

# **certBox**

## **User-Guide**

Secardeo GmbH  
Release: 16.05.2023

## Table of Contents

1	Search and retrieve Public Key Certificates .....	1
1.1	Search by an e-mail address .....	1
1.2	Download of a certificate, vCard, certificate chain or PGP key .....	1
2	Upload or remove your Public Key Certificate .....	4
3	Outlook .....	5
3.1	Encrypt an e-mail .....	5
3.2	LDAP configuration for automated certificate search .....	7
3.3	Import certificate in the Outlook Contacts .....	8
3.3.1	Add certificate to an existing contact .....	8
3.3.2	Create a new contact with the help of a vCard .....	9
3.3.3	Create new contacts with the address book search .....	10
3.4	Import certificate into the Windows certificate store .....	10
3.5	Import certificate chain into the Windows certificate store .....	13
4	Mozilla Thunderbird .....	15
4.1	Encrypt an e-mail .....	15
4.2	LDAP configuration for automated certificate search .....	16
4.3	Import a certificate .....	18
4.4	Import a certificate chain .....	19
5	Outlook for iOS and Android .....	21
6	Apple Mail .....	23
6.1	Encrypt an e-mail .....	23
6.2	LDAP configuration for automated certificate search .....	24
6.3	Import a certificate manually from the HTML-Search .....	24

## 1 Search and retrieve Public Key Certificates

End-to-end encryption requires the sender of a message to possess the public key of the recipient. The Secardeo certBox provides clients with X.509 certificates or PGP keys. The certificates can be retrieved through a manual search on the web page or automatically through configuration in a client application.

### 1.1 Search by an e-mail address

In order to search for X.509 certificates or PGP keys, please enter the letters displayed on the left into the box on the right. If you are an internal user the captcha code will not appear. Afterwards enter the desired e-mail address and click the “search” button. The certBox will automatically search for X.509 certificates. If you want to search for PGP-keys, please select “PGP” from the drop down menu.




The screenshot shows the certBox web interface. At the top is a dark blue header with the certBox logo and four navigation links: "Find Certificate", "Upload Certificate", "Remove Certificate", and "DE Help". Below the header is a search form. On the left, there is a captcha image showing the letters "deu?". To the right of the captcha is a text input box with the instruction "Enter the letters shown on the left into the box below:". Below the captcha is a dropdown menu currently set to "X.509". To the right of the dropdown is a larger text input box for an email address. A "search" button is located to the right of the email input box. At the bottom of the form, there is a message: "Please enter a valid e-mail address."

The search interface may be protected by login data. If you do not know the login data, please contact the certBox administrator.




To perform a search, you might have to enter the login data into the corresponding fields.

### 1.2 Download of a certificate, vCard, certificate chain or PGP key

The search result is displayed in a table beneath the search form. In the section “Download” you can download the certificate in your desired format.


[Find Certificate](#)
[Upload Certificate](#)
[Remove Certificate](#)
[DE Help](#)

X.509

Name	Issuer	Valid until	Key usage	Download
Faridul Alam	SwissSign Personal Gold CA 2014 - G22	16.12.2022	Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement TLS Web Client Authentication E-mail Protection Microsoft Encrypted File System Microsoft Smartcardlogin	 vCard  Certificate (binary)  Certificate (ASCII)

Click on the desired link, select "Save" and save it to a folder on your computer.

## Explanation of the search result:

Name: This is the common name from the certificate.

Issuer: This is the common name of the issuing CA

Valid until: The certificate is valid until this date.

Validation: This column is optional and will only be displayed if the validation feature of the certBox is active. The sign "validated by certBox" means that the found certificate is validated and approved to be used. If a question mark appears the certificate is not classified as trustworthy by the certBox, but the revocation status has not been verified.

Key usage: The certificate can only be used for these purposes.

## Download:

vCard A vCard includes the digital certificate and also information about the contact, such as e-mail, name, phone etc. The vCard can be opened, for example, directly from Outlook and saved as a contact.

Certificate (ASCII) The digital certificate of the person that is listed in the "Name" field. It is encoded in PEM format, which is a sub-set of ASCII.

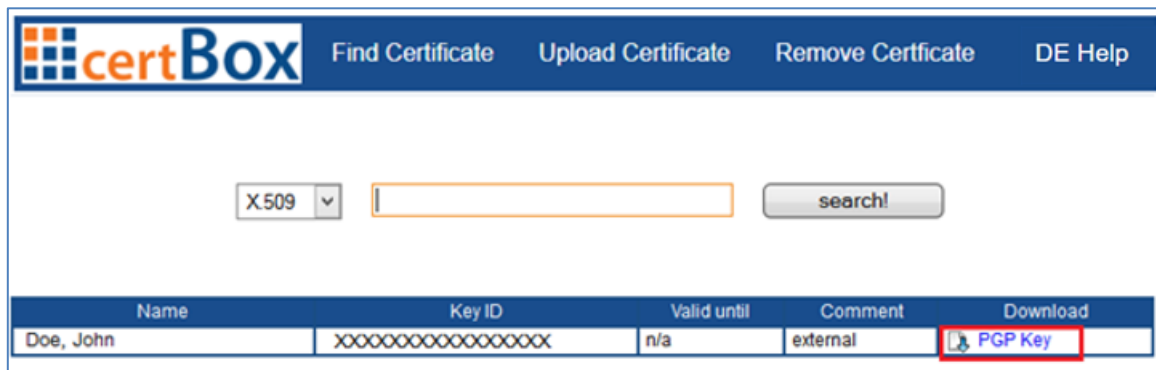
Certificate (binary) The certificate in binary format (DER).

Certificate chain (if available) A certificate chain is a PKCS#7 container which contains the complete associated certificate chain. That is, the root certificate, any intermediate CA and the user certificate. The chain is required by some programs to trust the user certificate because otherwise, it will not encrypt with this certificate. Unfortunately we


can't offer a complete chain for all certificates.

---

If you want to search for a PGP key just click on the link "PGP Key" in the download section. Select "Save" to save it to a folder on your computer.



The screenshot shows the certBox web interface. At the top is a dark blue header with the certBox logo and navigation links: "Find Certificate", "Upload Certificate", "Remove Certificate", and "DE Help". Below the header is a search area with a dropdown menu set to "X.509", an empty text input field, and a "search!" button. Below the search area is a table with the following columns: "Name", "Key ID", "Valid until", "Comment", and "Download". The table contains one row for "Doe, John" with a Key ID of "XXXXXXXXXXXXXXXXXXXX", a "Valid until" value of "n/a", and a "Comment" of "external". In the "Download" column for this row, there is a link labeled "PGP Key" with a small icon, which is highlighted by a red rectangle.

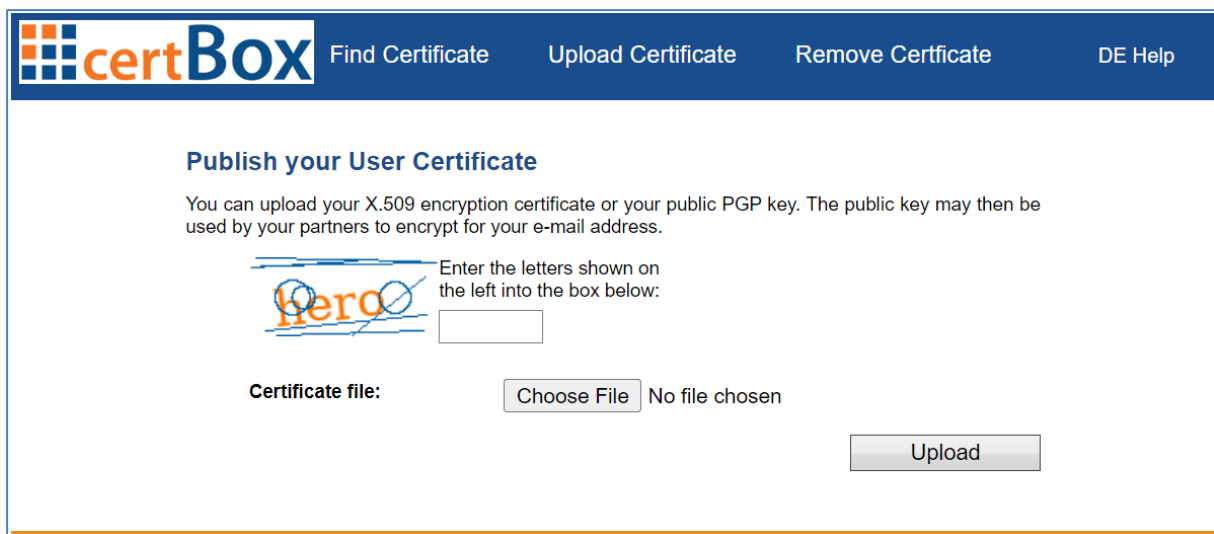
Name	Key ID	Valid until	Comment	Download
Doe, John	XXXXXXXXXXXXXXXXXXXX	n/a	external	 <a href="#">PGP Key</a>

## 2 Upload or remove your Public Key Certificate

By clicking on “Upload certificate” you can publish your Public Key Certificate for the internal users of the certBox. Your certificate can then be found by them and they can send you encrypted e-mails. If the Button is not available this feature is currently not activated on the certBox.

A login dialog may appear. If so, enter “partner” for user and the password you have been told by the certBox administrator.


The “Upload Certificate” dialog appears. You have to browse for the local certificate file and press the “Upload” button. The certificate will then be published. Depending on the configured policy the upload may have to be approved by the certBox administrator.



**certBox** Find Certificate Upload Certificate Remove Certificate DE Help

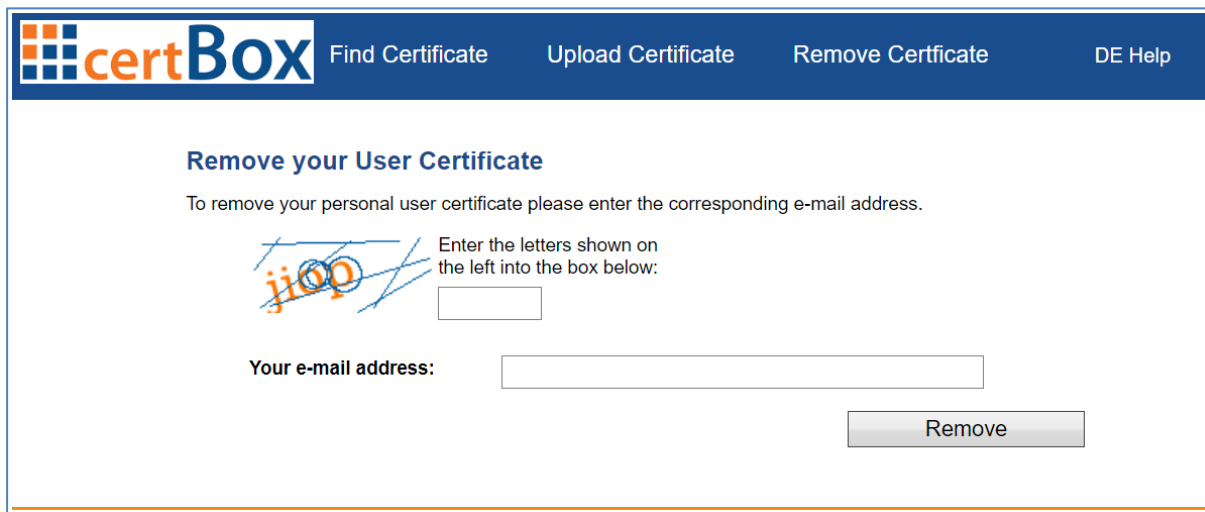
### Publish your User Certificate

You can upload your X.509 encryption certificate or your public PGP key. The public key may then be used by your partners to encrypt for your e-mail address.

 Enter the letters shown on the left into the box below:

Certificate file:  No file chosen

If you want to remove a certificate you have previously uploaded click on the link "Remove Certificate".



The screenshot shows the 'Remove your User Certificate' page on the certBox website. The page has a blue header with the certBox logo and navigation links: 'Find Certificate', 'Upload Certificate', 'Remove Certificate', and 'DE Help'. The main content area is white and contains the title 'Remove your User Certificate' in blue. Below the title, it says 'To remove your personal user certificate please enter the corresponding e-mail address.' There is a CAPTCHA image showing the letters 'ijoo' with a blue scribble over it. To the right of the CAPTCHA, it says 'Enter the letters shown on the left into the box below:' followed by a small text input box. Below the CAPTCHA, it says 'Your e-mail address:' followed by a larger text input box. At the bottom right, there is a 'Remove' button.

