



Создание сертификатов

РУСТЭК.VDI 4.0.4

Содержание

1	Требования.....	3
2	Создание шаблона	4
3	Выпуск сертификата.....	12
4	Загрузка сертификата в инсталлятор	23

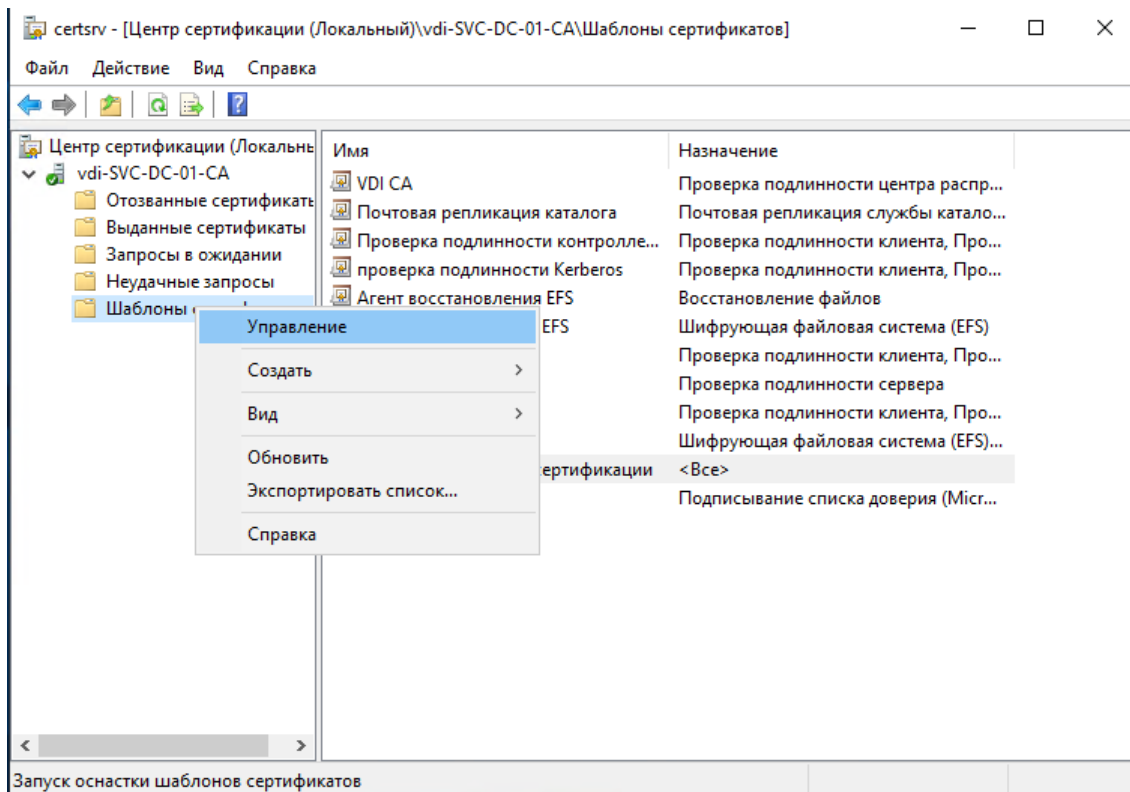
1 Требования

Убедитесь, что у вас установлены:

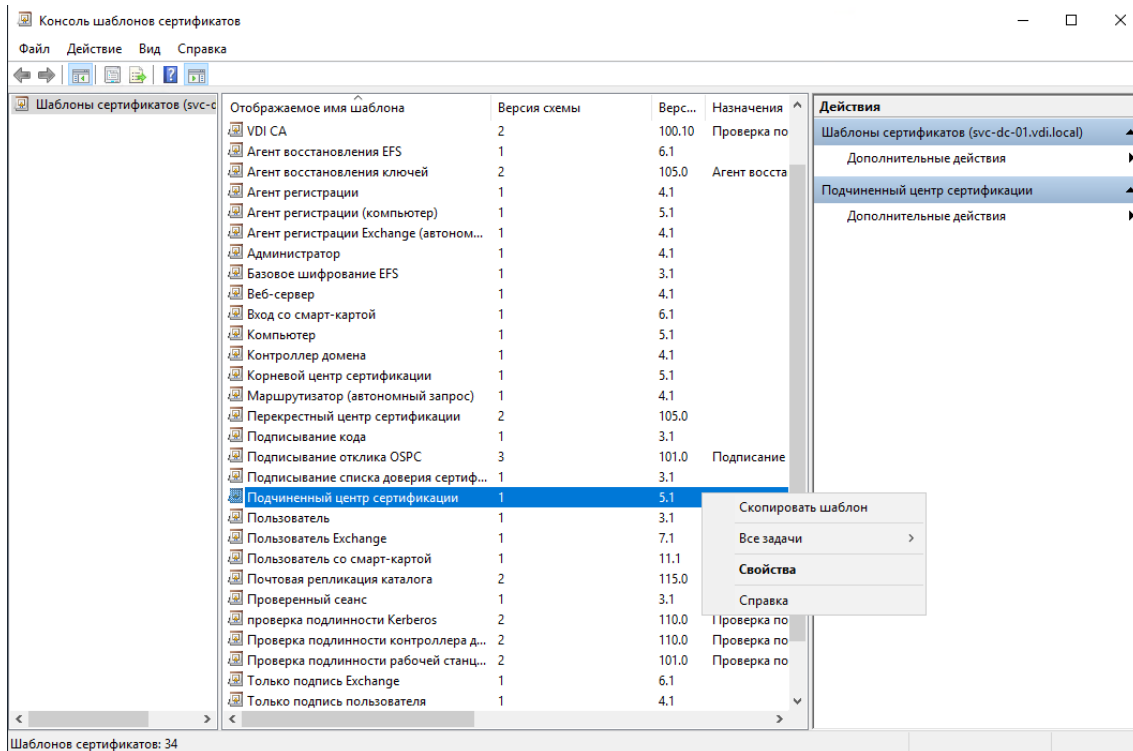
1. Active Directory (AD).
2. Active Directory Certificate Authority (AD CA).

2 Создание шаблона

1. Откройте приложение **Центр сертификации**.
2. В открывшемся окне **Центр сертификации** выберите ваш сервер с AD, раскройте его и перейдите к разделу **Шаблоны сертификатов**.



3. Щелкните правой кнопкой мыши по разделу **Шаблоны сертификатов** выберите «**Управление**».
4. В открывшемся окне **Консоль шаблонов сертификатов** найдите **Подчиненный центр сертификации** и выберите **Скопировать шаблон**.



5. Перейдите на вкладку **Общие** в открывшемся окне свойств нового шаблона. Задайте отображаемое имя, например, **VDI CA**.

Убедитесь, что в разделе **Общие** выбран пункт **Опубликовать сертификат в Active Directory**.

Свойства нового шаблона

Устаревшие шаблоны	Расширения	Безопасность
Совместимость	Общие	Требования выдачи

Отображаемое имя шаблона:
VDICA

Имя шаблона:
VDICA

Период действия: 5 г.
Период обновления: 6 нед.

Опубликовать сертификат в Active Directory:
 Не использовать автоматическую перезагрузку, если такой сертификат уже существует в Active Directory

OK Отмена Применить Справка

6. В том же окне свойств нового шаблона открываем вкладку **Расширение**.

Свойства нового шаблона

Устаревшие шаблоны	Расширения	Безопасность
Совместимость	Общие	Требования выдачи

Чтобы изменить расширение, выделите его и нажмите кнопку "Изменить".

