**Сертификаты**

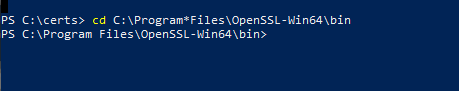
**Установка в AD**

Устанавливаем https://slproweb.com/download/Win64OpenSSL-3\_0\_1.exe

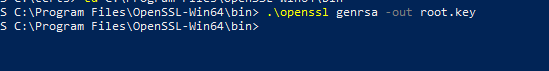
В папке bin копируем файл openssl.conf  

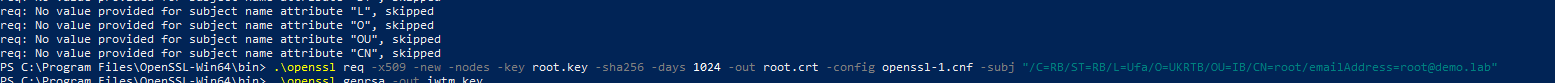

Затем заходим от админа в PowerShell

Вводим cd C:\Program\*Files\OpenSSL-Win64\bin



Далее вводим .\openssl.exe genrsa -out root.key





Создаем новый конфиг openssl-1.cnf

subjectAltName = @alt\_names

[ alt\_names ]

IP.0 = 192.168.99.15

DNS.0 = iwtm

DNS.1 = iwtm.demo.lab

DNS.2 = \*.iwtm.demo.lab

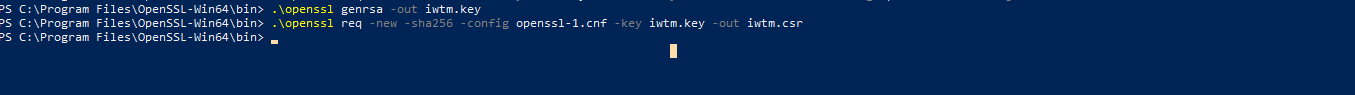
.\openssl.exe req -x509 -new -nodes -key root.key -sha256 -days 365 -out root.crt -config openssl-1.cnf -subj "/C=RU/ST=Moskow/L=Moskow/O=demo lab/OU=IT/CN=demo.lab/emailAddress=admin@demo.lab"

Добавляем промежуточный сервер iwtm

.\openssl.exe genrsa -out iwtm.key

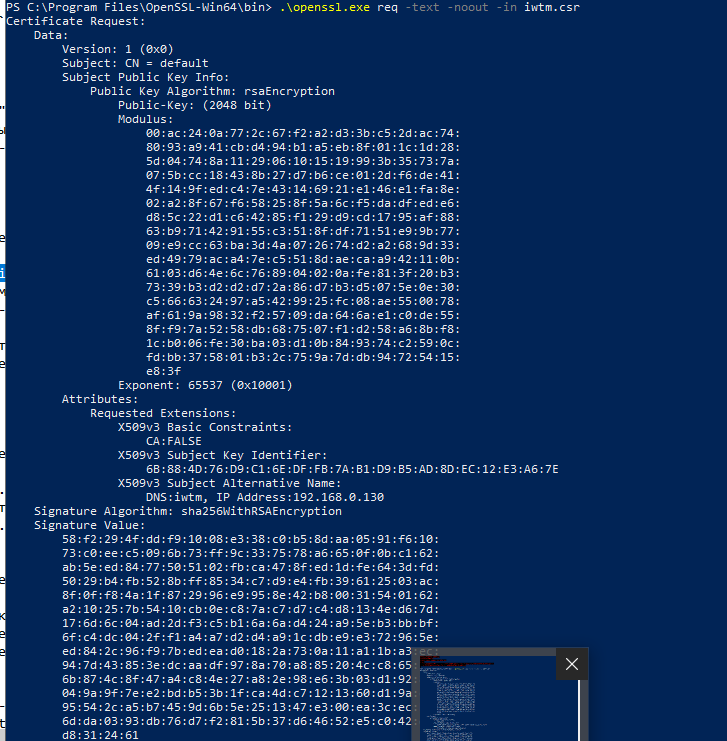
.\openssl.exe req -new -sha256 -config openssl-1.cnf -key iwtm.key -out iwtm.csr