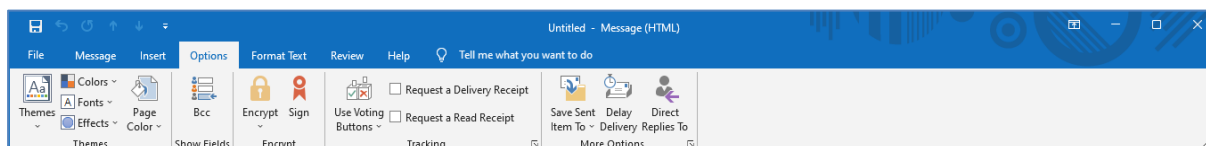
Enter the e-mail address for the certificate to be removed. The request may have to be approved by the certBox administrator. An e-mail with a confirmation link will be sent to the certificate owner. The certificate owner can confirm the certificate removal just by clicking on the link. If the request is not made by the certificate owner, then simply ignore the email.

## 3 Outlook

To encrypt an e-mail, it is mandatory to install your own certificate into the certificate store of the application. This will be a prerequisite for the following steps.

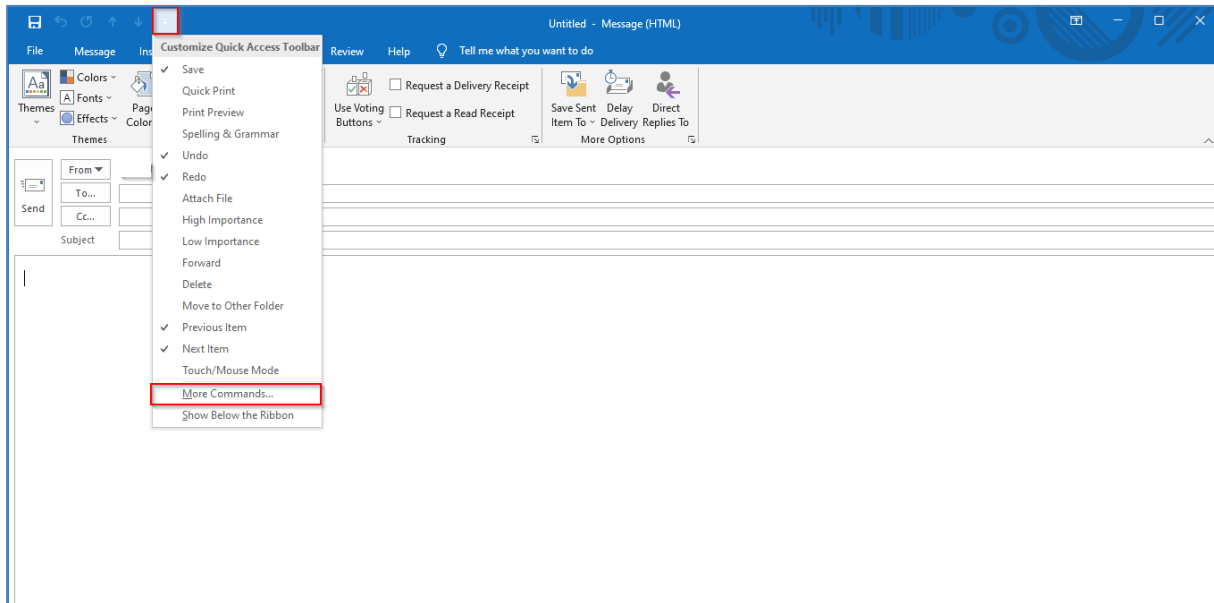
### 3.1 Encrypt an e-mail

You can encrypt or sign e-mails in Outlook by enabling the respective buttons that can be found under the tab "Options" and "Permission". Alternatively, it is also possible to add the buttons to the Quick Access Toolbar.

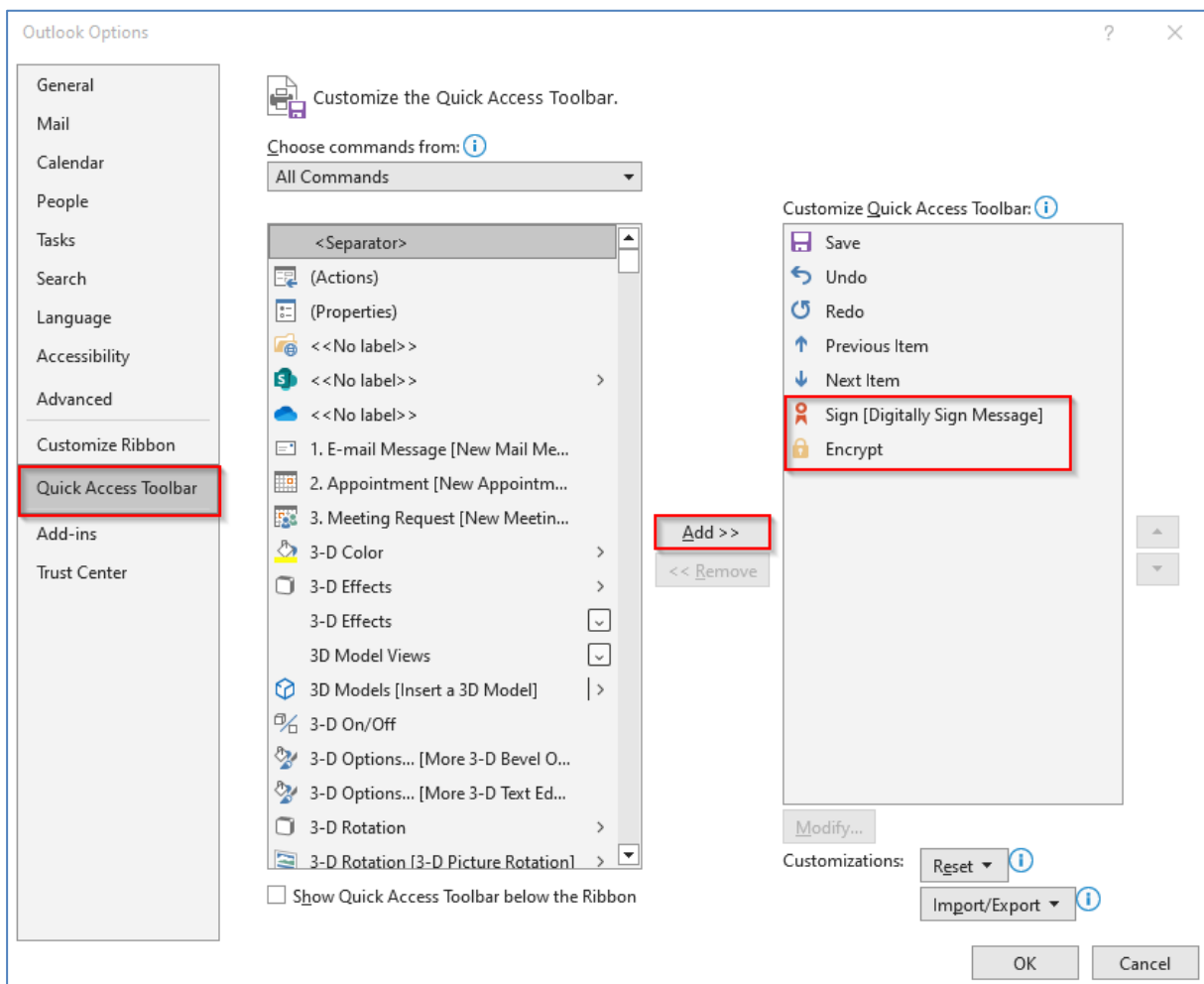


#### Customize the Quick Access Toolbar

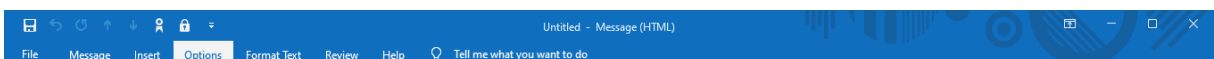
Create a new e-mail. Click on the little arrow in the top ("Customize Quick Access Toolbar") and then click on "More Commands..."



On the left side select “All Commands” and add “Digitally Sign Message” and “Encrypt”. Then click “OK”



Now there should be two new symbols on your Quick Access Toolbar.



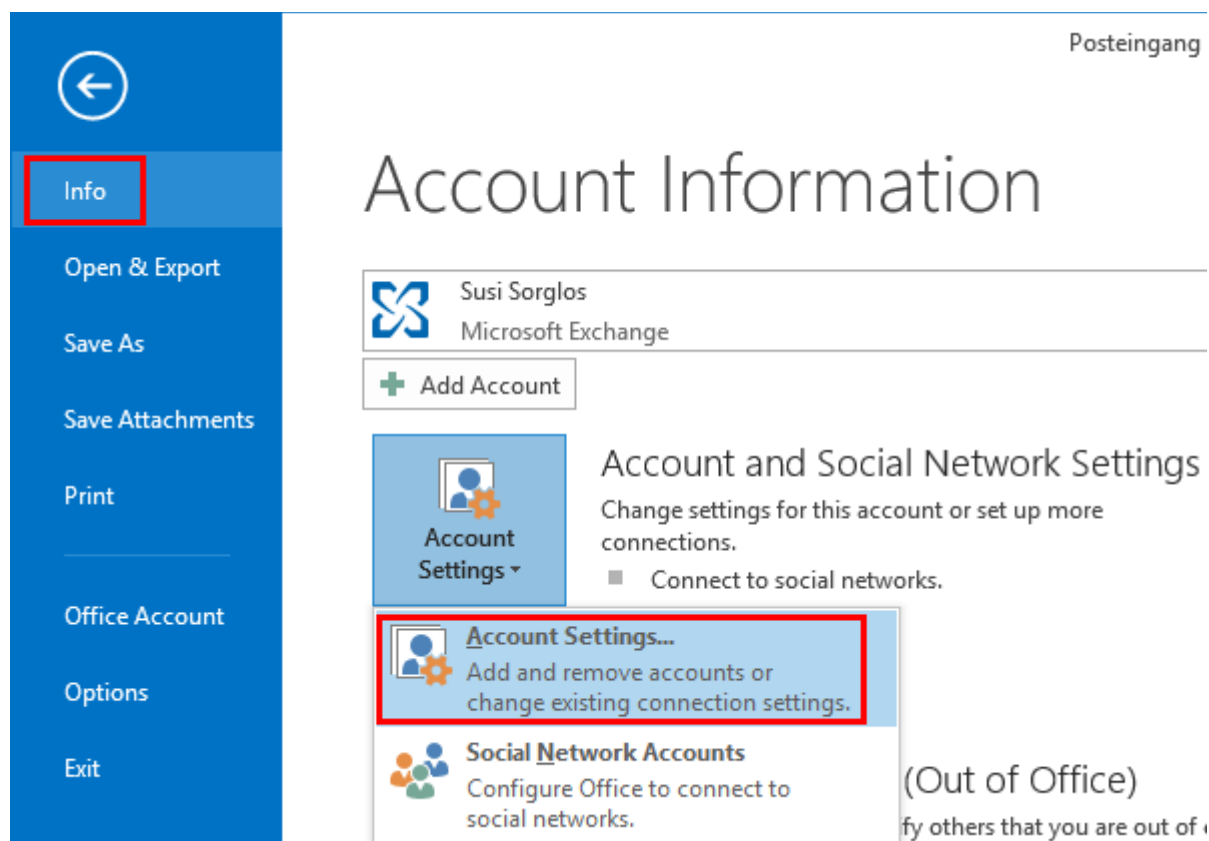


Whenever you write an e-mail in the future you can sign and encrypt it with these symbols.

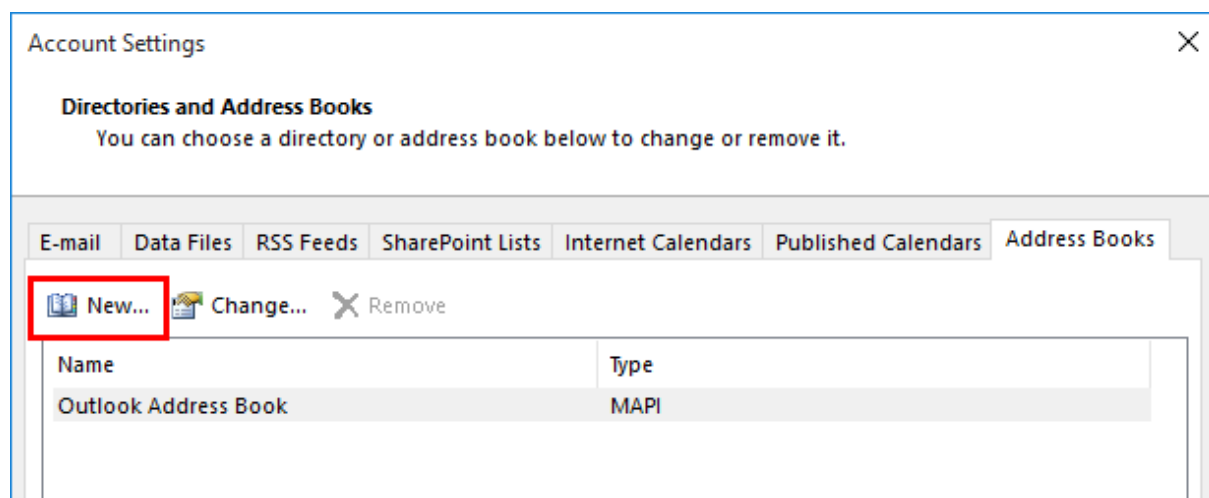
## 3.2 LDAP configuration for automated certificate search

If you encrypt frequently, you should consider setting up a directory server (LDAP) which will automatically download the recipients' certificates.

