

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Российский экономический университет им. Г.В. Плеханова»  
**Московский приборостроительный техникум**

ПРАКТИЧЕСКАЯ РАБОТА №17  
«Работа с сертификатами в целевом домене»

Москва, 2024 г.

**Цель работы:** в ходе выполнения лабораторной работы рассмотреть процесс добавления шаблонов цифровых сертификатов в ОС Windows.

**Ход работы:**

**Если вы создали пользователя в подразделении Krypto при подготовке ВМ, то пункты на рисунках 1-3 можно пропустить и использовать данного пользователя!**

Открываем на сервере «Active Directory – пользователи и компьютеры» и создаем нового пользователя.

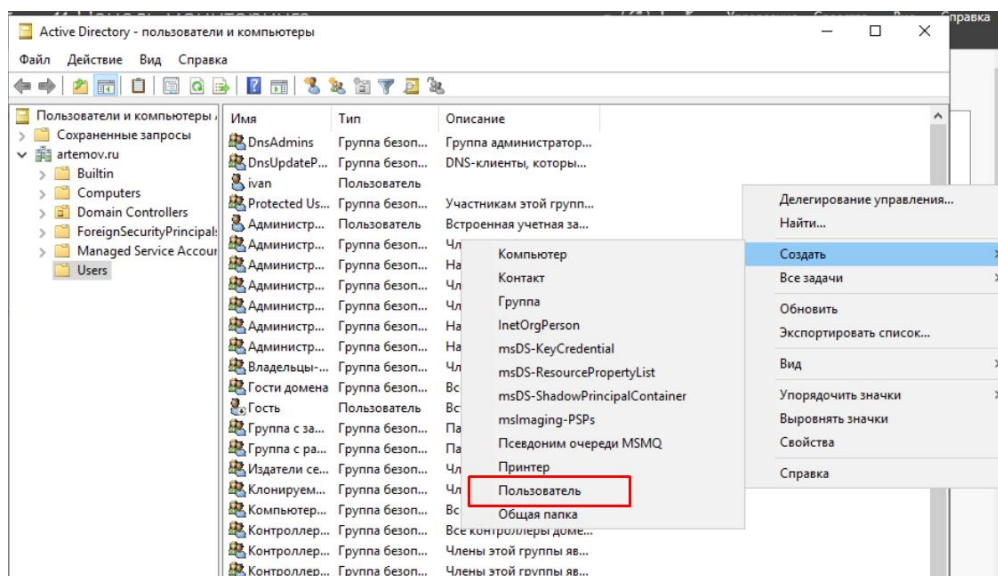
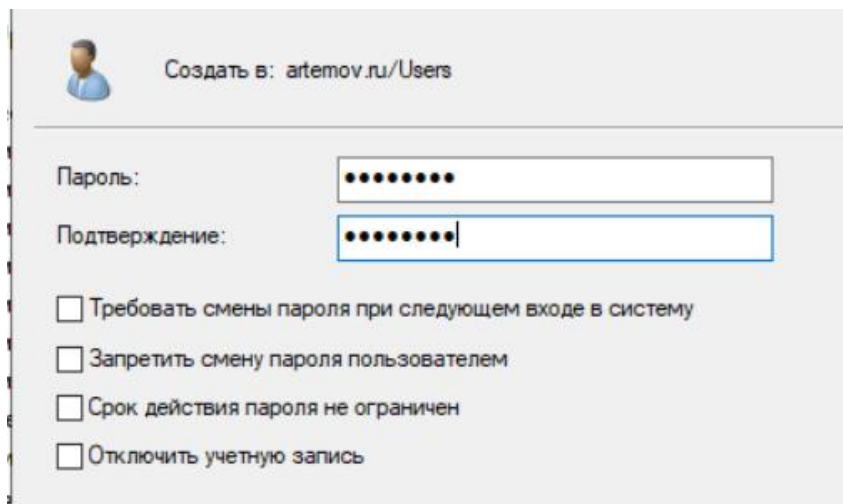


Рисунок 1 – создание пользователя

Задаем имя пользователю домена.

Рисунок 2 – учетные данные

Задаем пароль и снимаем галочки, если они есть.



Создать в: artemov.ru/Users

Пароль: [masked]

Подтверждение: [masked]

☐ Требовать смены пароля при следующем входе в систему

☐ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

Рисунок 3 – пароль пользователя.

1. Открываем «Центр сертификации» на сервере.

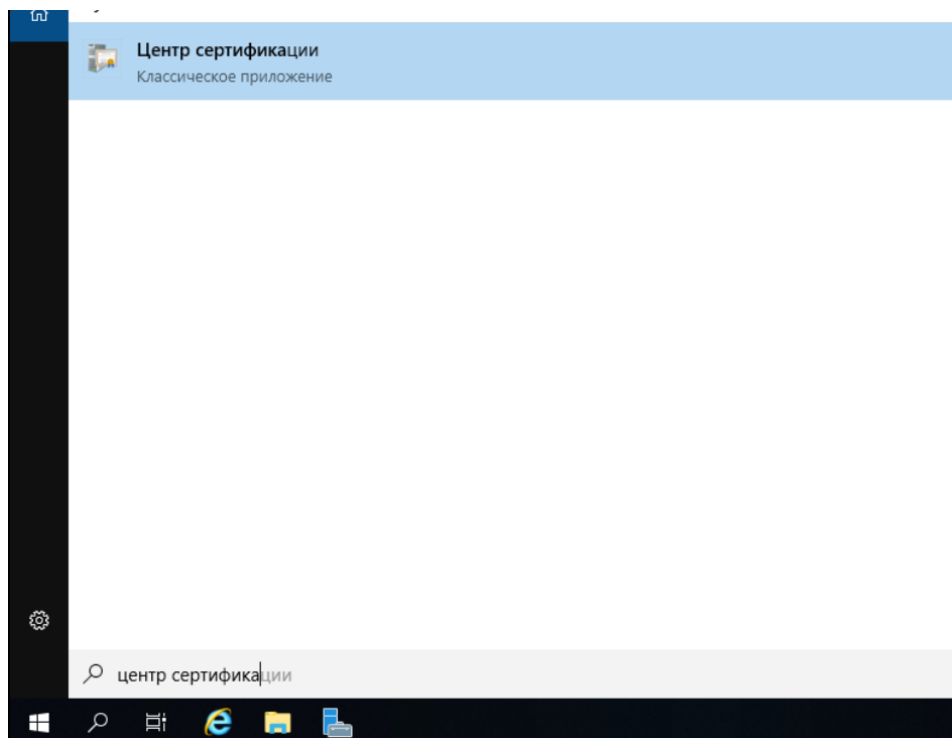


Рисунок 4 – центр сертификации

ПКМ на «шаблоны сертификатов» - «управление».