Расширения, включенные в этот шаблон:

- Использование ключа
- Основные ограничения
- Политики выдачи
- Политики применения
- Сведения о шаблоне сертификата

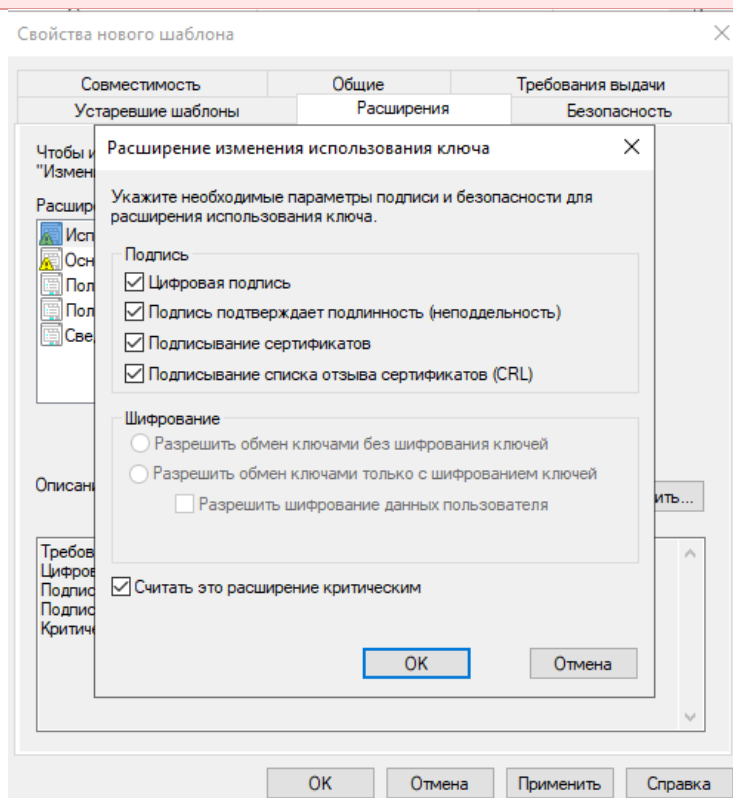
Описание Использование ключа: Изменить...

Требования к подписи:
 Цифровая подпись
 Подписывание сертификатов
 Подписывание списка отзыва (CRL)
 Критическое расширение.

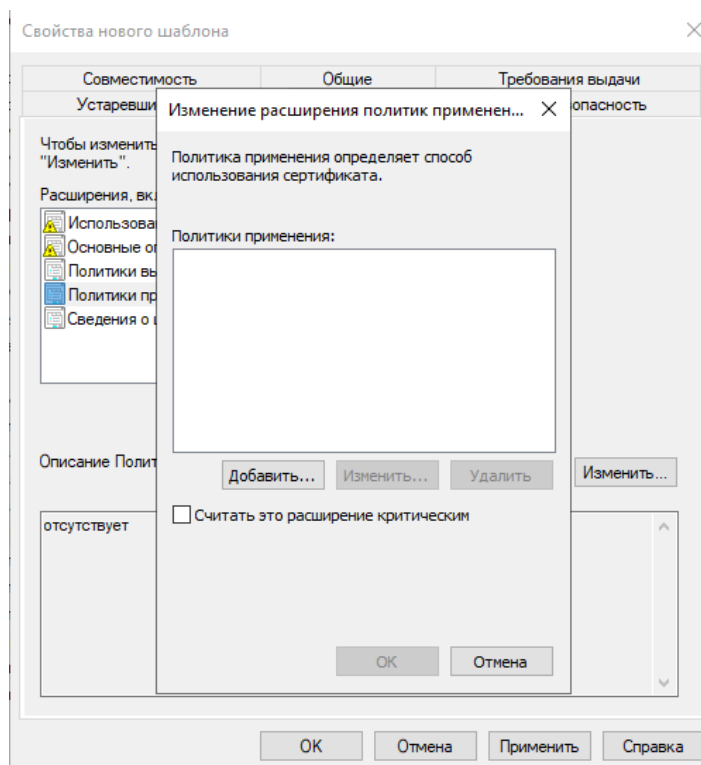
OK Отмена Применить Справка

7. В окне расширений, выберите **Использование ключа** и нажмите кнопку **Изменить**.
8. В открывшемся окне **Изменение использования ключа** установите галочку напротив **Подпись подтверждает подлинность (неподдельность)**.

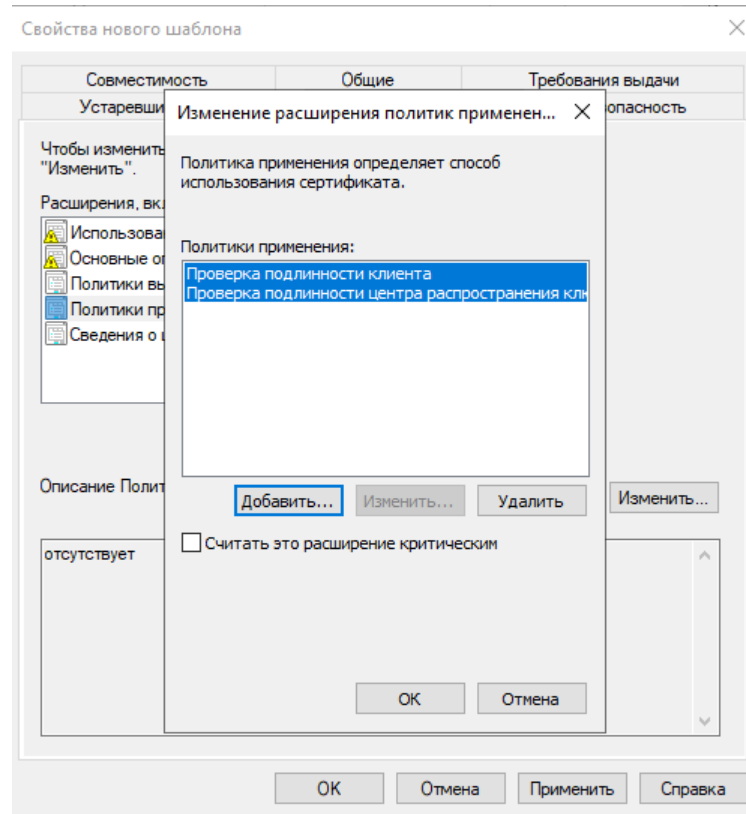
Удостоверьтесь, что выбран пункт **Считать это расширение критическим**



9. Нажмите **Ок**.
10. В окне **Свойств нового шаблона**, найдите и выберите **Политики применения**, затем нажмите кнопку **Изменить**.

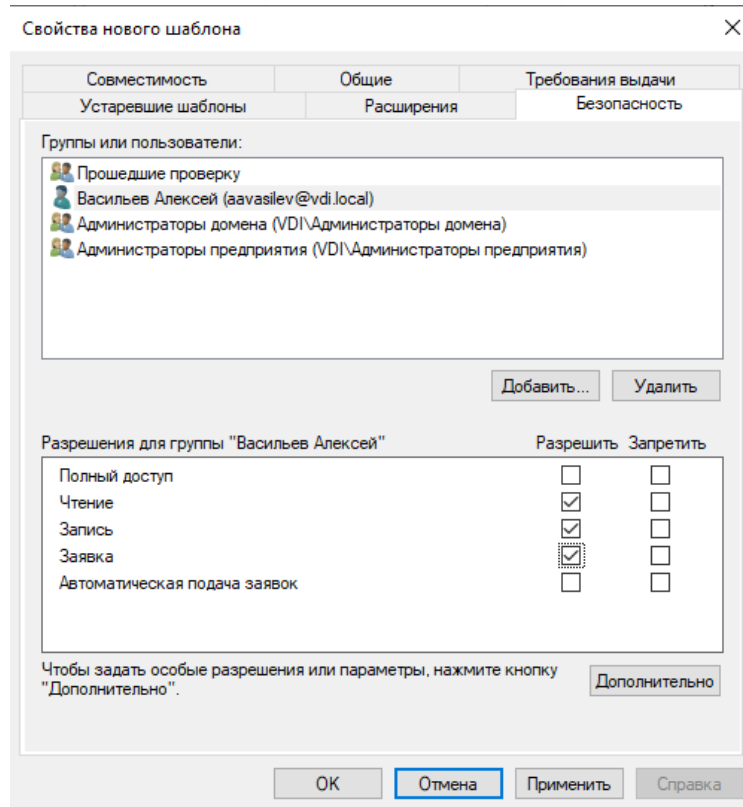


11. После этого нажмите кнопку **Добавить**.
12. Откроется окно **Добавление политики применения**. Из списка политик применения выберите: **Проверка подлинности клиента** и **Проверка подлинности центра распространения ключей**.



