

Mozilla Thunderbird

Zertifikat installieren, Signieren, Verschlüsseln E-Mail, LDAP-Verzeichnisdienst V1.2

Inhalt

1 Grundlagen	2
1.1 Ziele des Dokuments	2
1.2 Definitionen und Kurzbezeichnungen	2
1.3 Änderungshistorie	2
1.3.1 V1.1 Stammfassung	2
1.3.2 V1.2 Ergänzung	2
2 Kurzfassung	3
3 Detail Dokumentation Zertifikatsverwaltung	4
3.1 Zertifikate installieren	4
3.1.1 GLOBALTRUST Root-CA Zertifikat importieren	4
3.1.2 Thunderbird Einstellungen öffnen	5
3.1.3 Zertifikat für Signieren installieren	7
3.1.3.1 Import Software-Zertifikate	7
3.1.3.2 Import E-Token Zertifikat Safenet (vormals Aladdin)	9
3.2 Zertifikate für Signieren einrichten	11
3.2.1 Nachricht erstellen und signiert versenden	12
3.3 E-Mail verschlüsseln	14
3.3.1 Empfänger Zertifikat importieren	14
3.3.2 Neue E-Mail verfassen + verschlüsseln	15
3.4 Signierte/Verschlüsselte E-Mails empfangen	16
3.4.1 Empfangene E-Mail öffnen	16
3.4.2 Signatur prüfen	16
3.4.3 Zertifikat Details anzeigen	17
4 Mozilla Thunderbird 31 LDAP Adressbuch	17
4.1 Kurzfassung LDAP-Installation	3
4.2 Deatildokumentation LDAP	18
4.2.1 Adressbuch öffnen	18
4.2.2 Serverdaten eingeben	19
4.2.3 Nach Einträgen suchen	19
5 Abbildungen	20

1 GRUNDLAGEN

1.1 ZIELE DES DOKUMENTS

Das Ziel dieses Dokuments ist es in einer Schritt-für-Schritt Anleitung zu zeigen, wie Zertifikate in Thunderbird installiert werden können, E-Mails signiert und verschlüsselt werden und wie, empfangene, signierte und verschlüsselte E-Mails gelesen werden.

1.2 DEFINITIONEN UND KURZBEZEICHNUNGEN

S/MIME:

- Standard zur Signierung und Verschlüsselung von E-Mails.
- **LDAP:** Ist die Abkürzung für „Lightweight Directory Access Protocol“ und ermöglicht es über ein IP-Netzwerk (z.B. Internet) auf einen Verzeichnisdienst zugreifen zu können. Das Verzeichnis kann etwa, wie in dieser Anleitung, ein Adressbuch sein.

1.3 ÄNDERUNGSHISTORIE

1.3.1 V1.1 STAMMFASSUNG

Redaktionsschluss: 5. Juni 2015

1.3.2 V1.2 ERGÄNZUNG

Redaktionsschluss: 3. Juli 2019

2 KURZFASSUNG

Zertifikat installieren:

- Root Zertifikat von <https://www.globaltrust.eu> herunterladen
- Im Zertifikat-Manager von Thunderbird im Tab „Zertifizierungsstellen“ die crt-Datei importieren
- Im Tab „Ihre Zertifikate“ das persönliche Zertifikat importieren (⇒ 3.1.3 Zertifikat für Signieren installieren p7)
- In den Kontoeinstellungen unter der Kategorie „S/MIME Sicherheit“ das Zertifikat zum signieren auswählen. ⇒ Fertig

E-Mail signieren:

- Neue E-Mail verfassen
- In der Menüleiste „S/MIME“ auswählen und „Nachricht unterschreiben“ auswählen. Rechts unten im Eck erscheint ein Symbol eines versiegelten Kuverts ⇒ Fertig

E-Mail verschlüsseln:

- Zertifikat-Manager öffnen und im Tab „Personen“ das Zertifikat des Empfängers importieren
- Neue E-Mail verfassen und in der Menüleiste „S/MIME“ auswählen und „Nachricht verschlüsseln“ auswählen. Rechts unten im Eck erscheint ein Vorhängeschloss Symbol ⇒ Fertig

Signierte/Verschlüsselte E-Mails empfangen:

- E-Mail mit Doppelklick öffnen
- Rechts oben sind das versiegelte Kuvert und, wenn die Nachricht auch verschlüsselt wurde, das Vorhängeschloss zu sehen. Bei einem Klick auf eines der Symbole können die Details zum Unterzeichner und zum Zertifikat des Unterzeichners abgerufen werden ⇒ Fertig

Kurzfassung LDAP-Installation

Im Adressbuch im Menü „Datei“ im Unterpunkt „Neu“ das LDAP Verzeichnis wählen
Serverdaten, ohne Anführungszeichen, eintragen:

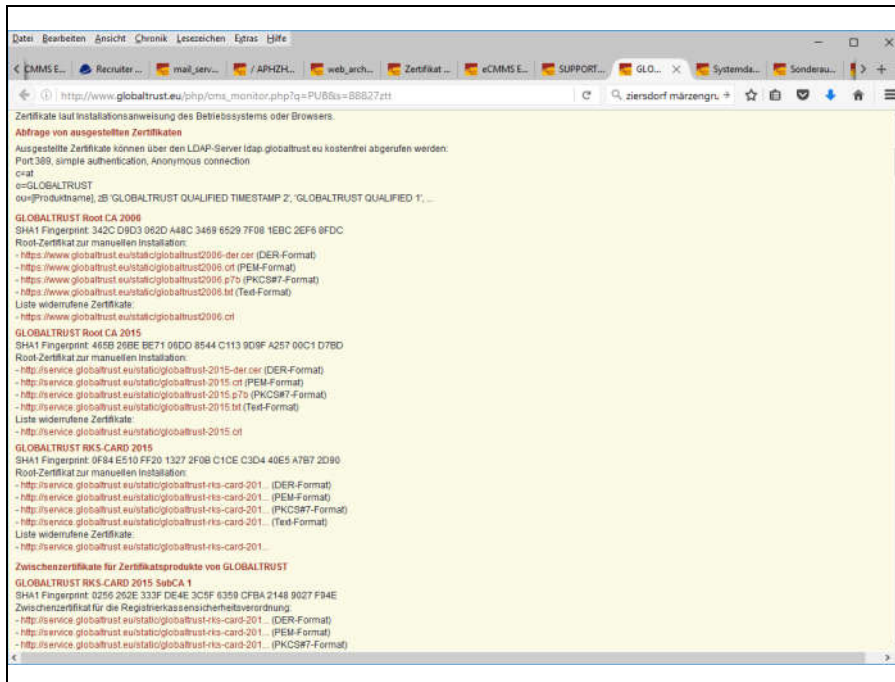
- Name: „GLOBALTRUST“
- Serveradresse: „ldap.globaltrust.eu“
- Basis-DN: „c=at“
- Port-Nummer: „389“

Im Adressbuch links „GLOBALTRUST“ auswählen und rechts oben Suchbegriff eingeben. ⇒ Fertig

3 DETAIL DOKUMENTATION ZERTIFIKATSVERWALTUNG

3.1 ZERTIFIKATE INSTALLIEREN

3.1.1 GLOBALTRUST Root-CA ZERTIFIKAT IMPORTIEREN



Screen 1: Download Root CA

Legende:

- URL <http://www.globaltrust.eu/certificate-policy.html> öffnen
- In den Abschnitten „GLOBALTRUST Root CA 2006“ und „GLOBALTRUST Root CA 2015“ auf die Download-Links für „DER-Format“ klicken und die Datei speichern.