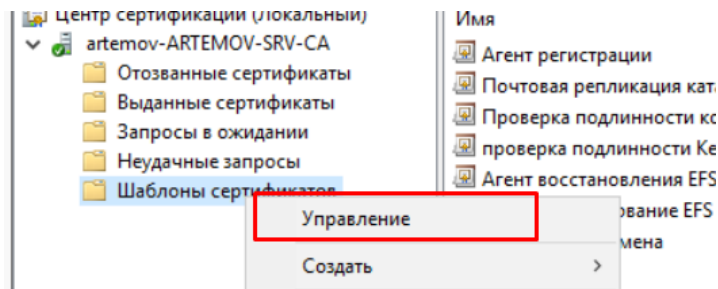


Рисунок 5 – выбор пункта «управление»

Копируем шаблон «Пользователь со смарт-картой»

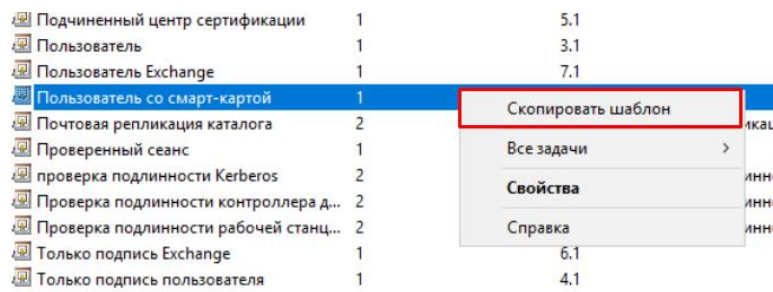


Рисунок 6 – пользователь со смарт-картой

Открывается окно со свойствами нового шаблона. В «Общие» задаем имя шаблона и периоды. Нажимаем «применить».

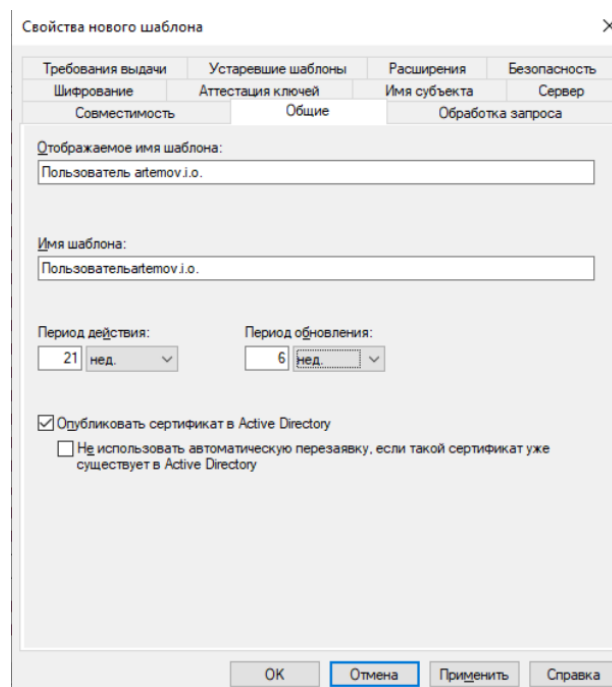


Рисунок 7 – вкладка «Общие»

В «Шифрование» указываем поставщика для запросов – «Microsoft Base Smart Card Crypto Provider». Нажимаем «применить».

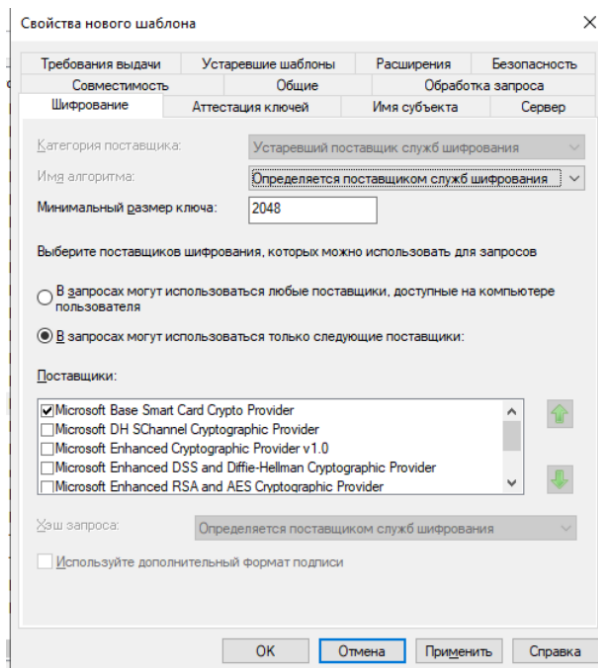


Рисунок 8 – вкладка «Шифрование»

В «Безопасность» выдаем разрешения для группы «Прошедшие проверку» на «Заявку» и «Автоматическую подачу заявок». Нажимаем «применить».

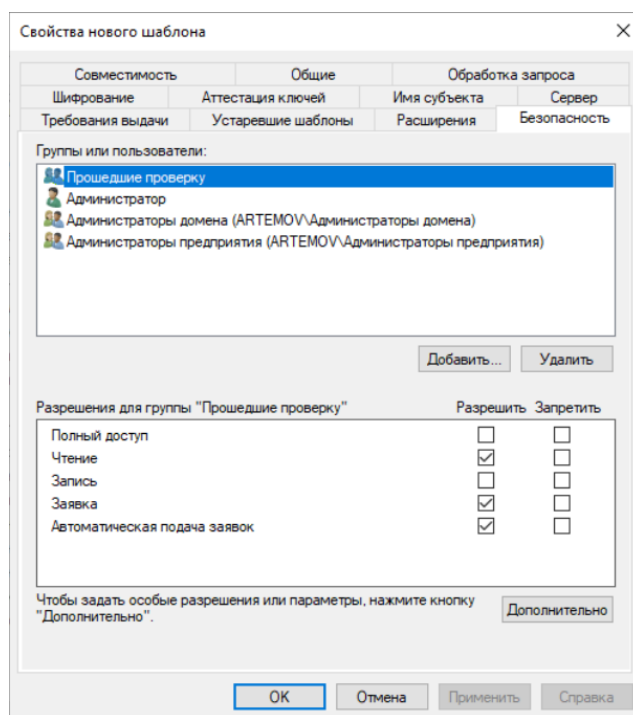


Рисунок 9 – вкладка «Безопасность»

В «Требования выдачи» указываем тип политики «Политика применения» и в политике применения «Агент запроса сертификата». Нажимаем «применить». Остальные свойства были оставлены по умолчанию.

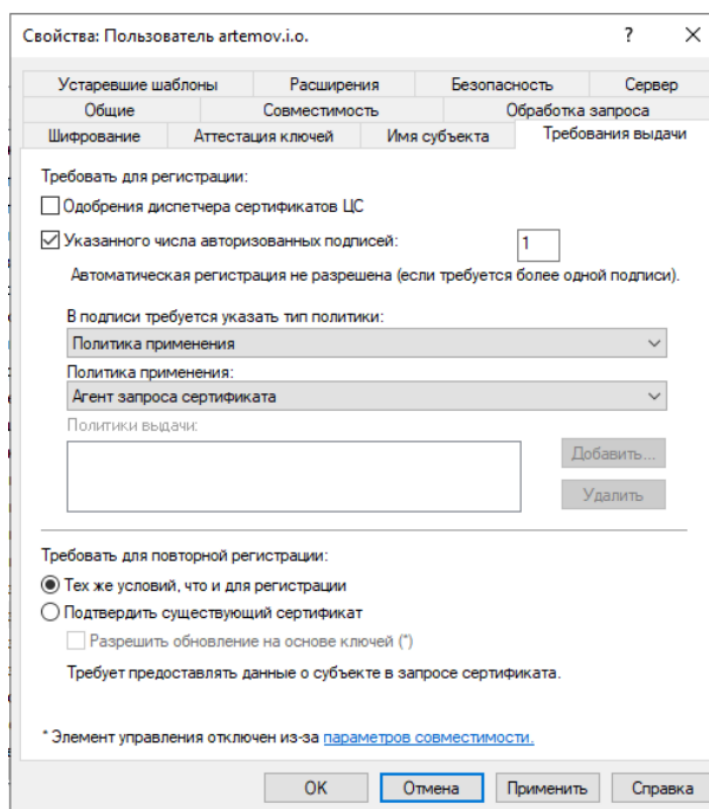


Рисунок 10 – вкладка «Требования выдачи»

После этого в консоли находим шаблон «Агент регистрации» и жмем ПКМ – «Свойства».