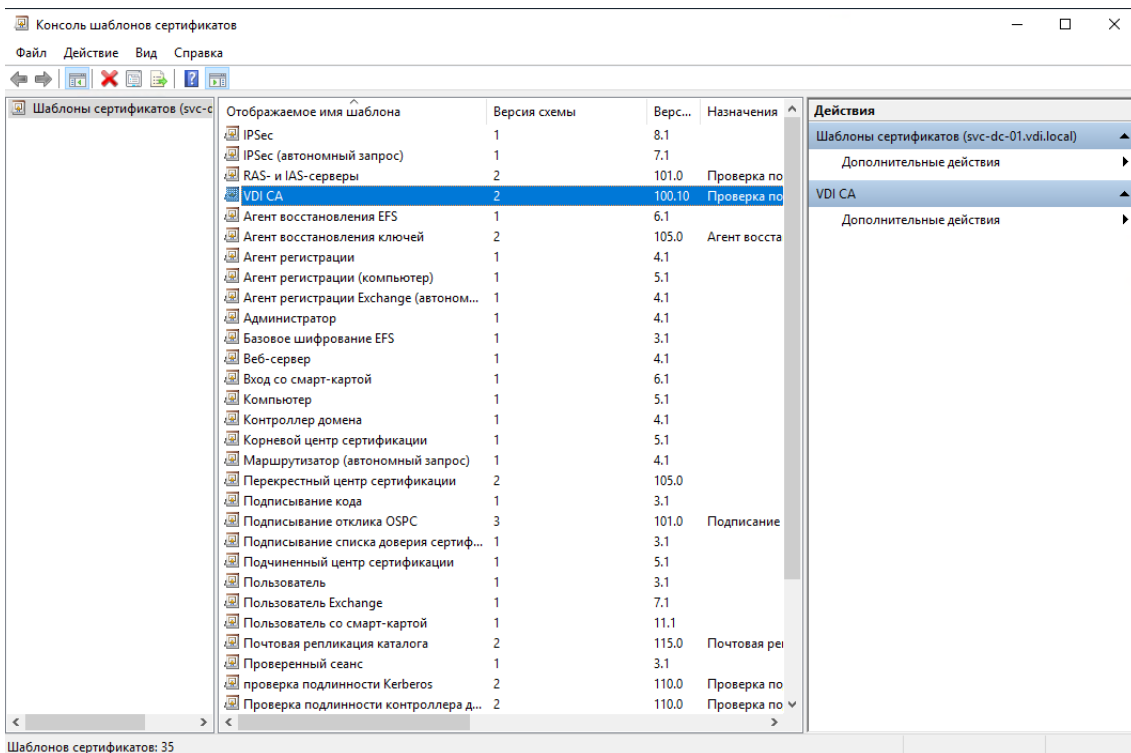
13. Нажмите **Ок**.

14. Перейдите на вкладку **Безопасность** в окне свойств нового шаблона. Проверить наличие у вашей группы или пользователя разрешений на **заявку** и **чтение**. В случае отсутствия установить соответствующие статусы.

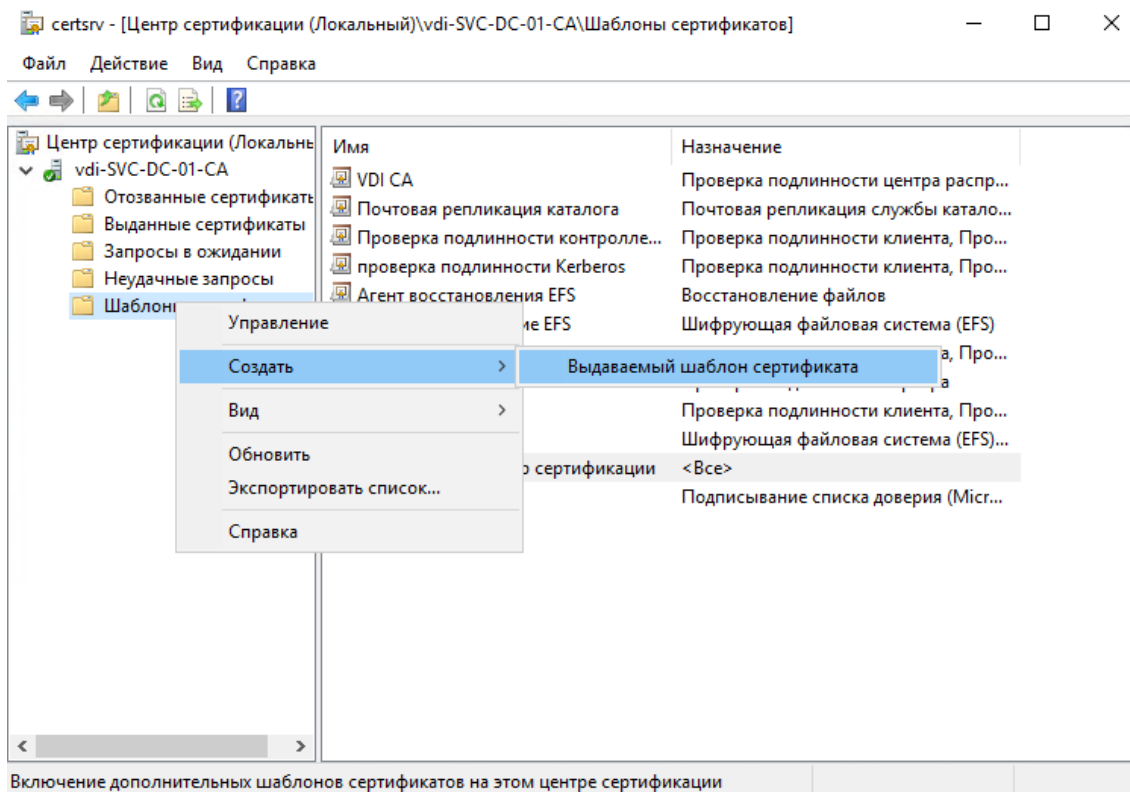


15. Нажимаем **Применить** и **Ок**.

16. Проверить наличие сертификата в шаблонах.



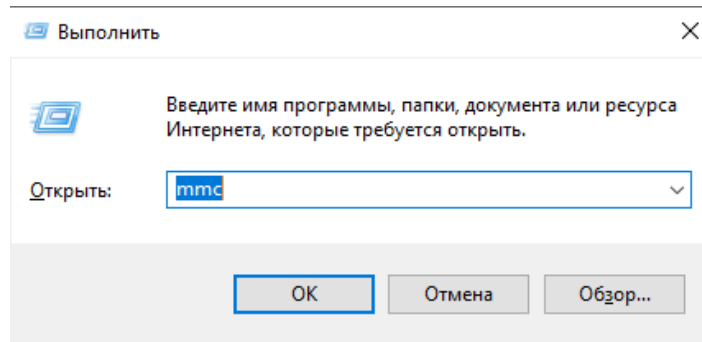
17. Перейдите в центр сертификации и щелкните правой кнопкой мыши **Шаблоны сертификатов** выберите «**Создать – Выдаваемый шаблон сертификата**».



