From NSP, get /opt/nsp/os/tls/nsp.truststore

You must also get knowledge of the truststore password

Copy the nsp.truststore file into the client Linux machine **/etc/ssl/certs**



You must get knowledge of the truststore password ( “NokiaNsp1!” , for example)

Run the command:

**keytool -list -rfc -keystore nsp\_truststore\_2 -storepass NokiaNsp1!**

A screenshot of a computer

Description automatically generated

Copy the displayed contents of the certificate file. Take only the parts between and including BEGIN and END

A screenshot of a computer

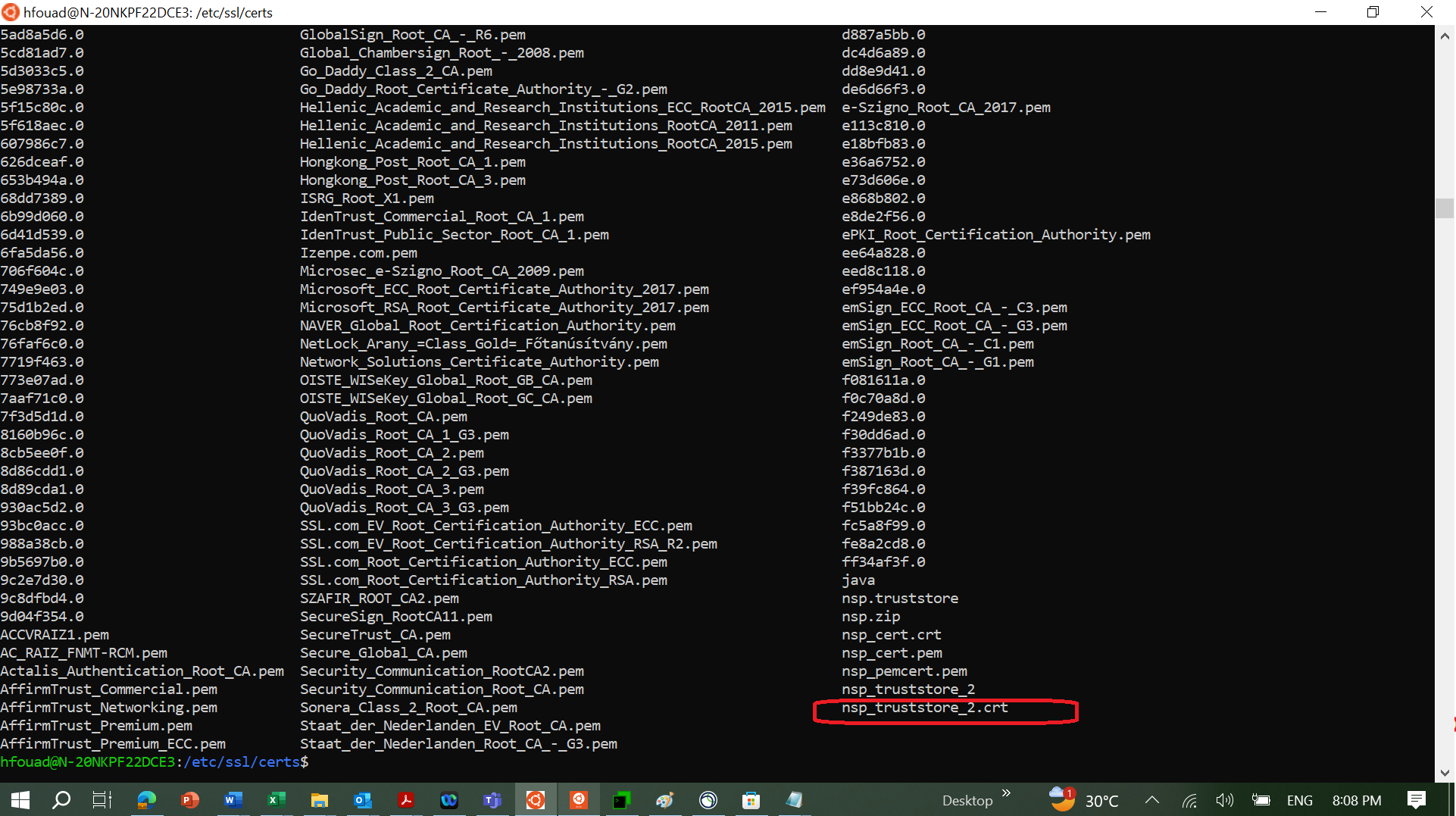
Description automatically generated

Create the .crt file (create a certificate file) using nano:

