

Lassine Pierre Guindo

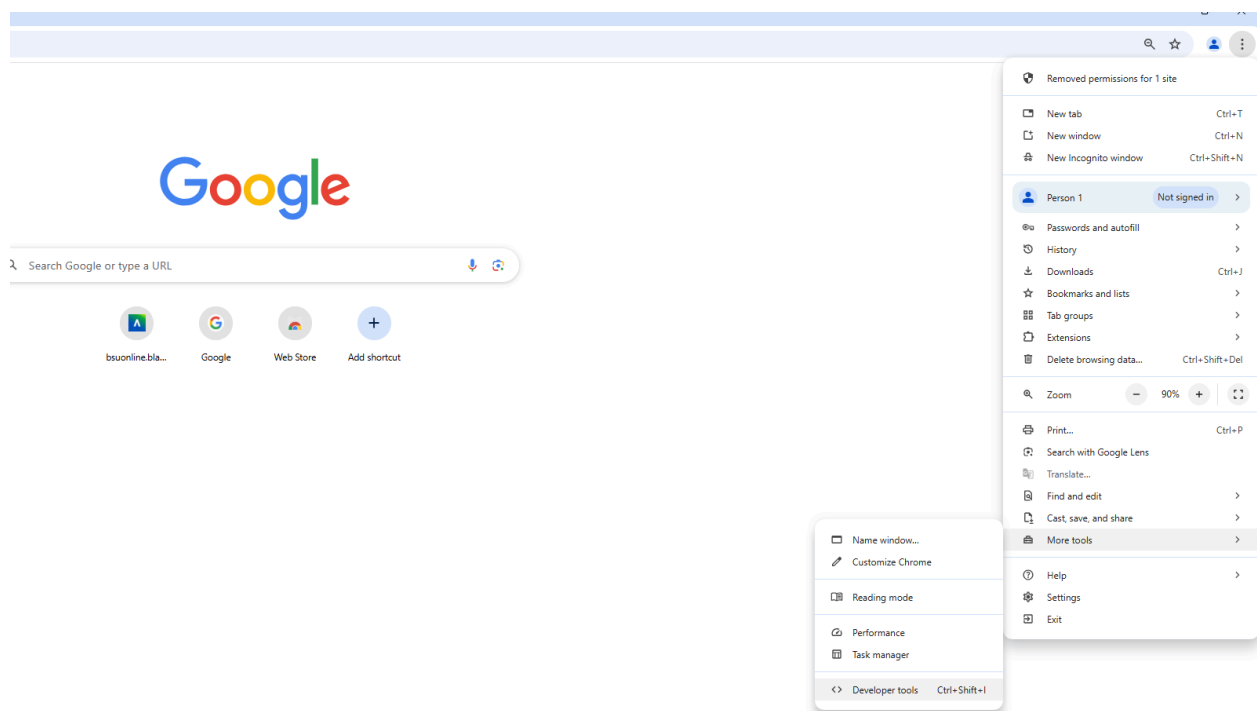
Lethia Jackson

CTEC445

February 27, 2025

## Digital certificate

### Project 4.2 Viewing Digital Certificates



**Step 1: Use the Google Chrome web browser to go to [www.google.com](https://www.google.com)**

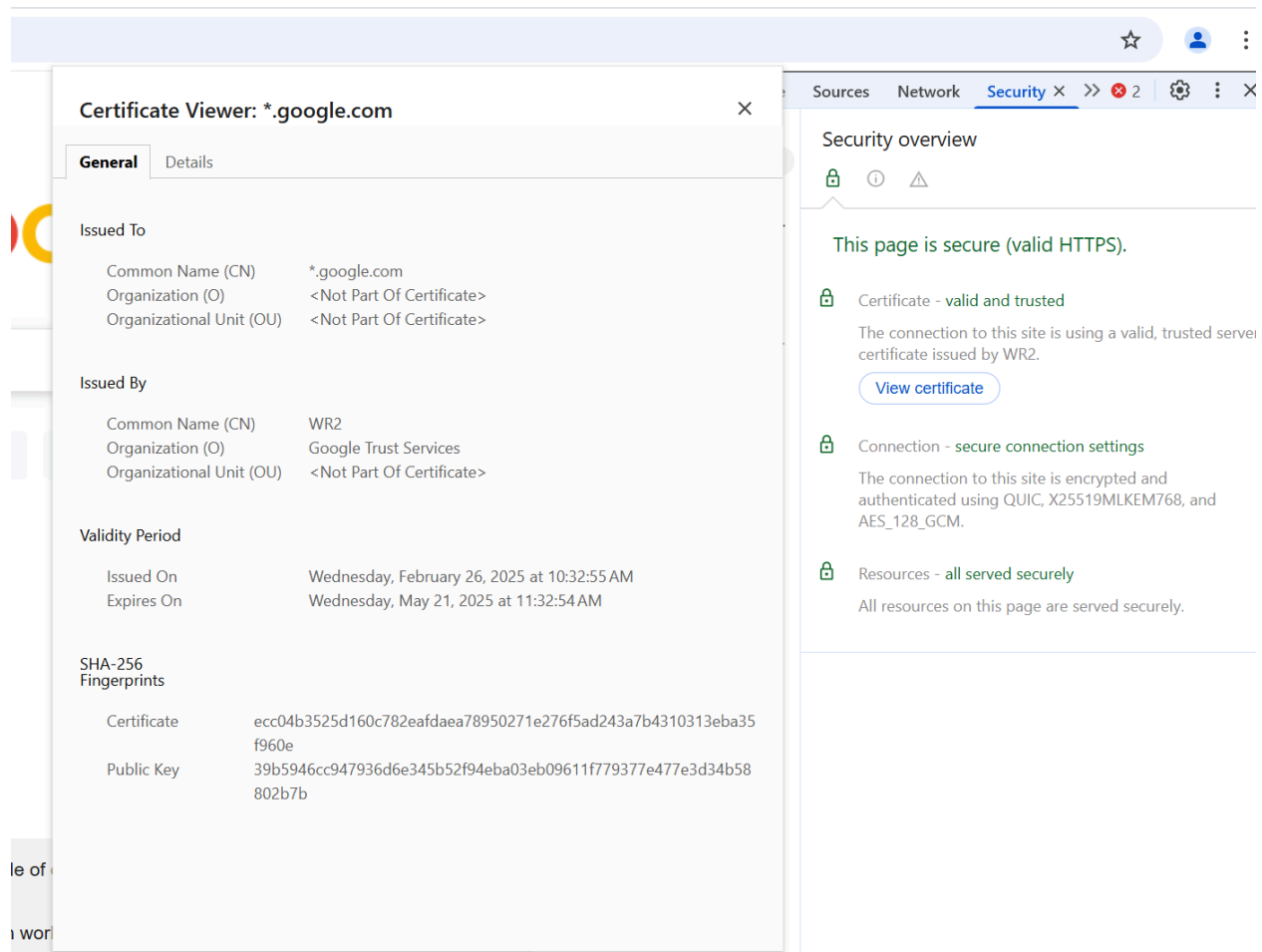
**Step 2: Note the green padlock in the address bar. Although you did not enter *https://*, nevertheless Google created a secure HTTPS connection. Why would it do that?**