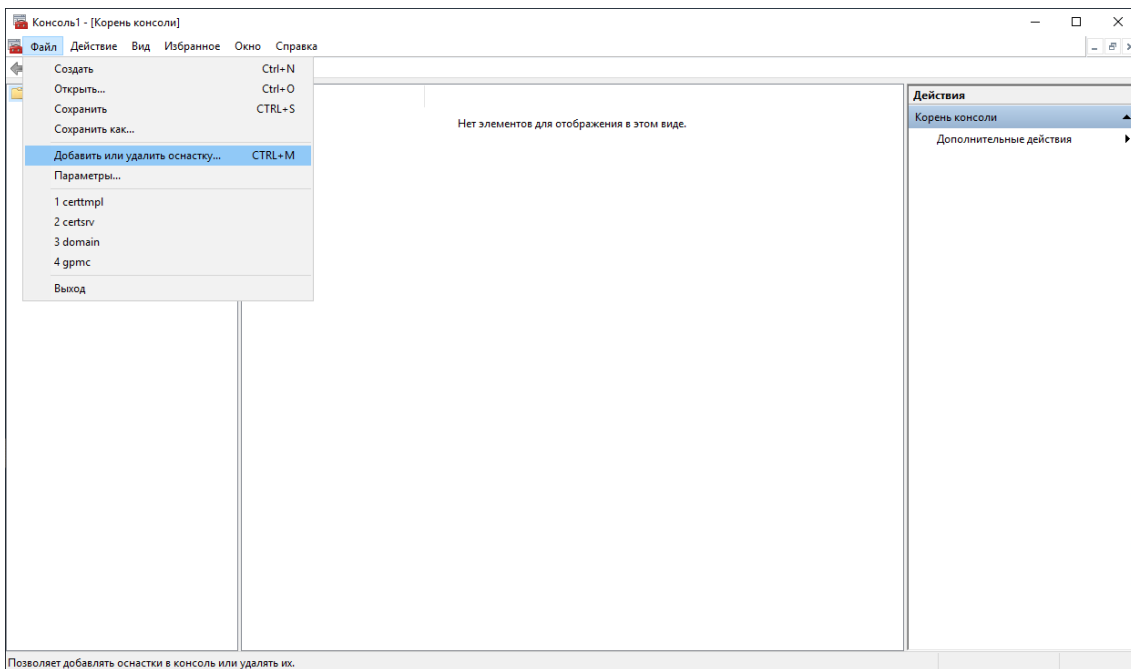
18. В открывшемся окне находим созданный сертификат **VDI CA** и добавляем его нажатием на кнопку **Ок**.

3 Выпуск сертификата

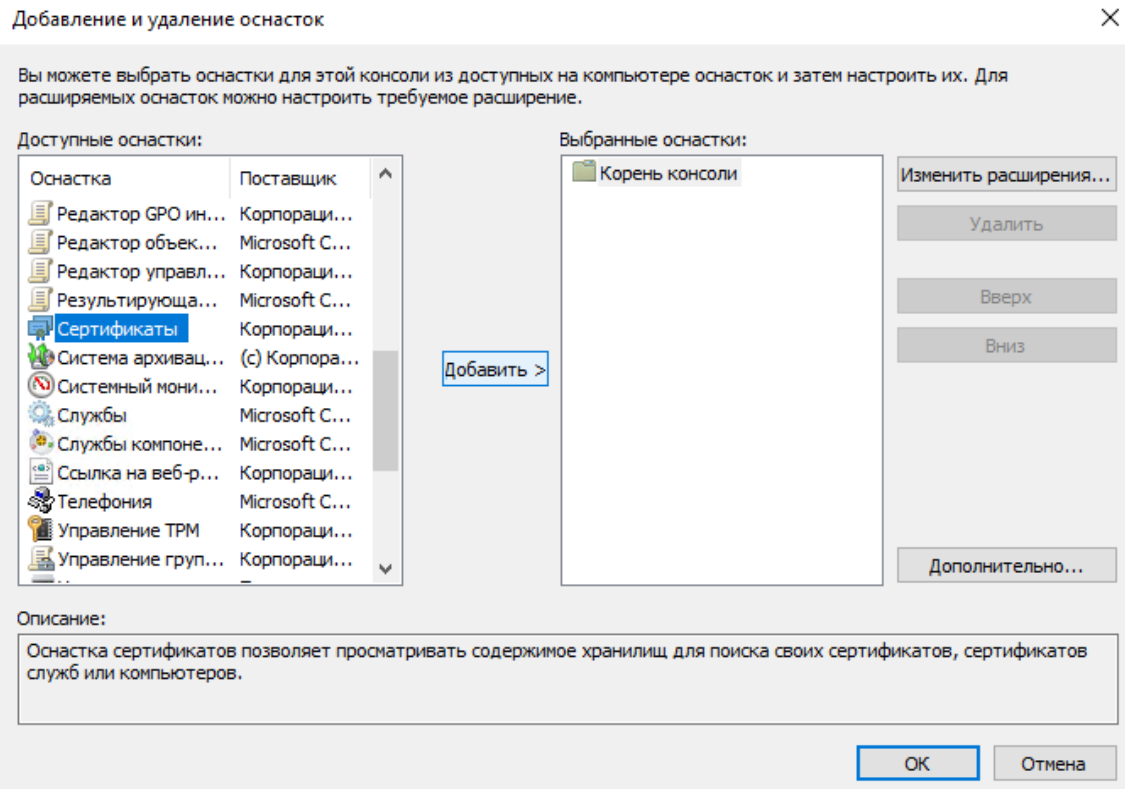
1. Откройте строку **Выполнить** в Windows и запустите консоль управления **MMC**.



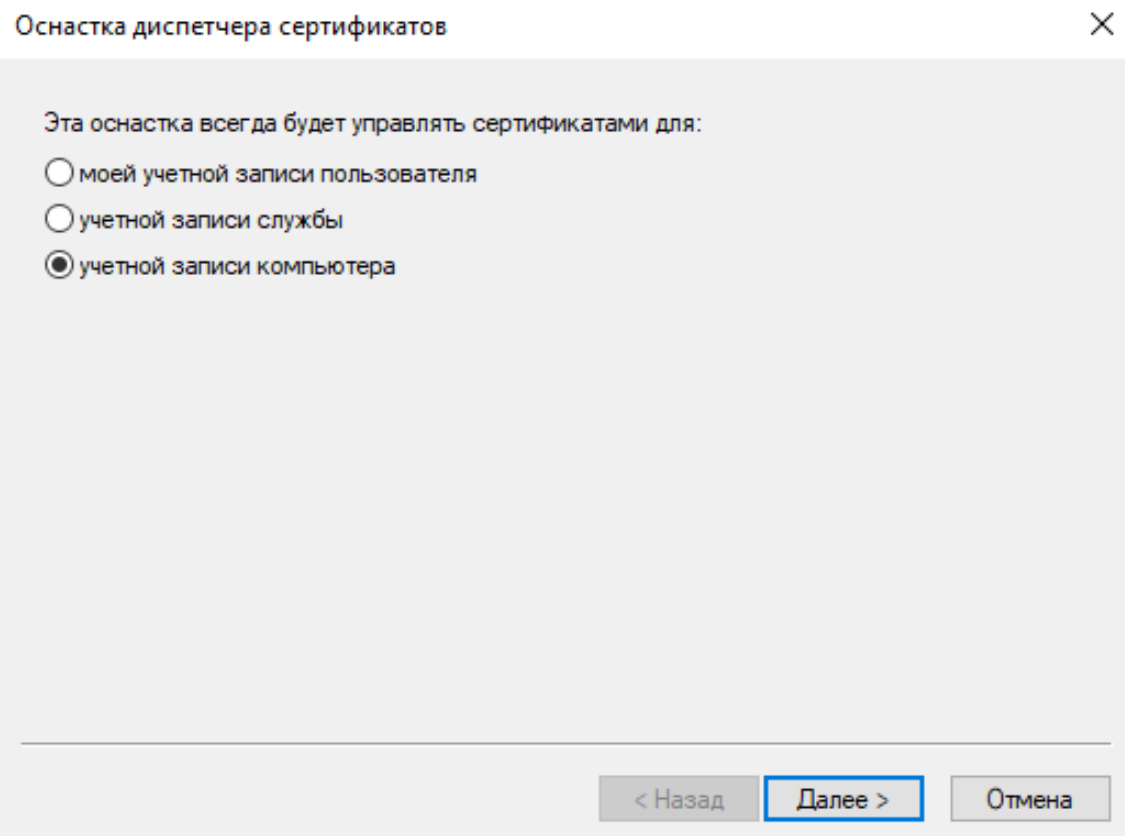
2. Добавьте оснастку сертификатов: нажмите **Файл – Добавить или удалить оснастку**.



