SECARDEO

certBox

certBox.org

User-Manual

Secardeo GmbH

Release: 07.11.2012

Contents

1 Introduction

1.1 General

For the encryption of e-mails or documents you need the recipients' digital certificates or public keys.

www.certBox.org offers a manual search for X.509 certificates and PGP keys using a HTML search page and an automated search using LDAP.

The manual search through the HTML search form is useful if you only occasionally encrypt to a few recipients.

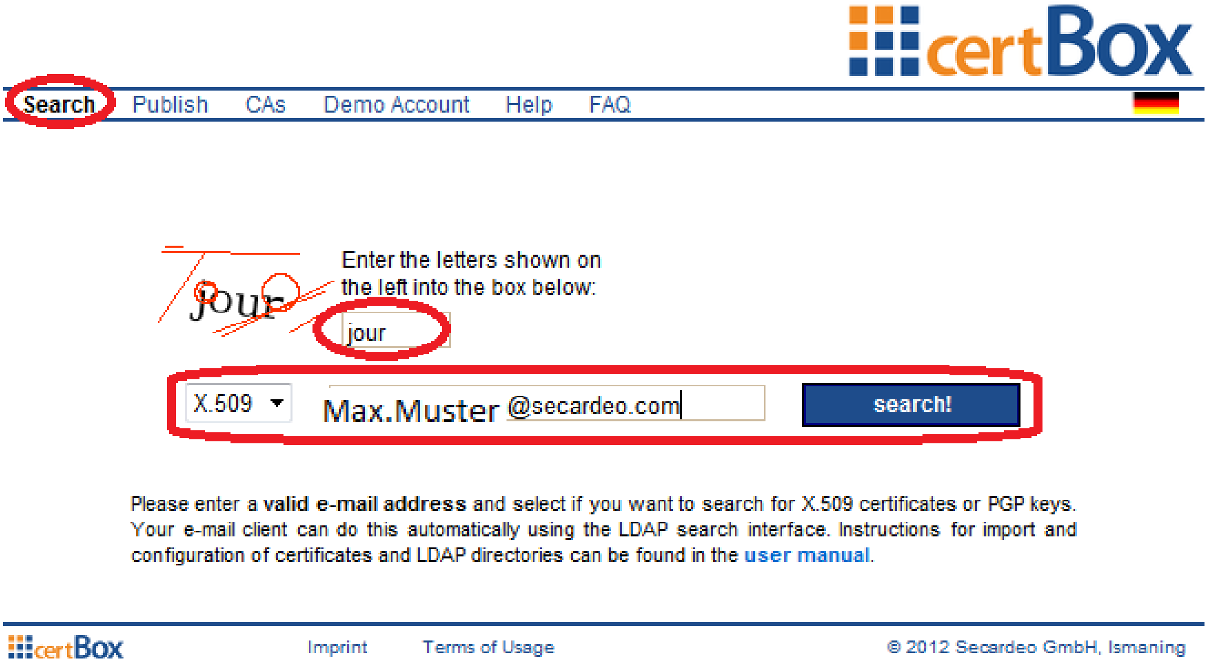
The automated search provides the highest user comfort, as only the option "Encrypt Message" must be selected in the application program.

2 HTML-Search and download

2.1 Manual search with the HTML-form

2.1.1 Entering the e-mail address

In order to search for certificates or keys please enter a complete and valid e-mail address into the address field and use the drop down box to select, if you want to search for X.509 certificates or PGP keys.
Before starting your first search please enter the random letters that are displayed on the left into the validation field. Click on “search!“.



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

jour

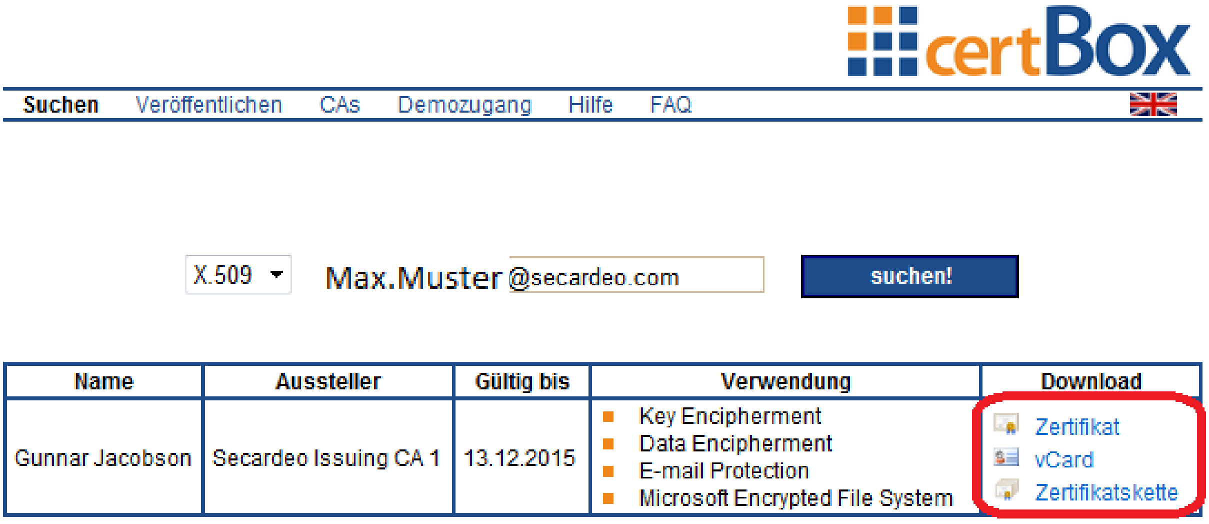
Max.Muster @secardeo.com

Please enter a **valid e-mail address** and select if you want to search for X.509 certificates or PGP keys. Your e-mail client can do this automatically using the LDAP search interface. Instructions for import and configuration of certificates and LDAP directories can be found in the **user manual**.

© 2012 Secardeo GmbH, Ismaning

2.1.2 Download of a certificate, a vCard or a certificate chain

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



Max.Muster @secardeo.com

Name	Aussteller	Gültig bis	Verwendung	Download
Gunnar Jacobson	Secardeo Issuing CA 1	13.12.2015	Key Encipherment Data Encipherment E-mail Protection Microsoft Encrypted File System	Zertifikat vCard Zertifikatskette

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

Explanation to 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 to:
The certificate is valid until this date.

Usage:
The certificate can only be used for these purposes.

Download:

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

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 chain:
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. Unfortunately we can’t offer a complete chain for all certificates. The chain is required by some programs to trust the user certificate because otherwise, it will not encrypt with this certificate.

For the import, please read the relevant section of your application.

2.1.3 Automated search with LDAP

For automated LDAP-queries please follow the following instructions for your program. If your program is not described here, please do as follows:

Configure your e-mail application according to your user guide with the address

ldap://ldap.certbox.org and

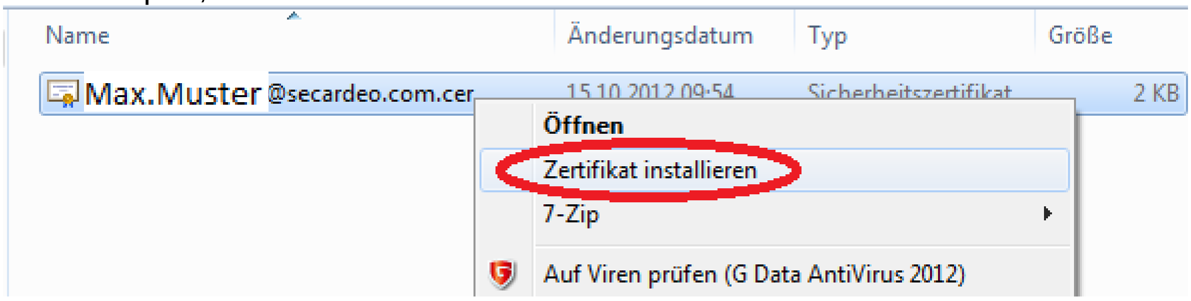
port 389.

The search base is empty.

3 Windows certificate store

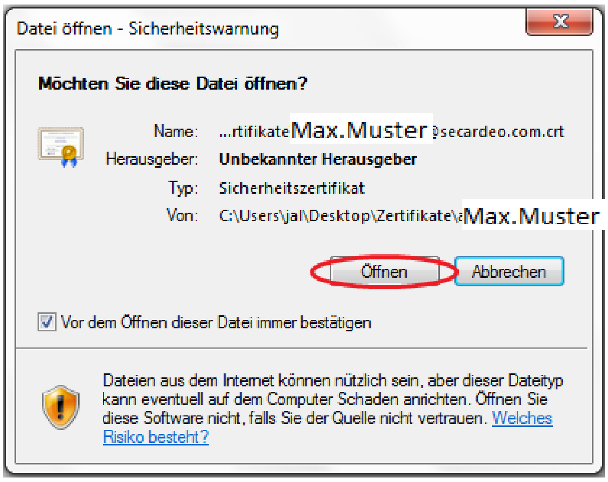
3.1 Import of a certificate

This certificate can later be used to encrypt, if your application can form the certificate chain. If not please follow the instructions in chapter 3.2.
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“



Name	Änderungsdatum	Typ	Größe
Max.Muster @secardeo.com.cer	15.10.2012 09:54	Sicherheitszertifikat	2 KB

Afterwards click on “Open“



Datei öffnen - Sicherheitswarnung

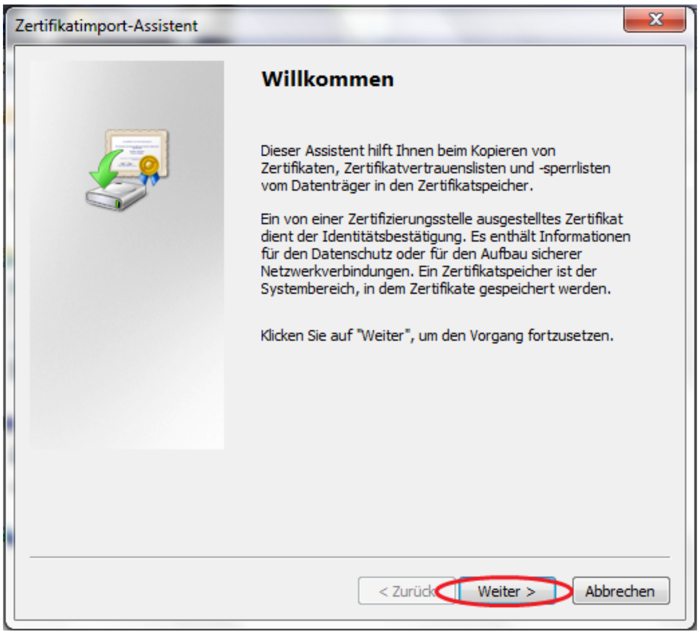
Möchten Sie diese Datei öffnen?

Name: ...rtifikateMax.Muster @secardeo.com.crt
Herausgeber: **Unbekannter Herausgeber**
Typ: Sicherheitszertifikat
Von: C:\Users\jal\Desktop\Zertifikate\Max.Muster

☑ Vor dem Öffnen dieser Datei immer bestätigen

Dateien aus dem Internet können nützlich sein, aber dieser Dateityp kann eventuell auf dem Computer Schaden anrichten. Öffnen Sie diese Software nicht, falls Sie der Quelle nicht vertrauen. Welches Risiko besteht?

Now click “Next“



Zertifikatimport-Assistent

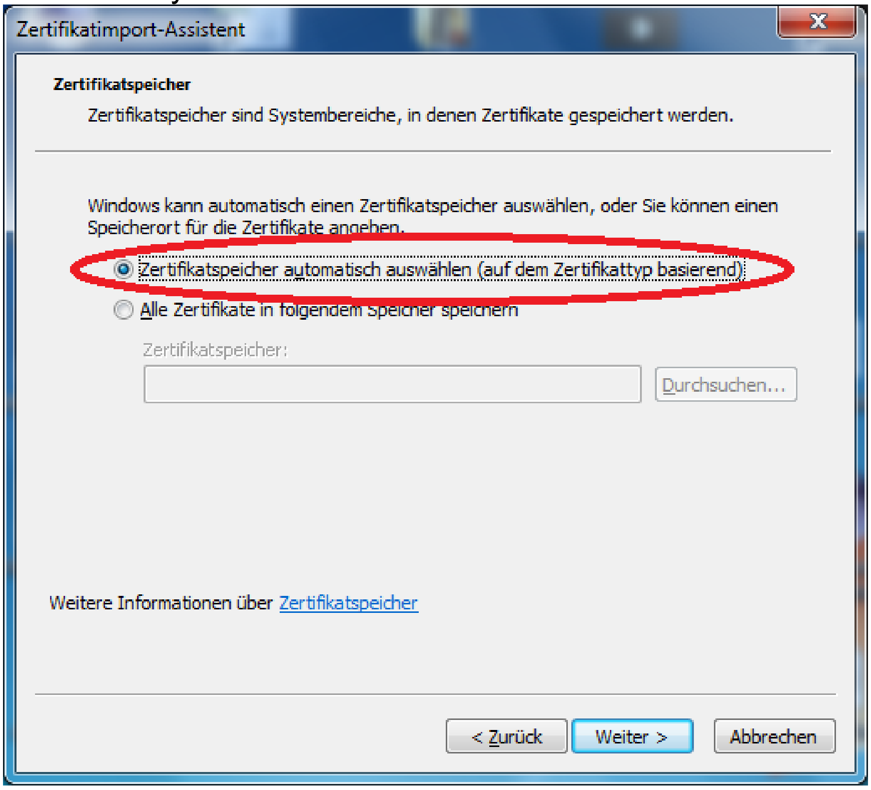
Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und -sperrlisten vom Datenträger in den Zertifikatspeicher.

Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

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



Zertifikatimport-Assistent

Zertifikatspeicher

Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

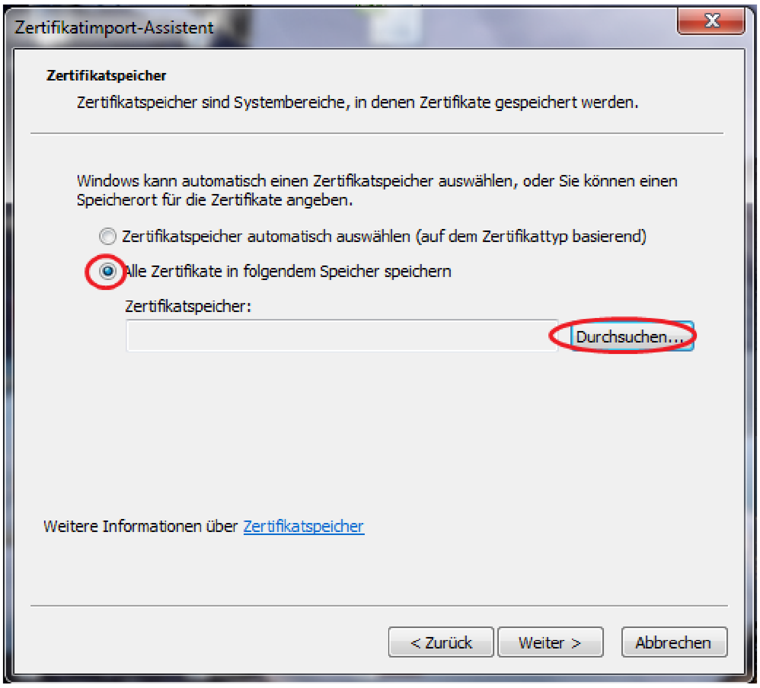
● Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)

○ Alle Zertifikate in folgendem Speicher speichern

Zertifikatspeicher:

Weitere Informationen über Zertifikatspeicher

Otherwise select “Place all certificates in the following store” and click “Search”



Zertifikatimport-Assistent

Zertifikatspeicher

Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

○ Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)

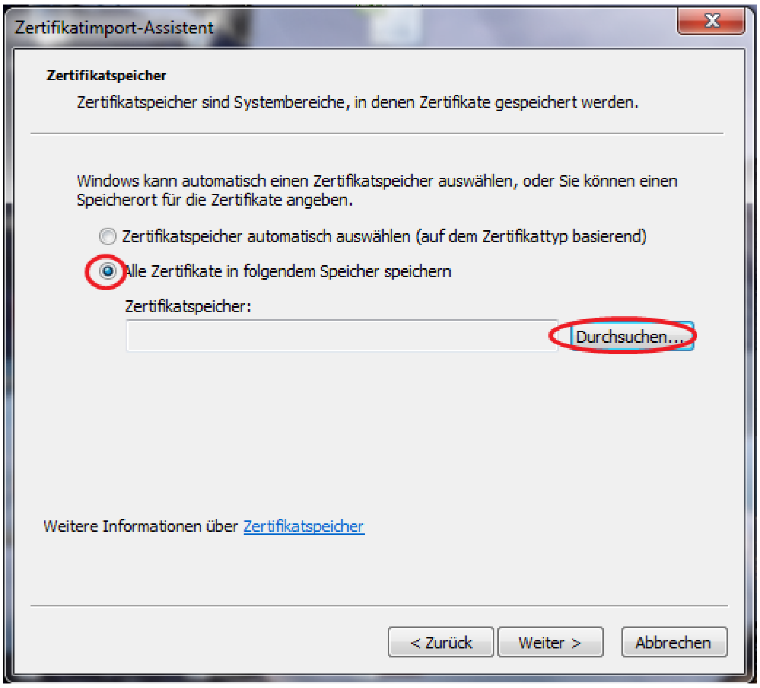
● Alle Zertifikate in folgendem Speicher speichern

Zertifikatspeicher:

Weitere Informationen über Zertifikatspeicher

Then you 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.



Zertifikatimport-Assistent

Zertifikatspeicher

Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

○ Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)

● Alle Zertifikate in folgendem Speicher speichern

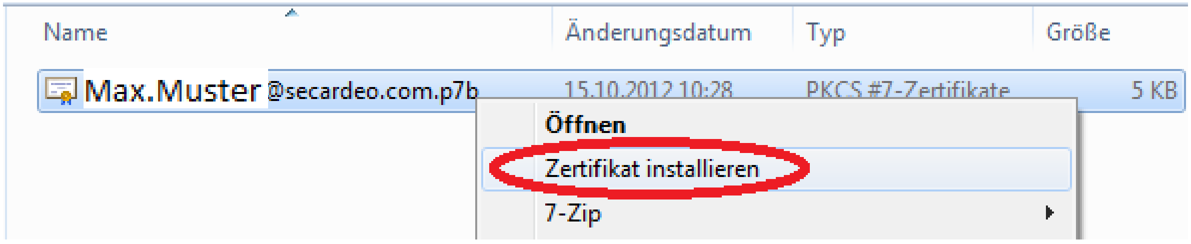
Zertifikatspeicher:

Weitere Informationen über Zertifikatspeicher

Now click „Next“ and then “Finish“.