**Google forces HTTPS to keep your connection secure and private. Even if you don't type *https://*.**

**Step 3: Click the three vertical buttons at the far edge of the address bar.**

**Step 4: Click More tools.**

## Step 5: Click Developer tools.

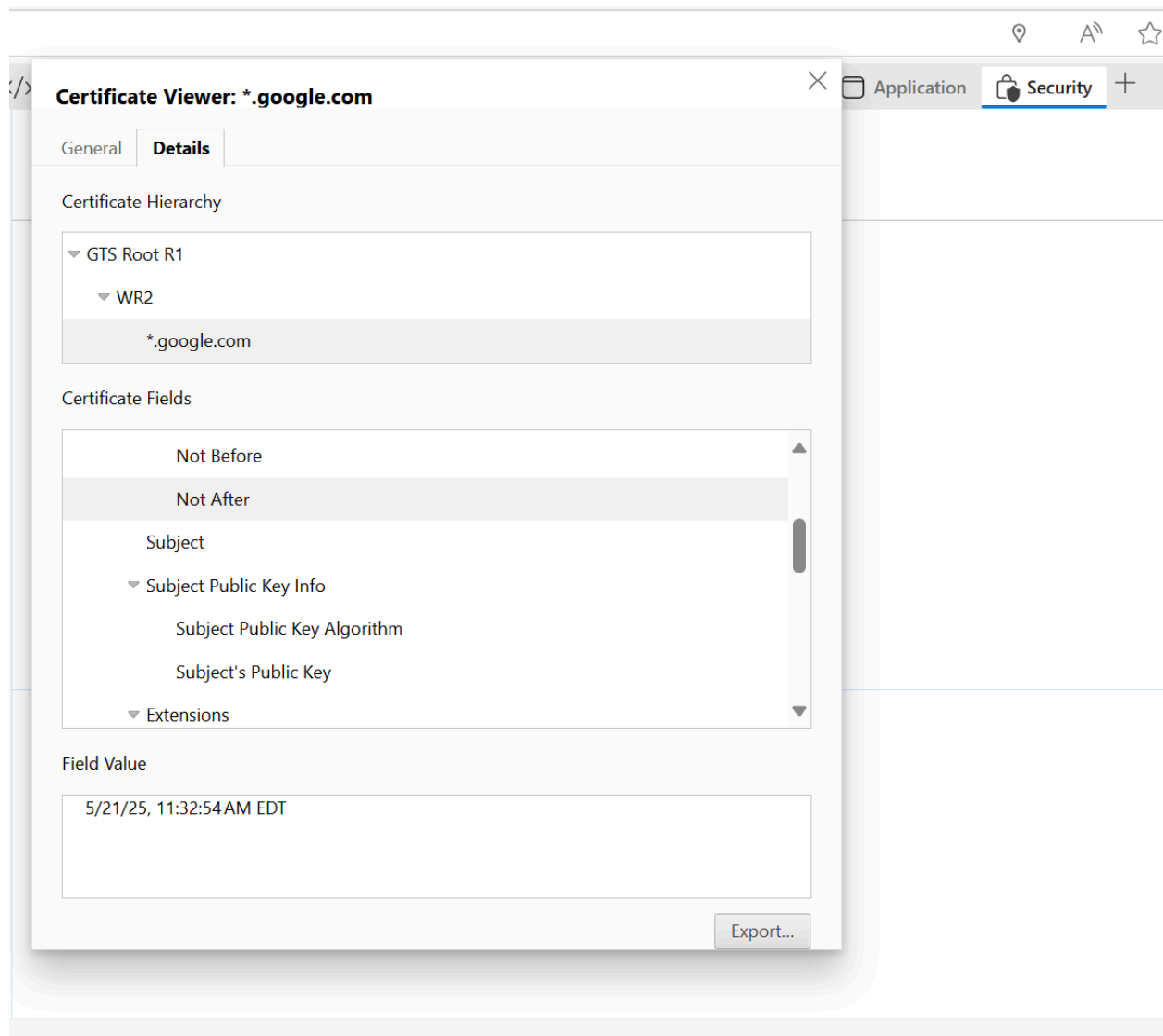


**Step 6: Click the Security tab (if the tab does not appear click the >> button to display more tabs).**

**Step 7: Read the information under Security Overview.