PS C:\Windows\system32> cd **C:\OpenSSL-Win64\bin**

PS C:\OpenSSL-Win64\bin> **.\openssl genrsa -out root.key**

PS C:\OpenSSL-Win64\bin> **.\openssl req -x509 -new -nodes -key root.key -sha256 -days 365 -out root.crt -config openssl-1.cnf -subj "/C=RU/ST=RB/L=Ufa/O=IB/OU=IT/CN=root/emailAddress=root@demo.lab"**

PS C:\OpenSSL-Win64\bin> **.\openssl.exe genrsa -out iwtm.key**

PS C:\OpenSSL-Win64\bin> **.\openssl.exe req -new -sha256 -config openssl-1.cnf -key iwtm.key -out iwtm.csr**

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-State]:**RB**

Locality Name (eg, city) []:**Ufa**

Organization Name (eg, company) [Internet Widgits Pty Ltd]:**IB**

Organizational Unit Name (eg, section) []:**IT**

Common Name (e.g. server FQDN or YOUR name) []:**root**

Email Address []:**iwtm@demo.lab**

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []**:xxXX1234**

An optional company name []:**iwtm**

PS C:\OpenSSL-Win64\bin> **./openssl.exe req -text -noout -in iwtm.csr**

Certificate Request:

Data:

Version: 1 (0x0)

Subject: C = RU, ST = RB, L = Ufa, O = IB, OU = IT, CN = root, emailAddress = iwtm@demo.lab

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:c7:c1:3a:0e:17:c7:96:f8:72:8a:85:c4:4f:19:

39:c7:19:d2:53:49:40:4d:57:81:68:95:b2:c0:93:

b6:a2:29:7d:2b:b8:7b:8f:db:53:bf:82:fc:6e:38:

55:58:c8:a5:7b:dd:5d:34:5e:d5:96:f7:4e:4e:73:

80:c5:d3:59:b6:c8:c0:8b:a0:d1:bb:c9:8f:b9:0e:

6e:29:31:db:a2:d8:ff:e4:7e:62:e2:07:17:da:d6:

2b:9e:61:b7:5c:4b:b9:73:6b:1c:fe:9c:67:25:42:

2d:f2:c7:62:b4:8c:cb:f3:34:e3:1a:c9:3d:62:ab:

46:ed:ef:3d:dd:7c:f0:be:6e:d0:62:c1:2b:bd:37:

51:4c:1b:51:51:75:1e:ae:fb:b6:c6:19:84:90:2d:

19:2b:92:88:c0:9e:33:0d:fe:08:c7:09:28:53:e3:

a5:53:98:f3:7e:d6:81:7b:a2:ce:b2:e2:c7:62:32:

c5:54:3d:ee:23:6e:5f:f4:28:74:40:a8:de:58:5f:

de:58:d1:c9:bf:6b:d4:34:1d:aa:07:76:92:bd:9b:

7b:2b:0d:b9:56:a5:af:55:7e:64:3e:c2:52:e6:53:

e6:68:a5:ac:d0:be:e4:75:72:e3:92:20:7f:4b:14:

d4:9f:82:04:ec:3b:05:7d:24:47:34:d9:6b:ab:0f:

79:e5

Exponent: 65537 (0x10001)

Attributes:

unstructuredName :iwtm

challengePassword :xxXX1234

Requested Extensions:

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

1d:fa:e6:d4:4c:fd:51:eb:3b:9b:cd:5a:12:b6:3e:20:58:97:

dc:ad:7b:5f:17:b7:ff:4c:dd:5d:47:eb:55:8f:61:d0:75:53:

3e:a2:89:69:5c:c6:eb:92:e7:9b:b7:0b:51:d5:45:a3:ab:28:

41:59:00:87:90:6e:82:33:66:a0:d5:9a:b4:0c:b9:a3:9e:68:

0c:b3:8f:5f:4f:6d:8a:d5:d7:b3:fb:19:e4:d1:5b:a0:49:a5:

dc:49:8c:ce:4b:fe:f2:06:51:fb:69:c4:83:9d:1a:f1:80:08:

a7:b5:18:2e:3d:4d:ca:0b:25:59:a5:10:a5:b5:bf:2a:1a:bf:

da:b1:9b:ca:e4:38:70:dc:21:67:7f:09:07:92:13:e3:ba:d2:

2d:eb:2d:ef:62:dd:c7:58:b9:d7:e3:80:d7:1a:54:a5:46:47:

f0:24:be:72:15:04:94:ed:4c:50:ee:a4:02:8f:03:45:45:21:

3c:4e:3b:5c:56:a0:5e:02:b6:af:c0:da:12:ee:b2:b7:ea:f3:

b9:d7:f2:22:0b:19:d4:52:28:e7:dc:34:17:d3:07:ee:64:0c:

43:38:91:60:f2:13:51:cd:1a:d7:e2:ce:48:ef:e7:4c:48:08:

18:c1:d5:19:06:b8:2c:91:0e:b2:3c:86:52:42:f2:39:07:d5:

b0:ce:9b:62

PS C:\OpenSSL-Win64\bin> **.\openssl ca -config opennssl-1.cnf -extensions v3\_intermediate\_ca -days 2650 -batch -in iwtm.csr -out iwtm.crt -subj "/C=RB/ST=RB/L=Ufa/O=UKRTB/OU=IB/CN=iwtm/emailAddress=iwtm@demo.lab"**

Using configuration from opennssl-1.cnf

Can't open "opennssl-1.cnf" for reading, No such file or directory

D0080000:error:80000002:system library:BIO\_new\_file:No such file or directory:crypto\bio\bss\_file.c:67:calling fopen(ope

nnssl-1.cnf, r)

D0080000:error:10000080:BIO routines:BIO\_new\_file:no such file:crypto\bio\bss\_file.c:75:

PS C:\OpenSSL-Win64\bin> **.\openssl x509 -req -in "iwtm.csr" -CA "root.crt" -CAkey "root.key" -CAcreateserial -out "iwtm.crt" -extensions v3\_req -extfile "openssl-1.cnf" -subj "/C=RU/ST=RB/L=Ufa/O=IB/OU=IT/CN=iwtm/emailAddress=iwtm@demo.lab"**

Certificate request self-signature ok

subject=C = RU, ST = RB, L = Ufa, O = IB, OU = IT, CN = root, emailAddress = iwtm@demo.lab

PS C:\OpenSSL-Win64\bin> .\openssl.exe genrsa -out arm.key

PS C:\OpenSSL-Win64\bin> .\openssl req -new -key arm.key -out arm.csr -config openssl-1.cnf

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-State]:**RB**

Locality Name (eg, city) []:**Ufa**

Organization Name (eg, company) [Internet Widgits Pty Ltd]:**IB**

Organizational Unit Name (eg, section) []:**IT**

Common Name (e.g. server FQDN or YOUR name) []:**iwtm**

Email Address []:**arm@demo.lab**

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:**xxXX1234**

An optional company name []:**arm**

PS C:\OpenSSL-Win64\bin> **.\openssl x509 -req -in arm.csr -CA iwtm.crt -CAkey iwtm.key -CAcreateserial -out arm.crt -extensions v3\_req -extfile openssl-1.cnf -subj "/C=RU/ST=RB/L=Ufa/O=UKRTB/OU=IT/CN=arm/emailAddress=arm@demo.lab"**

