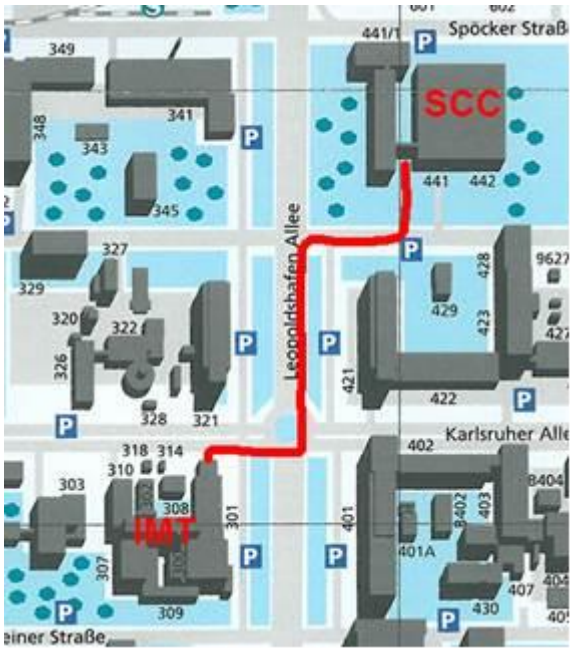
Configuration of Outlook for digital signing and encryption

On the following pages you will find instructions on what you need to do in order to sign e-mails in Outlook and if necessary encrypt them.

First, you must apply for a certificate from KIT-CA.

- **Instructions for applying for certificates**
  - Internet Explorer (Microsoft Windows)
  - Mozilla Firefox (all systems)

The printed form must be taken to the service desk of the computing center SCC (Bldg. 441, Room 165). The best way is to go into the glazed passageway between the two parts of the building and then turn right. The Service Desk will then be on the right-hand side. It is clearly marked by a sign. Please do not forget your passport. With the form you do not need any additional signatures from the Institute other than your own signature.



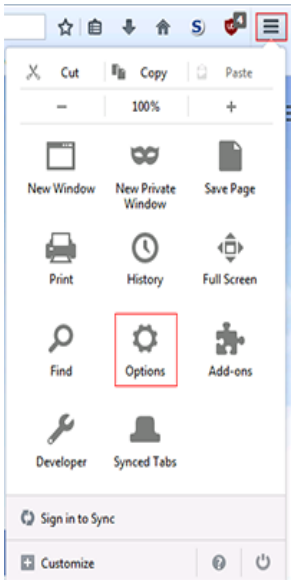
If you have applied for a certificate, you must first wait until you receive your certificate from SCC by e-mail. In this mail there is a link with which you can and must import your certificate into the browser. You have to use the same PC and the same browser you used for applying for the certificate! For IMT PCs you can ignore the link for the CA certificates specified in the mail, since these certificates are usually already installed there. For non-IMT PCs however, all these CA certificates must also be imported in the order specified on https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2&RA_ID=0 (from left to right).

Afterwards, you must create a backup of the certificate and configure the certificate in Outlook. On the following pages you will find instructions on how to back up the certificate using Firefox. For instructions on how to use Internet Explorer, visit https://www.ca.kit.edu/129.php

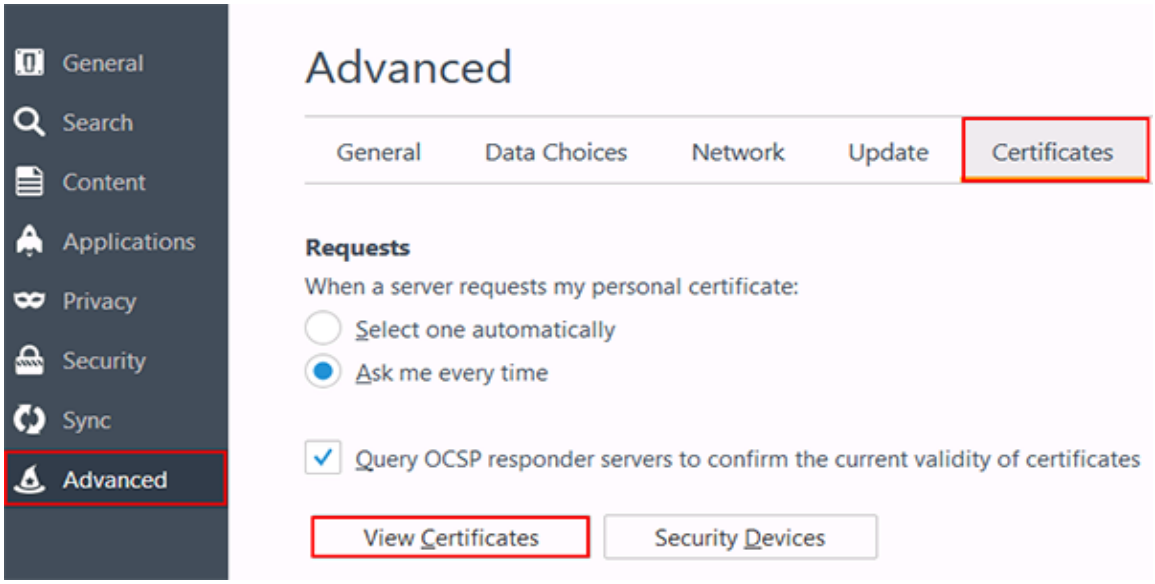
Create certificate backup - Mozilla Firefox