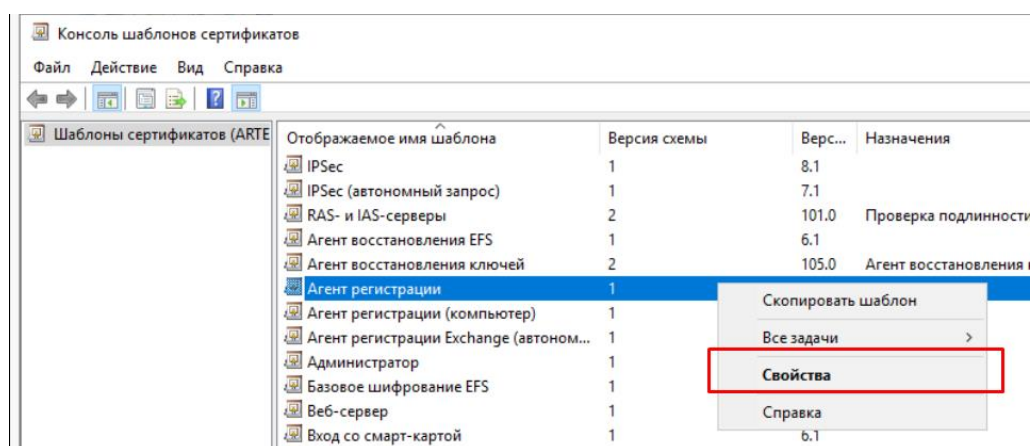


Рисунок 11 – агент регистрации

Во вкладке «Безопасность» выдаем право на «Заявку» и «Чтение» для группы «Прошедшие проверку». Нажимаем «применить».

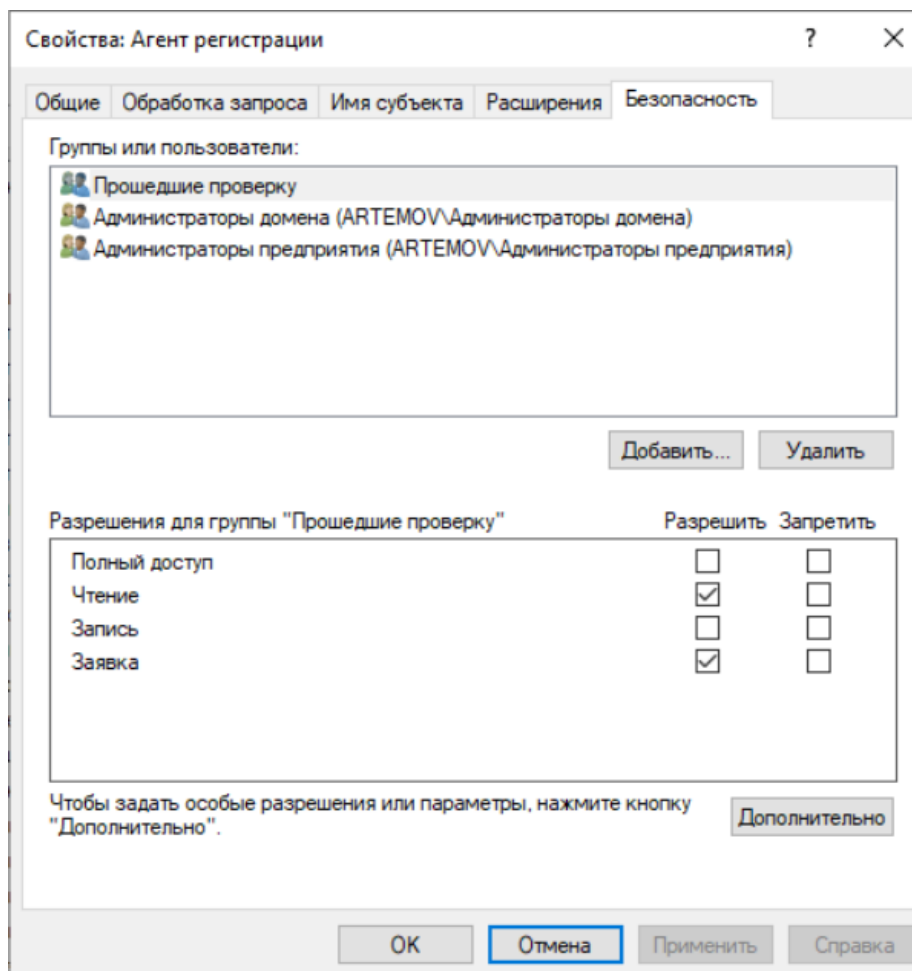


Рисунок 12 – вкладка «Безопасность» агента регистрации

Возвращаемся в Центр сертификации и жмем ПКМ – «Создать» - «Выдаваемый шаблон сертификата».

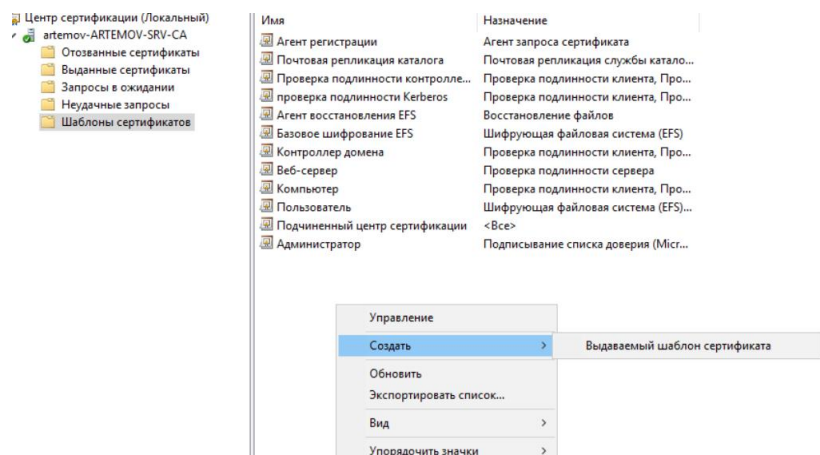


Рисунок 13 – выдаваемый шаблон сертификата



Выбираем ранее созданный шаблон для пользователя.

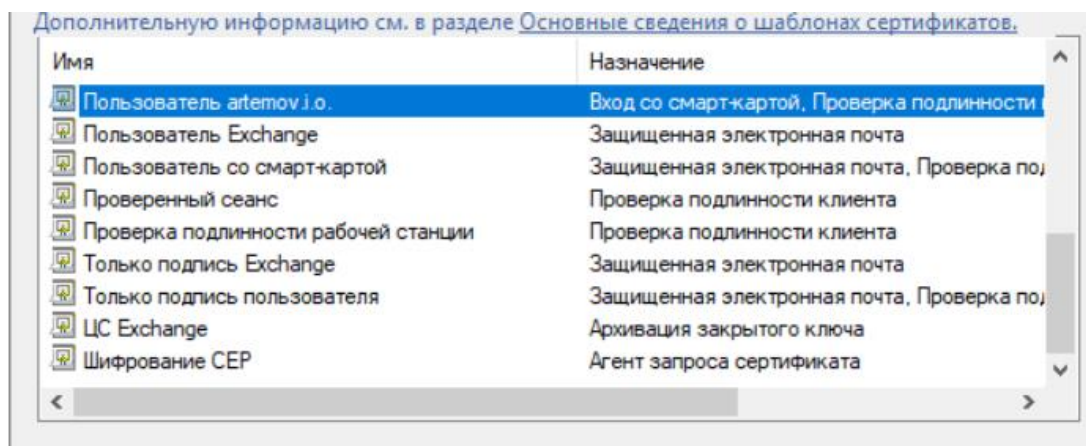


Рисунок 14 – ранее созданный шаблон

Создаем еще один выдаваемый шаблон сертификата – «Агент регистрации».