Создание приватного ключа сертификата

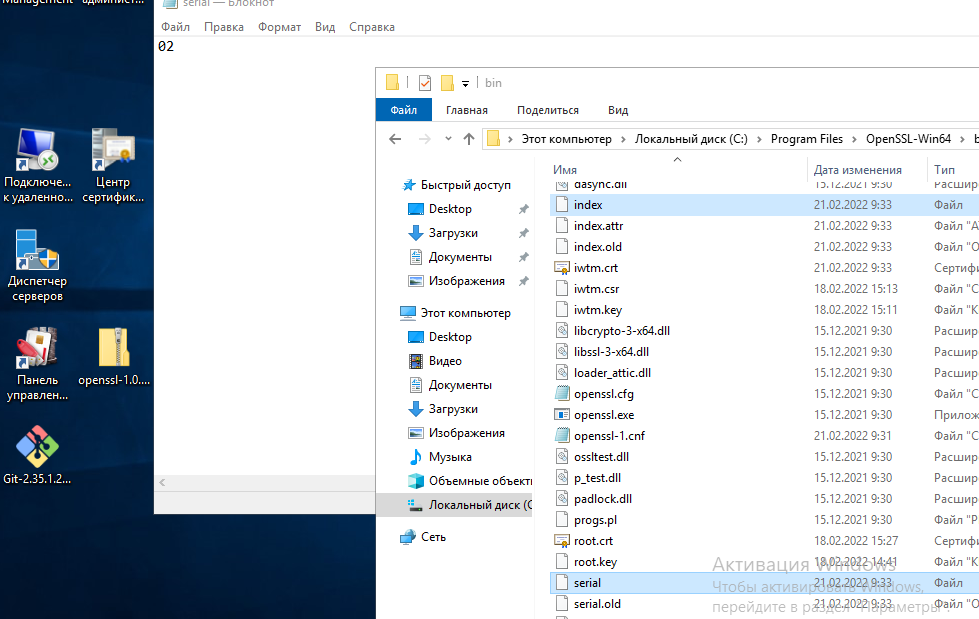


Проверим, что созданный запрос на подпись сертификата (CSR) содержит то, что нам нужно:

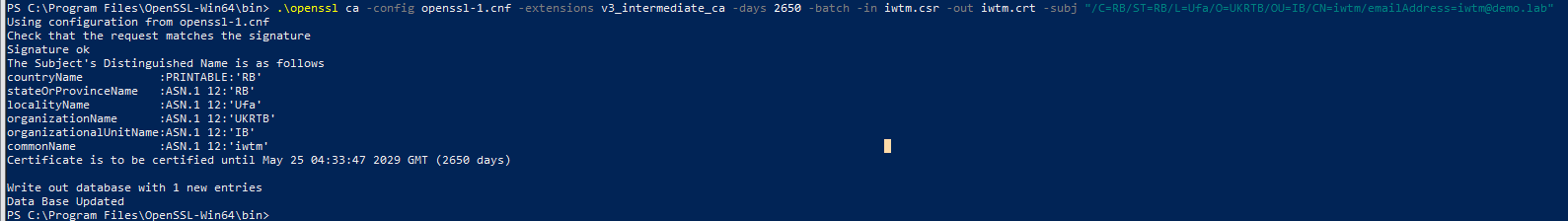
.\openssl.exe req -text -noout -in iwtm.csr



Создаем файлы serial с содержимым “02” и пустой файл index без расширений!



