

Лабораторная работа 4

УСТАНОВКА И УПРАВЛЕНИЕ КОРНЕВЫМ ЦЕНТРОМ СЕРТИФИКАЦИИ

Цель лабораторной работы

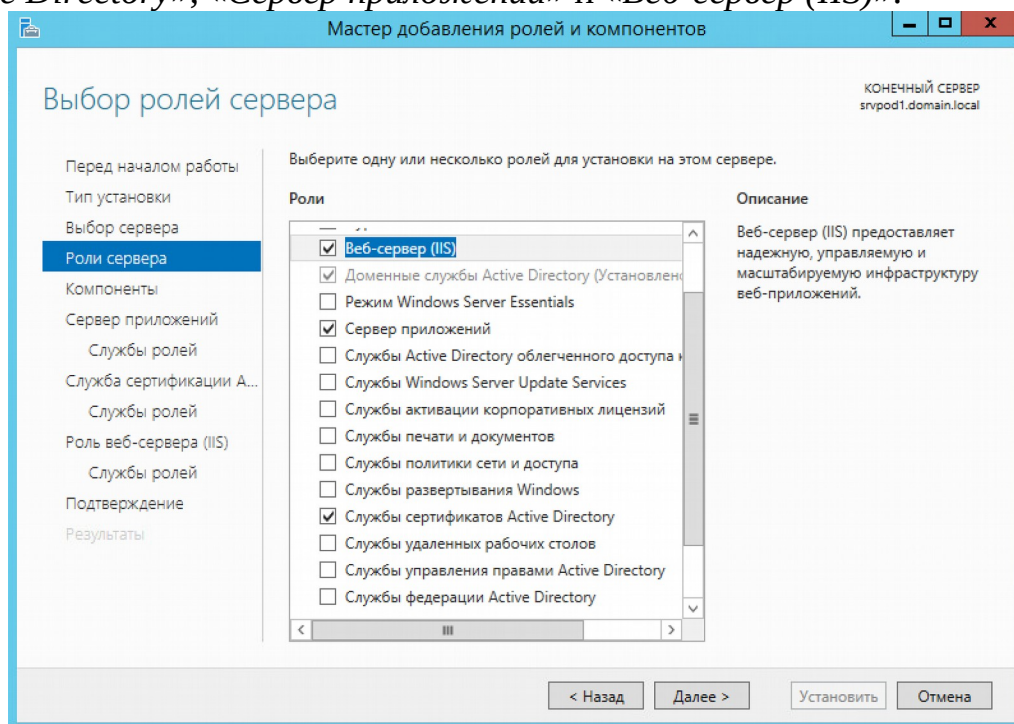
1. Установка центра сертификации.
2. Получения сертификатов посредством мастера запроса сертификатов.
3. Получения сертификатов посредством веб-интерфейса.