Certificate request self-signature ok

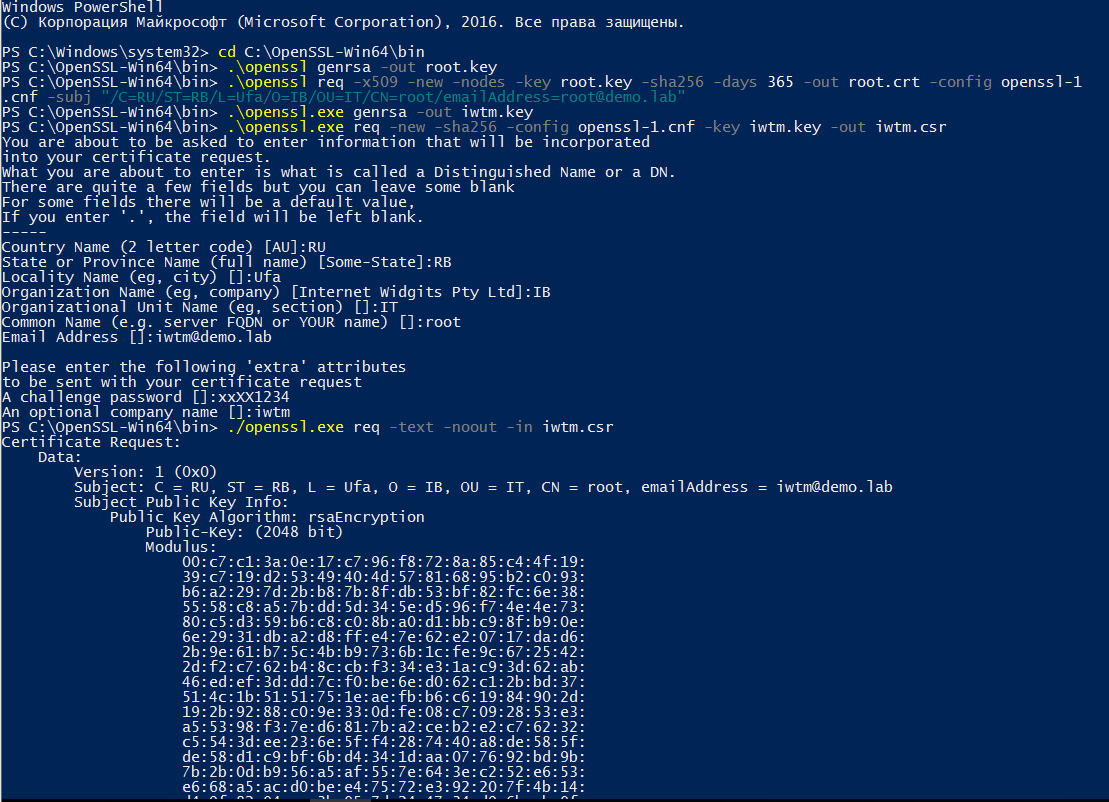
subject=C = RU, ST = RB, L = Ufa, O = IB, OU = IT, CN = iwtm, emailAddress = arm@demo.lab

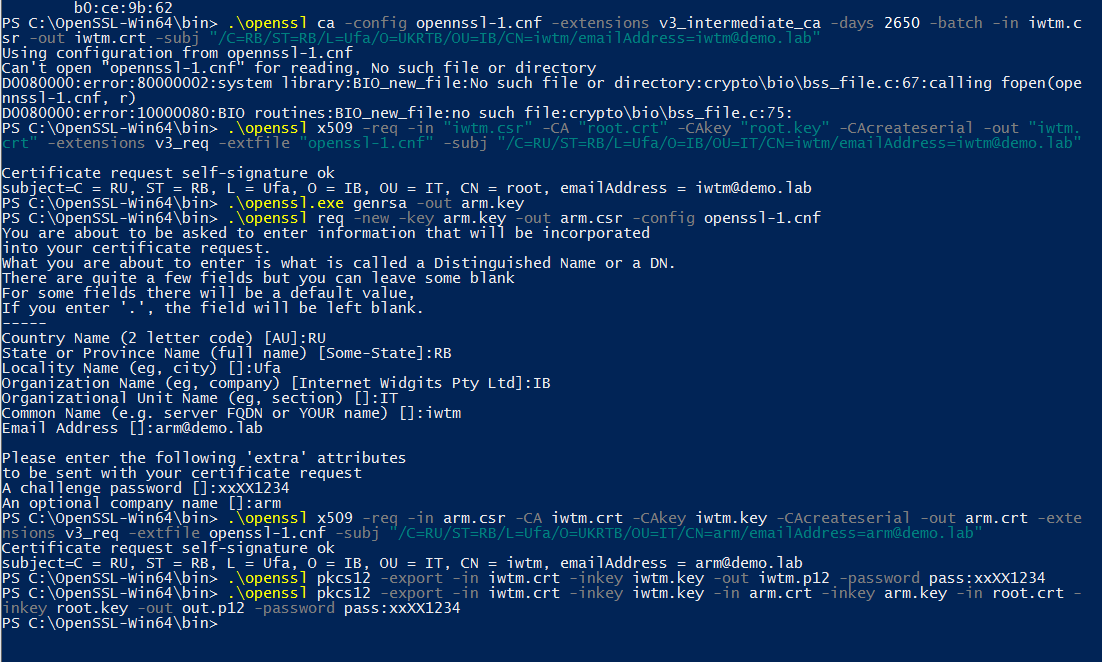
PS C:\OpenSSL-Win64\bin> **.\openssl pkcs12 -export -in iwtm.crt -inkey iwtm.key -out iwtm.p12 -password pass:xxXX1234**