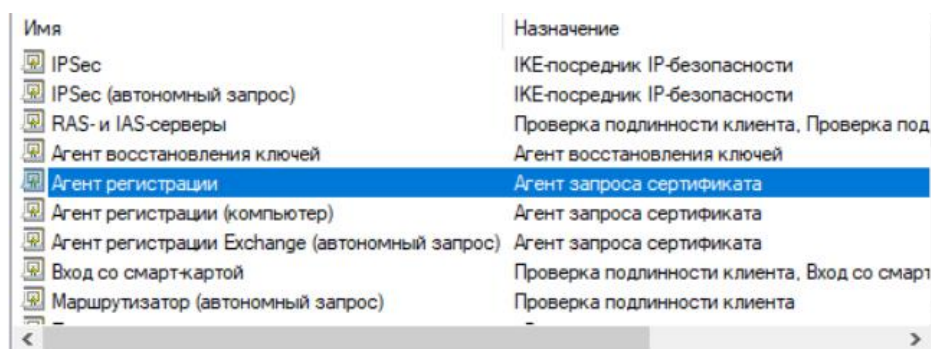


Рисунок 15 – агент регистрации

По итогу окно «Центра сертификации» должно выглядеть следующим образом.

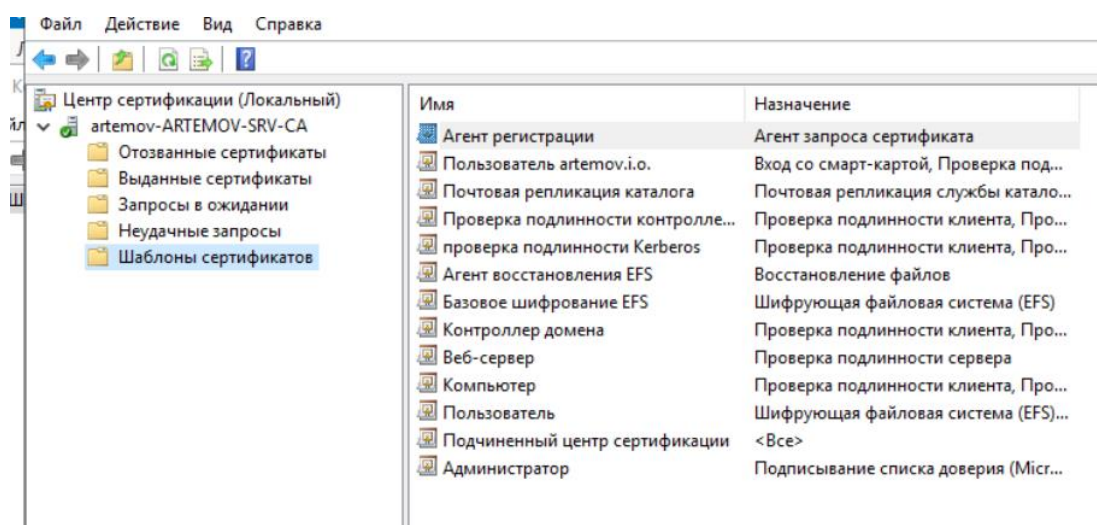


Рисунок 16 – итог промежуточной работы



Заходим в проводник на сервере и идем по пути C:\Windows\System32\CertSrv\CertEnroll и находим там файл сертификата сервера.

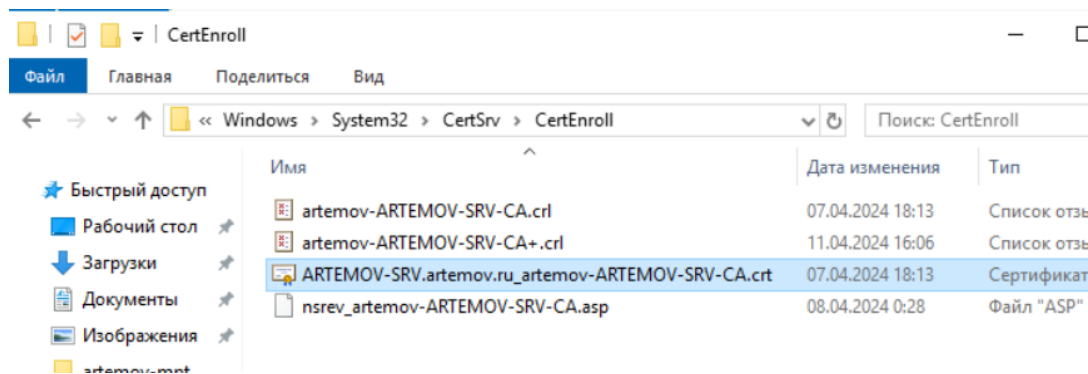


Рисунок 17 – сертификат сервера

ПКМ по файлу сертификата – «Установить сертификат».

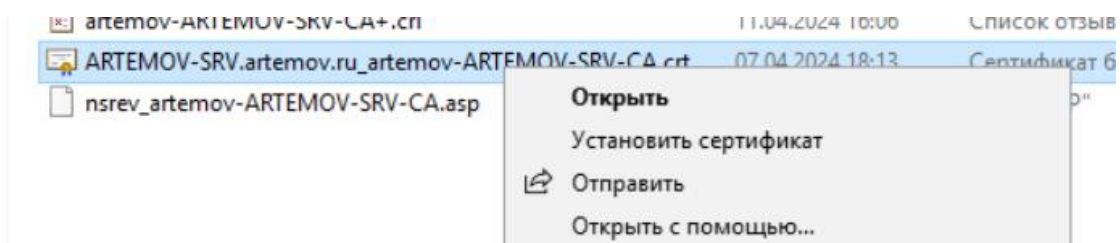


Рисунок 18 – установка сертификата

Откроется мастер импорта сертификатов. Выбираем «Локальный компьютер».

## Мастер импорта сертификатов

Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.

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.

Расположение хранилища

☐ Текущий пользователь

☒ Локальный компьютер

Для продолжения нажмите кнопку "Далее".

Рисунок 19 – мастер импорта

Выбираем «Поместить все сертификаты в следующее хранилище» - «Обзор» - «Доверенные корневые центры сертификации».

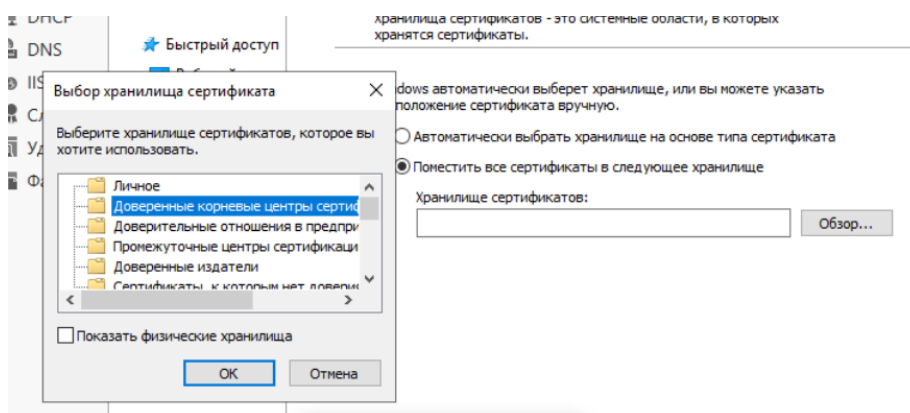


Рисунок 20 – выбор хранилища

Жмем на следующем этапе «Готово» и видим сообщение об успешном импорте.

