**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Лабораторная работа № 2

по дисциплине

«Защита электронного технологического документооборота»

«Создание центра сертификации (удостоверяющего центра)»

|  |  |  |
| --- | --- | --- |
| **Выполнил обучающийся**  Курс 5  Группа КИБ-012 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | Г.Е. Груздев |
|  |  |  |
| **Проверил** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | М.Ф. Соломатова |

Санкт-Петербург

2024

**Цель работы**

Изучение возможностей центра сертификации.

**Ход работы**

1. Изучить функции и архитектуру центра сертификации (ЦС).

Установить на компьютер виртуальную машину с серверной операционной системой.

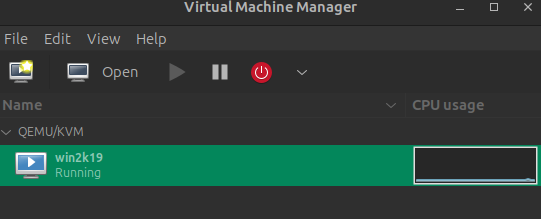


Рис. 1.1 – Установленная Windows Server 2019 на виртуальной машине.

1. Добавить серверу роль Active Directory Certificate Services с помощью оснастки Server Manager, которую можно запустить из раздела Administrative Tools в стартовом меню. В Server Manager раскрыть список ролей и выбрать добавление роли (Add Roles). В списке доступных ролей выбрать Active Directory Certificate Services.

На рисунке 2.1 показан процесс добавления роли:

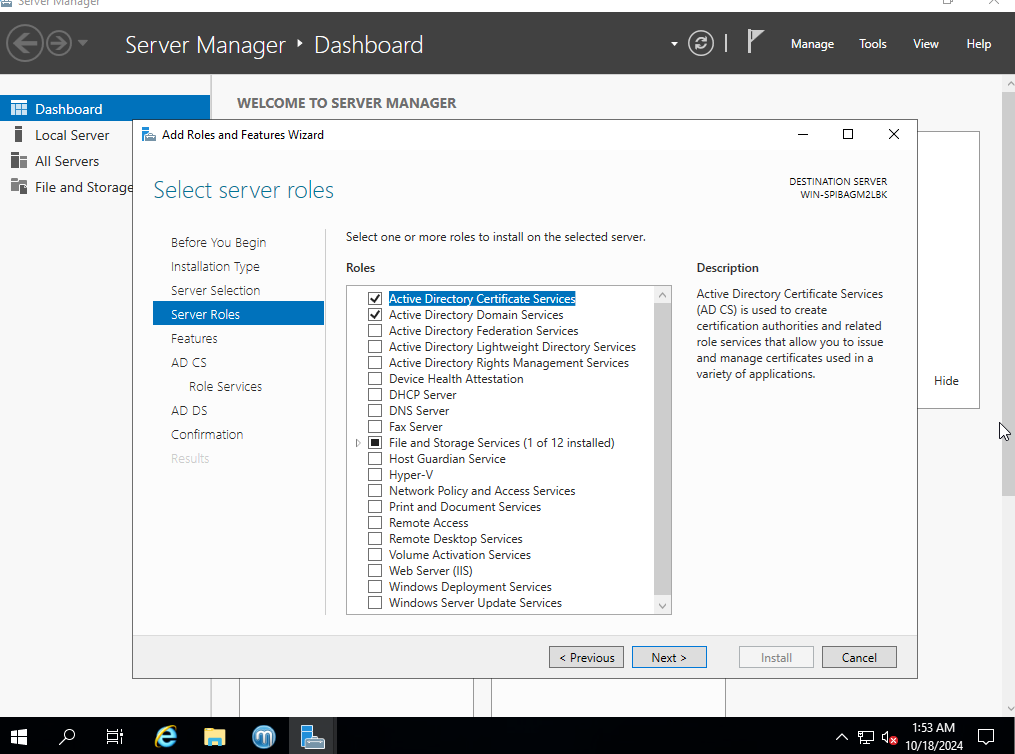


Рис 2.1. – Процесс добавления роли

1. Определить тип центра сертификации как корпоративный (Enterprise). Тип Certification Authority Enterprise может быть установлен только на сервер, являющийся членом домена, т.к. для его работы требуется служба каталога Active Directory. Так что сначала устнаовим Active Directory Domain Service. Certification Authority Standalone может работать вне домена, например, обрабатывая запросы пользователей, полученные через web-интерфейс. Определить иерархический тип ЦС – корневой (Root) или подчиненный (Subordinate). Создаваемый ЦС является первым и единственным, поэтому для него определен тип Root.

