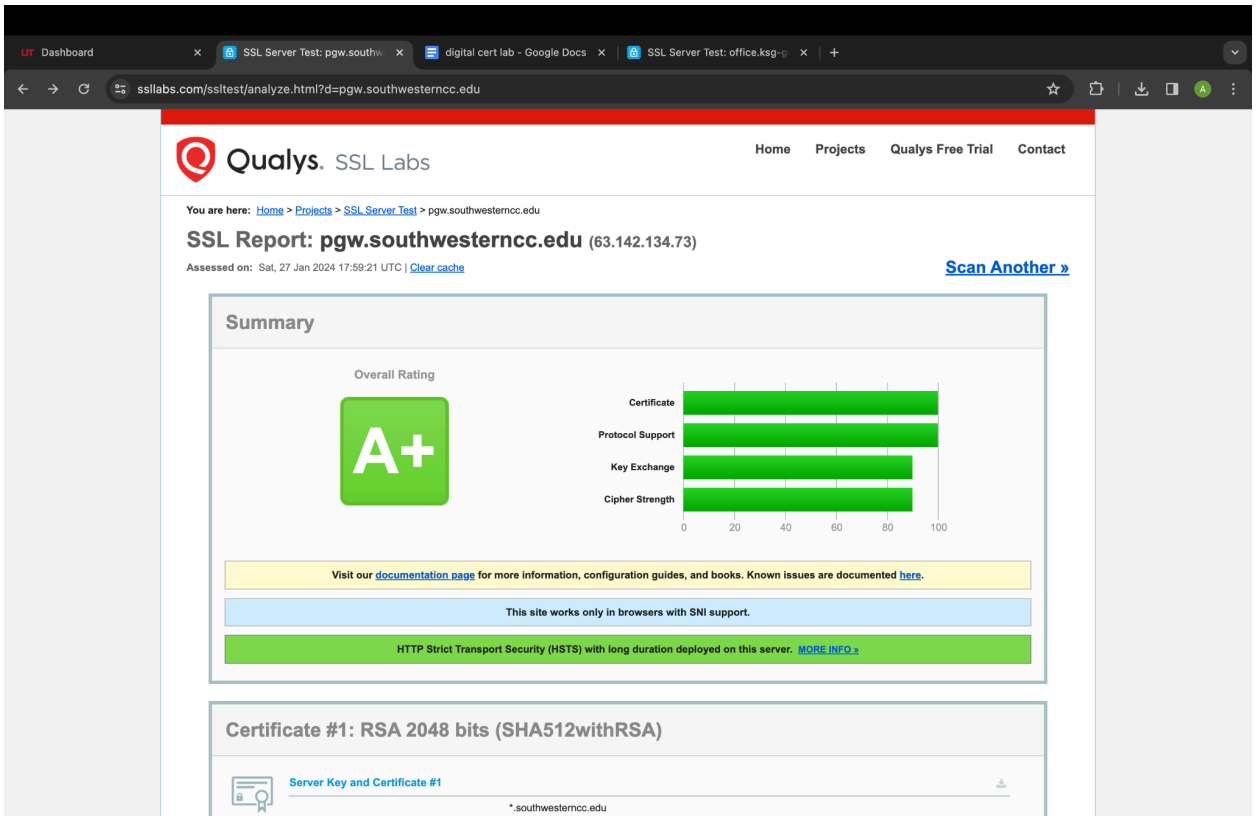
Good: pgw.southwesterncc.edu

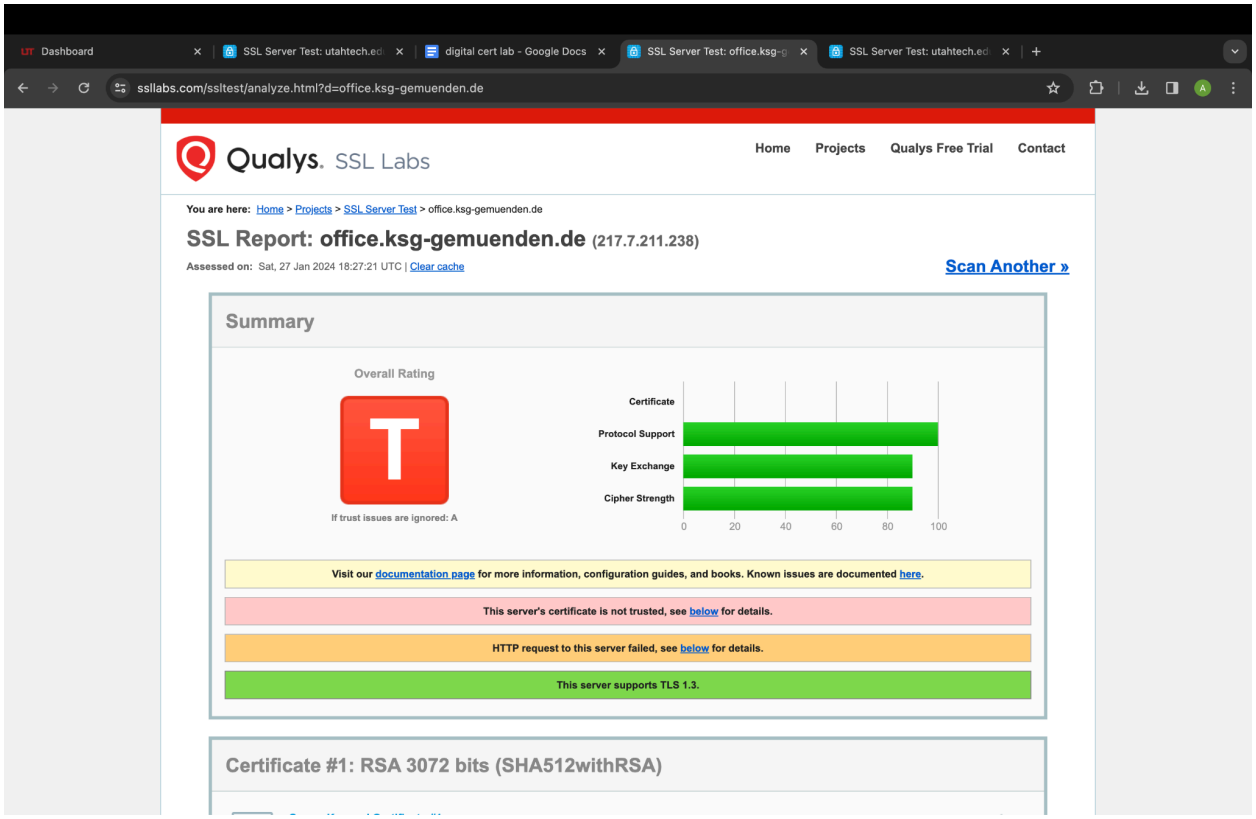
Asymmetric key: RSA 2048 bits (e 65537)

Revocation info: CRL, OCSP
CRL: http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crl
OCSP: http://ocsp.digicert.com
No ocsp stapling.
Most secure: TLS 1.2
Not secure: on there is says no to all the other ones
Vulnerabilities: no



