# Virtuelle Poststelle

## Mailverschlüsselung (mit S/MIME)

### Überblick

E-Mail-Kommunikation ist nicht nur für Unternehmen zu einem wichtig Bestandteil des Tagesgeschäfts geworden. Wobei die herkömmliche E-Mail-Kommunikation alles andere als ein hohes Vertrauen verdient, denn Sie ist vergleichbar mit dem Transport einer Postkarte durch eine unbekannte Personen. E-Mail-Inhalte sind für Fremde nicht nur lesbar sondern auch manipulierbar und der Empfänger der E-Mail kann diese Änderungen nicht einmal erkennen bzw. feststellen.

Erste Schritte zur vertrauenswürdigen E-Mail-Kommunikation ist die elektronische Signatur von E-Mails mit Benutzerzertifikaten. Das dabei verwendete standardisierte S/MIME  Verfahren stellt sicher, dass E-Mails unverändert beim Empfänger ankommen. Falls nicht, wird der Empfänger der E-Mail von jedem modernen E-Mail Programm gewarnt.

Der nächste Schritt zu einer vertrauenswürdigen E-Mail-Kommunikation ist die Verschlüsslung von E-Mails. Somit wird aus der „Postkarte“ sogar mehr als nur ein verschlossener Brief. Denn nur der vorgesehene Empfänger der E-Mail kann diese lesen.

### Vorgang

Zur Verschlüsselung einer E-Mail benötigen Sie ein Zertifikat zur E-Mail-Verschlüsselung. Zu einem Zertifikat gehört ein Schlüsselpaar: Der private Schlüssel ist ausschließlich für Sie gedacht, den öffentliche Schlüssel kann jeder nutzen, der Ihnen eine verschlüsselte Nachricht senden möchte. Der öffentliche Schlüssel ist zudem Bestandteil des Zertifikats.

Mit Hilfe des Zertifikates können Sie E-Mails signieren. Das E-Mail-Programm des Empfängers hat die Möglichkeit anhand der Signatur festzustellen, ob die E-Mail während der Übertragung manipuliert wurde und ob sie von der im Zertifikat angegebenen Absenderadresse stammt. Beim Signieren einer E-Mail erhält der Empfänger zudem Ihr Zertifikat und somit ebenfalls Ihren öffentlichen Schlüssel. Mit diesem Schlüssel kann er in Zukunft E-Mails an Sie verschlüsseln. Nur Sie sind im Stande mit Hilfe Ihres privaten Schlüssels, diese E-Mail zu entschlüsseln. Deshalb ist es besonders wichtig den privaten Schlüssel Ihres Zertifikats vor Diebstahl zu schützen und ihn niemals Anderen zur Verfügung zu stellen.

Durch die Verwendung von Zertifikaten bei beiden Kommunikationspartnern können E-Mails mit dem privaten Schlüssel des Absenders signiert und gleichzeitig mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden. Da die Übermittlung des öffentlichen Schlüssels bei einer signierten Mail Bestandteil des Zertifikates ist, ist der Kommunikationspartner in der Lage, bereits bei einer Antwort auf eine signierte E-Mail, diese sowohl zu signieren als auch zu verschlüsseln.

### Vorteile

Die Verschlüsselung durch S/MIME bietet zwei Funktionen:

- Signatur einer zu versendenden E-Mail mit dem privaten Schlüssel des Versenders
- Verschlüsselung einer zu versenden E-Mail mit dem öffentlichen Schlüssel eines Empfängers

Durch die Signatur kann sichergestellt werden, dass die E-Mail während der Übermittlung nicht verändert / manipuliert wurde. Die Verschlüsselung schützt die E-Mail vor der Einsichtnahme unbefugter Dritter.

## Zertifikat

Ein Zertifikat ist ein öffentlicher Schlüssel, der von einer Zertifizierungsstelle (Certification Authority) beglaubigt und unterschrieben ist. Ein Zertifikat belegt, dass der Schlüssel wirklich zu derjenigen Person gehört, die in der Benutzerkennung des Schlüssels angegeben ist. Es ist deshalb vergleichbar mit einem elektronischen Ausweis.

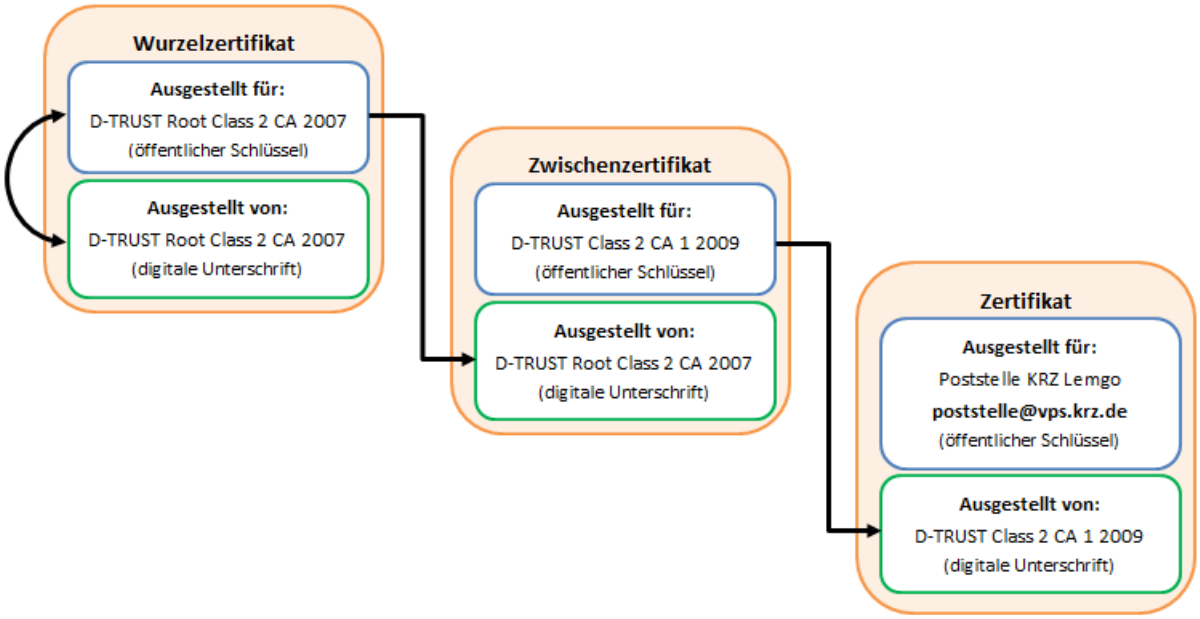
## Zertifikatsketten

Um Zertifikate überprüfen zu können, enthält jedes Zertifikat einen Verweis auf das Zertifikat der Zertifizierungsstelle, welche das Zertifikat ausgestellt hat. Technisch gesprochen handelt es sich bei diesem Verweis um eine digitale Unterschrift (Signatur) der Zertifizierungsstelle. Anwendungsprogramme können mit Hilfe des Zertifikats der Zertifizierungsstelle die Gültigkeit eines Zertifikats überprüfen.

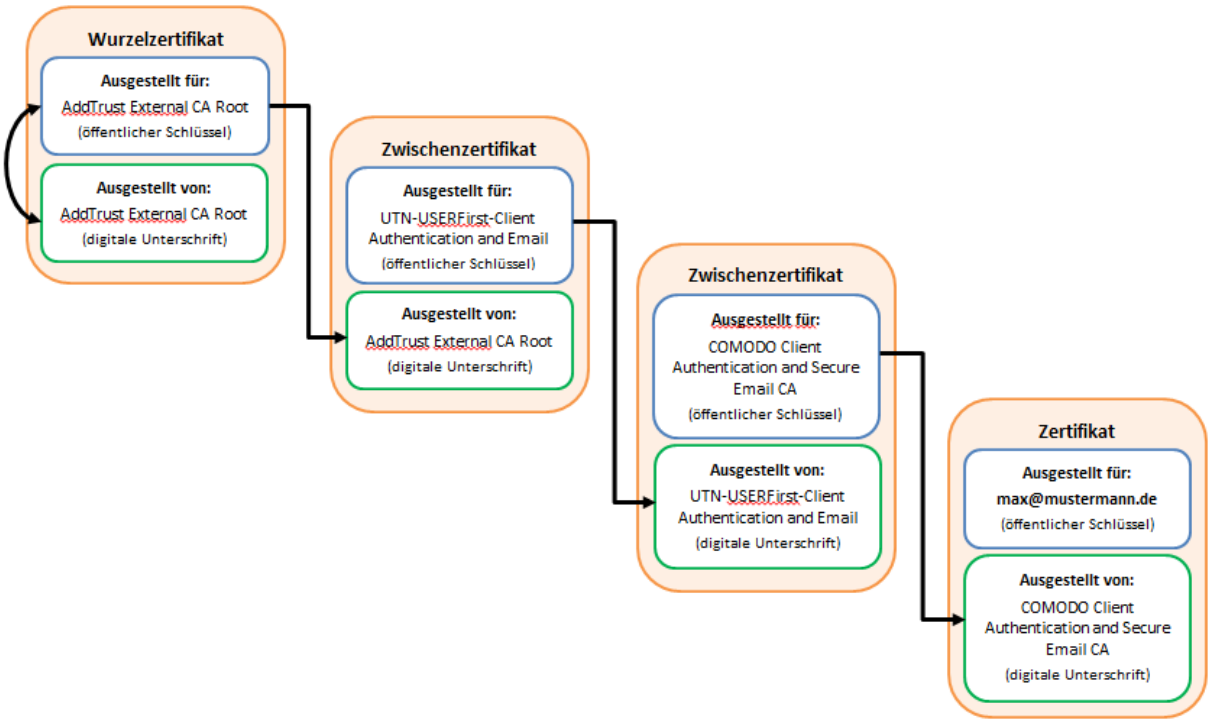
Aus technischen oder organisatorischen Gründen, kann es sein, dass das Zertifikat einer Zertifizierungsinstanz seinerseits wieder einen Verweis auf ein Zertifikat einer übergeordneten Zertifizierungsinstanz enthält.