Подпись и создание сертификата



**Подпись и создание сертификата**

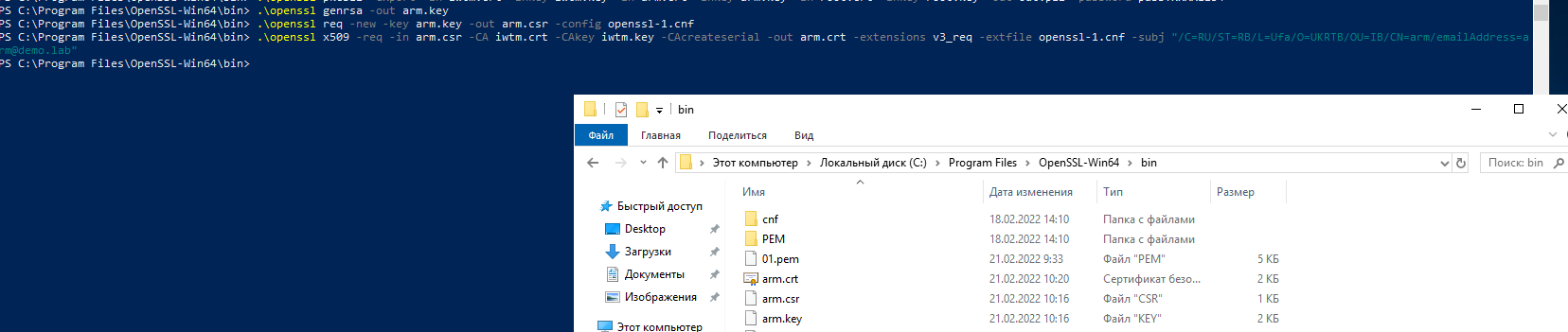
**.\openssl x509 -req -in "iwtm.csr" -CA "root.crt" -CAkey "root.key" -CAcreateserial -out "iwtm.crt" -extensions v3\_req -extfile "openssl-1.cnf" -subj** **"/C=RU/ST=Moskow/L=Moskow/O=demolab/OU=IT/CN=iwtm/emailAddress=iwtm@demo.lab"**

**Добавляем пользователя arm**

.\openssl.exe genrsa -out user.key

.\openssl.exe req -new -key user.key -out user.csr -config openssl-1.cnf

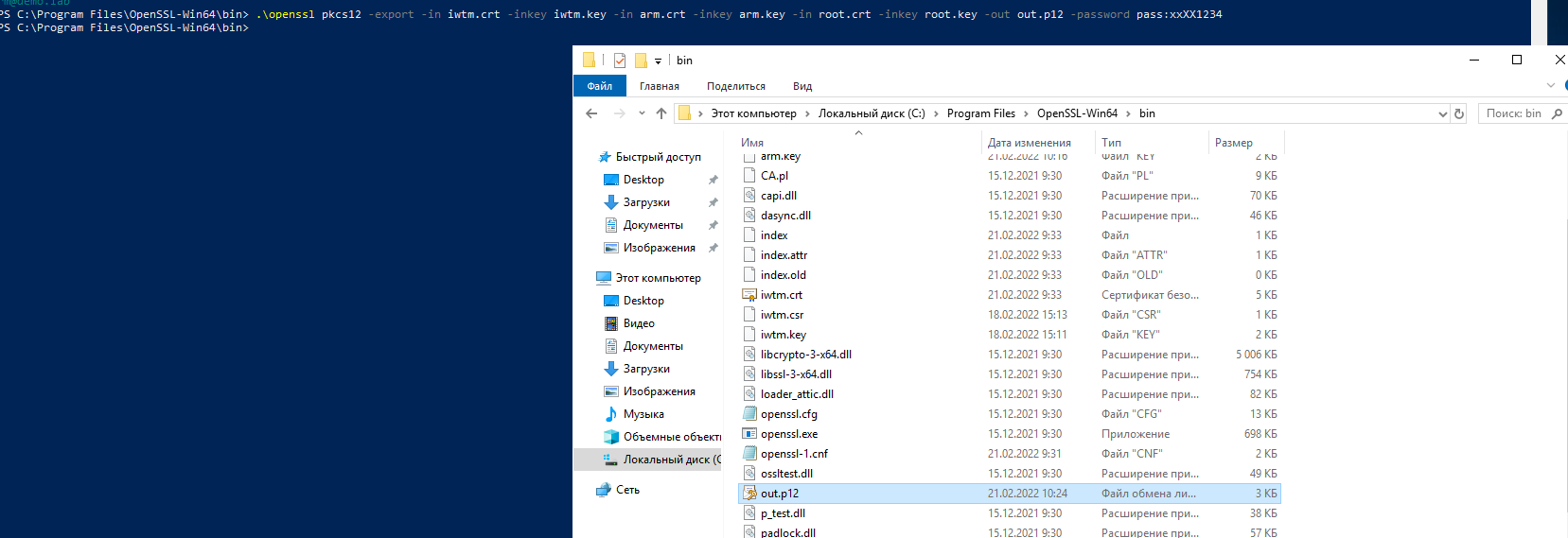
.\openssl.exe x509 -req -in user.csr -CA iwtm.crt -CAkey iwtm.key -CAcreateserial -out user.crt -extensions v3\_req -extfile openssl-1.cnf -subj **"**/C=RU/ST=Moskow/L=Moskow/O=demolab/OU=IT/CN=user/emailAddress=user@demo.lab**"**