Используемое программное обеспечение

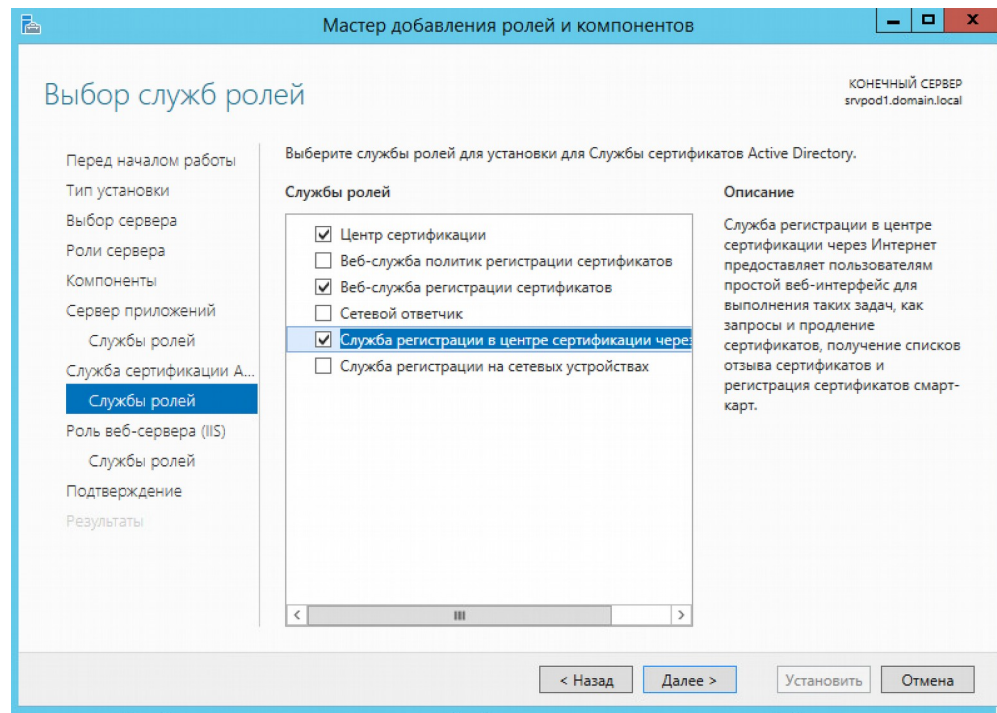
Для выполнения лабораторной работы используются ОС Windows Server 2012 и Windows 7.

Порядок выполнения работы

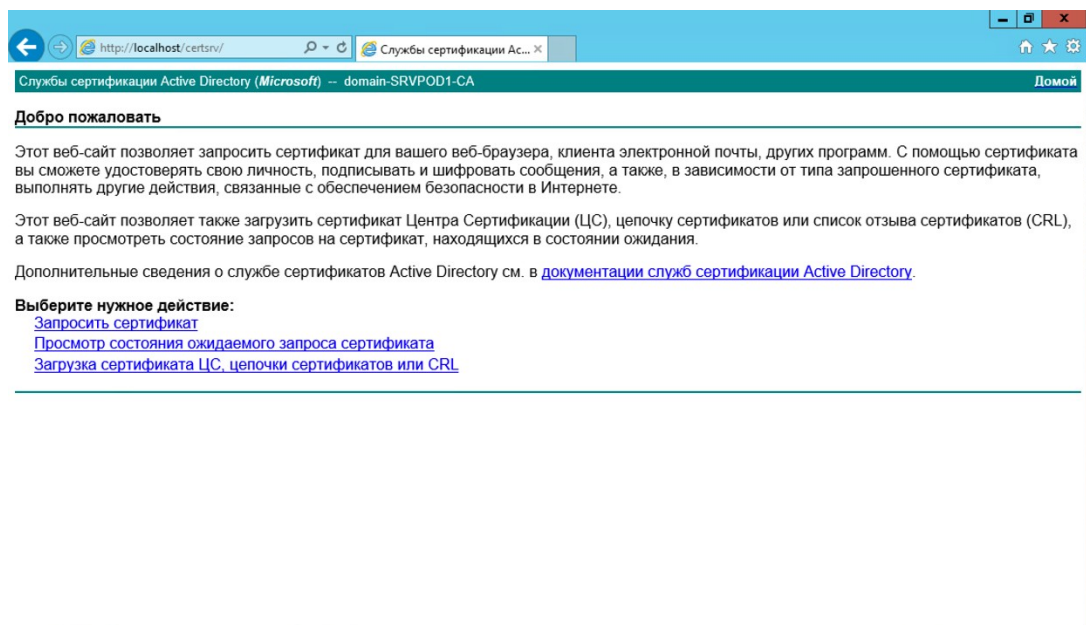
1. Подключиться по протоколу к Windows 7 и Windows Server 2012 R2.
2. Установить корневой, корпоративный Центр сертификации (ЦС) с крипто провайдером «RSA#Microsoft Software Key Storage Provider» и алгоритмом хэш «SHA256», при помощи добавления роли «Службы сертификатов Active Directory», «Сервер приложений» и «Веб-сервер (IIS)».