Daraus ergibt sich eine Kette oder eine Hierarchie von Zertifikaten, die überprüft werden müssen, um die Gültigkeit eines Zertifikats zu prüfen.

Zertifikatskette der Poststelle KRZ Lemgo (poststelle@vps.krz.de)




Zertifikatskette eines kostenlosen Zertifikats für max@mustermann.de von COMODO




## Wurzelzertifikat

Am Anfang der Kette/Hierarchie von Zertifikaten steht das Wurzelzertifikat (top-level certificate). Die Wurzelzertifikate werden von keiner anderen Zertifizierungsinstanz ausgestellt und enthalten somit keinen nachprüfbaren Verweis auf ein anderes Zertifikat. Die Zertifizierungsinstanz „unterschreibt“ vielmehr ihr eigenes Zertifikat (selbst-signiert).

Wurzelzertifikate müssen in den Anwendungsprogrammen installiert sein, damit die Anwendungsprogramme die Hierarchie/Kette von Zertifikaten überprüfen können.

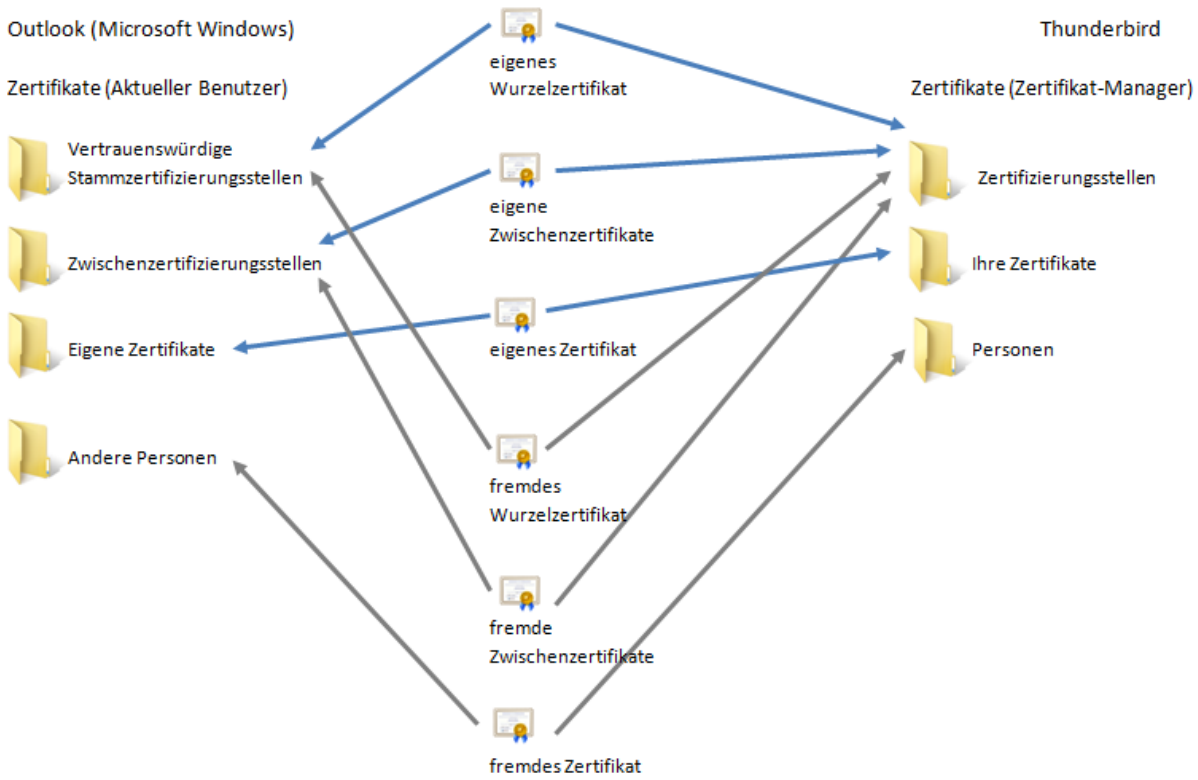
## Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Der Absender muss im Besitz eines gültigen X.509-Zertifikates sein und dieses auch installiert haben.
- Für die Empfänger müssen ebenfalls gültige Zertifikate installiert sein.
- Es müssen die Zertifikate der herausgebenden Zertifizierungsstellen installiert sein.
- Den Zertifikaten der Empfänger und der Herausgeber ist das Vertrauen ausgesprochen.

## Zuordnung der Zertifikate

Zuordnung der Zertifikate in die jeweiligen Zertifikatsspeicher



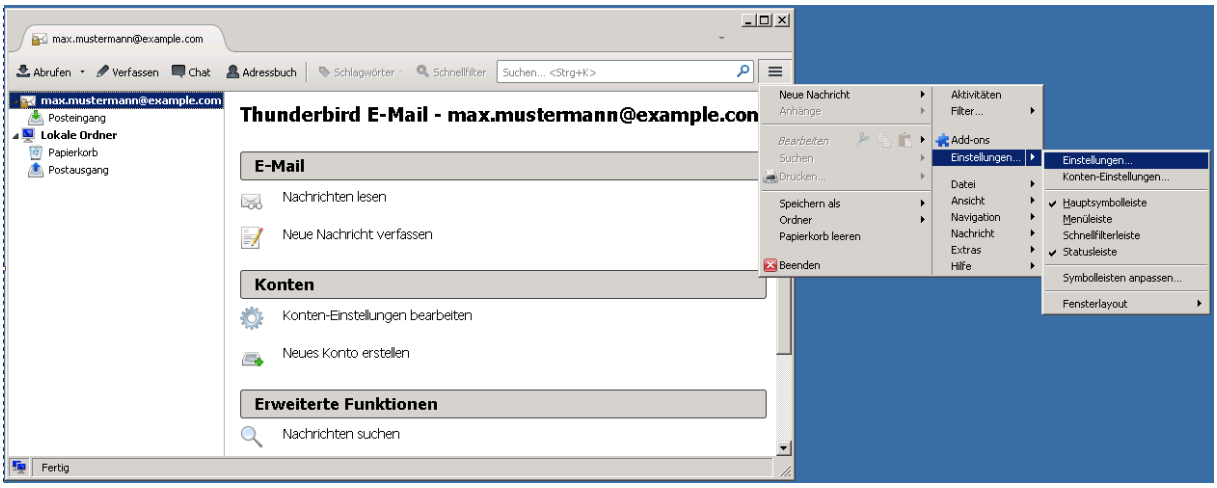

Installation des X.509-Zertifikates

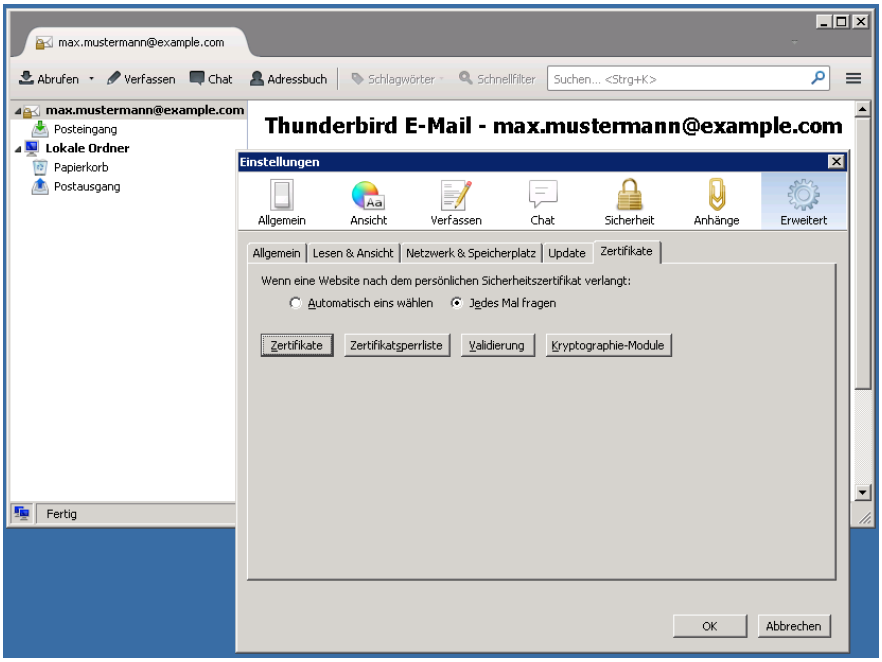
## Installation der erforderlichen Ausstellerzertifikate