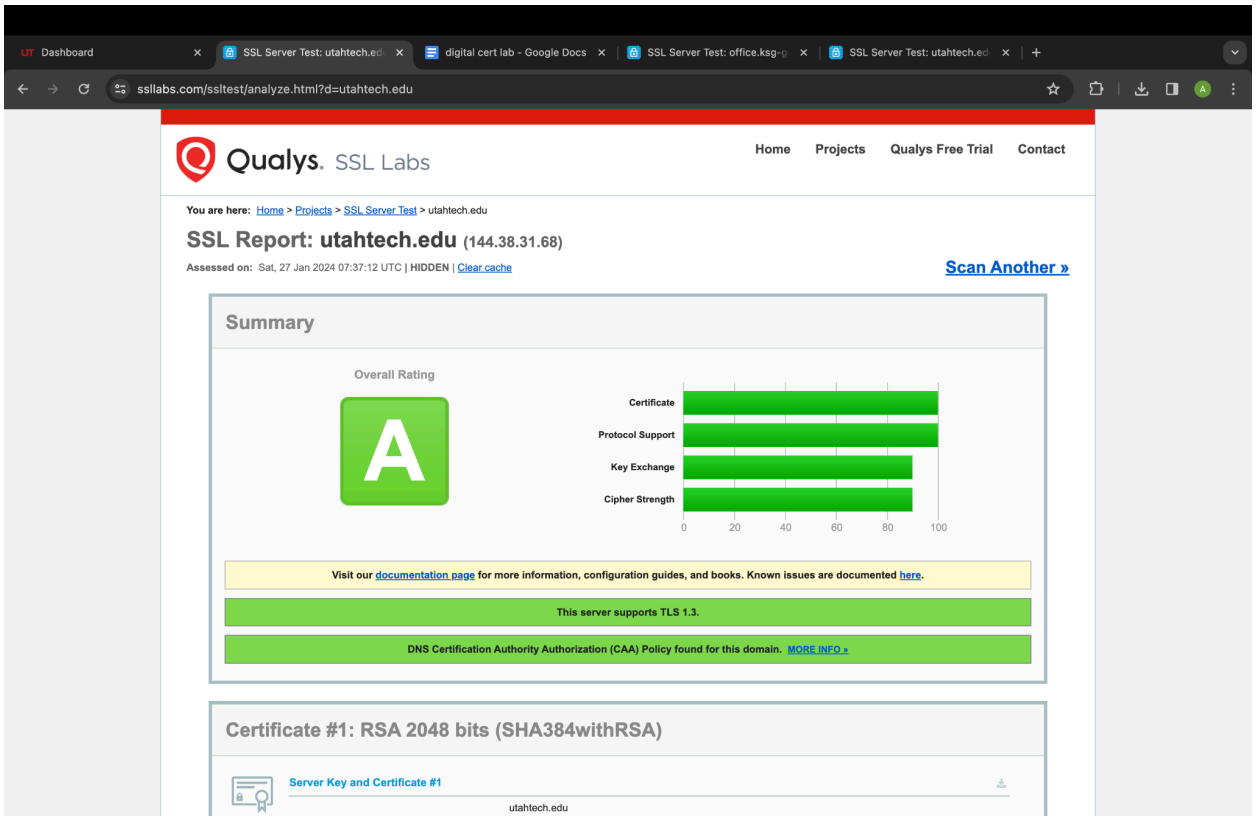
Bad: office.ksg-gemuenden.de

Asymmetric key: RSA 3072 bits (e 65537)
Revocation info: none
Most secure: TLS 1.3
Vulnerabilities: Unknown: goldendoodle, sleeping poodle, zombie poodle, openSSL 0-length, ticketbleed



Other: Utahtech.edu

Key: RSA 2048 bits (e 65537)
Revocation: CRL, OCSP
CRL: http://crl.sectigo.com/InCommonRSAServerCA2.crl
OCSP: http://ocsp.sectigo.com
Most secure: TLS 1.3
Vulnerabilities: no



