

certBox

Help-Manual

Secardeo GmbH
Release: 29.12.2023

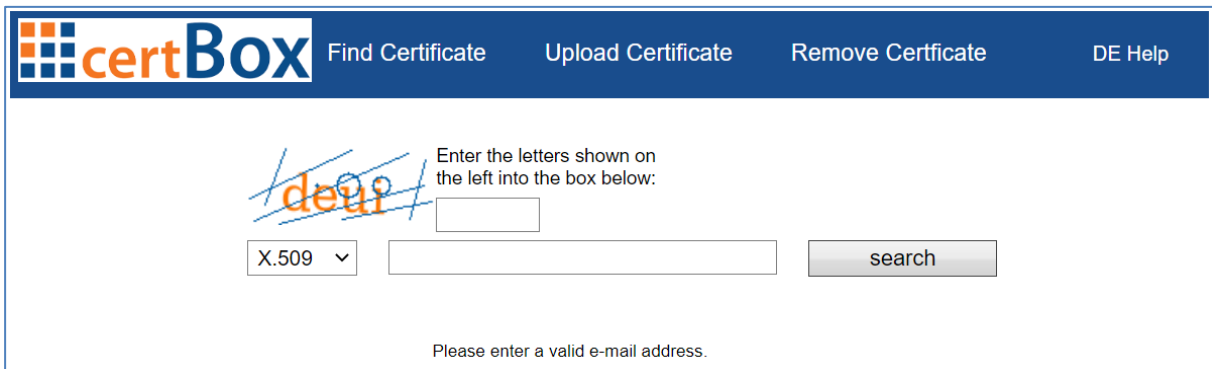
Table of Contents

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.....	2
2	Upload or Remove your Public Key Certificate.....	4
3	Decrypting an E-Mail with ICE	6
3.1	Using a local E-Mail client	6
3.1.1	Download of the ICE-Certificate.....	6
3.1.2	Outlook	6
3.1.3	Thunderbird.....	9
3.1.4	iOS.....	12
3.2	Using a Web-Mailer and certBox Web-Decrypter.....	13

1 Search and retrieve Public Key Certificates

1.1 Search by an e-mail address

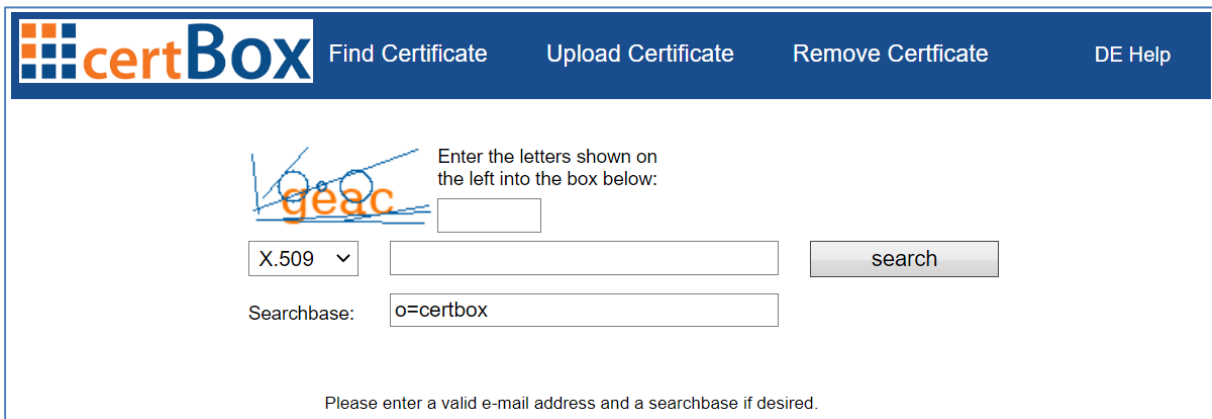
In order to search for X.509 certificates or PGP keys, please enter the letters displayed on the left into the box on the right. If you are an internal user the captcha code will not appear. Afterwards enter the desired e-mail address and click the “search” button. The certBox will automatically search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



The screenshot shows the top navigation bar with the certBox logo and links for 'Find Certificate', 'Upload Certificate', 'Remove Certificate', and 'DE Help'. Below the navigation bar, there is a captcha image with the text 'deu?' and a small input box for the captcha code. To the right of the captcha, there is a larger input box for the email address and a 'search' button. Below the search 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.

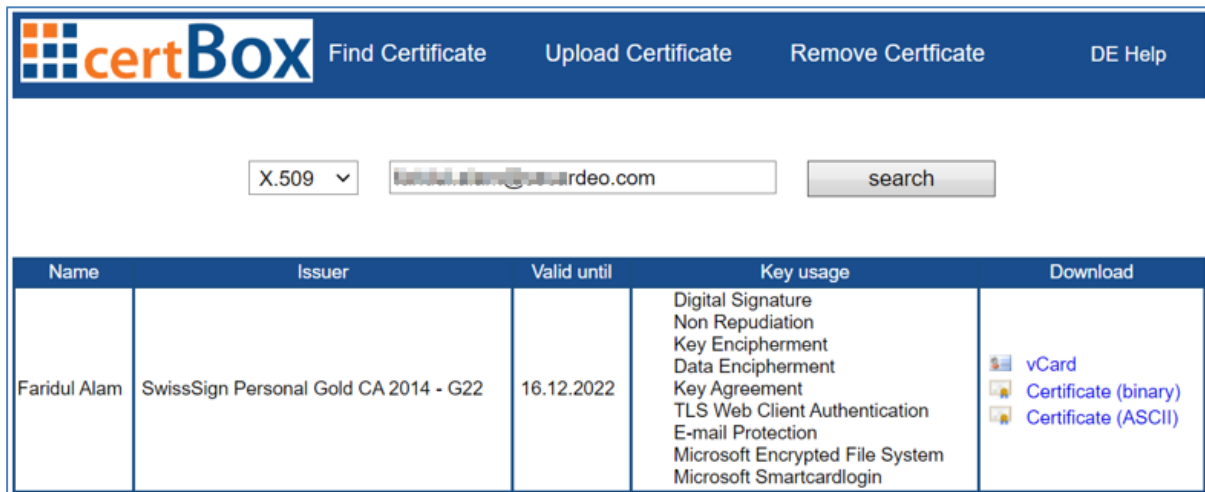
To perform a search you have to enter the login data into the corresponding fields.