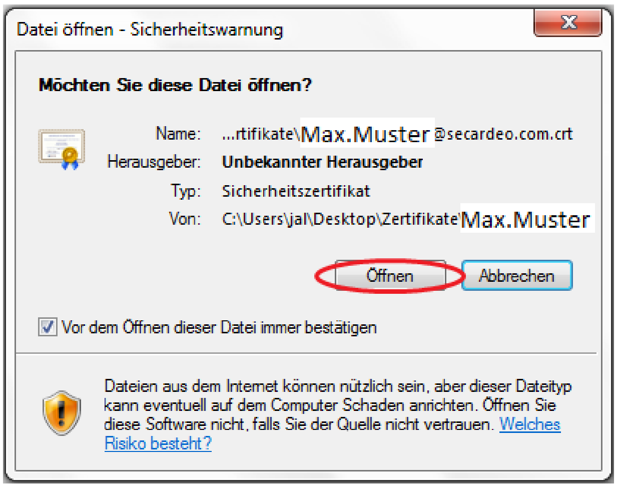
3.2 Import of a certificate chain

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



Name	Änderungsdatum	Typ	Größe
Max.Muster @secardeo.com.p7b	15.10.2012 10:28	PKCS #7-Zertifikate	5 KB

Then click “Open“



Datei öffnen - Sicherheitswarnung

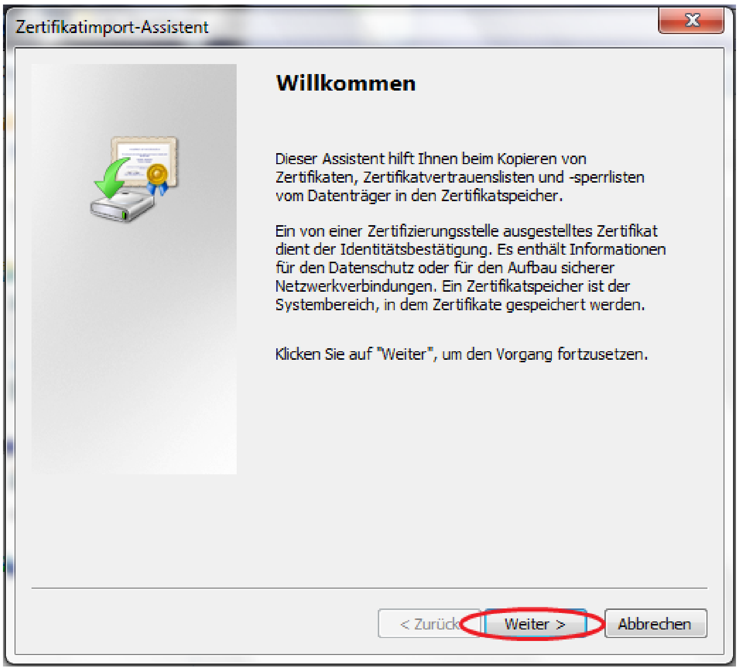
Möchten Sie diese Datei öffnen?

Name: ...rtifikate\Max.Muster @secardeo.com.crt
Herausgeber: **Unbekannter Herausgeber**
Typ: Sicherheitszertifikat
Von: C:\Users\jal\Desktop\Zertifikate\Max.Muster

☑ Vor dem Öffnen dieser Datei immer bestätigen

Dateien aus dem Internet können nützlich sein, aber dieser Dateityp kann eventuell auf dem Computer Schaden anrichten. Öffnen Sie diese Software nicht, falls Sie der Quelle nicht vertrauen. Welches Risiko besteht?

Now click “Next“



Zertifikatimport-Assistent

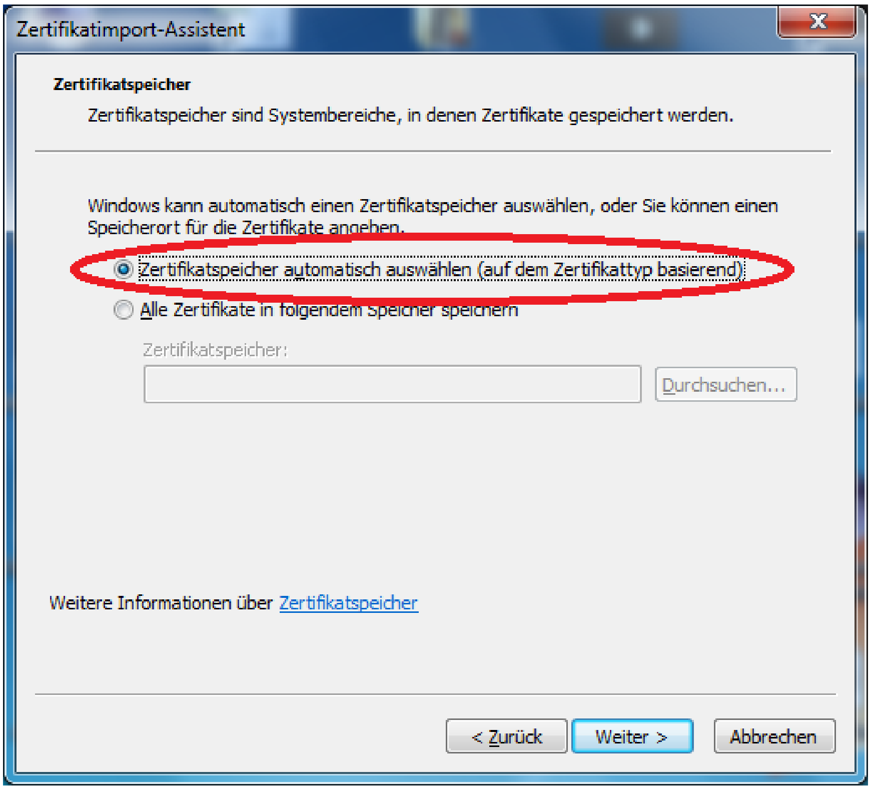
Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und -sperrlisten vom Datenträger in den Zertifikatspeicher.

Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

Now select “Choose Certificate store automatically(…)“



Zertifikatimport-Assistent

Zertifikatspeicher

Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

● Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)

○ Alle Zertifikate in folgendem Speicher speichern

Zertifikatspeicher:

Weitere Informationen über Zertifikatspeicher

Now click „Next“ and then “Finish“.

3.3 Download and import of the Certificate-trust-list

You can find the trust list via the link “CAs“. Here you can download the trust list in the desired format

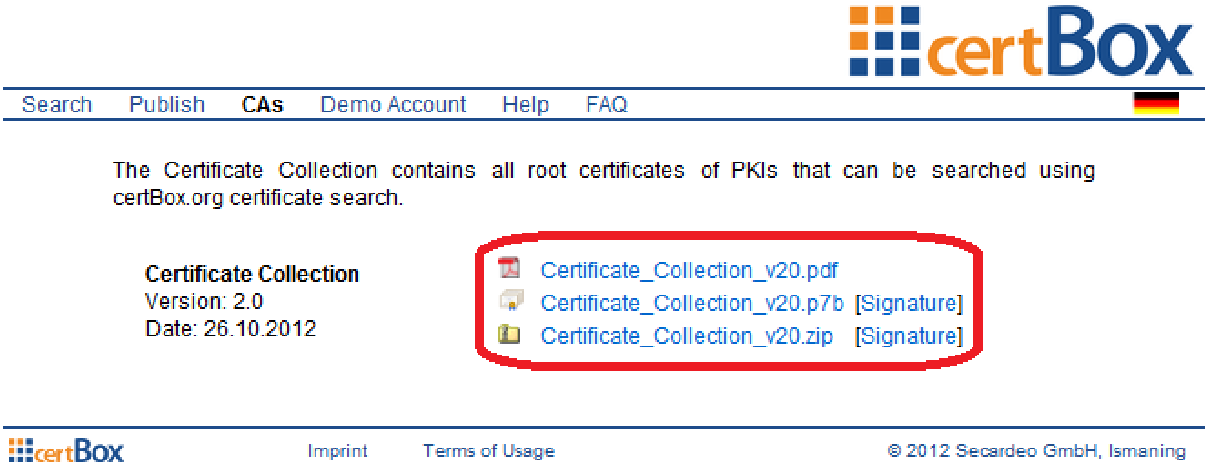
The Certificate Collection contains X.509 root certificates that can be used for validating X.509 user certificates found on certBox.org.

If you use digital certificates, your client application builds a certificate chain that has to end with a trust anchor, which is normally a root certificate.

For this, a client application will use a certificate trust list (CTL). The CTL can be provided by the operating system (for any application) or by the application itself. This Certificate Collection can be used for importing root certificates to your CTL. In the following chapters you will find a description how to to import these certificates.

Legal Notice:

Secardeo will not assume any warranty or liability for the correctness, validity or trustworthiness of the data maintained in the Certificate Collection. The decision about trusting these certificates has to be done by the person who is responsible for the CTL that will import the certificates.



The Certificate Collection contains all root certificates of PKIs that can be searched using certBox.org certificate search.

Certificate Collection
Version: 2.0
Date: 26.10.2012

Certificate_Collection_v20.pdf
Certificate_Collection_v20.p7b [Signature]
Certificate_Collection_v20.zip [Signature]

The Certificate Collection is available in the following formats:

PDF:

> In the PDF all certificates are listed in a table. The certificates are additionally added as an attachment. Should you, for example, looking for a particular root certificate by its applicant, you can use the text search. The associated file name is specified in the corresponding entry.

p7b(PKCS#7-Container):

> The p7b file contains all the certificates. You can import this container completely with one import operation.

zip:

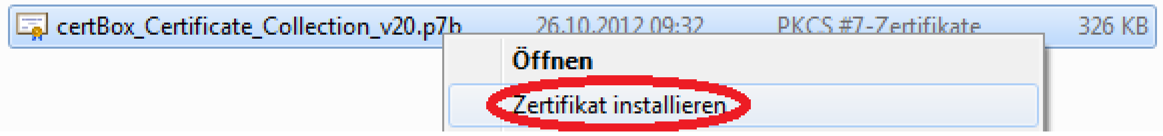
> The zip file also contains all certificates, but you can extract individual certificates. Use this download if you want to install only certain root certificates.

For the p7b and zip files, there is also a PKCS#7 signature for download. You can check these as described in Section 3.3.3.

Since the PDF has an embedded signature it is not necessary to provide a separate signature.

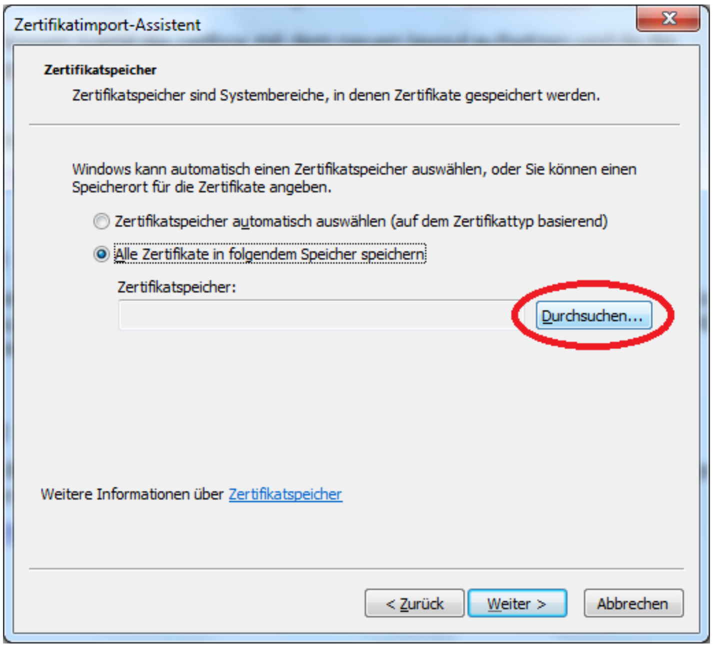
3.3.1 Import of the p7b file

Right click on the downloaded p7b file and click on “Install certificate”.



certBox_Certificate_Collection_v20.p7b 26.10.2012 09:32 PKCS #7-Zertifikate 326 KB

The “Certificate import assistant” is opening. Click on “Next” and select „Place all certificates in the following store“. Now click on “Search…”



Zertifikatimport-Assistent

Zertifikatspeicher

Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

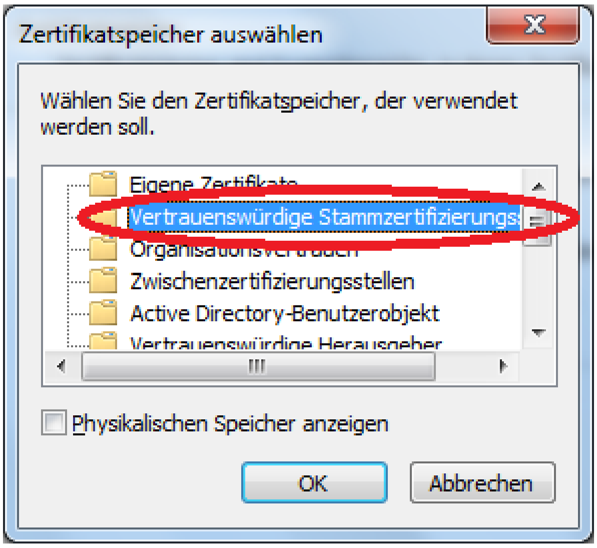
○ Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)

● Alle Zertifikate in folgendem Speicher speichern

Zertifikatspeicher:

Weitere Informationen über Zertifikatspeicher

Select “Trusted CAs“ and click “OK“.



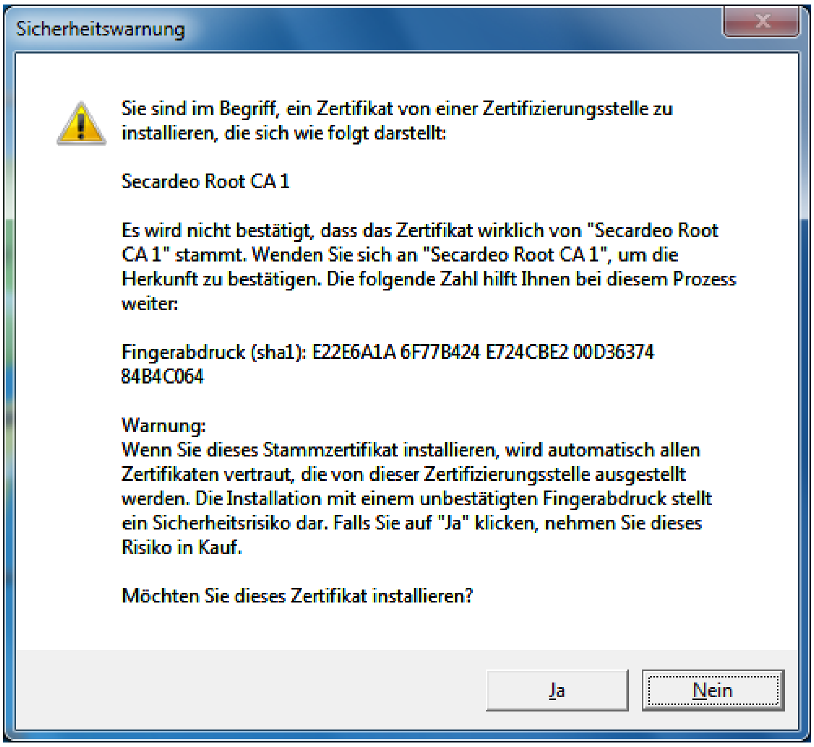
Zertifikatspeicher auswählen

Wählen Sie den Zertifikatspeicher, der verwendet werden soll.

Eigene Zertifikate
Vertrauenswürdige Stammzertifizierungs
Organisationsvertrauen
Zwischenzertifizierungsstellen
Active Directory-Benutzerobjekt
Vertrauenswürdige Herausgeber

□ Physikalischen Speicher anzeigen

Click on “Next” and then on “Finish”. This process may take a few minutes to complete. During this time notifications like this can appear:



Sicherheitswarnung

Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:

Secardeo Root CA 1

Es wird nicht bestätigt, dass das Zertifikat wirklich von "Secardeo Root CA 1" stammt. Wenden Sie sich an "Secardeo Root CA 1", um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:

Fingerabdruck (sha1): E22E6A1A 6F77B424 E724CBE2 00D36374 84B4C064

Warnung:
Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.

Möchten Sie dieses Zertifikat installieren?

Confirm these with “Yes”.

3.3.2 Distribute using Group Policies (for administrators)

To distribute the downloaded p7b file as a domain administrator via Group Policies for a Windows domain and thus make it available for all Windows systems, please follow these instructions:

http://technet.microsoft.com/en-us/library/cc772491(v=ws.10).aspx

3.3.3 Verifying the p7s signatures

The signatures can be verified with "openssl" or other signature tools.

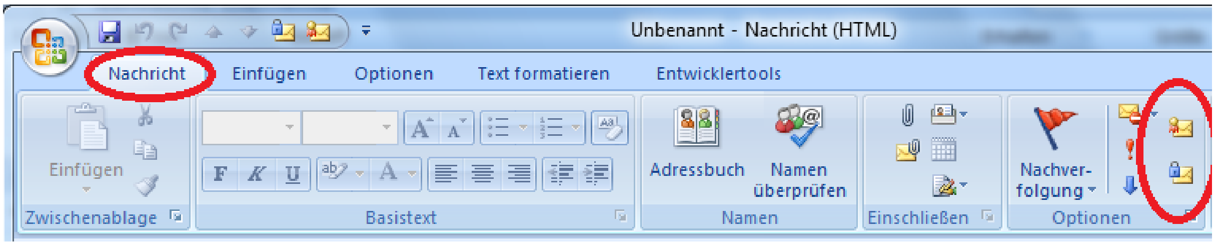
(http://www.openssl.org/related/binaries.html).

The embedded PDF signature can be verified using Adobe Reader.