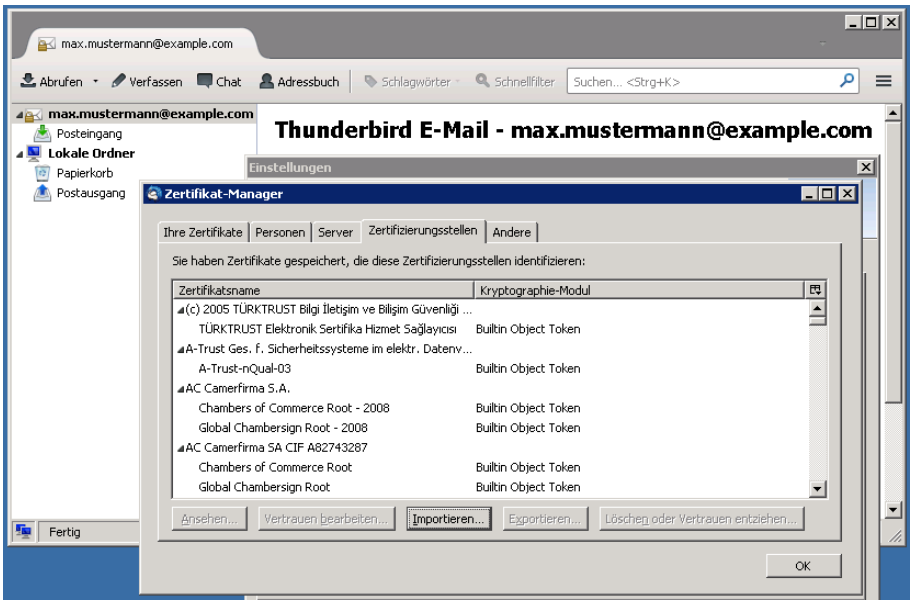
Thunderbird

Während eine Vielzahl von Ausstellerzertifikaten bereits im Zertifikatsspeicher des Thunderbird installiert sind, müssen Sie gegebenenfalls Ihre Ausstellerzertifikate (Wurzelzertifikat, Zwischenzertifikate) nachträglich installieren:

*Einstellungen... > Einstellungen… > Zertifikate > Zertifikate... > Zertifizierungsstellen*


max.mustermann@example.com
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
max.mustermann@example.com
Posteingang
Lokale Ordner
Papierkorb
Postausgang
Thunderbird E-Mail - max.mustermann@example.com
E-Mail
Nachrichten lesen
Neue Nachricht verfassen
Konten
Konten-Einstellungen bearbeiten
Neues Konto erstellen
Erweiterte Funktionen
Nachrichten suchen
Fertig
Neue Nachricht
Anhänge
Bearbeiten
Suchen
Drucken...
Speichern als
Ordner
Papierkorb leeren
Beenden
Aktivitäten
Filter...
Add-ons
Einstellungen...
Datei
Ansicht
Navigation
Nachricht
Extras
Hilfe
Einstellungen...
Konten-Einstellungen...
Hauptsymbolleiste
Menüleiste
Schnellfilterleiste
Statusleiste
Symbolleisten anpassen...
Fensterlayout

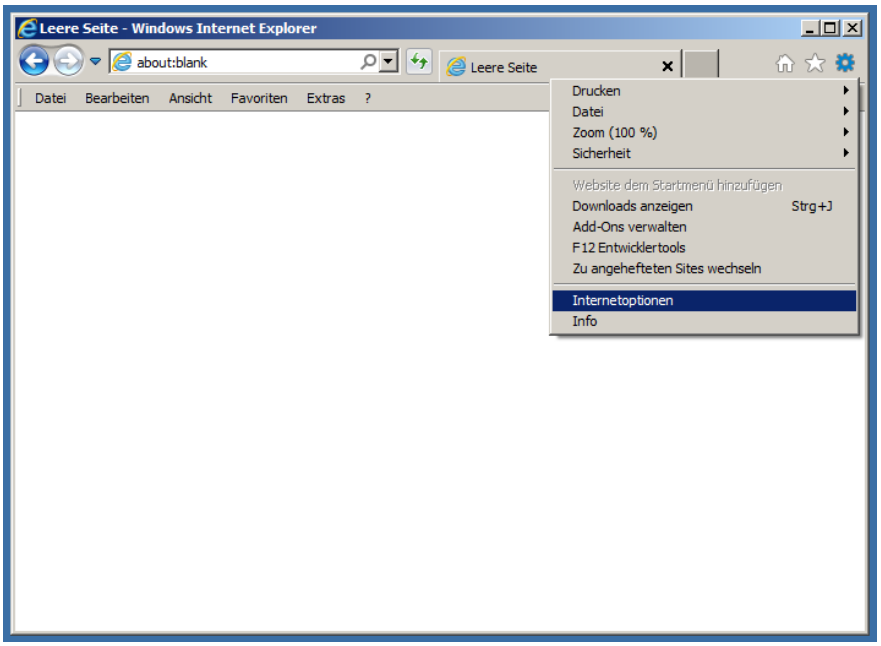

max.mustermann@example.com
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
max.mustermann@example.com
Posteingang
Lokale Ordner
Papierkorb
Postausgang
Thunderbird E-Mail - max.mustermann@example.com
Einstellungen
Allgemein
Ansicht
Verfassen
Chat
Sicherheit
Anhänge
Erweitert
Allgemein
Lesen & Ansicht
Netzwerk & Speicherplatz
Update
Zertifikate
Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt:
Automatisch eins wählen
Jedes Mal fragen
Zertifikate
Zertifikatsperrliste
Validierung
Kryptographie-Module
OK
Abbrechen
Fertig


max.mustermann@example.com
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
max.mustermann@example.com
Posteingang
Lokale Ordner
Papierkorb
Postausgang
Thunderbird E-Mail - max.mustermann@example.com
Einstellungen
Zertifikat-Manager
Ihre Zertifikate
Personen
Server
Zertifizierungsstellen
Andere
Sie haben Zertifikate gespeichert, die diese Zertifizierungsstellen identifizieren:
Zertifikatsname
Kryptographie-Modul
(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği ...
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı
Builtin Object Token
A-Trust Ges. f. Sicherheitssysteme im elektr. Datenv...
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
Ansehen...
Vertrauen bearbeiten...
Importieren...
Exportieren...
Löschen oder Vertrauen entziehen...
OK
Fertig

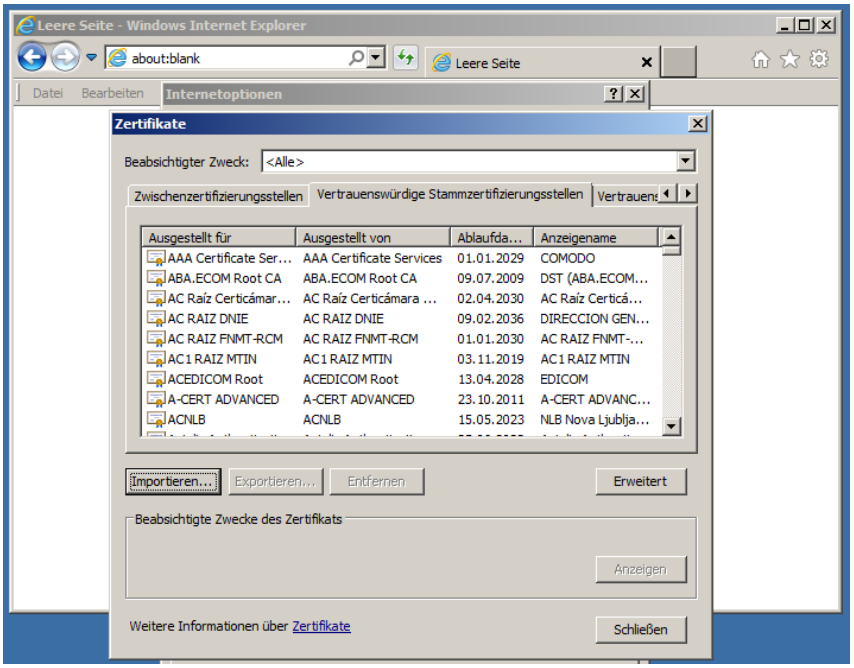
Klicken Sie auf „Importieren“ und wählen Sie das Ausstellerzertifikat aus. Danach ist diesem importierten Zertifikat durch "Bearbeiten" der Vertrauensstatus einzustellen. Hier ist zumindest das Vertrauen für die Identifikation von Mail-Benutzern erforderlich.