**sudo nano nsp\_truststore\_2.crt**

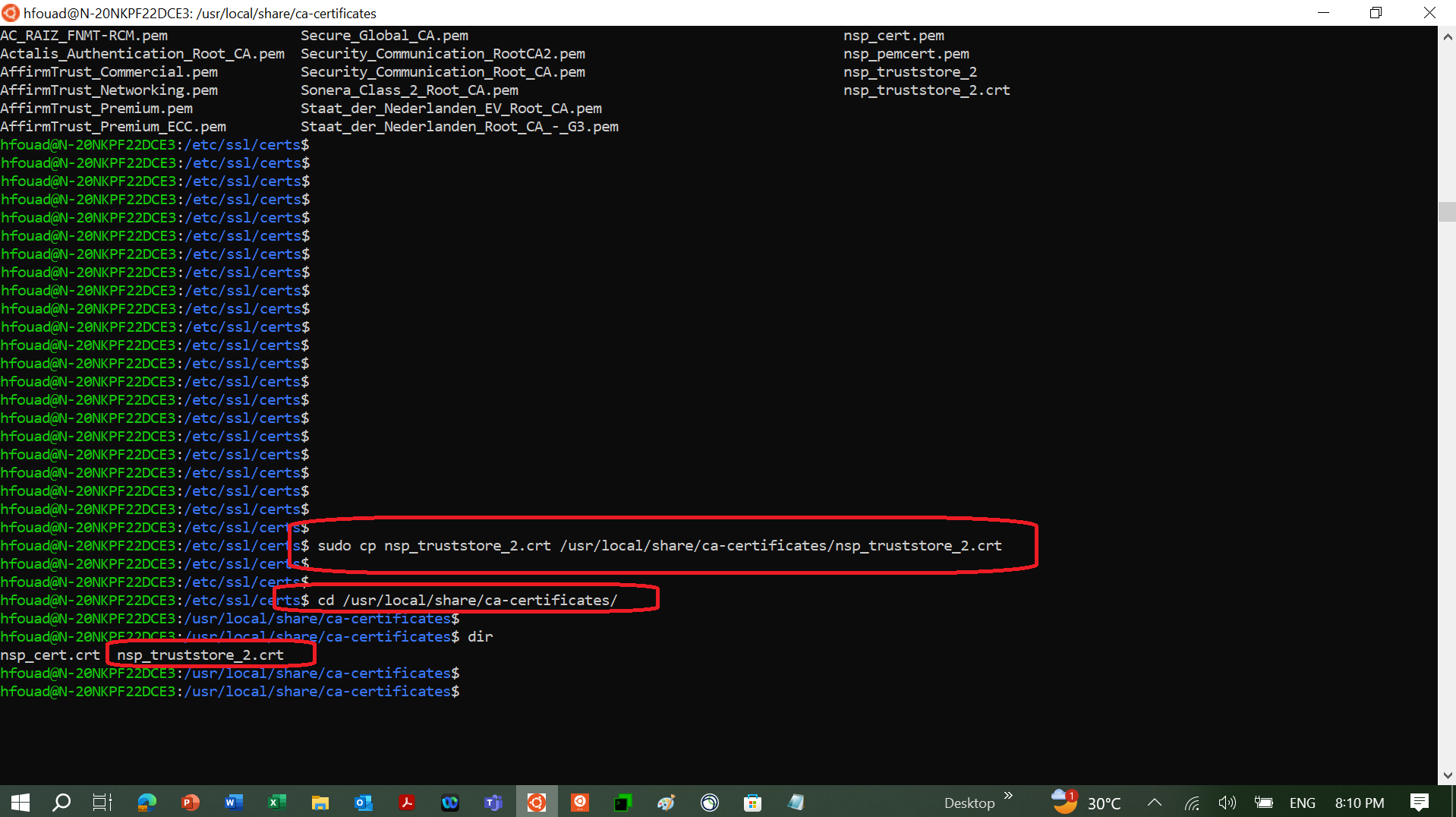
A screenshot of a computer

Description automatically generated