4 Outlook 2010

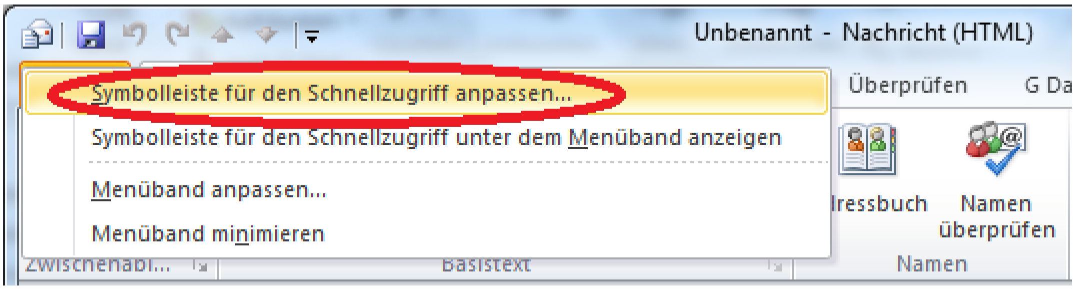
4.1 Encrypt an e-mail

To encrypt or sign without the help of the Quick Access toolbar, you can also find the buttons under the tab "Message" and then “Options".

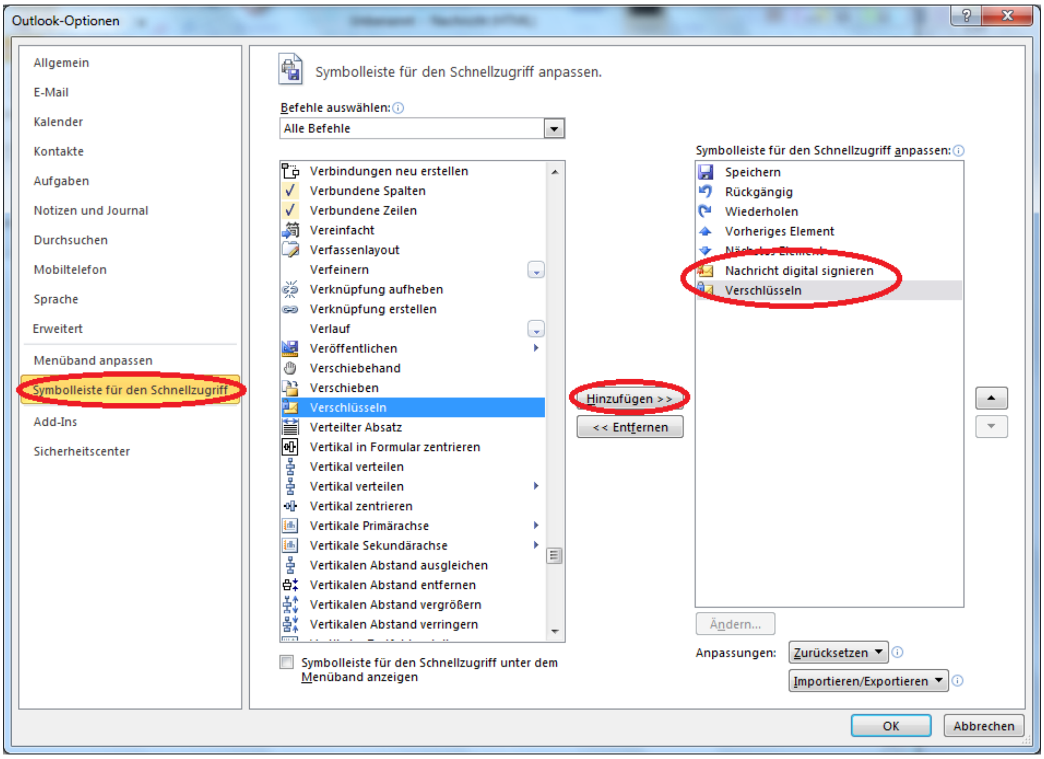


4.1.1 Customize the Quick Access Toolbar

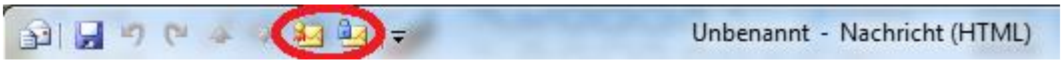
Create a new e-mail. Right click on “File” and then click on “Customize the Quick Access Toolbar…”


Unbenannt - Nachricht (HTML)
Symbolleiste für den Schnellzugriff anpassen...
Symbolleiste für den Schnellzugriff unter dem Menüband anzeigen
Menüband anpassen...
Menüband minimieren
Überprüfen
G Da
lressbuch
Namen überprüfen
Namen
Zwischenabl...
Basistext

On the left side select “All commands” and add “Sign message“ and “Encrypt“. Then click “OK”.



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

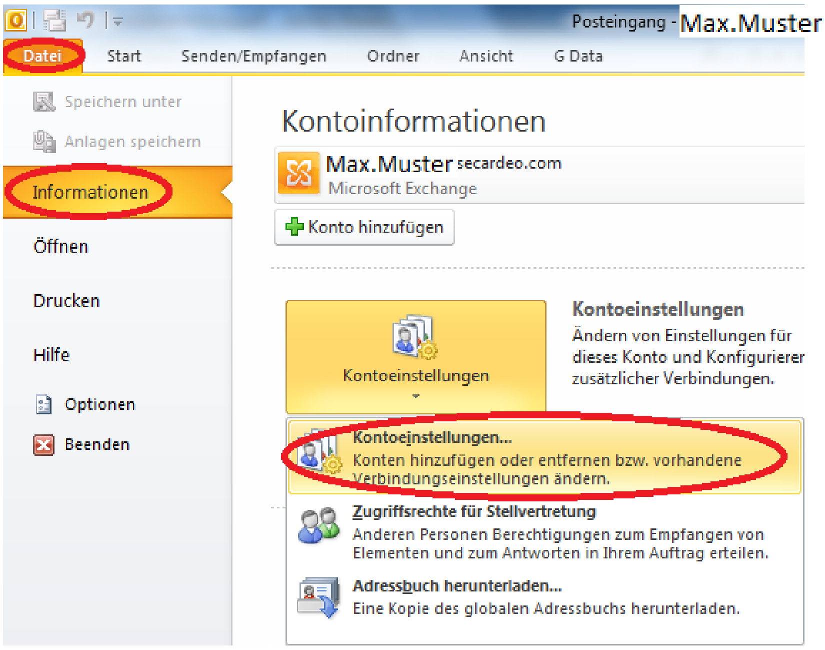


Whenever you write an e-mail in the future you can sign and encrypt it with these symbols.

4.2 LDAP-configuration for the 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



Kontoinformationen

Max.Muster secardeo.com
Microsoft Exchange

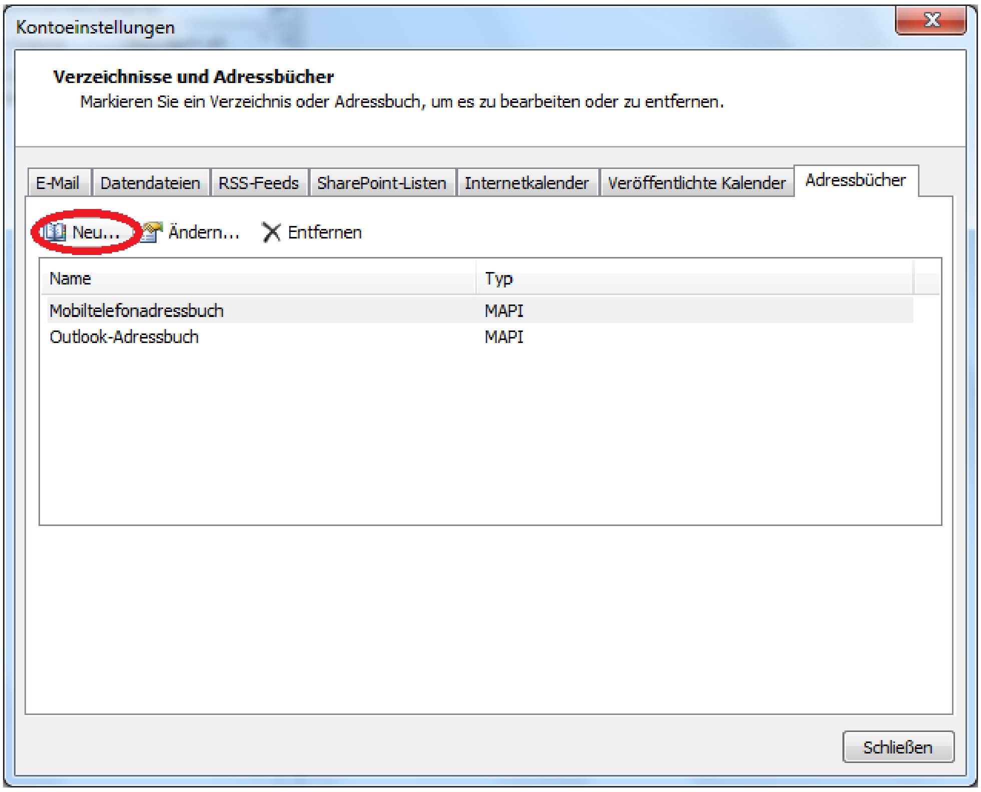
Kontoeinstellungen
Ändern von Einstellungen für dieses Konto und Konfigurierer zusätzlicher Verbindungen.

Kontoeinstellungen...
Konten hinzufügen oder entfernen bzw. vorhandene Verbindungseinstellungen ändern.

Zugriffsrechte für Stellvertretung
Anderen Personen Berechtigungen zum Empfangen von Elementen und zum Antworten in Ihrem Auftrag erteilen.

Adressbuch herunterladen...
Eine Kopie des globalen Adressbuchs herunterladen.

Click on "Address books" and select "New"



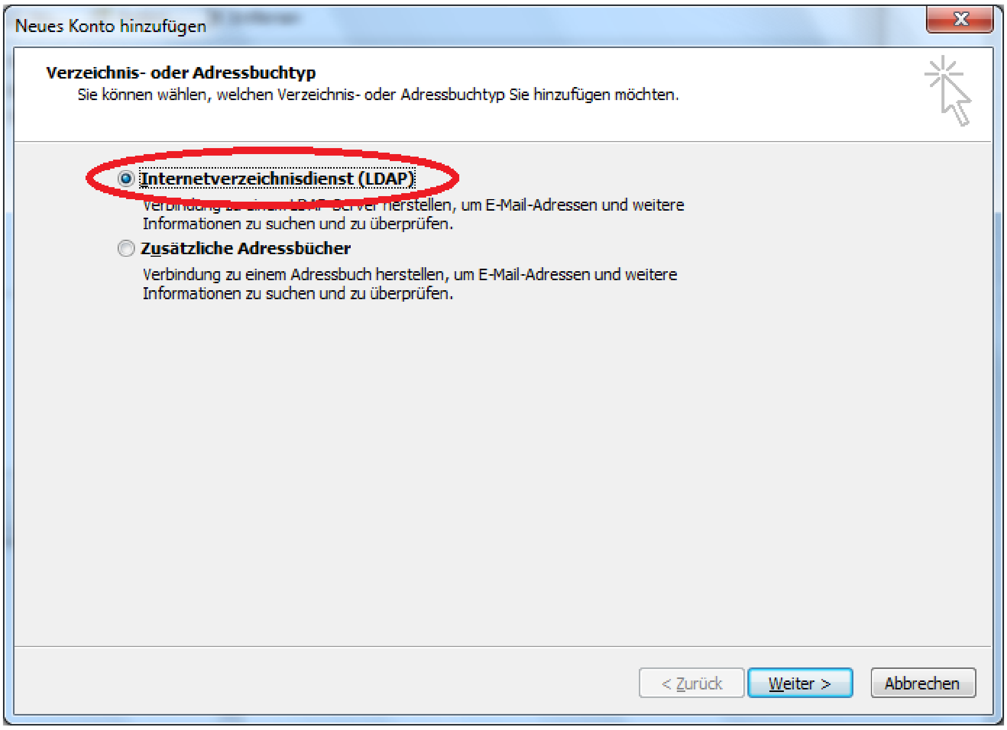
Kontoeinstellungen

Verzeichnisse und Adressbücher

Markieren Sie ein Verzeichnis oder Adressbuch, um es zu bearbeiten oder zu entfernen.

Name	Typ
Mobiltelefonadressbuch	MAPI
Outlook-Adressbuch	MAPI

There you select “Internet directory service (LDAP)” and click “Next”



Neues Konto hinzufügen

Verzeichnis- oder Adressbuchtyp

Sie können wählen, welchen Verzeichnis- oder Adressbuchtyp Sie hinzufügen möchten.

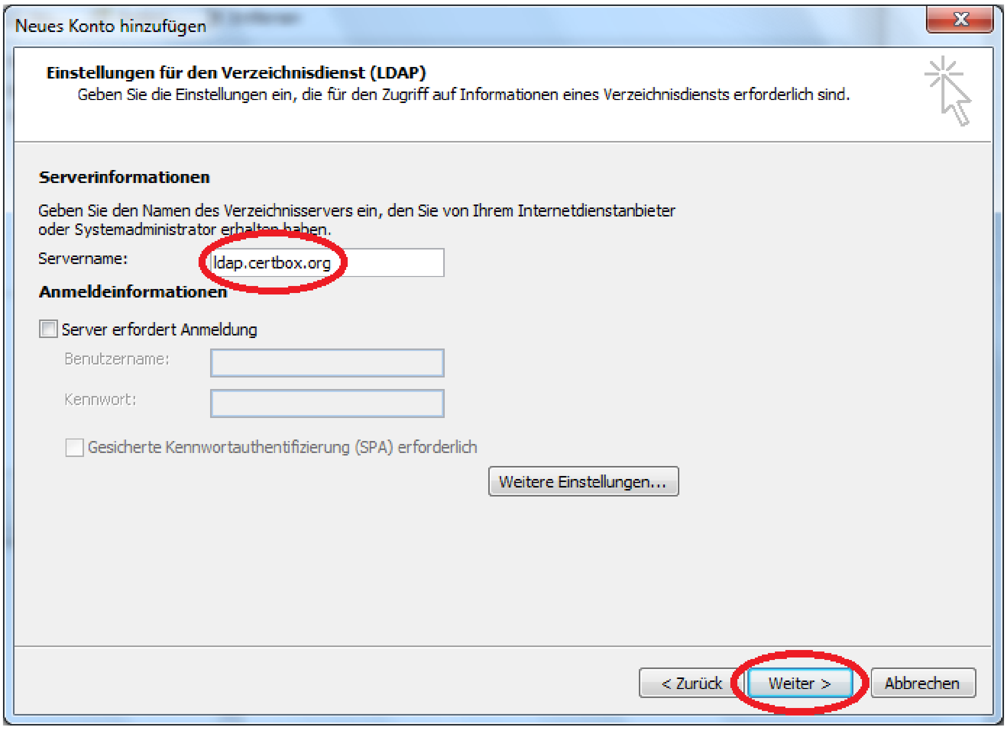
● **Internetverzeichnisdienst (LDAP)**

Verbindung zu einem LDAP-Server herstellen, um E-Mail-Adressen und weitere Informationen zu suchen und zu überprüfen.

○ **Zusätzliche Adressbücher**

Verbindung zu einem Adressbuch herstellen, um E-Mail-Adressen und weitere Informationen zu suchen und zu überprüfen.

Afterwards you enter “ldap.certbox.org” for the server name



Neues Konto hinzufügen

Einstellungen für den Verzeichnisdienst (LDAP)
Geben Sie die Einstellungen ein, die für den Zugriff auf Informationen eines Verzeichnisdiensts erforderlich sind.

Serverinformationen

Geben Sie den Namen des Verzeichnisservers ein, den Sie von Ihrem Internetdienstanbieter oder Systemadministrator erhalten haben.

Servername: ldap.certbox.org

Anmeldeinformationen

□ Server erfordert Anmeldung

Benutzername:

Kennwort:

□ Gesicherte Kennwortauthentifizierung (SPA) erforderlich

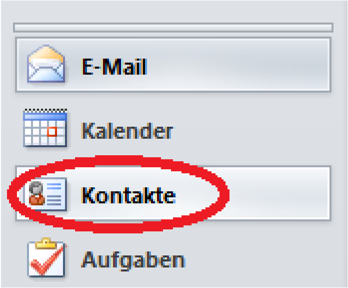
Now click “Next“ and then “Finish”.

4.3 Import of certificates in the Outlook Contacts

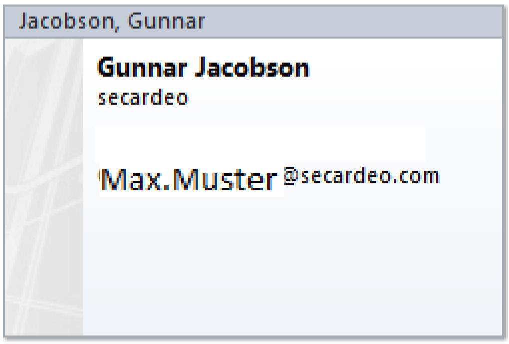
4.3.1 Add certificate to an existing contact

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

For the import, click on “Contacts”



Double click the contact of your choice.

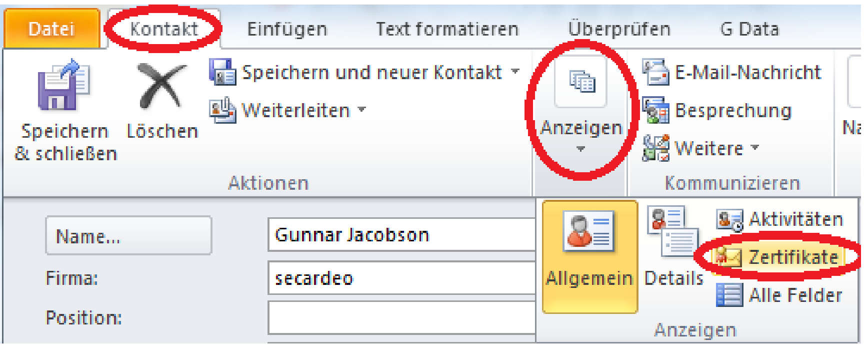


Jacobson, Gunnar

Gunnar Jacobson
secardeo

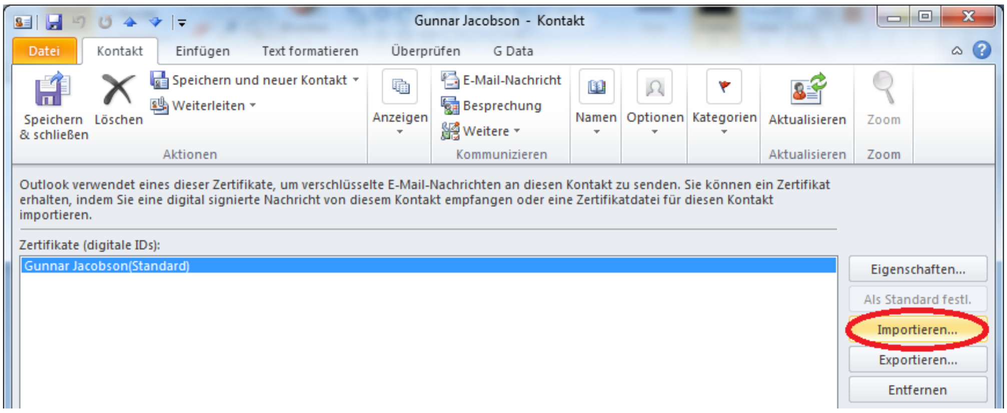
Max.Muster@secardeo.com

Click then on “Contact” and the little arrow below “Show”. Here click on “Certificates”.



