



certBox Help-Manual

Secardeo GmbH Release: 14.02.2025

certBox Help Manual

14.02.2025



Table of Contents

Sea	arch 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
Uplo	oad or Remove your Public Key Certificate	4
Dec	crypting 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 iOS1	2
3.2	Using a Web-Mailer and certBox Web-Decrypter1	3
	Sea 1.1 1.2 Upl Dec 3.1 3.1 3.1 3.1 3.1 3.2	Search and retrieve Public Key Certificates



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 PGPkeys, please select "PGP" from the drop down menu.

	Upload Certificate	Remove Certficate	DE Help
X.509 ~	letters shown on to the box below:	search	
Please ent	er 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.

EcertBOX	Find Certificate	Upload Certificate	Remove Certficate	DE Help
X.509 Searchba	Enter the the left int int int int	letters shown on o the box below:	search	
F	Please enter a valid e-ma	il 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.

се		Upload (Certificate Remove Certficat	e DE Help
Name	X.509 V Future la suer	Valid until	om search 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:

This is the name of the applicant for the certificate.
This is the name of the certificate that has signed the key of the user certificate.
The certificate is valid until this date.
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.
The certificate can only be used for these purposes.
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.
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.

	Find Certificate	Upload Certificate	Remove Certfic	ate DE Help
X.509	~		search!)
Name	Key ID	Valid until	Comment	Download
Doe, John	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	xx n/a	external	🕞 PGP Key



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.

Elect Box	Find Certificate	Upload Certificate	Remove Certficate	DE Help
Publish yo You can upload used by your pa	ur User Certificat your X.509 encryption c inters to encrypt for you Enter the the left int	e ertificate or your public PGP I r e-mail address. letters shown on o the box below:	key. The public key may then be	
Certific	ate file:	Choose File No file chose	n Upload	



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

	Upload Certificate	Remove Certficate	DE Help
Remove your User Certifi To remove your personal user certific	icate cate please enter the correspon	ding e-mail address.	
the lef	the letters shown on it into the box below:		
Your e-mail address:		Remove	

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 email"
- 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".

End		DE Help
Login to the Web-Decryp To decrypt your data, please enter below. Your e-mail:	oter your e-mail address and the password you received into the box	
Password:	Login	

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.

Zertifikatimport-Assistent	Zertifikatimport-Assistent
Kennwort Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.	Zertifikatspeicher Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
Geben Sie das Kennwort für den privaten Schlüssel ein. Kennwort: Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert. Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.	Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.
Alle erweiterten Eigenschaften mit einbeziehen.	Weitere Informationen über Zertifikatsneicher
<pre>// Claride Entering of the Content product du libised // Claride Entering of the Claride Entering</pre>	<zurück weiter=""> Abbrechen</zurück>



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.

Posteingang - Microsoft Outlook						
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht	Datei Bearbeiten Ansicht Wechseln zu Extras Aktionen ? Adobe PDF Frage hier eingeben -					
E-Mail «	Posteingang Posteingang durchsuchen	ج م	×			
E-Mail-Ordner 🕆	🖼 🖞 🖄 🖞 🕼 Von 🛛 Erhalten 🔻 🛛 Betreff	G 🖗				
🔎 Alle E-Mail-Elemente 🛛 🔻	Datum: Heute	L				
Posteingang (1) 📥						
Privat 💌	E Guinial Jacobson Di 22.07.2014 09: ICE Test	2				
- 🔁 📰 💷 🗳 🐷 🕞	Datum: Gestern		Ŧ			

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" \rightarrow "Security" you can check whether the option "Encrypt messages and attachments" is checked.

ê 🖬 🚽	U 🍝 🕈	<u>∎⊿}a</u> -	T:	AW: Test I	CE - Nachricht (HTML)	11:	cho	-	
Datei	Nachricht	Einfügen	Optionen	Text formatieren	Überprüfen	G Data				 ~ ?
	Von -	Jac-Exchange								
Senden	An	Gunnar Jacobs	on_							
Senden	Сс									
	Betreff:	AW: Test ICE								
Antwor	t									
Von: Gu Gesend An: Betreff:	innar Jacobs l et: Sonntag : Test ICE	son [mailto g, 20. Juli 2014	17:29	· 1]						
test										•
G	unnar Jacobs	son								Ω

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" \rightarrow "Advanced" \rightarrow "Certificates" in Thunderbird. Click on the button "Certificates" and the dialog "Certificate Manager" will open.





Choose "Your Certificates" and click "Import...".

Zertifikat-Manager	CAL GUILIT	numerica i i				
Ihre Zertifikate Personen S	erver Zertifizierungsstellen Ander	e				
Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:						
Zertifikatsname	Kryptographie-Modul	Seriennummer	Läuft ab am	E\$		
Accelor Cicker						
<u>Ansenen</u>	<u>Alle sichern</u>	<u>L</u> oschen				
				ОК		

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.

