

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

The screenshot shows the Qualys SSL Labs SSL Report for the domain pgw.southwesterncc.edu. The report is dated Sat, 27 Jan 2024 17:59:21 UTC. The overall rating is A+. The summary section includes a large green 'A+' icon and a bar chart showing scores for Certificate (~95), Protocol Support (~95), Key Exchange (~85), and Cipher Strength (~85). Below the chart, a yellow box contains a link to the documentation page and a link to known issues. A blue box states that the site works only in browsers with SNI support. A green box indicates HSTS deployment. The certificate details section shows 'Certificate #1: RSA 2048 bits (SHA512withRSA)' and a server key and certificate icon.

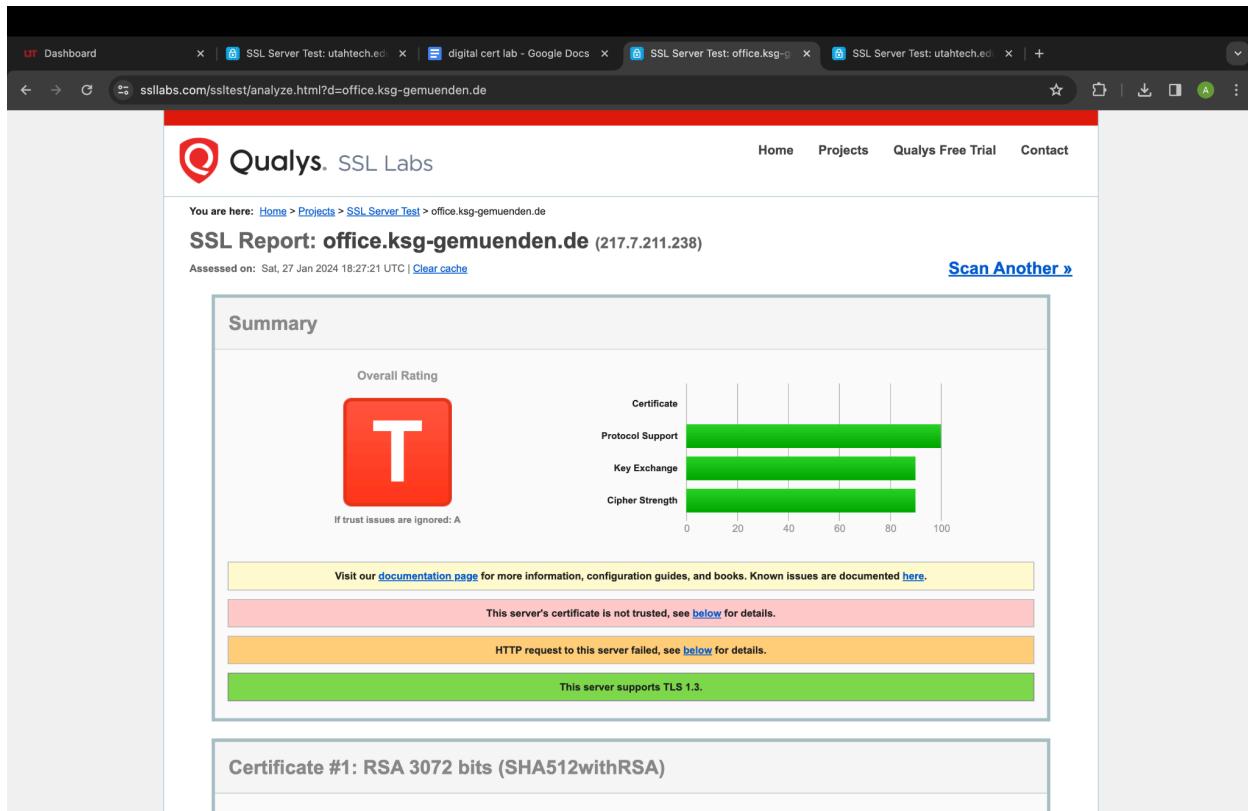
Bad: office.ksg-gemuenden.de

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



The screenshot shows a Qualys SSL Labs report for the domain office.ksg-gemuenden.de. The report is titled "SSL Report: office.ksg-gemuenden.de (217.7.211.238)". It was assessed on Saturday, January 27, 2024, at 18:27:21 UTC. A "T" grade is displayed prominently. The overall rating is "A". The report includes a summary of certificate support, protocol support, key exchange, and cipher strength. It also lists several issues and successes, such as "This server's certificate is not trusted" and "This server supports TLS 1.3". The report concludes with a note about documentation and known issues.