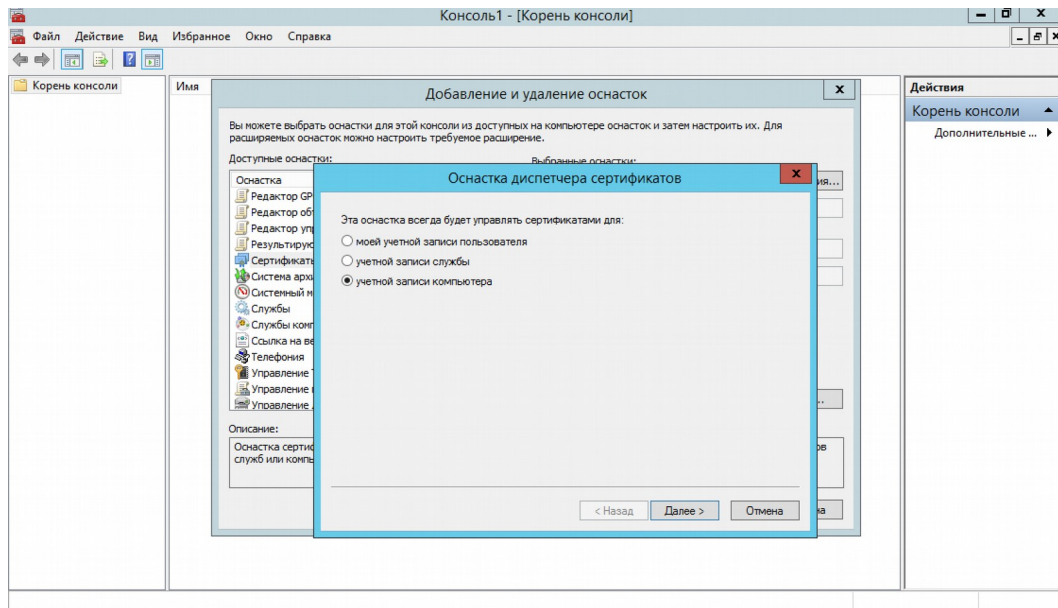
3. Все дополнительные настройки принять и продолжить установку.
4. Дополнительно указать роли служб сертификации: «Центр сертификации», «Веб-служба регистрации сертификатов» и «Служба регистрации в центре сертификации через Интернет».



5. Произвести настройку трех служб согласно заданным параметрам.
6. Если служба сертификация была установлена корректно, и корневой сертификат добавлен, АЦС сможет обратиться на Веб-сервис для создания запроса на выпуск сертификатов по адресу «<http://localhost/certsrv>» с сервера.