Name... Gunnar Jacobson
Firma: secardeo
Position:

Now import the previously downloaded certificate via the “Import“-button.



Outlook verwendet eines dieser Zertifikate, um verschlüsselte E-Mail-Nachrichten an diesen Kontakt zu senden. Sie können ein Zertifikat erhalten, indem Sie eine digital signierte Nachricht von diesem Kontakt empfangen oder eine Zertifikatdatei für diesen Kontakt importieren.

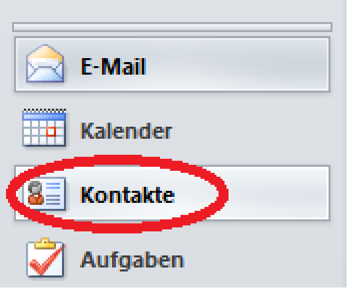
Zertifikate (digitale IDs):

Gunnar Jacobson(Standard)

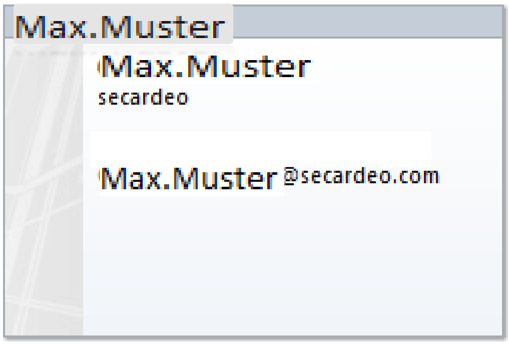
If you don’t have the root certificate, you can also use the "Properties" button to explicitly trust the certificate (This is necessary in order to encrypt).

4.3.2 Add certificate chain to an existing contact

For the import click on “Contacts”

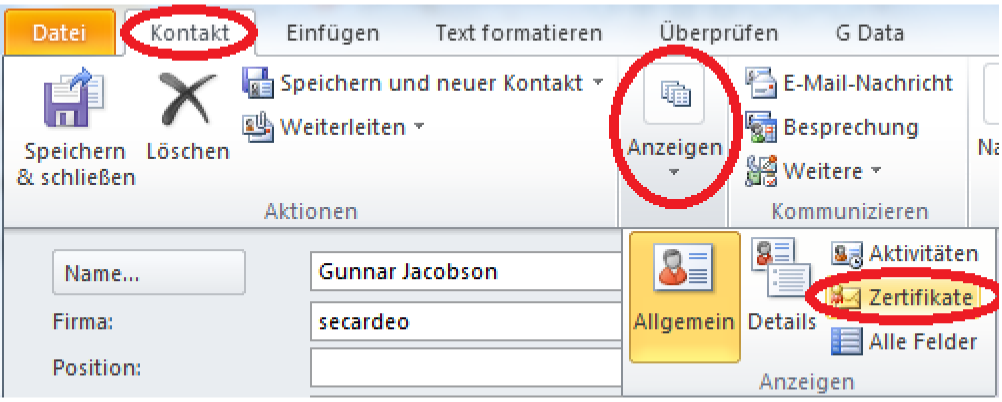


Double click the contact of your choice.



Max.Muster
Max.Muster
secardeo
Max.Muster @secardeo.com

Click then on “Contact” and the little arrow below “Show”. Here click on “Certificates”.

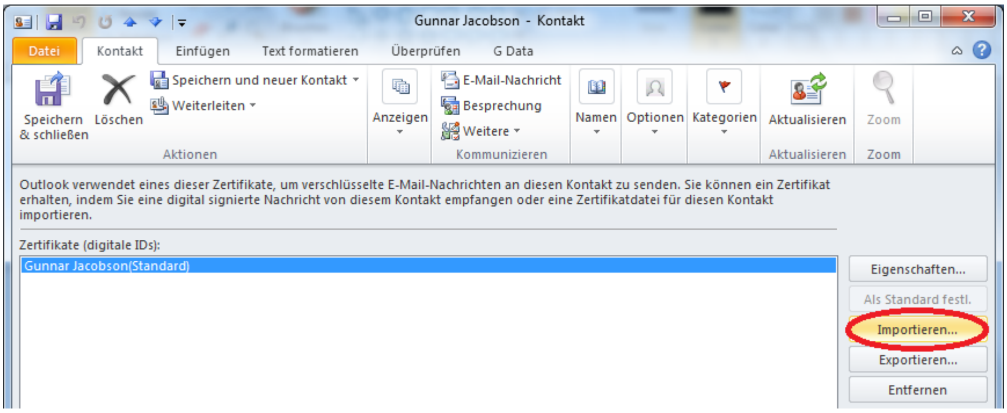


Name... Gunnar Jacobson

Firma: secardeo

Position:

Now import the previously downloaded certificate via the “Import“-button. Maybe you have to select “All files” in the dialog in order to see the file.



Outlook verwendet eines dieser Zertifikate, um verschlüsselte E-Mail-Nachrichten an diesen Kontakt zu senden. Sie können ein Zertifikat erhalten, indem Sie eine digital signierte Nachricht von diesem Kontakt empfangen oder eine Zertifikatdatei für diesen Kontakt importieren.

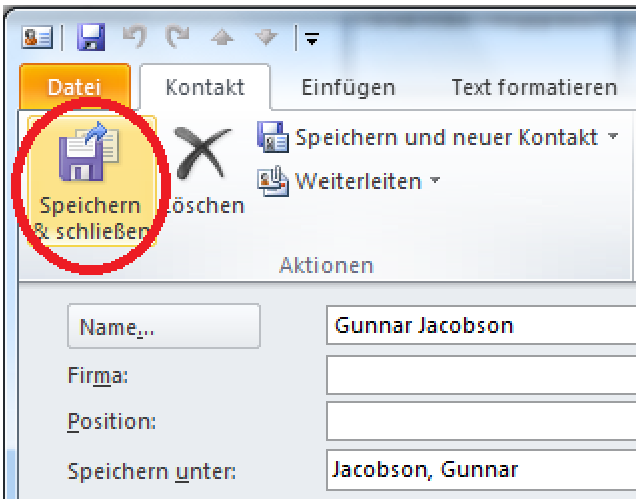
Zertifikate (digitale IDs):

Gunnar Jacobson(Standard)

4.3.3 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 & Quit“



Name... Gunnar Jacobson

Firma:

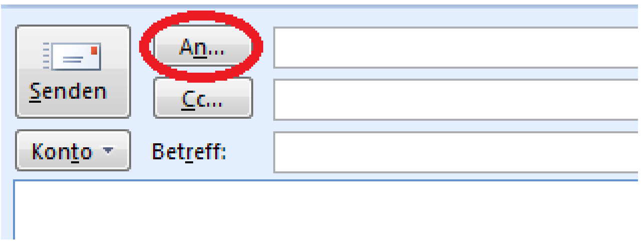
Position:

Speichern unter: Jacobson, Gunnar

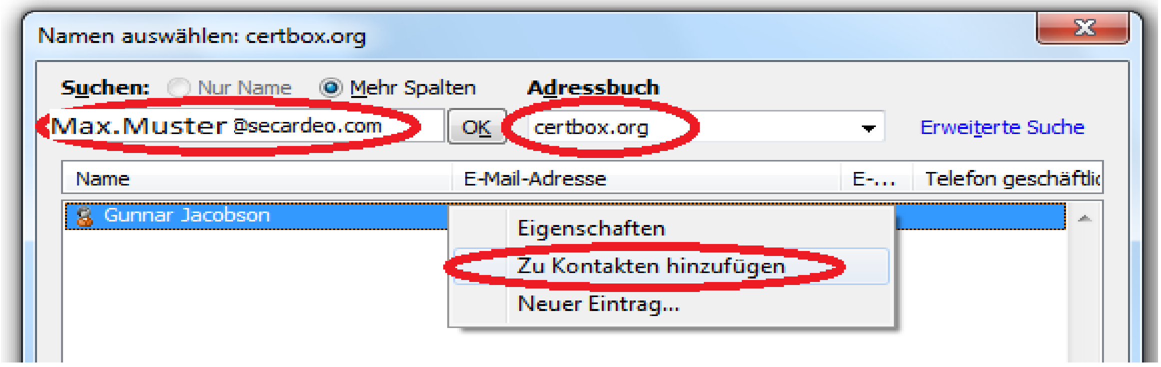
If you don’t have a fitting root certificate you can also explicitly trust the certificate as described at the end of chapter 4.3.1.

4.3.4 Create new contacts with the address book search

Create a new e-mail and click on “To…“



Enter the desired e-mail address and choose “certBox.org” as address book. Then right click on the contact and click “add to contacts”.


Namen auswählen: certbox.org

Suchen: ○ Nur Name ● Mehr Spalten

Max.Muster @secardeo.com

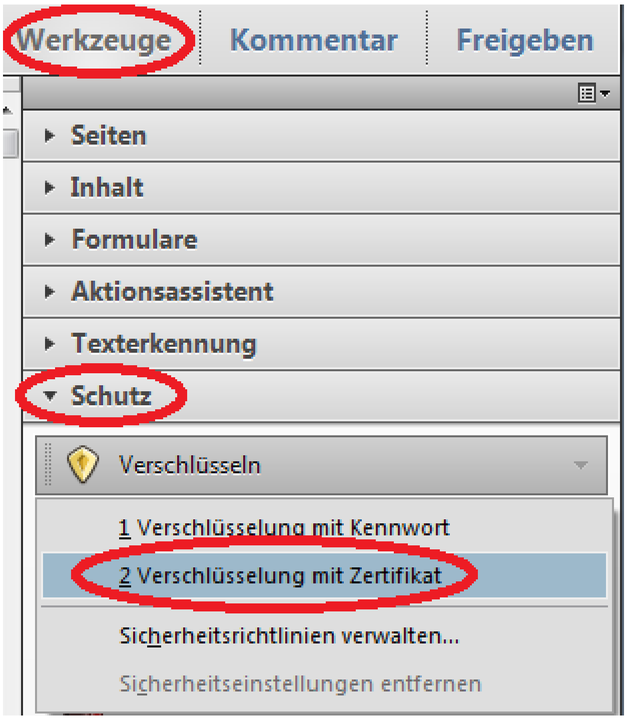
Adressbuch: certbox.org

Name	E-Mail-Adresse	E-...	Telefon geschäftlic
Gunnar Jacobson			

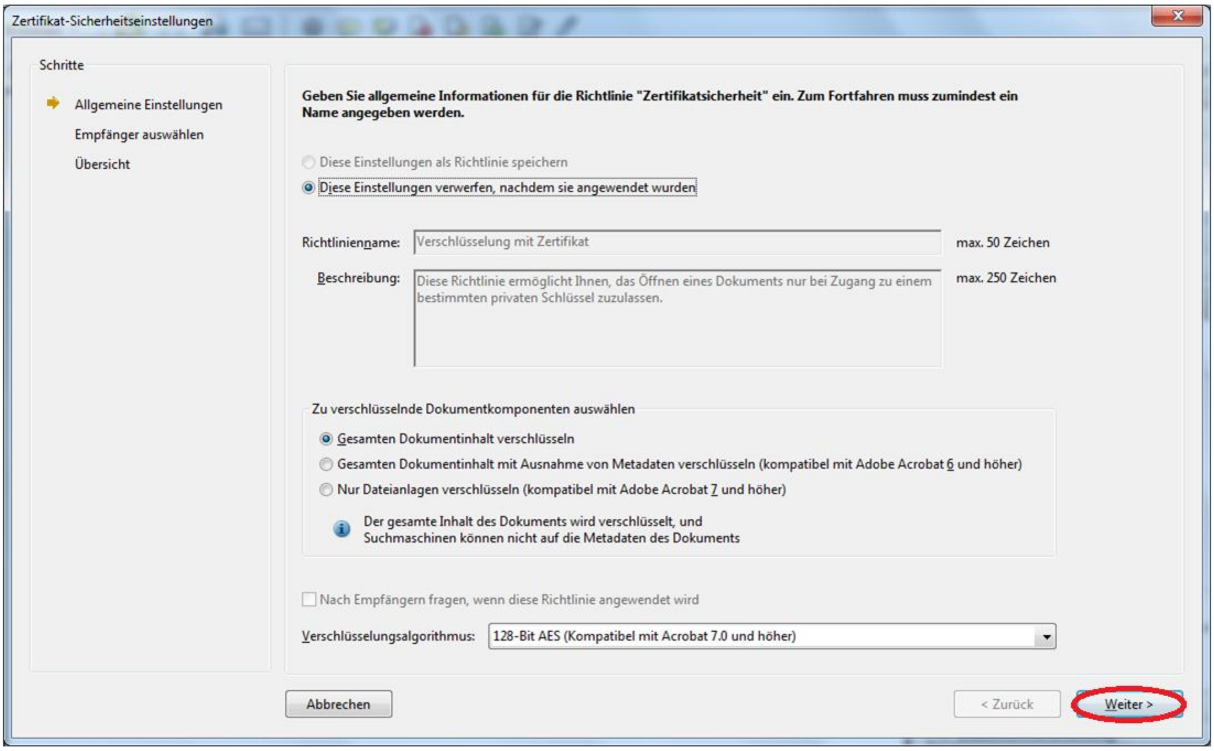
5 Adobe Acrobat X

5.1 Encrypt a document

Navigate to “Encrypt with certificate“


Werkzeuge
Kommentar
Freigeben
Seiten
Inhalt
Formulare
Aktionsassistent
Texterkennung
Schutz
Verschlüsseln
1 Verschlüsselung mit Kennwort
2 Verschlüsselung mit Zertifikat
Sicherheitsrichtlinien verwalten...
Sicherheitseinstellungen entfernen

Make your default settings and click “Next“



Geben Sie allgemeine Informationen für die Richtlinie "Zertifikatsicherheit" ein. Zum Fortfahren muss zumindest ein Name angegeben werden.

○ Diese Einstellungen als Richtlinie speichern

● Diese Einstellungen verwerfen, nachdem sie angewendet wurden

Richtlinienname: Verschlüsselung mit Zertifikat max. 50 Zeichen

Beschreibung: Diese Richtlinie ermöglicht Ihnen, das Öffnen eines Dokuments nur bei Zugang zu einem bestimmten privaten Schlüssel zuzulassen. max. 250 Zeichen

Zu verschlüsselnde Dokumentkomponenten auswählen

● Gesamten Dokumentinhalt verschlüsseln

○ Gesamten Dokumentinhalt mit Ausnahme von Metadaten verschlüsseln (kompatibel mit Adobe Acrobat 6 und höher)

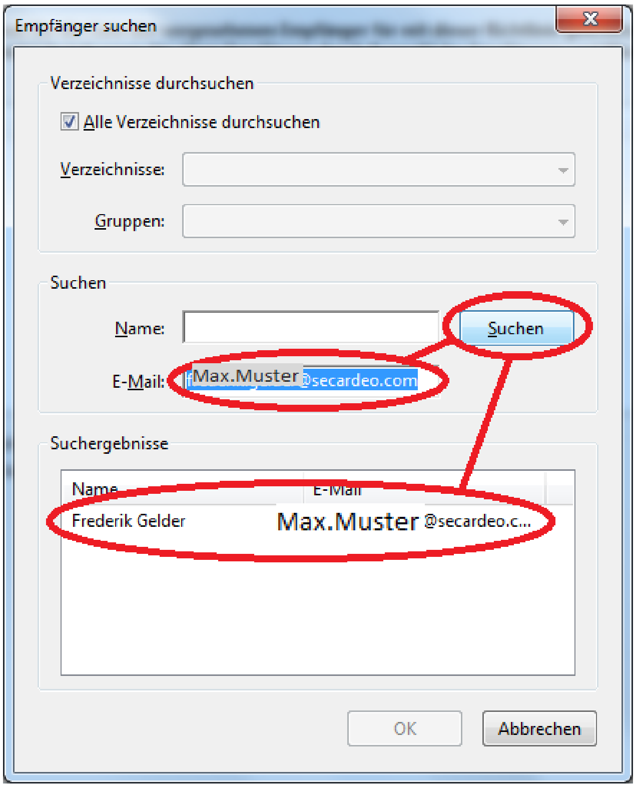
○ Nur Dateianlagen verschlüsseln (kompatibel mit Adobe Acrobat 7 und höher)

Der gesamte Inhalt des Dokuments wird verschlüsselt, und Suchmaschinen können nicht auf die Metadaten des Dokuments

□ Nach Empfängern fragen, wenn diese Richtlinie angewendet wird

Verschlüsselungsalgorithmus: 128-Bit AES (Kompatibel mit Acrobat 7.0 und höher)

A dialog pops up. Close this until you are back at the window “Certificate security preferences“. Manually search for the recipient. In order to do so, enter his e-mail and click on “Search”. The recipient should appear in the search results.