In order to create a backup with Mozilla Firefox, a certificate must have been requested and collected beforehand. If you have not already done so, please do so before:
https://www.ca.kit.edu/61.php

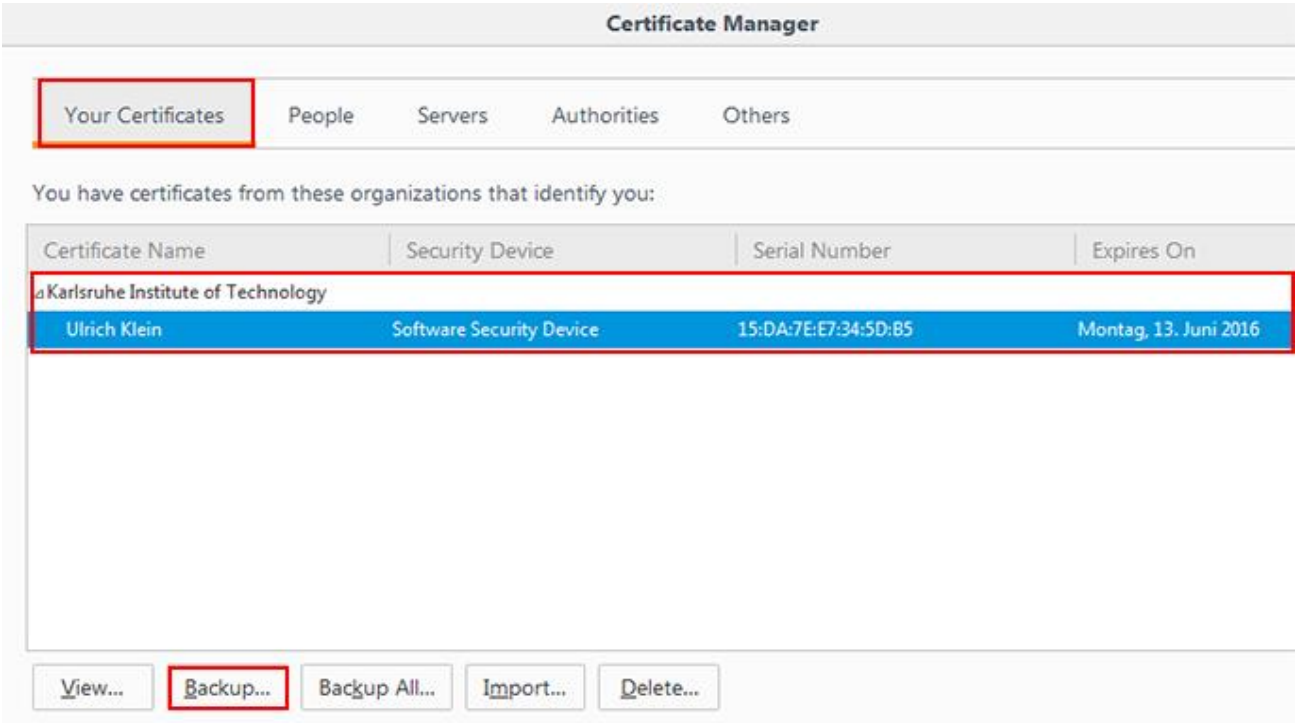
Open Firefox and navigate to the following menu: **Firefox→ menu → settings**.



Select **Advanced→ certificates** and click **View Certificates**.



The Certificate Manager opens: Select your certificate to be backed up from **Your Certificates** and click **Save**.