The screenshot shows the top navigation bar with the certBox logo and links for 'Find Certificate', 'Upload Certificate', 'Remove Certificate', and 'DE Help'. Below the navigation bar, there is a captcha image with the text 'geac' and a small input box for the captcha code. To the right of the captcha, there is a larger input box for the email address and a 'search' button. Below the search form, there is a 'Searchbase:' label and an input box containing 'o=certbox'. Below the search form, there is a message: 'Please enter a valid e-mail address and a searchbase if desired.'

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.



The screenshot shows the certBox interface with a search bar containing 'Faridul Alam@secardeo.com' and a dropdown menu set to 'X.509'. Below the search bar is a table with the following data:

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 name of the applicant for the certificate.

Issuer: This is the name of the certificate that has signed the key of the user certificate.

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 different sign appears (e.g. a question mark) the certificate is classified trustworthy by the certBox, but the revocation status has not been verified.

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

Download:

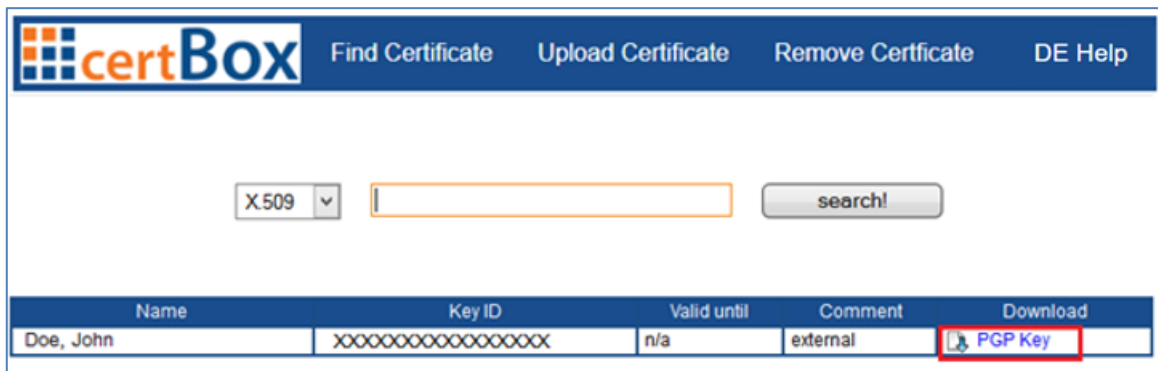
vCard A vCard includes not only the information necessary to encrypt, but also information about the contact, such as e-mail, name, phone etc. The vCard can be opened, for example, directly from Outlook and saved as a contact.

Certificate (ASCII) A certificate contains information to send an encrypted e-mail to its owner. It needs to be imported into the program to be used.

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 were searching 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.