☑ Alle Verzeichnisse durchsuchen

Verzeichnisse:

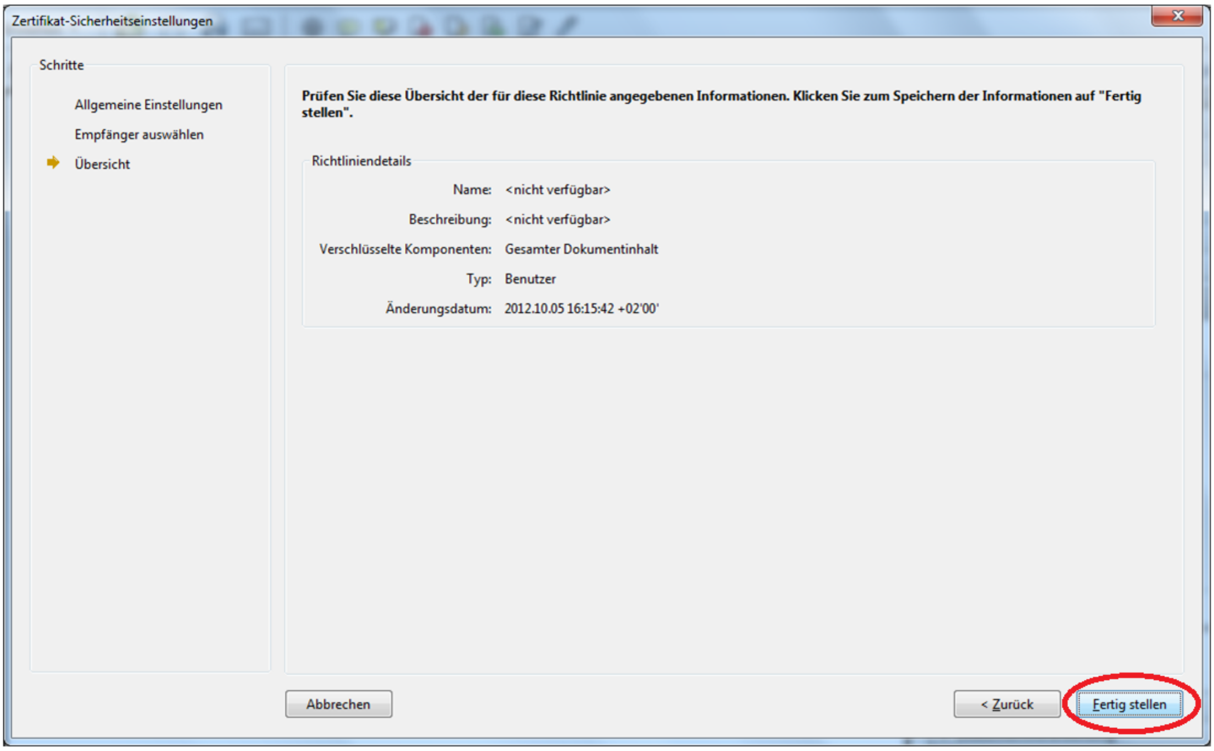
Gruppen:

Name:

E-Mail: Max.Muster@secardeo.com

Name	E-Mail
Frederik Gelder	Max.Muster @secardeo.c...

Select the correct result and click “OK“. Click “Next” and then “Finish”



Prüfen Sie diese Übersicht der für diese Richtlinie angegebenen Informationen. Klicken Sie zum Speichern der Informationen auf "Fertig stellen".

Name: <nicht verfügbar>

Beschreibung: <nicht verfügbar>

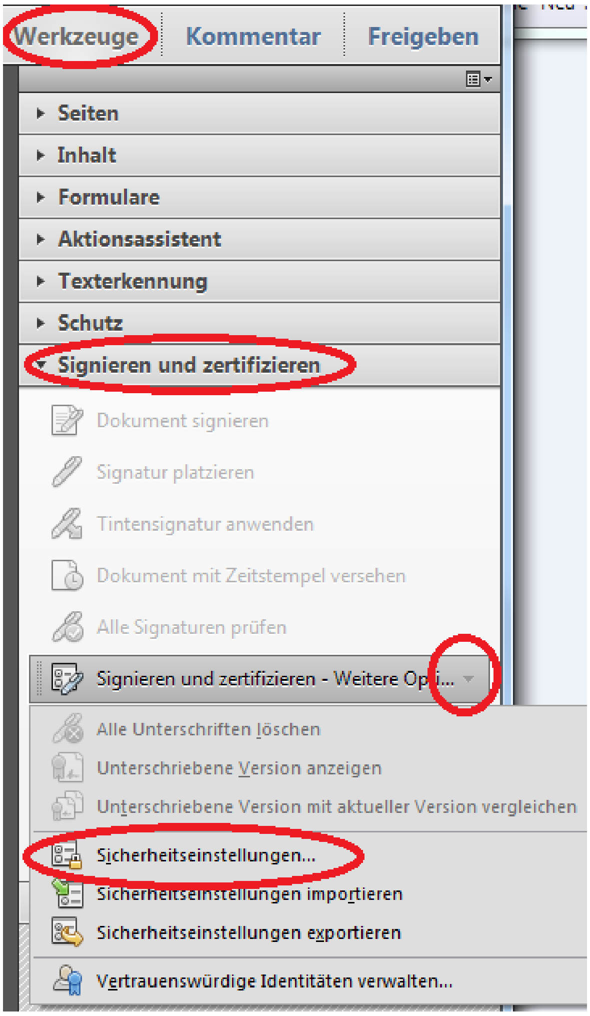
Verschlüsselte Komponenten: Gesamter Dokumentinhalt

Typ: Benutzer

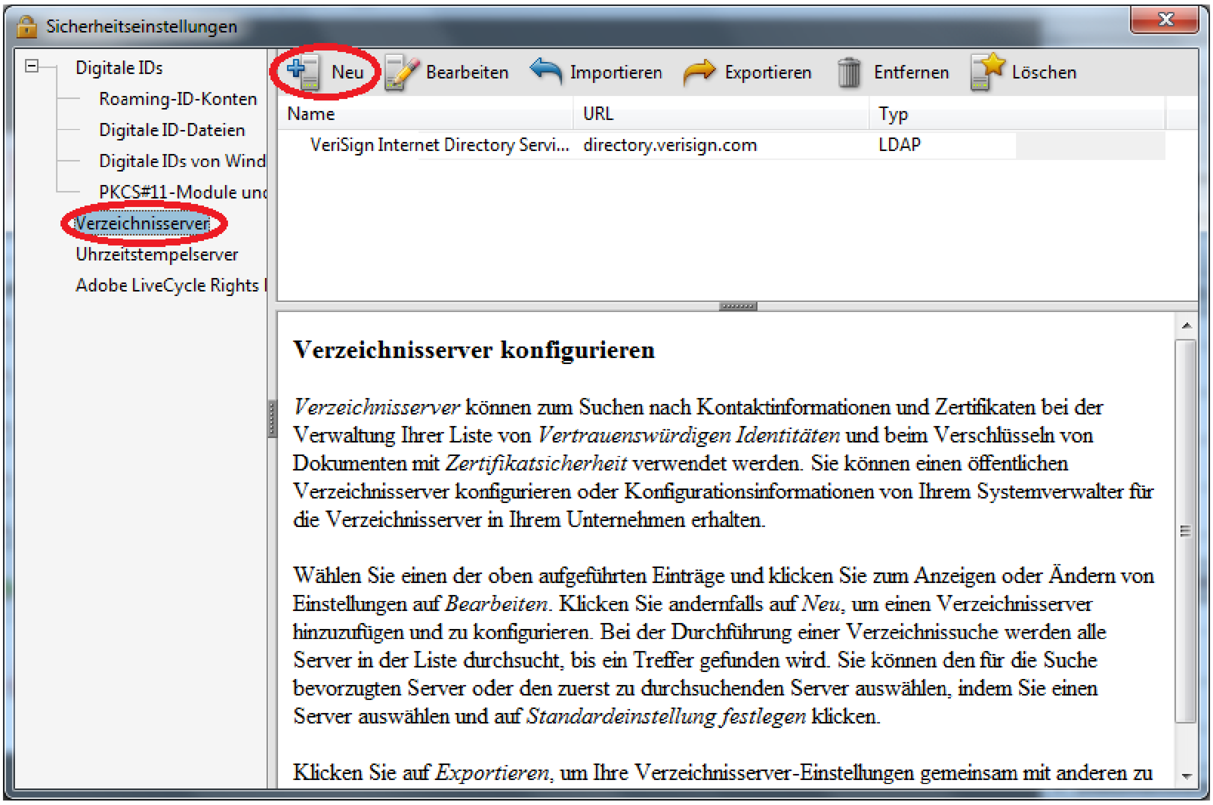
Änderungsdatum: 2012.10.05 16:15:42 +02'00'

5.2 LDAP-configuration

Navigate to the “Security preferences“.


Werkzeuge
Kommentar
Freigeben
Seiten
Inhalt
Formulare
Aktionsassistent
Texterkennung
Schutz
Signieren und zertifizieren
Dokument signieren
Signatur platzieren
Tintensignatur anwenden
Dokument mit Zeitstempel versehen
Alle Signaturen prüfen
Signieren und zertifizieren - Weitere Opti...
Alle Unterschriften löschen
Unterschriebene Version anzeigen
Unterschriebene Version mit aktueller Version vergleichen
Sicherheitseinstellungen...
Sicherheitseinstellungen importieren
Sicherheitseinstellungen exportieren
Vertrauenswürdige Identitäten verwalten...

Click on “Directory server“ and then on “New“.



Name	URL	Typ
VeriSign Internet Directory Servi...	directory.verisign.com	LDAP

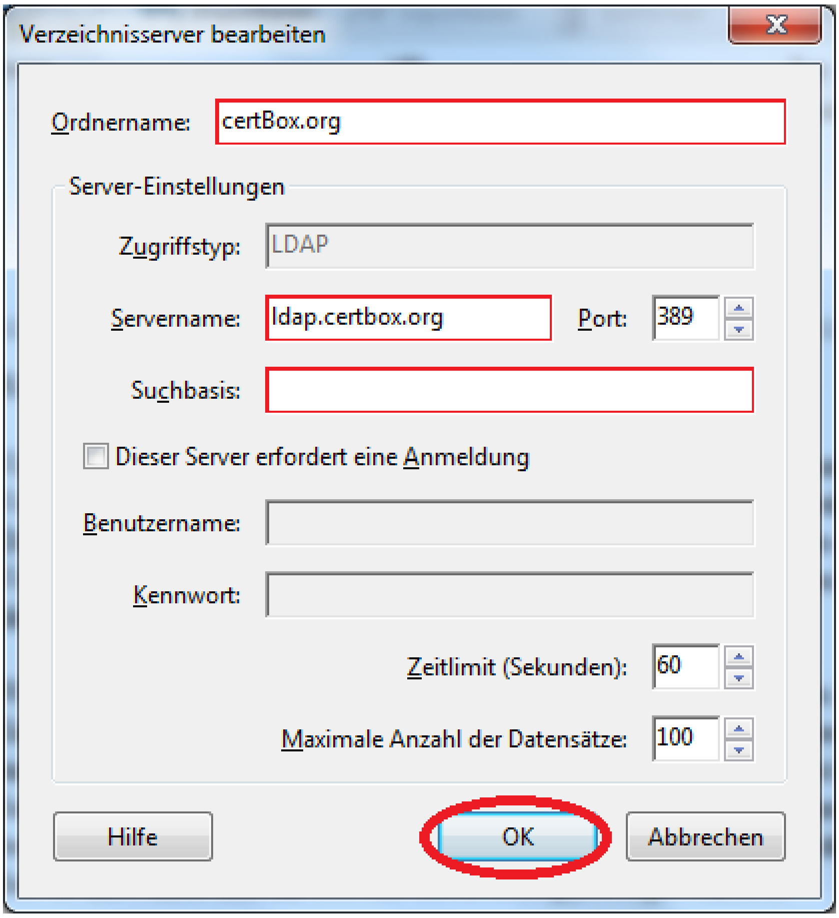
Verzeichnisserver konfigurieren

Verzeichnisserver können zum Suchen nach Kontaktinformationen und Zertifikaten bei der Verwaltung Ihrer Liste von *Vertrauenswürdigen Identitäten* und beim Verschlüsseln von Dokumenten mit *Zertifikatsicherheit* verwendet werden. Sie können einen öffentlichen Verzeichnisserver konfigurieren oder Konfigurationsinformationen von Ihrem Systemverwalter für die Verzeichnisserver in Ihrem Unternehmen erhalten.

Wählen Sie einen der oben aufgeführten Einträge und klicken Sie zum Anzeigen oder Ändern von Einstellungen auf *Bearbeiten*. Klicken Sie andernfalls auf *Neu*, um einen Verzeichnisserver hinzuzufügen und zu konfigurieren. Bei der Durchführung einer Verzeichnissuche werden alle Server in der Liste durchsucht, bis ein Treffer gefunden wird. Sie können den für die Suche bevorzugten Server oder den zuerst zu durchsuchenden Server auswählen, indem Sie einen Server auswählen und auf *Standardeinstellung festlegen* klicken.

Klicken Sie auf *Exportieren*, um Ihre Verzeichnisserver-Einstellungen gemeinsam mit anderen zu

Use “certBox.org“ as folder name and “ldap.certbox.org” as server name. The search-base stays empty. Confirm with “OK”.



Ordnername: certBox.org

Zugriffstyp: LDAP

Servername: ldap.certbox.org

Port: 389

Suchbasis:

□ Dieser Server erfordert eine Anmeldung

Benutzername:

Kennwort:

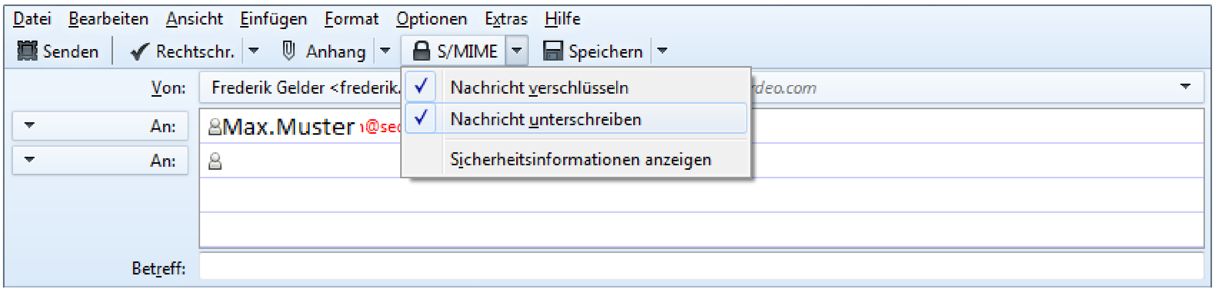
Zeitlimit (Sekunden): 60

Maximale Anzahl der Datensätze: 100

6 Mozilla Thunderbird 15

6.1 Encrypt an e-mail

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.



Von: Frederik Gelder <frederik...deo.com

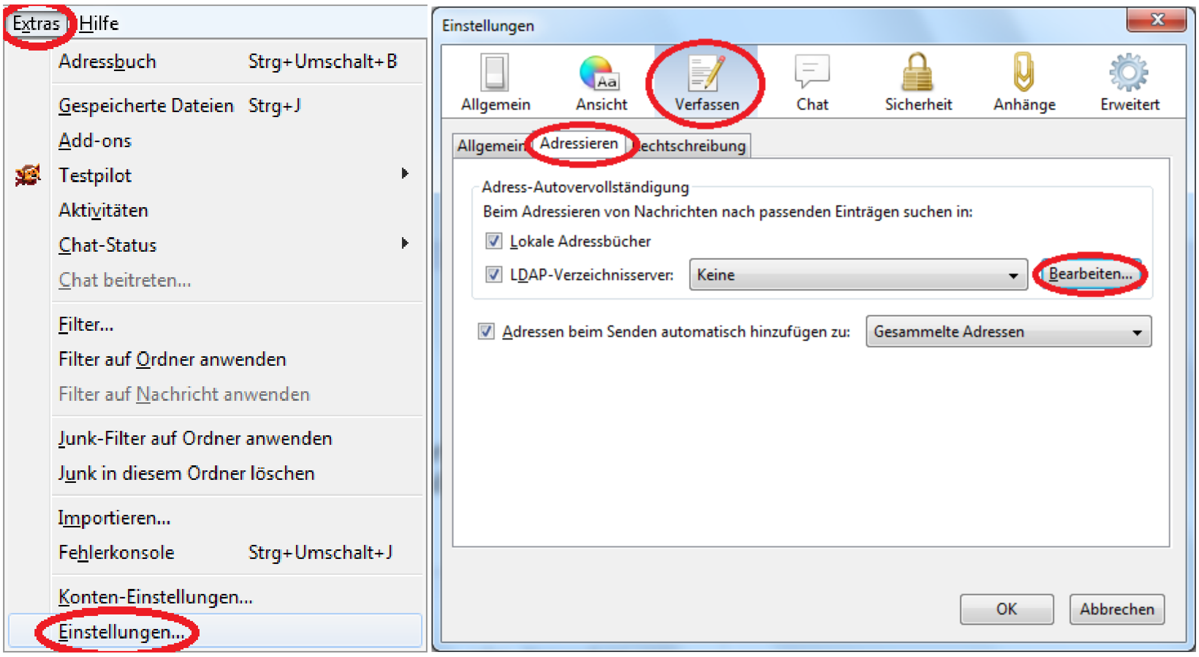
An: Max.Muster @sec...