Outlook 2010

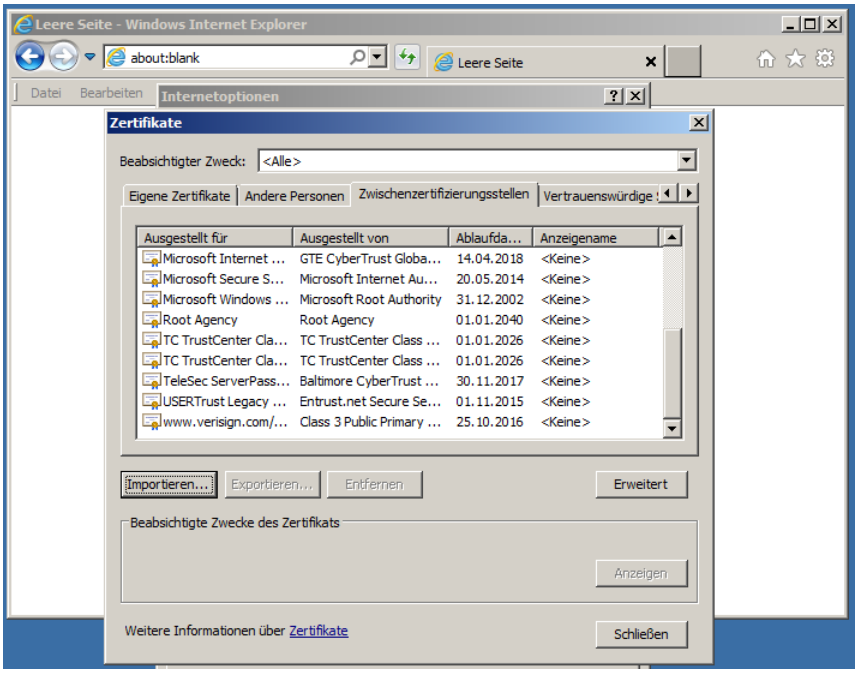
Während eine Vielzahl von Ausstellerzertifikaten bereits im Zertifikatsspeicher von Windows installiert sind, müssen Sie gegebenenfalls Ihre Ausstellerzertifikate (Wurzelzertifikat, Zwischenzertifikate) nachträglich installieren. Hierzu gehen Sie im Internet Explorer über *Extras > Internetoptionen > Inhalte*




und klicken auf "Zertifikate".



Im folgenden Dialogfenster „Zertifikate“ wählen wir den Reiter „Zwischenzertifizierungsstellen“ aus und klicken auf „Importieren“. Falls Sie ein Wurzelzertifikat installieren müssen, wählen Sie stattdessen den Reiter „Vertrauenswürdige Stammzertifizierungsstellen“ und klicken auf „Importieren“.



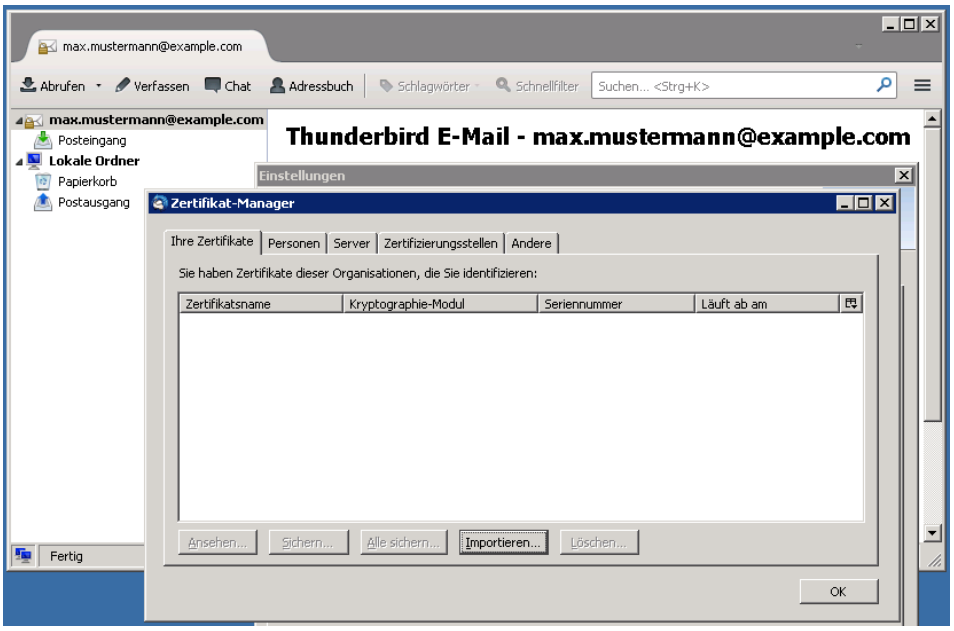

Wählen Sie das Ausstellerzertifikat und bestätigen mit OK.

## Installation des eigenen Zertifikates

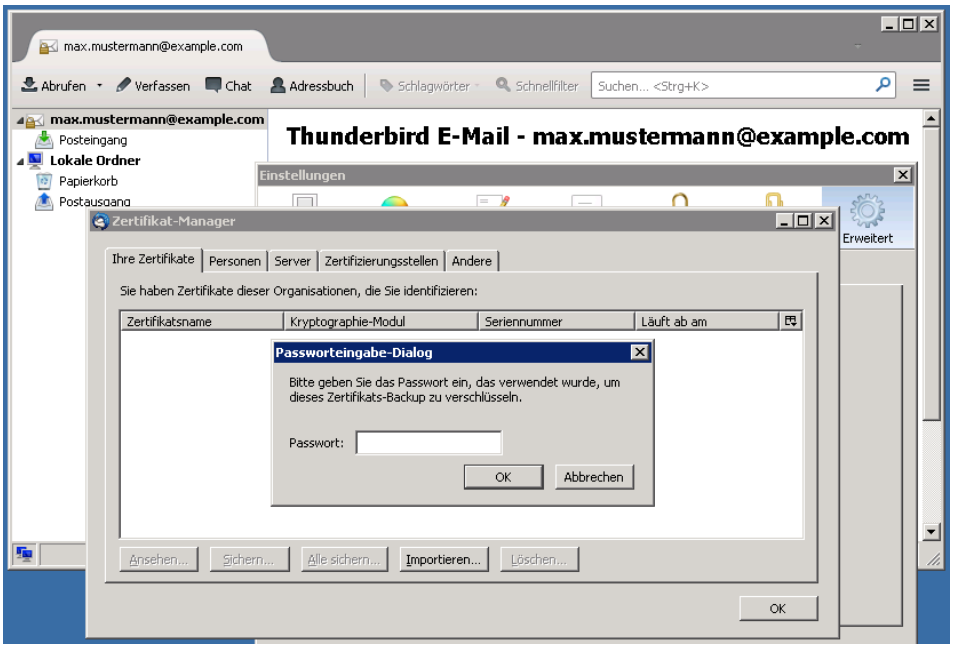
Thunderbird

Dazu ist hier die aus dem Browser exportierte .pfx- oder .p12-Datei mit dem geheimen Schlüssel auszuwählen:

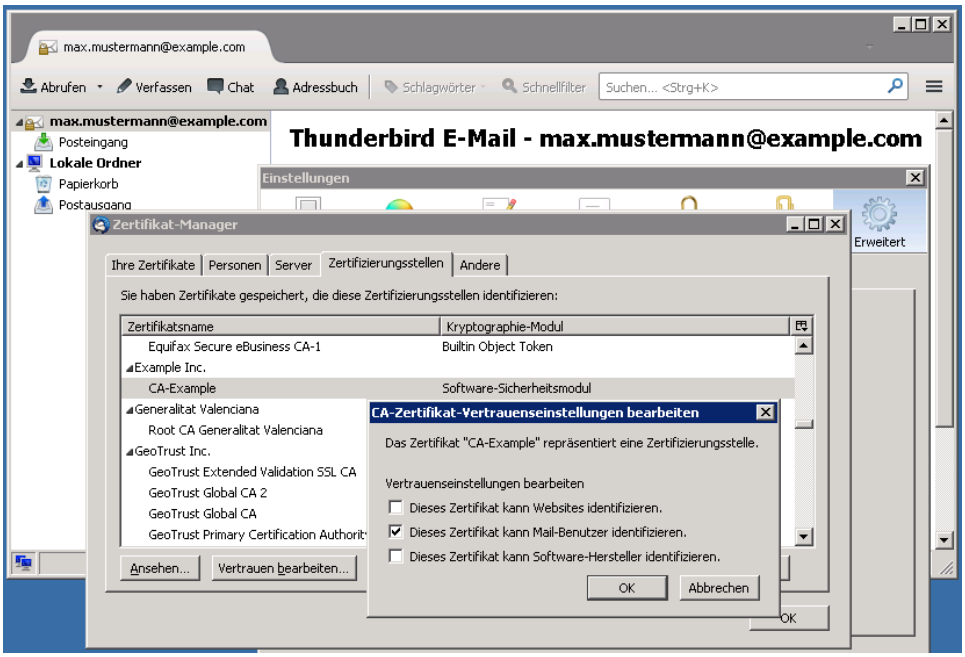
*Einstellungen... > Einstellungen… > Zertifikate > Zertifikate... > Ihre Zertifikate > Importieren*




Hierbei werden Sie zuerst nach dem Masterpasswort des "Software-Sicherheitsmoduls" und danach nach dem "Transportpasswort" der .pfx- bzw. .p12-Datei gefragt.