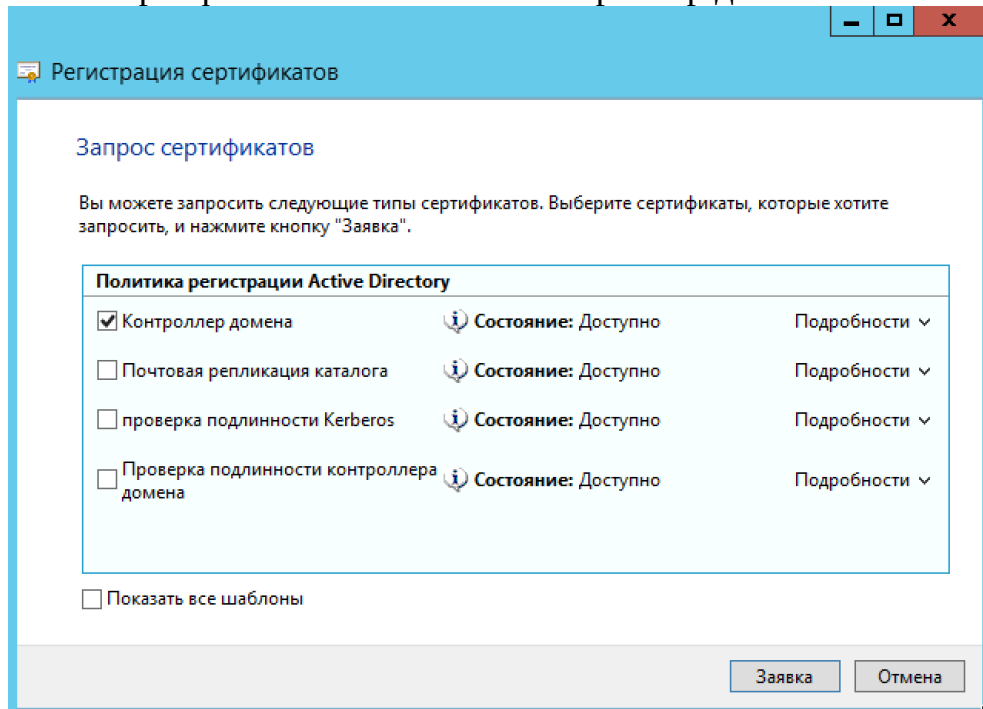


7. Перезагрузите *Windows Client*.
8. Откройте консоль «mmc» на Windows Server.
9. Добавить оснастку «Сертификаты» для всех учетных записей компьютера.

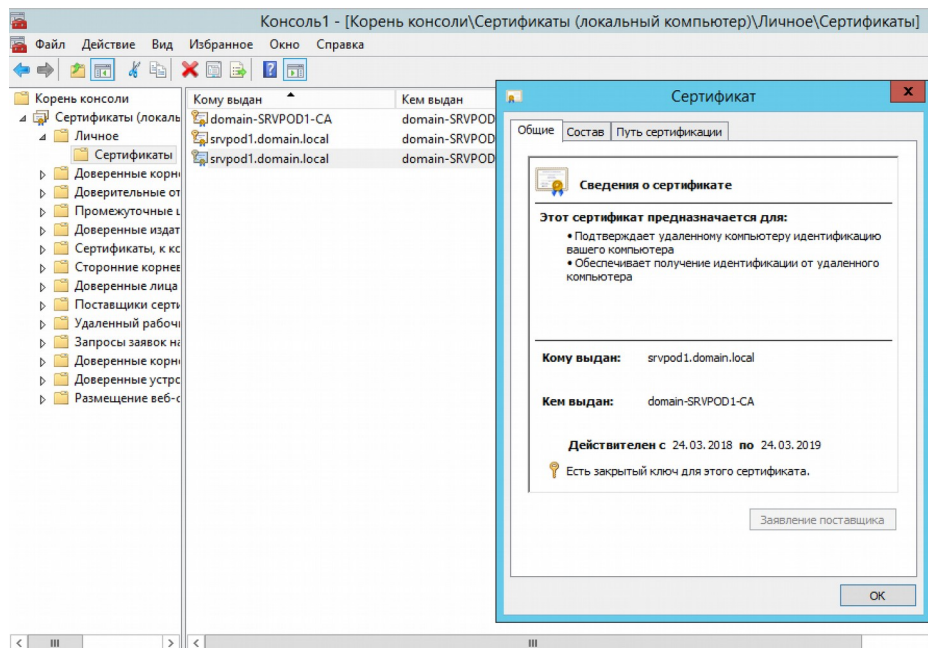


10. Нажав ПКМ на персональных сертификатах, запустить мастер запроса сертификатов (Все задачи → Запросить новый сертификат).

