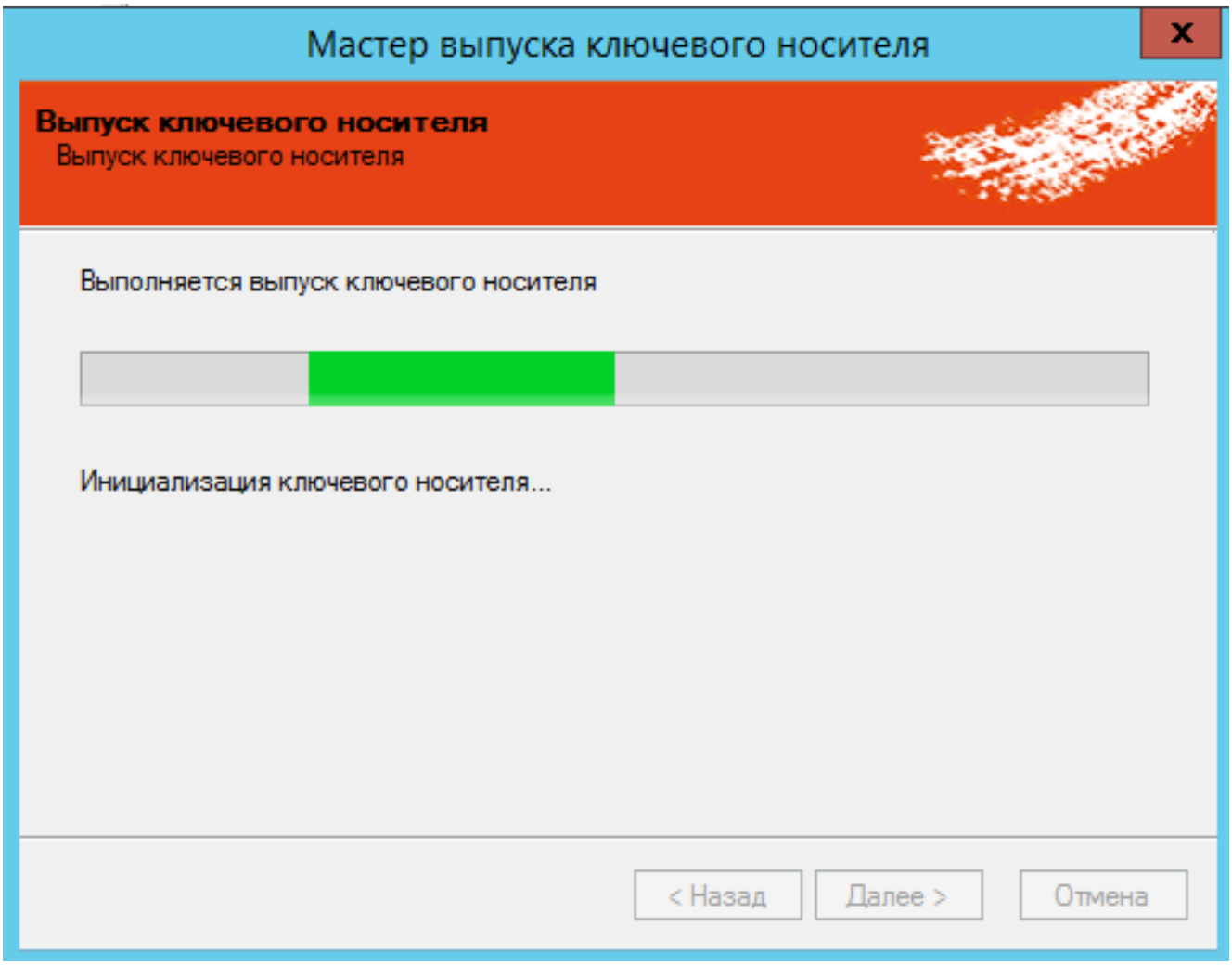


Следующие 4 экрана оставьте без изменений.