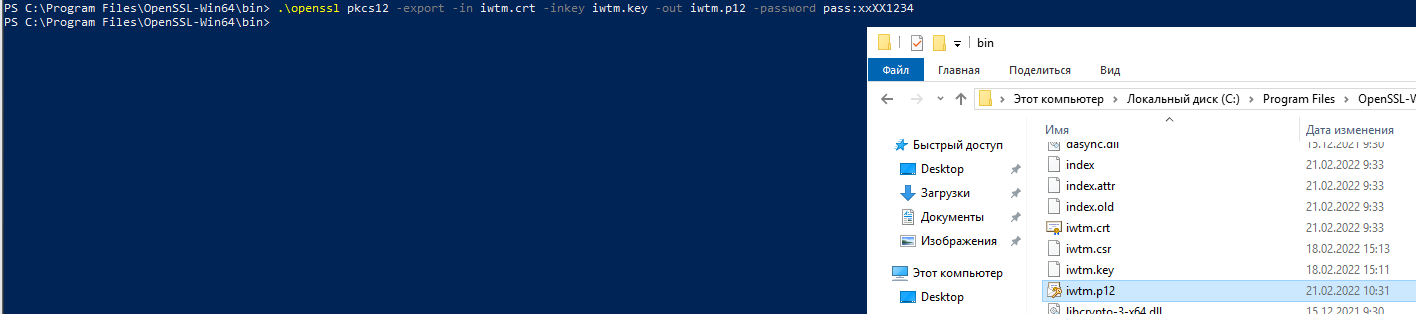


Упаковка ключа и сертификата в файл PKCS12

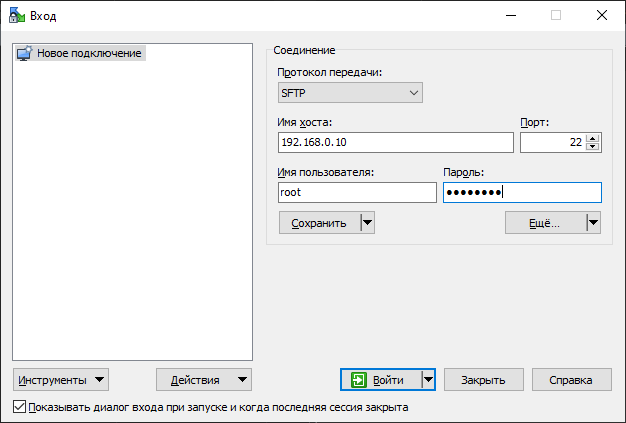
**.\openssl.exe pkcs12 -export -in iwtm.crt -inkey iwtm.key -out iwtm.p12 -password pass:xxXX1234**

**.\openssl.exe pkcs12 -export -in iwtm.crt -inkey iwtm.key -in root.crt -inkey root.key -out out.p12 -password pass:xxXX1234**