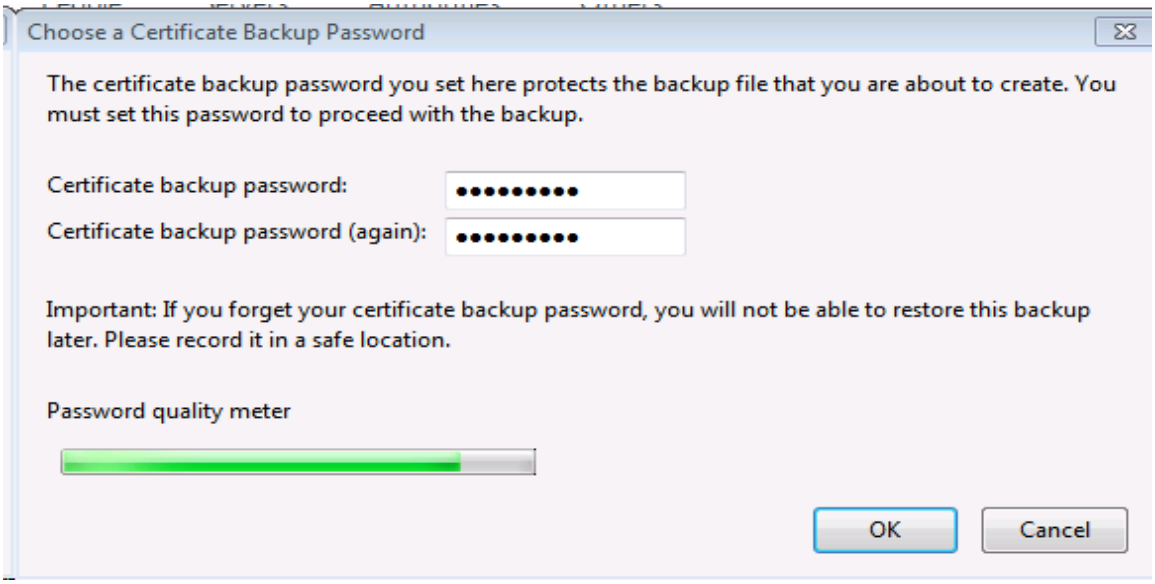
Select name and location for backup

Choose a suitable name for your certificate backup. We recommend the following scheme: YYYYY-MM-DD_Name. p12.

Select a suitable location for your backup. You should be able to find your backup in several years' time. In case of doubt, speak to your IT representative or administrator.

Set password for backup

Enter a password to encrypt the backup. Select the backup password so that you can remember it after several years. You will need the backup and password if you want to install the certificate on a new PC later on. You will not be able to read encrypted messages you received before on a new PC without the old certificate. **Never delete certificate backups! You'll need it in the future.**



A message about the successful backup of the certificate appears.

Importing a certificate into the e-mail client

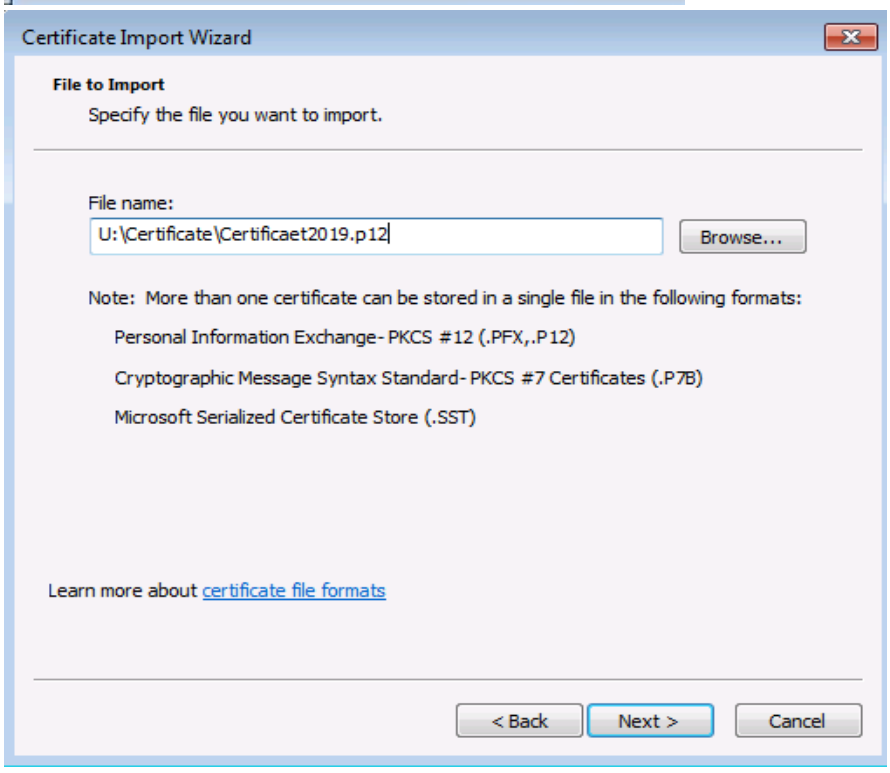
To import a backup, it is necessary that the certificate has already been applied for, retrieved and a backup has been created. If you have not already done so, please do so.