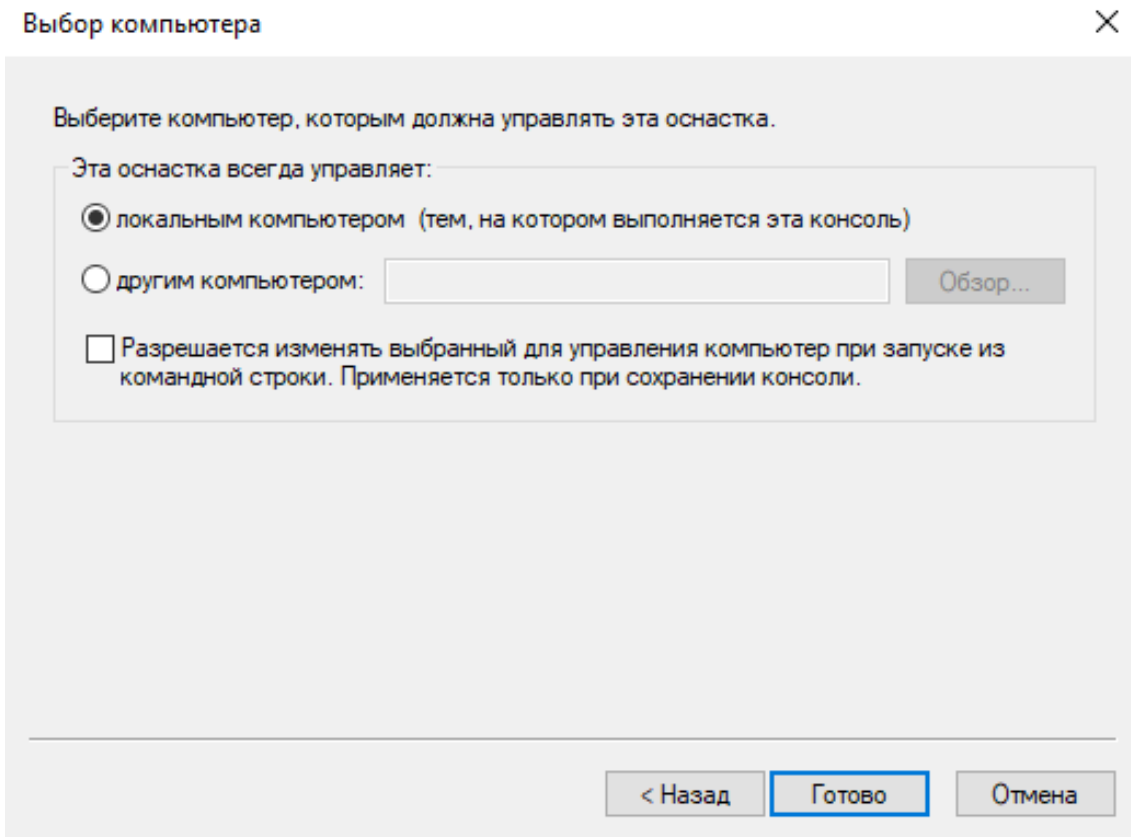
3. В открывшемся окне **Добавление и удаление оснасток** выберите папку **Сертификаты** и нажмите **Добавить**.



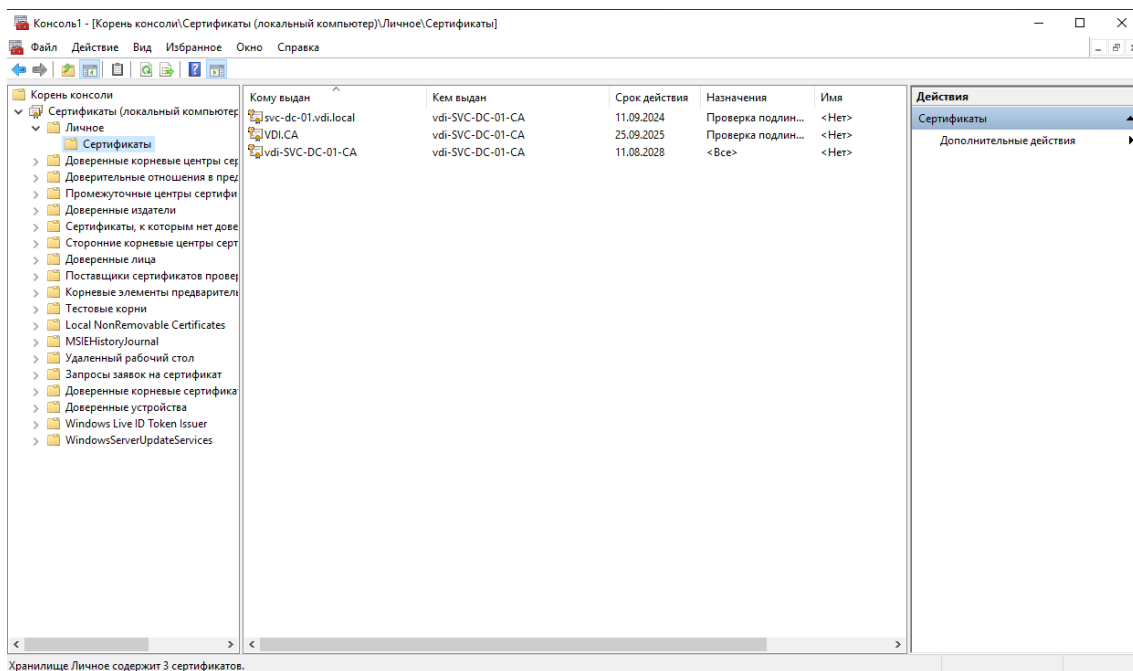
4. В окне **Оснастка диспетчера сертификатов** выберите **Учетная запись компьютера**. Нажать **Далее**.