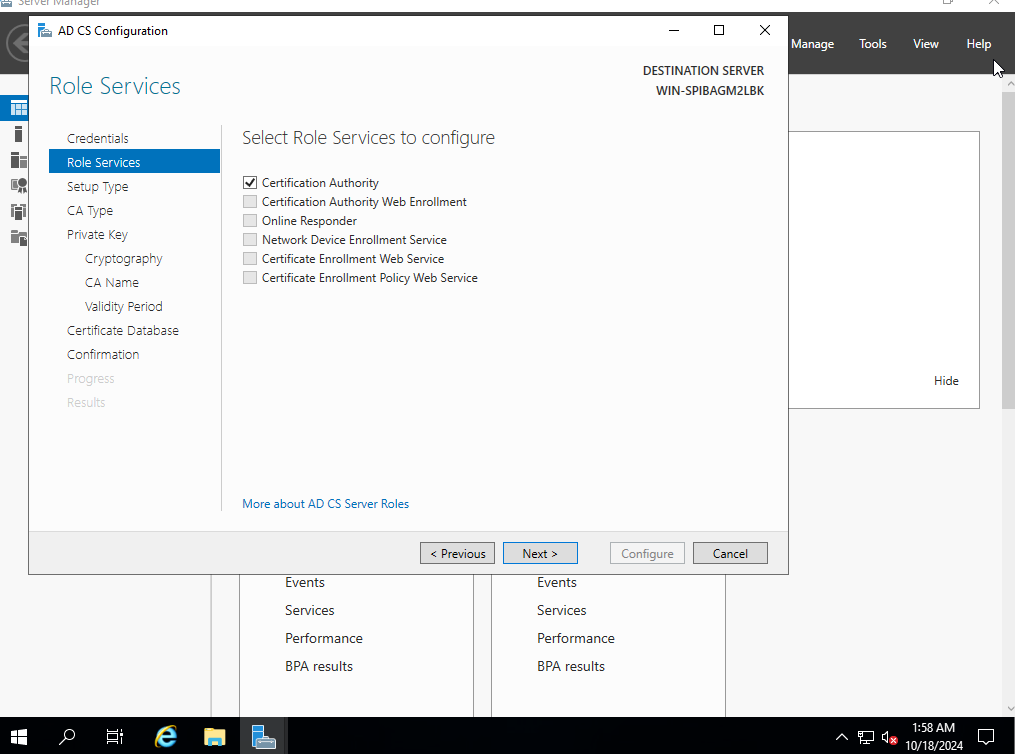


Рис. 3.1 – Определение варианта установки центра сертификации.

1. Настройка ключей шифрования. Создаваемый центр сертификации должен будет использовать при работе как минимум одну ключевую пару - открытый и секретный ключ (иначе он не сможет подписывать выпускаемые сертификаты). Поэтому необходимо определить, нужно ли создать новый секретный ключ или будет использоваться уже существующий (тогда надо будет указать, какой ключ использовать). В лабораторной работе надо создать новый ключ, для чего. требуется выбрать "криптографический провайдер" (программный модуль, реализующий криптоалгоритмы) и алгоритм хеширования. Предлагается использовать настройки по умолчанию. Необходимо также указать имя ЦС, размещение базы сертификатов и лог-файлов.

