SUMO KB Article work in progress: Instructions for obtaining a personal S/MIME certificate by creating a CSR
WARNING: This feature is currently being developed. It is scheduled to be released in Thunderbird 128. This feature is not supported until 128 is released which is currently planned for summer 2024.

Obtaining a personal S/MIME certificate is a multi-step process:

1. Create your public and secret key
2. Get a certificate using your public key from your Certificate Authority (CA)
3. Import the certificate into Thunderbird
4. Configure Thunderbird to use S/MIME security
5. Backup your certificate

Create your public and secret key

A personal certificate is required for using end-to-end encryption and digital signatures with the S/MIME technology.

A certificate consists of a key pair: a secret key and a public key. The keys will be randomly created by Thunderbird. The private key will be stored by Thunderbird, optionally protected by the Primary Password. The public key will be included in the certificate. Before you get your certificate, the public key must be submitted to a CA as part of a Certificate Signing Request (CSR), which Thunderbird will create for you.

1. Click ≡ > Account Settings> End-To-End Encryption for the desired email account or identity.
2. Scroll down to **S/MIME**: click Generate and save a CSR file as…

First, you will be asked to select a directory and a filename in which the CSR text will be saved. You should remember what you enter here, because at a later time, you will have to use your computer's file explorer to locate this file and open it, because you will need to submit the contents of this file to a CA.

Second, you will be asked several questions about the cryptographic type and strength of the S/MIME certificate that you wish to obtain. Unless you have a detailed understanding of your requirements, use the defaults.

After you have answered all questions, Thunderbird will proceed with an intensive calculation process, during which your new key pair will be randomly created. Please be patient while this operation executes, Thunderbird may appear to be stuck for a few seconds, but it should be done within a minute on modern computers.

Thunderbird will show a confirmation after the operation has completed.

Get a certificate using your public key from your CA

The next step is that you get in contact with a CA of your choice. If you are associated with a company or an organization, you may wish to ask your staff which CA you should use. If you are acting as an individual, you may wish to search the web for CAs that issue S/MIME certificates and that accept a CSR. (At this time, Thunderbird doesn't recommend any specific CA.)

The process to obtain a certificate may require you to setup a user account with a CA, register your personal details, set up a payment method, and it typically involves verification of your email address.

Eventually the CA should ask you to submit your CSR. At this point, use your computer's file management tool, and open the file that Thunderbird had saved earlier, in the directory and using the filename that you had chosen. Your computer should show you the contents of the file. The first line of the file will contain the text:"`-----BEGIN CERTIFICATE REQUEST-----`".

Please select the full contents of the file, and use the copy command to copy all of the text. Then navigate back to your interaction with the CA (for example to the web form in your browser, on the CA's web page, which asks to you submit the CSR), and paste the text into that location, and continue.

After your interaction with the CA is complete, it should notify you that the certificate has been issued or will be issued soon. It may offer you the certificate for download immediately or at a later time, or send it to you by email.

Save the certificate you have received to your local computer and remember where you have saved it. If you're using Firefox, it might save it in your Downloads folders.

If you are downloading from a web page using your browser, check whether that page lists additional intermediate certificates, which you also might have to download.

Note: If the CA delivered the certificate to you in a file with a filename extension .p12 or .pfx, it may indicate that the CA didn't use the key that you had submitted, but instead generated a secret key on their systems. This may not be what you want.

Import the certificate into Thunderbird

1. Click ≡ > Account Settings> End-To-End Encryption for the email account or identity you used earlier.
2. Click Manage S/MIME Certificates. If the **Certificate Manager** window is too small, drag its lower right corner to increase the window size.

3. **Certificate Manager** has five tabs at the top. Click the People tab > Import button at the bottom. Select the file that you have obtained from the CA, and confirm. If the import was successful, no further information will be shown, you'll simply return to the certificate manager window. Because Thunderbird still had remembered the corresponding secret key, which was created during the initial steps of this process, Thunderbird should have been able to combine it with the certificate you just imported.
4. Still in **Certificate Manager**, click Your Certificates. You should see your new personal certificate in the list.

Backup your certificate

Now that you have added your personal certificate to Thunderbird (which consists of a secret key and public certificate combined), you should create a backup. Select the entry that shows your new personal certificate, and click Backup.

First, you will be asked to select the directory and the filename in which the backup will be stored.

Then, follow the steps shown on screen, which includes defining a password of your choice to protect the backup file, to complete the backup procedure. Make sure to save the backup file to an appropriate location, such as a flash drive on which you keep important backups, and save the password somewhere secure like your password manager.

Configure Thunderbird to use S/MIME security

1. Click ≡ > Account Settings> End-To-End Encryption for the email account or identity you used earlier.
2. In the section below the ```S/MIME heading```, you will find two selection boxes labeled: “**Personal certificate for digital signing** and” **Personal certificate for encryption". Click the Select... button on the right.**
3. A list will be shown with your personal certificates for this email address. The certificate that you have just obtained should be offered in that list. Select it and confirm it. Thunderbird may ask you to use the same certificate for both encryption and signing, which usually you should confirm.
4. If your CA offered you additional intermediate (or subordinate) certificates to download, click the Authorities tab, click the Import button, and import them one after the other. Note that when importing a CA in this place, Thunderbird will offer you to mark a CA as trusted, and also warn you about the associated risks. Please leave the checkboxes

unchecked, do NOT check them. Confirm by clicking OK which will import the intermediate without assigning explicitly trust.

Now you should be able to use your personal certificate for sending digitally signed email, and for receiving encrypted email using the S/MIME technology, as long as the certificate has not expired. Once the certificate expires, you will have to repeat the procedure to obtain a new personal certificate.