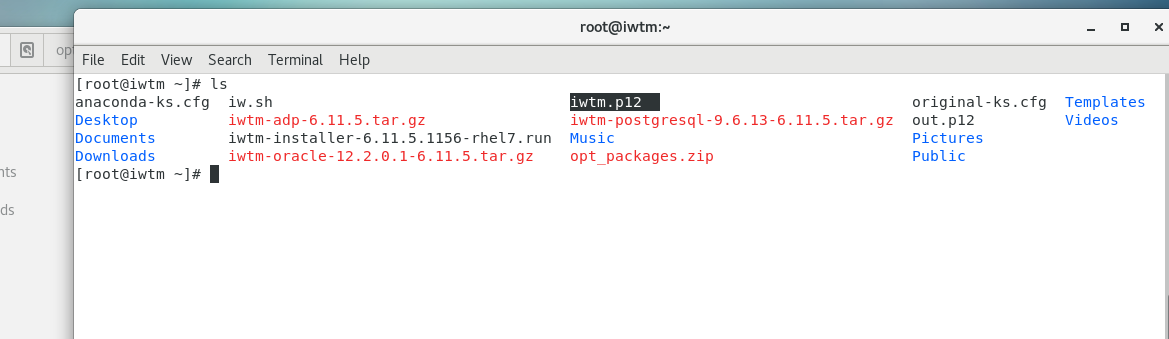




Подключаемся к ТМ через WinCSP

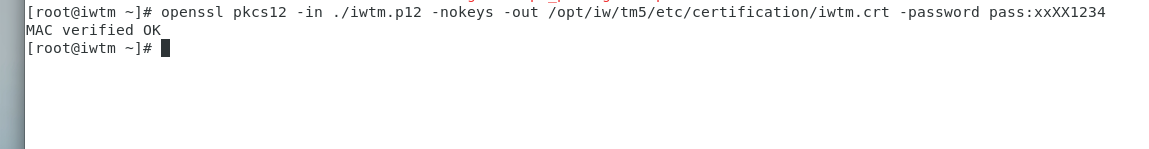


Перекидываем наш сертификат



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

Извлекаем из сертификата закрытый ключ



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

openssl pkcs12 -in /root/iwtm.p12 -clcerts -nokeys -out /root/iwtm.cer

**Извлекаем из сертификата закрытый ключ**

openssl pkcs12 -in /root/iwtm.p12 -nocerts -nodes -out /root/iwtm.key

**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**

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

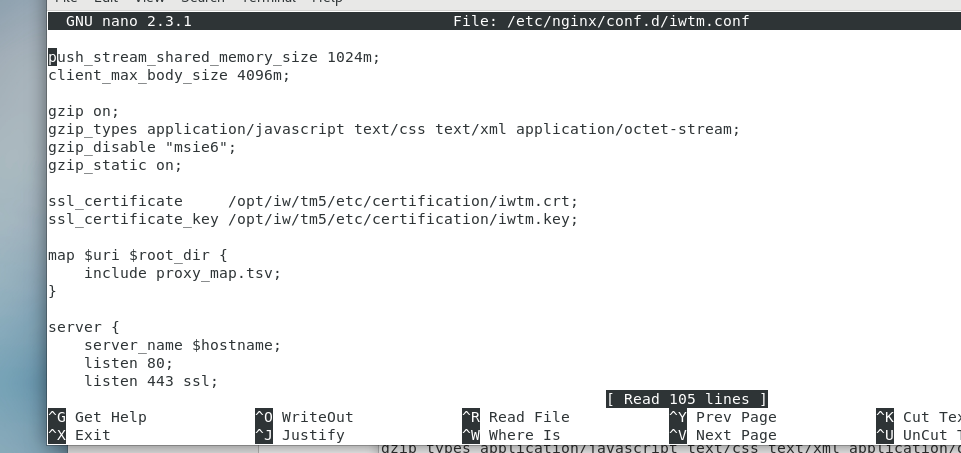
/opt/iw/tm5/etc/certification/iwtm.cer;

/opt/iw/tm5/etc/certification/iwtm.key;