PS C:\OpenSSL-Win64\bin> **.\openssl pkcs12 -export -in iwtm.crt -inkey iwtm.key -in arm.crt -inkey arm.key -in root.crt -**

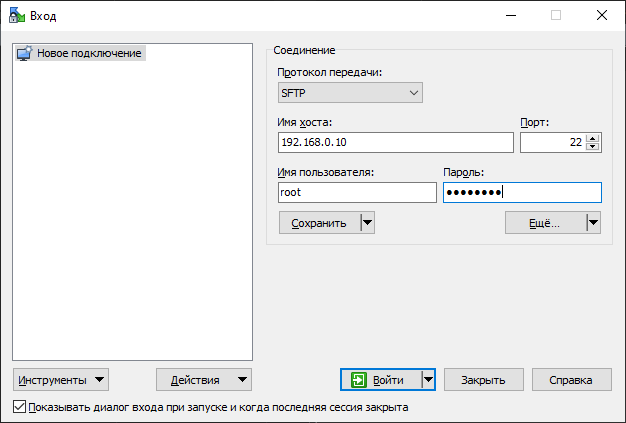
**inkey root.key -out out.p12 -password pass:xxXX1234**

PS C:\OpenSSL-Win64\bin>

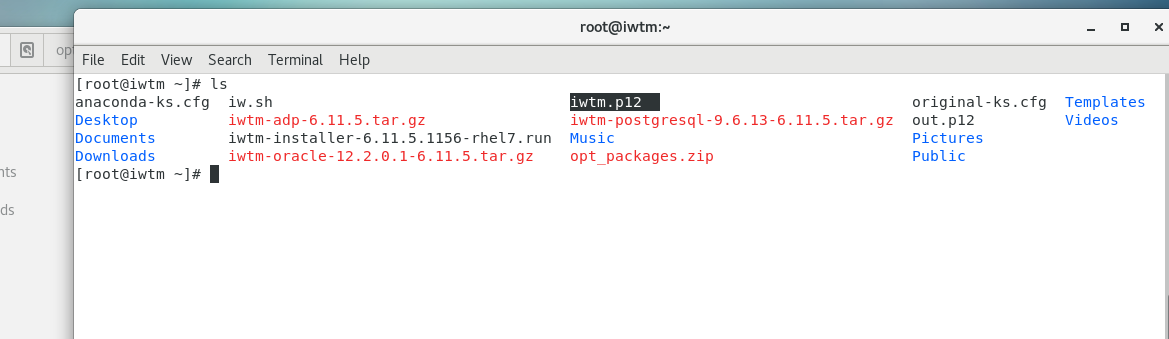




Подключаемся к ТМ через WinCSP

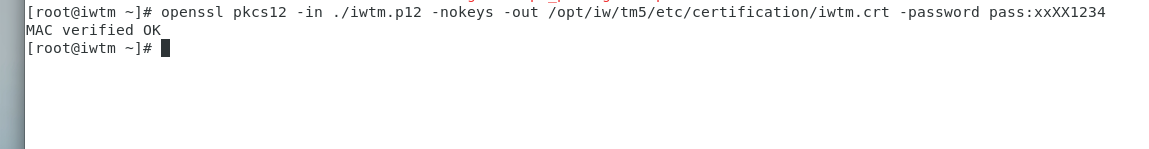


Перекидываем наш сертификат

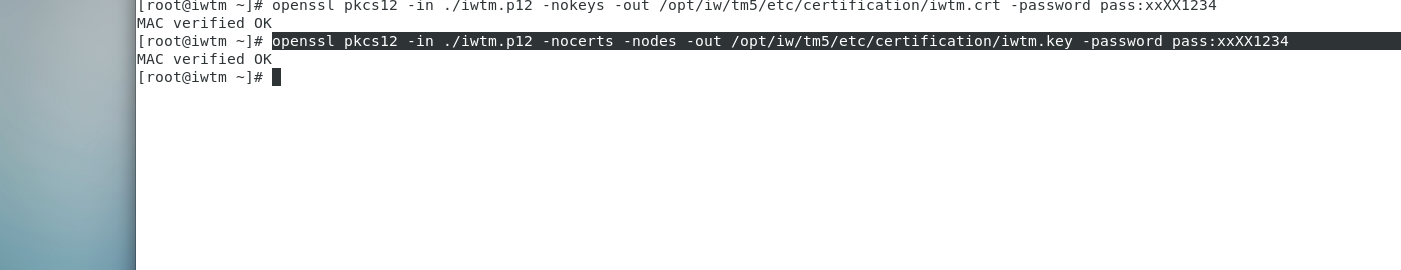