Overall Rating: **T** (A)

Certificate Support: 98/100

Protocol Support: 98/100

Key Exchange: 88/100

Cipher Strength: 88/100

If trust issues are ignored: A

Assessed on: Sat, 27 Jan 2024 18:27:21 UTC | [Clear cache](#)

[Scan Another »](#)

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server's certificate is not trusted, see [below](#) for details.

HTTP request to this server failed, see [below](#) for details.

This server supports TLS 1.3.

Certificate #1: RSA 3072 bits (SHA512withRSA)

Other: Utahtech.edu

Key: RSA 2048 bits (e 65537)

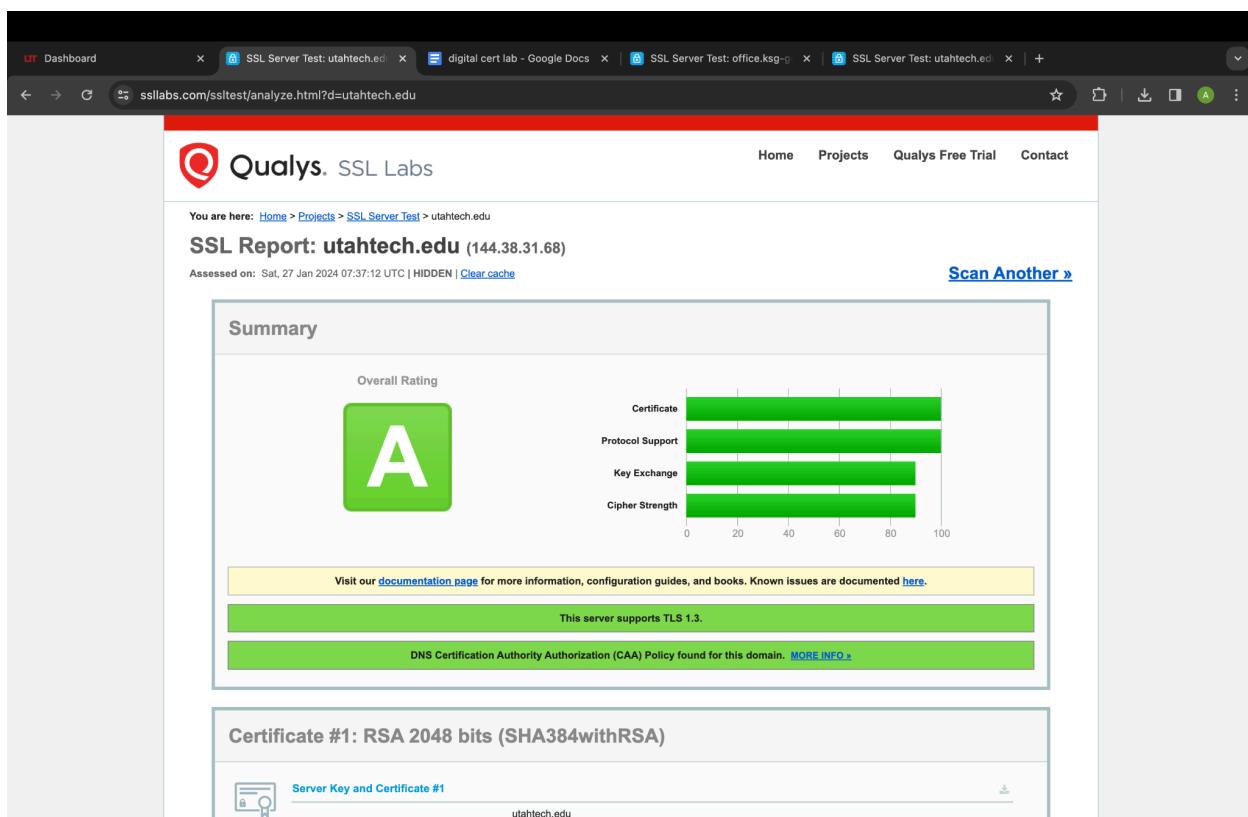
Revocation: CRL, OCSP

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:

The screenshot shows a Qualys SSL Labs test results page for a Google browser. The browser's address bar shows the URL: clienttest.ssllabs.com:8443/sslttest/viewMyClient.html. The page header includes the Qualys logo and navigation links for Home, Projects, Qualys Free Trial, and Contact. The main content area displays three sections: 'Protocol Support' (showing good protocol support), 'CVE-2020-0601 (CurveBall) Vulnerability' (showing non-vulnerability), and 'Logjam Vulnerability' (showing non-vulnerability). The 'Protocol Support' section notes that the user agent supports TLS 1.2 and TLS 1.3. The 'CVE-2020-0601' section provides a link to CVE-2020-0601 information and a manual test link. The 'Logjam' section also provides a link to weakdh.org and a manual test link.

Not vulnerable

Protocols: TLS 1.2, TLS 1.3

OCSP stapling: Yes

Safari:

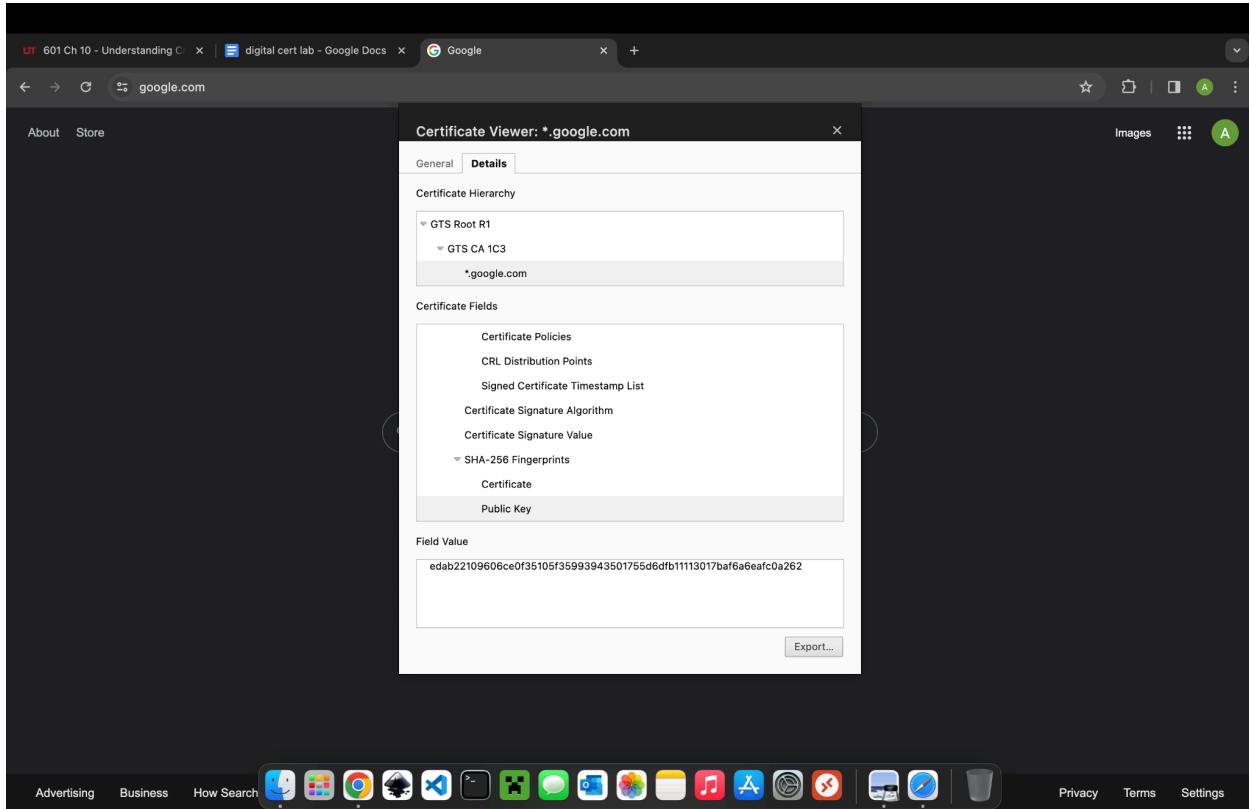
The screenshot shows a Safari browser window displaying the SSL Client Test page from SSL Labs. The page header includes the SSL Labs logo and navigation links for Home, Projects, Qualys Free Trial, and Contact. The main content area is titled "SSL/TLS Capabilities of Your Browser". It provides information about the user agent (Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.2.1 Safari/605.1.15). Below this, there are three sections: "Protocol Support" (Your user agent has good protocol support), "CVE-2020-0601 (CurveBall) Vulnerability" (Your user agent is not vulnerable), and "Logjam Vulnerability" (Your user agent is not vulnerable). At the bottom, a section titled "Part III: Viewing Digital Certificates" provides instructions to open a browser to www.google.com. A timestamp in the bottom right corner indicates the screenshot was taken on Saturday, January 27, 2024, at 12:18 PM.