Desc: A poodle attack is when an attacker exploits the weakest cipher allowed by the browser or website and takes what data they can.
SSL is weak to the poodle attack
It was discovered by Bodo Möller, Thai Duong and Krzysztof Kotowicz

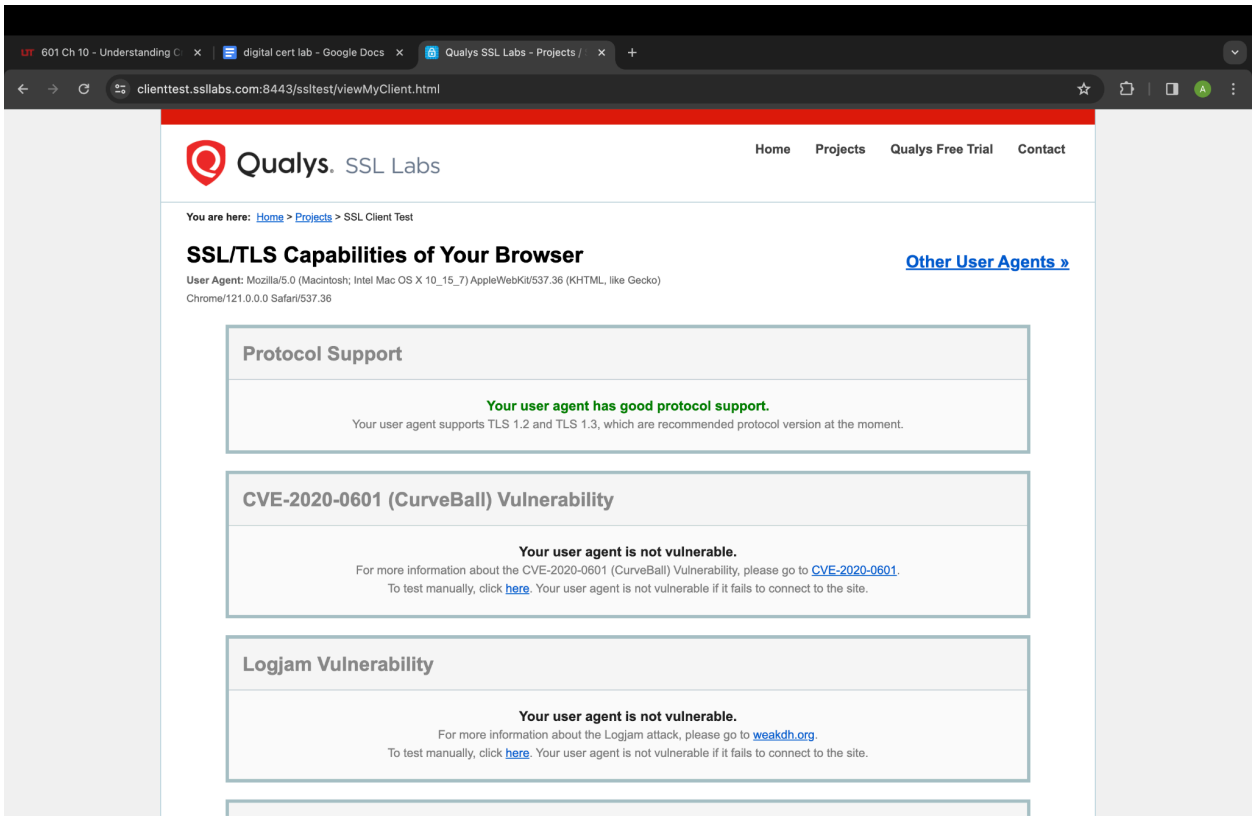
Short or long life: I think for a smaller company it is better to have one that lasts longer to help mitigate cost. For a large company that can spare the funds I think a shorter one would be better because bigger companies are targeted more frequently because of larger profits.