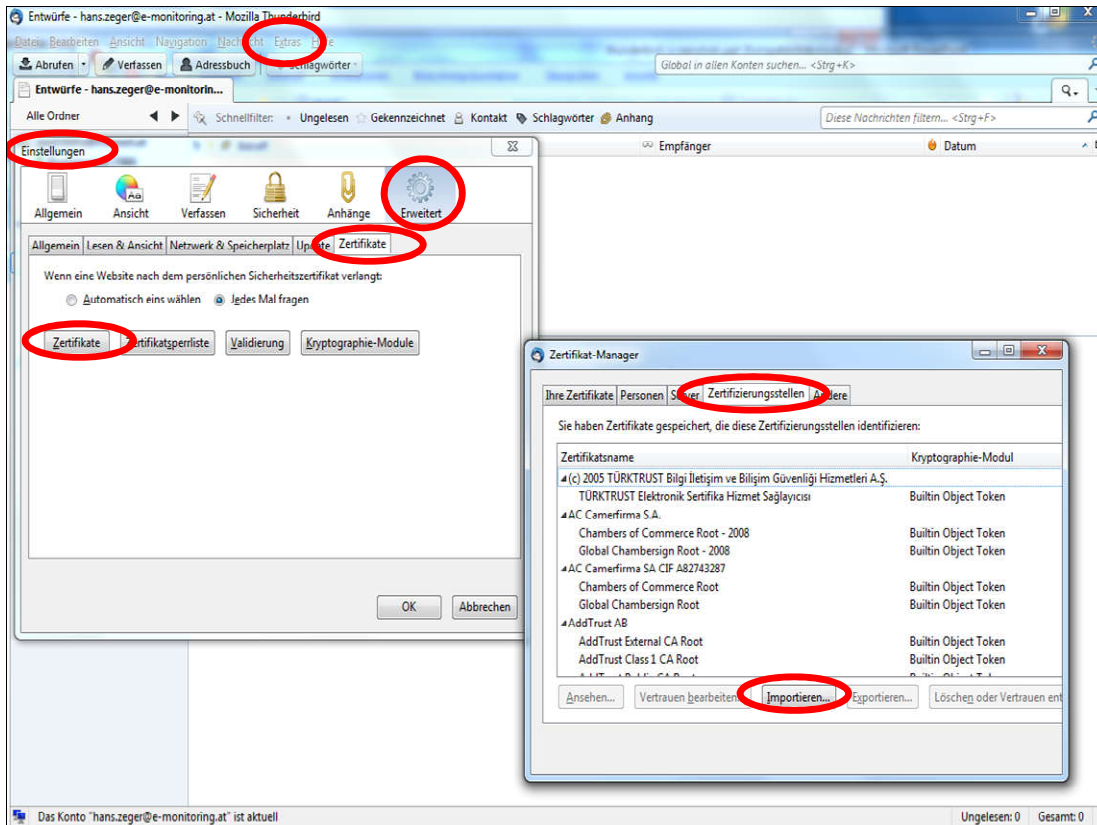
Direktlink der GLOBALTRUST Root-CA Zertifikate:

<http://www.globaltrust.eu/static/globaltrust2006-der.cer>

<http://www.globaltrust.eu/static/globaltrust-2015-der.cer>

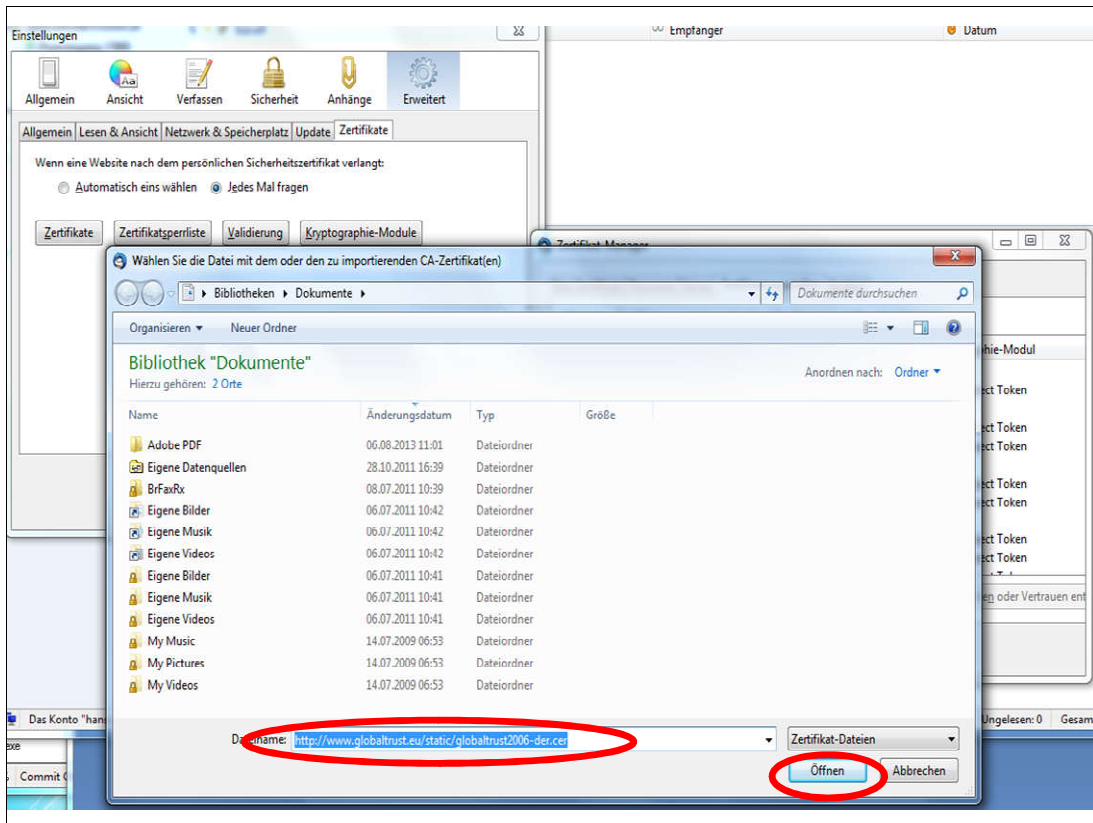
3.1.2 THUNDERBIRD EINSTELLUNGEN ÖFFNEN

⇒ Extras ⇒ Einstellungen ⇒ Erweitert ⇒ Zertifikate ⇒ Zertifikate ⇒ Zertifizierungsstellen ⇒ Importieren