Not Vulnerable

Protocols: TLS 1.2, TLS 1.3

OCSP stapling: Yes

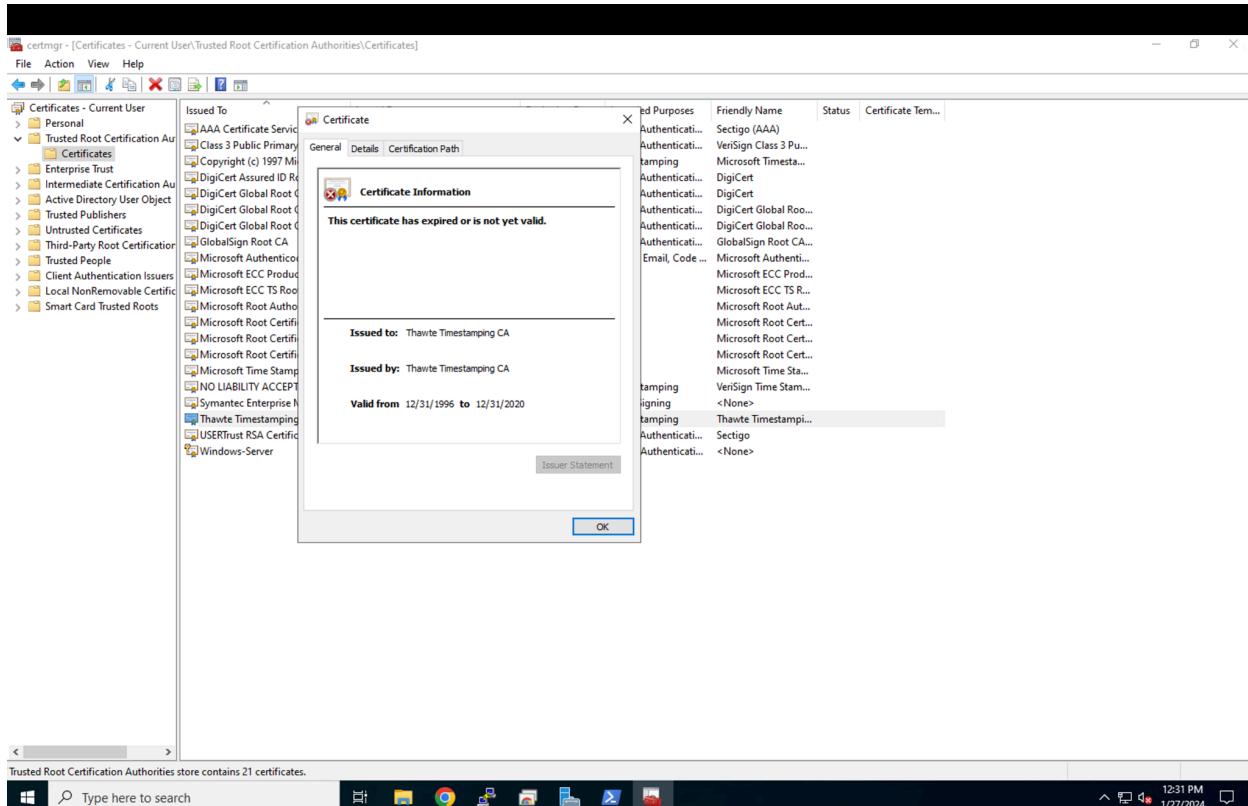
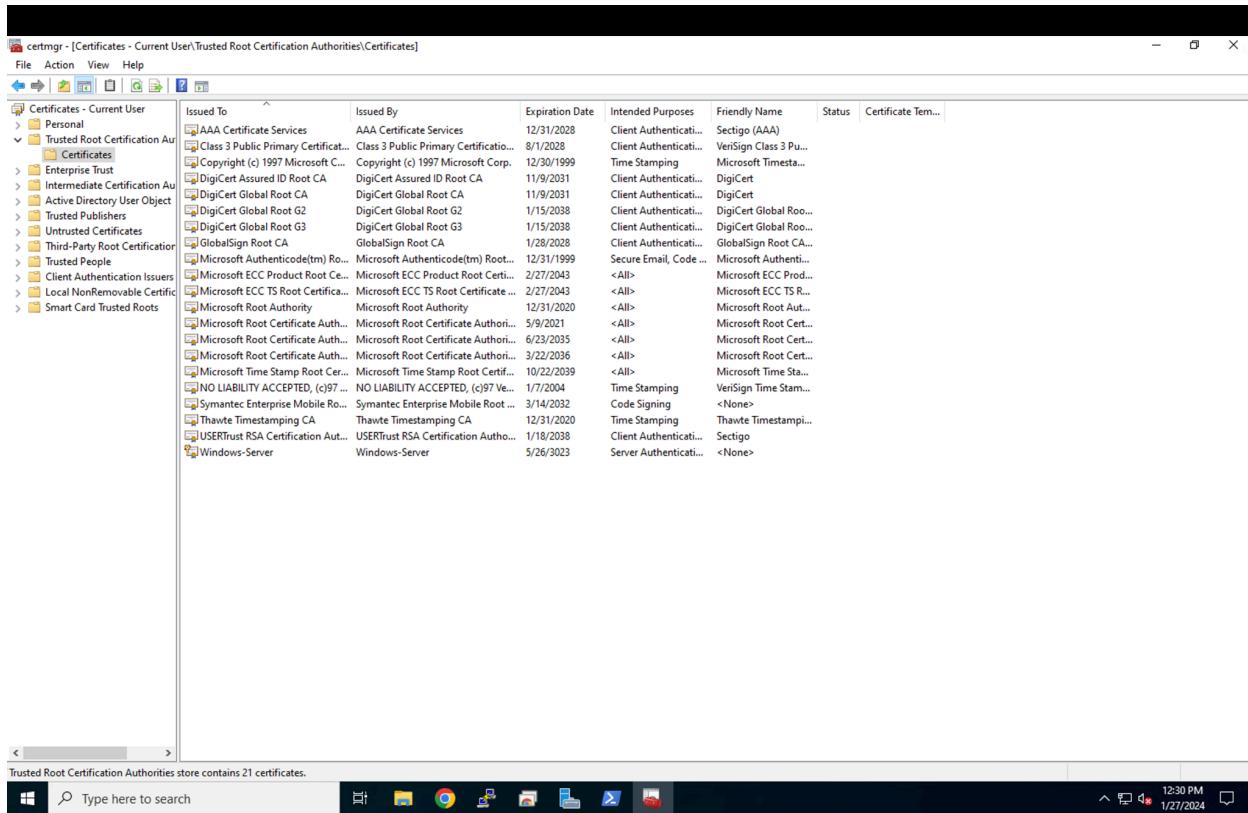
Google Certificate:



Expires sooner: google

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

Windows stuff :(



intermediate:

The screenshot shows the Windows Certificate Manager (certmgr.msc) window. The left pane displays a tree view of certificate categories under 'Certificates - Current User'. The 'Intermediate Certification Authorities' node is expanded, showing its sub-categories: 'Certificates' and 'Certificate Revocation List'. The right pane lists the certificates in the store, with columns for 'Issued To', 'Issued By', 'Expiration Date', 'Intended Purposes', 'Friendly Name', 'Status', and 'Certificate Type'. There are four certificates listed:

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Type
Microsoft Windows Hardware ...	Microsoft Root Authority	12/31/2002	<None>	Code Signing, Win...	Not Valid	Root
RapidSSL TLS RSA CA G1	DigiCert Global Root G2	11/2/2027	Server Authentication	<None>	Valid	Root
Root Agency	Root Agency	12/31/2039	<All>	<None>	Valid	Root
www.verisign.com/CPS Incorpor...	Class 3 Public Primary Certificatio...	10/24/2016	Server Authentication	<None>	Valid	Intermediate

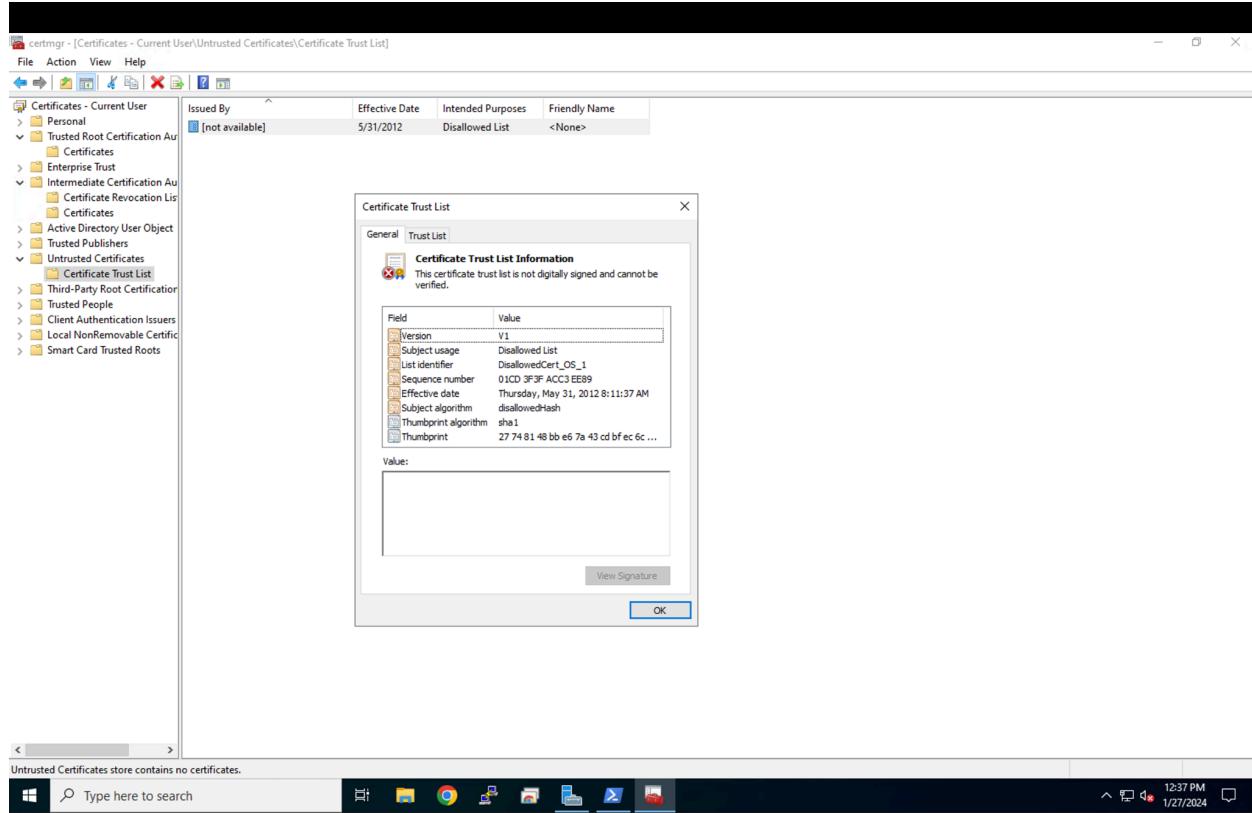
At the bottom of the right pane, it says 'Intermediate Certification Authorities store contains 4 certificates.'

Revoked

The screenshot shows the Windows Certificate Manager (certmgr.msc) window. The left pane displays a tree view of certificate categories under 'Certificates - Current User'. The 'Intermediate Certification Authorities' node is expanded, showing its sub-categories: 'Certificates' and 'Certificate Revocation List'. The right pane shows the properties of a certificate revocation list (CRL). A 'Certificate Revocation List' dialog box is open, displaying 'General' and 'Revocation List' tabs. The 'General' tab shows 'Certificate Revocation List Information' with fields like Version (V2), Issuer (VeriSign Commercial Software Publ...), Effective date (Friday, March 23, 2001 5:00:00 PM), and Next update (Wednesday, January 7, 2004 4:5...). The 'Revocation List' tab shows a table of revoked certificates, which is currently empty.

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.