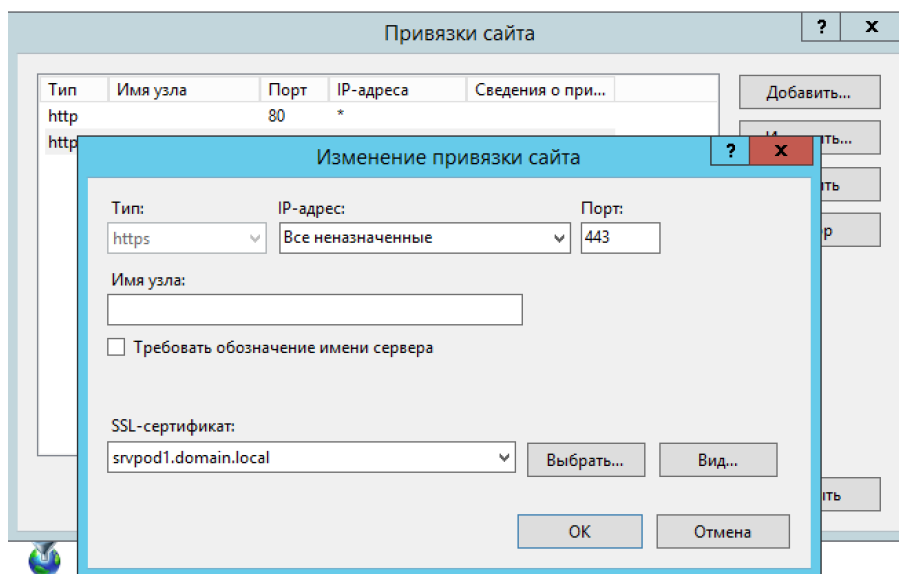
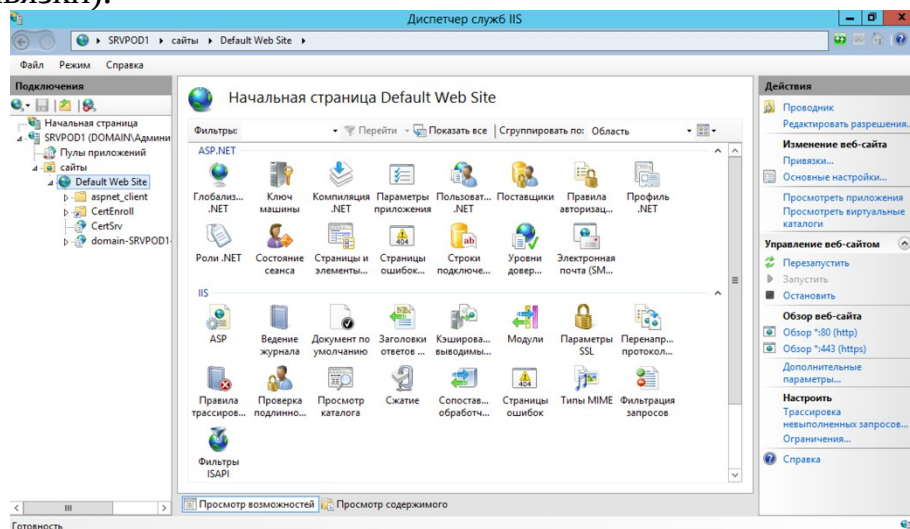
11. Запросить сертификат с шаблоном «Контроллер домена».