**

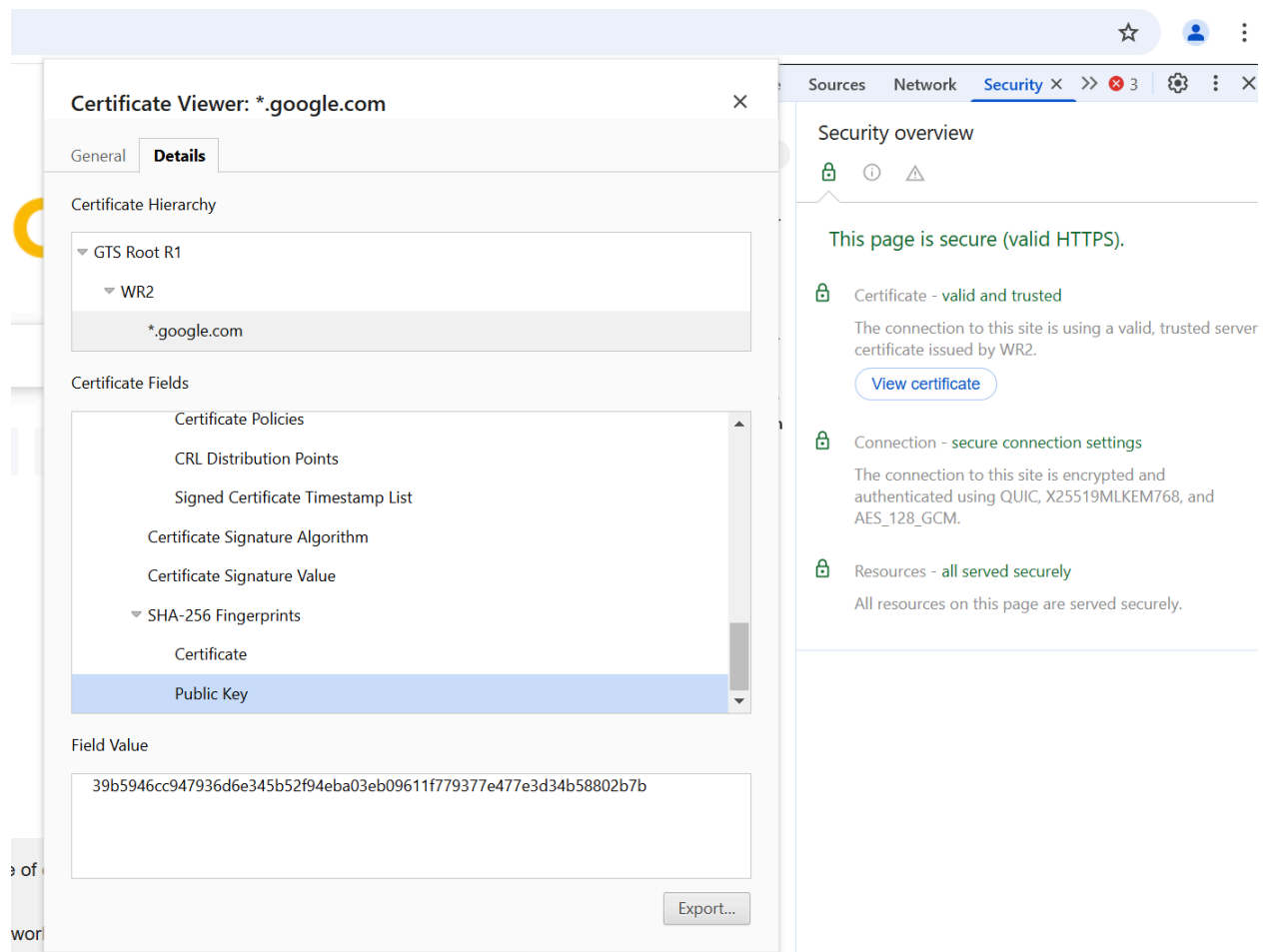
**Step 8: Click View certificate.**

**Step 9: Note the general information displayed under the General tab.**



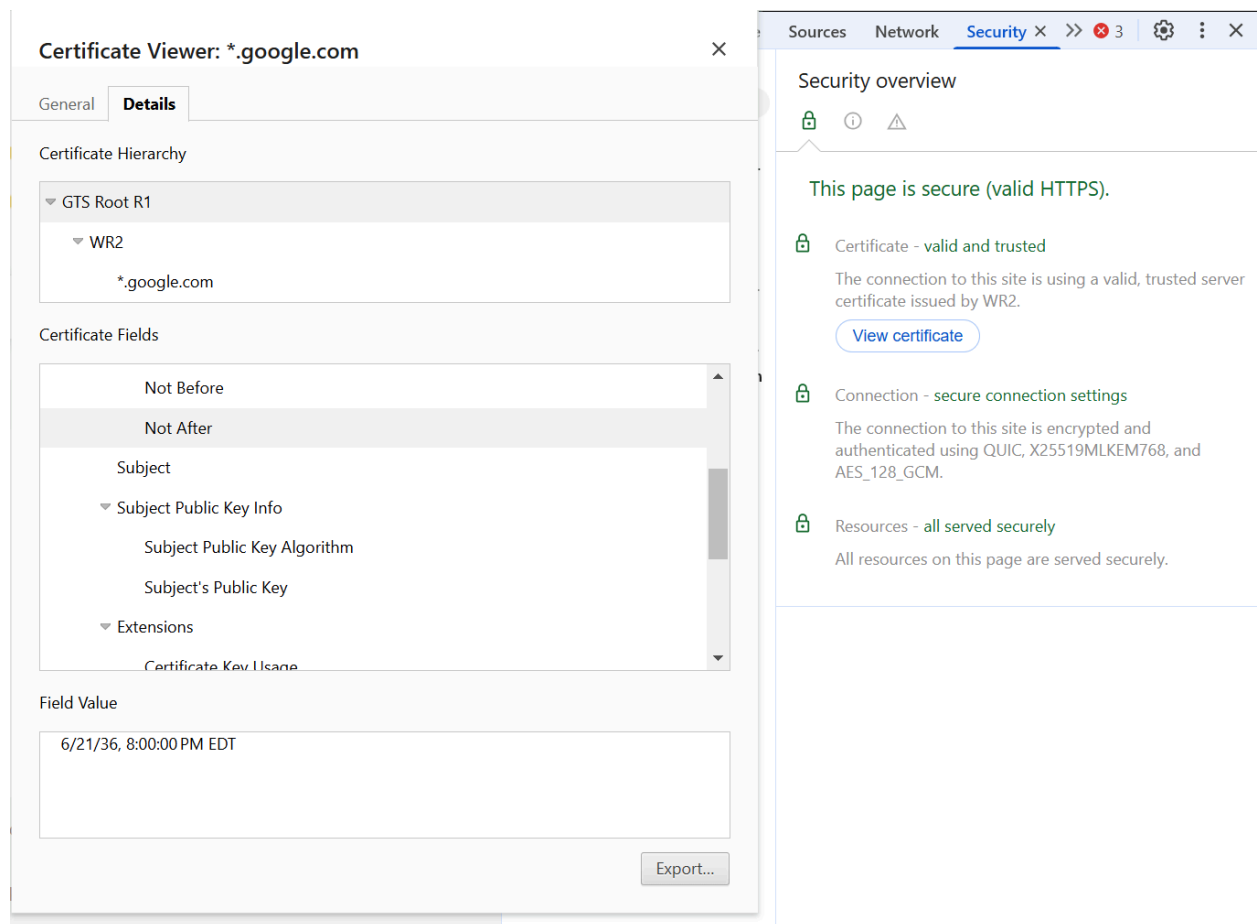
**Step 10 : Now click the Details tab. The fields are displayed for this digital certificate.**

**Step 11: Click Not After to view the expiration date of this certificate.**



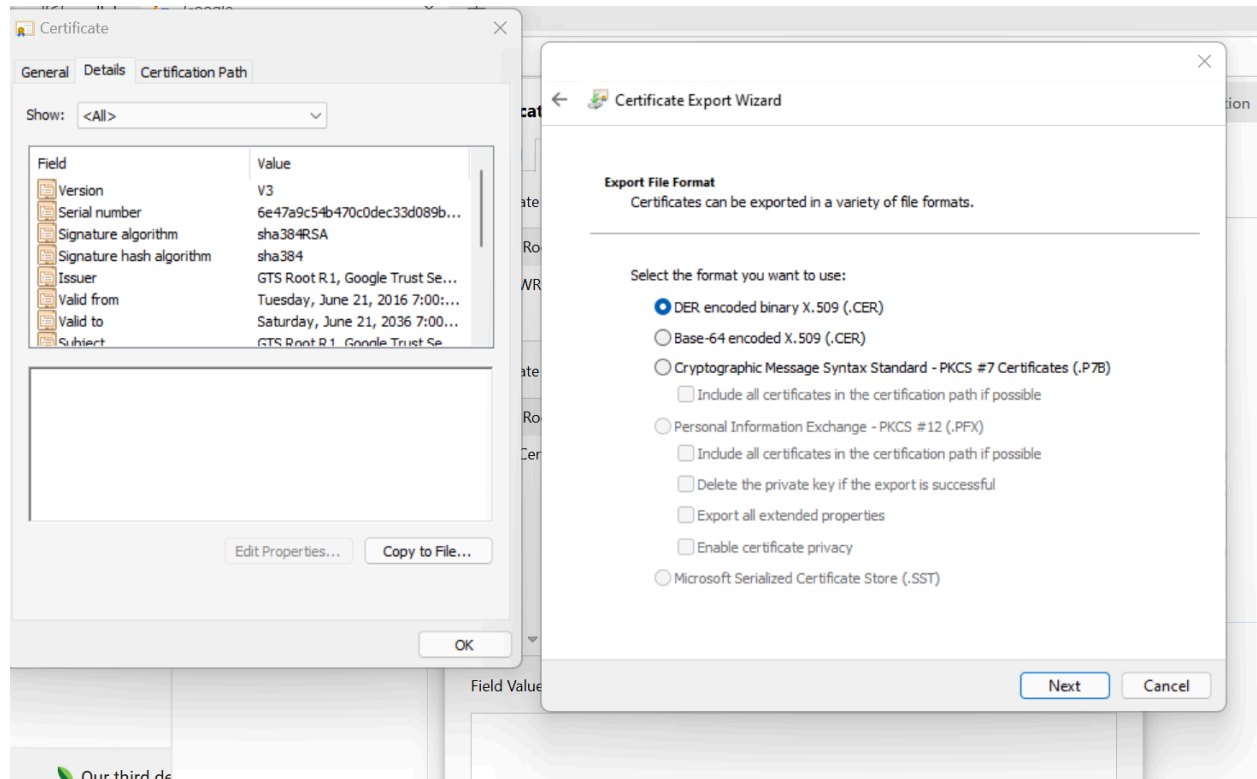
**Step 12: Click Public key to view the public key associated with this digital certificate. Why is this site not concerned with distributing this key? How does embedding the public key in a digital certificate protect it from impersonators?**

**Google shares its public key because it is safe to share. It only locks or encrypts data, but only Google's private key, which is kept secret, can unlock it.**