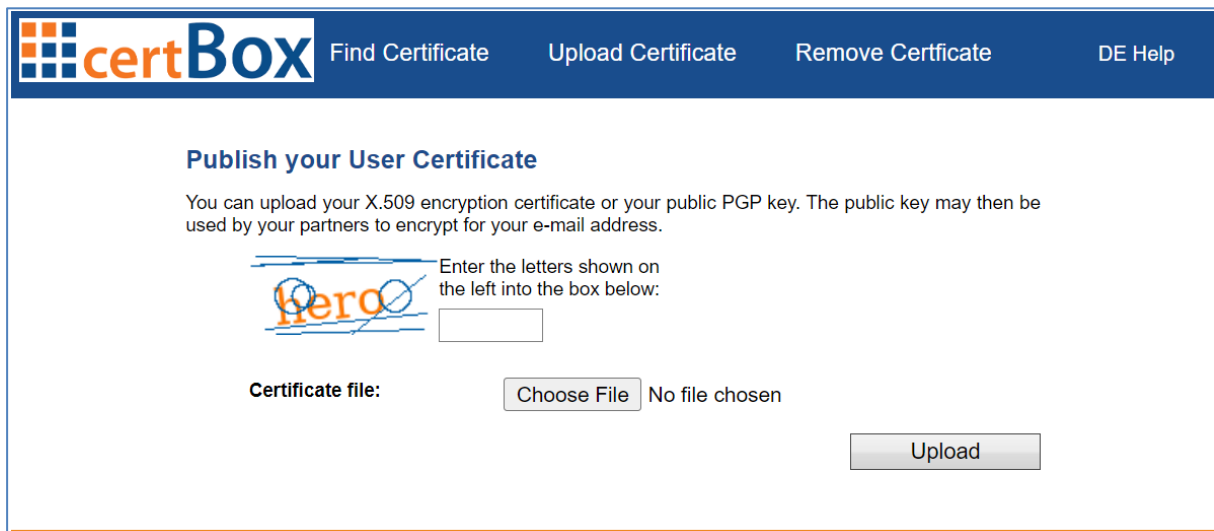


2 Upload or Remove your Public Key Certificate

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

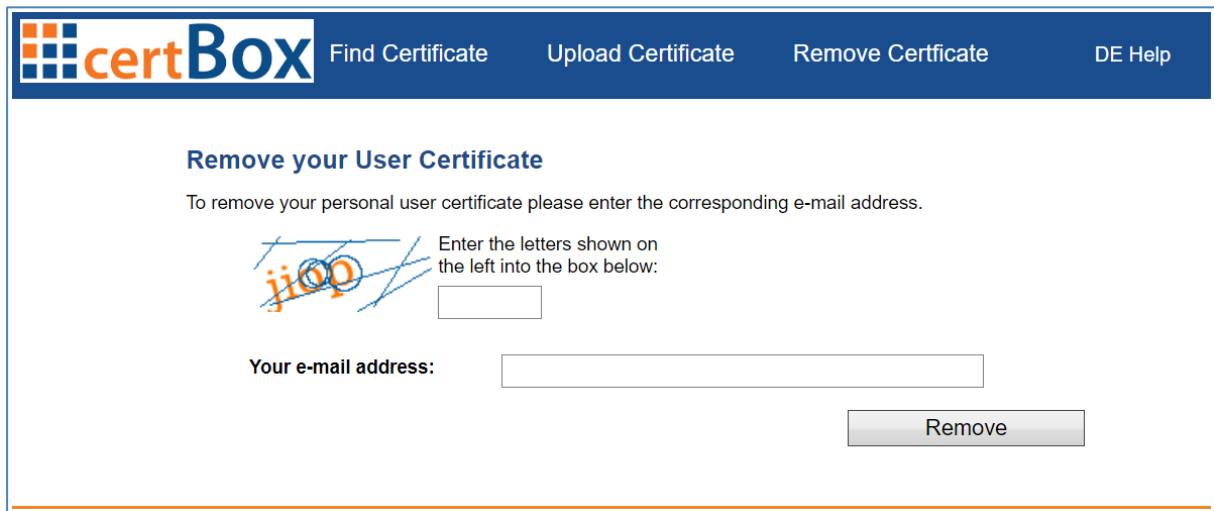
Publish your User Certificate

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 a web interface for removing a user certificate. At the top is a dark blue navigation bar with the certBox logo and four menu items: "Find Certificate", "Upload Certificate", "Remove Certificate", and "DE Help". The main content area has a white background with a blue header "Remove your User Certificate". Below this is a short instruction: "To remove your personal user certificate please enter the corresponding e-mail address." There is a CAPTCHA section with a distorted image of the letters "jjoo" and a small input box to its right with the text "Enter the letters shown on the left into the box below:". Below the CAPTCHA is a label "Your e-mail address:" followed by a long text input field. At the bottom right of the form is a grey "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 email 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 simple ignore the email.

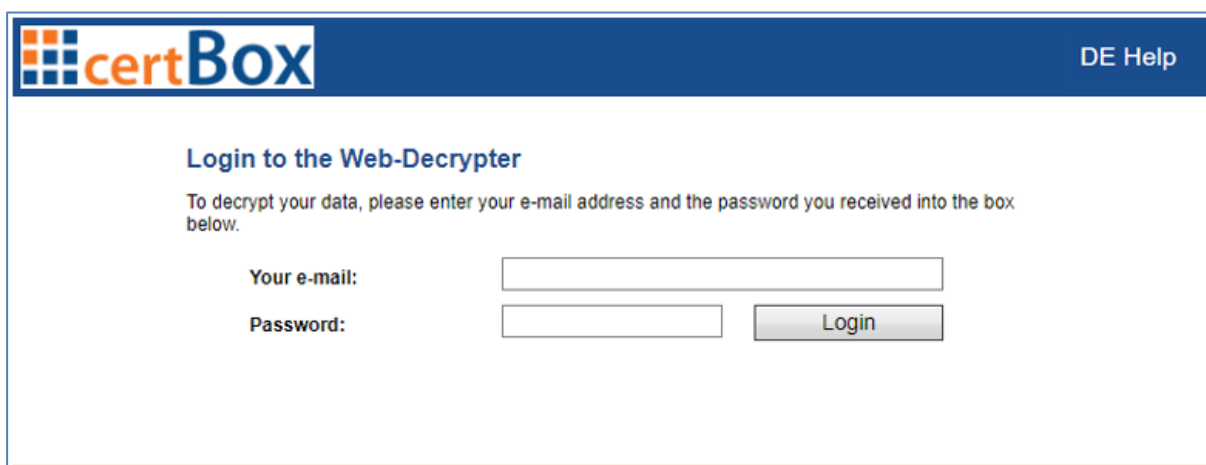
3 Decrypting an E-Mail with ICE

3.1 Using a local E-Mail client

3.1.1 Download of the ICE-Certificate

First your ICE certificate with your private key has to be downloaded.

1. Open the notification e-mail from your partner's certBox "Your key for your e-mail"
2. Click on the link containing your e-mail address, e.g.
<https://certbox.secardeo.com/ice/yourname@yourcompany.com>
3. To fetch your ICE certificate enter your e-mail address and the password given in the notification e-mail and click on "Download".

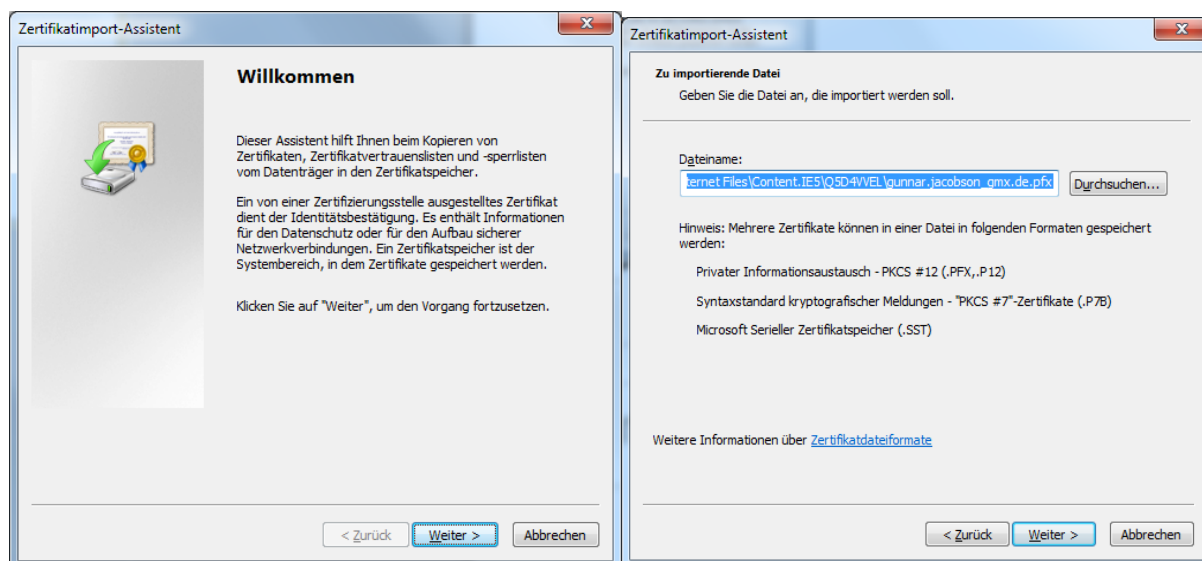


The screenshot shows the 'Login to the Web-Decrypter' page. At the top left is the certBox logo, and at the top right is a 'DE Help' link. The main heading is 'Login to the Web-Decrypter'. Below it, a message reads: 'To decrypt your data, please enter your e-mail address and the password you received into the box below.' There are two input fields: 'Your e-mail:' and 'Password:'. To the right of the password field is a 'Login' button.