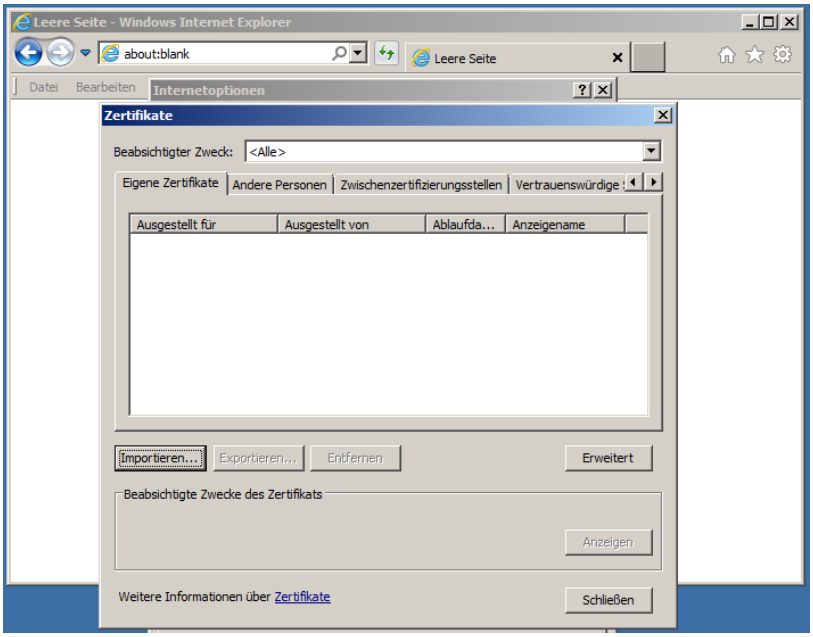

Voraussetzung für einen erfolgreichen Import ist das Vorhandensein der Herausgeberzertifikate (unter "Zertifizierungsstellen") sowie das ausgesprochene Vertrauen in diese Zertifikate (=> "Bearbeiten").



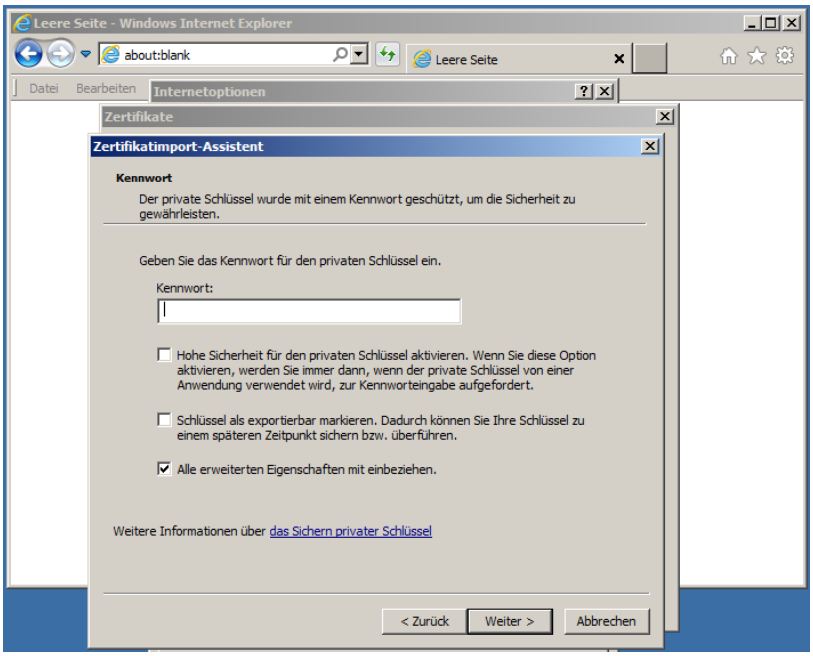

Nach dem erfolgreichen Import des eigenen Zertifikates übernimmt das Software-Sicherheitsmodul des Thunderbird durch die Verschlüsselung mit dem Masterpasswort den Schutz des eigenen privaten Schlüssels.

Outlook 2010

Im Internet Explorer wählen Sie *Extras > Internetoptionen > Inhalte* und klicken auf "Zertifikate". Im folgenden Dialogfenster „Zertifikate“ wählen Sie den Reiter „Eigene Zertifikate“ aus und klicken auf „Importieren“.




Wählen Sie Ihr Zertifikat aus und bestätigen, anschließend werden Sie nach dem "Transportpasswort" der .pfx- bzw. .p12-Datei gefragt.