Извлекаем из сертификата публичный ключ (считаем, что pfx-ключ находится в папке root)

Извлекаем из сертификата закрытый ключ



**openssl pkcs 12 -in ./iwtm.p12 -nokeys -out /opt/iw/tm5/etc/certification/iwtm.crt -password pass:xxXX1234**

****

**openssl pkcs 12 -in ./iwtm.p12 -nocerts -nodes -out /opt/iw/tm5/etc/certification/iwtm.key -password pass:xxXX1234**

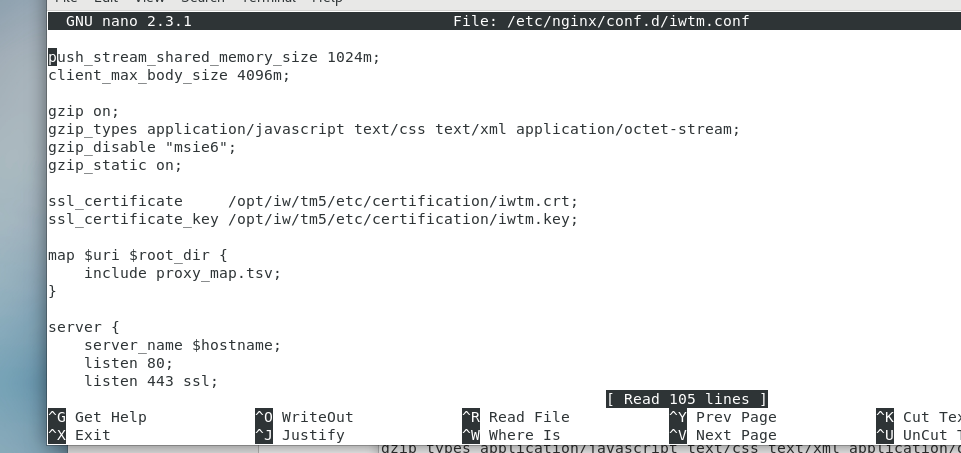
Переносим полученные файлы в папку сертификатов