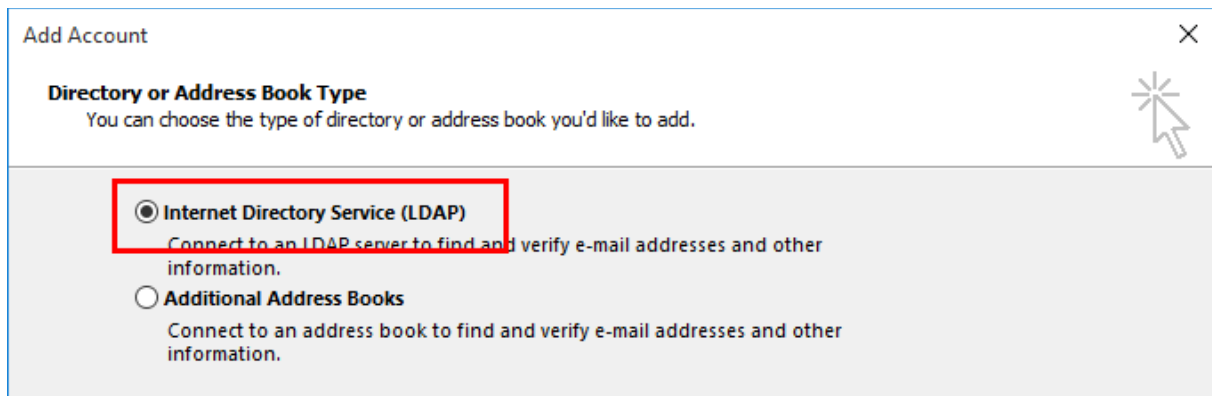
Navigate to your account preferences



Click on "Address Books" and select "New"



There you select "Internet Directory Service (LDAP)" and click "Next"



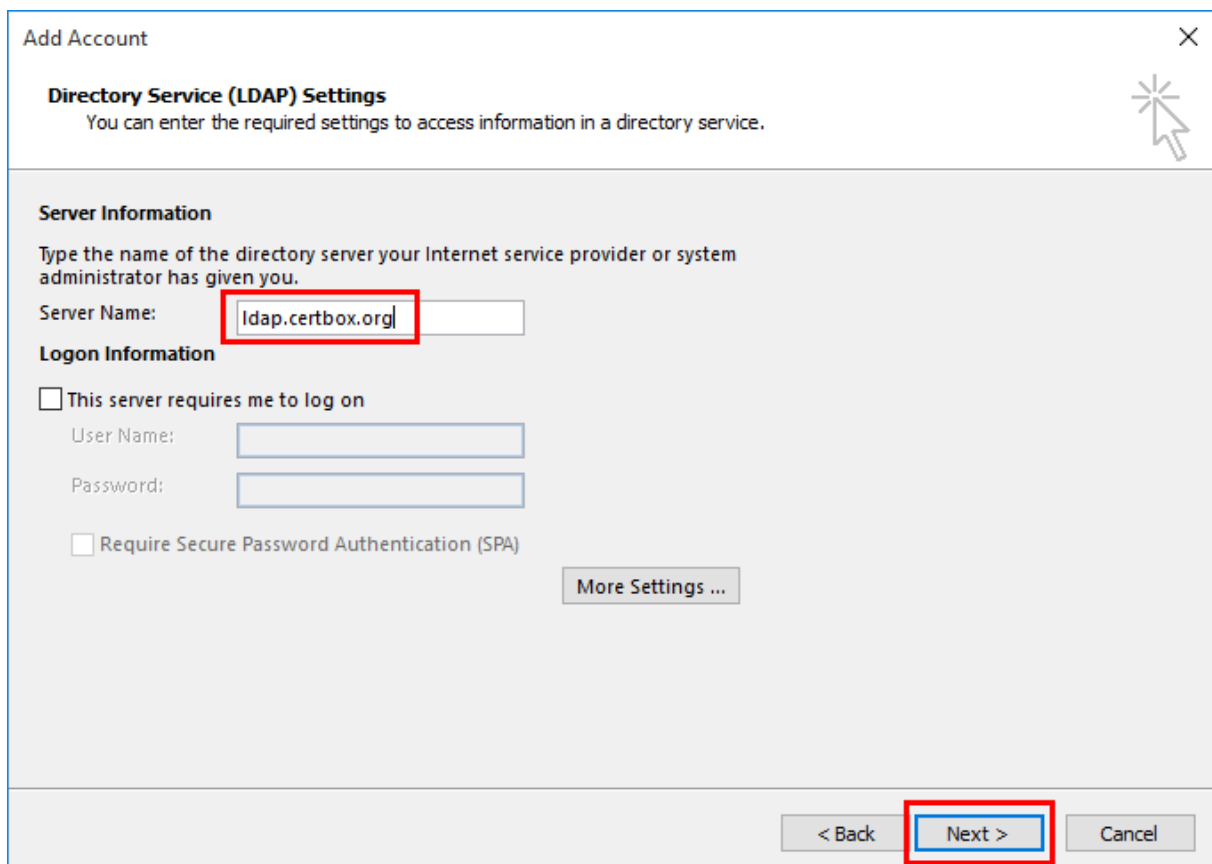
Add Account

**Directory or Address Book Type**  
You can choose the type of directory or address book you'd like to add.

☒ **Internet Directory Service (LDAP)**  
Connect to an LDAP server to find and verify e-mail addresses and other information.

☐ **Additional Address Books**  
Connect to an address book to find and verify e-mail addresses and other information.

Afterwards you enter "ldap.certbox.org" for the server name



Add Account

**Directory Service (LDAP) Settings**  
You can enter the required settings to access information in a directory service.

**Server Information**  
Type the name of the directory server your Internet service provider or system administrator has given you.

Server Name:

**Logon Information**

☐ This server requires me to log on

User Name:

Password:

☐ Require Secure Password Authentication (SPA)

[More Settings ...](#)

< Back **Next >** Cancel

Now click "Next" and then "Finish"

### 3.3 Import certificate in the Outlook Contacts

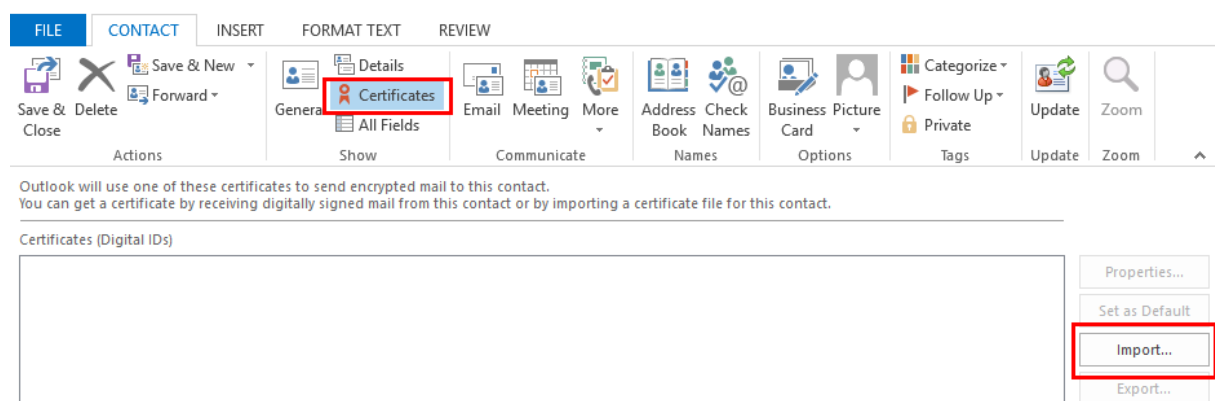
#### 3.3.1 Add certificate to an existing contact

Follow these instructions if you want to encrypt once to an existing contact.

For the import, click on "Contacts" and double click the contact of your choice



Click then on “Contact” and click on “Certificates”. Now import the previously downloaded certificate via the “Import...” button.

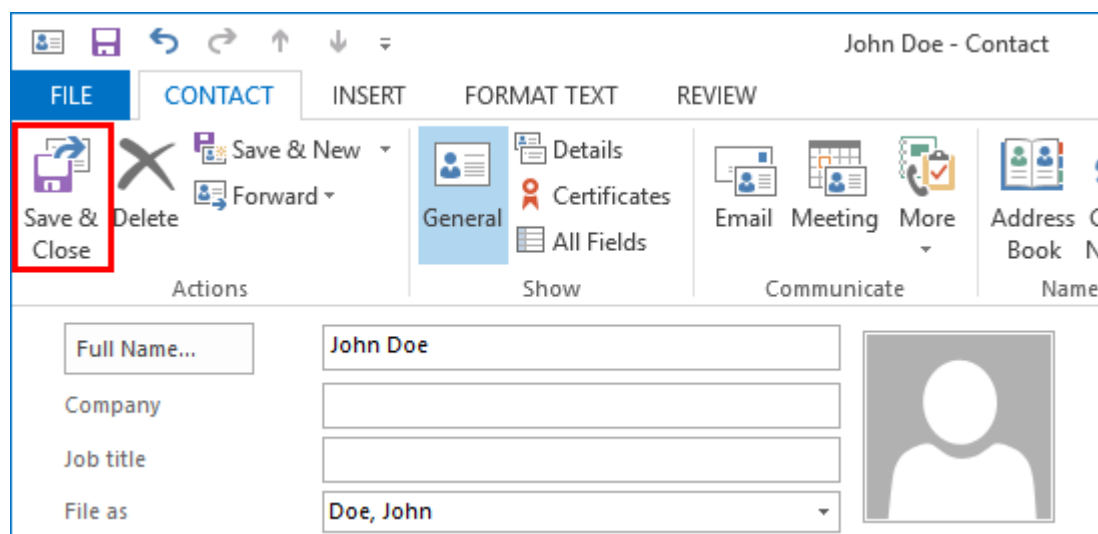


If you don't have the root certificate, you can also use the "Properties" button to explicitly trust the certificate (This is necessary in order to encrypt).

### 3.3.2 Create a new contact with the help of a vCard

Follow these instructions if you want to encrypt to a not yet existing contact.

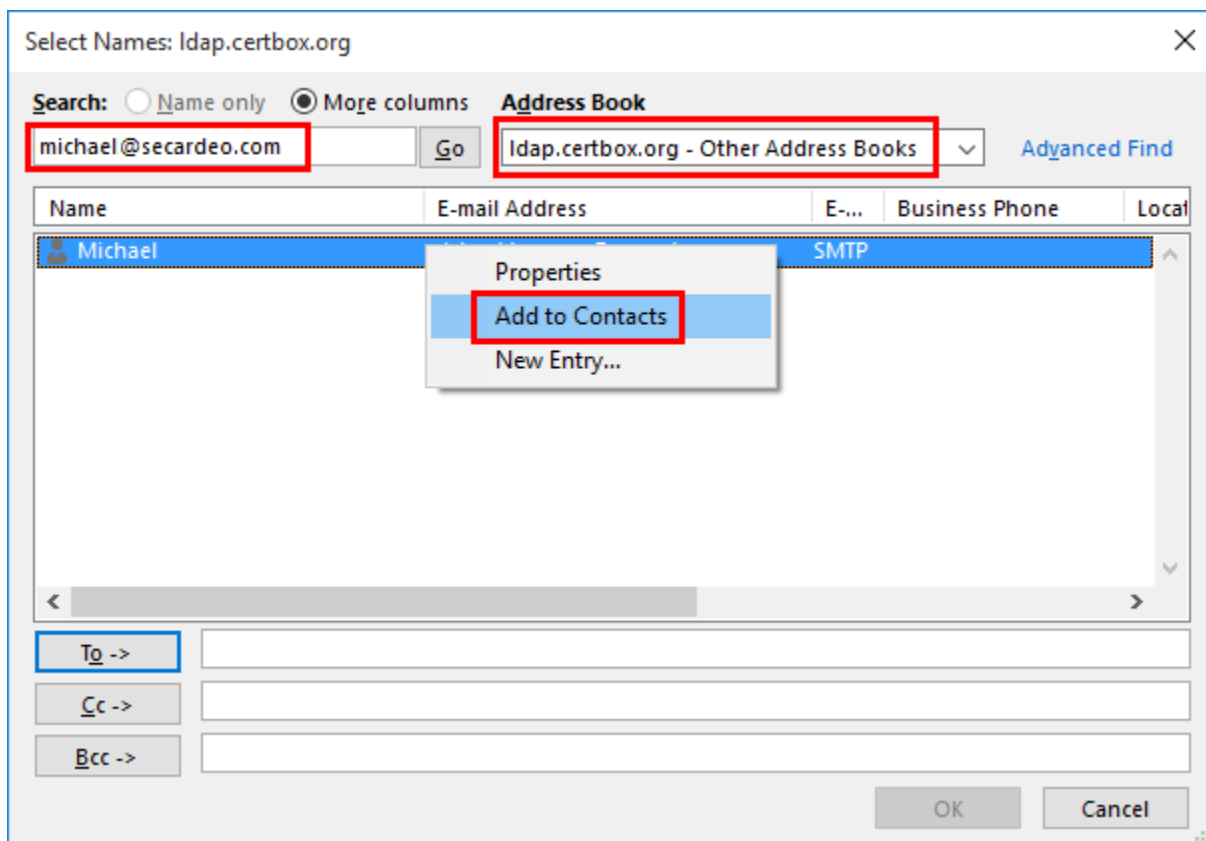
Open the vCard. Now select “Save & Close”



If you don't have a fitting root certificate you can also explicitly trust the certificate as described at the end of chapter 3.3.1.