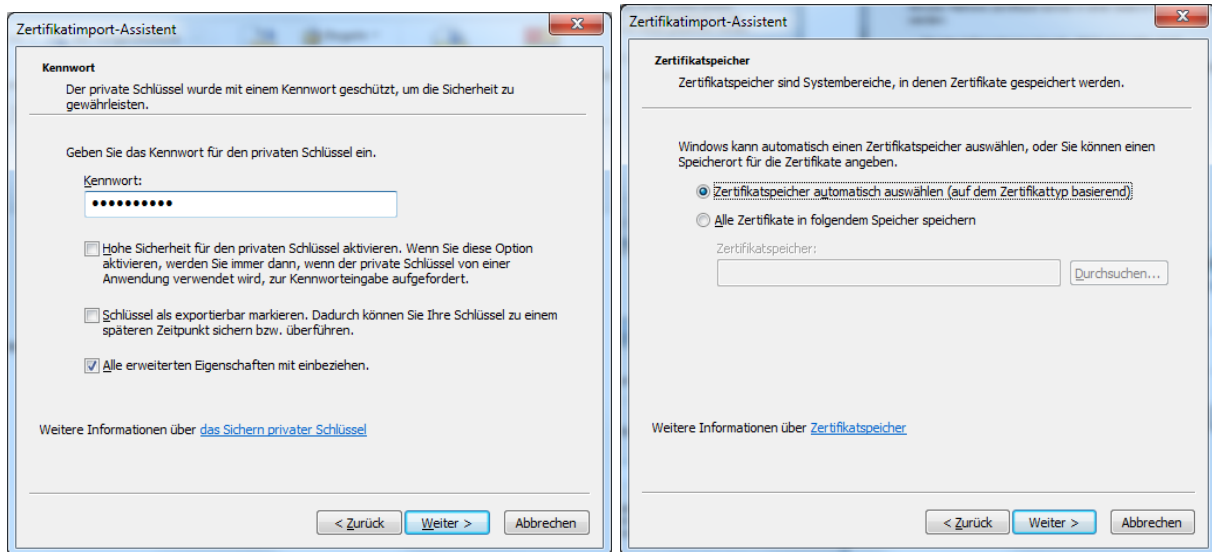
3.1.2 Outlook

3.1.2.1 Import of the ICE certificate

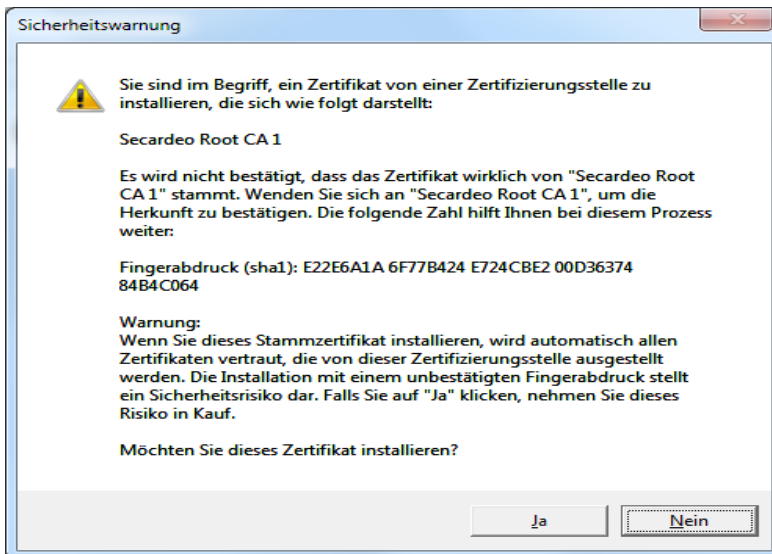
After downloading your certificate with the Internet Explorer please click "Open". The certificate import assistant will start. In the first two dialogs click "Continue".



Now you will be prompted to enter the password for your private key. The password is the one you received in your notification e-mail. Click “Continue” in this and the next dialog.

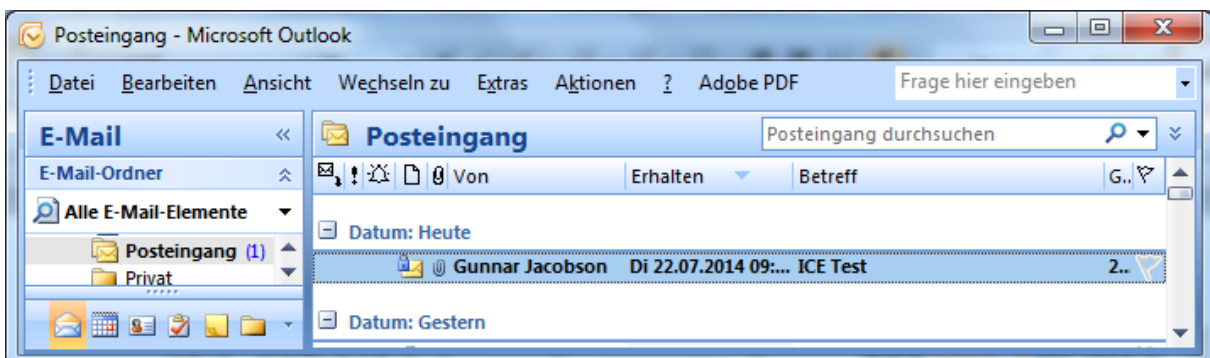


If the root certificate of your partner is not already installed you have to do this in the next dialog clicking “Yes”.