**mv /root/iwtm.cer /opt/iw/tm5/etc/certification**

**mv /root/iwtm.key /opt/iw/tm5/etc/certification**

Изменяем файл конфигурации Nginx /etc/nginx/conf.d/iwtm.conf



Перезапускаем Nginx

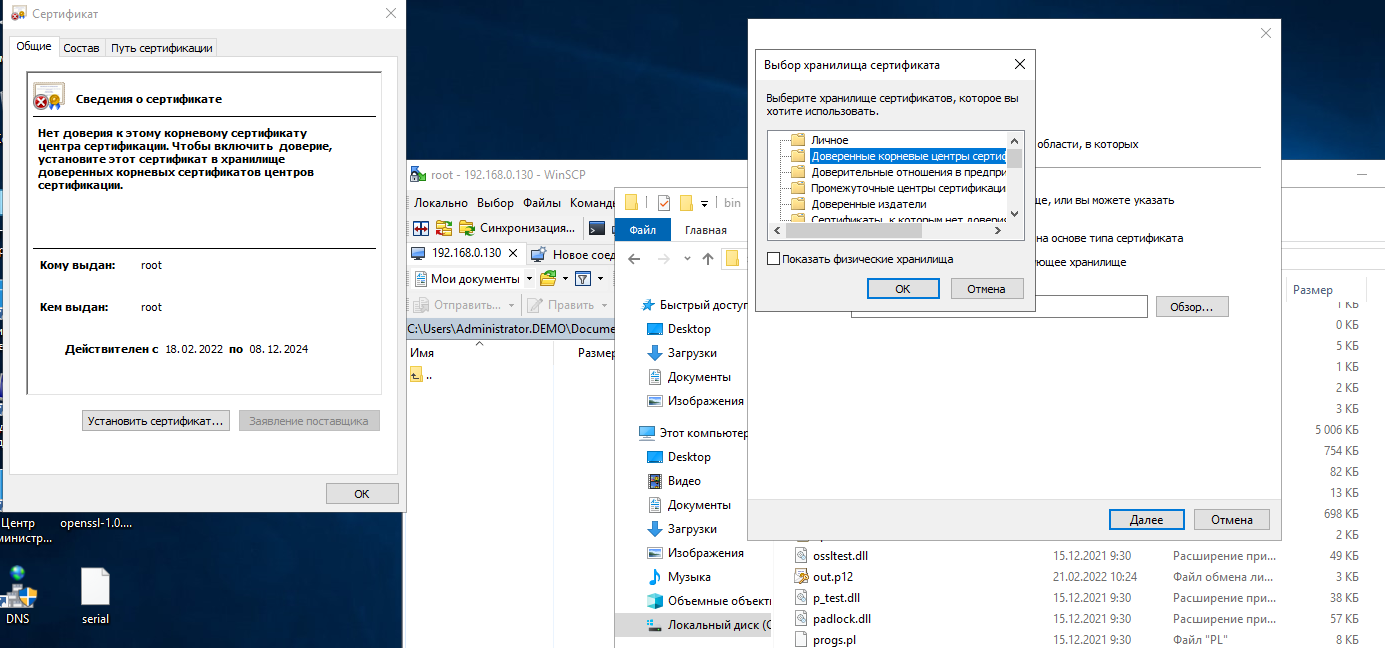


systemctl restart nginx.service

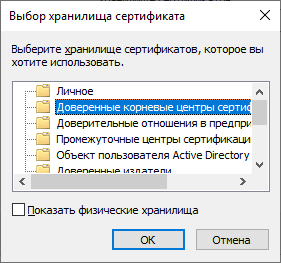