### 3.3.3 Create new contacts with the address book search

Create a new e-mail and click on “To...”. Then enter the desired e-mail address and choose “ldap.certbox.org” as address book. Then right click on the contact and click “Add to Contacts”.

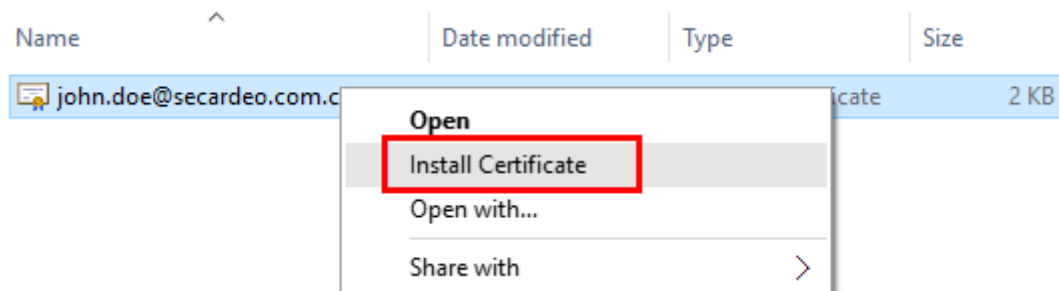


### 3.4 Import certificate into the Windows certificate store

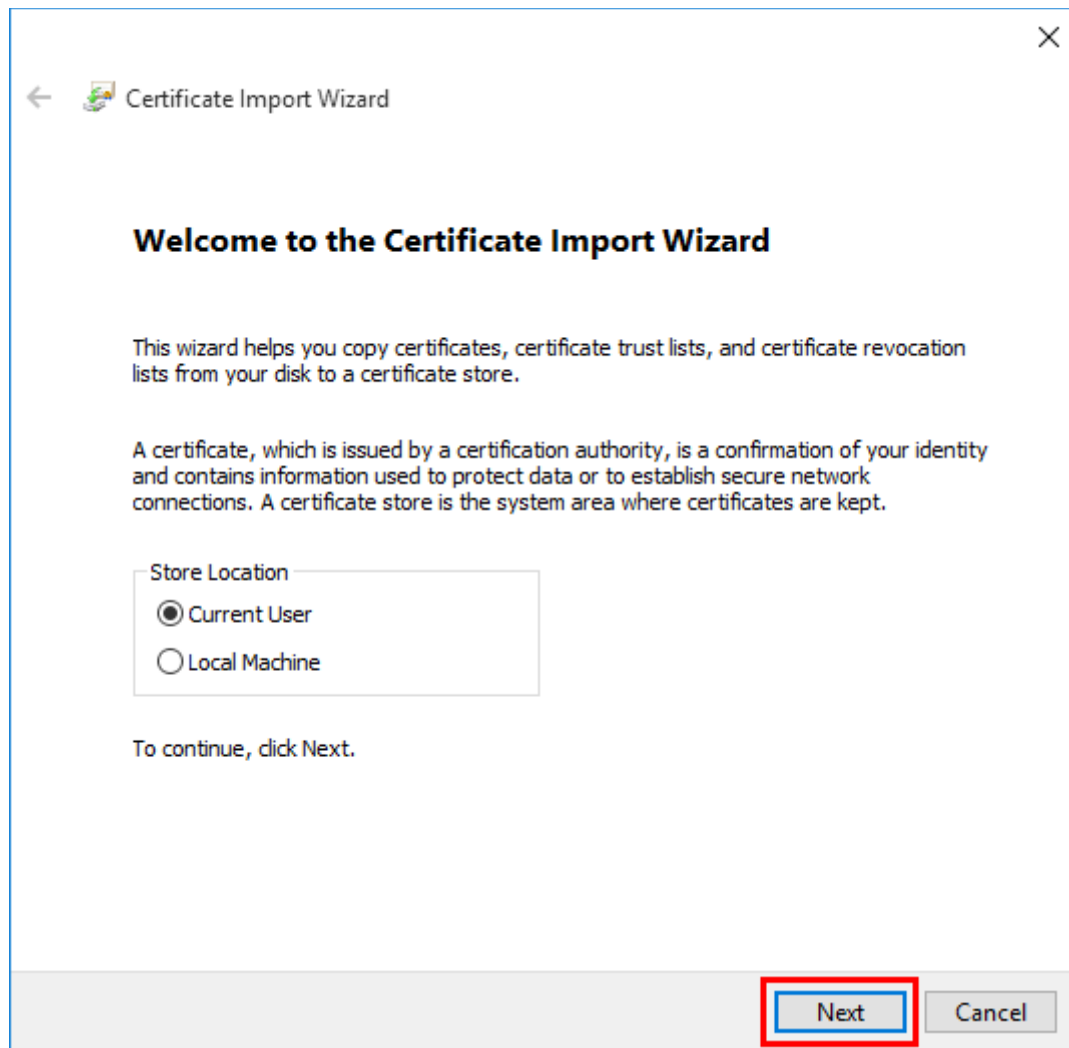
This certificate can later be used to encrypt, if your application can form the certificate chain. If not please follow the instructions in chapter 3.5.

You can check this with opening the downloaded certificate file. Navigate to the tab “Certification path”. If one of the shown certificates is marked with a red “X” the chain cannot be formed. For this case there is a solution at the end of this chapter.

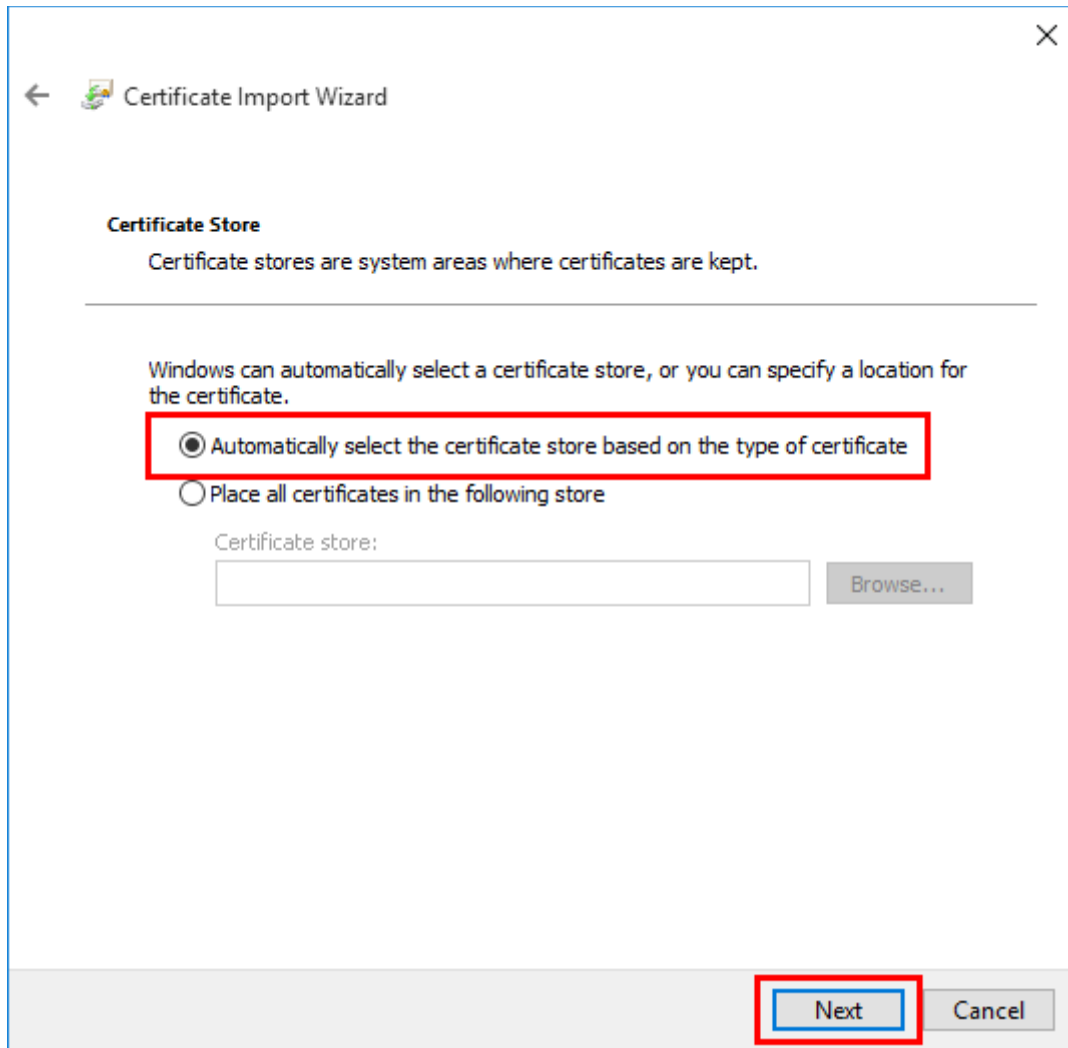
For the import, select the certificate and click on “Install Certificate”



Afterwards click on “Next”

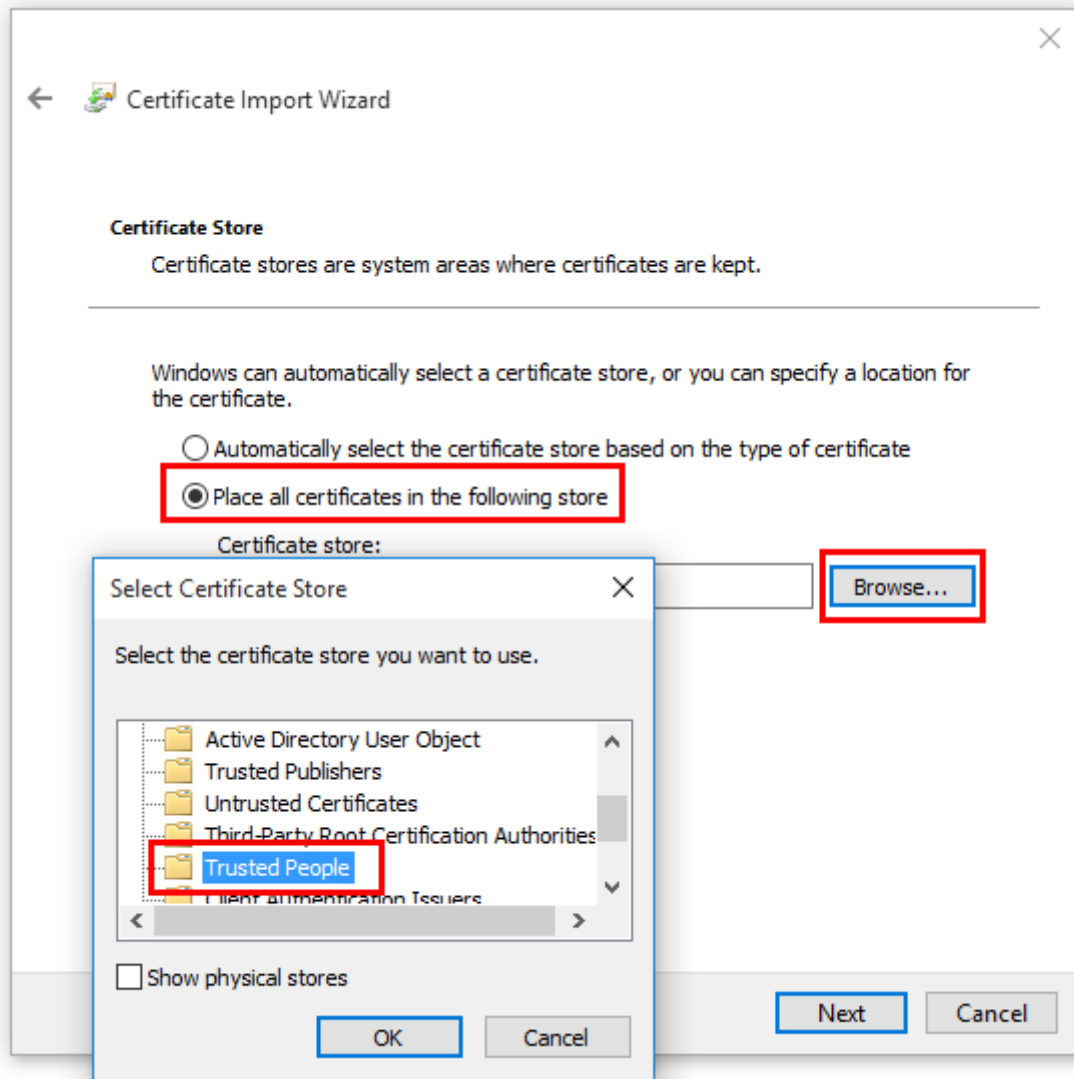


If the certificate chain can be formed select “Automatically select the certificate store” and click on “Next” and “Finish”.