3.1.2.2 Reading the encrypted e-mail

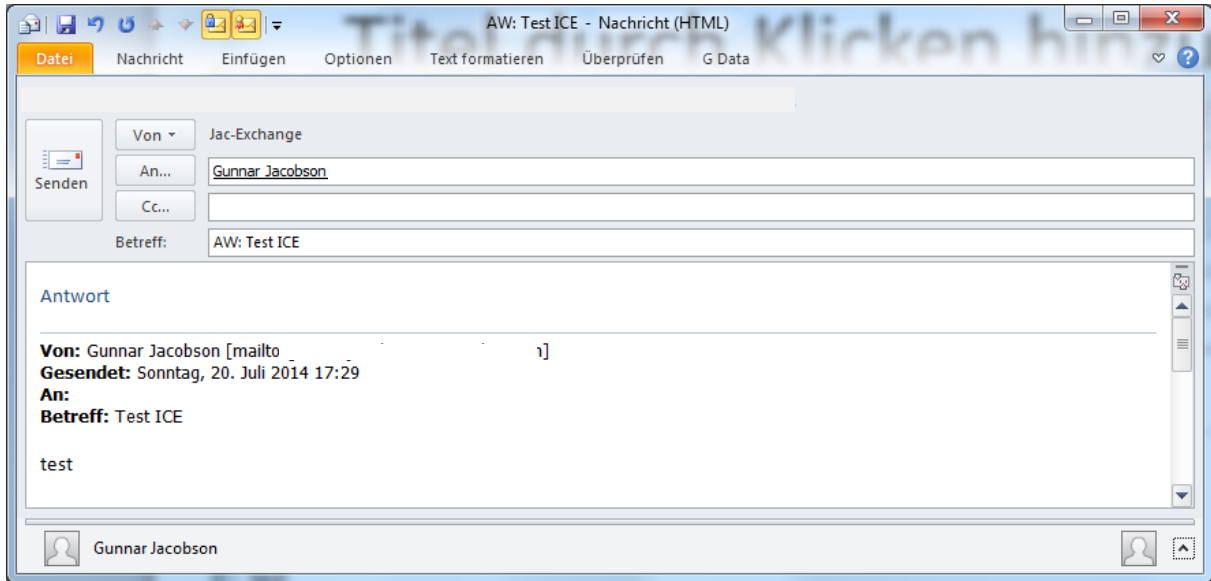
The encrypted e-mail is marked with a padlock in your inbox. After the import of your certificate and private key you can now open the encrypted e-mail by double clicking it.



3.1.2.3 Answering with an encrypted e-mail

You can also easily answer with an encrypted e-mail, because Outlook automatically adopts the security settings of the original e-mail.

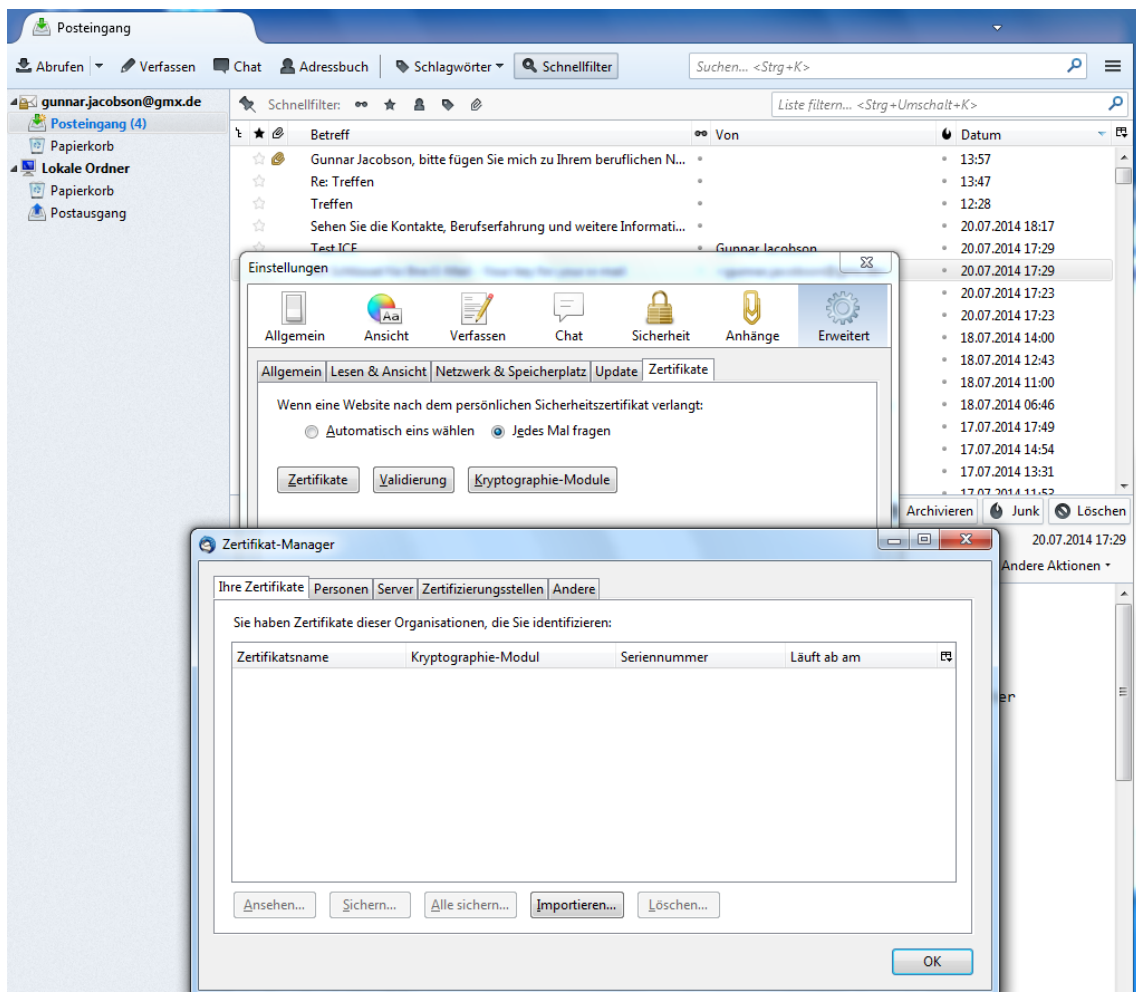
Under “Properties” → “Security” you can check whether the option “Encrypt messages and attachments” is checked.