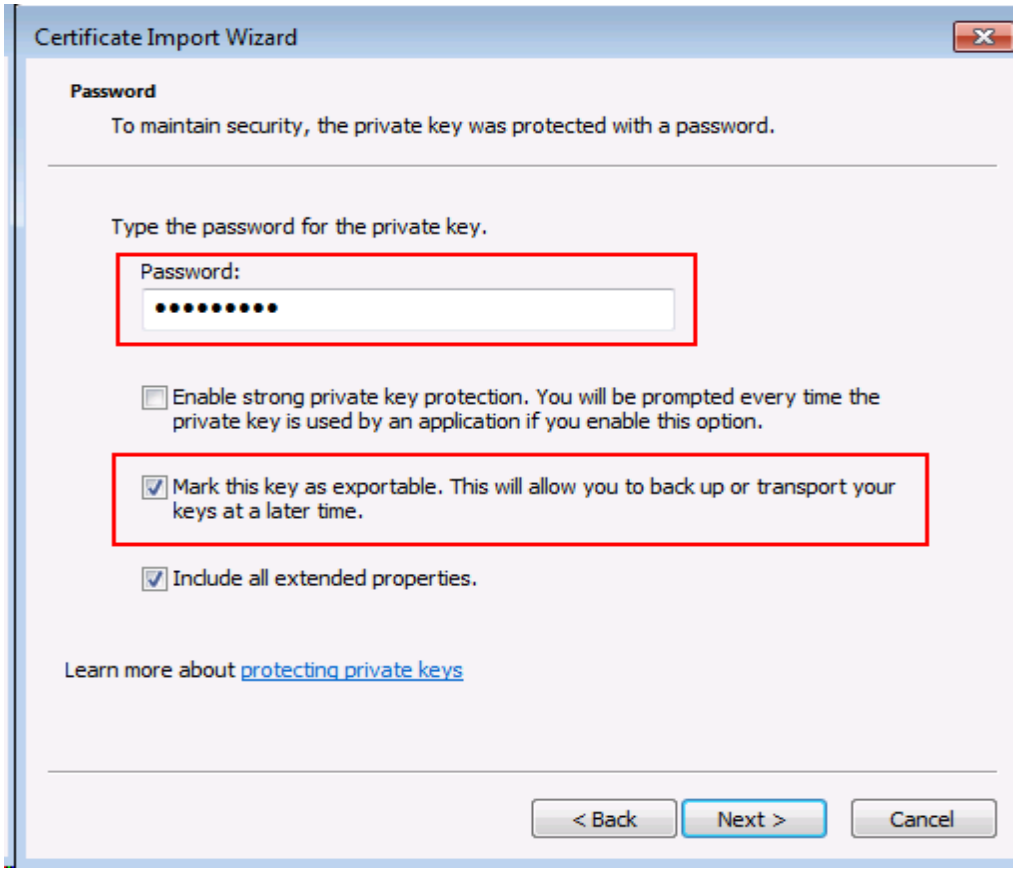
Importing a certificate into the e-mail client - Windows/Outlook

This guide describes how to add a certificate to the Windows certificate store. Importing the certificate is necessary if you have applied for the certificate on a different computer or not using Internet Explorer.

Open the backup of your certificate (YYYYY-MM-DD_Name. p12) by double-clicking it.

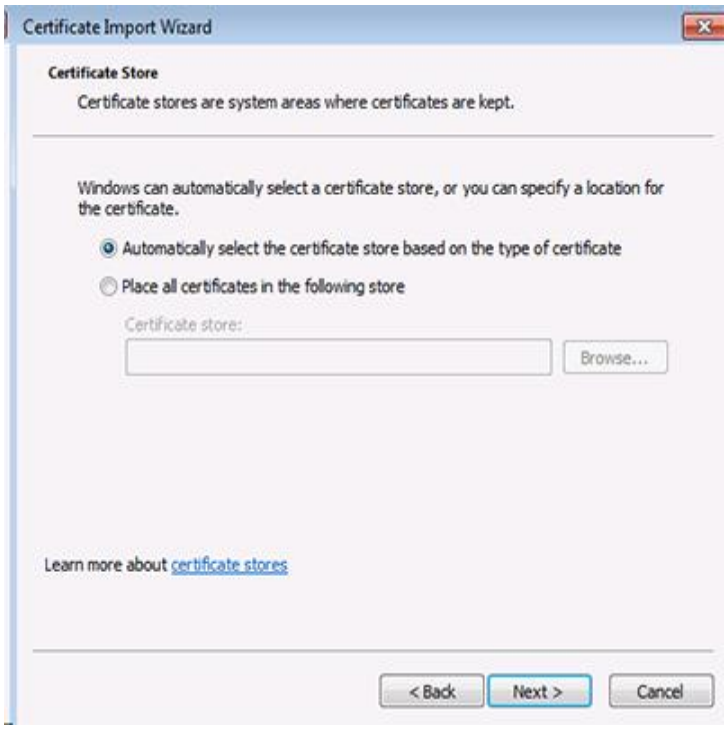
The Windows Certificate Import Wizard opens, in which you select the **Next** button.