CRL: CRL is a good baseline; it just takes a while to be updated and takes the browser a long time to search through the whole thing for the certificate.

OCSP: OCSP mitigates a lot of problems. It takes less time for the user when they log on to a website because after the browser sends a request the CA replies with a good revoked or unknown. It can be a lot for the CA for high traffic websites though.

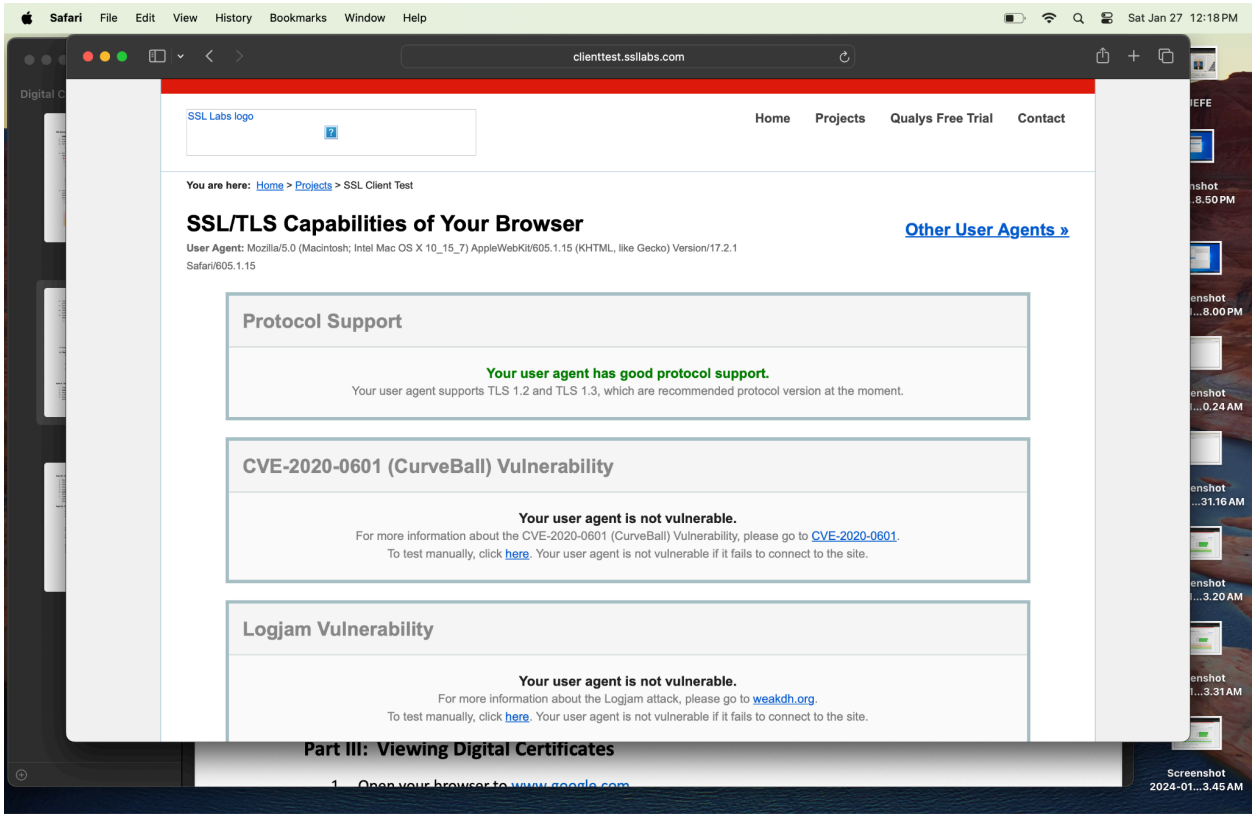
OCSP stapling: This staples the certificate itself with the good revoked or unknown so the overhead at the CA is reduced. It is sent through the handshake at the beginning.

Google browser:



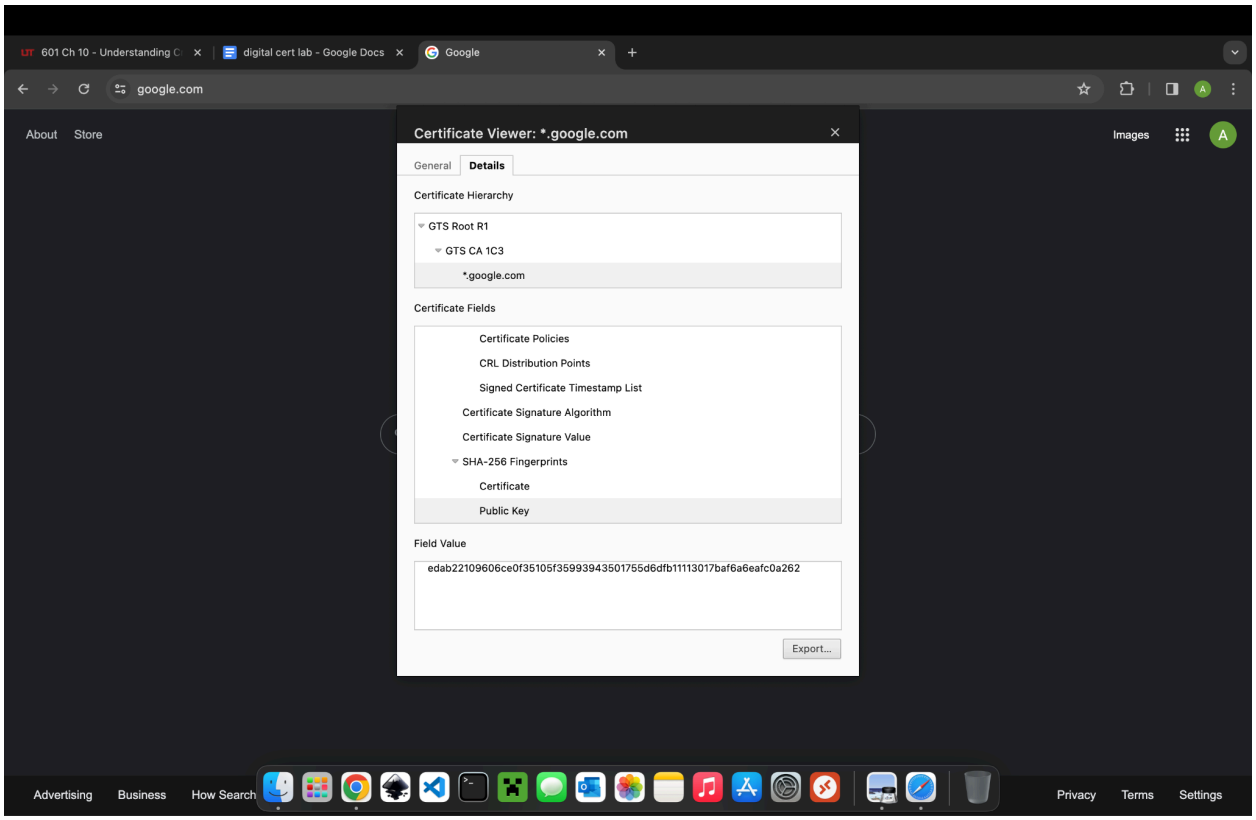
Not vulnerable
Protocols: TLS 1.2, TLS 1.3
OCSP stapling: Yes

Safari:



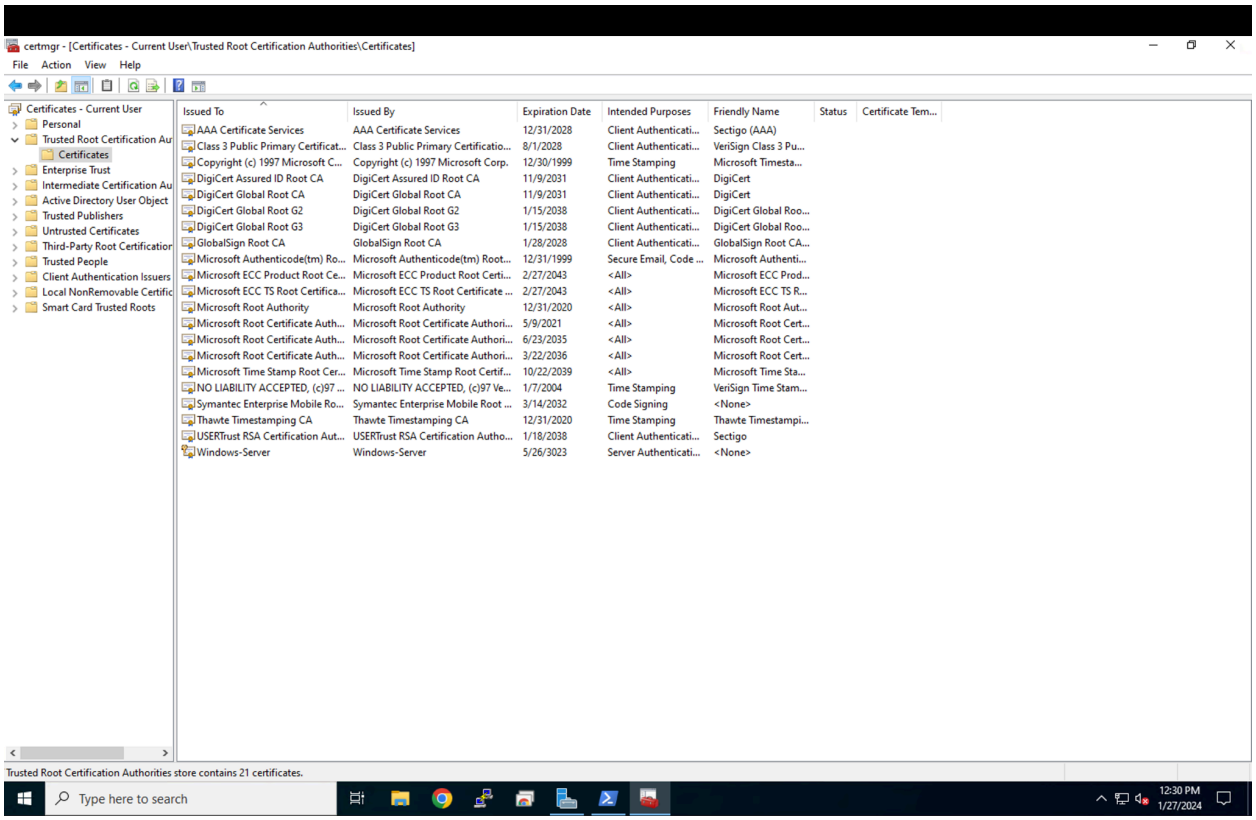
Not Vulnerable
Protocols: TLS 1.2, TLS 1.3
OCSP stapling: Yes