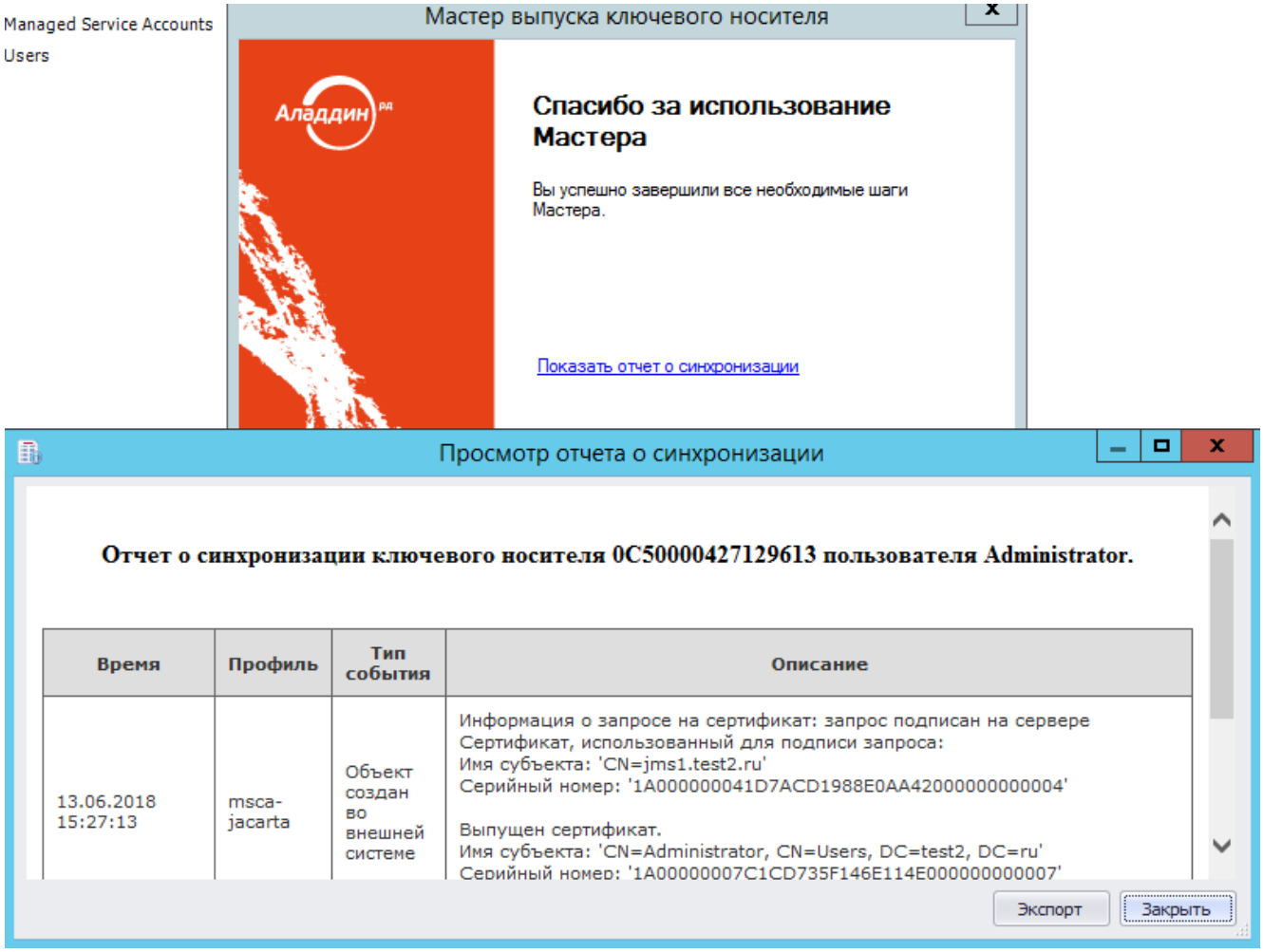
Далее отобразятся параметры предполагаемого выпуска токена.



Далее начнется процесс выпуска токена:



В последнем окне вы увидите ссылку на окно отчёта о выпуске. Если она синего цвета, значит процесс прошёл успешно. Если ссылка красного цвета, значит имели место ошибки.



ID статьи: 285

Последнее обновление: 09 Jul, 2018

Ревизия: 1

JaCarta Management System -> JMS. Типовой сценарий развертывания (MSCA)

https://kbp-6.aladdin-rd.ru/index.php?View=entry&EntryID=285