Otherwise select “Place certificates in the following store” and click “Browse”. Then select “Trusted persons” and click “OK”.

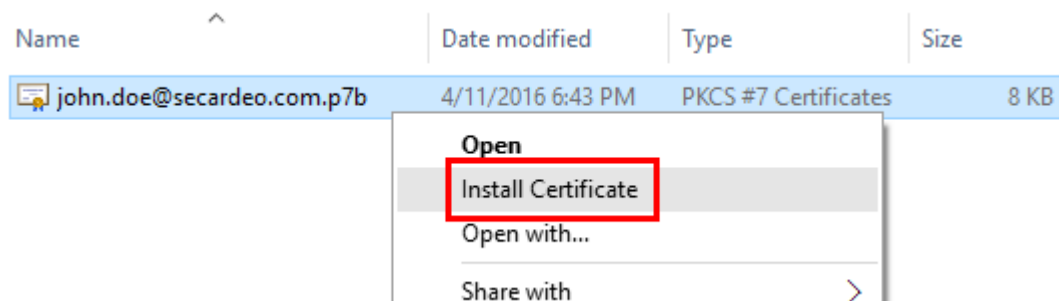
You should only choose this option when you are sure, that the certificate is owned by the recipient and that it is valid.



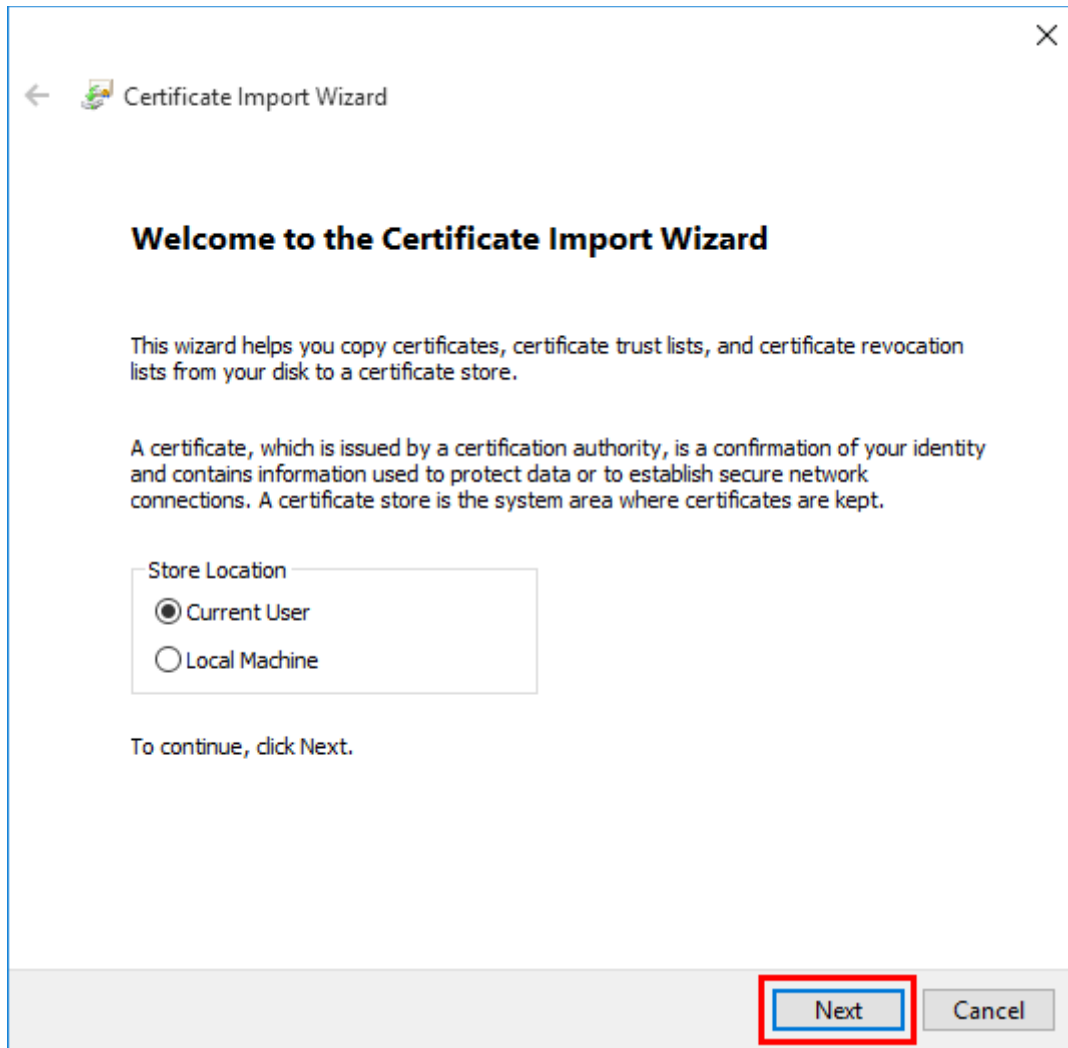
Now click “Next” and then “Finish”.

### 3.5 Import certificate chain into the Windows certificate store

For the import, select the certificate chain and click on “Install Certificate”

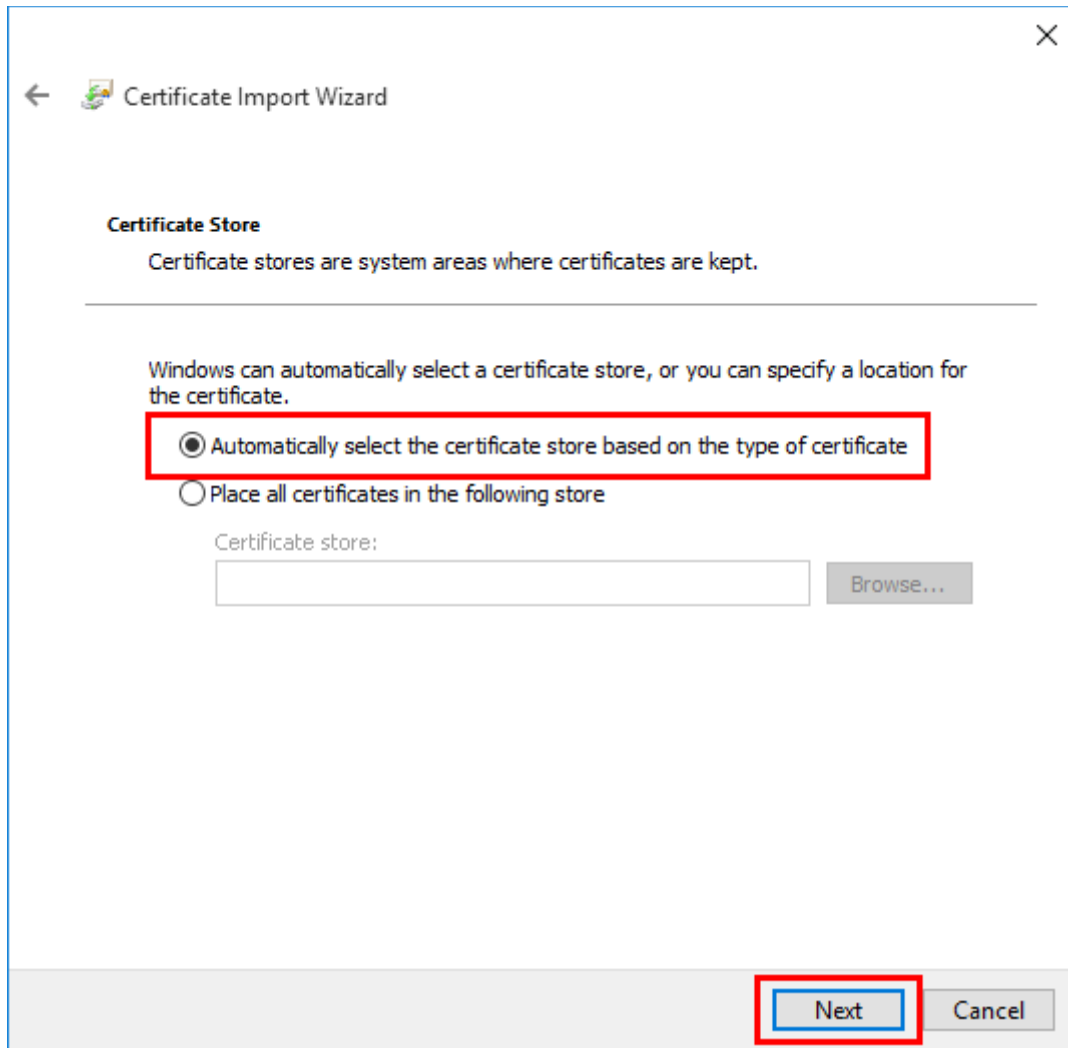


Afterwards click on “Next”



If the certificate chain can be formed select “Automatically select the certificate store” and click on “Next” and “Finish”.





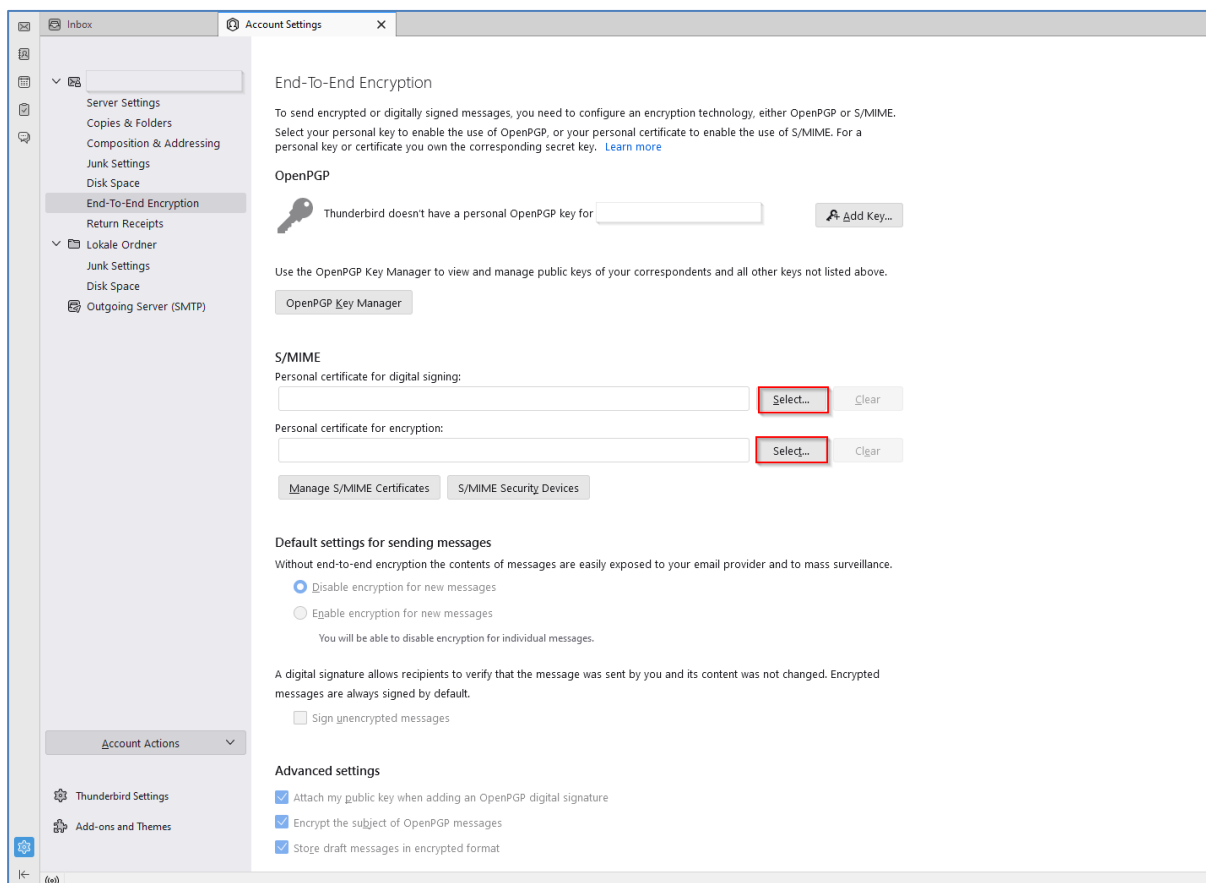
Now click “Next” and then “Finish”.