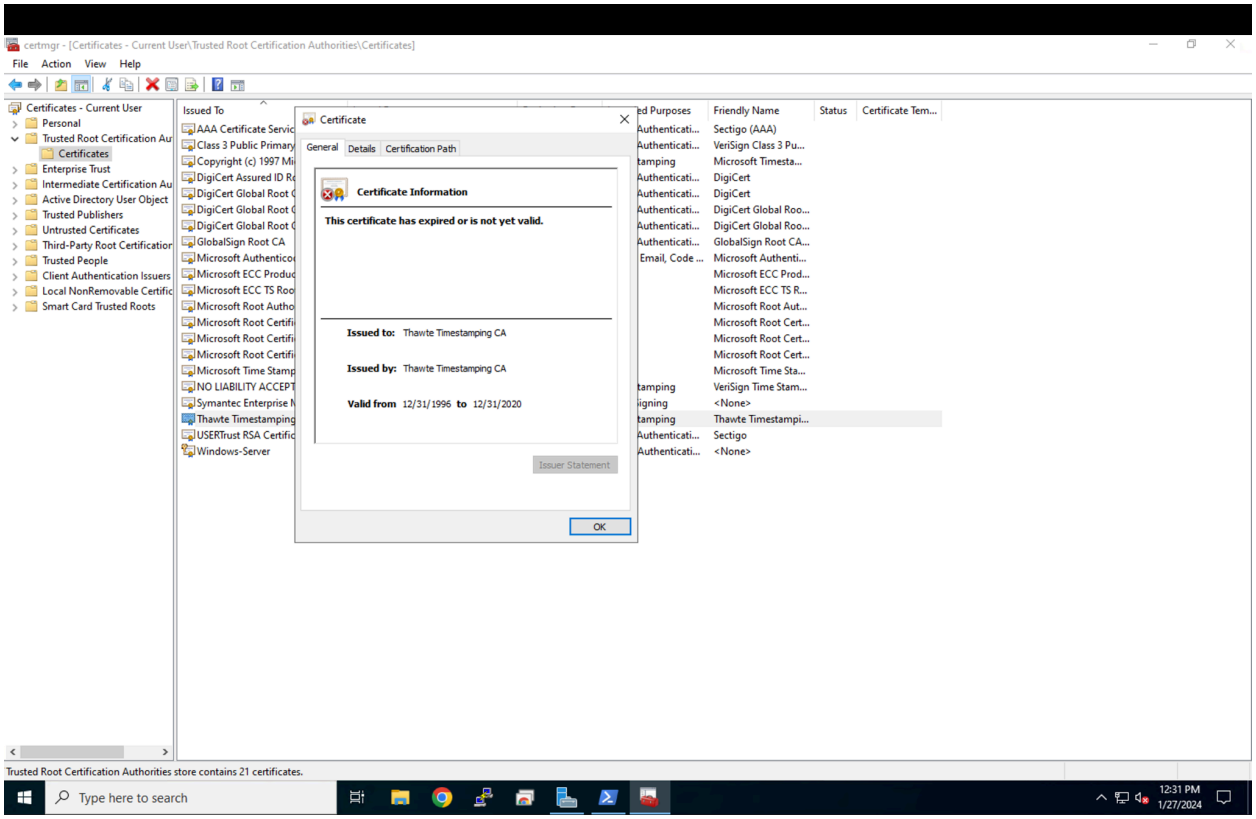
Google Certificate:



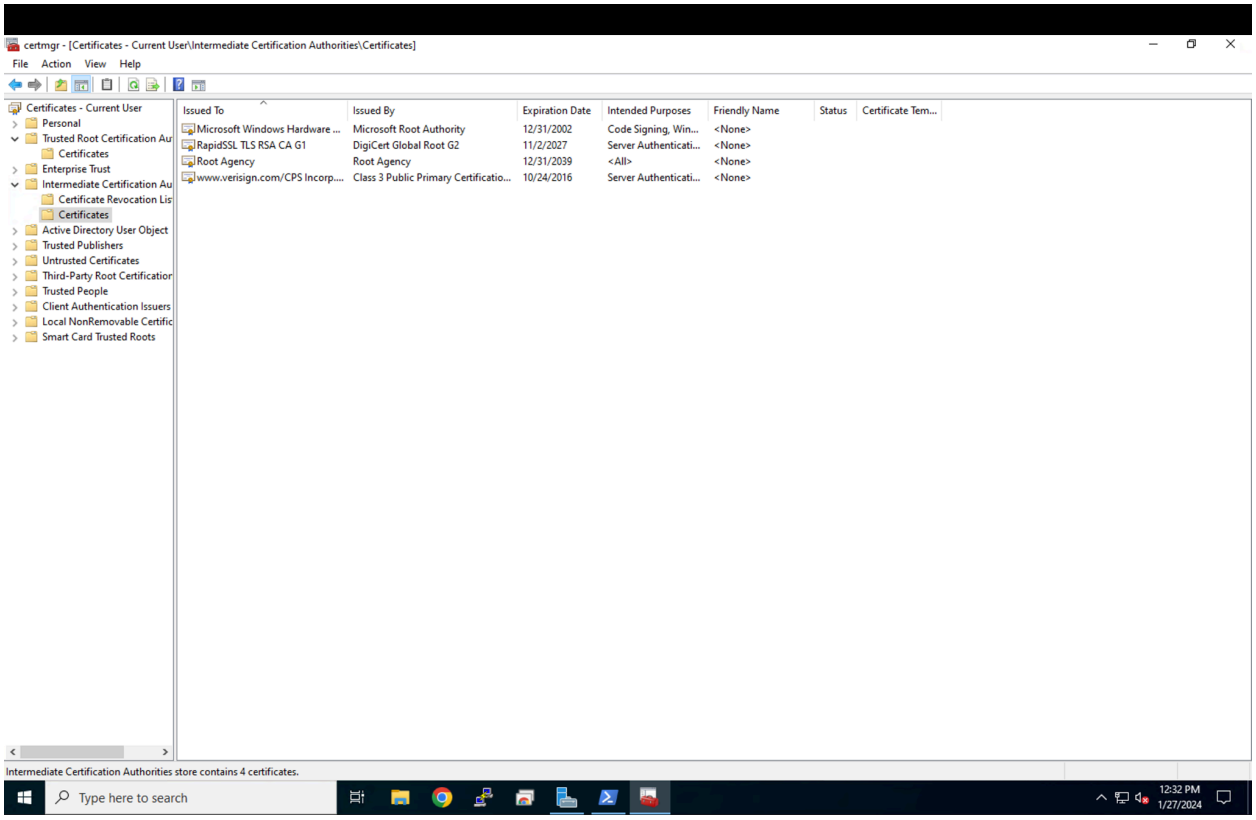
Expires sooner: google
If google expired after the root certificate information could be stolen.