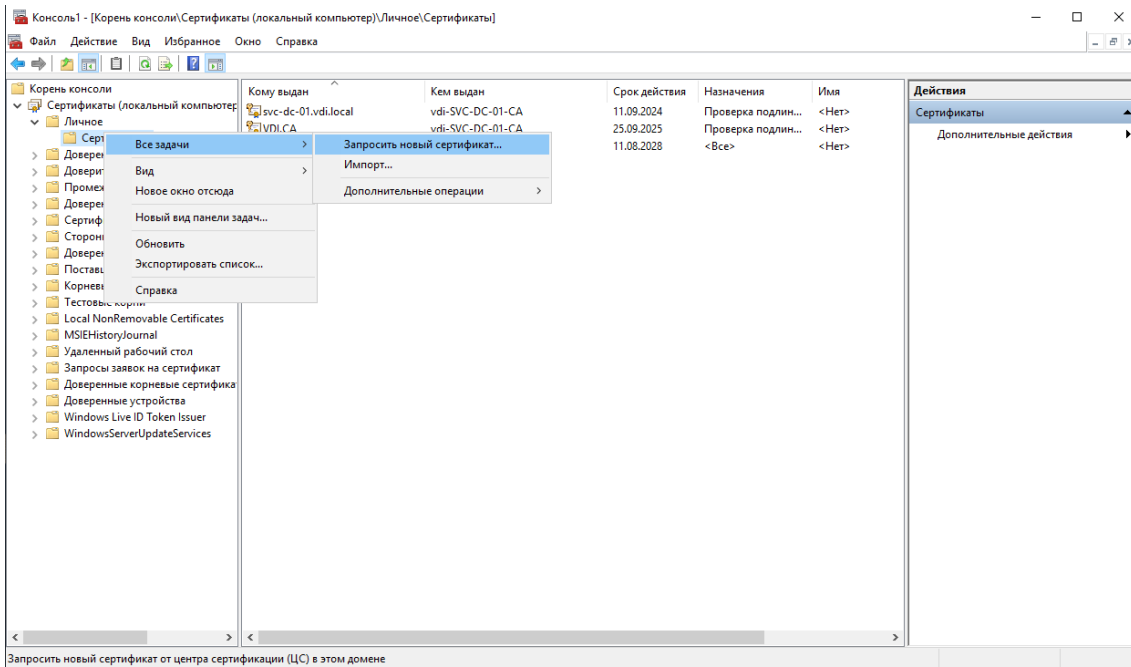
5. В открывшемся окне **Выбор компьютера** указать, что оснастка всегда управляет локальным компьютером. Нажать **Готово**.



6. В папке **Сертификаты** выберите **Личное – Сертификаты**.



7. Щелкните правой кнопкой мыши на **Сертификаты** и выберите **«Все задачи – Запросить новый сертификат...»**.

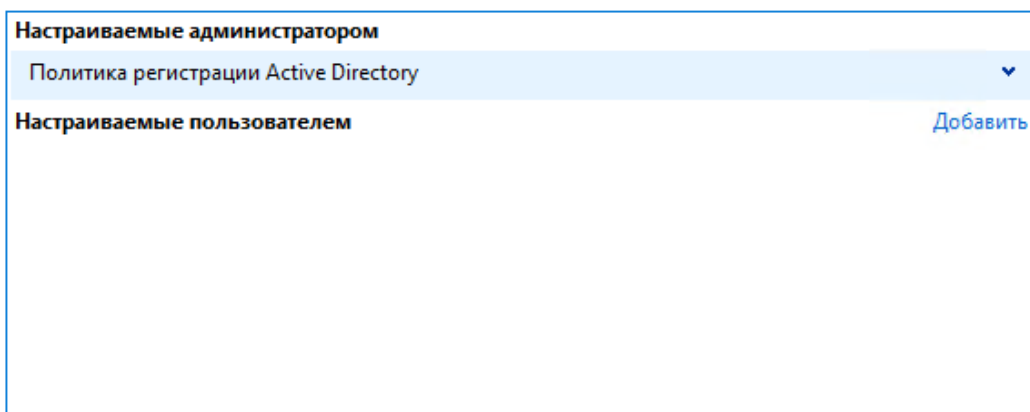


8. В окне выбора политики регистрации сертификатов нажимаем **Далее**.

 Регистрация сертификатов

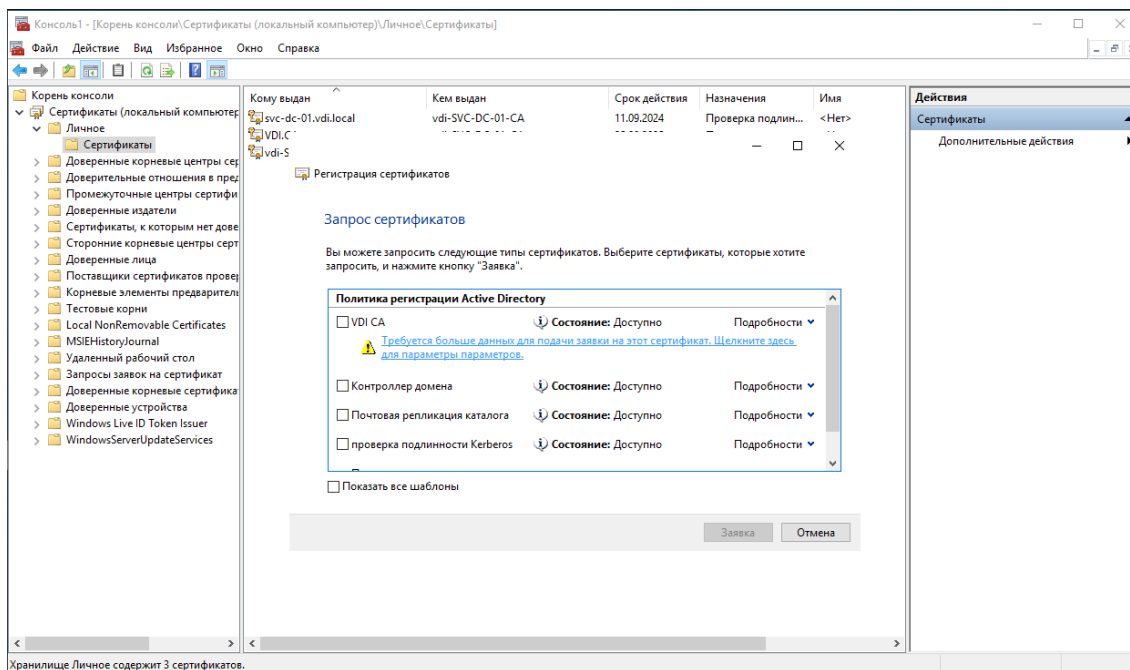
Выбор политики регистрации сертификатов

Политика регистрации сертификатов позволяет регистрировать сертификаты на основании заданных заранее шаблонов сертификатов. Политика регистрации сертификатов уже могла быть настроена.

**Далее**

Отмена

9. В окне **Запрос сертификатов** выберите нужный сертификат: VDI CA и нажмите на подсказку **Требуется больше данных для подачи заявки**.



10. Во вкладке **Субъект** в окне **Имя субъекта** выбрать **Тип: Общее имя** и присвойте любое значение, например, VDI.CA. Затем нажать **Добавить – Применить – Ок**.

Свойства сертификата

Субъект | Общие | Расширения | Закрытый ключ | Центр сертификации | Подпись

Субъект сертификата - пользователь или компьютер, для которого выпущен сертификат. Можно описать типы имен субъектов и указать альтернативные имена, которые могут использоваться в сертификате.

Субъект сертификата
Пользователь или компьютер, получающий сертификат

Имя субъекта:

Тип:

Значение:

Дополнительное имя:

Тип:

Значение:

OK Отмена Применить

11. Проверьте, чтобы подсказка в окне выбора сертификата пропала.
Нажмите **Заявка**.