**Step 13: Click the Details Tab, there is a *path* to the root certificate. Click the GTS ROOT R1, and then click Not After. Why is the expiration date of this root certificate longer than that of the website certificate? Click OK and then click OK again to close the Certificate window.**

**The root certificate has a longer expiration date because it is issued by a trusted authority (CA) and is used to verify many other certificates. It lasts 10–20 years to avoid frequent updates.**



**Step 14: Click copy the File**

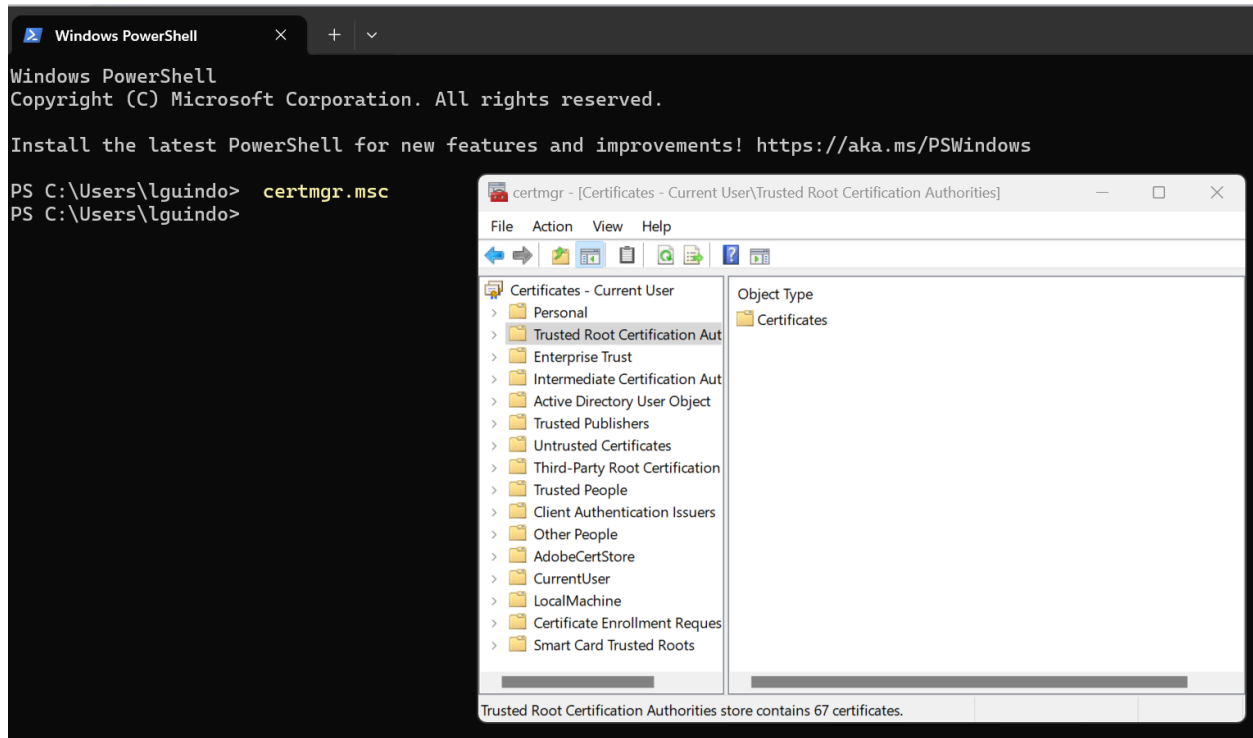
**Step 15: Click Next**

**Step 16: Note the different file formats that are available. What do you know about each of these formats?**

- **DER-encoded binary X.509** - Its a binary format, and used mainly for Windows and Java-based systems
- **Base-64 encoded X.509**- It is text-based format, and common for Linux, macOS, and web servers
- **PKCS#7**- Can include the full certificate chain (root + intermediate + website certificate,used in Windows and Java environments, and does not store private keys.and Close all windows.