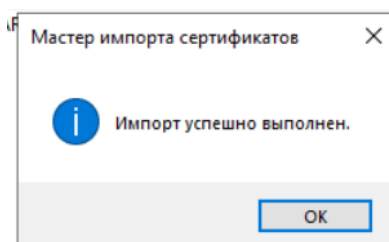


Рисунок 21 – успешный импорт

Заходим на клиенте за ранее созданного пользователя.

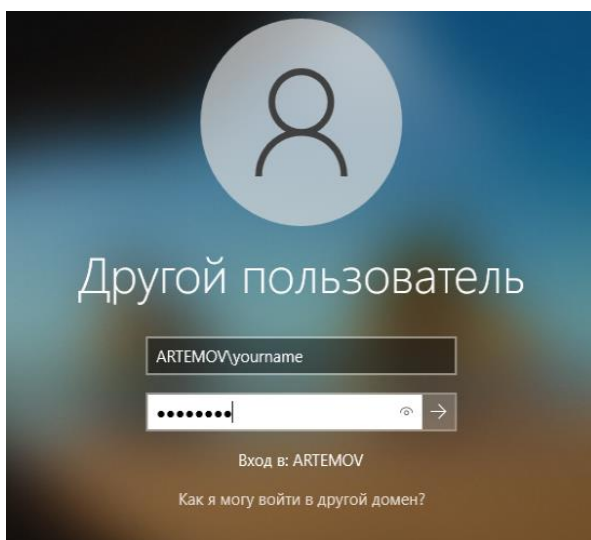


Рисунок 22 – вход за созданного пользователя

Далее стоит задача скопировать сертификат сервера с самого сервера на клиент. Это можно сделать любым удобным способом (сетевая папка, SFTP и т.д.). В данной же работе передача сертификата была выполнена при помощи перетаскивания файла с VM на хост, и наоборот с функцией Drag'n'drop.

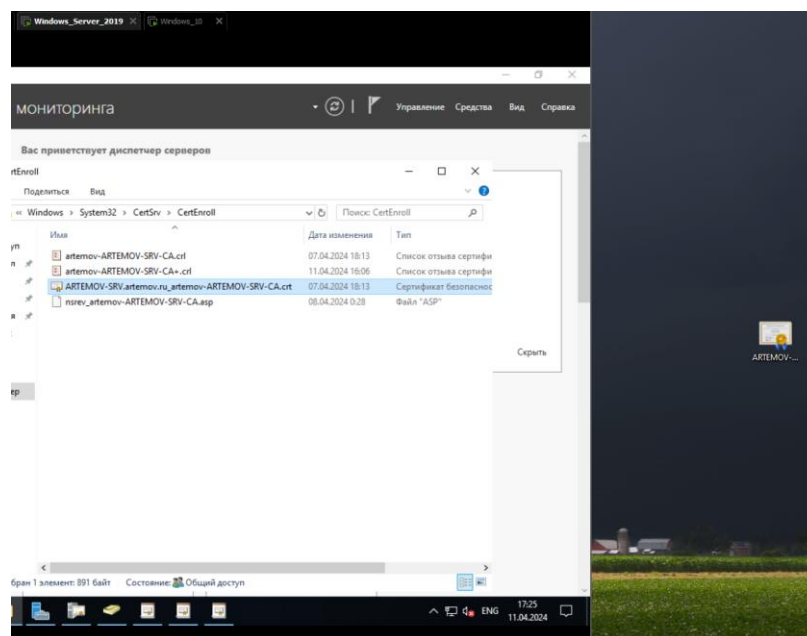


Рисунок 23 – передача сертификата

Перетаскивание файла сертификата с хоста на VM клиента (если перетаскивание не работает – попробуйте Ctrl+C, Ctrl+V).

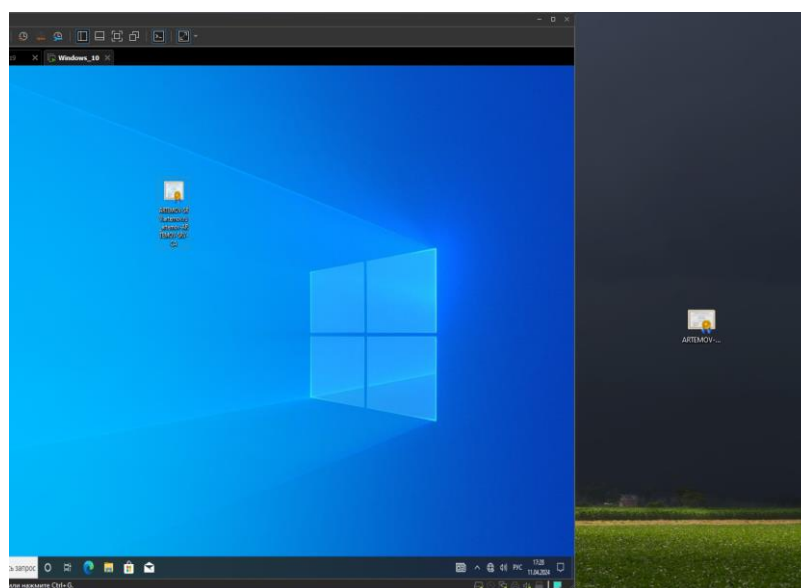


Рисунок 24 – перетаскивание файла

**Устанавливаем сертификат, также, как и на сервере (шаги 18 – 21).**

В ходе установки сертификата на локальный компьютер потребуют учетные данные администратора, используем «Администратор» и пароль от администратора домена.

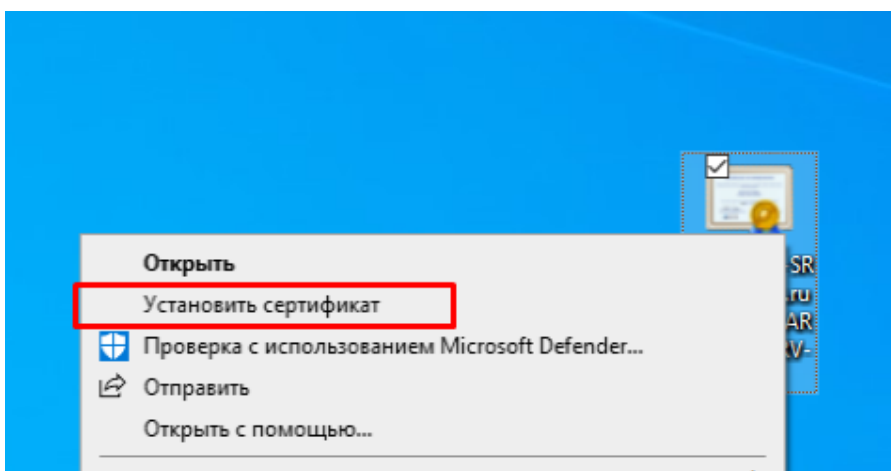


Рисунок 25 – установка сертификата

Открываем на клиенте «Управление сертификатами пользователей».