## 4 Mozilla Thunderbird

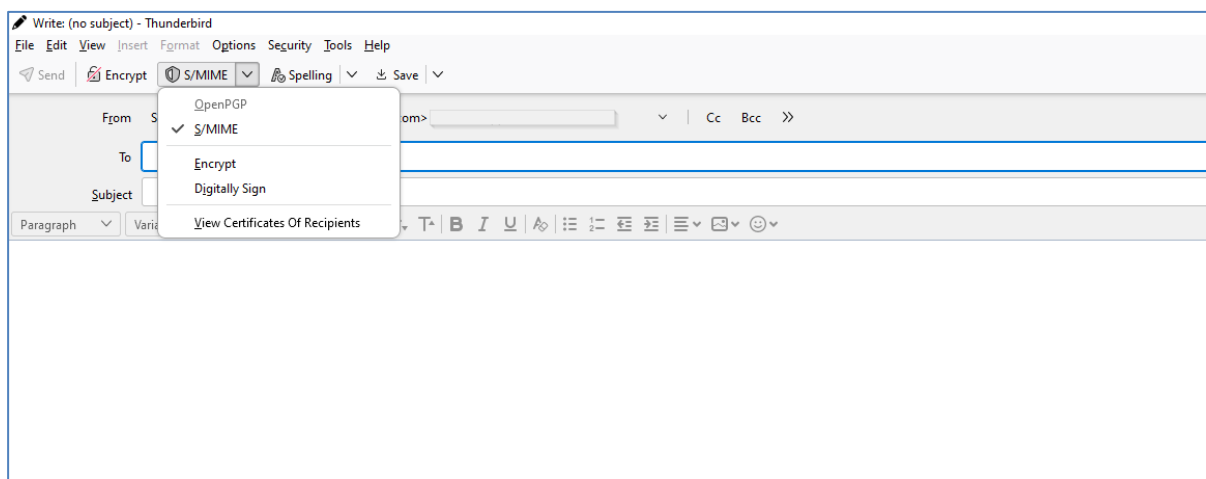
To encrypt an e-mail, it is mandatory to install your own certificate into the certificate store of the application. This will be a prerequisite for the following steps.

### 4.1 Encrypt an e-mail

Configure your certificate for encryption and digital signing at “Account Settings”, then “End-To-End Encryption”.

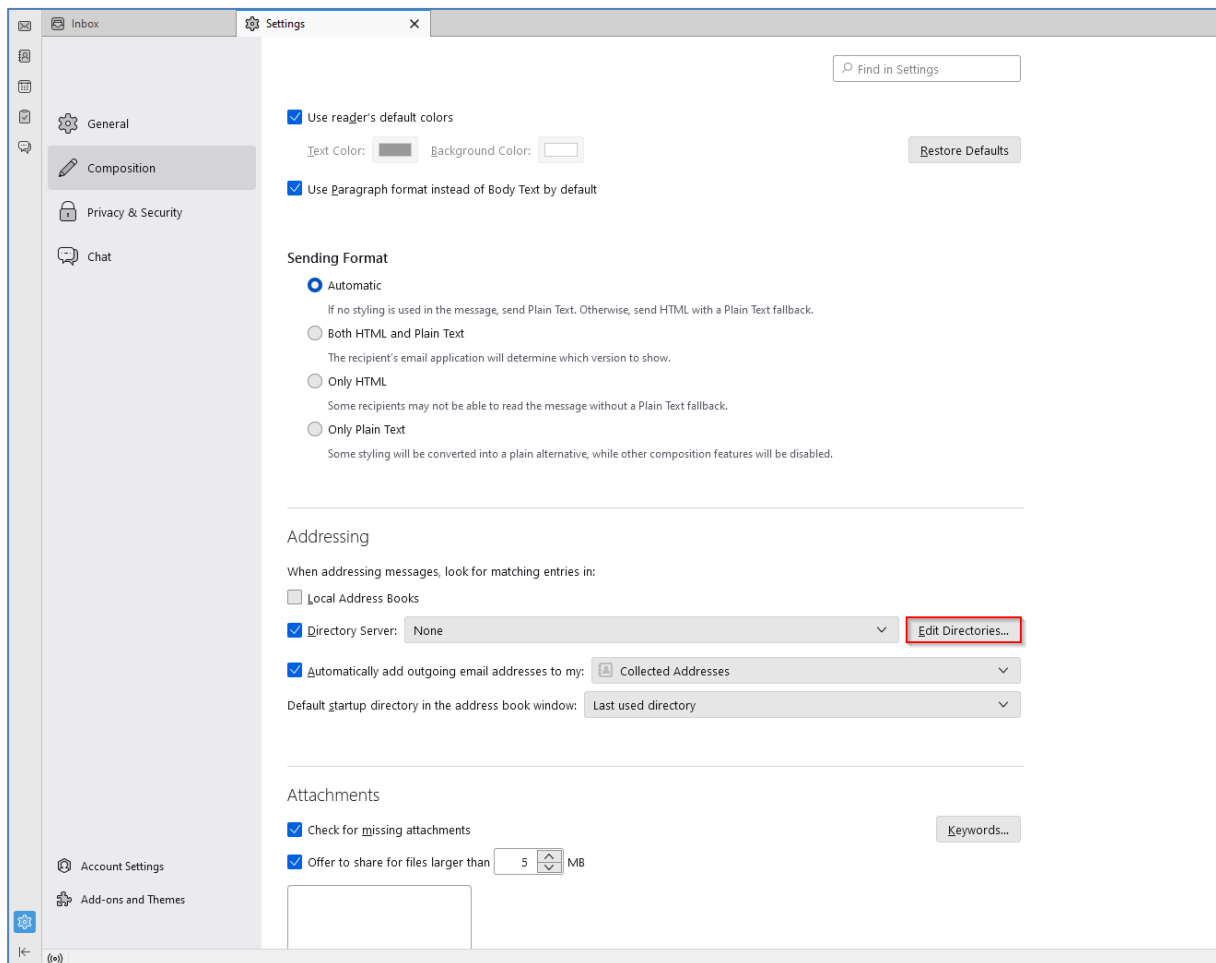


Begin to write a new e-mail and click on the arrow next to “S/MIME”. Select if you want to encrypt or sign the email.

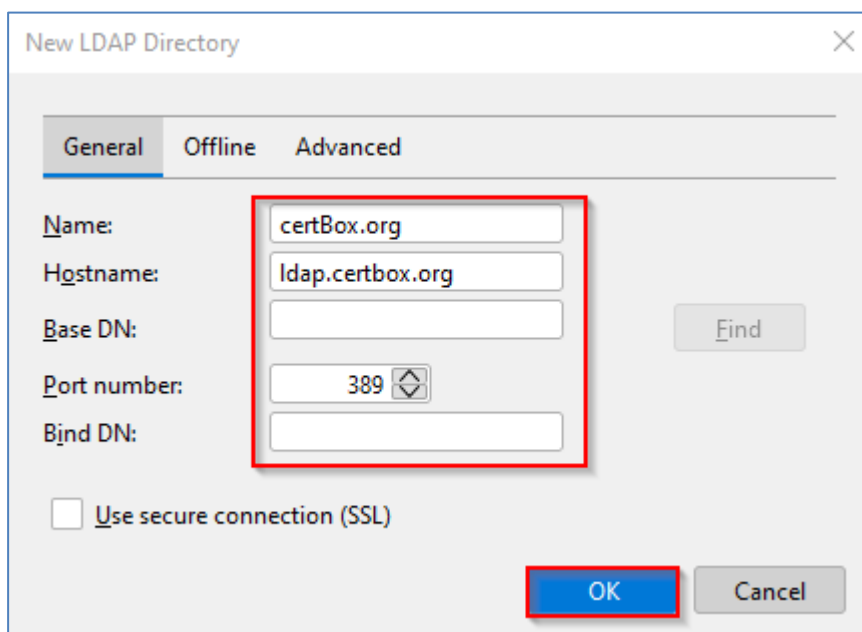


## 4.2 LDAP configuration for automated certificate search

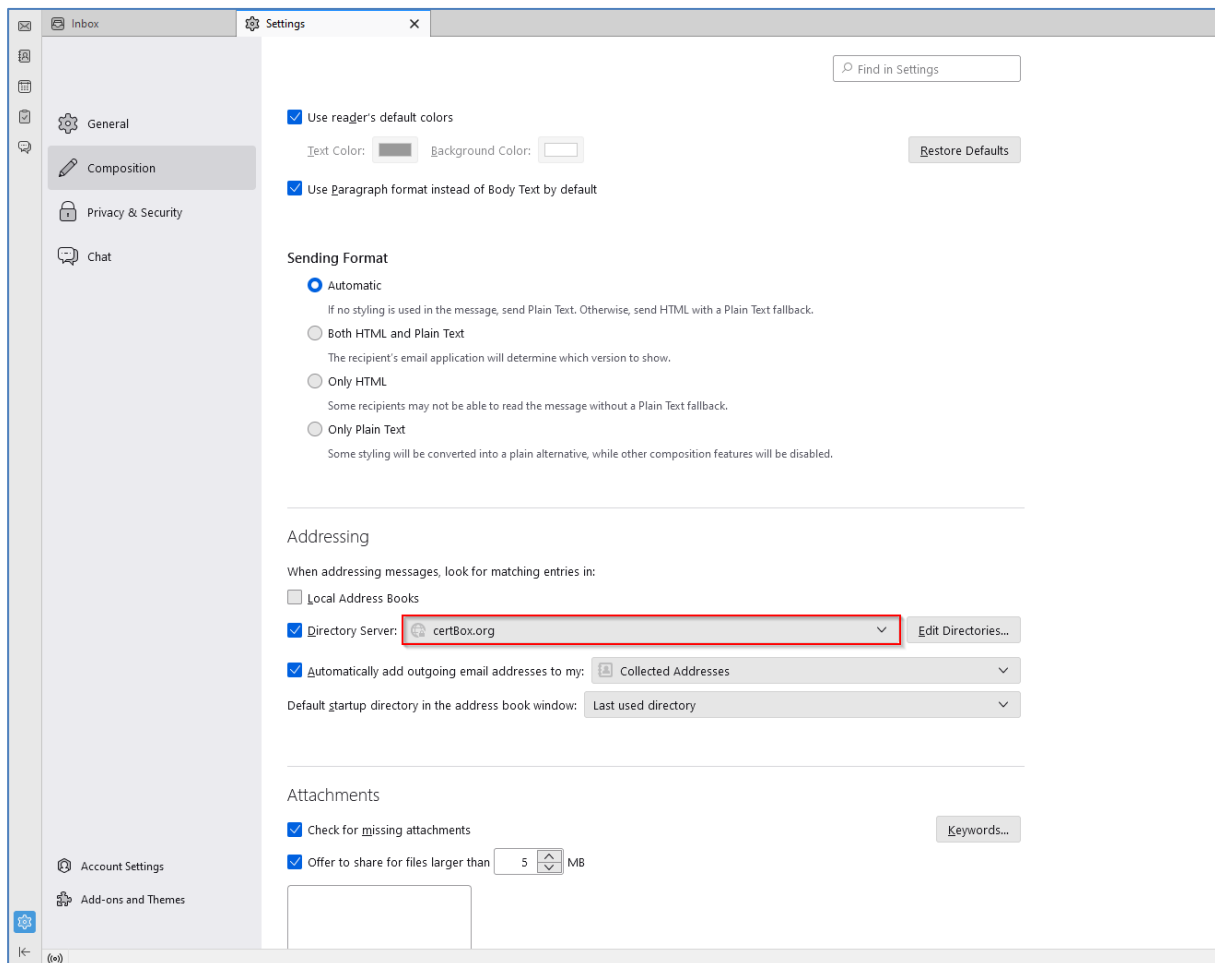
Go to the “Account Settings”, then “Composition” and then “Addressing”. Enable “Directory Server” and click “Edit Directories...” and then “Add”



Complete the dialog as follows and click “OK“. Close all dialogs until you are back at “Addressing“.