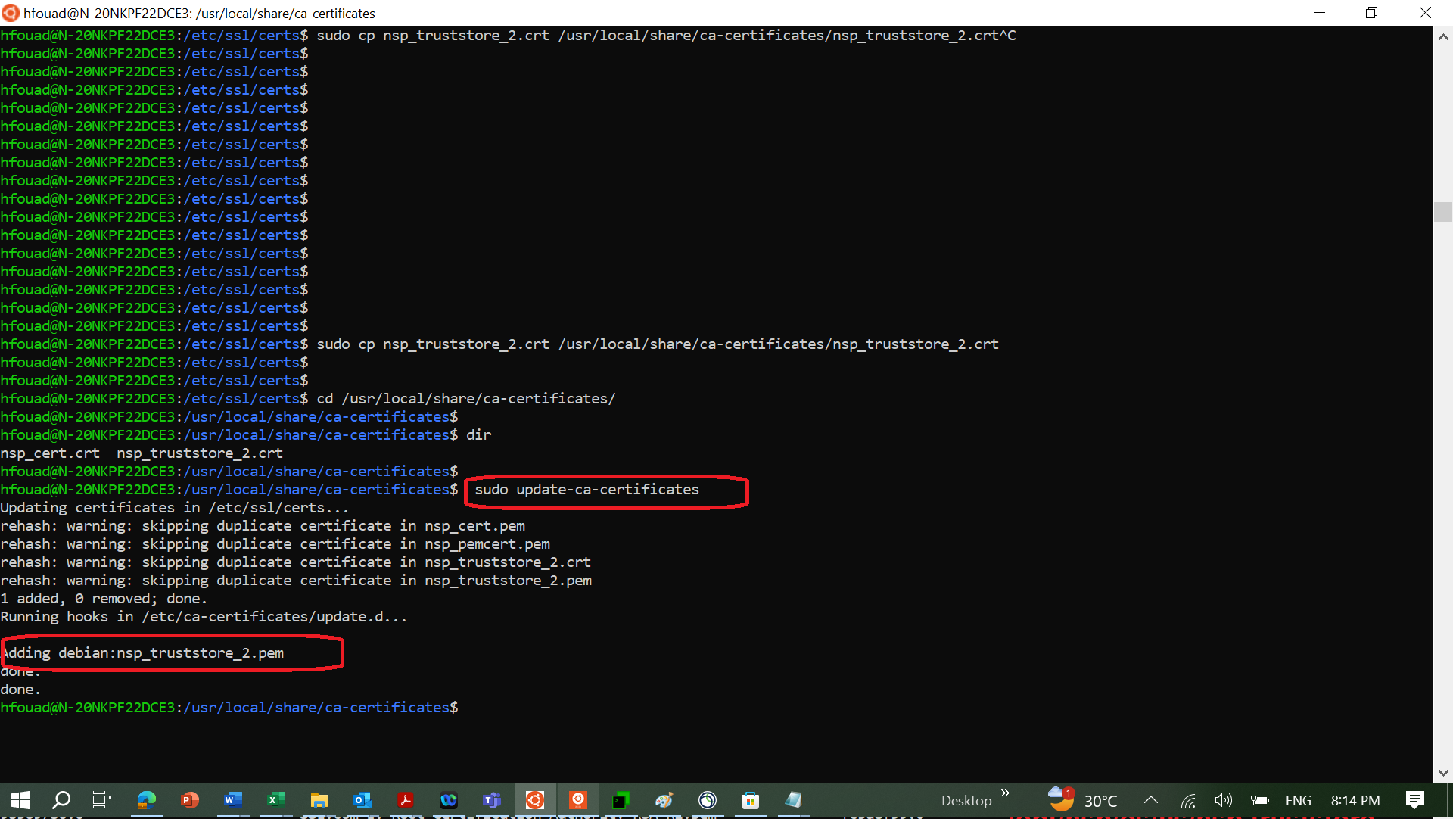


Copy the .crt file that is created to /usr/local/share/ca-certificates/ by cp command:

**sudo cp nsp\_truststore\_2.crt /usr/local/share/ca-certificates/nsp\_truststore\_2.crt**

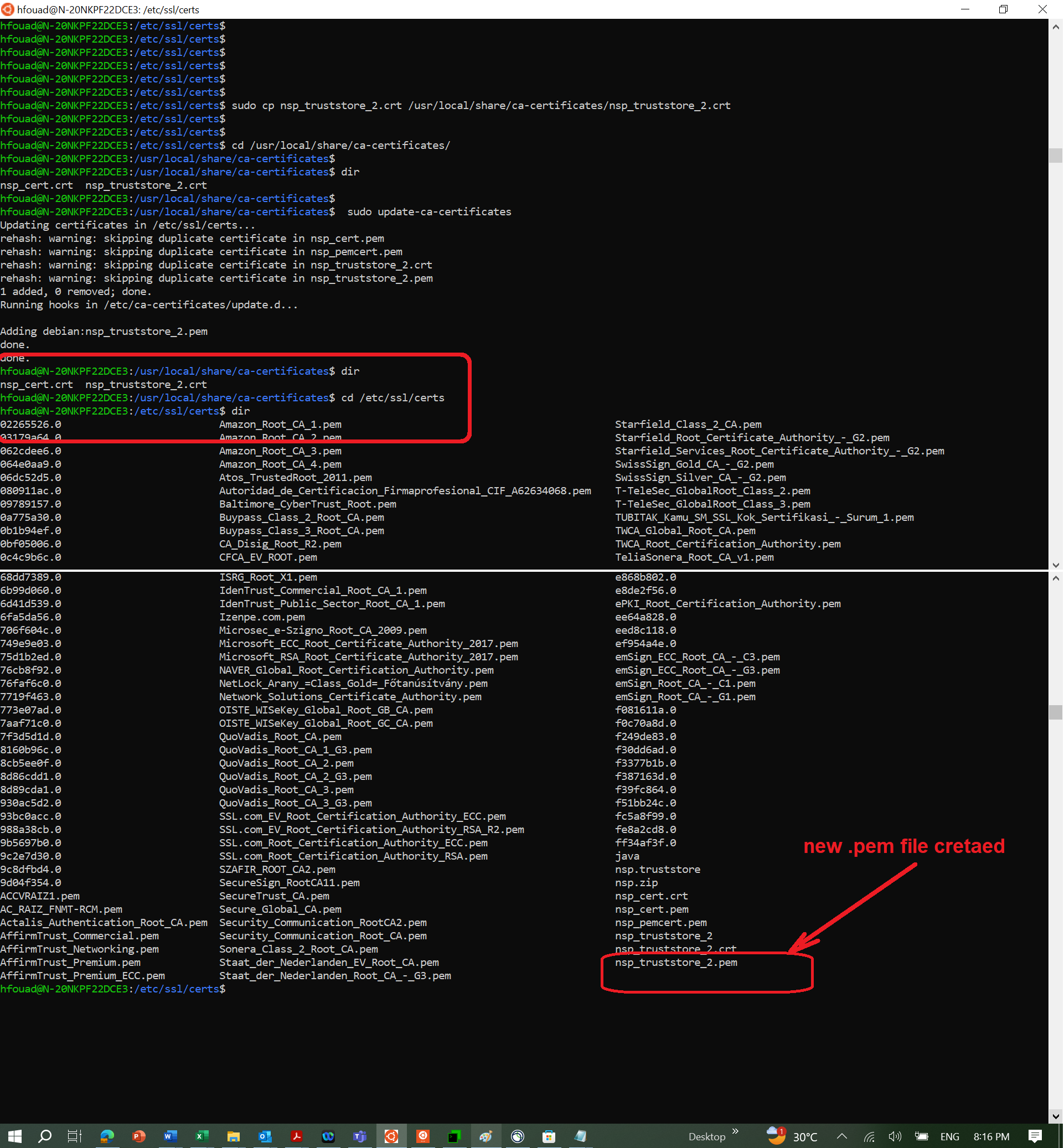


Update the CA store using the command:

sudo update-ca-certificates

Go back to /etc/ssl/certs

Check that a new .pem file has been created successfully



Now the curl command can work smoothly, there will be no SSL error (60) due to self-signed certificate of NSP:

[Access & Authentication APIs - Nokia Network Developer Portal](https://network.developer.nokia.com/learn/23_4/common-base-function/access-authentication-apis/)

[NSP 23.4 Common Base Functions (getpostman.com)](https://documenter.getpostman.com/view/26248101/2s93RRxZ5t#5b3de086-3afb-4e3d-a253-e69fa7a4ce3d)

OSS user credentials:

hanyfouad:hanyoss\_Pass12%

Base64 encoded:

aGFueWZvdWFkOmhhbnlvc3NfUGFzczEyJQ==

curl --location -g 'https://**10.133.210.13**/rest-gateway/rest/api/v1/auth/token' \

--header 'Content-Type: application/json' \

--header 'Authorization: Basic **aGFueWZvdWFkOmhhbnlvc3NfUGFzczEyJQ==**' \

--data '{

"grant\_type": "client\_credentials"

}'

A screenshot of a computer

Description automatically generated