**nano /etc/nginx/conf.d/iwtm.conf**

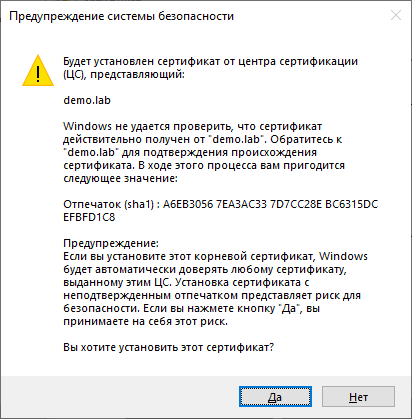
**Service nginx restart**

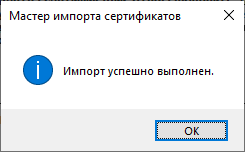
Нажимаем установить сертификат



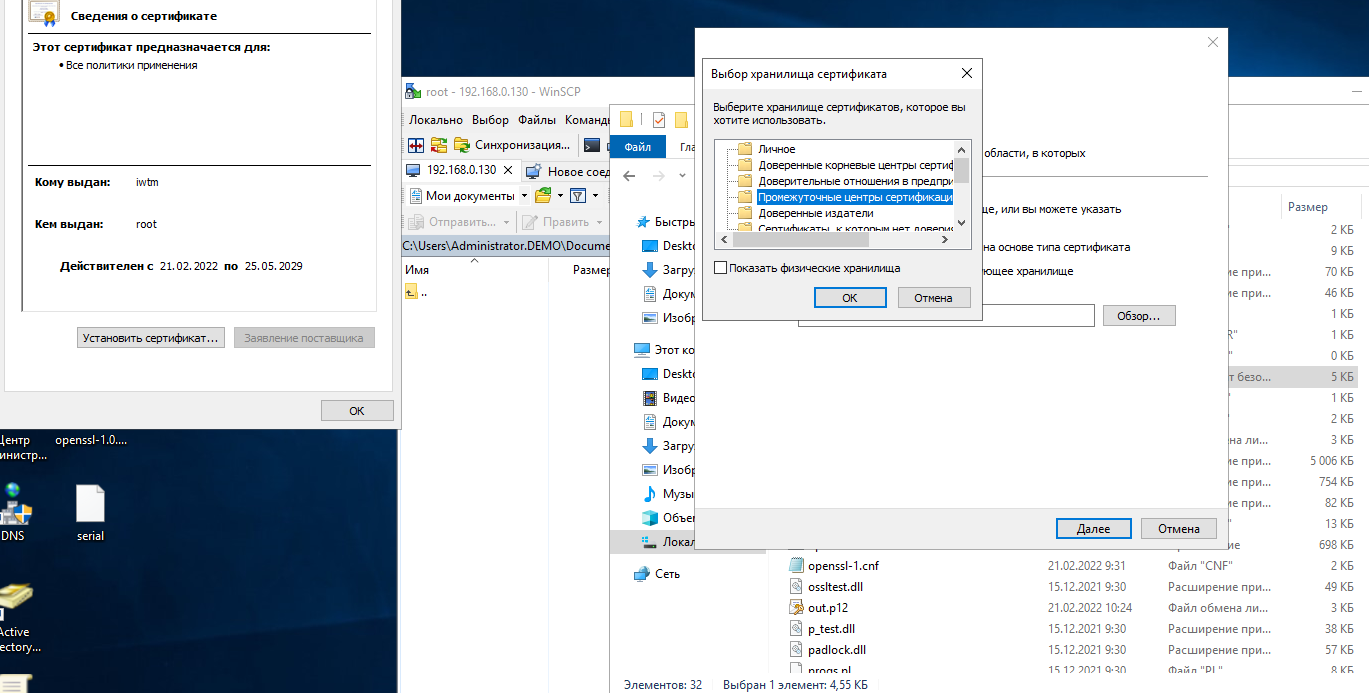
Выбираем Доверенные корневые центры