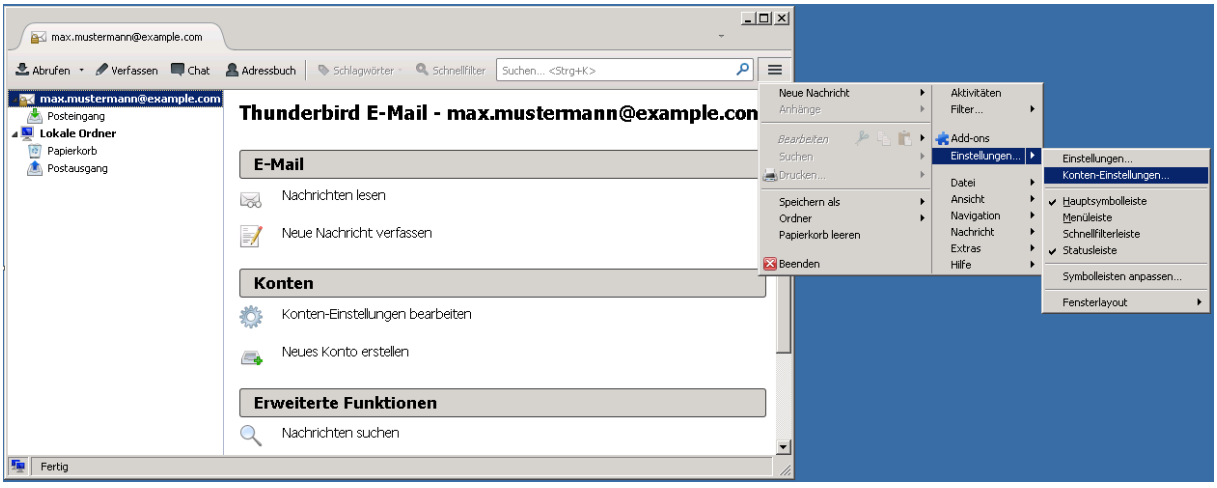


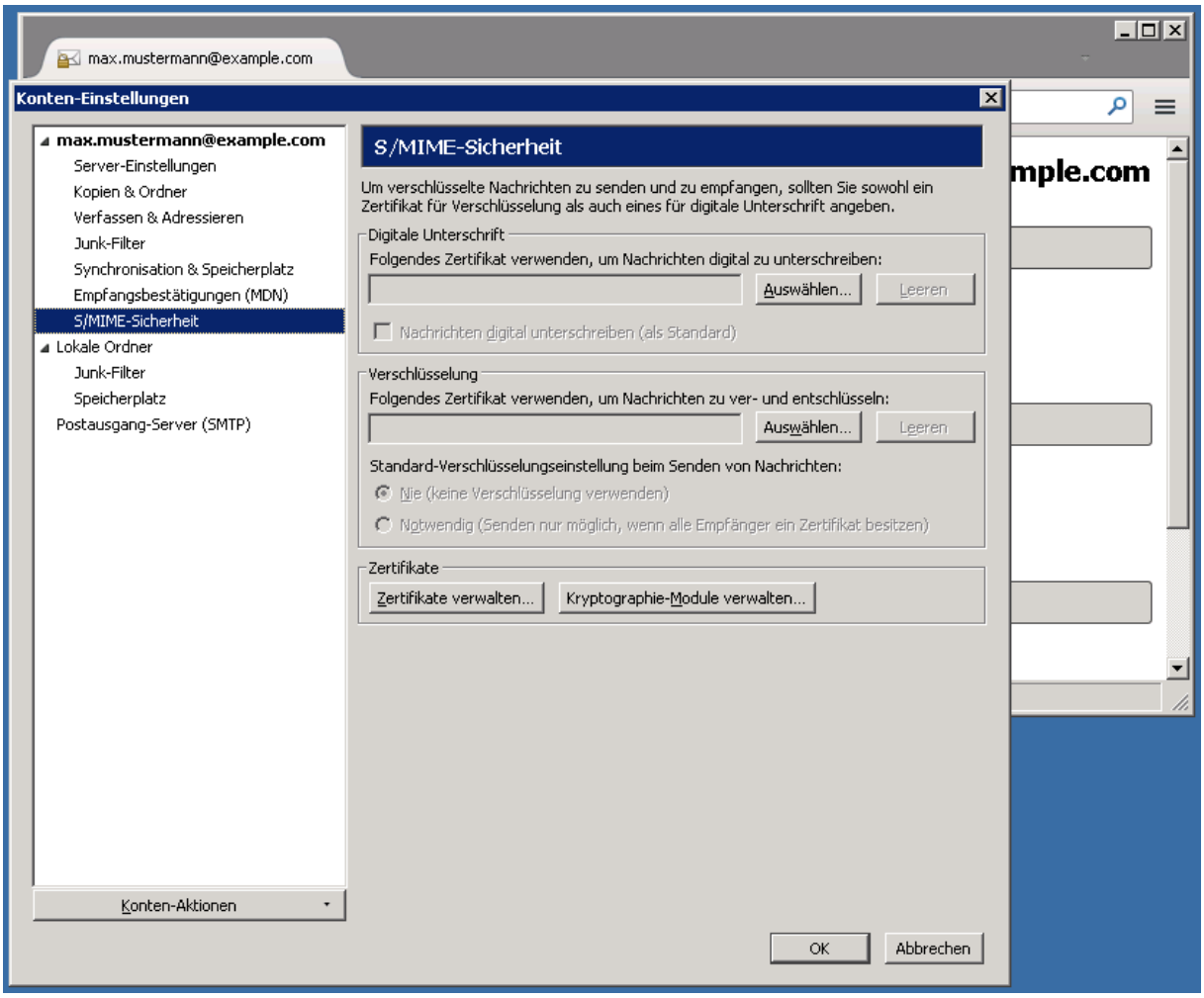

## Einstellen der S/MIME-Sicherheit des Mailkontos

Thunderbird

Jetzt ist die Verknüpfung des Zertifikates mit dem Mailkonto herzustellen. Dazu ist hier das richtige Zertifikat auszuwählen:

*Einstellungen… > Konten-Einstellungen... > **%Kontenname%** > S/MIME-Sicherheit*

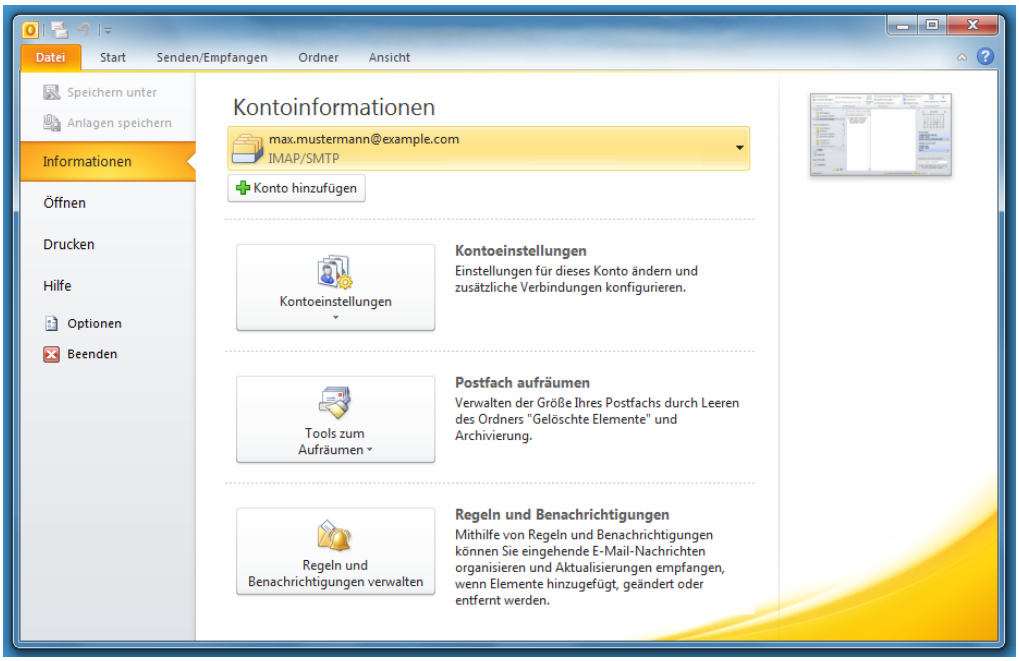




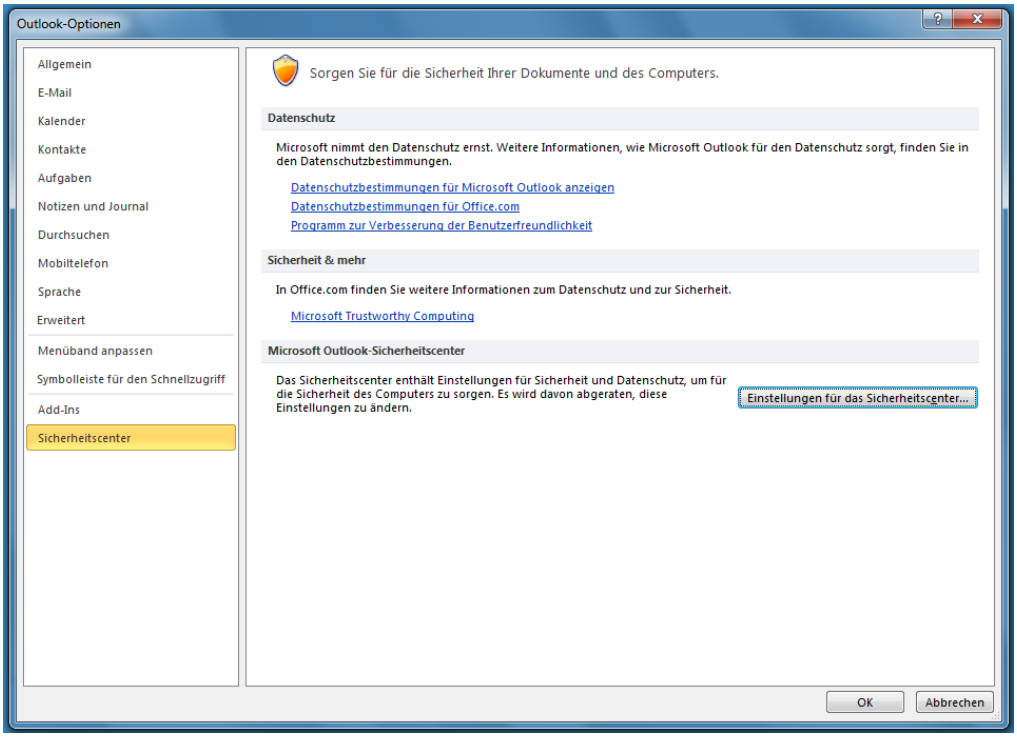

Das Zertifikat ist sowohl für die „Digitale Unterschrift“ (Signatur) als auch für die „Verschlüsselung“ auszuwählen. Die standardmäßige Anwendung der digitalen Unterschrift bei allen Nachrichten ist empfohlen, die standardmäßige Anwendung der Verschlüsselung nur dann, wenn von allen Adressaten ein Zertifikat vorhanden ist.