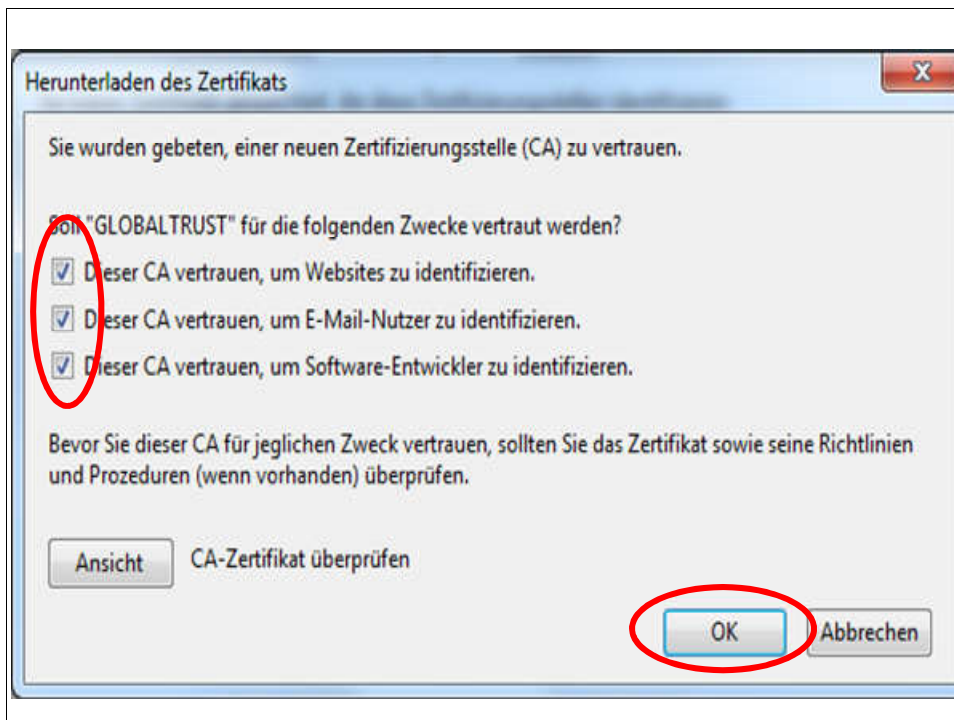
Screen 2: Einstellungen öffnen

⇒ Öffnen



Screen 3: Zertifikat importieren

⇒ alle Zwecke markieren ⇒ OK



Screen 4: Zertifikatseigenschaften festlegen

offene Fenster: ⇒ **Zertifikats-Manger** ⇒ **Einstellungen** schließen

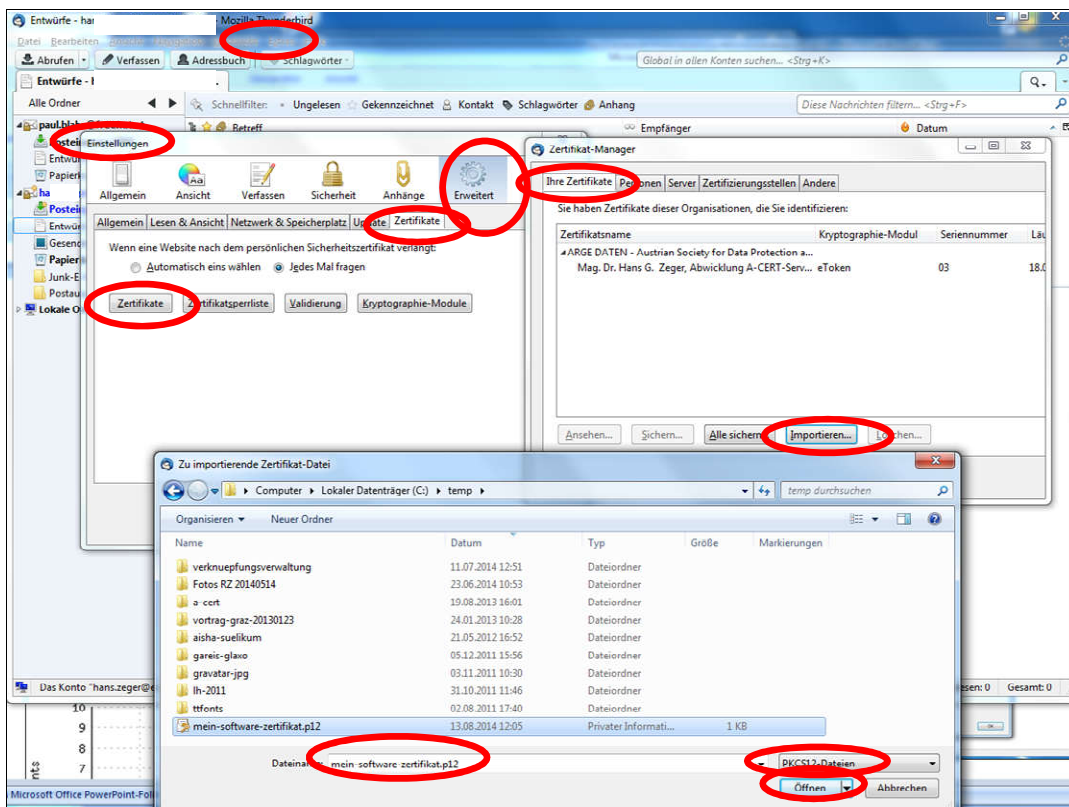
Das GLOBALTRUST Root-CA Zertifikat ist installiert.

3.1.3 ZERTIFIKAT FÜR SIGNIEREN INSTALLIEREN

3.1.3.1 IMPORT SOFTWARE-ZERTIFIKATE

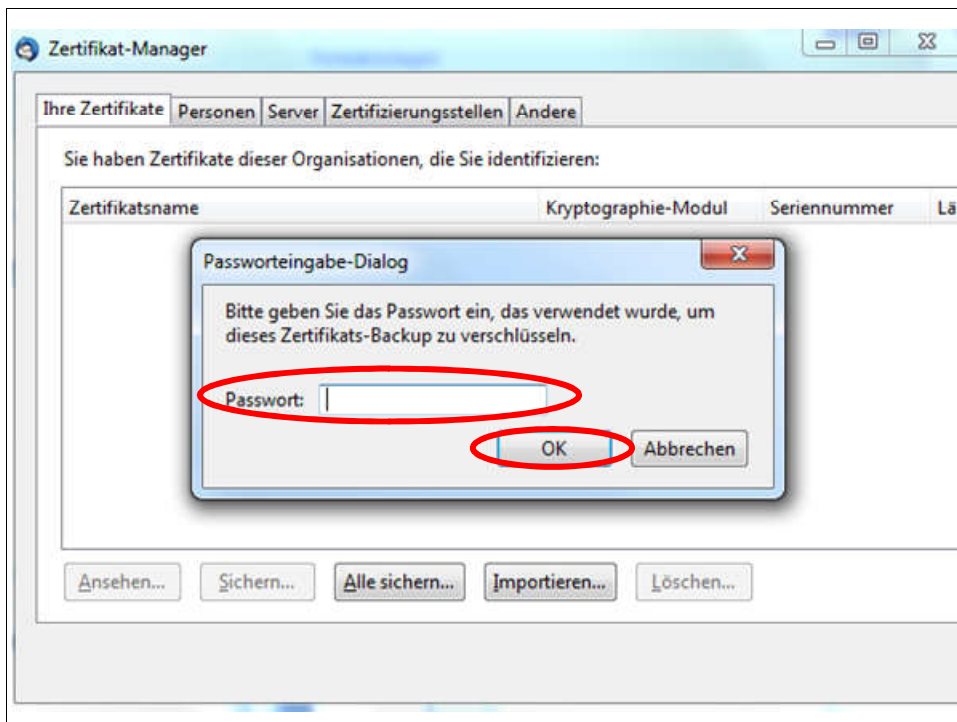
Software-Zertifikate + Schlüssel können durch Import der PKCS#12-Datei genutzt werden.