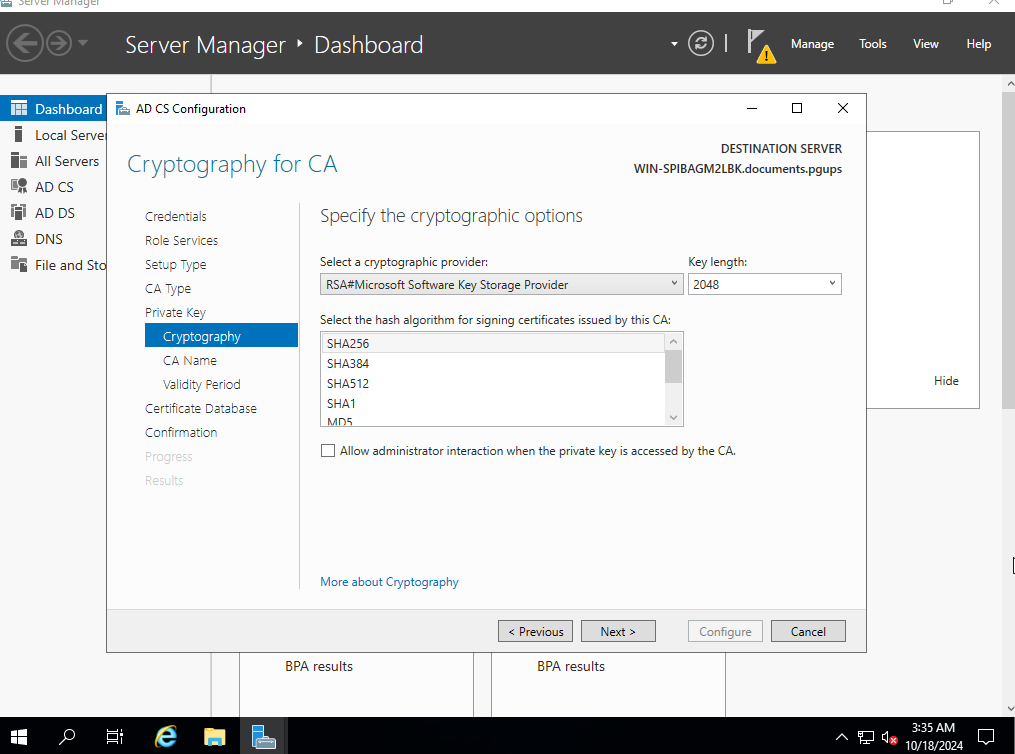


Рис. 4.1 – Настройка способа шифрования

1. Управление центром сертификации

Управлять работой ЦC можно из оснастки Certification Authority, которая должна появиться в разделе Administrative Tools. Просмотреть сделанные настройки в свойствах данного сервера (пункт Properties контекстного меню).

На закладке Policy Module (пункт Properties) проверить текущую настройку, определяющую порядок выдачи сертификатов. (Set the certificate request status to pending. The administrator must explicitly issue the certificate. / Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate.) Описать, какие шаблоны сертификатов (Certificate Templates) определены и для каких целей служит каждый тип сертификатов. Посмотреть, какие сертификаты выпущены (Issued Certificates), есть ли отозванные сертификаты (Revoked Certificates).