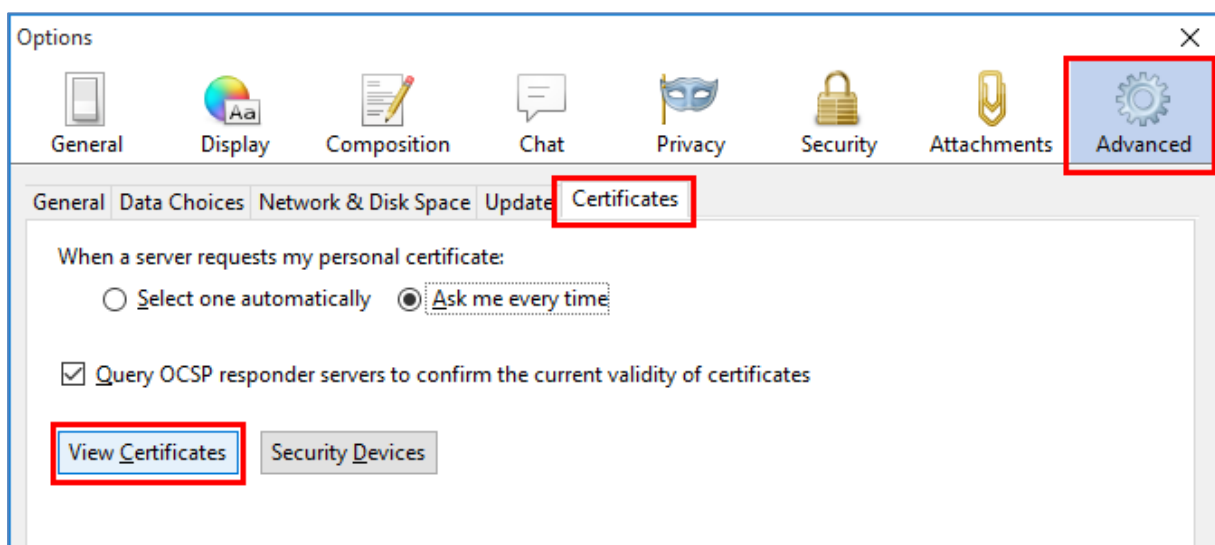
Back at “Addressing” select “certBox.org” as LDAP-directory server.



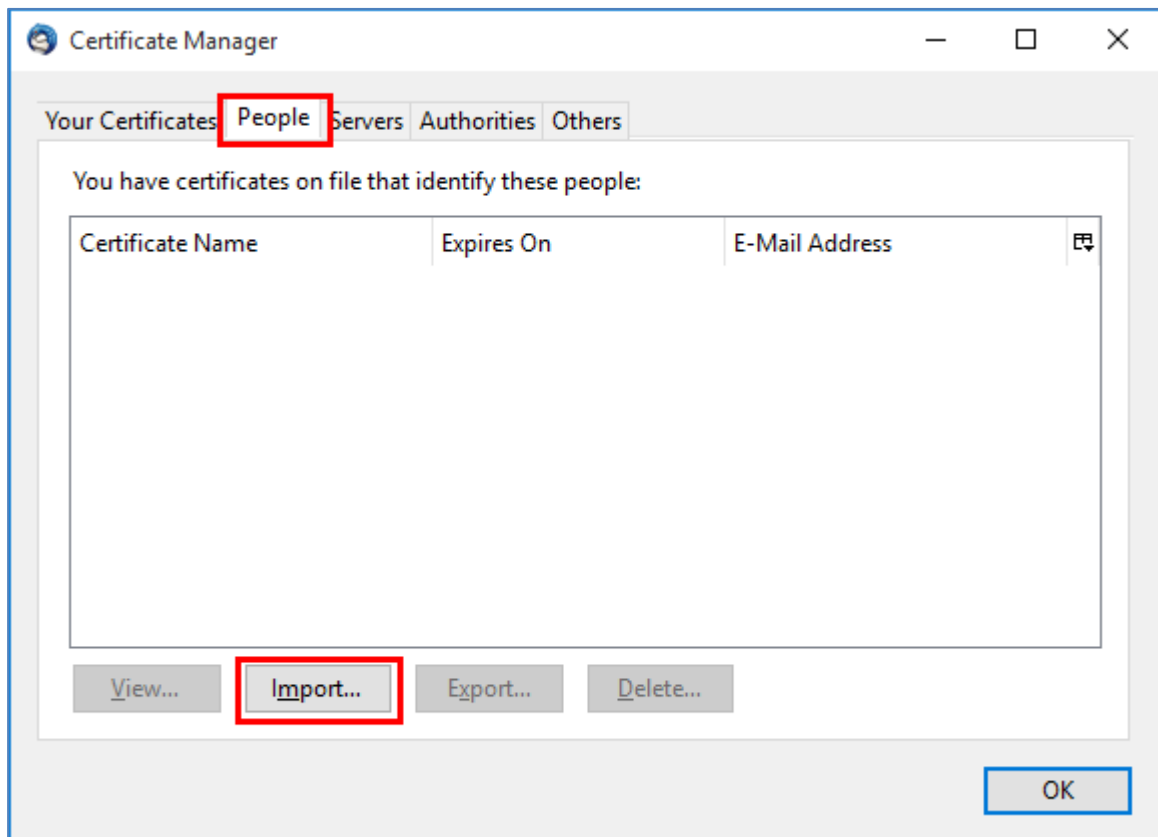
## 4.3 Import a certificate

Thunderbird only allows certificates to be imported, when it can form a complete certificate chain for it. For this you have to import the certificate chain as described in the next chapter.

Got to the settings and click on “Advanced” and then on “Certificates”



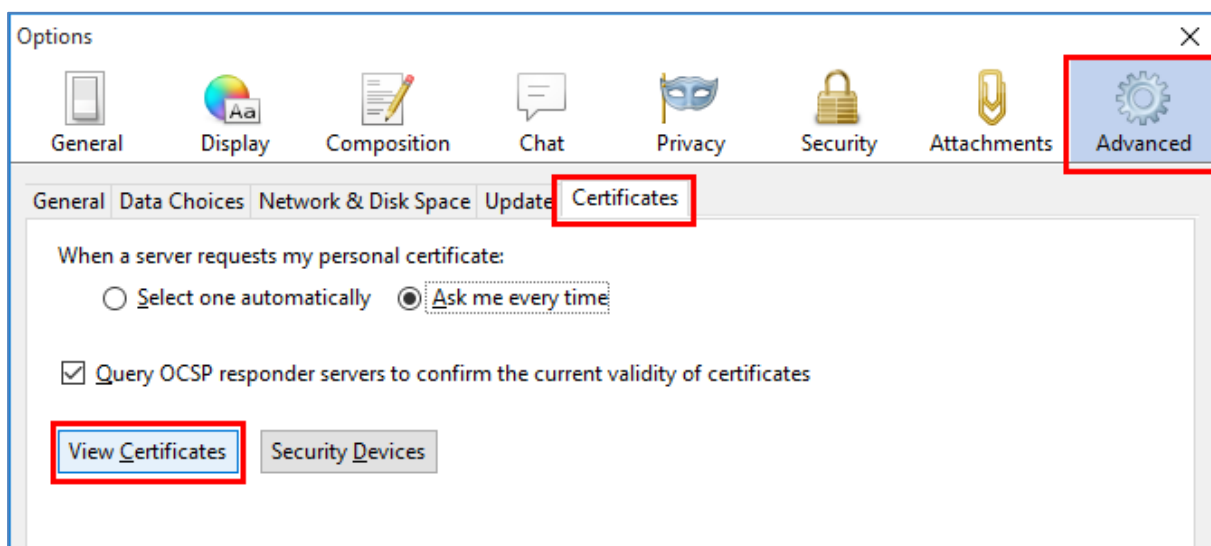
Click on “People” and then on “Import”



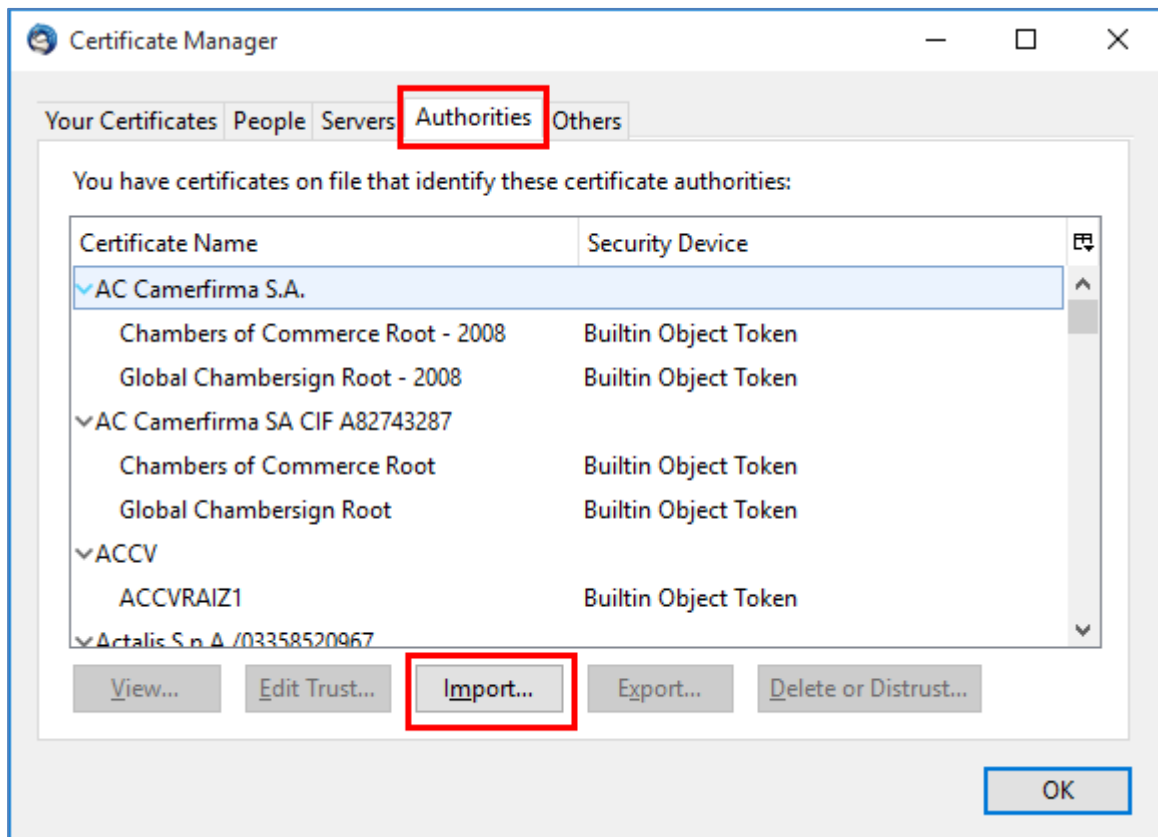
Open the previously downloaded certificate.

#### 4.4 Import a certificate chain

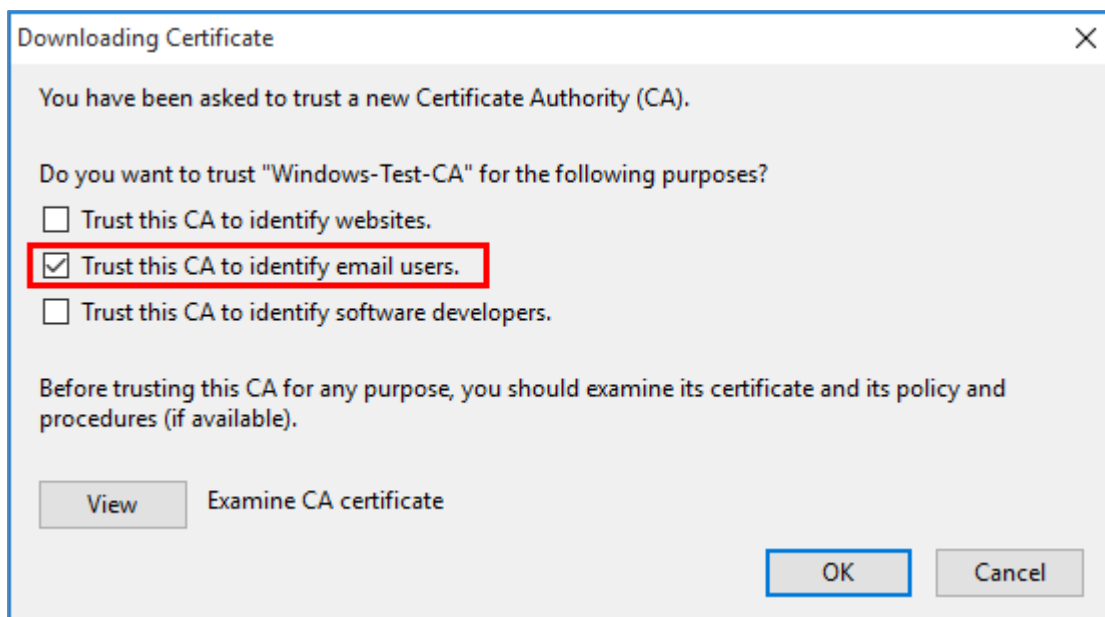
Got to the settings and click on “Advanced” and then on “Certificates”



Click on “Authorities” and then on “Import”



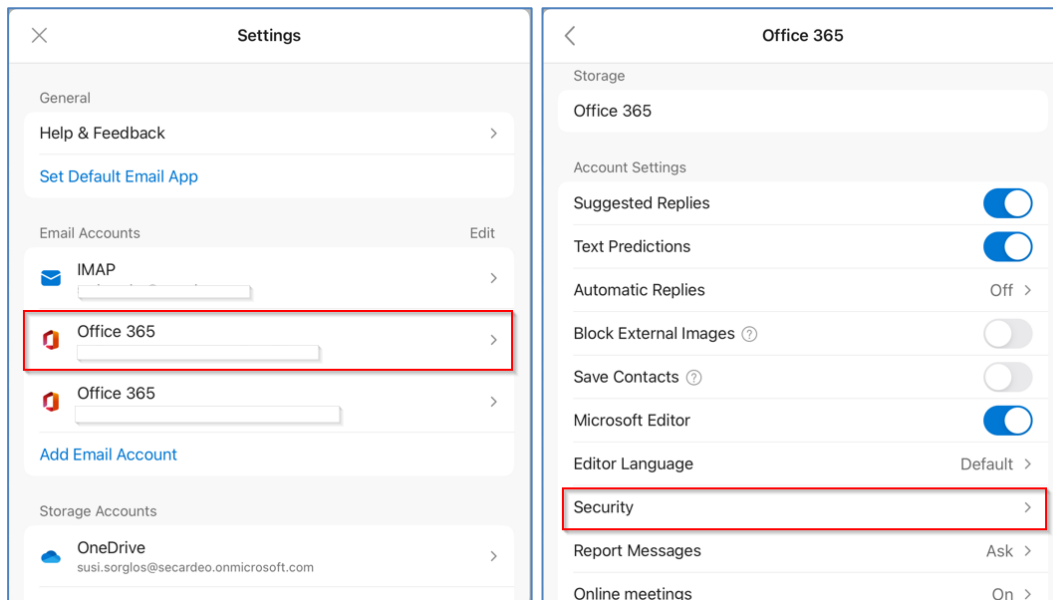
Now check the middle check box and click "OK".