⇒ Extras ⇒ Einstellungen ⇒ Erweitert ⇒ Zertifikate ⇒ Zertifikate ⇒ Ihre Zertifikate ⇒ Importieren ⇒ Verzeichnis auswählen (hier C:\temp) ⇒ Dateityp PKCS12-Dateien auswählen ⇒ geeignete PKCS#12-Datei auswählen (hier Dateiname: mein-software-zertifikat.p12) ⇒ Öffnen



Screen 5: Eigenes Zertifikat installieren

⇒ **Passworteingabe-Dialog** ⇒ **Passwort:** Ihr vergebenes PKCS#12-Passwort ⇒ **OK**



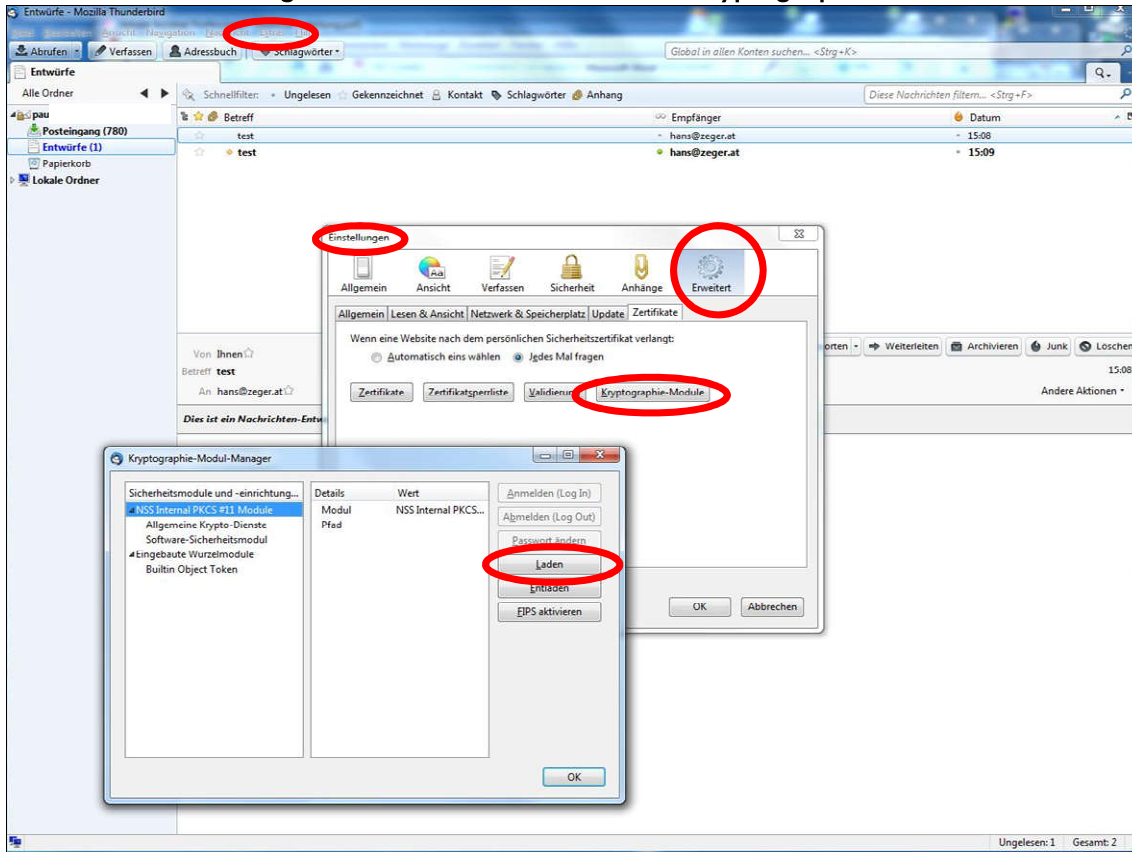
Screen 6: Passwort vergeben

Ihr Software-Zertifikat + Schlüssel sind installiert!

3.1.3.2 *IMPORT E-TOKEN ZERTIFIKAT SAFENET (VORMALS ALADDIN)*

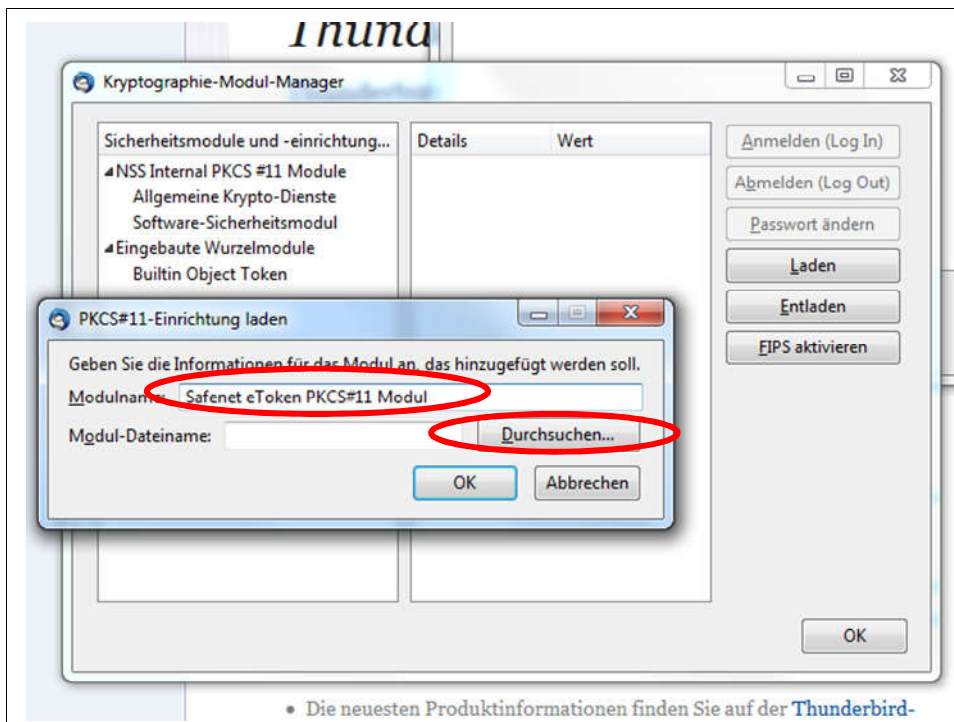
Zertifikate auf externen Trägern (Smartcards, eToken) können über eine PKCS#11 Schnittstelle angesprochen/genutzt werden. Das Modul zu dieser PKCS#11-Schnittstelle muss in Thunderbird übernommen werden.