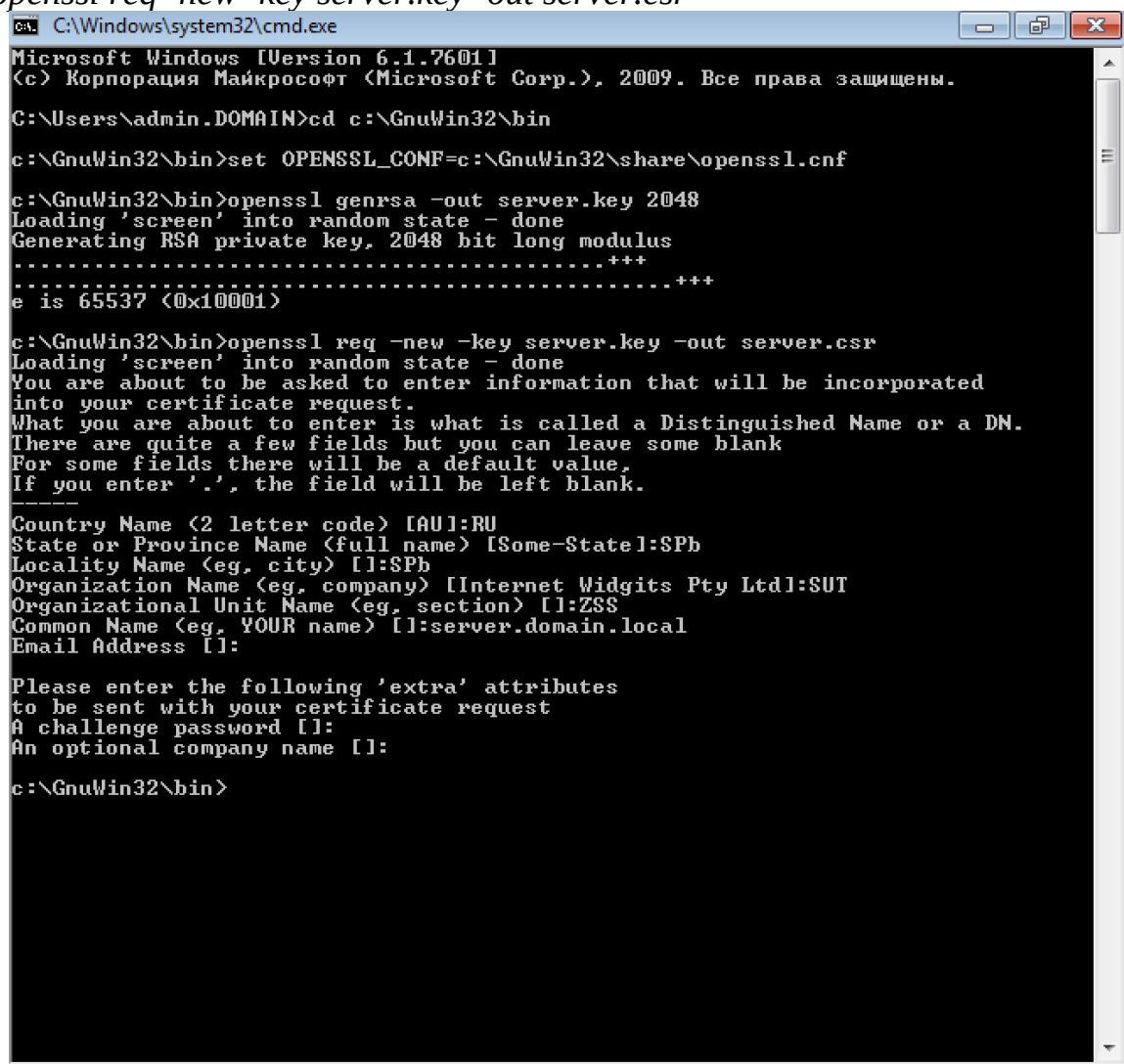
12. Проверить появление нового сертификата.



13. В оснастке «Диспетчер служб IIS» настроить протокол *TLS* для веб-сайта и использовать запрошенный ранее сертификат (*Default Web Site* → Привязки).



14. Проверить результат работы на *Windows Client* в браузере *Internet Explorer* по вашему адресу (например, «<https://srvpod1.domain.local/certsrv>»). В качестве логина и пароля использовать данные текущего пользователя.
15. На *Windows 7 Client* установите *Notepad ++* и *openssl*.
16. *Openssl* установите по адресу «*C:\GnuWin32*».
17. После установки, запустить консоль и перейти в каталог «*C:\GnuWin32\bin*».
18. Выполнить команды:
set OPENSSL_CONF=C:\GnuWin32\share\openssl.cnf
openssl genrsa -out server.key 2048
openssl req -new -key server.key -out server.csr



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\admin.DOMAIN>cd c:\GnuWin32\bin

c:\GnuWin32\bin>set OPENSSL_CONF=c:\GnuWin32\share\openssl.cnf

c:\GnuWin32\bin>openssl genrsa -out server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
e is 65537 (0x10001)

c:\GnuWin32\bin>openssl req -new -key server.key -out server.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-Statel]:SPb
Locality Name (eg, city) []:SPb
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SUT
Organizational Unit Name (eg, section) []:ZSS
Common Name (eg, YOUR name) []:server.domain.local
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

c:\GnuWin32\bin>
```

19. Открыть файл *C:\GnuWin32\bin\server.csr* с помощью *Notepad ++*.