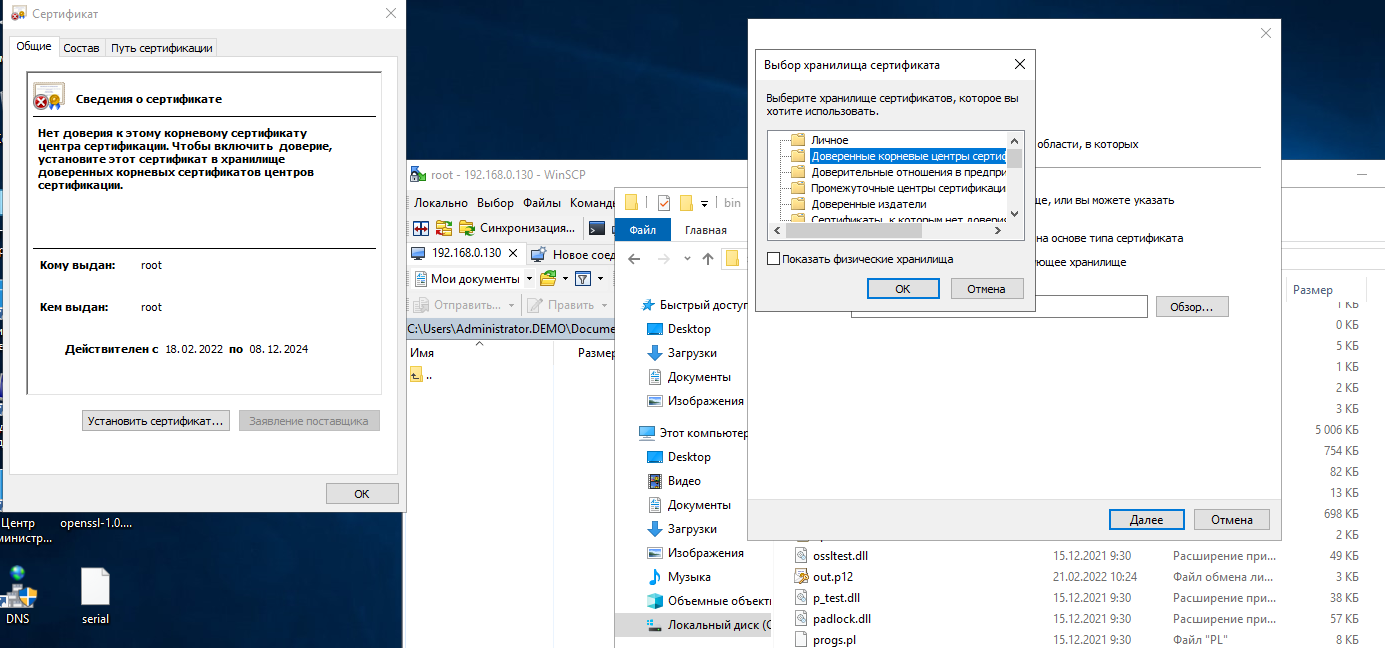
**Перезапускаем Nginx**

systemctl restart nginx.service

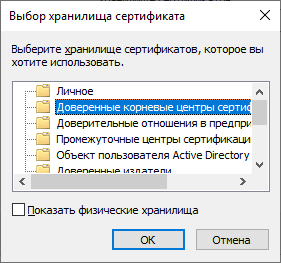
Упаковка всех ключей и сертификатов в out.p12