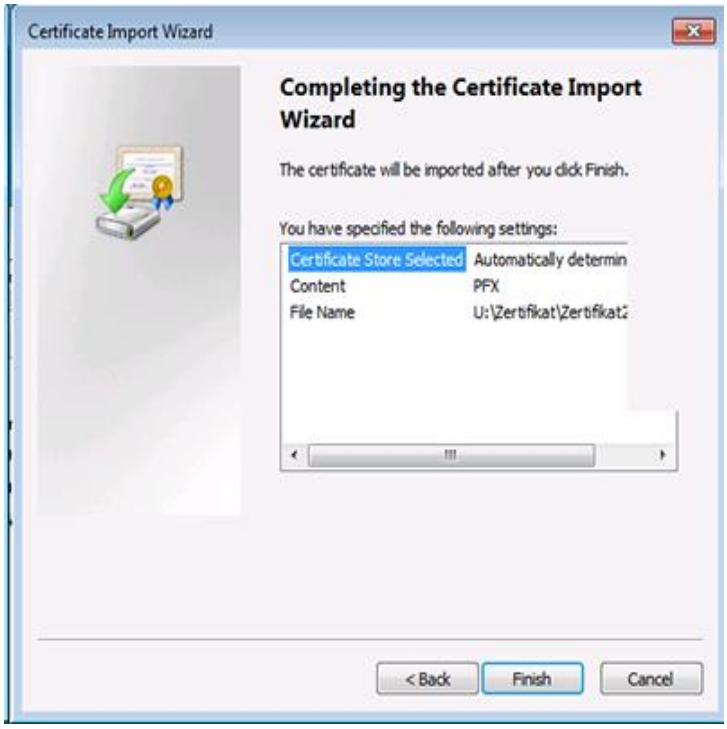


Enter the backup password, tick the option **Mark this key as exportable** and confirm your entry with **Next**

In the next view, select **Automatically select the certificate store** and then click **Next**.



The successful import is now confirmed.

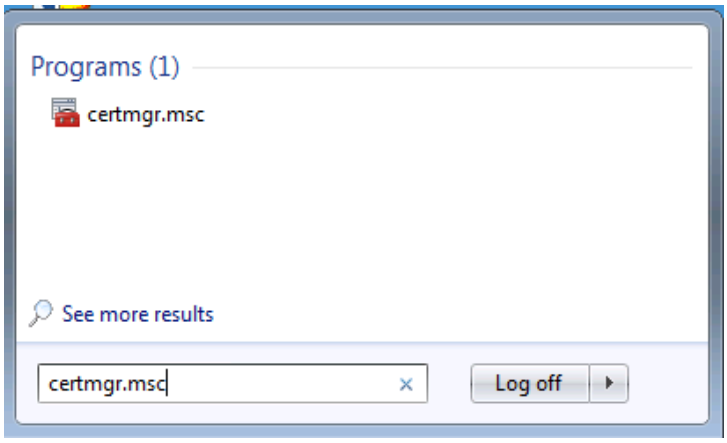


Click **Finish**.