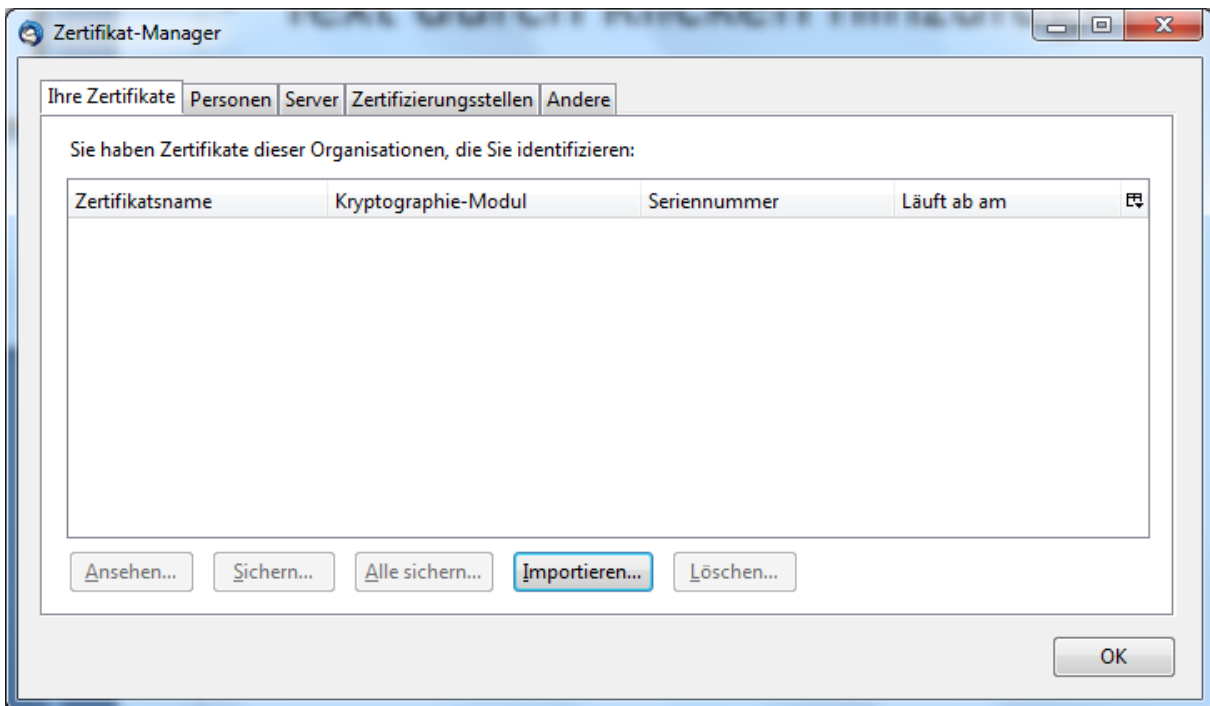
3.1.3 Thunderbird

3.1.3.1 Import of the ICE certificate

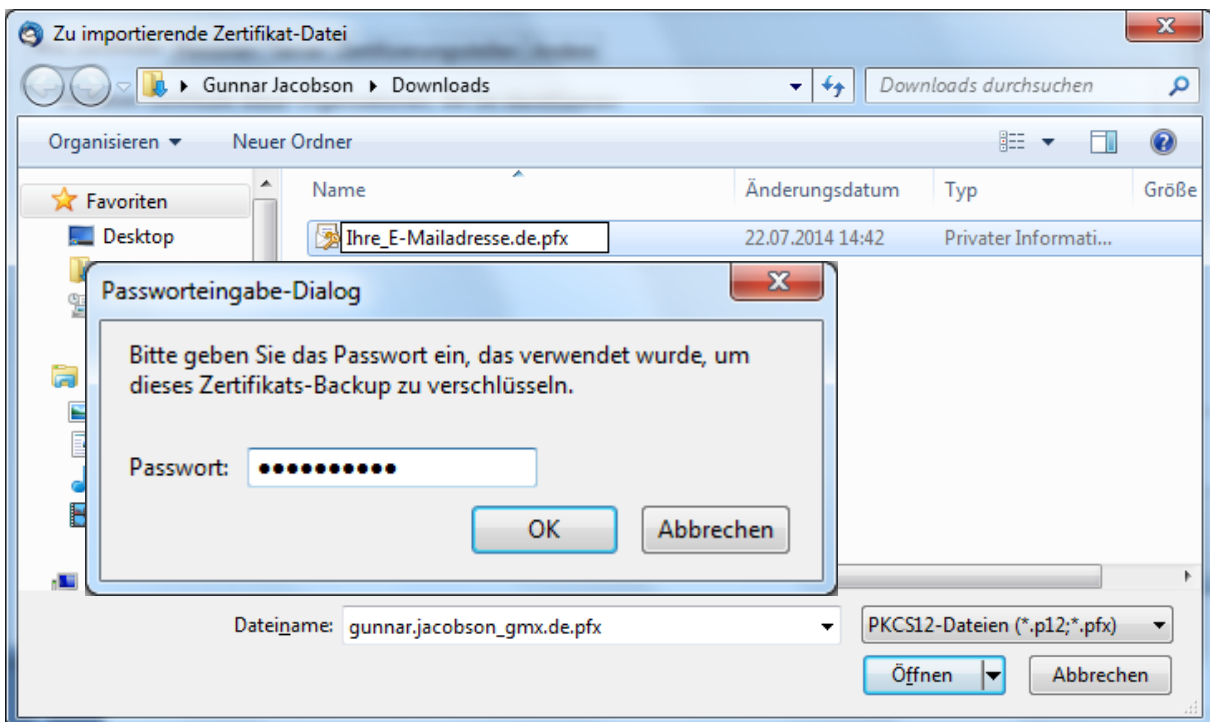
After downloading your certificate with your Web browser please click “Save”. Open “Settings” → “Advanced” → “Certificates” in Thunderbird. Click on the button “Certificates” and the dialog “Certificate Manager” will open.



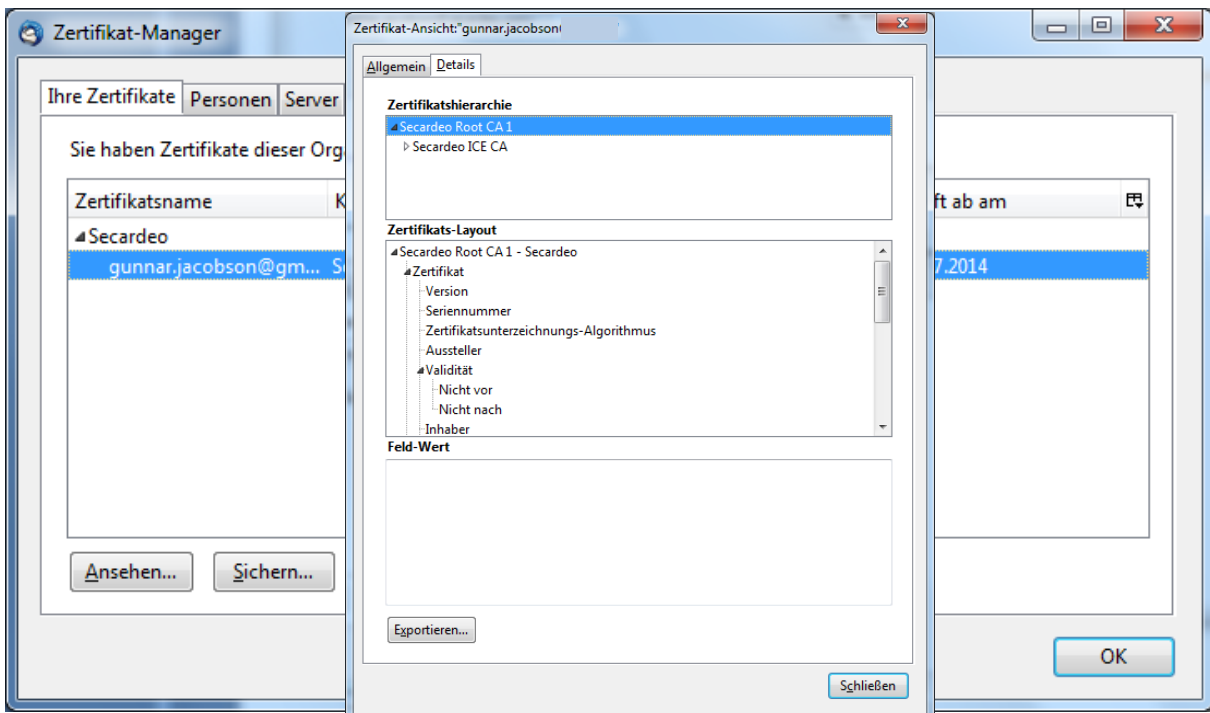
Choose “Your Certificates” and click “Import...”.