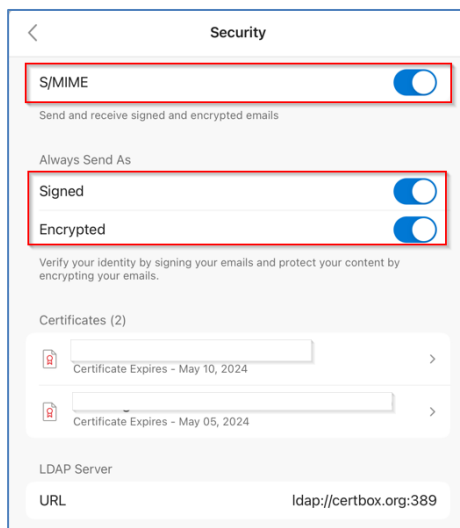
## 5 Outlook for iOS and Android

To encrypt an e-mail, it is mandatory to install your own certificate into the certificate store of the application. This will be a prerequisite for the following steps.

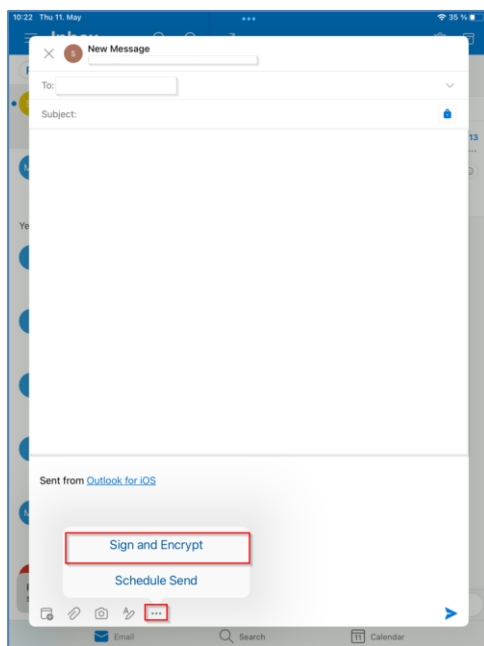
To activate encryption and digital signature, inside the Outlook app, you need to go to “Settings”, then “Email-Accounts” and “Security.”



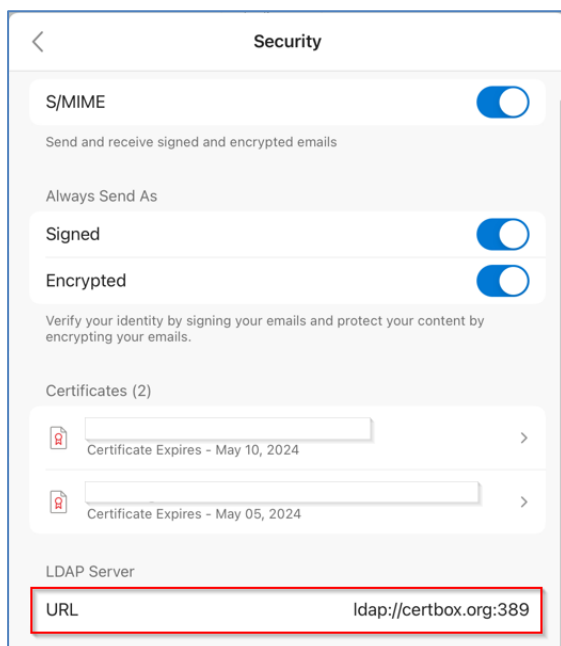
There you can now activate S/MIME and your installed certificates should be displayed here. You can now activate signature and encryption as the default for your e-mails.



It is also possible to activate and deactivate encryption and signature on any email individually by clicking on the three dots and then on “Sign and Encrypt”.

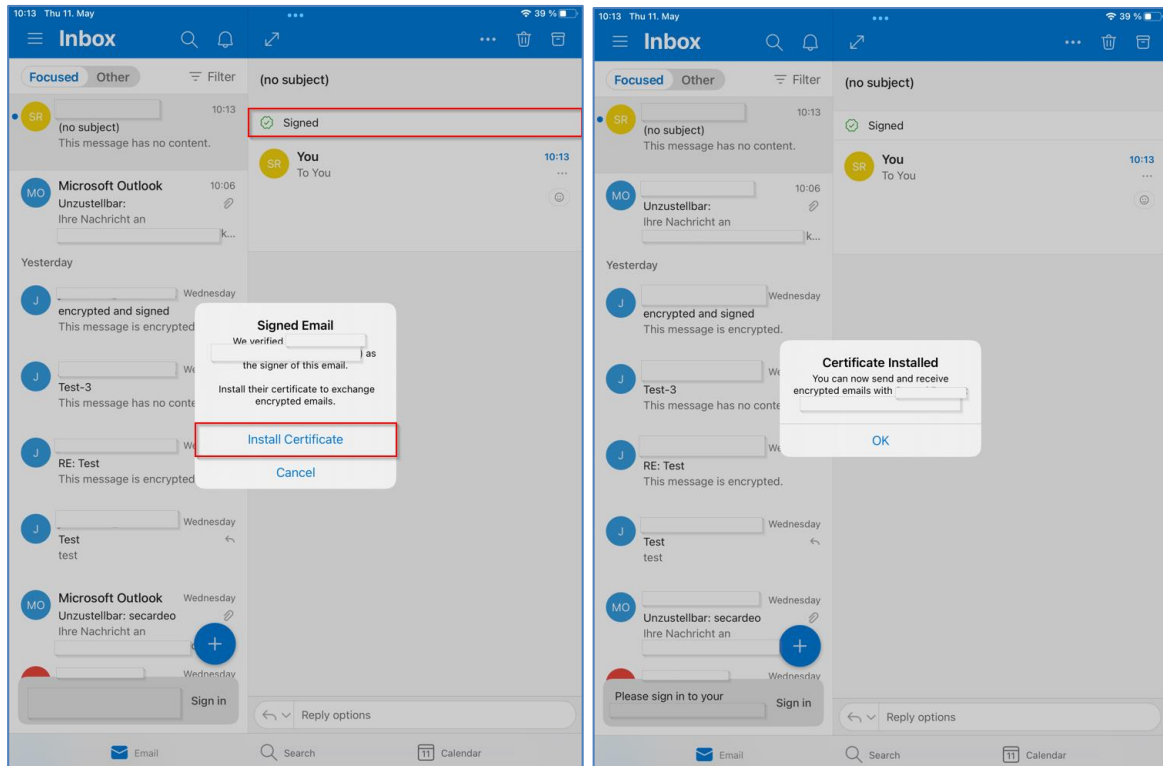


In order to send out an encrypted e-mail, you need to first install the certificate of the recipient into your Outlook app. This can be done automatically through certBox or manually. In order to automatically search the certBox for the recipient's certificate, you can configure the LDAP-Directory at "Settings – E-Mail Accounts – Security – LDAP Server".



In order to manually add a certificate, you can press on the banner "Signed" when receiving an e-mail from them and the app will ask you to import their certificate and to use it for future encryption.



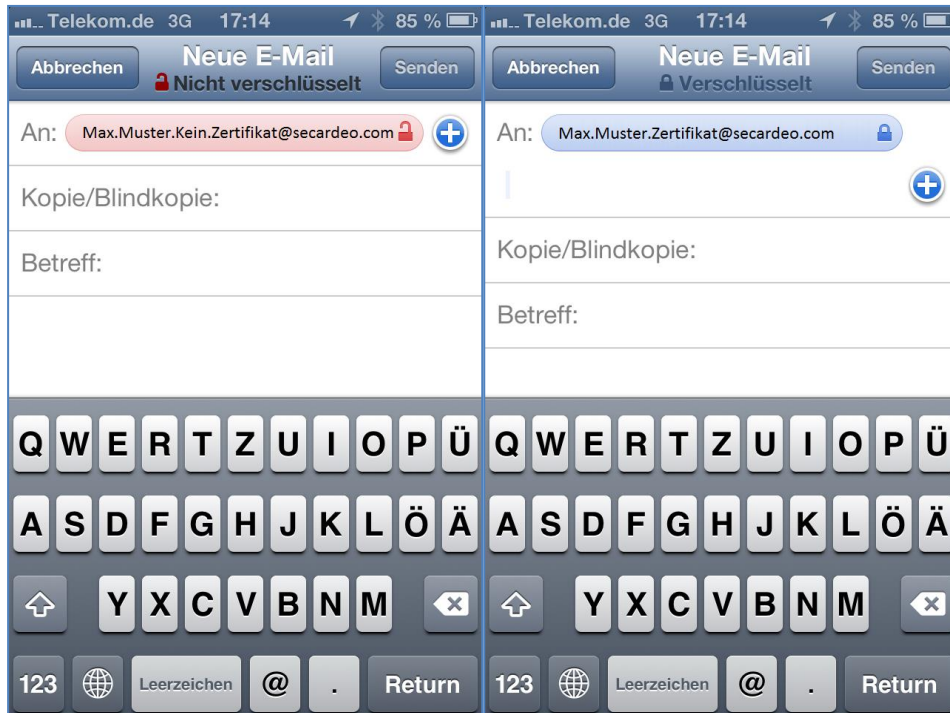


## 6 Apple Mail

To encrypt an e-mail, it is mandatory to install your own certificate into the certificate store of the application. This will be a prerequisite for the following steps.

### 6.1 Encrypt an e-mail

Encryption can be turned on and off in Mail by pressing on the padlock symbol if the certificate is available.

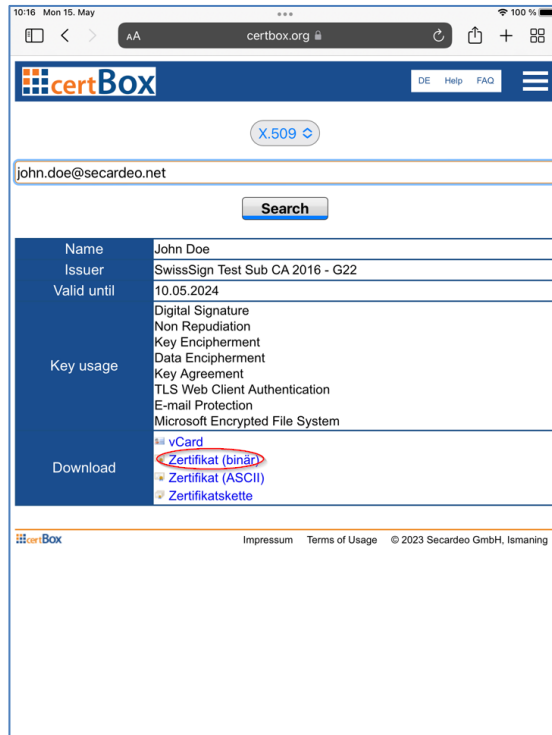


## 6.2 LDAP configuration for automated certificate search

The import of certificates via the LDAP interface of the certBox is currently not supported by the iOS.

## 6.3 Import a certificate manually from the HTML-Search

Press the link "Search" and enter the requested e-mail address



Afterwards press on the link “Certificate”.

The device automatically recognizes, that the file is a certificate and it will be available in “Settings”

Press on “Install”.