⇒ Extras ⇒ Einstellungen ⇒ Erweitert ⇒ Zertifikate ⇒ Kryptographie-Module ⇒ Laden



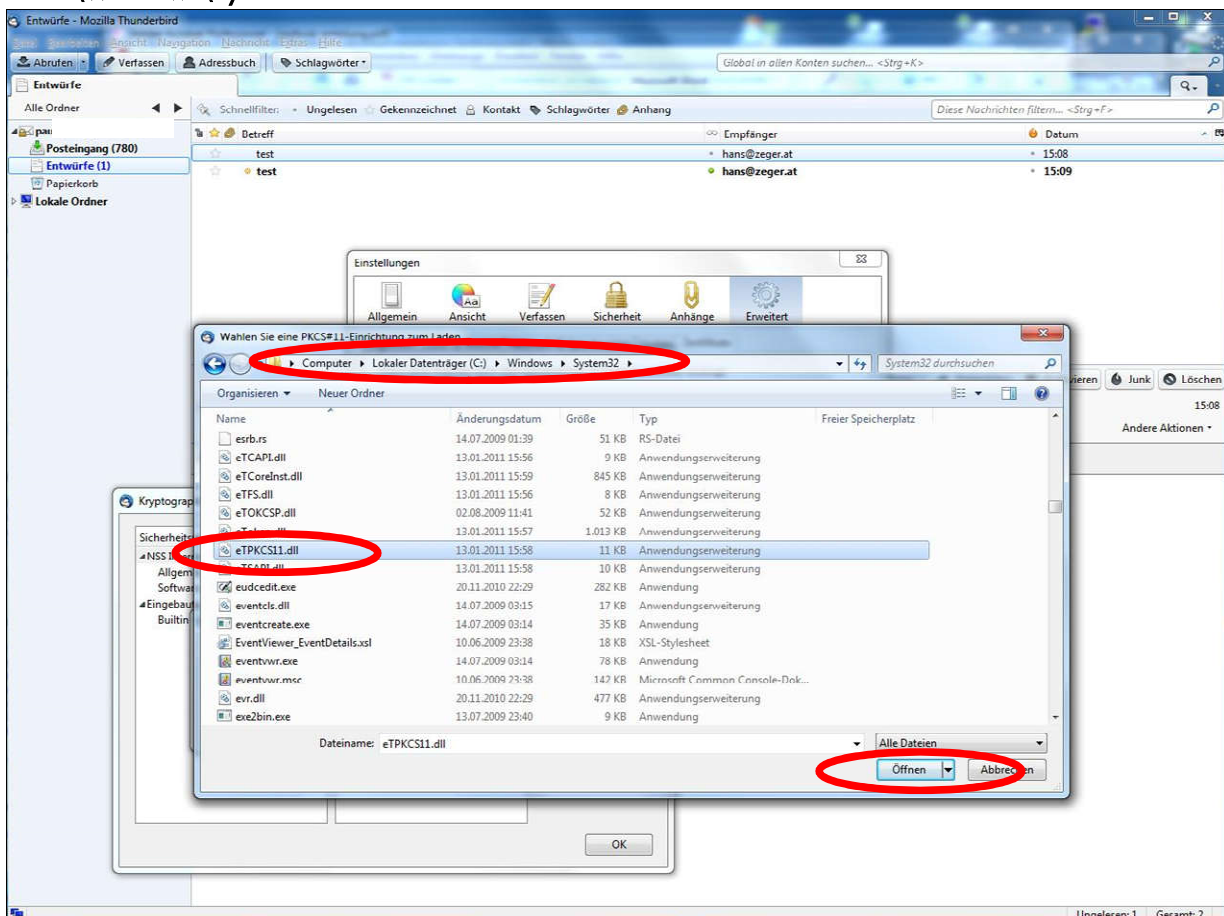
Screen 7: Kryptographie-Modul installieren I

⇒ geeigneten **Modulname** vergeben, Empfehlung: Safenet eToken PKCS#11 Modul ⇒ **Durchsuchen**