**Step 17/18: Click Cancel to close this window, close all windows.**

## Project 4.3 Viewing Digital Certificate Revocation Lists (CRL) and Untrusted Certificates

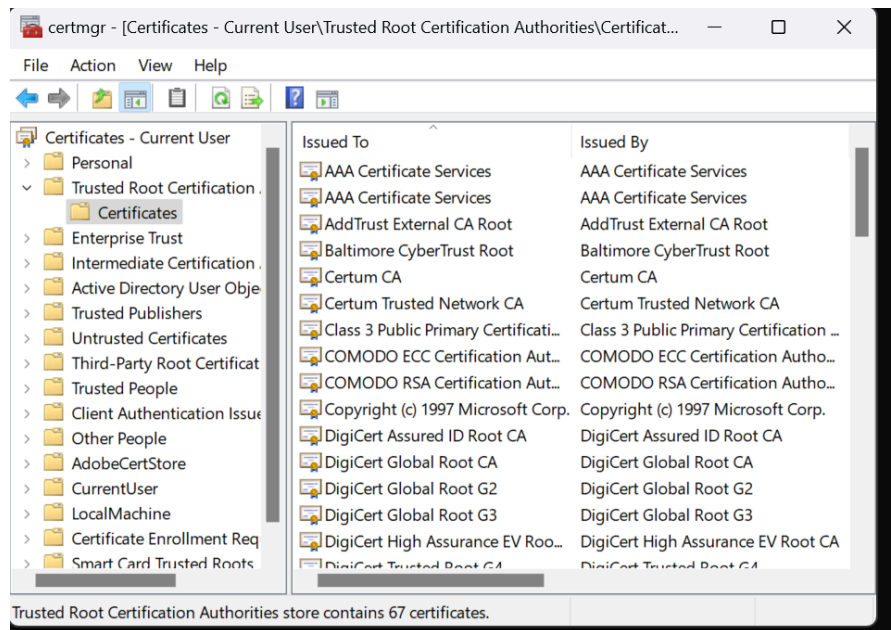


**Step 1: Click the Windows + X keys.**

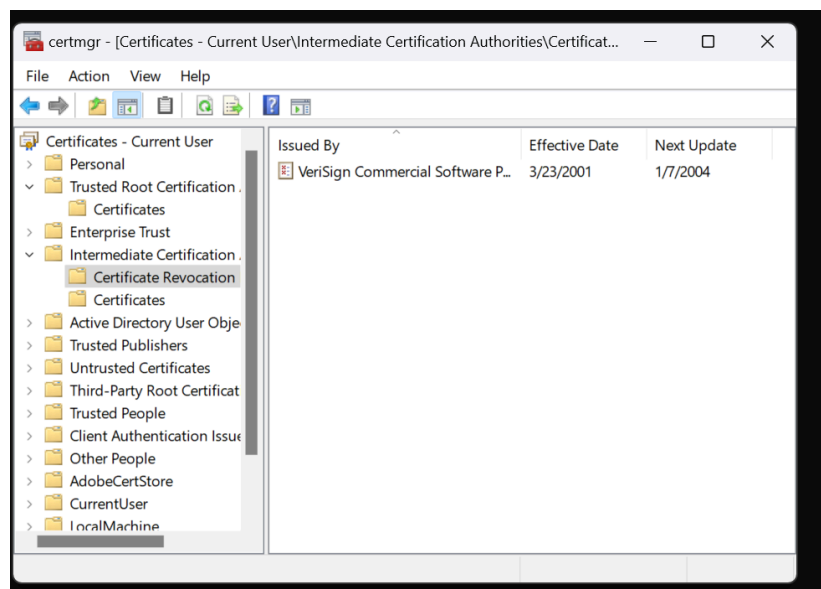
**Step 2: Click Terminal.**

**Step 3: Type certmgr.msc and then press Enter.**

**Step 4 : In the left pane, expand Trusted Root Certification Authorities.**



**Step 5: In the left pane, double click Certificates. These are the CAs approved for this computer. Scroll through this list. How many of these have you heard of before? I have heard of 5 of them**