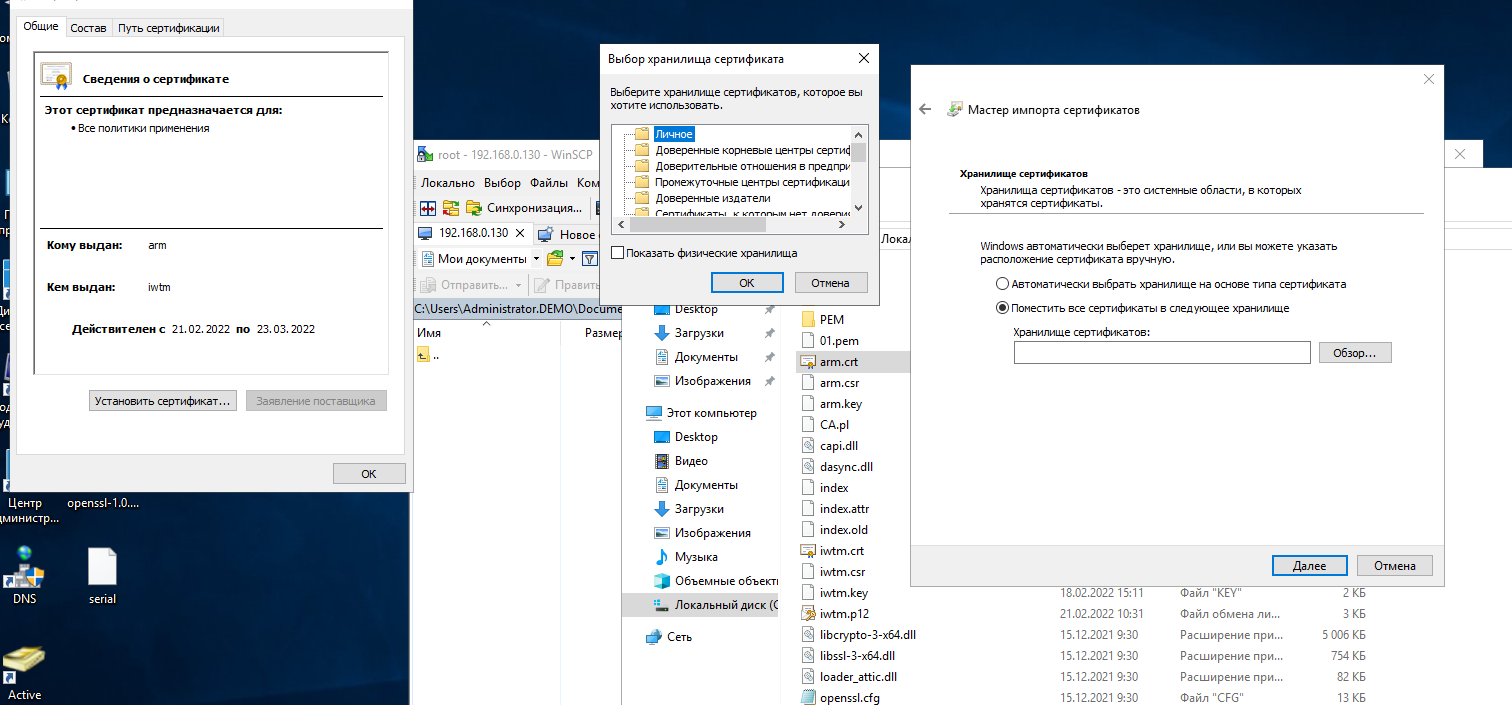


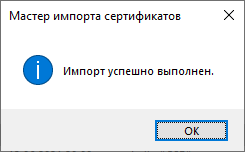


Добавляем сертификат сервера в промежуточные доверенные центры сертификации

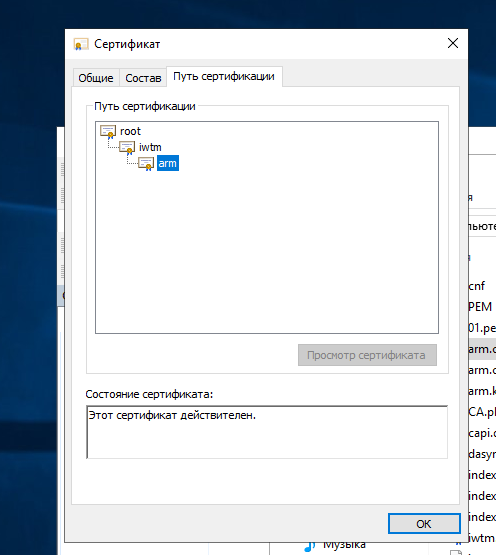


Далее также только в Личное





Видим путь сертификатов



Видим безопасное подключение к ТМ