✓ Nachricht verschlüsseln

✓ Nachricht unterschreiben

6.2 LDAP-Configuration

Click “Extras“, then “Settings“, then “Post“ and then “Addressing“



Adress-Autovervollständigung

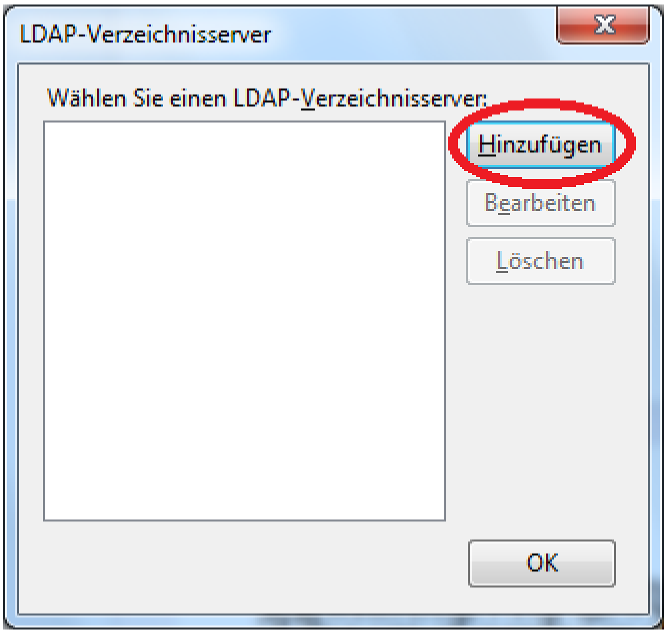
Beim Adressieren von Nachrichten nach passenden Einträgen suchen in:

☑ Lokale Adressbücher

☑ LDAP-Verzeichnisserver: Keine

☑ Adressen beim Senden automatisch hinzufügen zu: Gesammelte Adressen

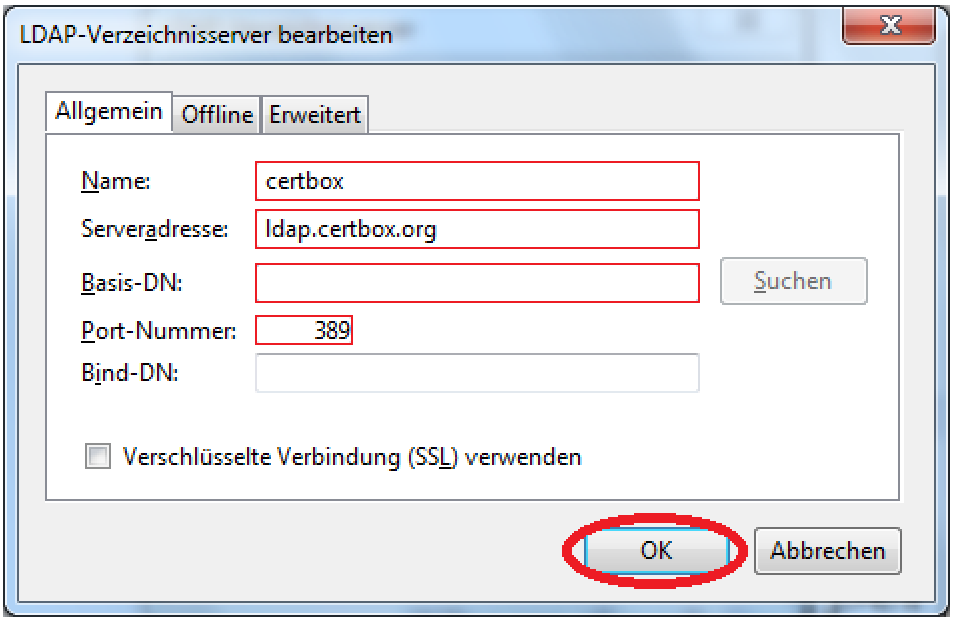
Click “Edit…“ and then “Add“



LDAP-Verzeichnisserver

Wählen Sie einen LDAP-Verzeichnisserver:

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



LDAP-Verzeichnisserver bearbeiten

Name: certbox

Serveradresse: ldap.certbox.org

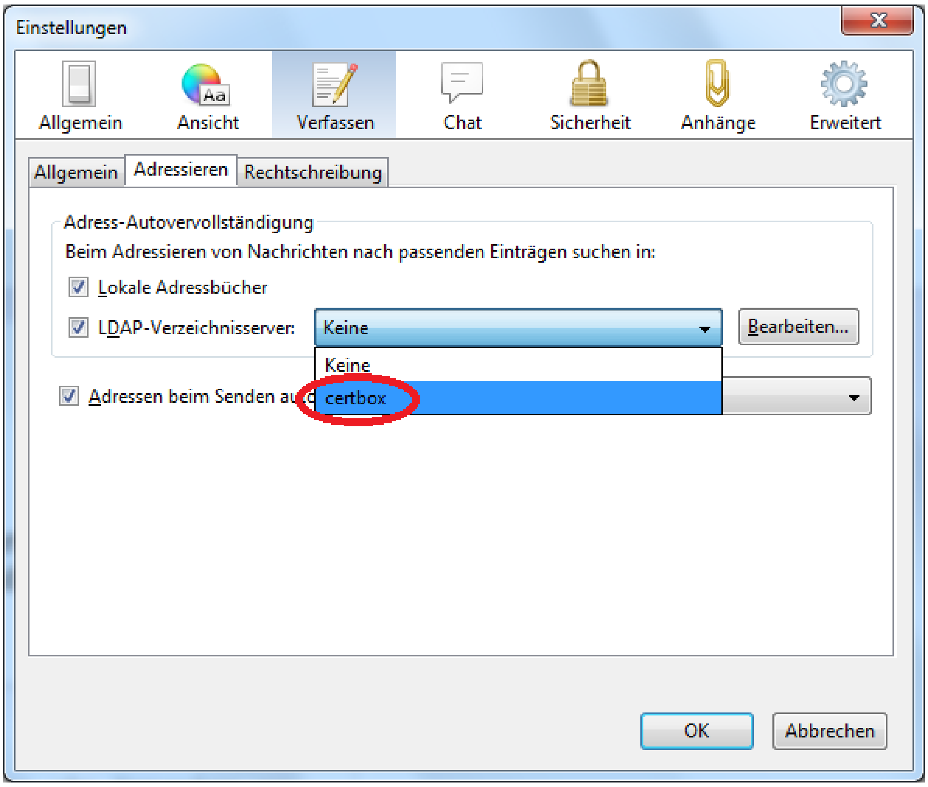
Basis-DN:

Port-Nummer: 389

Bind-DN:

□ Verschlüsselte Verbindung (SSL) verwenden

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



Adress-Autovervollständigung

Beim Adressieren von Nachrichten nach passenden Einträgen suchen in:

☑ Lokale Adressbücher

☑ LDAP-Verzeichnisserver: Keine

Keine

certbox

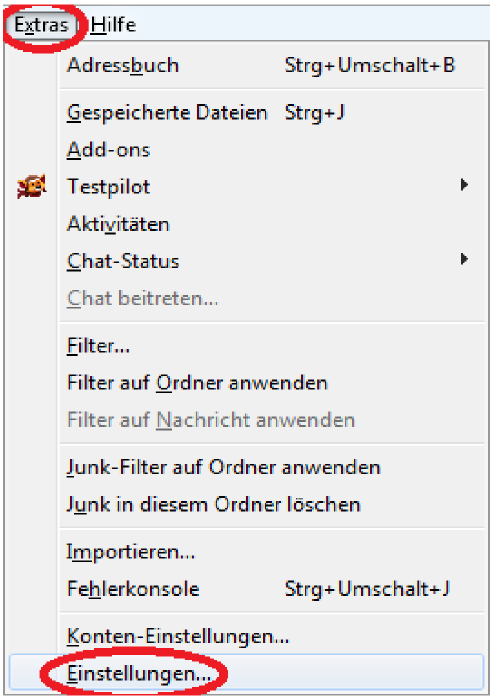
☑ Adressen beim Senden au

6.3 Certificates

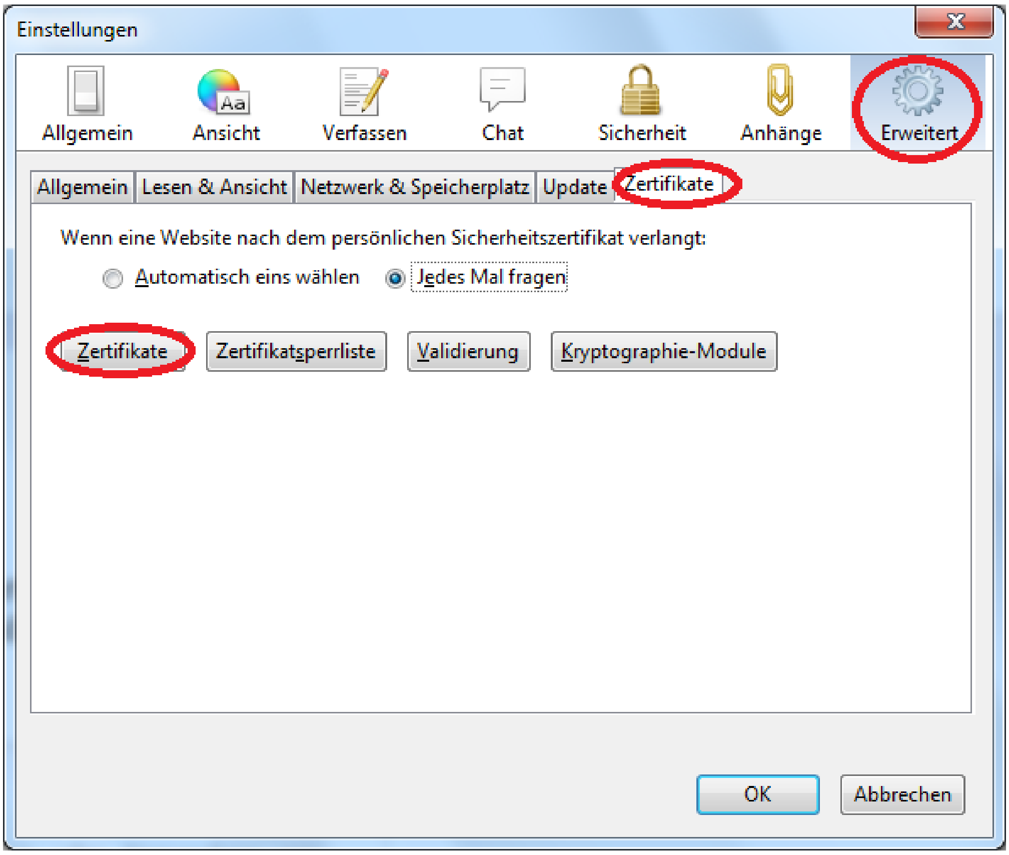
6.3.1 Import of a certificate

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.

For the import click on “Extras” and on “Settings”


Extras
Hilfe
Adressbuch Strg+Umschalt+B
Gespeicherte Dateien Strg+J
Add-ons
Testpilot
Aktivitäten
Chat-Status
Chat beitreten...
Filter...
Filter auf Ordner anwenden
Filter auf Nachricht anwenden
Junk-Filter auf Ordner anwenden
Junk in diesem Ordner löschen
Importieren...
Fehlerkonsole Strg+Umschalt+J
Konten-Einstellungen...
Einstellungen...

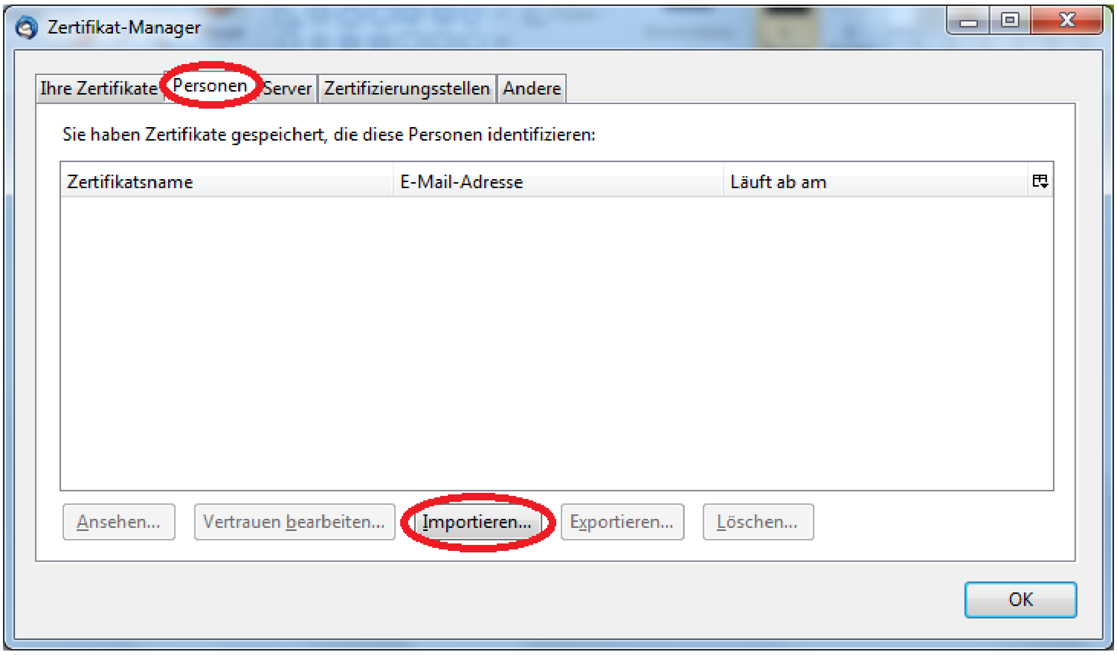
Click on “Advanced“ and then on “Certificates“



Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt:

○ Automatisch eins wählen ● Jedes Mal fragen

Click on “Persons“ and then on “Import“



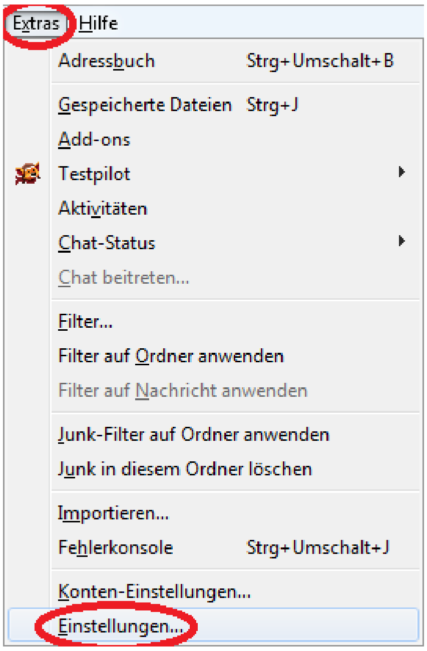
Sie haben Zertifikate gespeichert, die diese Personen identifizieren:

Zertifikatsname	E-Mail-Adresse	Läuft ab am

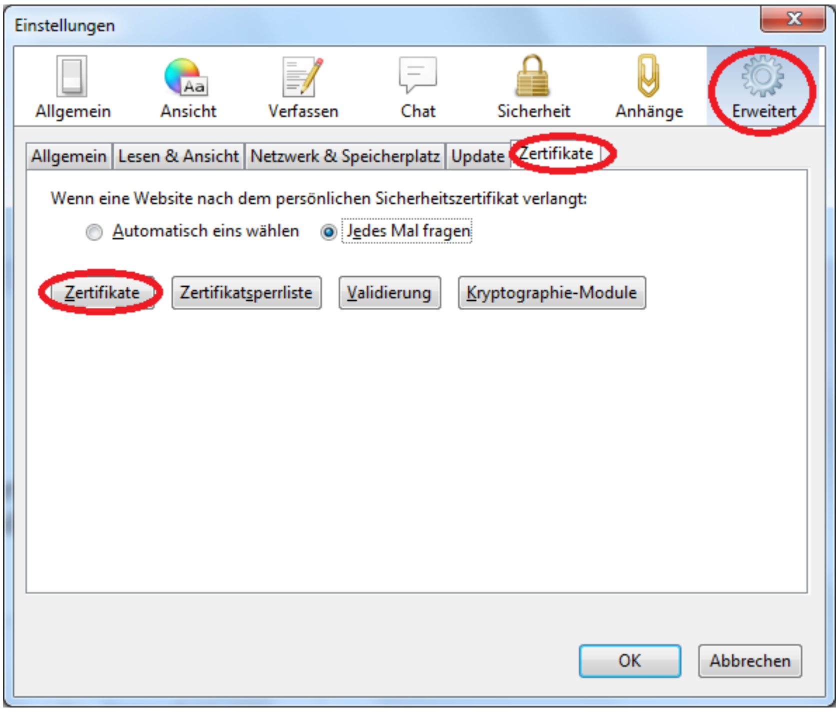
Open the previously downloaded certificate.

6.3.2 Import of a certificate chain

For the import click on “Extras” and on “Settings”


Extras
Hilfe
Adressbuch Strg+Umschalt+B
Gespeicherte Dateien Strg+J
Add-ons
Testpilot
Aktivitäten
Chat-Status
Chat beitreten...
Filter...
Filter auf Ordner anwenden
Filter auf Nachricht anwenden
Junk-Filter auf Ordner anwenden
Junk in diesem Ordner löschen
Importieren...
Fehlerkonsole Strg+Umschalt+J
Konten-Einstellungen...
Einstellungen...

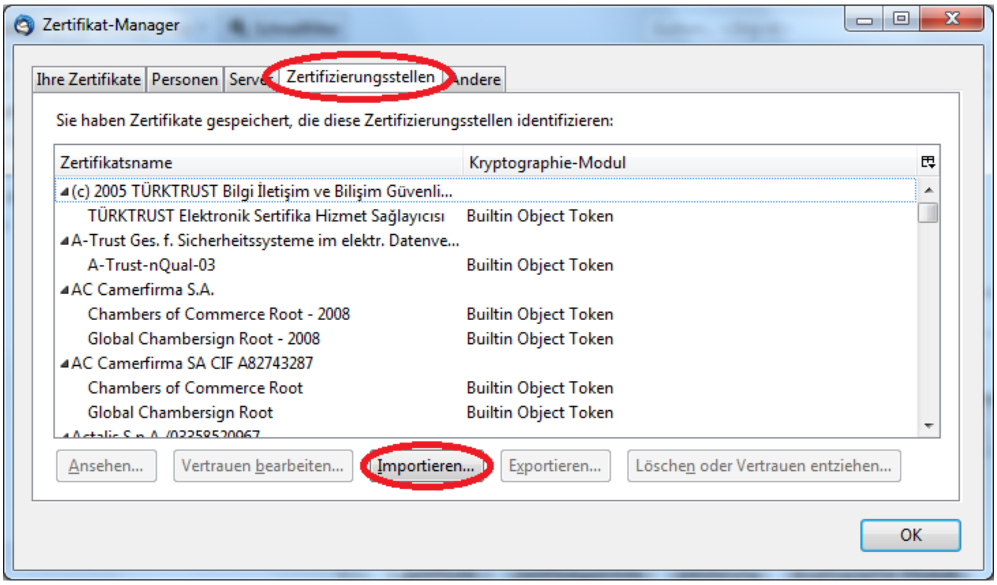
Click on “Advanced“ and then on “Certificates“



Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt:

○ Automatisch eins wählen ● Jedes Mal fragen

Select “Certificate Authorities“, Click “Import“ and open the downloaded container.