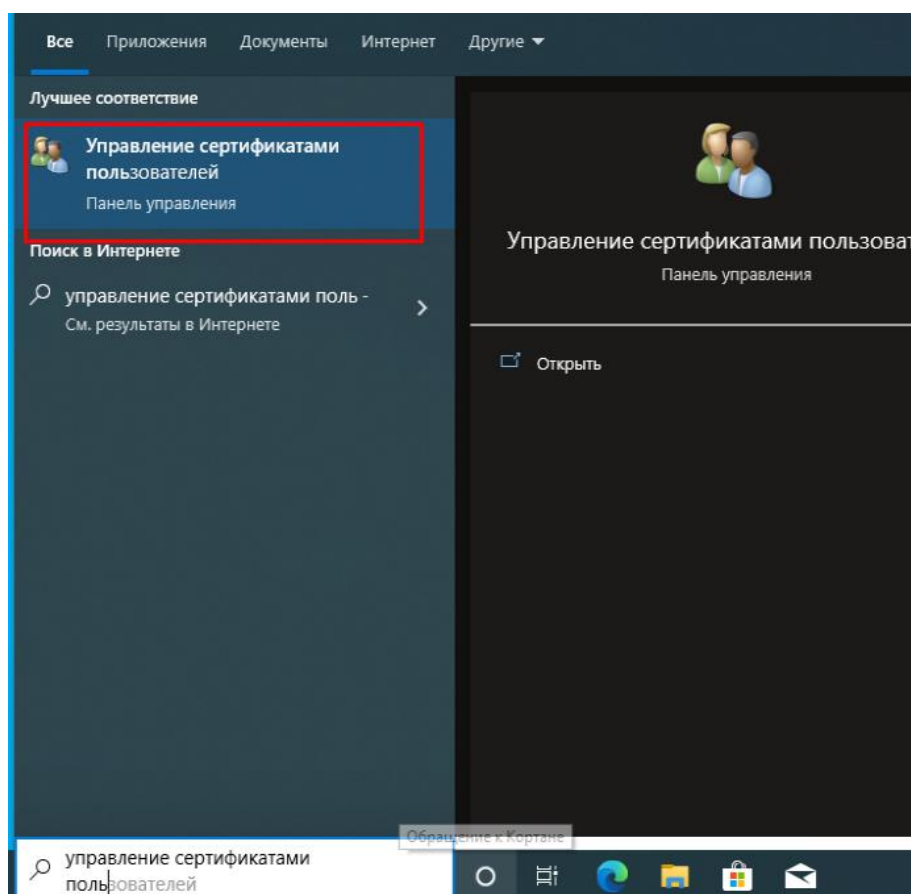


Рисунок 26 – управление сертификатами пользователей

Нажимаем на папку «Личное», затем ПКМ по пустой области, «Все задачи» - «Запросить новый сертификат».

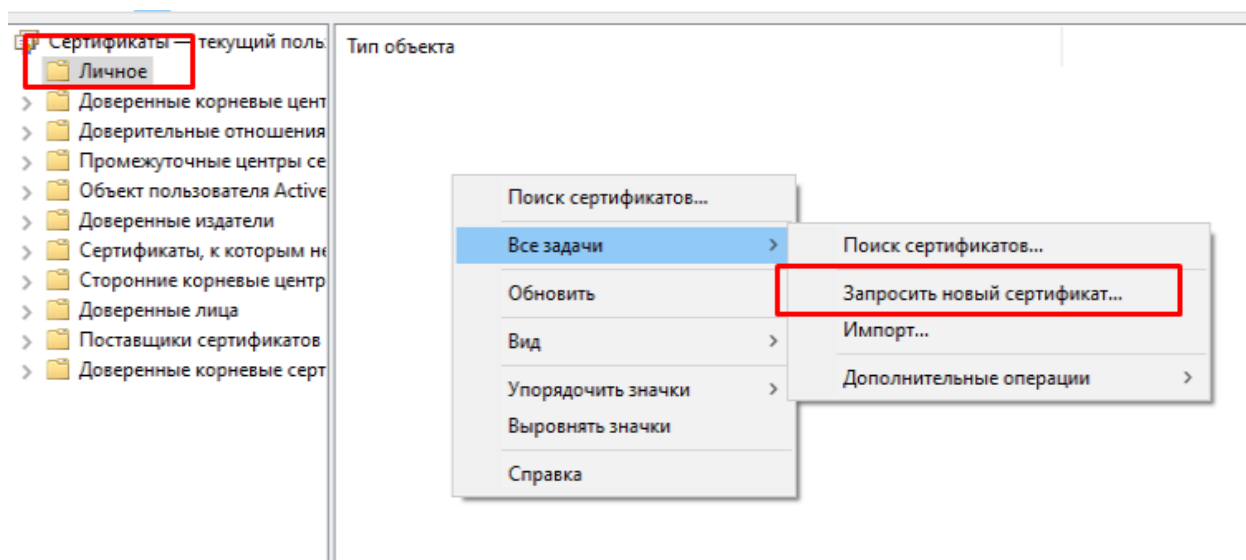


Рисунок 27 – запрос нового сертификата

Нажимаем «Далее», «Далее» и видим список доступных для запроса сертификатов. В первую очередь запрашиваем «Агента регистрации», нажимаем «Заявка».

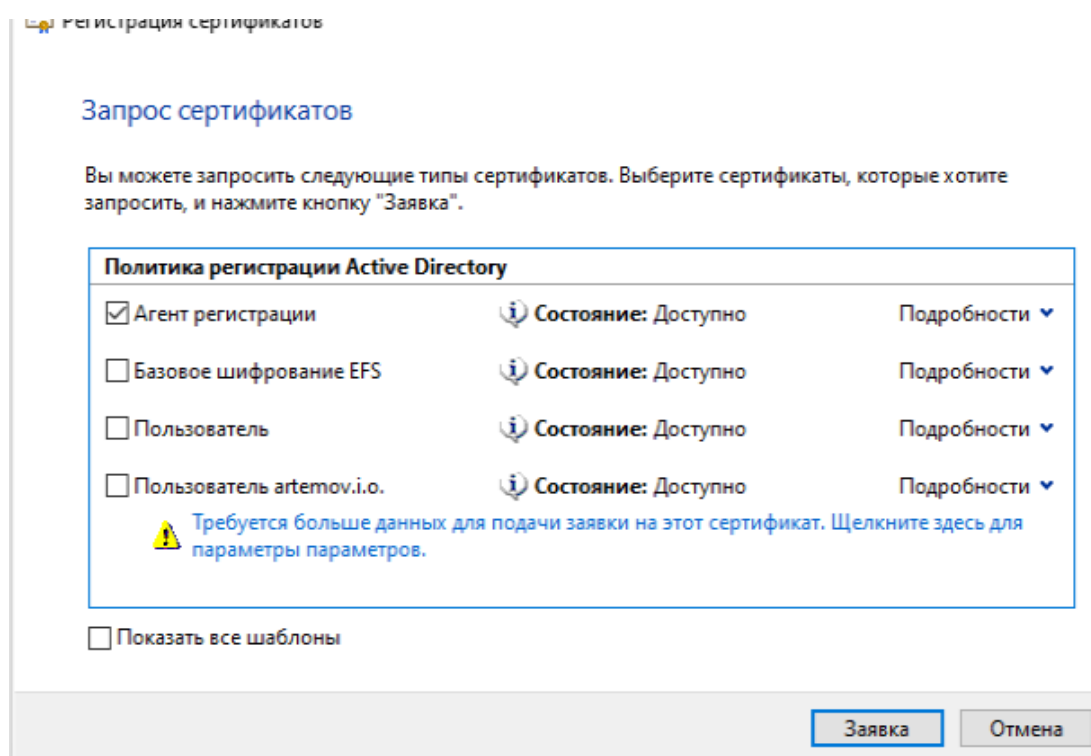


Рисунок 28 – агент регистрации

Результатом установки сертификатов должно быть следующее сообщение.

### Результаты установки сертификатов

Следующие сертификаты были получены и установлены на данном компьютере.