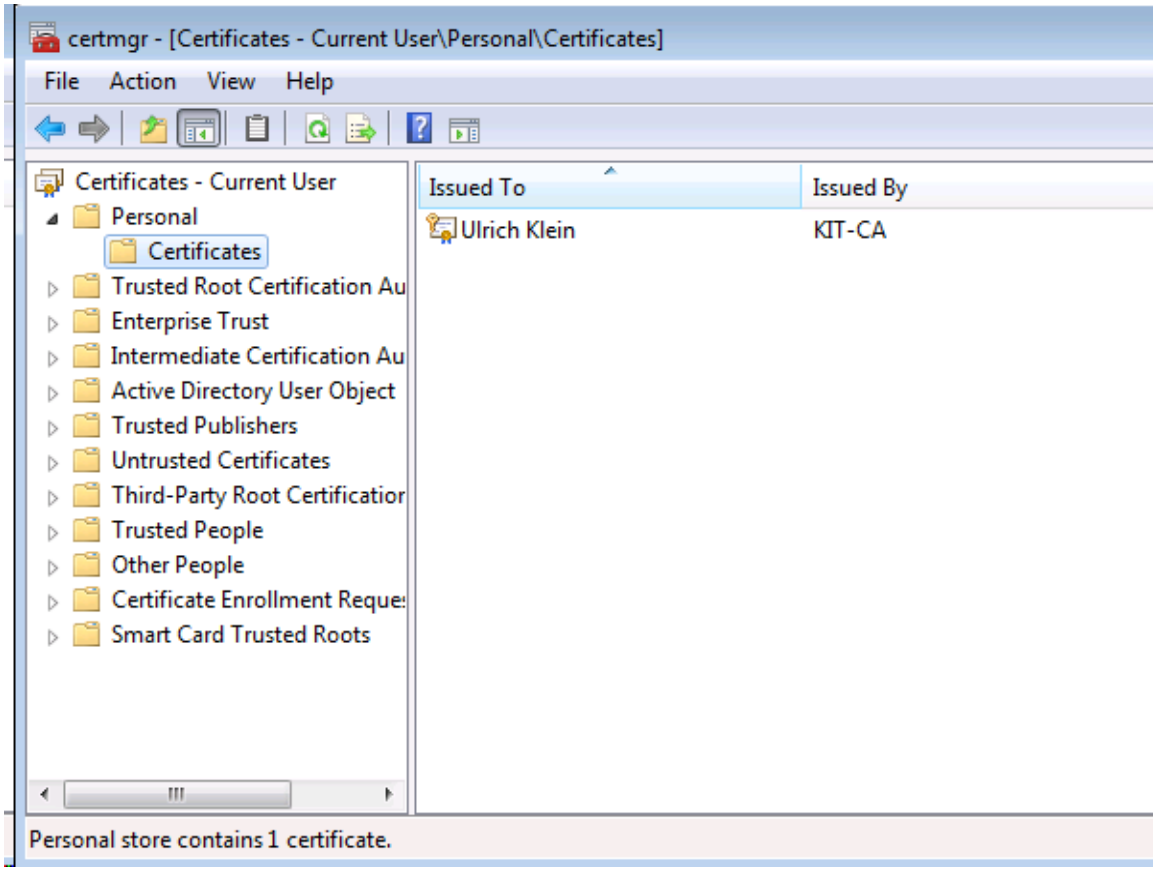
To check the successful import, go to the Windows certificate manager.

Opening the Certificate Manager

Open the certificate manager by running the **certmgr.msc** program. The program can be found using the search function from the Windows Start menu. Enter **certmgr.msc** as search term.



At **Personal → Certificates** you should find your certificate listed in the column on the right side.



Now that you have added the certificate to the Windows certificate store, you can configure Outlook.

Configuration of Outlook 2010

If you have applied for the certificate on a different computer but with Internet Explorer and have not yet created the backup of the certificate, please return to the following step:
Create certificate backup - Windows / Internet Explorer

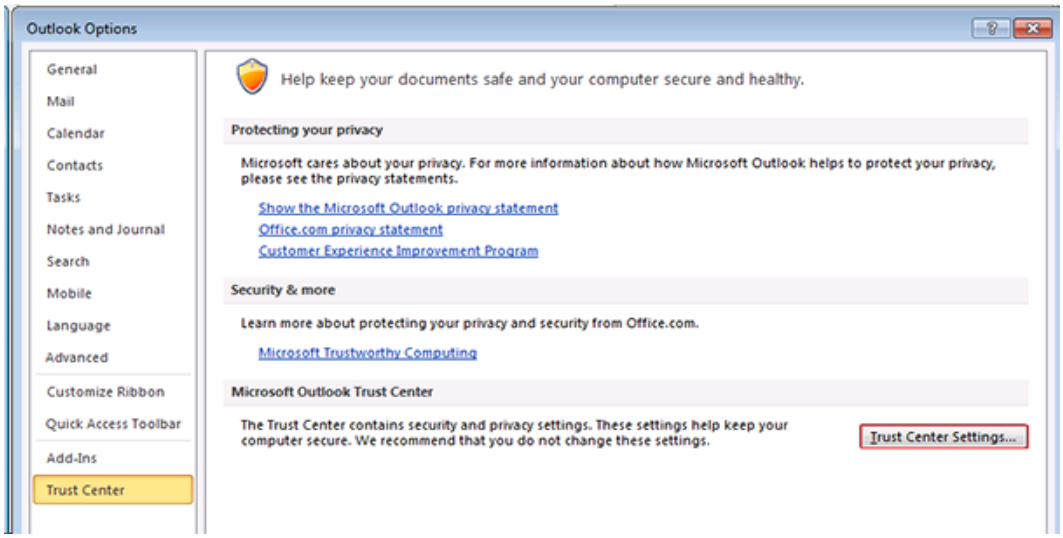
If you have applied for the certificate with Firefox (regardless on which computer) but have not yet created a backup, please go to the following page and go through the steps there:
Create certificate backup - Mozilla Firefox