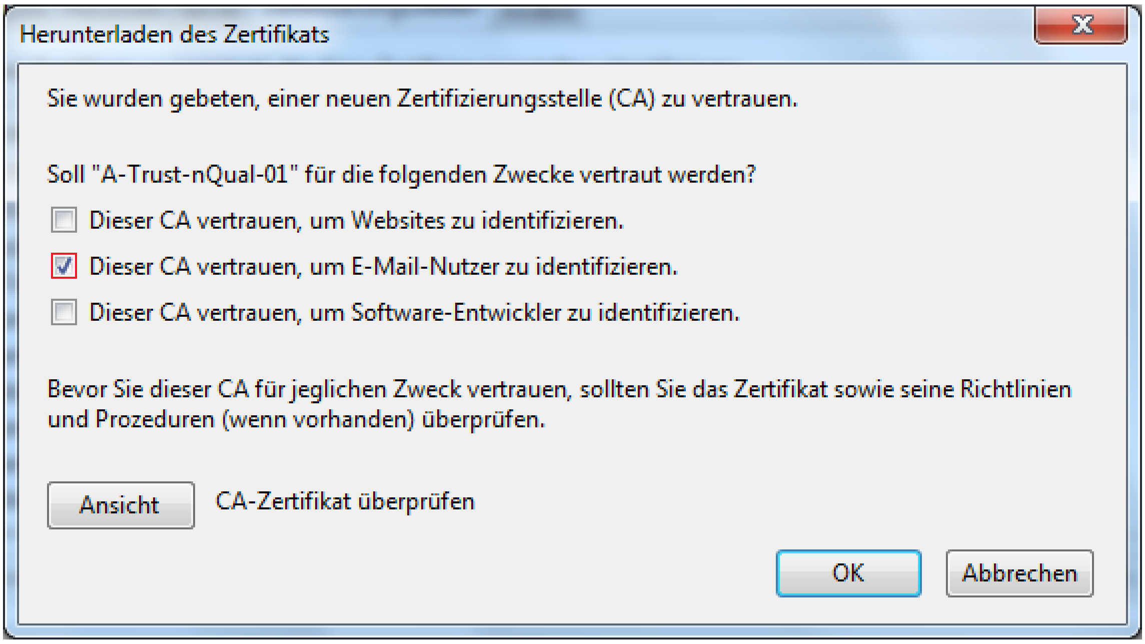


Zertifikat-Manager

Sie haben Zertifikate gespeichert, die diese Zertifizierungsstellen identifizieren:

Zertifikatsname	Kryptographie-Modul
◢ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenli...	
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	Builtin Object Token
◢ A-Trust Ges. f. Sicherheitssysteme im elektr. Datenve...	
A-Trust-nQual-03	Builtin Object Token
◢ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
◢ AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
◢ Actalis S.p.A./03358520067	

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



Herunterladen des Zertifikats

Sie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.

Soll "A-Trust-nQual-01" für die folgenden Zwecke vertraut werden?

☐ Dieser CA vertrauen, um Websites zu identifizieren.

☑ Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.

☐ Dieser CA vertrauen, um Software-Entwickler zu identifizieren.

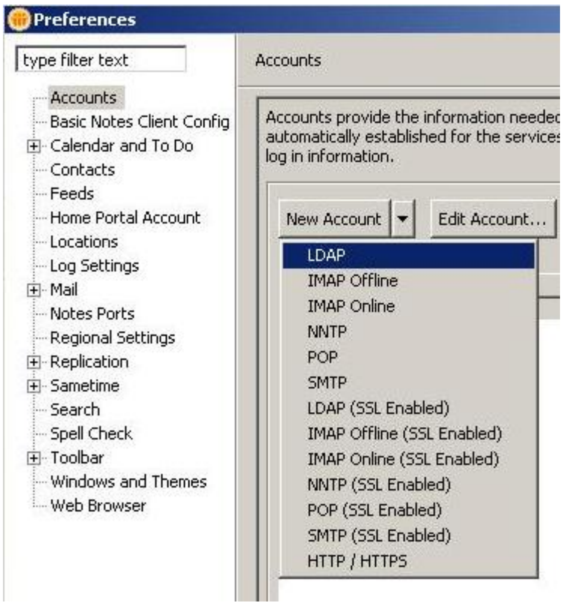
Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien und Prozeduren (wenn vorhanden) überprüfen.

CA-Zertifikat überprüfen

7 Lotus Notes 8

7.1 LDAP-Configuration

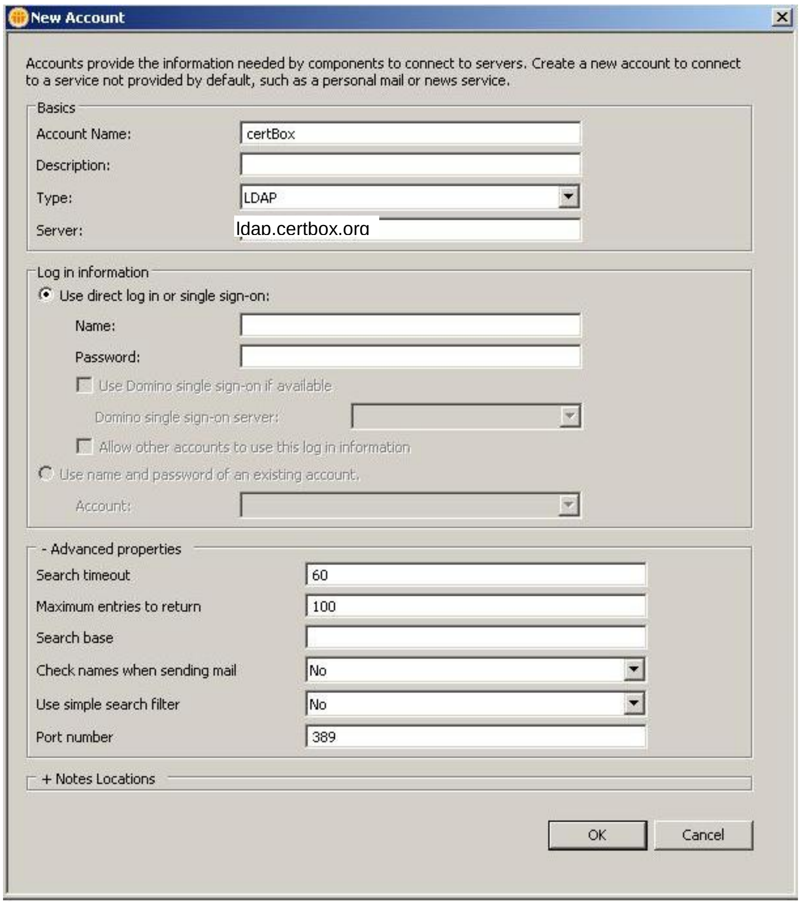
Select “Preferences\Accounts” click “New Account“, and select LDAP.



Accounts

Accounts provide the information neede automatically established for the service log in information.

Enter “certBox” as Account Name, select LDAP as Type and enter “ldap.certbox.org“, as Server.



Accounts provide the information needed by components to connect to servers. Create a new account to connect to a service not provided by default, such as a personal mail or news service.

Basics

Account Name: certBox

Description:

Type: LDAP

Server: ldap.certbox.org

Log in information

● Use direct log in or single sign-on:

Name:

Password:

□ Use Domino single sign-on if available

Domino single sign-on server:

□ Allow other accounts to use this log in information

○ Use name and password of an existing account.

Account:

- Advanced properties

Search timeout: 60

Maximum entries to return: 100

Search base:

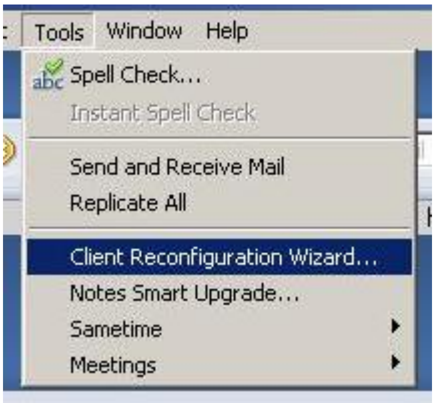
Check names when sending mail: No

Use simple search filter: No

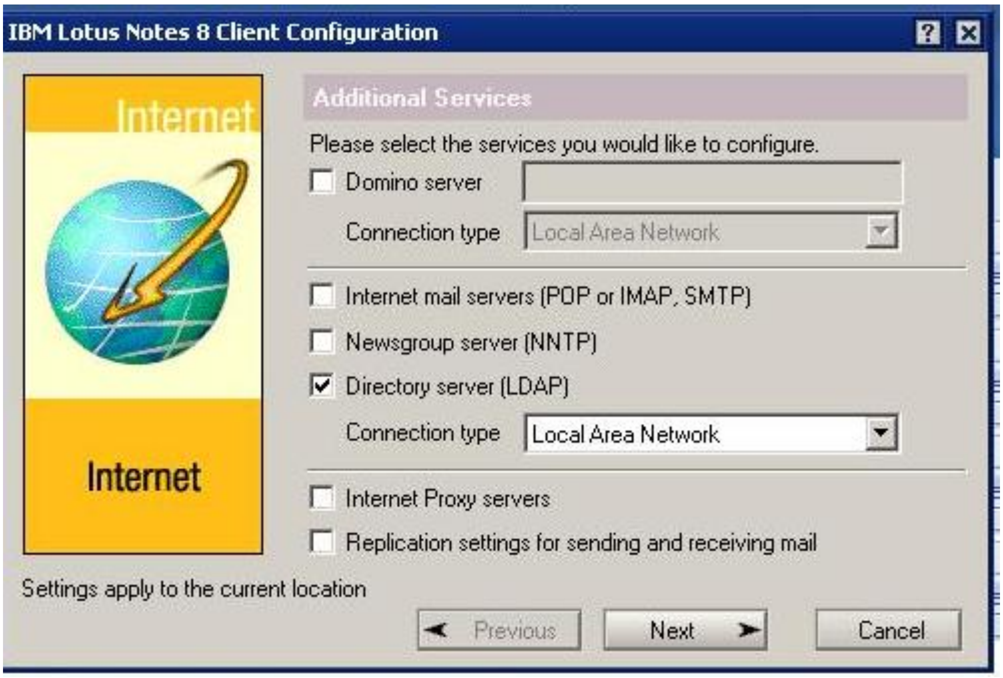
Port number: 389

+ Notes Locations

Now click “Tools“, and then “Client Reconfiguration Wizard“



Then select “Directory Server (LDAP)“ with the Connection type: “Local Area Network“.



IBM Lotus Notes 8 Client Configuration

Additional Services

Please select the services you would like to configure.

□ Domino server

Connection type: Local Area Network

□ Internet mail servers (POP or IMAP, SMTP)

□ Newsgroup server (NNTP)

☑ Directory server (LDAP)

Connection type: Local Area Network

□ Internet Proxy servers

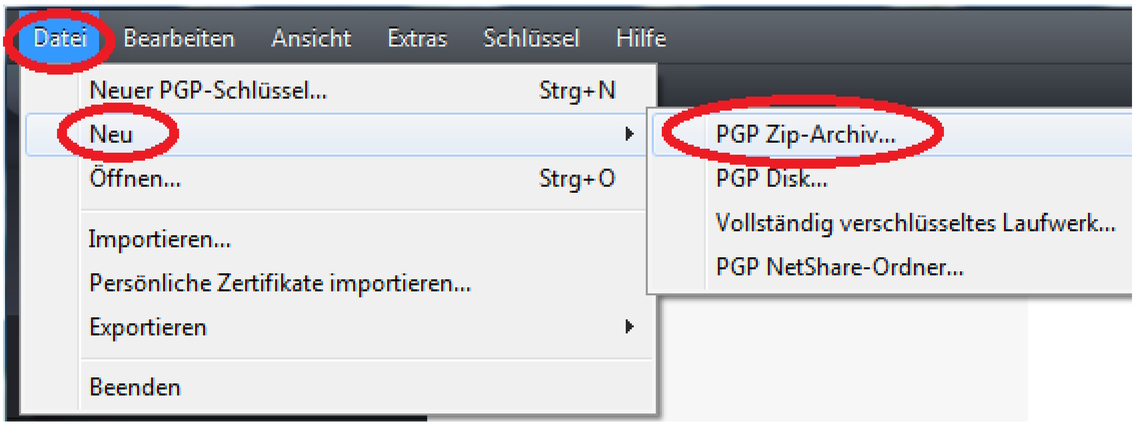
□ Replication settings for sending and receiving mail

Settings apply to the current location

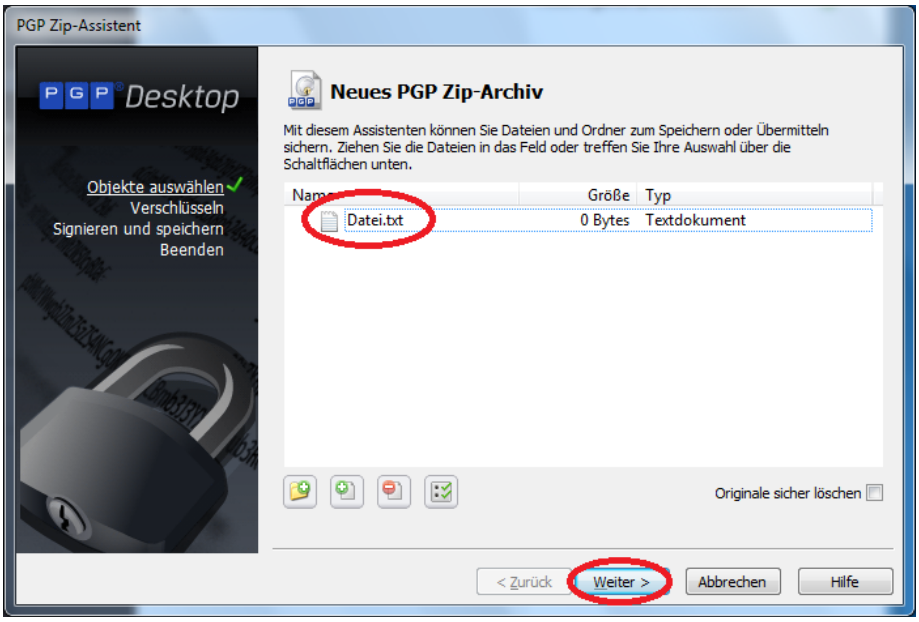
8 PGP-Desktop 10

8.1 Encrypt files

Click on „File“, then on „New“ and on „PGP Zip-archive“



Add the files via Drag&Drop and click „Next“



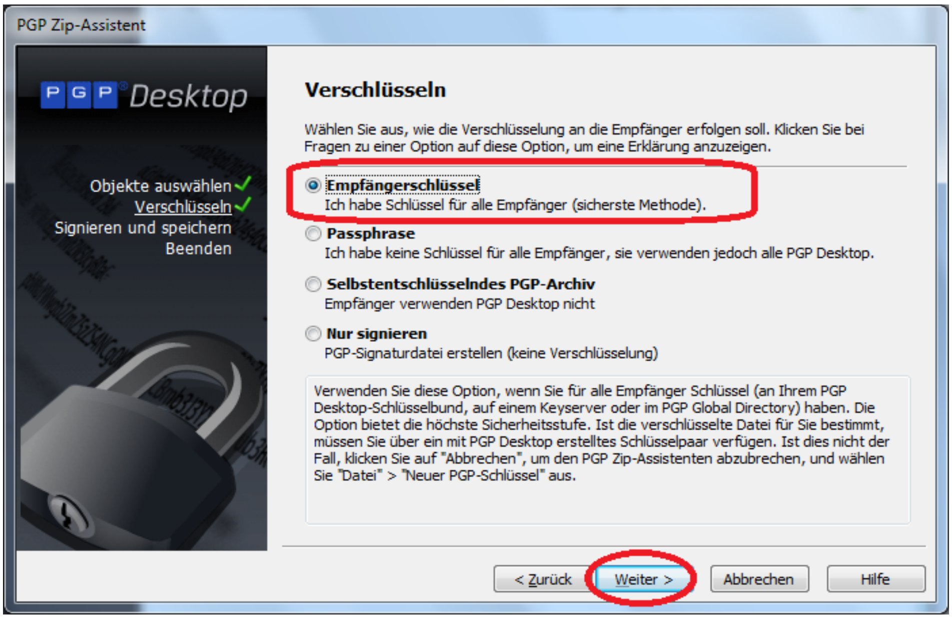
Neues PGP Zip-Archiv

Mit diesem Assistenten können Sie Dateien und Ordner zum Speichern oder Übermitteln sichern. Ziehen Sie die Dateien in das Feld oder treffen Sie Ihre Auswahl über die Schaltflächen unten.

Name	Größe	Typ
Datei.txt	0 Bytes	Textdokument

Originale sicher löschen □

Now select „Recipient key“ and click „Next“.



PGP Zip-Assistent

Verschlüsseln

Wählen Sie aus, wie die Verschlüsselung an die Empfänger erfolgen soll. Klicken Sie bei Fragen zu einer Option auf diese Option, um eine Erklärung anzuzeigen.

● **Empfängerschlüssel**
Ich habe Schlüssel für alle Empfänger (sicherste Methode).

○ **Passphrase**
Ich habe keine Schlüssel für alle Empfänger, sie verwenden jedoch alle PGP Desktop.

○ **Selbstentschlüsselndes PGP-Archiv**
Empfänger verwenden PGP Desktop nicht

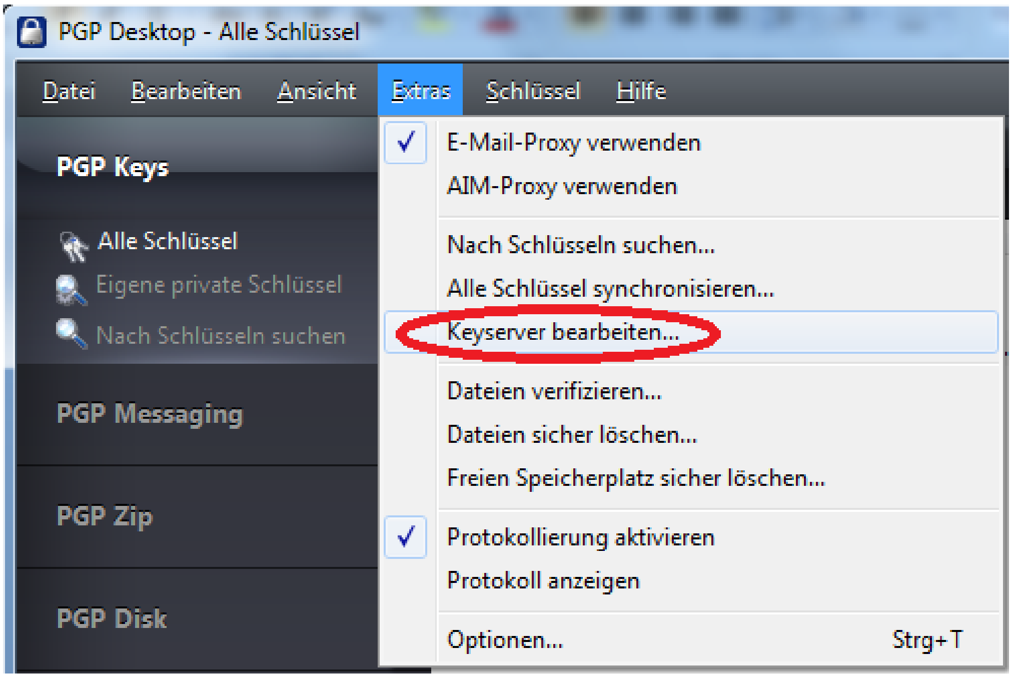
○ **Nur signieren**
PGP-Signaturdatei erstellen (keine Verschlüsselung)

Verwenden Sie diese Option, wenn Sie für alle Empfänger Schlüssel (an Ihrem PGP Desktop-Schlüsselbund, auf einem Keyserver oder im PGP Global Directory) haben. Die Option bietet die höchste Sicherheitsstufe. Ist die verschlüsselte Datei für Sie bestimmt, müssen Sie über ein mit PGP Desktop erstelltes Schlüsselpaar verfügen. Ist dies nicht der Fall, klicken Sie auf "Abbrechen", um den PGP Zip-Assistenten abzubrechen, und wählen Sie "Datei" > "Neuer PGP-Schlüssel" aus.