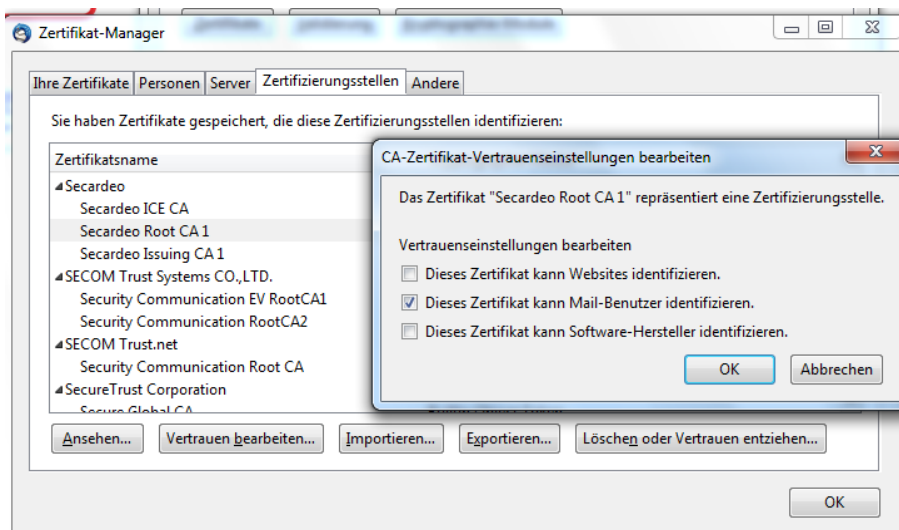
Navigate to the folder “Downloads” and open the file <e-mail address>.pfx. Enter the password for your private key which you have received in your notification e-mail.



The ICE certificate will now be listed in the “Certificate Manager”. Click “Show...” and then “Details”. The first entry in the certificate hierarchy is the Root CA for your ICE certificate. Close the dialog.



Now choose “Certificate Authorities”. Select the Root CA Certificate you just determined and click “Edit trust...”. Choose “Mail User” for the trust setting and click “Ok”.

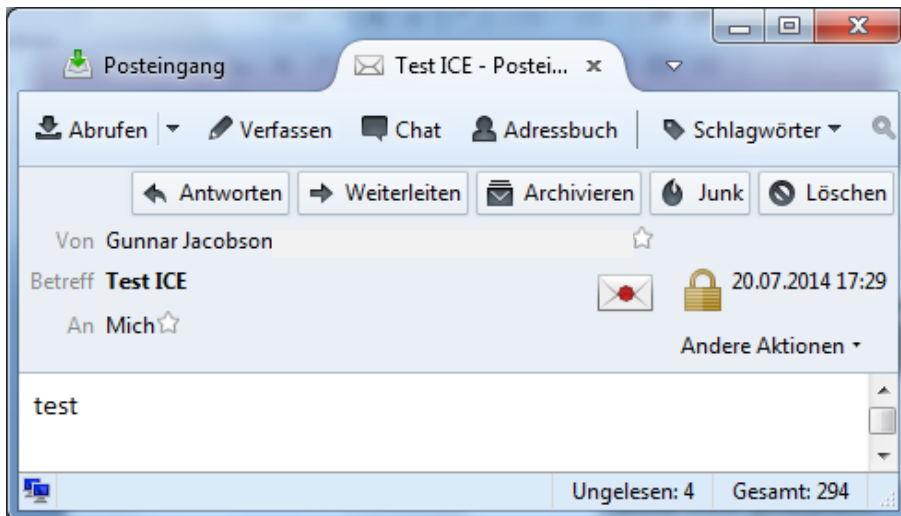


Close the Certificate Manager with “Ok”.

3.1.3.2 Reading the encrypted e-mail

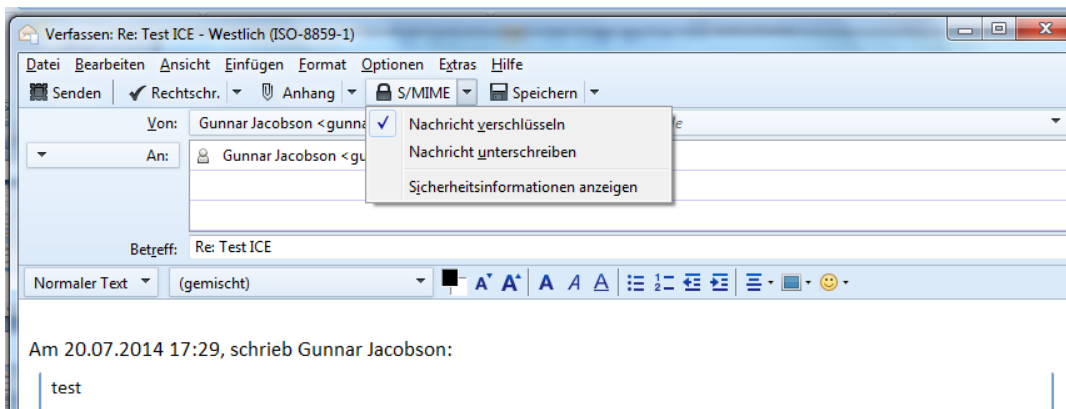
After the import of your certificate and private key you can now open the encrypted e-mail by double clicking it in your inbox.