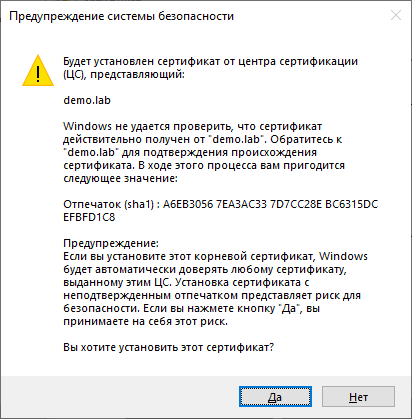


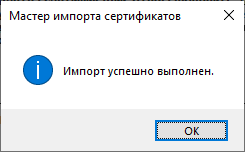
Нажимаем установить сертификат



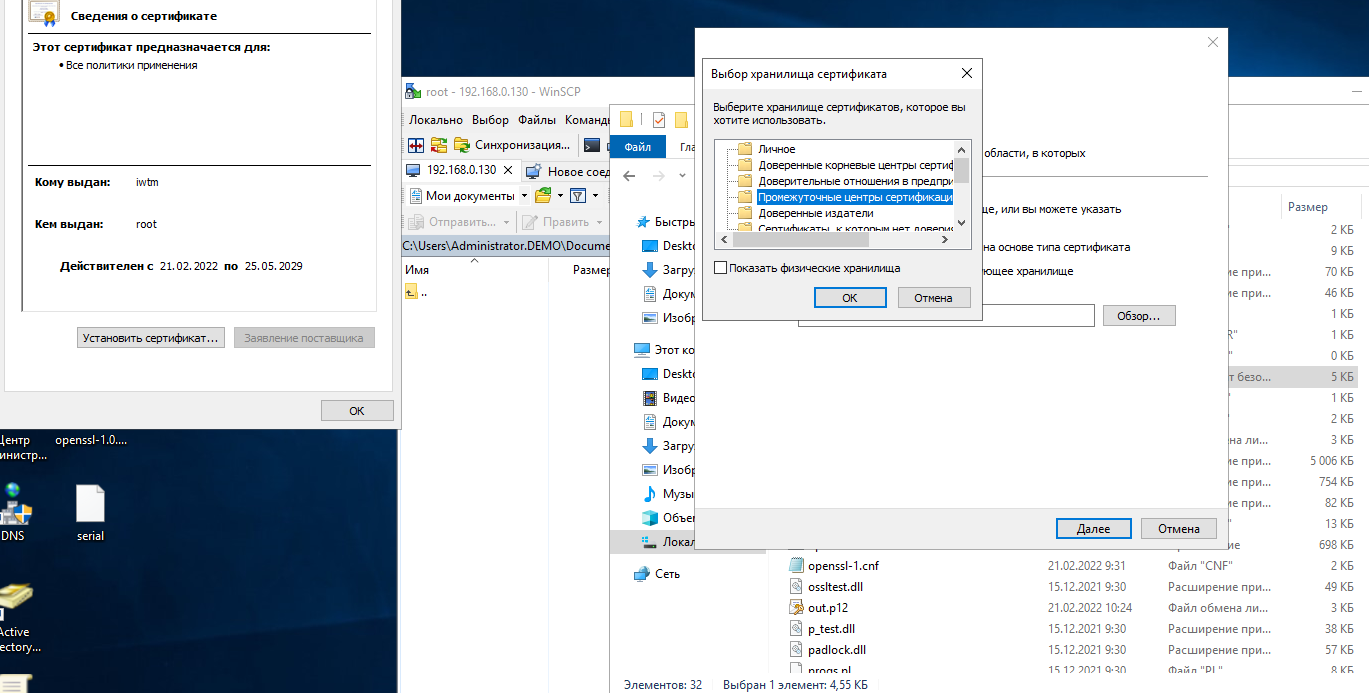
Выбираем Доверенные корневые центры



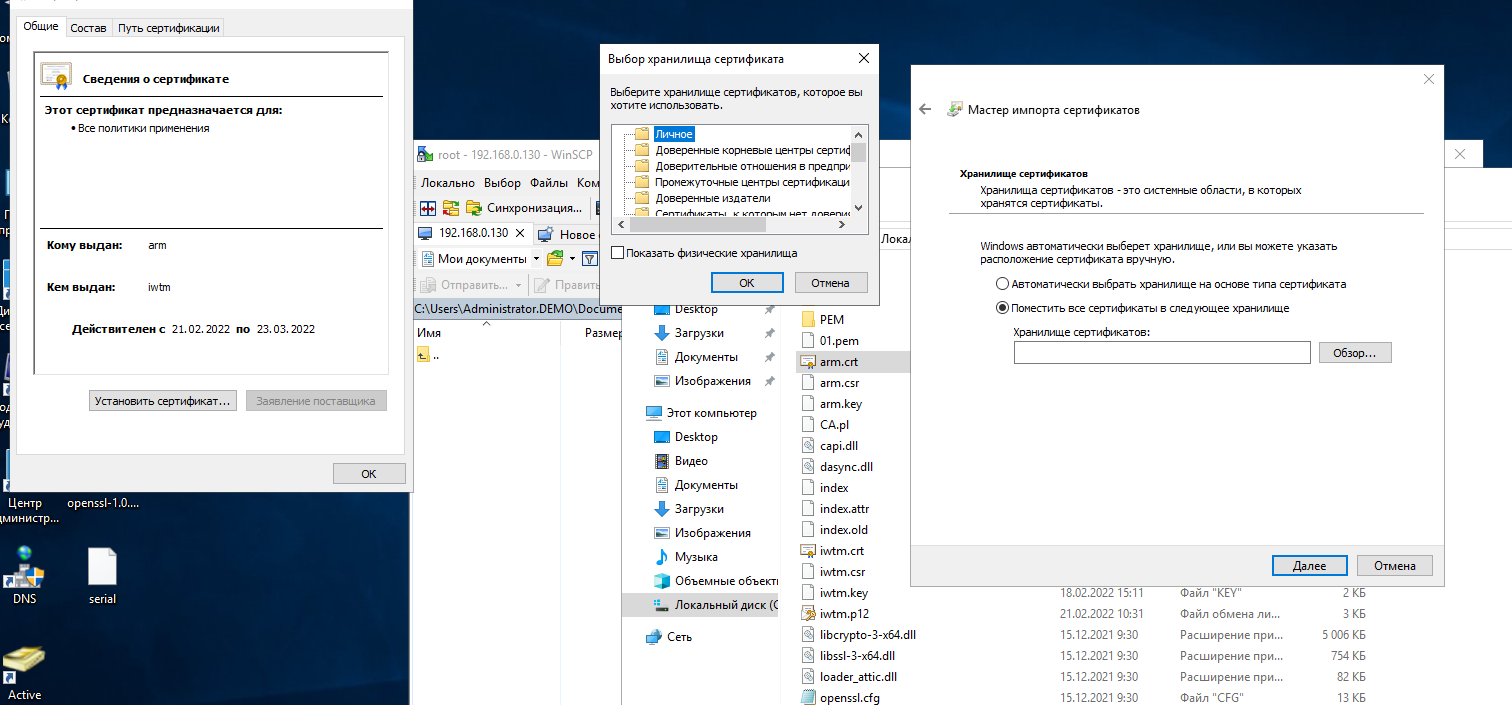


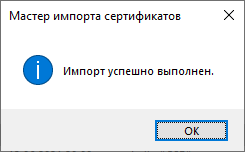


Добавляем сертификат сервера в промежуточные доверенные центры сертификации

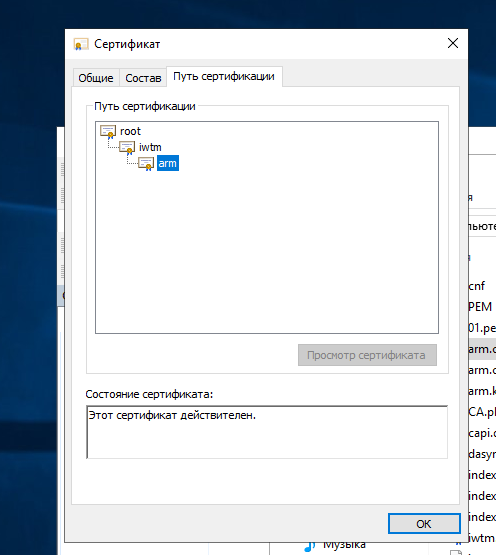


Далее также только в Личное





Видим путь сертификатов



Видим безопасное подключение к ТМ