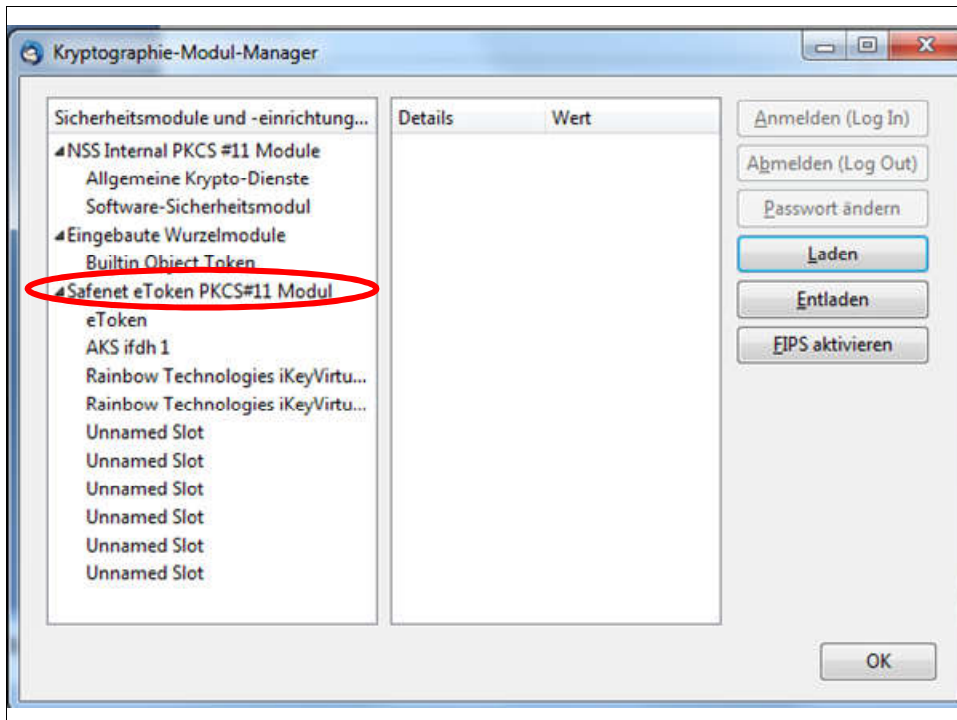


Screen 8: Kryptographie-Modul installieren II

⇒ C:\Windows\System32 ⇒ Datei **eTPKCS11.dll** auswählen ⇒ **Öffnen**



Screen 9: Kryptographie-Modul installieren III

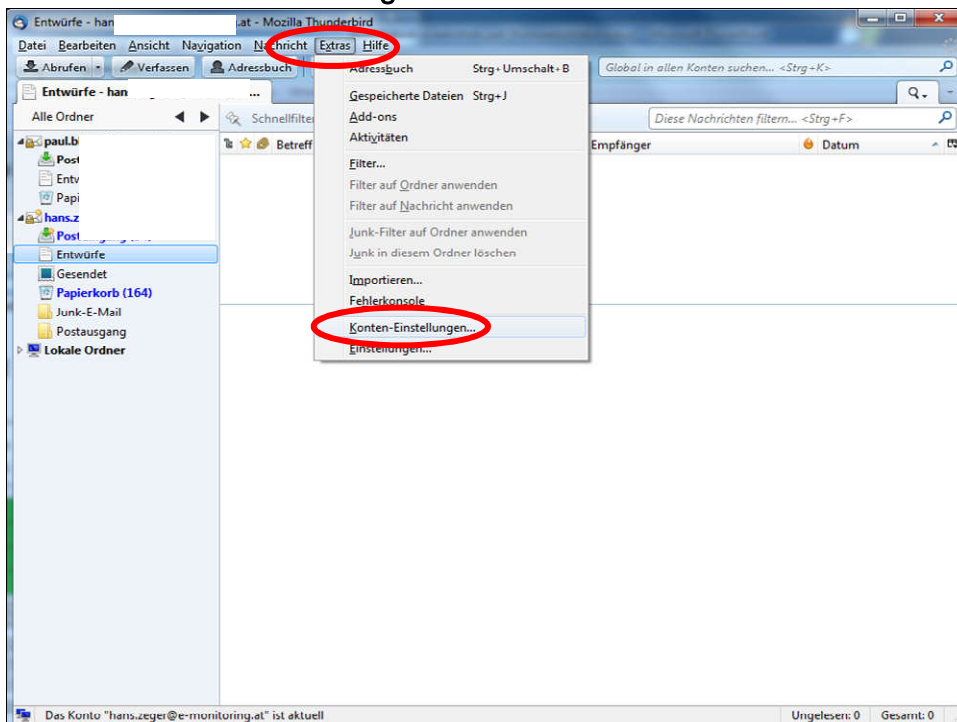


Screen 10: Kryptographie-Modul installieren IV

Safenet-E-Token ist für signieren / verschlüsseln vorbereitet!

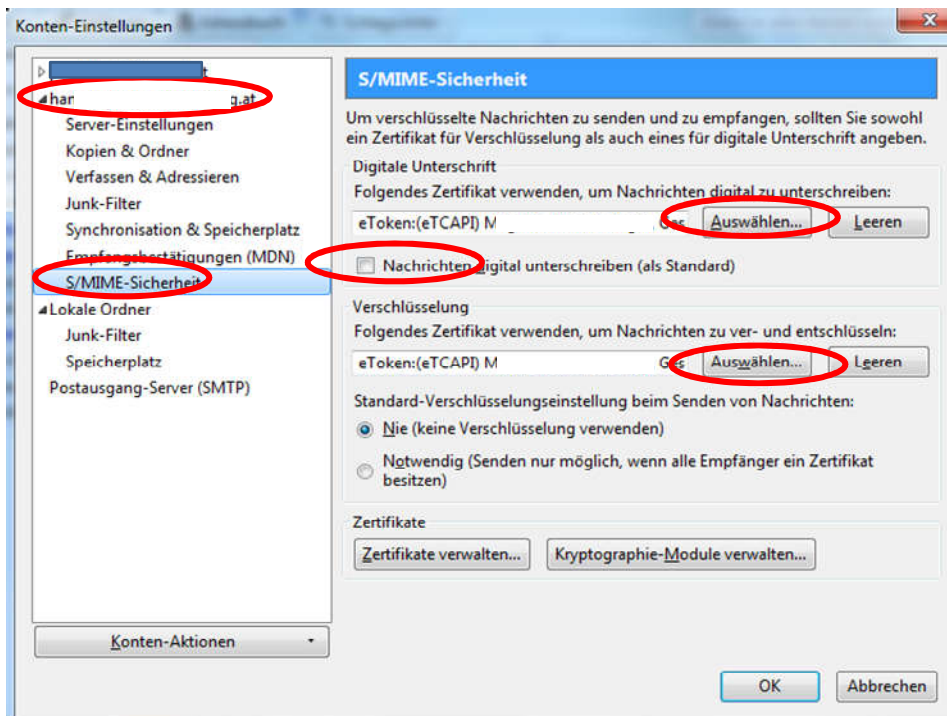
3.2 ZERTIFIKATE FÜR SIGNIEREN EINRICHTEN

⇒ Extras ⇒ Konten-Einstellungen



Screen 11: eMail-Konto auswählen

⇒ Benutzerkonto auswählen Beispiel: **hanxxxx@xxx.at** ⇒ **S/MIME-Sicherheit** ⇒ **Auswählen** (Zertifikat für Unterschriften) + **Auswählen** (Zertifikat für Verschlüsseln Hinweis! Hier muss das Empfängerzertifikat ausgewählt werden, nicht das eigene, da ansonsten der Empfänger die E-Mail nicht entschlüsseln kann!)

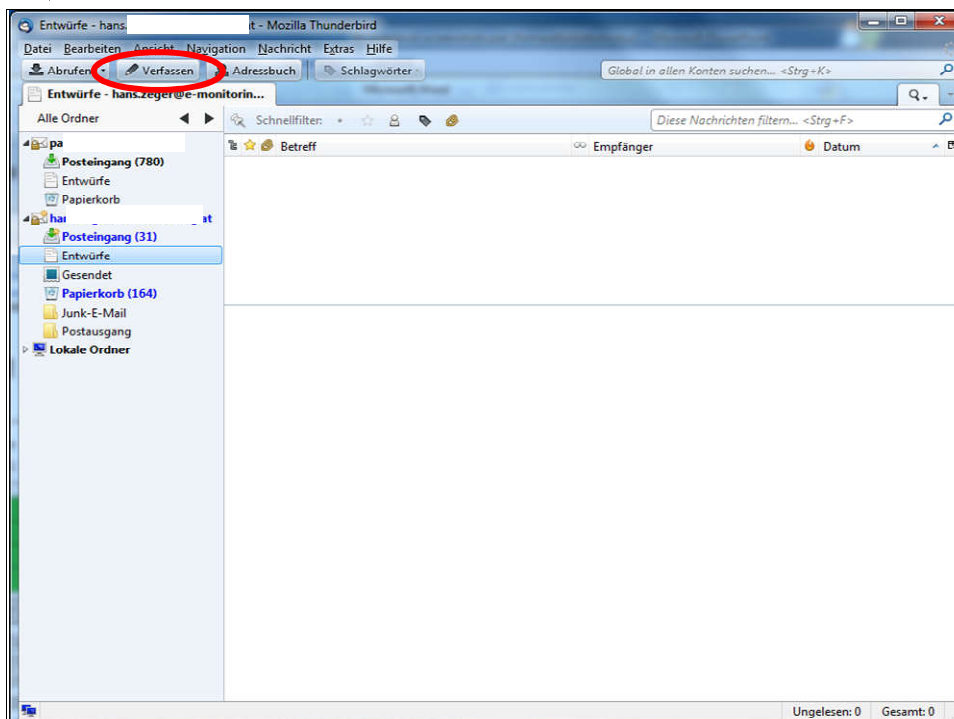


Screen 12: Einstellungen konfigurieren

Optional: ⇒ **Nachrichten digital unterschreiben** auswählen, dann wird immer unterschrieben