3 Zu importierende Zertifikat-Datei						
Gunnar Jacobson Downloads		• • Dowr	nloads durchsuchen	٩		
Organisieren 🔻 Neuer Ordner				0		
Favoriten Name	Änder	ungsdatum	Тур	Größe		
Desktop	se.de.pfx 22.07.2	2014 14:42	Privater Informati			
Passworteingabe-Dialog Bitte geben Sie das Passwort ein, da dieses Zertifikats-Backup zu versch Passwort: Datei <u>n</u> ame: gunnar.jacobson	as verwendet wurde, um lüsseln. OK Abbrechen _gmx.de.pfx	▼ PKCS1 Õffr	2-Dateien (*.p12;*.pfx) nen I▼ Abbrech	► ■ ■		



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.

Zertifikat-Manager	Zertifikat-Ansicht:"gunnar.jacobson	
Ihre Zertifikate Personen Server Sie haben Zertifikate dieser Org Zertifikatsname K	Allgemein Details Zertifikatshierarchie ✓ ✓Secardeo Root CA1 > > Secardeo Root CA1 ✓ ✓Secardeo Root CA1 - Secardeo ✓ ✓Zertifikats-Layout ✓ ✓Secardeo Root CA1 - Secardeo ✓ ✓Zertifikats ✓ ✓Version ■ ✓Zertifikatsunterzeichnungs-Algorithmus ✓ ✓Validität ✓ ✓Nicht vor ✓ ✓Nicht nach ✓ ✓Feld-Wert ✓	ft ab am 🛤
<u>A</u> nsehen <u>S</u> ichern	Exportieren Schließen	ОК

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".

Sie haben Zertifikate gespeichert, die diese Zertifizierungsstellen identifizieren:					
Zertifikatsname	CA-Zertifikat-vertrauenseinstellungen bearbeiten				
▲Secardeo Secardeo ICE CA	Das Zertifikat "Secardeo Root CA 1" repräsentiert eine Zertifizierungsstel				
Secardeo Root CA 1	Vertrauenreinstellungen hearheiten				
Secardeo Issuing CA 1	Dieses Zertifikat kann Websites identifizieren.				
▲ SECOM Trust Systems CO.,LTD.					
Security Communication EV RootCA1	Dieses Zertifikat kann Mail-Benutzer identifizieren.				
Security Communication RootCA2	Dieses Zertifikat kann Software-Hersteller identifizieren.				
▲ SECOM Trust.net					
Security Communication Root CA	OK Abbrecher				
SecureTrust Corporation					
Secure Global CA					
Ansehen Vertrauen <u>b</u> earbeiten Importieren Exportieren Lösche <u>n</u> oder Vertrauen entziehen					

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 email 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.

🔄 Verfassen: Re: Test IC	E - Westlich (ISO-8859-1)					
Datei Bearbeiten Ansicht Einfügen Format Optionen Extras Hilfe						
Senden 🖌 🖌 Rech	tschr. 🔻 🕖 Anhang 🔻 🔒 S/MIME 👻 🔚 Speichern 💌					
<u>V</u> on:	Gunnar Jacobson < gunna 🗸 Nachricht verschlüsseln e					
▼ An:	B Gunnar Jacobson < gu Nachricht unterschreiben					
	Sicherheitsinformationen anzeigen					
Bet <u>r</u> eff:	Re: Test ICE					
Normaler Text 🔻 (gemischt) ▼ 🖣 A' A' A A A 🖂 🗄 ½二 🗄 🙂 🐨					
Am 20.07.2014 17:29, schrieb Gunnar Jacobson:						

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.



certBox Help Manual



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.

••••• Telekom.de 3G 17:42 7 87 %			●●●○○ Telekom.de	🕇 87 % 🔳 🗖	
	Code eingeber	Abbrechen	Abbrechen	Kennwort	Weiter
_	Code eingeben	_	Kennw "Identitä	vort für das Zer ätszertifikat" eir	tifikat ngeben
			••••••	••	\otimes
			Erforderlich	für Profil "Identitäts	szertifikat"
1	2 ABC	3 Def	QWE	RTZU	ΙΟΡ
4 _{GHI}	5 JKL	6 MNO	ASD	FGH	JKL
7 PQRS	8 TUV	9 wxyz	► Y X	CVB	N M 💌
	0	⊗	123	Leerzeichen	Return

3.1.4.2 Reading the encrypted e-mail

After the import of your certificate and private key you can now open the encrypted email 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 emails:

- 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.

	Find Certificate	Upload Certificate	Remove Certficate	DE Help
Decrypt yo Upload the sm	our e-mail ime.p7m attachment from	your e-mail.	Durchsuchen Upload	
If you don't hav	ve a smime.p7m attachme	nt 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.

cert	Box	DE Help
E Ir D W b	Decrypt your e-mail as one cases an e-mail service will not offer the encrypted message for download. .g. Outlook.com isplay your e-mail and on the right side, click on "Actions" and select "View Message Source". A new window elow and select "paste". Press the Submit button and your e-mail will be decrypted.	

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.



Example 2 Contract of the second se	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 includeded 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	