```
server.csr
1 -----BEGIN CERTIFICATE REQUEST-----
2 MIICqTCCAQECAQAwZDELMakGA1UEBhMCU1UxDDAKBgNVBAgTA1NQYjEMMAoGA1UE
3 BxMDU1B1MQwwCgYDVQQKEwNTVVVQxNDjAMBgNVBAStBWRvbWVuMRswGQYDVQQDExJz
4 ZXJ2ZXIuZG9tZW4ubG9jYWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
5 AQDFUJbsjWLYcS+A9JLexzMu54kOBBD2maCdJKe1LRSpRsvIMGNK33sKwSrH5e6A
6 Ja0qseUv/tD87YQbtkNu5xtKNYpIeh1S2/f1PlDDE0XdZh9JeTpOAdPnf0x+XTkN
7 hftcqhUI1YjmephL17Sdx6ZvDucoFSxmdi5727Ey6rGdcjY7Y9BuwuTMwg7qgKhX
8 McjCGywanIAITEJt9GqoK1DCshGN0TsQ9zL2YF7Id472Q74T/oWjy5zy13VJt3F
9 NqwJYhgFXLZToPBivMW80Np8H8I/UJqy447AccaQBmThrLGjrssvjbwkX3Vn2GWN
10 fna1LW59C2SYy83v2nCeH2A/AgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEApUbX
11 lqcEfCIQEmvzLjZ271UwKUugFKur3oJvVN1AaEdyYcE6wFTPUEI2CpMPqeXSmN05
12 1HRLIrR+Se0BpMKJwXm+HGJpwSk/deIG9wWYGM0DIuXzKCBd2P2JrfAkVTh783Ix
13 Zjd5Fca6n8T5n5KDpP7yTs+Btv3WuKxWjf0AdlyDYrY7+swiLV/LmI5SVV3X15Hp
14 jrqEu7OXpa8hh1CoBaq7Zp54ETb6GD9THTWrsTVLL1uV8bdA/yNYCwxdyJvwS+L
15 191YMP8bVmBY1q09hfkfKtCt1Cfm61kNRyMal5qG6x0sAIouPLNR1LdMNdW+FP38
16 hK13CyXr8jETmJDiVA==
17 -----END CERTIFICATE REQUEST-----
18
```

20. С помощью *Internet Explorer* перейти по адресу ЦС (например, «<https://srvpod1.domain.local/certsrv>»). Использовать логин и пароль Администратора.
21. Запросить сертификат используя текстовый запрос (Запроса сертификата → Расширенный запрос сертификата → Выдать запрос, используя base-64...).
22. В поле для ввода запроса скопируйте содержимое файла *server.csr* и выберете шаблон Веб-сервер.

Службы сертификации Active Directory (Microsoft) -- domain-SRVPOD1-CA [Домой](#)

Выдача запроса на сертификат или на обновление сертификата