Регистрация сертификатов

Запрос сертификатов

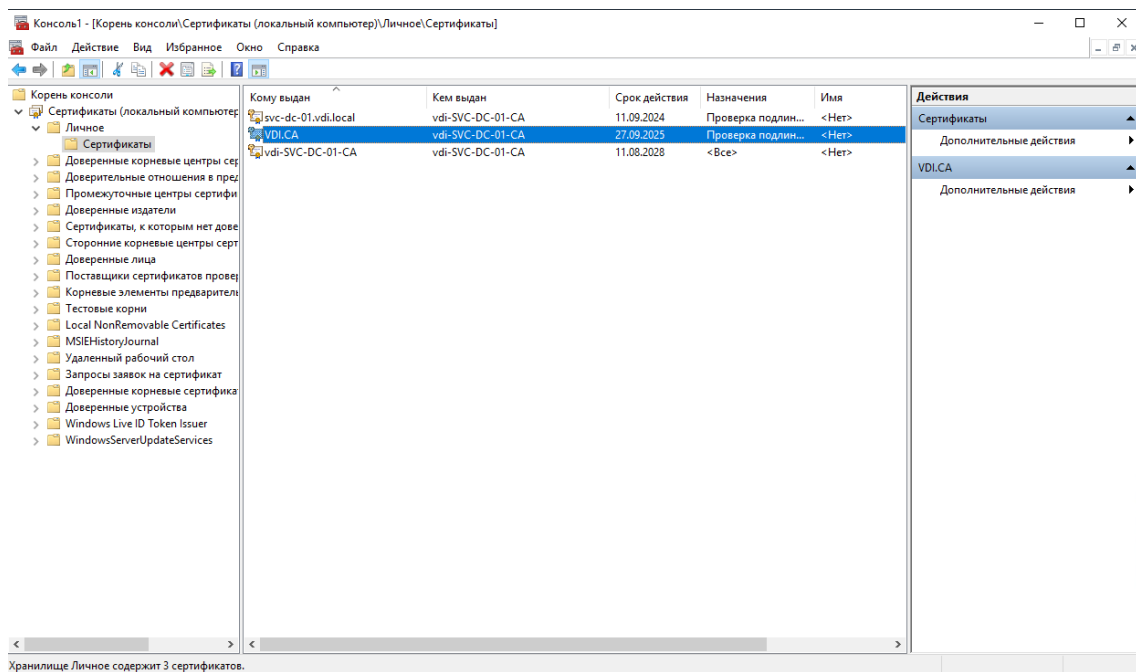
Вы можете запросить следующие типы сертификатов. Выберите сертификаты, которые хотите запросить, и нажмите кнопку "Заявка".

Политика регистрации Active Directory		
<input checked="" type="checkbox"/> VDI CA	Состояние: Доступно	Подробнее ▾
<input type="checkbox"/> Контроллер домена	Состояние: Доступно	Подробнее ▾
<input type="checkbox"/> Почтовая репликация каталога	Состояние: Доступно	Подробнее ▾
<input type="checkbox"/> проверка подлинности Kerberos	Состояние: Доступно	Подробнее ▾
<input type="checkbox"/> Проверка подлинности контроллера домена	Состояние: Доступно	Подробнее ▾

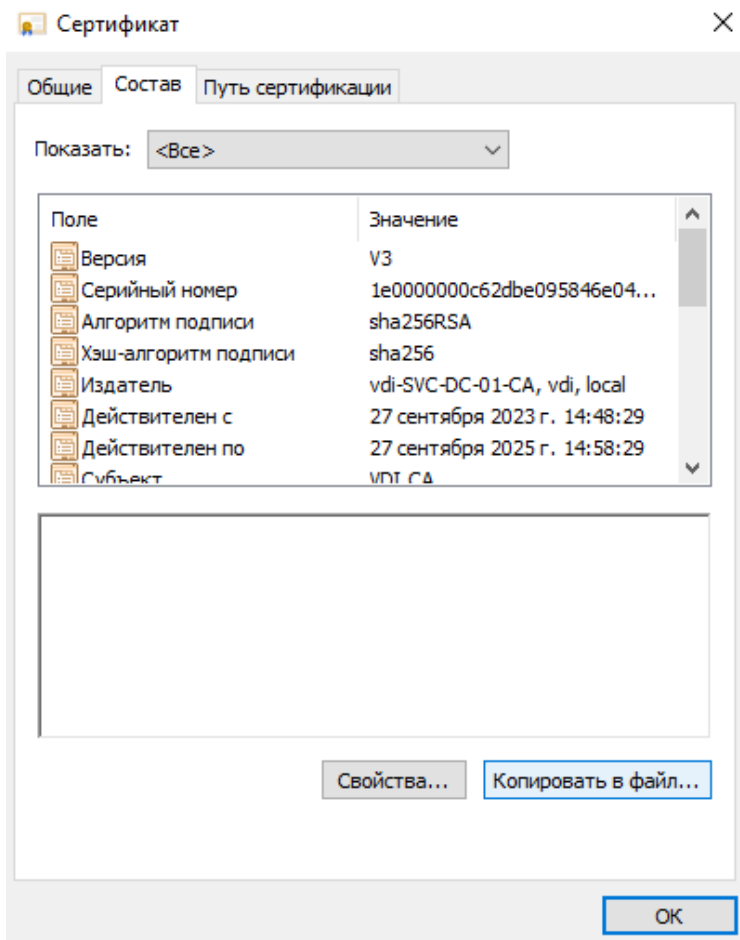
Показать все шаблоны

Заявка Отмена

12. Теперь в папке **Сертификаты** должен появиться сертификат **VDI CA**.



13. Откройте сертификат и перейдите на вкладку **Состав** нажмите на **Копировать файл...**



14. Откроется окно **Мастера экспорта сертификатов**. Нажмите **Далее**.

←  Мастер экспорта сертификатов

Мастер экспорта сертификатов

Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов из хранилища сертификатов на локальный диск.

Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.

Для продолжения нажмите кнопку "Далее".

Далее

Отмена

15. Подтвердите, что готовы экспортировать закрытый ключ вместе с сертификатом. Нажмите **Далее**.

←  Мастер экспорта сертификатов

Экспортирование закрытого ключа

Вы можете экспортировать закрытый ключ вместе с сертификатом.

Закрытые ключи защищены паролем. Чтобы экспортировать закрытый ключ вместе с сертификатом, укажите пароль.

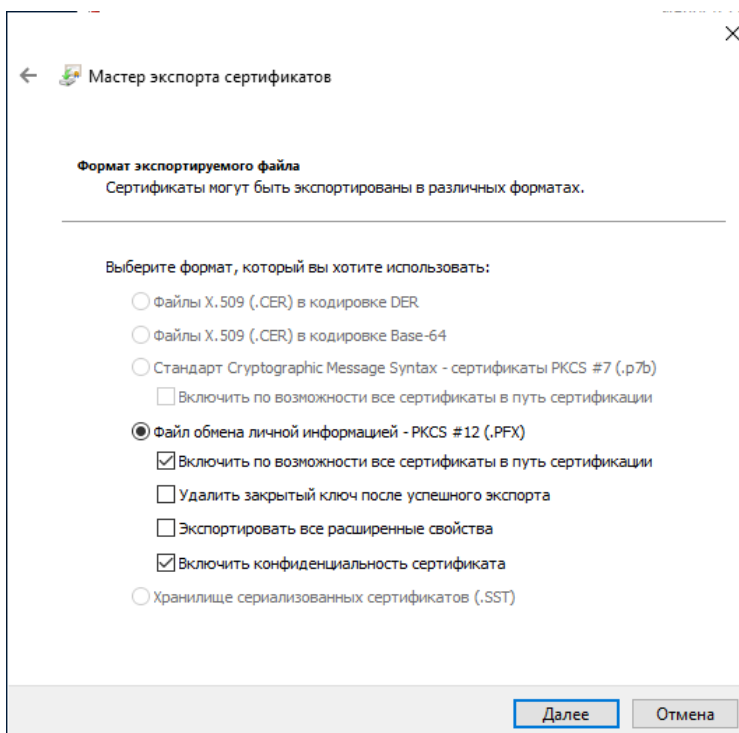
Вы хотите экспортировать закрытый ключ вместе с сертификатом?