Windows stuff :(

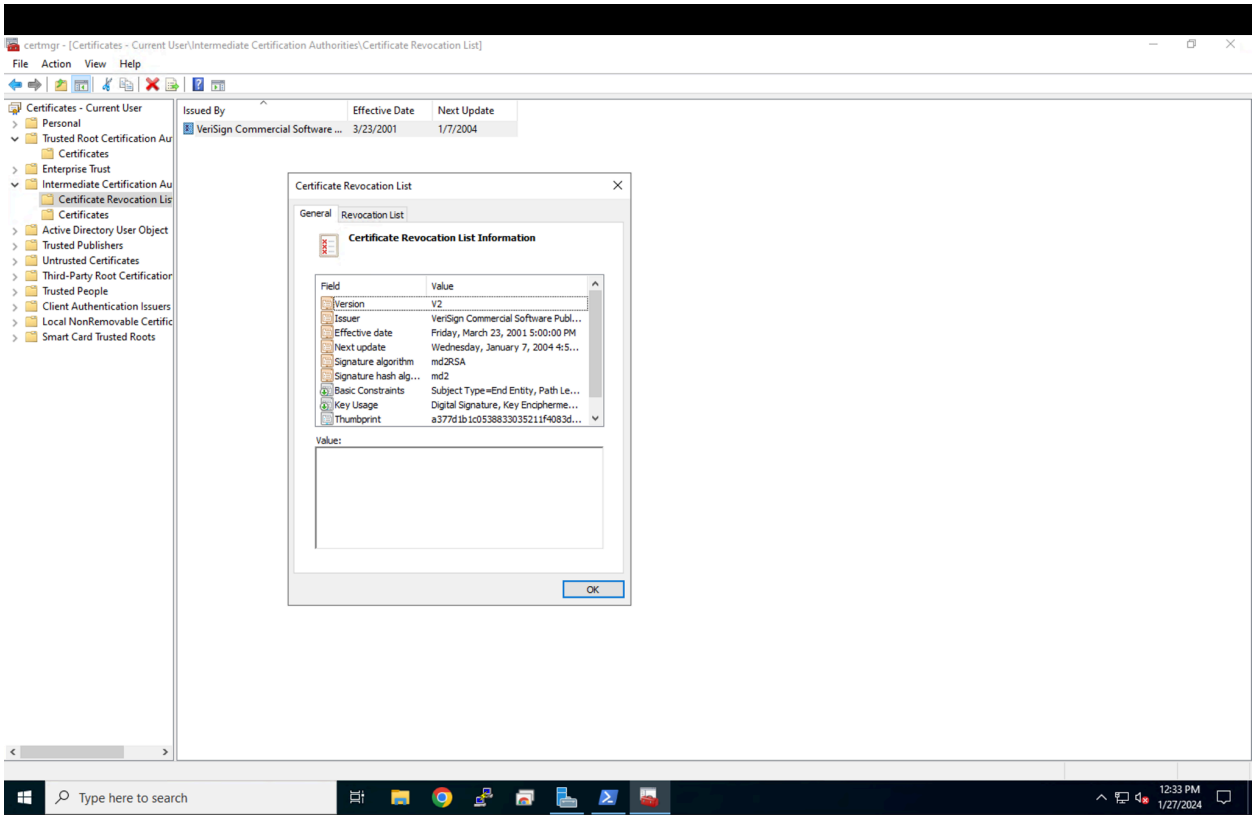




intermediate:

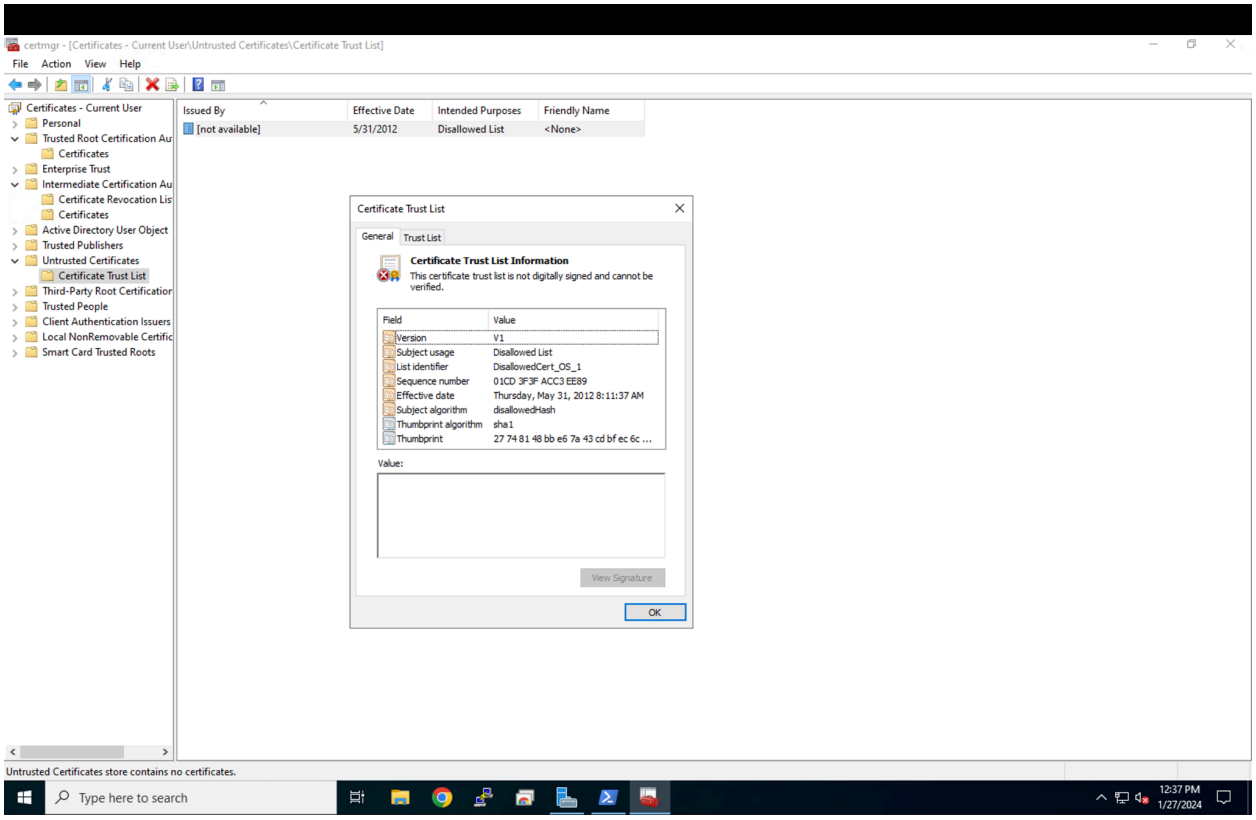


Revoked



The above certificate was revoked because it is super old, like older than me old.

Untrusted:



The above certificate was untrusted because it used sha1.