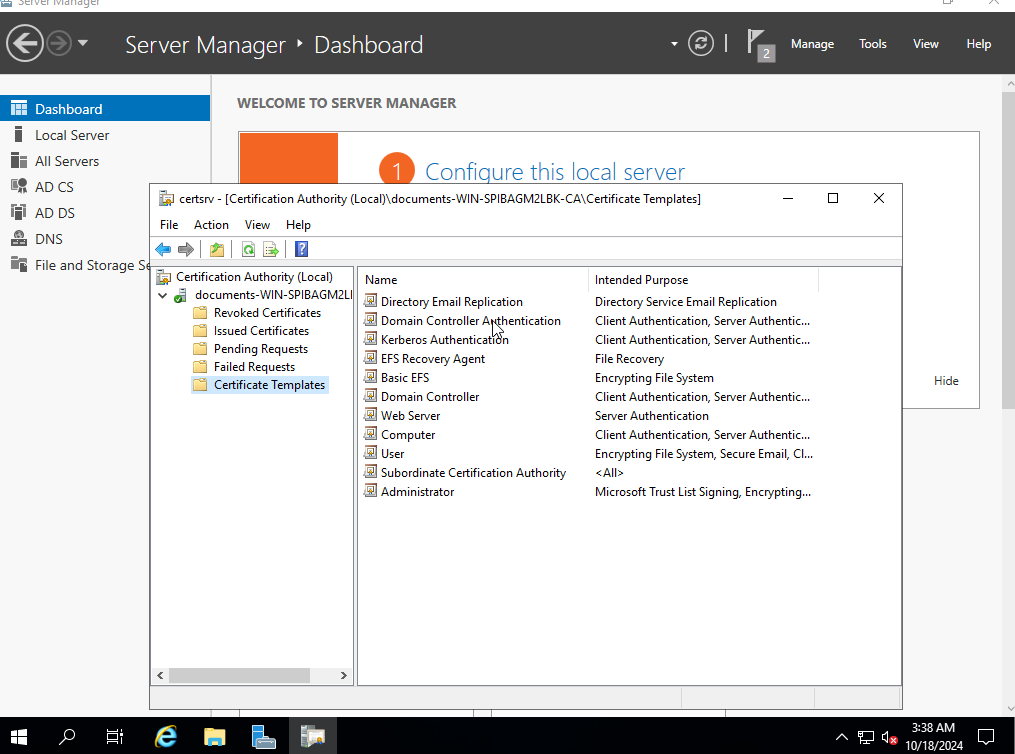


Рис. 5.1 — Шаблоны сертификатов

Выполнить процесс получения цифрового сертификата с помощью оснастки Certificates, в разделе сертификатов пользователя (Personal). Из перечня предложенных шаблонов сертификатов выберать User. Данный тип сертификатов может использоваться для шифрования файлов с помощью EFS, защиты электронной почты и аутентификации пользователей. Для пользователя будет сгенерирована ключевая пара, и на основе данных, взятых из базы службы Active Directory и шаблона, будет выпущен сертификат, удостоверяющий открытый ключ. Этот сертификат будет виден и в оснастке Certification Authority, в списке выпущенных данным сервером.