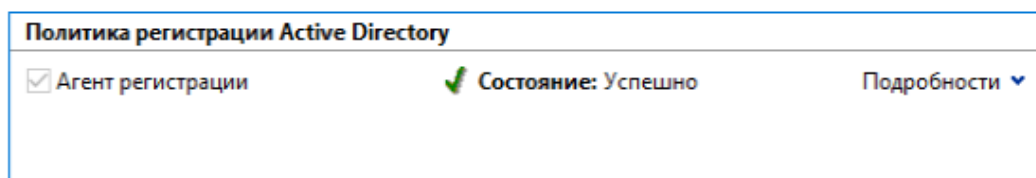


Рисунок 29 – результат установки

Появляется папка «Сертификаты», а в ней новый сертификат. Повторяем процедуру с запросом.

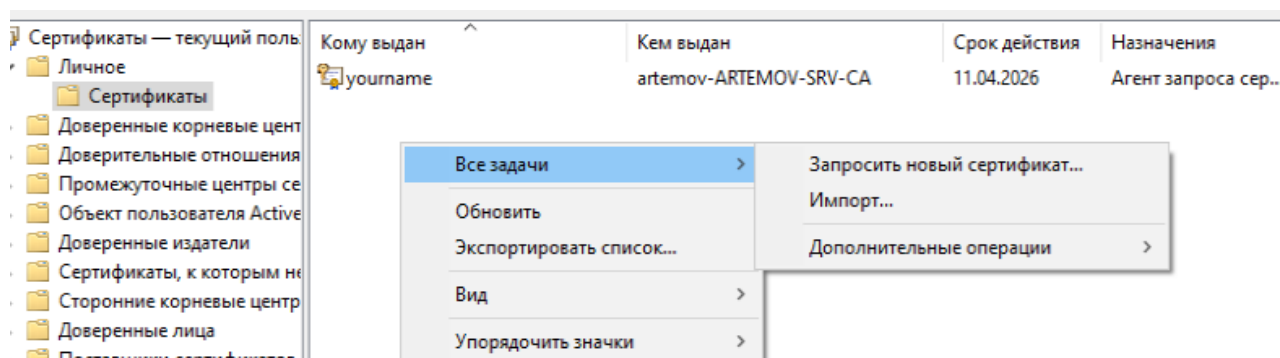


Рисунок 30 – папка «Сертификаты»

Нажимаем на синее сообщение под нашим созданным шаблоном «Пользователь familia.i.o.»

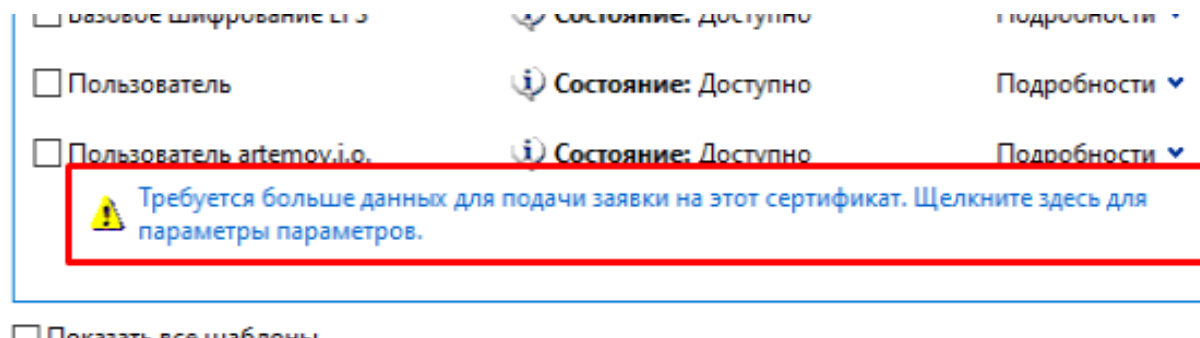


Рисунок 31 – данные для подачи заявки

Нажимаем на «Обзор» рядом с «Сертификатом подписи».

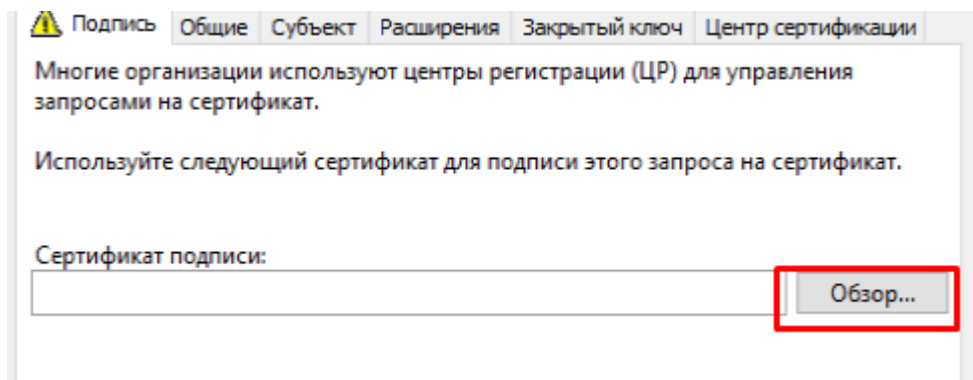


Рисунок 32 – кнопка «Обзор»

Появляется окно о подтверждении сертификата, жмем «ОК».

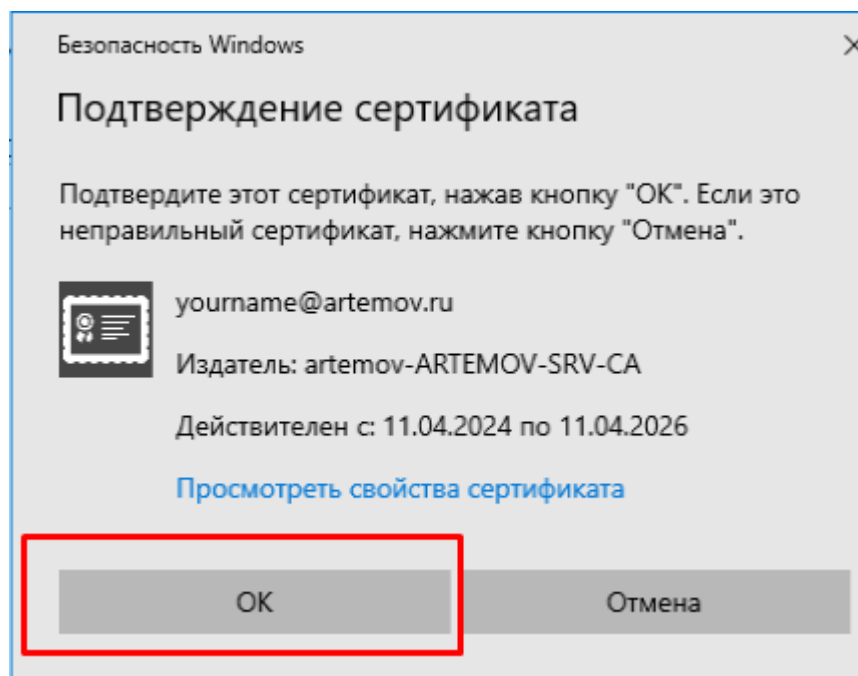


Рисунок 33 – окно подтверждения сертификата

После этого жмем «Применить» и «ОК».



Рисунок 34 – подтверждение



Теперь сообщения нет и можно делать заявку на сертификат созданного шаблона.