The padlock symbol means that the e-mail is encrypted. An envelope with seal means that it has a digital signature.



3.1.3.3 Answering with an encrypted e-mail

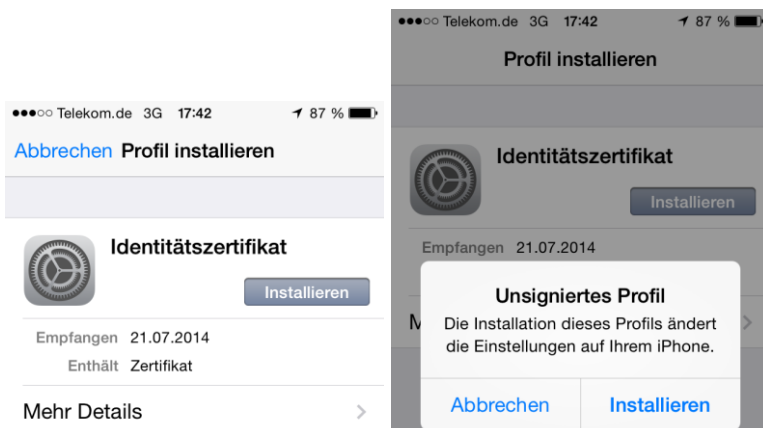
You can easily answer with an encrypted e-mail. To do so, check that “encrypt message” under “S/MIME” is activated.



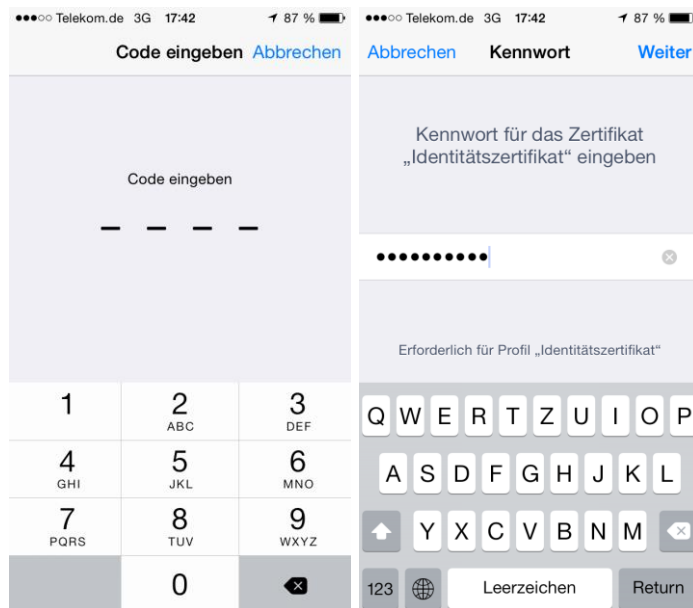
3.1.4 iOS

3.1.4.1 Import of the ICE certificate

After clicking “Download” the Profile Installation Dialog will open with the ICE certificate. Click “Install” in this and the following dialog.



You will now be asked to enter your personal PIN Code and then the password for the private key which you have received in the notification e-mail.



3.1.4.2 Reading the encrypted e-mail

After the import of your certificate and private key you can now open the encrypted e-mail just like the others. The padlock symbol shows that the e-mail is encrypted.

3.2 Using a Web-Mailer and certBox Web-Decrypter

If you are using a Webmail service like GMX or Gmail, you will have received two e-mails:

1. A notification e-mail from ICE which will contain an instruction and a link to the certBox Web-Decrypter.
2. An (empty) e-mail from the internal originator with an attachment “smime.p7m”

Please click on the Web-Decrypter link in the ICE notification and a login dialog appears. You may log in using your e-mail address and the password you received. Your e-mail address must be entered into the “Your e-mail” field. The password must be entered into the “Password” field.

Note: If you received a 2nd password from your partner organization, you will have to register first, using the “ICE registration form” (please contact your partner).

After logging in, you are prompted to upload the “smime.p7m” attachment, which you have previously downloaded from your Webmail service.

The screenshot shows the 'certBox' logo in the top left of a blue header bar. To the right of the logo are four navigation links: 'Find Certificate', 'Upload Certificate', 'Remove Certificate', and 'DE Help'. Below the header, the main content area is titled 'Decrypt your e-mail'. Underneath this title is the instruction 'Upload the smime.p7m attachment from your e-mail.' There is a text input field with a 'Durchsuchen...' button to its right. Below the input field is an 'Upload' button. At the bottom of the form, there is a link: 'If you don't have a smime.p7m attachment please [click here](#).'


Figure 49: Web-Decrypter upload form

Some Webmail services do not provide the smime.p7m for download, e.g. outlook.com. In this case, you may select “click here” and a new page will open. Copy the HTML source code from your Webmailer and paste it into the Web-Decrypter form. After pressing the “Submit” button, the decrypted e-mail content will be displayed.



The screenshot shows the 'certBox' logo in the top left of a blue header bar. To the right of the logo is a 'DE Help' link. Below the header, the main content area is titled 'Decrypt your e-mail'. Underneath this title is the instruction 'In some cases an e-mail service will not offer the encrypted message for download.' Below this is an example: 'e.g. Outlook.com' followed by detailed instructions: 'Display your e-mail and on the right side, click on "Actions" and select "View Message Source". A new window will open. Select all the text (or press CTRL+A), right-click on it and then "copy". Now right-click into the box below and select "paste". Press the Submit button and your e-mail will be decrypted.' Below the instructions is a large, empty text input box. At the bottom right of the form is a 'Submit' button.

Figure 50: Web-Decrypter HTML input form

After decrypting the e-mail, it will displayed on a new page. You can choose to download the attachments, save the message, or open the message in a new window.


DE Help

Recipient: secqsmail@gmail.com

File: smime.p7m


Attachments

- To display the user friendly view, click on the "Open in new window" button in the top right corner -

Dear Mr. Brown,

Thank you for your interest in our products.

I have included an offer and further information for you.

Please contact me if you have any questions or concerns.

I am looking forward to hear from you.

Sincerely,

John Doe

Figure 51: Web-Decrypter display e-mail