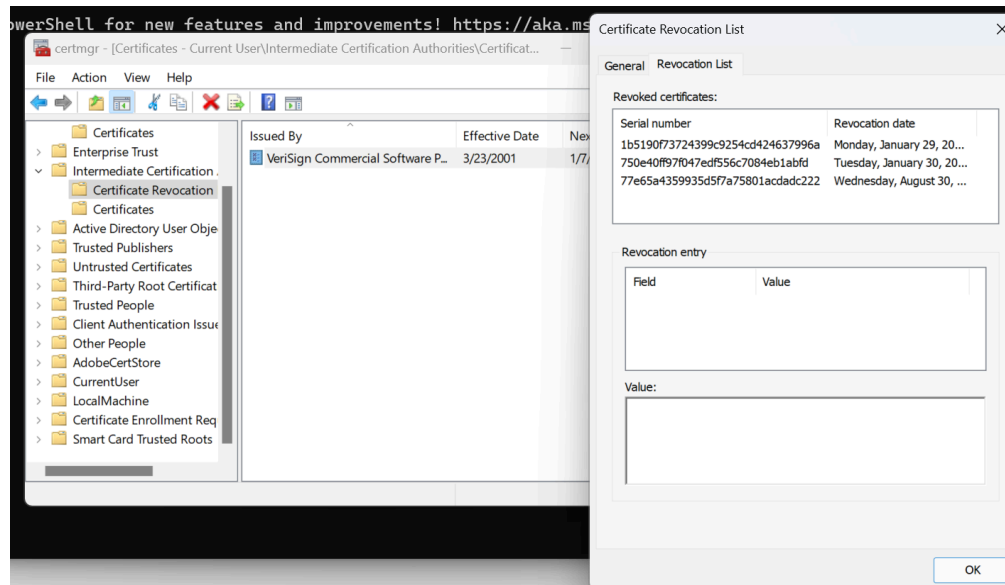


**Step 6: In the left pane, expand Intermediate Certification Authorities.**

**Step 7: Double-click Certificates to view the intermediate CAs. Scroll through this list.**

**Step 8: Click Certificate Revocation List.**

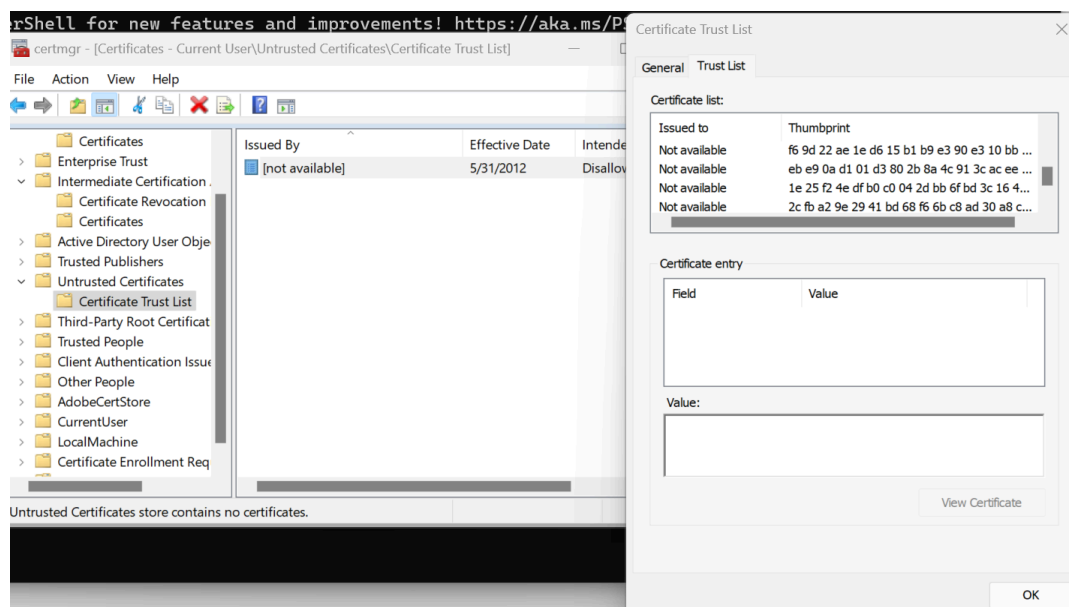




**Step 9: In the right pane, all revoked certificates will display. Select a revoked certificate and double-click it.**

**Step 10: Read the information about it and click fields for more detail if necessary. Why do you think this certificate has been revoked? Close the Certificate Revocation List by clicking the OK button.**

**A certificate is usually revoked if it is compromised, expired, or no longer trusted.**



**Step 11: In the left pane, expand Untrusted Certificates.**

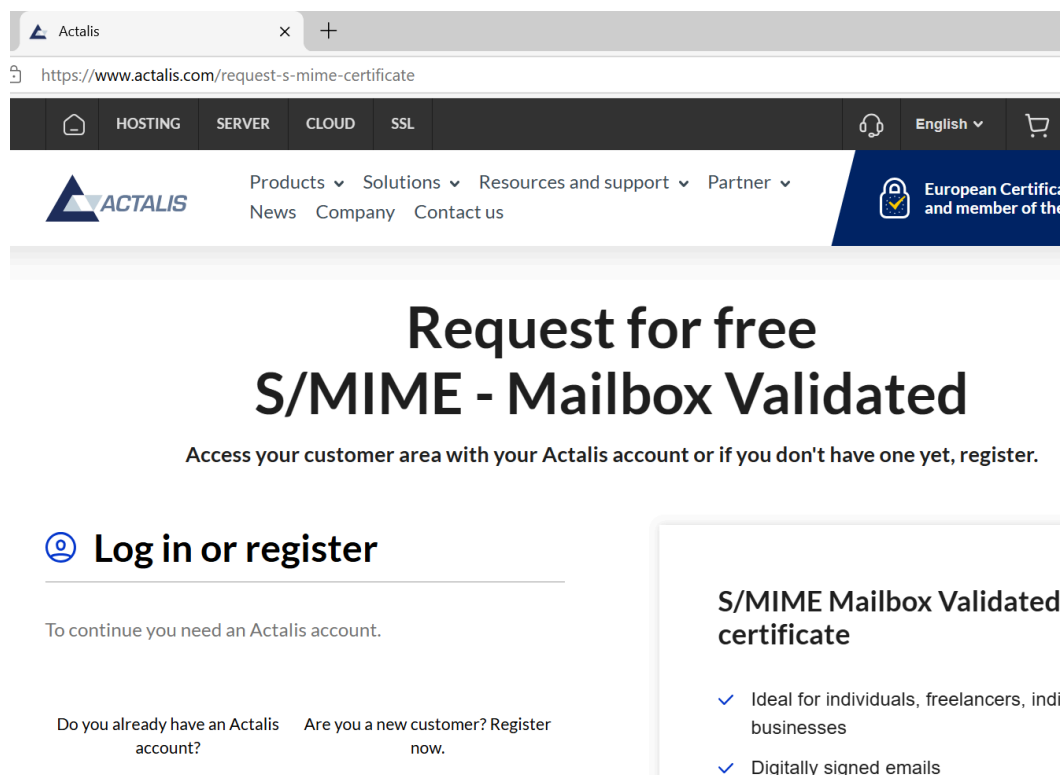
**Step 12: Click Certificates. The certificates that are no longer trusted are listed in the right pane.**

**Step 13: Double-click one of the untrusted certificates. Read the information about it and click fields for more detail if necessary. Why do you think this certificate is no longer trusted?**

**A certificate is no longer trusted if it is expired, revoked, or issued by an untrusted authority. Click OK to close the Certificate dialog box.**

**Step 15: Close all windows.**

## **Project 4.4 Downloading and Installing a Digital Certificate**



Actalis

https://www.actalis.com/request-s-mime-certificate

HOSTING SERVER CLOUD SSL

English

ACTALIS

Products Solutions Resources and support Partner News Company Contact us

European Certificate and member of the

# Request for free S/MIME - Mailbox Validated

Access your customer area with your Actalis account or if you don't have one yet, register.

## Log in or register

To continue you need an Actalis account.

Do you already have an Actalis account? Are you a new customer? Register now.

### S/MIME Mailbox Validated certificate

- ✓ Ideal for individuals, freelancers, indi businesses
- ✓ Digitally signed emails

**Step 1: Use the Microsoft Edge browser to go to <https://extrassl.actalis.it/portal/uapub/freemail?lang=en>.**

#### Email

Insert an email address

#### Password

\*\*\*\*\*



A secure and strong password must contain at least 10 characters, numbers and letters, one uppercase and one lowercase letter and at least one special character between !"#%&'()\*+,-./:;<=>?@[\\]^\_`{|}~

#### Repeat password

\*\*\*\*\*



By pressing the "Confirm and continue" button I declare that I have read the [Privacy Policy](#) of Actalis S.p.A.

I give my consent to receive discounts and promotions on all services offered by Actalis and Group companies.