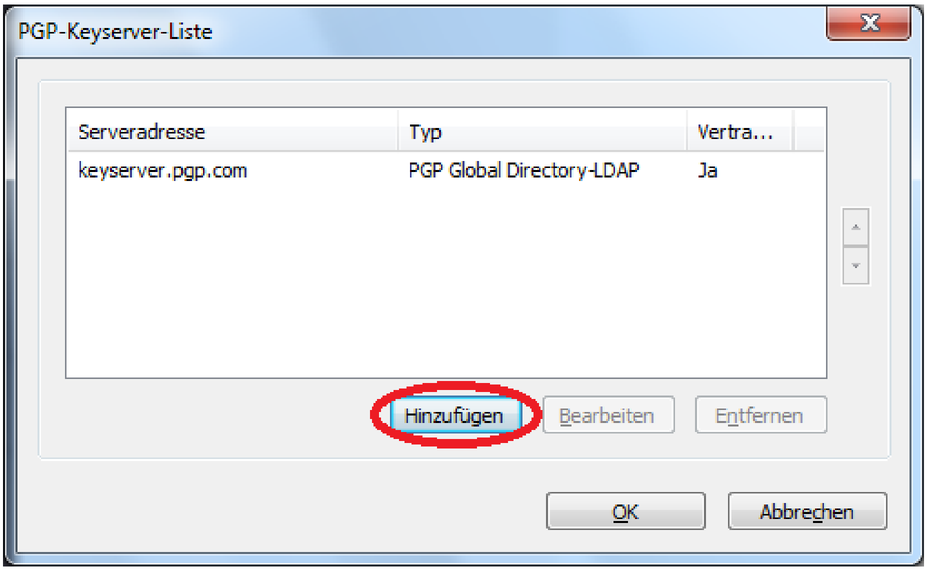
Then add the desired contacts, click two times „Next“ and then click „Finish“

8.2 LDAP-Configuration

Click “Extras“ and then on “Edit key servers…”



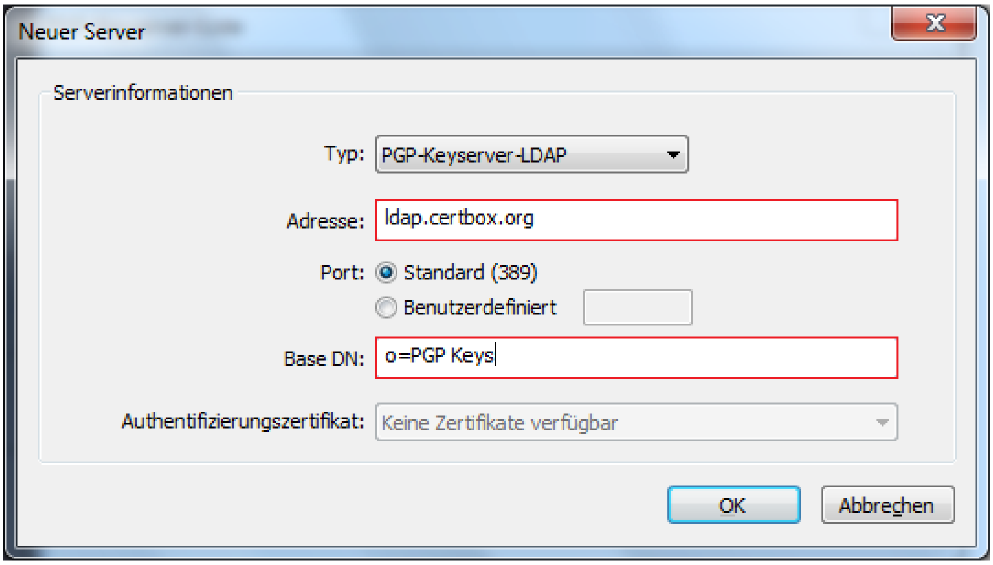
Click on “Add“



PGP-Keyserver-Liste

Serveradresse	Typ	Vertra...
keyserver.pgp.com	PGP Global Directory-LDAP	Ja

Select “PGP-Keyserver-LDAP“ as type and enter “ldap.certbox.org“ as address. Enter “o=PGP Keys” in the field “Base DN”.



Neuer Server

Serverinformationen

Typ: PGP-Keyserver-LDAP

Adresse: ldap.certbox.org

Port: ● Standard (389)

○ Benutzerdefiniert

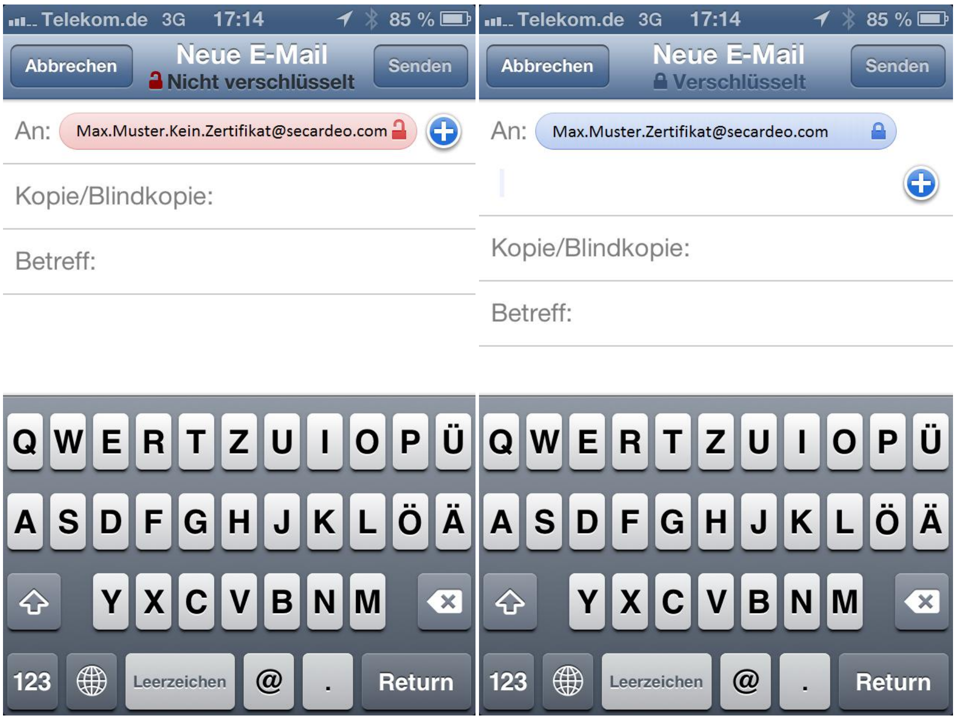
Base DN: o=PGP Keys

Authentifizierungszertifikat: Keine Zertifikate verfügbar

9 iOS (iPhone & iPad)

9.1 Encrypt an e-mail

iOS doesn’t offer the possibility to explicitly turn the encryption on or off. As soon as you got a certificate for a recipient it automatically encrypts.



Telekom.de 3G 17:14 85 %

Neue E-Mail

Nicht verschlüsselt

An: Max.Muster.Kein.Zertifikat@secardeo.com

Kopie/Blindkopie:

Betreff:

Telekom.de 3G 17:14 85 %

Neue E-Mail

Verschlüsselt

An: Max.Muster.Zertifikat@secardeo.com

Kopie/Blindkopie:

Betreff:

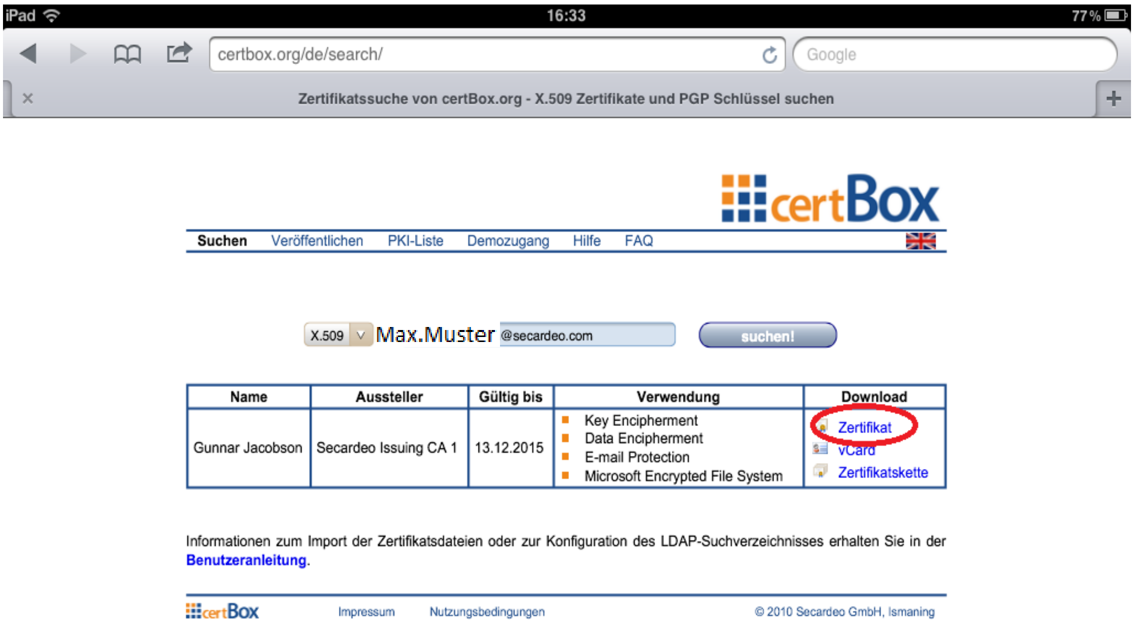
9.2 LDAP-Configuration

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

9.3 HTML-Search

9.3.1 Download and import of a certificate

Press the link “Search“ and enter the requested e-mail adress



iPad 16:33 77 %

certbox.org/de/search/

Zertifikatssuche von certBox.org - X.509 Zertifikate und PGP Schlüssel suchen

Suchen Veröffentlichen PKI-Liste Demozugang Hilfe FAQ

X.509 Max.Muster @secardeo.com suchen!

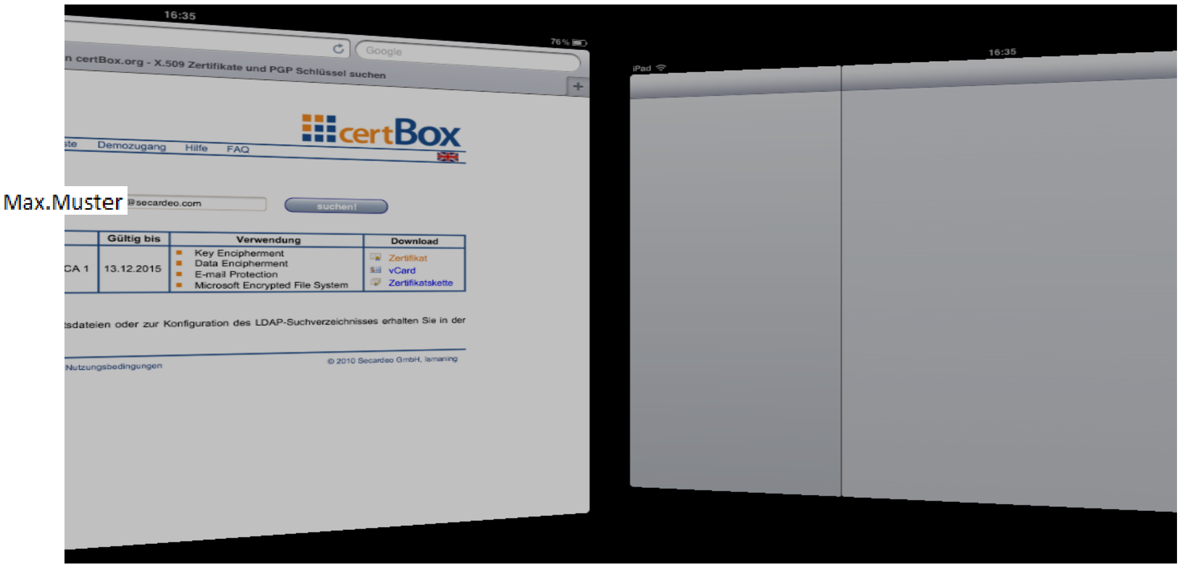
Name	Aussteller	Gültig bis	Verwendung	Download
Gunnar Jacobson	Secardeo Issuing CA 1	13.12.2015	Key Encipherment Data Encipherment E-mail Protection Microsoft Encrypted File System	Zertifikat vCard Zertifikatskette

Informationen zum Import der Zertifikatsdateien oder zur Konfiguration des LDAP-Suchverzeichnisses erhalten Sie in der **Benutzeranleitung**.

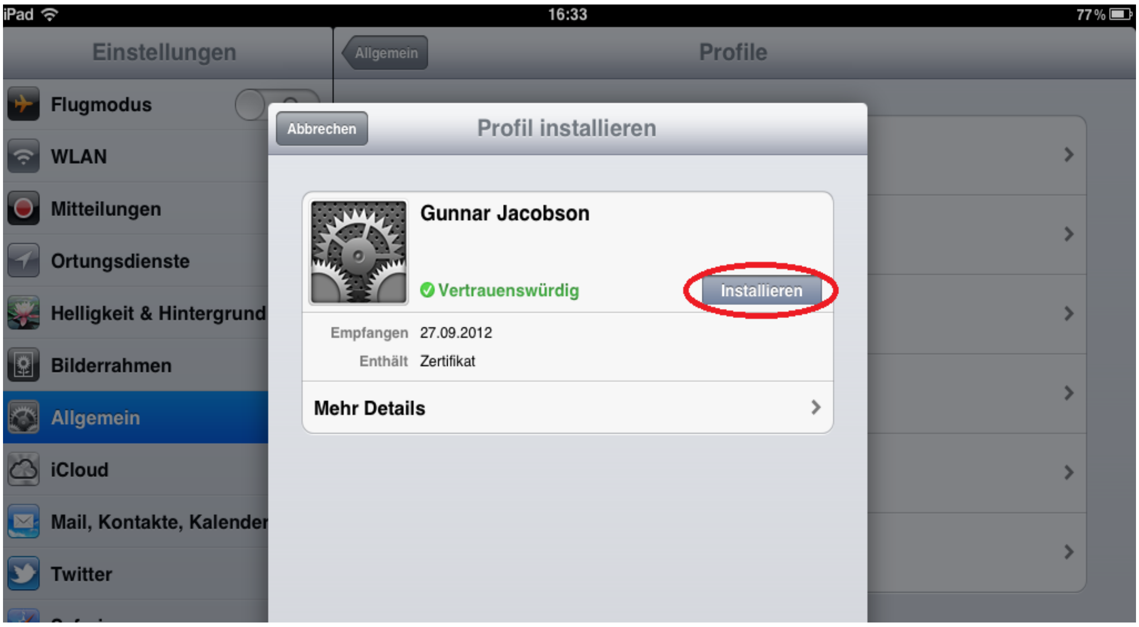
certBox Impressum Nutzungsbedingungen © 2010 Secardeo GmbH, Ismaning

Afterwards press on the link “Certificate”.

The device automatically recognizes, that the file is a certificate and switches to “Settings”



Press on “Install“.



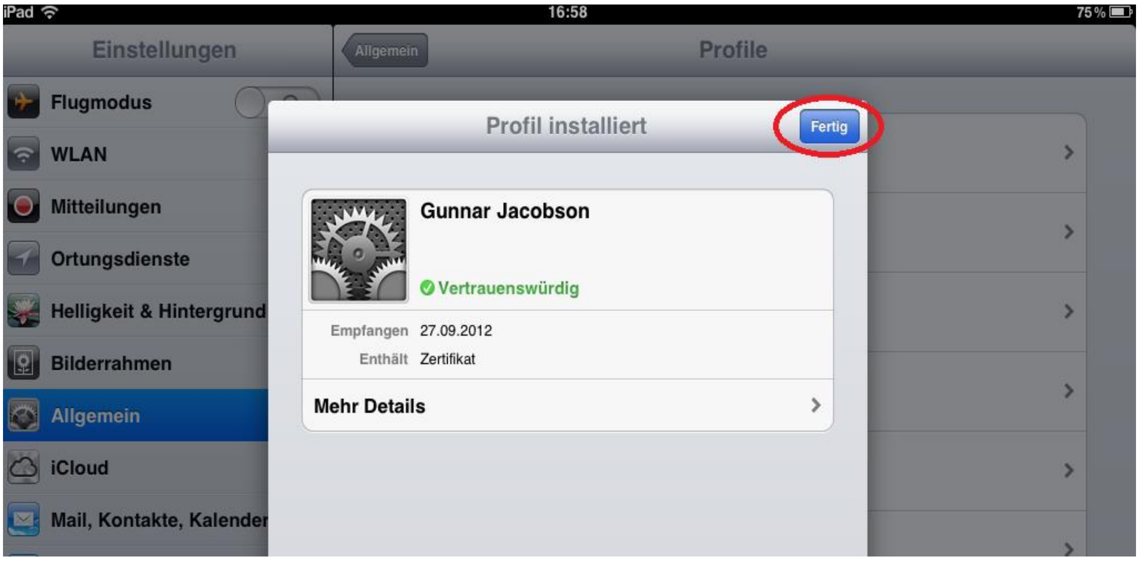
Gunnar Jacobson

✓ Vertrauenswürdig

Empfangen 27.09.2012

Enthält Zertifikat

The certificate is installed now. You can close the windows with a press on “Done”.



Gunnar Jacobson

✓ Vertrauenswürdig

Empfangen 27.09.2012

Enthält Zertifikat