Чтобы выдать сохраненный запрос к ЦС, вставьте base-64-шифрованный запрос сертификата PKCS #10 или запрос обновления PKCS #7, созданный в внешнем источнике (например, веб-сервером) в поле "Сохраненный запрос".

Сохраненный запрос:

Base-64-шифрованный запрос сертификата (CMS или PKCS #10 или PKCS #7):
-----BEGIN CERTIFICATE REQUEST-----
MIICqTCCAQECAQAwZDELMakGA1UEBhMCU1UxDDAKBgNVBAgTA1NQYjEMMAoGA1UE
BxMDU1B1MQwwCgYDVQQKEwNTVVVQxNDjAMBgNVBAStBWRvbWVuMRswGQYDVQQDExJz
ZXJ2ZXIuZG9tZW4ubG9jYWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDFUJbsjWLYcS+A9JLexzMu54kOBBD2maCdJKe1LRSpRsvIMGNK33sKwSrH5e6A
Ja0qseUv/tD87YQbtkNu5xtKNYpIeh1S2/f1PlDDE0XdZh9JeTpOAdPnf0x+XTkN
hftcqhUI1YjmephL17Sdx6ZvDucoFSxmdi5727Ey6rGdcjY7Y9BuwuTMwg7qgKhX
McjCGywanIAITEJt9GqoK1DCshGN0TsQ9zL2YF7Id472Q74T/oWjy5zy13VJt3F
NqwJYhgFXLZToPBivMW80Np8H8I/UJqy447AccaQBmThrLGjrssvjbwkX3Vn2GWN
fna1LW59C2SYy83v2nCeH2A/AgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEApUbX
lqcEfCIQEmvzLjZ271UwKUugFKur3oJvVN1AaEdyYcE6wFTPUEI2CpMPqeXSmN05
1HRLIrR+Se0BpMKJwXm+HGJpwSk/deIG9wWYGM0DIuXzKCBd2P2JrfAkVTh783Ix
Zjd5Fca6n8T5n5KDpP7yTs+Btv3WuKxWjf0AdlyDYrY7+swiLV/LmI5SVV3X15Hp
jqEu7OXpa8hh1CoBaq7Zp54ETb6GD9THTWrsTVLL1uV8bdA/yNYCwxdyJvwS+L
191YMP8bVmBY1q09hfkfKtCt1Cfm61kNRyMal5qG6x0sAIouPLNR1LdMNdW+FP38
hK13CyXr8jETmJDiVA==
-----END CERTIFICATE REQUEST-----

Шаблон сертификата:

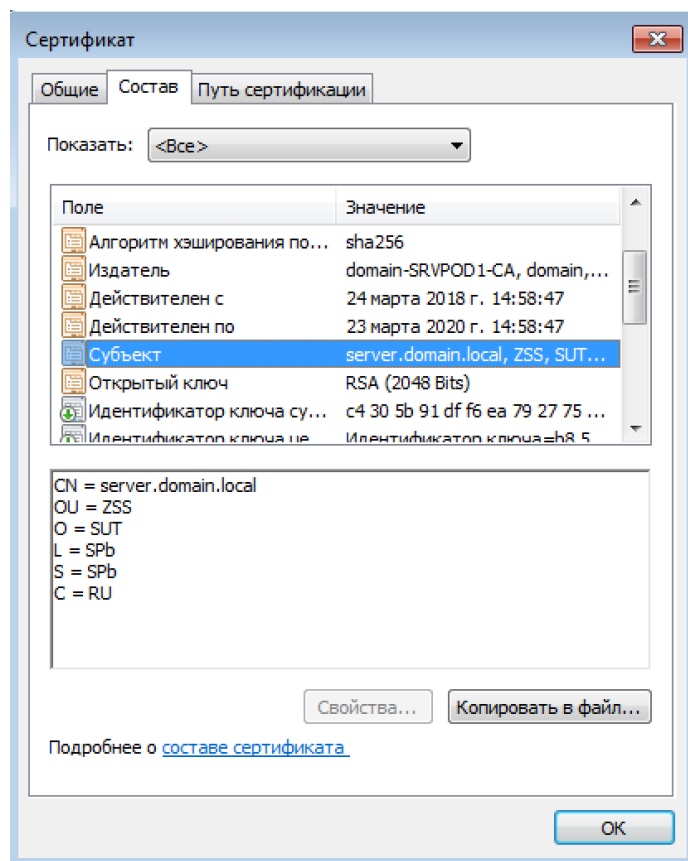
Веб-сервер

Дополнительные атрибуты:

Атрибуты:

Выдать >

23. Скачайте сертификат и просмотрите его содержимое.



Отчет должен содержать

1. Титульный лист.
2. Текст задания.
3. Схема сети.
4. Скриншоты выполненных действий по пунктам 5-23.
5. Выводы.