- Да, экспортировать закрытый ключ
 Нет, не экспортировать закрытый ключ

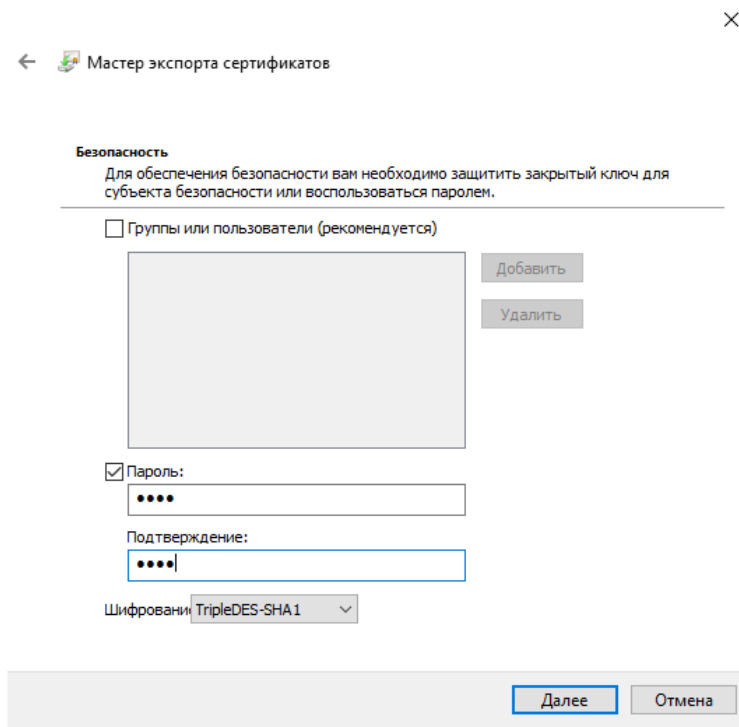
Далее

Отмена

16. Проверьте наличие галочек в пункте **Файл обмена личной информации**. Нажмите **Далее**.

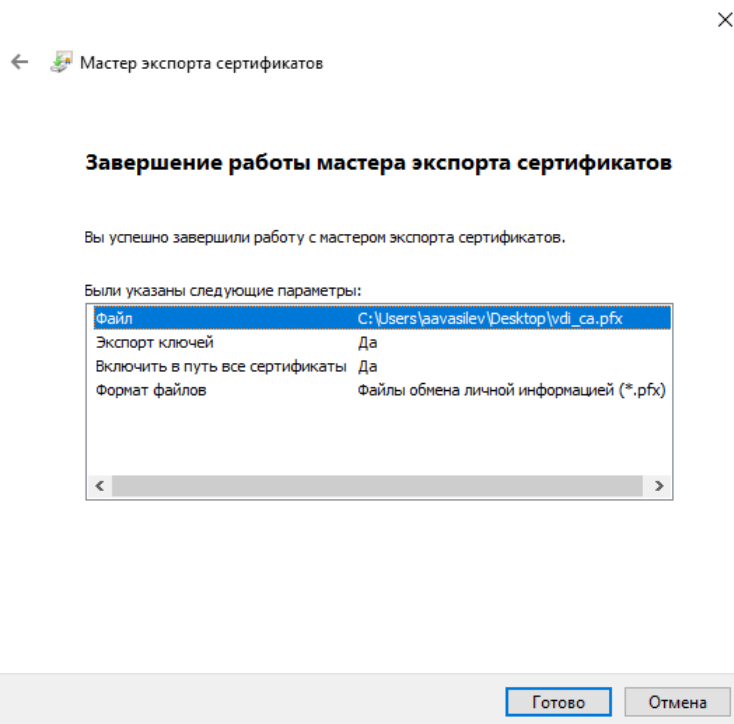


17. Введите пароль и нажмите **Далее**.



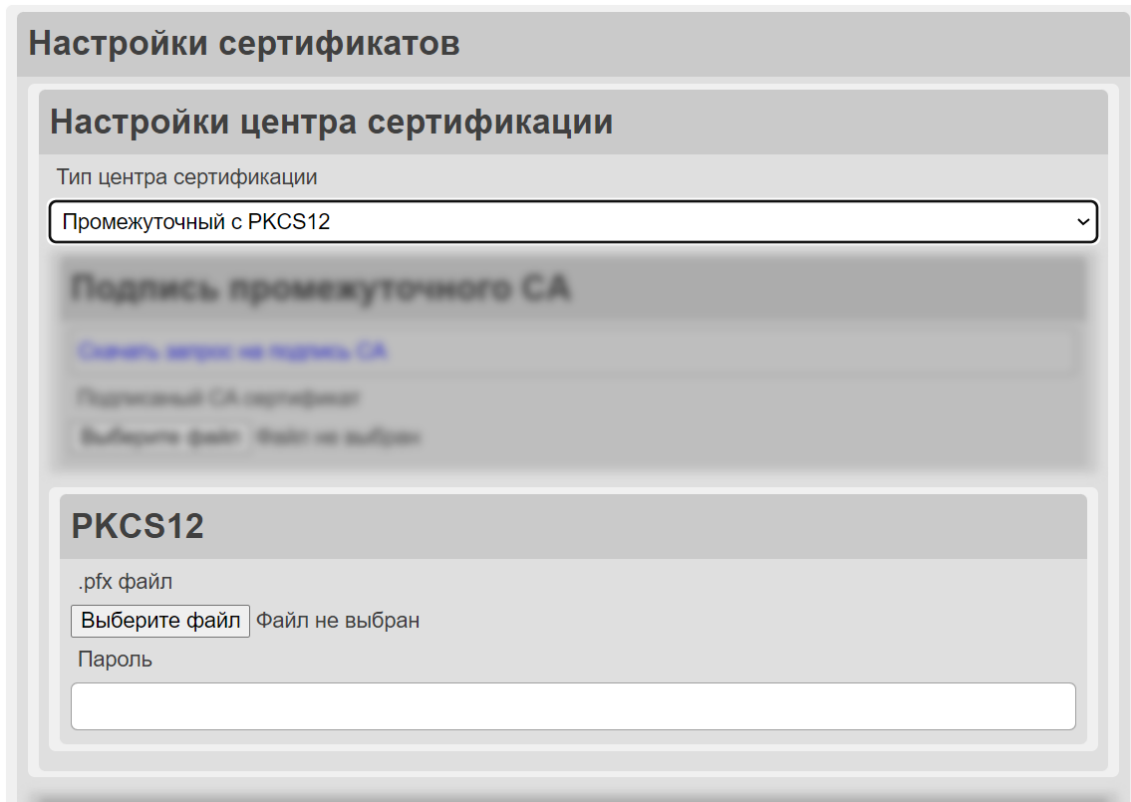
18. В открывшемся окне укажите путь сохранения сертификата. Нажмите **Далее**.

19. Для завершения экспорта сертификата нажмите **Готово**.



4 Загрузка сертификата в инсталлятор

1. Откройте инсталлятор и выберите тип центра сертификации
Промежуточный с PKCS12.



2. В открывшемся окне **PKCS12** нажмите на кнопку **Загрузить файл** и выберите файл формата .pfx, который содержит сертификат и связанный с ним закрытый ключ.
3. Введите пароль для файла .pfx в соответствующем поле, чтобы разблокировать его содержимое.