If you have already created the backup of the certificate (but on a different computer or with Firefox) and you have not yet familiarized yourself with the Windows certificate store, please return to the following step:
Importing a certificate into the e-mail client - Windows / OutlooK (Import backup to the Windows certificate store)

Step 1: Set up Outlook

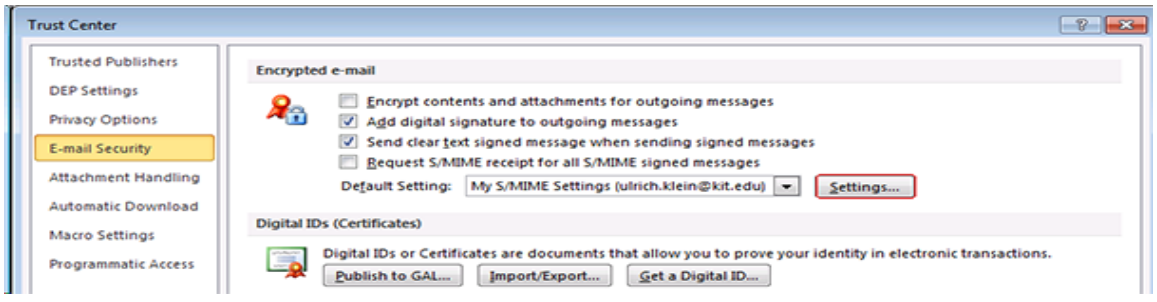
To use the imported certificates, it is necessary to configure the mail program accordingly before emails can be signed or encrypted.

Open your Outlook program. Then at **File → Options** select the **Trust Center** tab. There, select the button for *Trust Center Settings* in the lower right corner, then select the **E-mail Security** tab.



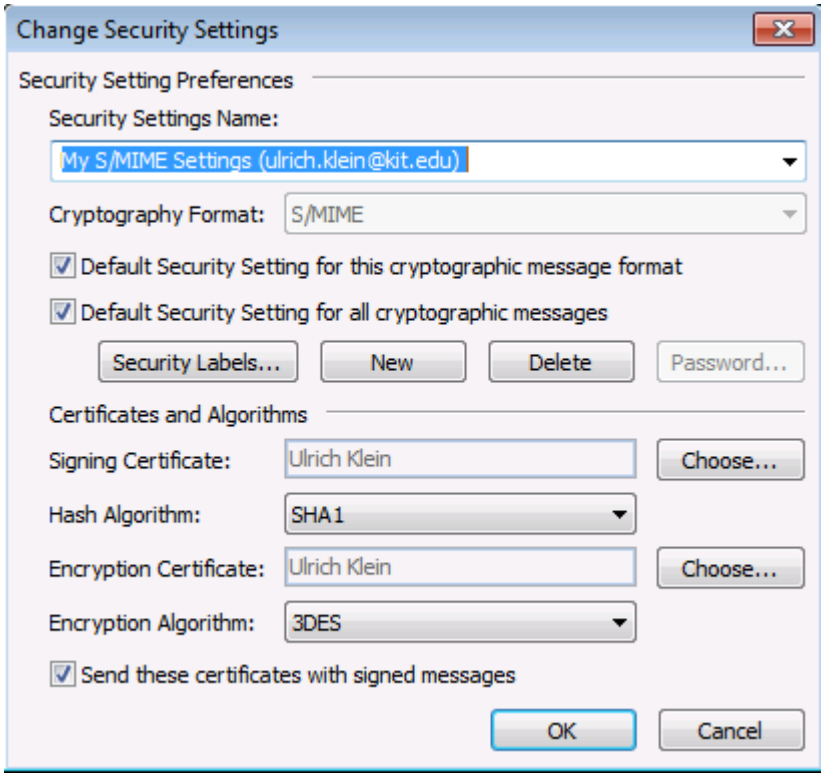
Then set the following checkboxes in the **Encrypted e-mail** section, and press the **Settings** button