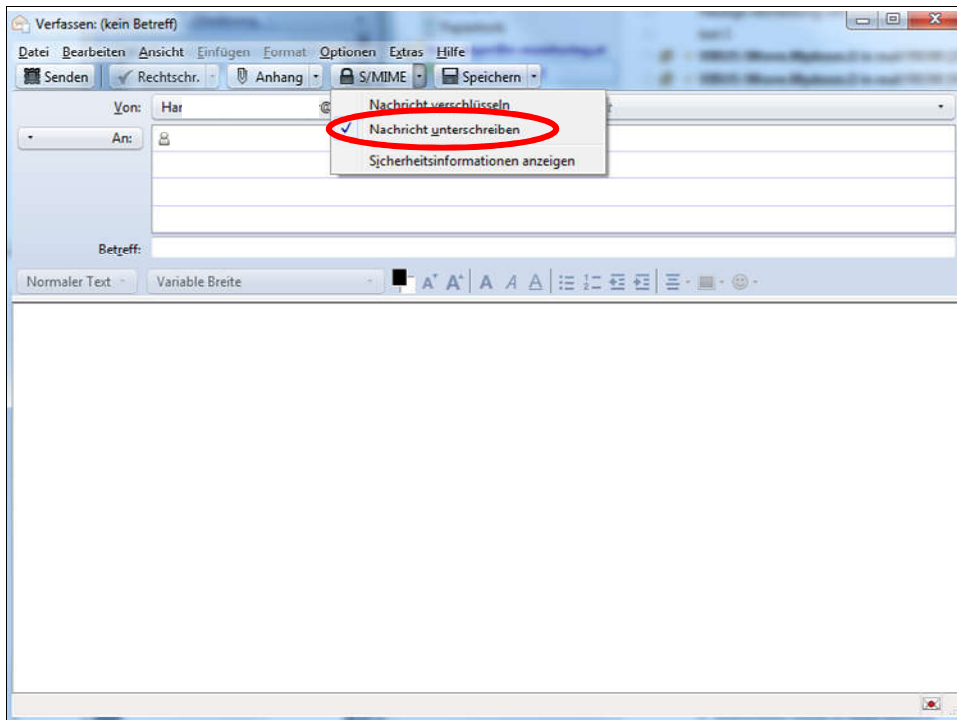
3.2.1 NACHRICHT ERSTELLEN UND SIGNIERT VERSENDEN

⇒ Verfassen



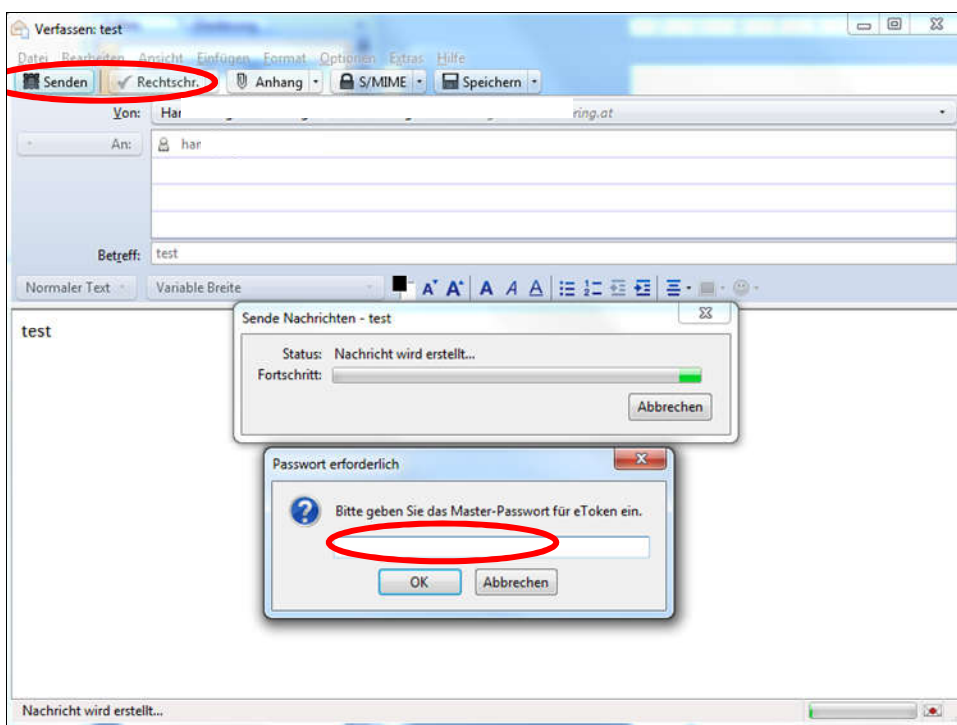
Screen 13: Nachrichten verfassen und signieren I

⇒ S/MIME ⇒ Nachricht unterschreiben



Screen 14: Nachrichten verfassen und signieren II

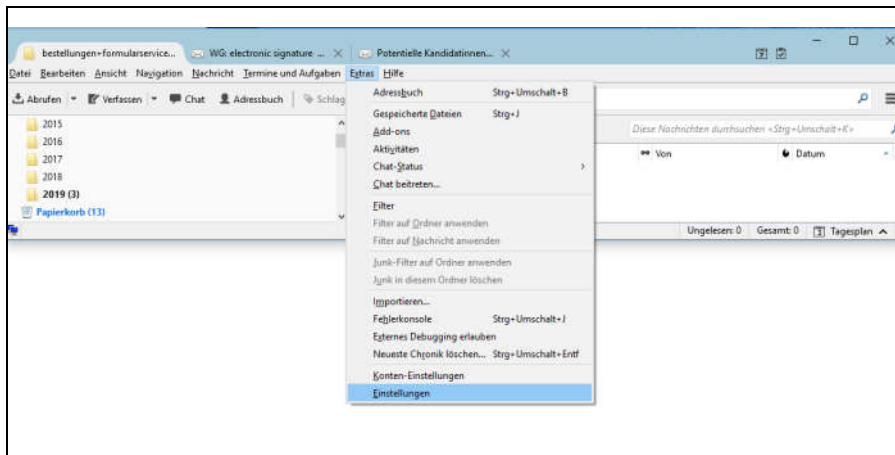
⇒ **senden** ⇒ es erfolgt die Aufforderung zur Eingabe des eToken-Passwortes (nur bei einem E-Token-Zertifikat), ansonsten wird nach dem Passwort des Software-Zertifikates gefragt