☒ Accept

☐ Decline

**Step 2: Click on create your Actalis account. Enter your email address and enter a password to create an account.**

**Step 3/4: Check your email, and retrieve the email verification code.**

#### Log in or register

We have sent an email with the verification code to the mailbox:  
**guindolassine2@gmail.com**

#### Verification code

Verification code

Verify

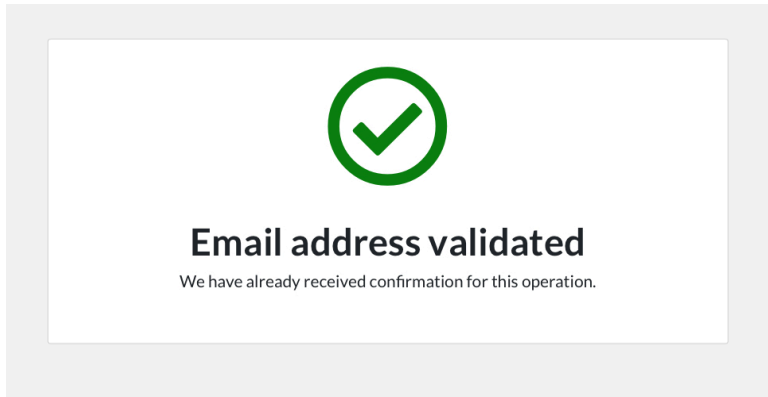
Didn't receive the email?

[Receive a new verification code](#)

#### S/MIME Mailbox Validated certificate

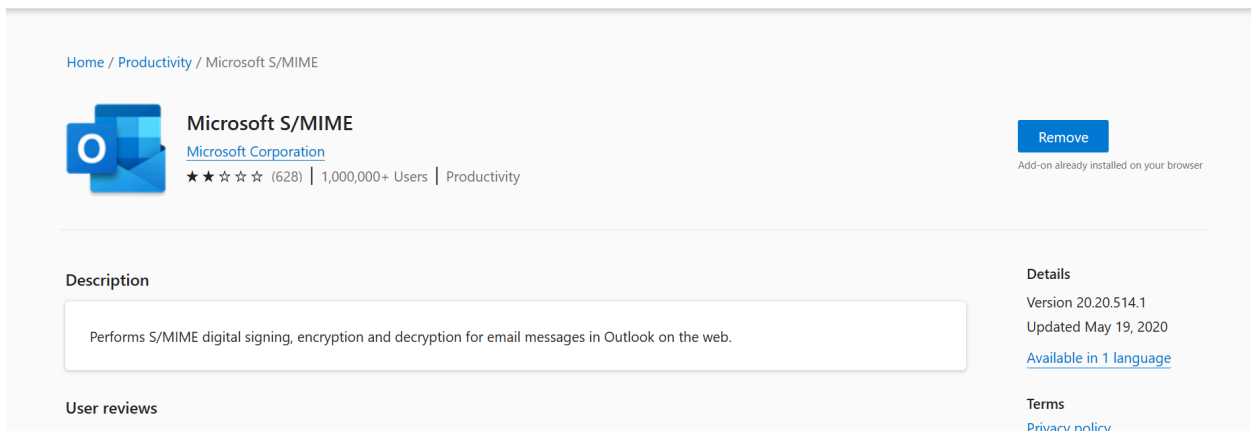
- ✓ Ideal for individuals, freelancers, individual businesses
- ✓ Digitally signed emails
- ✓ Encrypted emails
- ✓ CA Root **Actalis S.p.A.**
- ✓ Release in a few minutes
- ✓ Valid for **1 year**

**Step 5: Return to the Actalis page and enter the verification code.**



**Step 6: Return to your Microsoft Outlook email account, and click on the confirm email.**

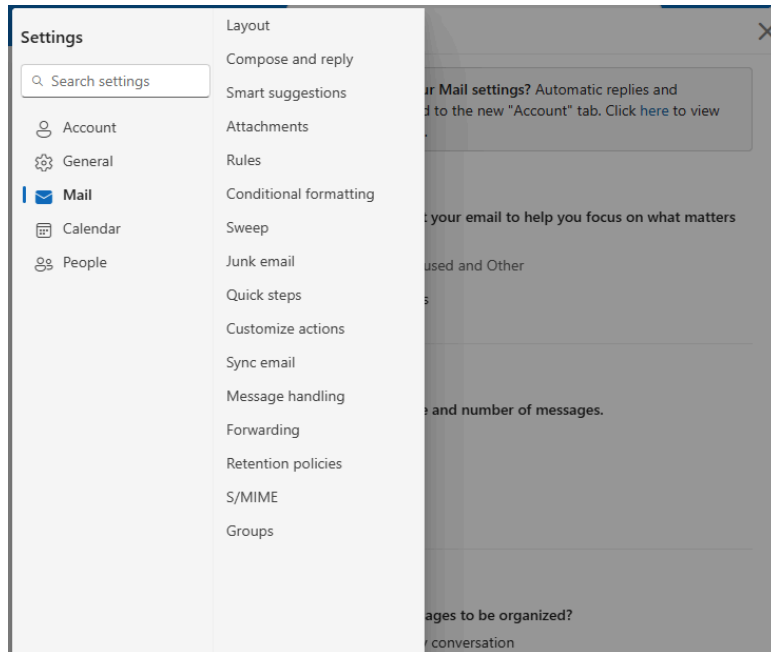
**Step 7: Record the displayed password.**



**Step 10: Click Get**

**Step 11: Click Add extension. An icon will appear at the top of the browser.**

**Step 12: Return to your Microsoft Outlook email account.**



**Step 13: Click the Outlook settings icon.**

**Step 14: Enter Mail in the search box.**

**Step 15: Click S/MIME.**

**STEP 16: Under To install S/MIME control click Click here.**

**Step 18: Now all of the messages sent will have a digital signature.**

**Step 19: Close all windows.**