- ***Add digital signature to outgoing messages***
- ***Send clear text signed messages when sending signed messages***



Accept the following settings and confirm the dialog with **OK**:

- *Enter a suitable name for the security setting.*
- *Cryptography Format:* ***S/MIME***
- *Check the box:* ***Default Security Setting for this cryptographic message format*** *and*
- ***Default Security Setting for all cryptographic messages***
- *Siging certificate: Press the* ***Choose*** *button, confirm your selection with* ***OK***
- *Hash algorithm:* ***SHA1***
- *Encryption certificate: Press the* ***Choose*** *button, select the correct certificate and confirm your selection with* ***OK***
- *Encryption algorithm:* ***3DES***
- *Check mark next to:* ***Send these certificates with signed messages***



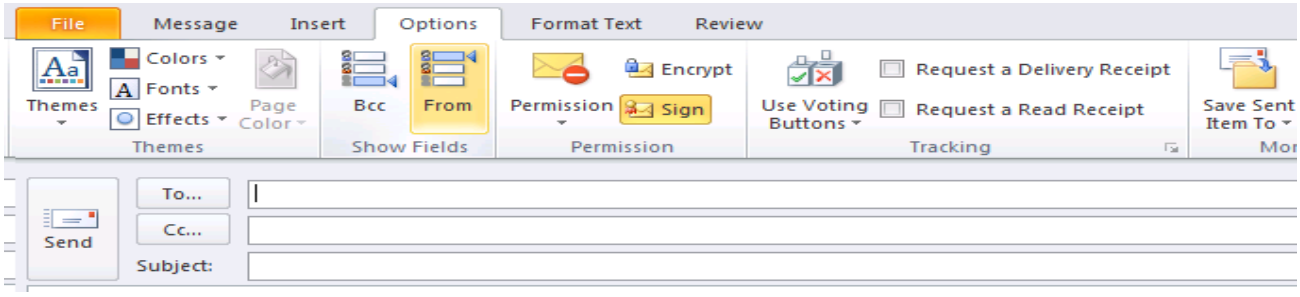
For compatibility reasons, encryption with AES256 is not recommended.

Step 2: Encrypting and signing

Signing E-Mail

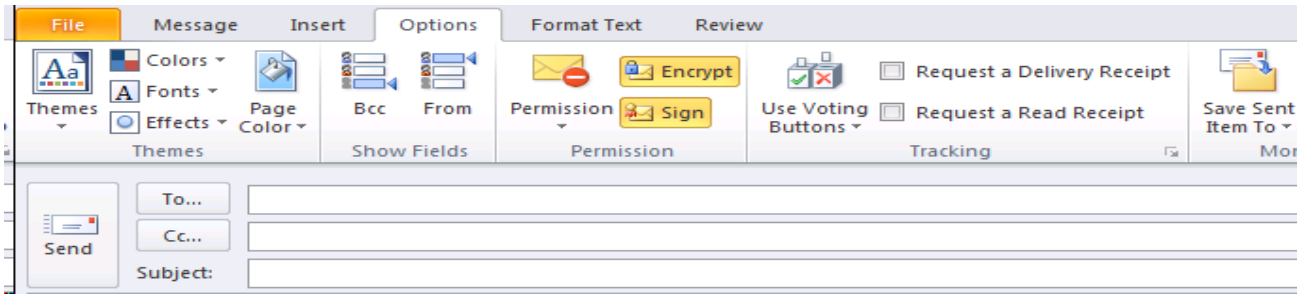
If you have ticked the checkbox **Add digital signature to outgoing messages** in the previous step (recommended), your e-mails will be automatically signed.

In the ribbon **Options**, you can sign your e-mail manually by clicking on **Sign** (button will be highlighted).



By pressing the Sign button again (button is no longer highlighted) the e-mail will be sent unsigned.

Encrypting e-mail



Hint:

In order for others to be able to send you an encrypted e-mail, they need your certificate. You can transmit this information by sending a signed e-mail. If you use Outlook on your KIT workstation, the public certificates are updated once a day in the global address list (Exchange GAL).

Only encrypt confidential content and only if you are sure that the recipient can read encrypted emails. Generally encrypting all e-mails does not make sense and in case of doubt only leads to problems on the recipient side, because encrypted e-mails can only be read on devices with a certificate installed! Encrypted messages you received can only be read in the future if the certificate you used at the time you received the message is still installed.

In the ribbon **Options**, you can encrypt your e-mail by clicking on **Encrypt** (button will be highlighted).

By pressing the **Encrypt** button again (button is no longer highlighted) the e-mail is sent unencrypted.