Outlook 2010

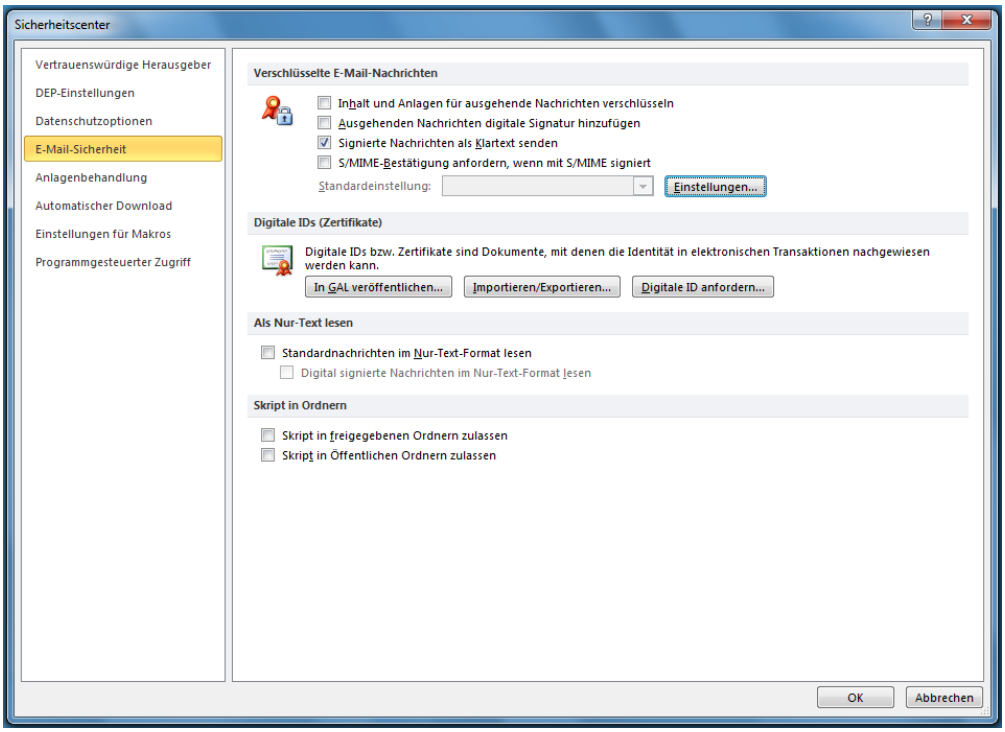
In Outlook klicken Sie auf den orangen „Datei“ Reiter oben links. Klicken Sie anschließend linker Hand auf „Optionen“.



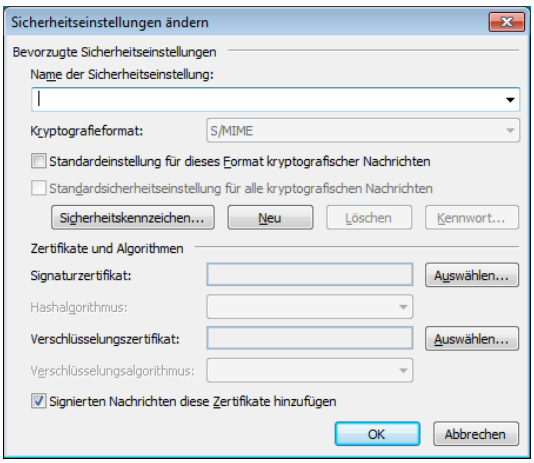

Das Dialog-Fenster „Outlook-Optionen“ öffnet sich. Klicken Sie linker Hand auf „Sicherheitscenter“. Danach klicken Sie rechter Hand auf „Einstellungen für das Sicherheitscenter“.




Das Fenster „Sicherheitscenter“ öffnet sich. Wählen Sie links in der Liste den Punkt „E-Mail-Sicherheit“. Um die Standardeinstellungen festzulegen, klicken Sie auf „Einstellungen“.




Das Fenster „Sicherheitseinstellungen ändern“ öffnet sich. Im Feld „Name der Sicherheitseinstellung“ tragen Sie nun einen beliebigen Namen ein. Als nächstes wählen Sie das Signaturzertifikat aus, klicken Sie dazu auf „Auswählen“ in der Zeile Signaturzertifikat. Wählen Sie nun Ihr Zertifikat aus und bestätigen mit ok. Wiederholen Sie nun den Vorgang für das Verschlüsselungszertifikat. Klicken Sie danach auf „OK“ um die Konfiguration abzuschließen.




## Installation der Zertifikate der Adressaten

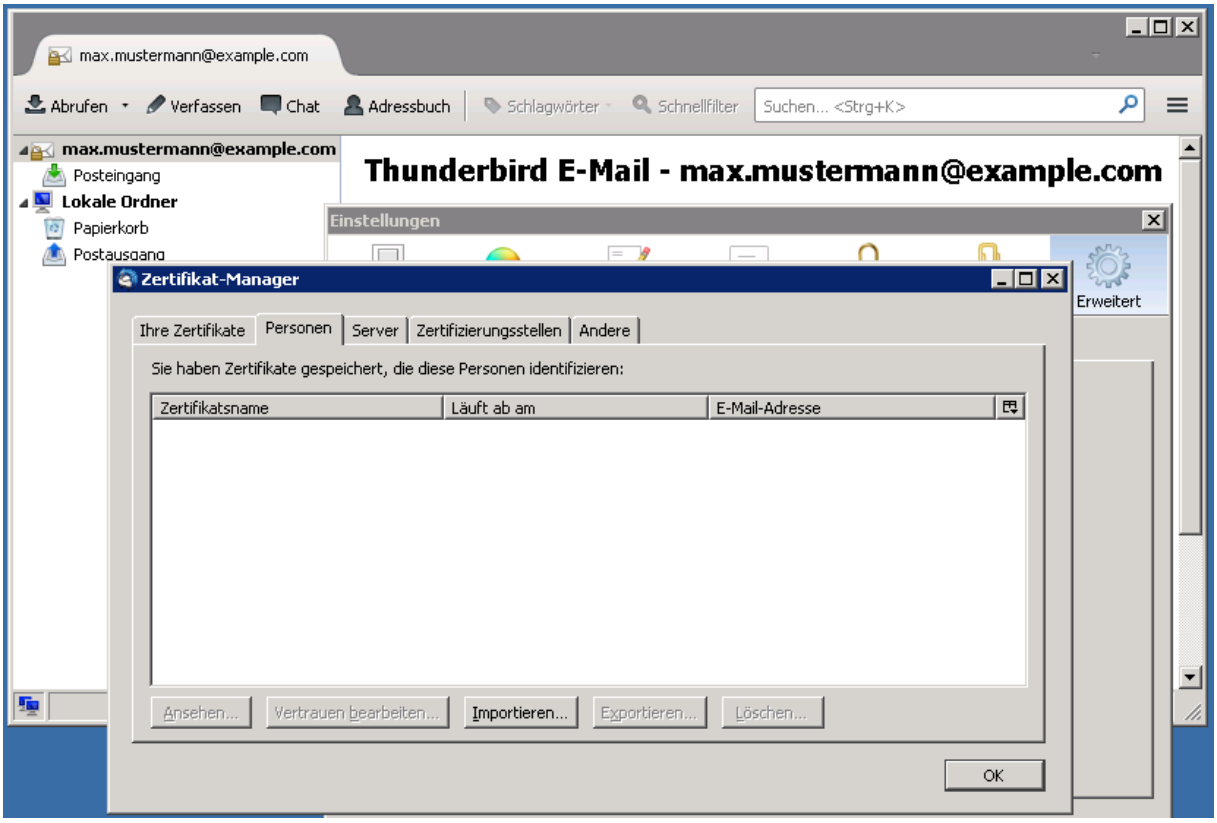
Um Nachrichten an einen Adressaten verschlüsseln zu können, ist die Installation seines Zertifikates erforderlich. Beim Öffnen einer vom diesem Adressaten signierten E-Mail erfolgt die Installation automatisch, aber auch hier ist das Aussprechen des Vertrauens notwendig.

Analog zu dem eigenen Zertifikat, ist auch hier zu nächst die Installation der Ausstellerzertifikate von Nöten (siehe „Installation der erforderlichen Ausstellerzertifikate“).

Thunderbird

Zur Installation des Zertifikats des Adressaten wählen Sie:

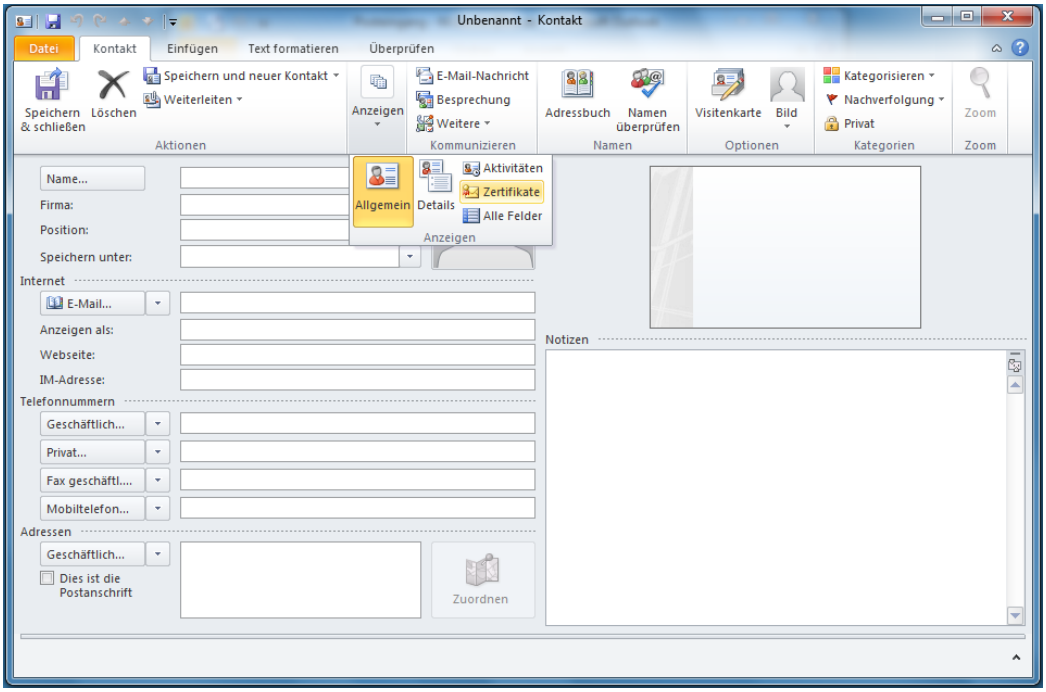
*Einstellungen... > Einstellungen… > Zertifikate > Zertifikate > Personen*