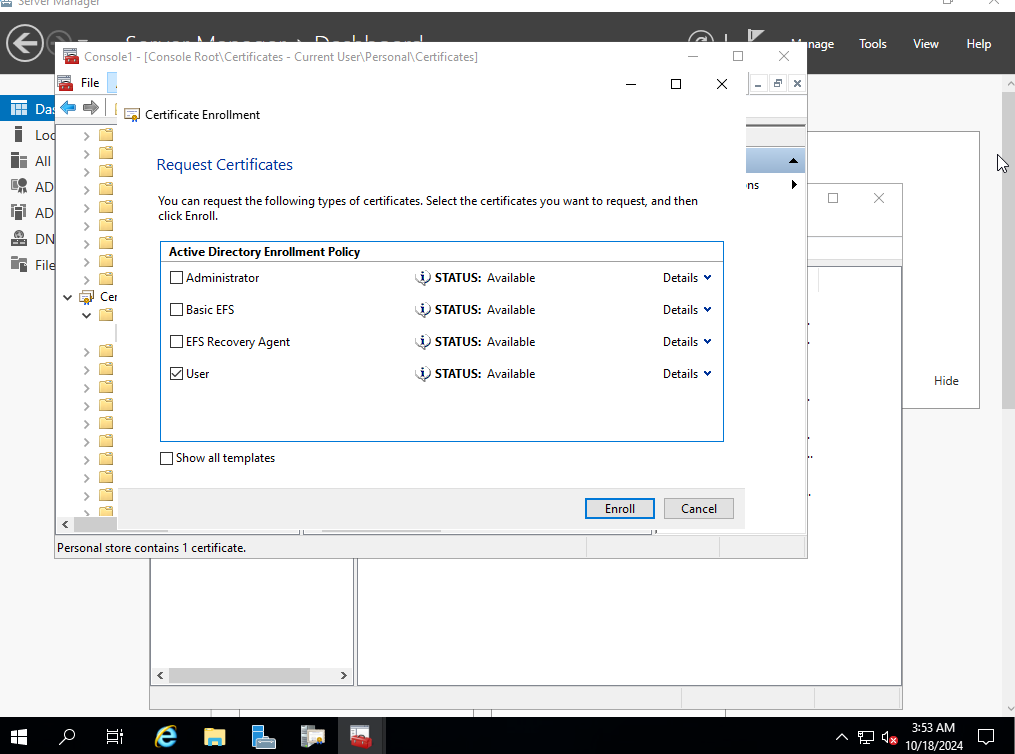


Рис. 5.2 – Запрос сертификата

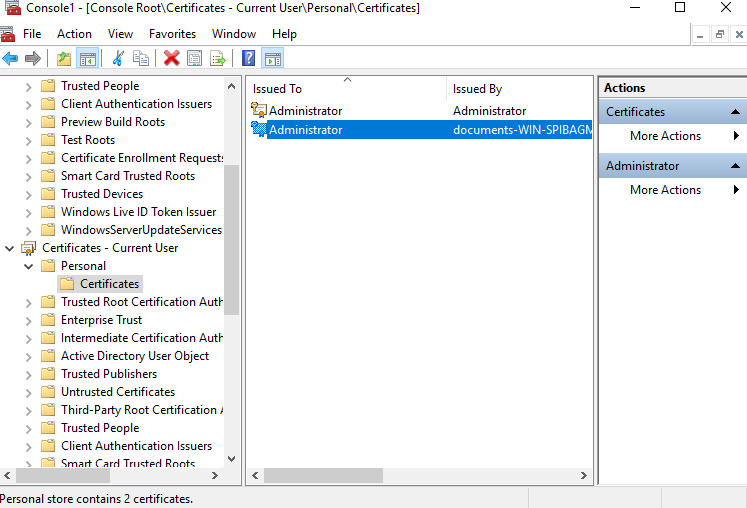


Рисунок 5.3 – Просмотр списка сертификатов

1. Изучить состав сертификата, его назначение.

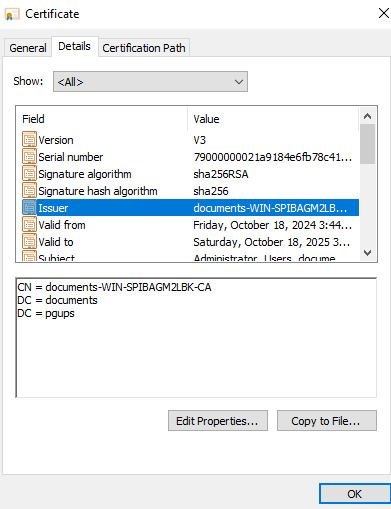


Рис.6.1 – Состав сертификата

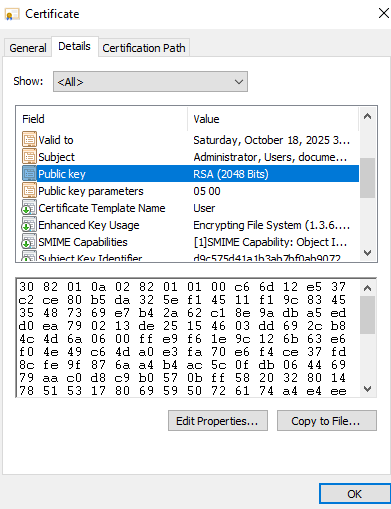


Рис.6.2 – Состав сертификата

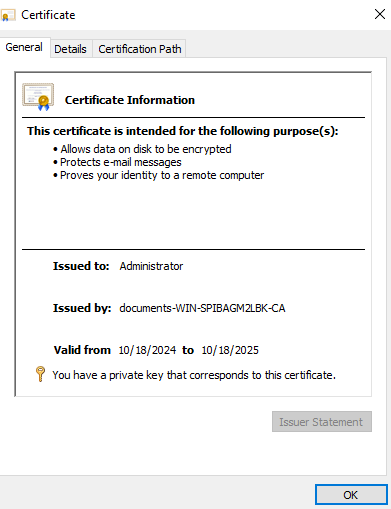


Рис.6.3 — Назначение сертификата

1. Выполнить экспорт сертификата (в оснастке Certificates выделить сертификат и в контекстном меню выберать All Tasks —> Export). Экспортировать можно только сертификат или сертификат вместе с секретным ключом (private key). Второй вариант надо использовать аккуратно, чтобы не раскрыть случайно секретный ключ шифрования. Такой тип экспорта нужен, если необходимо сохранить резервную копию ключевой пары и сертификата.



Рис.7.1 – Успешный экспорт сертификата