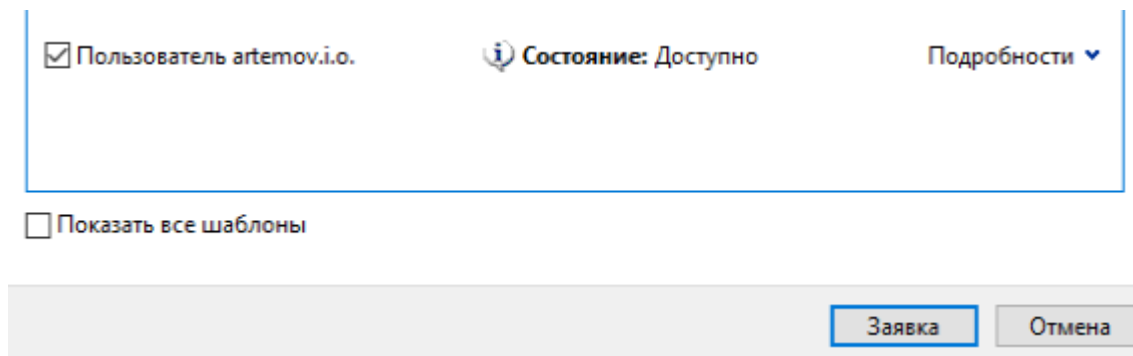


Рисунок 35 – заявка на сертификат

Появляется сообщение о подключении «Смарт-карты», жмем «Отмена» и радуемся жизни

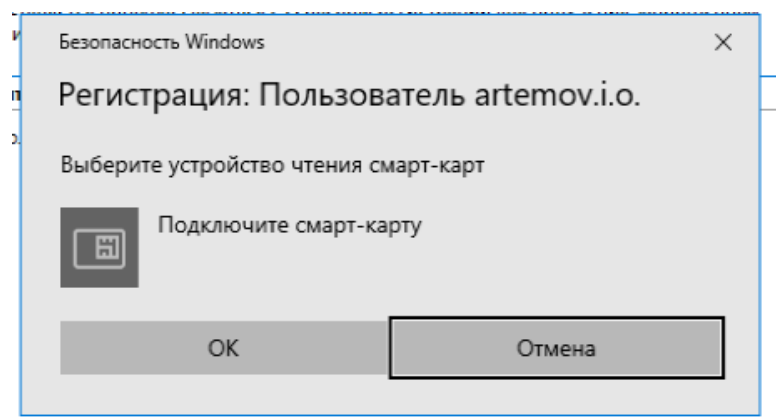


Рисунок 36 – подключение по смарт-карте

Возвращаемся на сервер, жмем «Локальный сервер» и включаем удаленный рабочий стол.

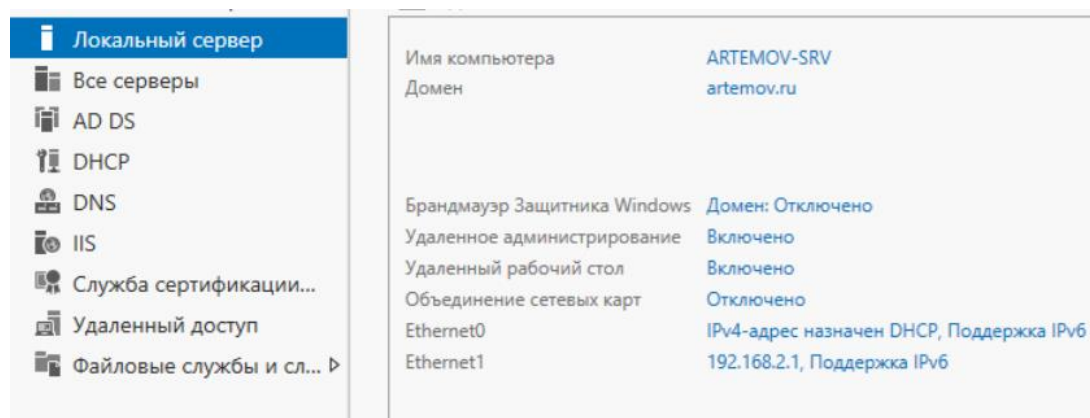


Рисунок 37 – локальный сервер

Открываем «Подключение к рабочему столу» на клиенте и в качестве компьютера пишем **полное доменное имя** сервера, а также пользователя «Администратор».

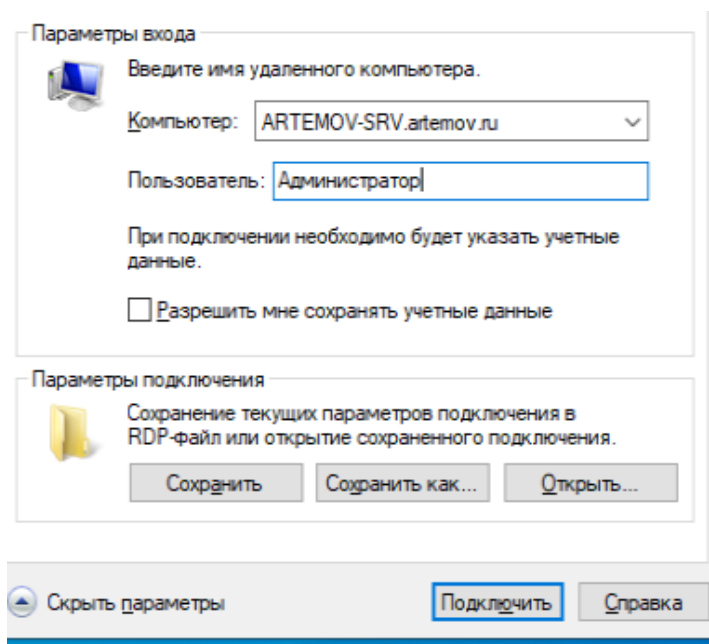


Рисунок 38 – подключение по RDP

После установки соединения в верхней панели появится значок замочка, нажав на который можно убедиться в защищенности соединения. В случае если его нет, попробуйте установить сертификат.

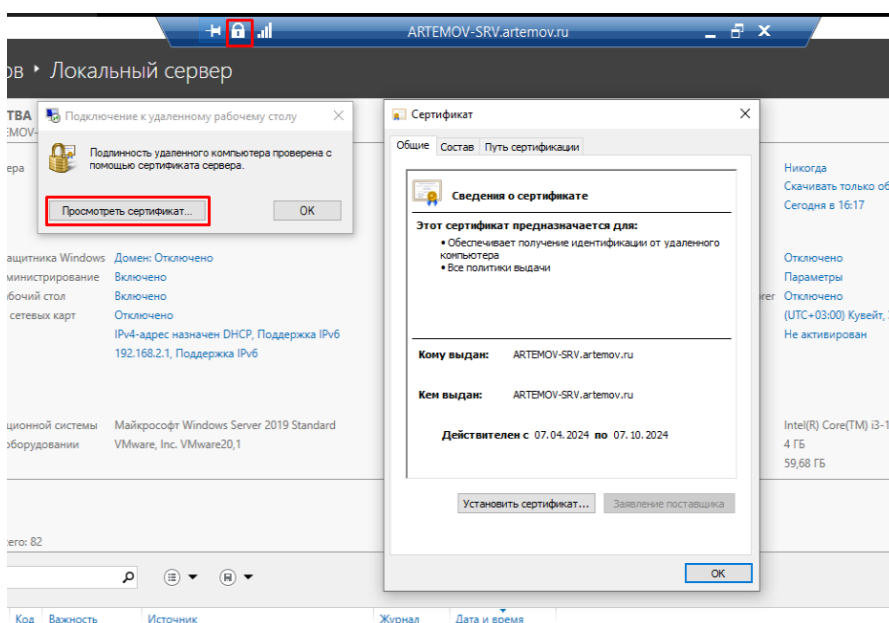


Рисунок 39 – успешное подключение