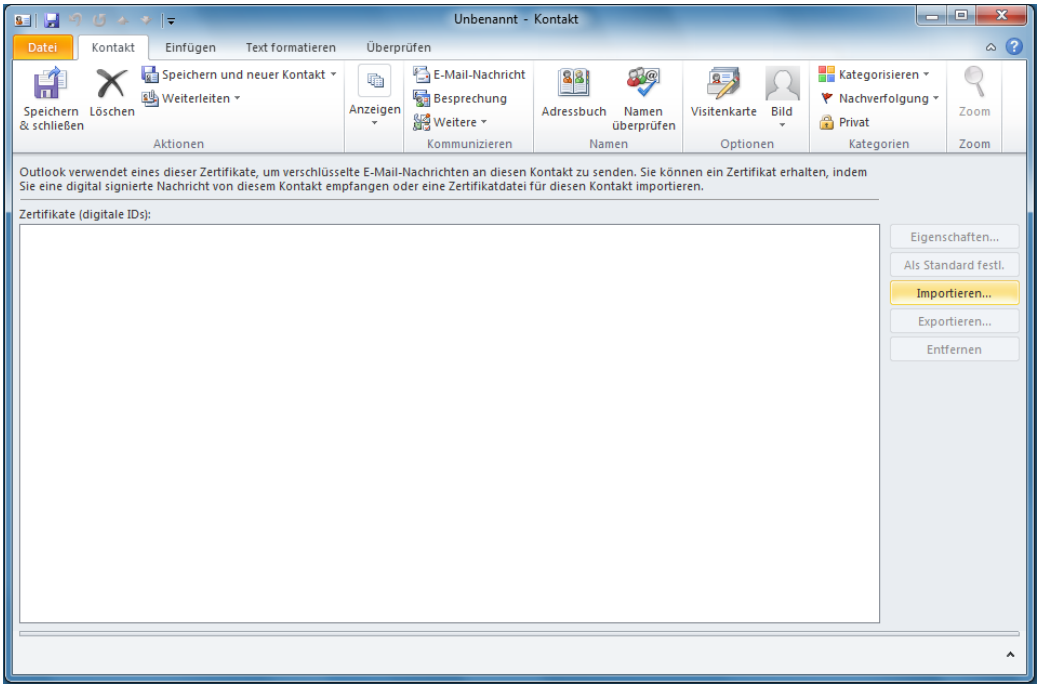

Klicken Sie auf „Importieren“ und wählen Sie das Zertifikat des Adressaten aus.

Outlook 2010

Erstellen Sie einen neuen „Kontakt“ in Outlook indem Sie den Reiter „Start“ auswählen und auf „Neue Elementen“ klicken und dabei „Kontakt“ wählen. Im folgenden Dialogfenster „Kontakt“ klicken Sie auf „Anzeigen“ und wählen „Zertifikate“.



Klicken  Sie nun auf „Importieren“ und wählen anschließend das Zertifikat des Adressaten aus und bestätigen mit „OK“.




Klicken Sie anschließend wieder auf „Anzeigen“ und wählen dann „Allgemein“ aus. Vervollständigen Sie nun die Angaben zu Ihrem E-Mail Kontakt (Name, E-Mail, usw.).

X.509-Zertifikat

### X.509

X.509 ist ein Standardformat der ITU-T (International Telecommunication Union-Telecommunication) für Zertifikate. Es beinhaltet den Namen des Ausstellers, üblicherweise eine Certification Authortity, Informationen über die Identität des Inhabers sowie die digitale Signatur des Ausstellers und den Gültigkeitszeitraum des Zertifikates. Auf dem X.509-Format basieren z. B. SSL und S/MIME.

X.509-Zertifikate für Einzelpersonen werden in folgenden Klassen herausgegeben:

### Class 0

Class 0-Zertifikate (Demo-Zertifikate) sind für Testzwecke gedacht und mit beschränkter Gültigkeitsdauer.

### Class 1

Class 1-Zertifikate bestätigen, dass die angegebene E-Mail-Adresse existiert und der Besitzer des zugehörigen öffentlichen Schlüssels Zugriff auf diese E-Mail-Adresse hat. Sie stellen damit nur einen sehr geringen Nachweis der Identität dar. Da keine Überprüfung anhand von Unterlagen stattfindet, können Class 1-Zertifikate (Express-Zertifikat) binnen weniger Minuten ausgestellt und an den Kunden ausgeliefert werden. Sie sind ideal für private Nutzer, die erste Schritte auf dem Weg zur

sicheren Internet-Kommunikation gehen wollen und den Umgang mit verschlüsselter E-Mail ausprobieren möchten, und sie werden von den meisten Trustcentern kostenlos herausgegeben.

### Class 2

Bei Class 2-Zertifikaten für Unternehmen wird auf eine persönliche Identitätsfeststellung verzichtet. Eine einfache Kopie des Handelsregisterauszuges zur Feststellung der zeichnungsberechtigten Person und ein schriftlicher Auftrag sind ausreichend. Diese Zertifikate sind hauptsächlich für die gesicherte Kommunikation zwischen einander bereits außerhalb des Internets bekannten Partnern gedacht.

### Class 3

Class 3 beinhaltet neben der E-Mail-Überprüfung eine persönliche Identitätsprüfung der Person. Mit der Ausstellung eines Class 3-Zertifikats bestätigt das Trustcenter, dass diese Person anhand ihres Personalausweises oder Reisepasses identifiziert worden ist und die im Zertifikat enthaltenen Angaben zur Person mit den Angaben im Ausweis übereinstimmen. Diese Zertifikate sind vor allem für Anwendungen im E-Commerce gedacht, wie beispielsweise Internet Banking und Online Shopping. Sie werden aber auch zunehmend für die elektronische Kommunikation mit Behörden eingesetzt (Übermittlung Steuerdaten und zukünftig elektronische Antragstellung).

## Certificate Authority (CA)?

Eine Zertifizierungsstelle (engl. Certificate Authority, kurz CA) ist eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat ist gewissermaßen das Cyberspace-Äquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie diese mit ihrer eigenen digitalen Unterschrift versieht. Die Zertifikate enthalten "Schlüssel" und Zusatzinformationen, die zur Authentifizierung sowie zur Verschlüsselung und Entschlüsselung sensitiver oder vertraulicher Daten dienen, die über das Internet und andere Netze verbreitet werden. Als Zusatzinformationen sind zum Beispiel Lebensdauer, Verweise auf Sperrlisten etc. enthalten, die durch die CA mit in das Zertifikat eingebracht werden.

Zunehmend bieten auch Banken und Sparkassen ihren Kunden qualifizierte Zertifikate auf Chipkarten an. Zertifikate werden durch die CA je nach Anforderung als Hardwaretoken (auf Chipkarte) oder als Softwarezertifikat herausgegeben. Für die außerordentlich hohen Anforderungen der so genannten „qualifizierten Signatur“ (Class 3) sind ausschließlich Hardwaretoken und die entsprechenden Kartenleser zugelassen.

Die für private Nutzung meist ausreichenden Class 1-Zertifikate werden dem Antragsteller als Softwaretoken übergeben. Beispiele für Trustcenter sind: http://www.trustcenter.de/, https://www.startssl.com

Selbstverständlich gibt es auch die Möglichkeit, X.509-Zertifikate speziell für geschlossene Nutzergruppen (Familie, Freunde, Forum, Firmen ...) selbst zu produzieren.

Ein ausgezeichnetes Werkzeug dafür ist das als Linux- und auch als Windowsversion erhältliche Freewareprogramm "XCA". http://xca.sourceforge.net/ Dieses Programm besticht nicht nur durch ein logisches Bedienkonzept, sondern auch durch die Möglichkeit, für alle gängigen Anwendungsfälle

Vorlagen zu erstellen. Selbstverständlich ist auch die Erstellung von Sperrlisten möglich und die produzierten Zertifikate lassen sich in allen gängigen Formaten exportieren.

### kostenloses X.509-Zertifikat (Class 1)?

Beispielsweise hier: trustcenter.de, StartSSL Free, Free Secure Email Certificate (Comodo)

## Qualifizierte elektronische Signatur

### Voraussetzungen

- Komfort Kartenlesegerät
- elektronische Signaturkarte
- Prüfsystem-/software
- Archiv