# How to Get an SMIME Certificate

## Step 3: install the certificate to your email programme

Now that you have downloaded your SMIME certificate, you can install it to your email programme. Please choose your favoured programme from the list and follow the respective instructions.

Mozilla Thunderbird Outlook Apple Mail

### Mozilla Thunderbird:

To be able to use your S/MIME certificate for your emails, you will have to first install it in the certificate manager. The path to get there differs a bit from Windows to Mac. Once there, the procedure is more or less the same.

#### **Open Certificate Manager in Windows:**

Open Thunderbird and go to "Tools" in the menu bar at the top, then select "Options". There, choose "Advanced" and "Certificates". Click on "Manage Certificates".

#### **Open Certificate Manager on Mac:**

Open Thunderbird and go to "Thunderbird" in the top menu bar and then on "Account Settings". There, choose "End-to-End Encryption" on the left hand side. Click on "Manage S/MIME Certificates".



#### Install certificate for both systems:

The certificate manager will open. There, please select "Your Certificates" and click on "Import". Select the .p12 certificate file from the folder you have saved it to earlier.

	Certificate Ma	anager		
Your Certificates	Authentication Decisions	People	Servers	Authorities
ou have certificates from	these organisations that identify you	I		
Certificate Name	Security Device	Serial Number	Expires	On [t
View Backup	Backup All Import	Delete		

You will be asked to enter the password you have set for your certificate. Please enter the password and click "Okay" (or "Sign In" on Mac).

You will be taken back to the certificate manager window where you should now be able to see your file in the list. Click on "Okay" to close the certificate manager.

Your Certifica	tes Auther	tication Decisions	People	Servers	Authorities	
u have certificate	s from these organi	sations that identify y	/ou			
Certificate Name	Secur	ity Device	Serial Number	Expires On		
<ul> <li>Verein zur Foer</li> </ul>	derung ei					
Lena Dreher	Softwar	e Security Device		13. Jun	une 2025	
		All Incoment	Delete			

Now, we need to implement the certificate for new emails.

For that, we go back to the Account Settings.

In **Mac**, you are already there, this was our starting point. Please click on "Select …" under "Personal certificate for digital signing"

<b>É Thunderbird</b> File Edit View	Go Message Events and Tasks Tools Window Help
🗧 🗧 🗧 🖾 Inbox	Account Settings X
<ul> <li>Inbox</li> <li>Inbox</li> <li>Server Settings Copies &amp; Folders</li> <li>Composition &amp; Addressing Junk Settings Synchronisation &amp; Storage End-To-End Encryption Return Receipts</li> <li>Local Folders Junk Settings Disk Space</li> <li>Outgoing Server (SMTP)</li> </ul>	<b>Control Settings</b> X <b>End-To-End Encryption</b> To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME. Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. Learn more <b>OpenPGP</b> Thunderbird doesn't have a personal OpenPGP key for <b>lena.dreher@uni-konstanz.de Add Key</b> Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above. <b>OpenPGP Key Manager S/MIME</b> Personal certificate for digital signing: <b>Select Clear</b>
Account Actions S Thunderbird Settings Add-ons and Themes	Manage S/MIME Certificates       S/MIME Security Devices         Default settings for sending messages         Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.         Disable encryption for new messages         Enable encryption for new messages         You will be able to disable encryption for individual messages.         A digital signature allows recipients to verify that the message was sent by you and its content was not changed. Encrypted messages are always signed by default.         Sign unencrypted messages

In **Windows**, please select "Tools" and "Account Settings" from the menu. On the left hand side, please choose "Security". For "Digital Signing", please click on "Select".

**In both systems**, a new window will open showing the details of your certificate file. Please check it is the file you have just imported and click on "OK".

A window will open asking you if you would like to use the same certificate to encrypt & decrypt messages. Click on "Yes".

You will now be back to the Account Settings. We recommend ticking the box for "Digitally sign messages (by default)" in **Windows**. To finish, please click "OK".

In **Mac**, please tick the box "Enable encryption for new messages" as the default settings for sending messages as well as the box "Sign encrypted messages" underneath (encrypted messages are signed by default).



To send signed and/or encrypted emails, when writing a new email, in **Windows** click on "Security" in the menu of the new email window. There, please select "Encrypt This Message" and "Digitally Sign This Message".

In **Mac**, please activate "Encrypt" and make sure under "S/MIME" the topics "S/MIME" and "Encrypt and Digitally Sign" are ticked.

Your emails should be automatically signed with your SMIME certificate now.



To send encrypted emails, you and your email partner will both need certificates. If both certificates are published, you can exchange encrypted emails from the first contact. If they are kept private, your email programme will need a first email contact with the new recipient/sender to be able to send/receive encrypted emails. So, please do not let yourself get confused if a failure message for encryption appears when sending emails to someone for the first time.