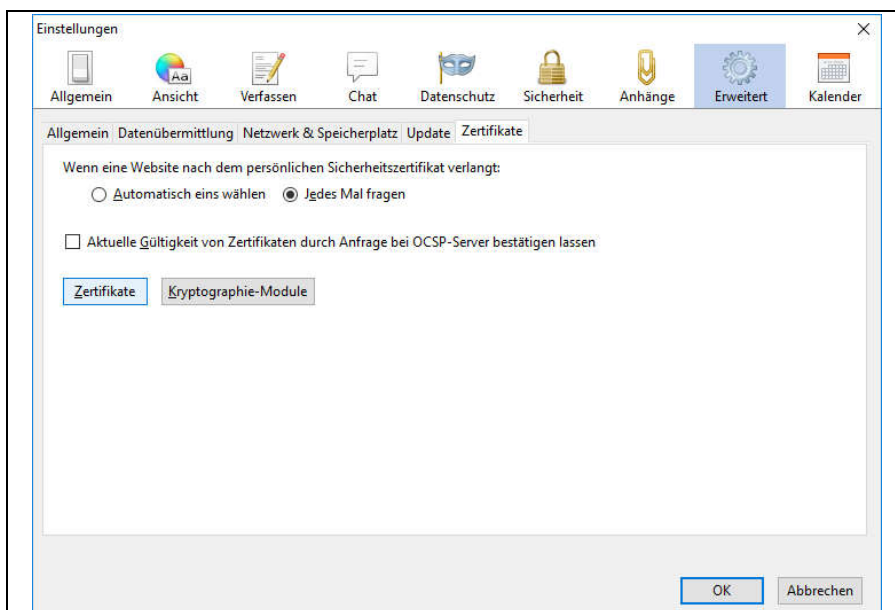
Screen 15: Nachrichten verfassen und signieren III

3.3 E-MAIL VERSCHLÜSSELN

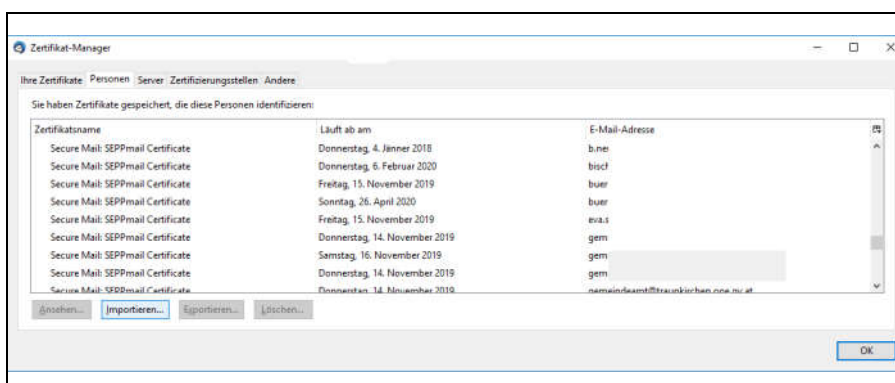
3.3.1 EMPFÄNGER ZERTIFIKAT IMPORTIEREN



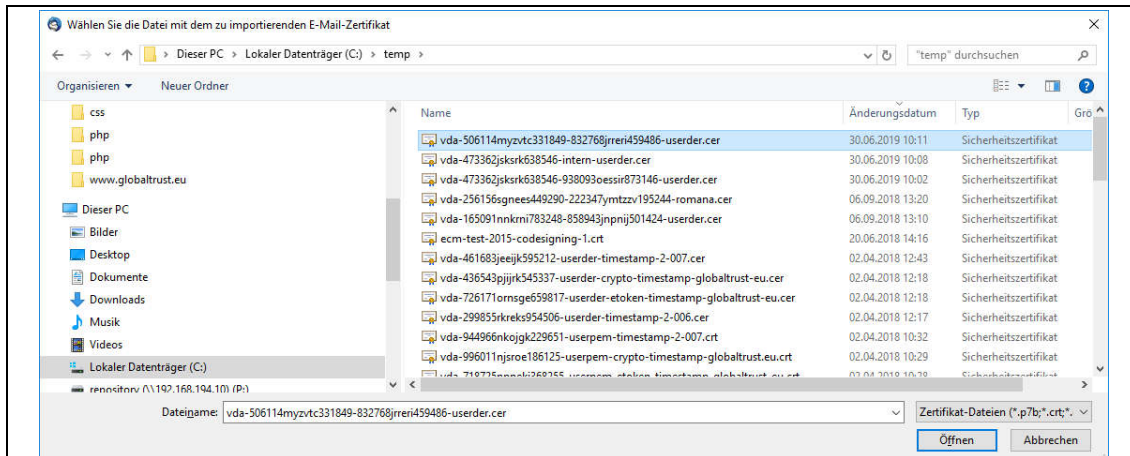
Screen 16: Empfänger Zertifikat importieren I



Screen 17: Empfänger Zertifikat importieren II



Screen 18: Empfänger Zertifikat importieren III

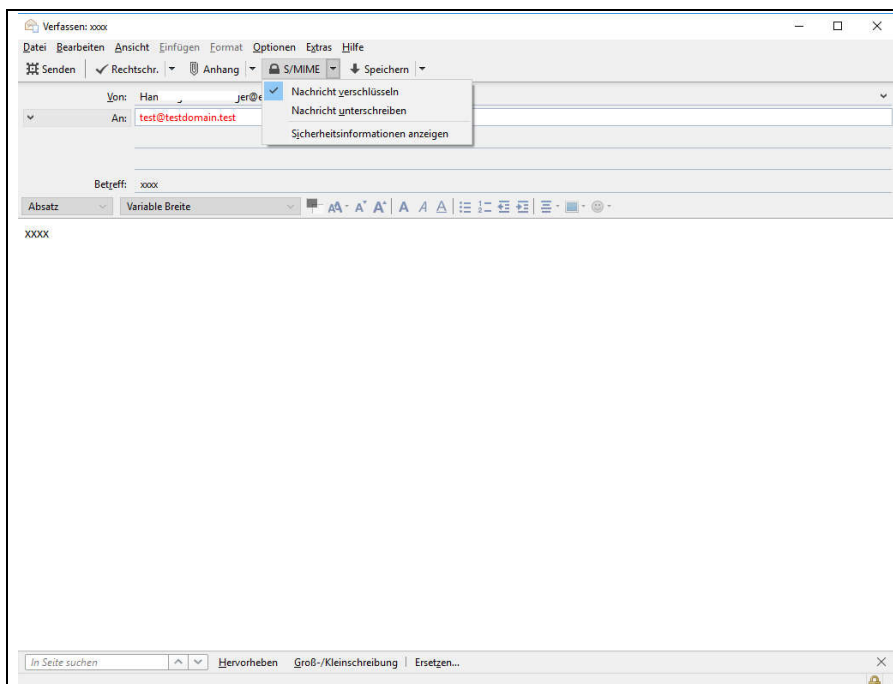


Screen 19: Empfänger Zertifikat importieren

"Öffnen" ⇒ OK ⇒ OK ⇒ fertig

3.3.2 NEUE E-MAIL VERFASSEN + VERSCHLÜSSELN

Im Hauptfenster links oben auf „Verfassen“ klicken



Screen 20: Neue E-Mail verfassen + verschlüsseln

Hinweis I:

"Nachricht verschlüsseln" ist nur möglich, wenn das Zertifikat der Empfänger-Mailadresse installiert ist (hier: **test@testdomain.test**).

Hinweis II:

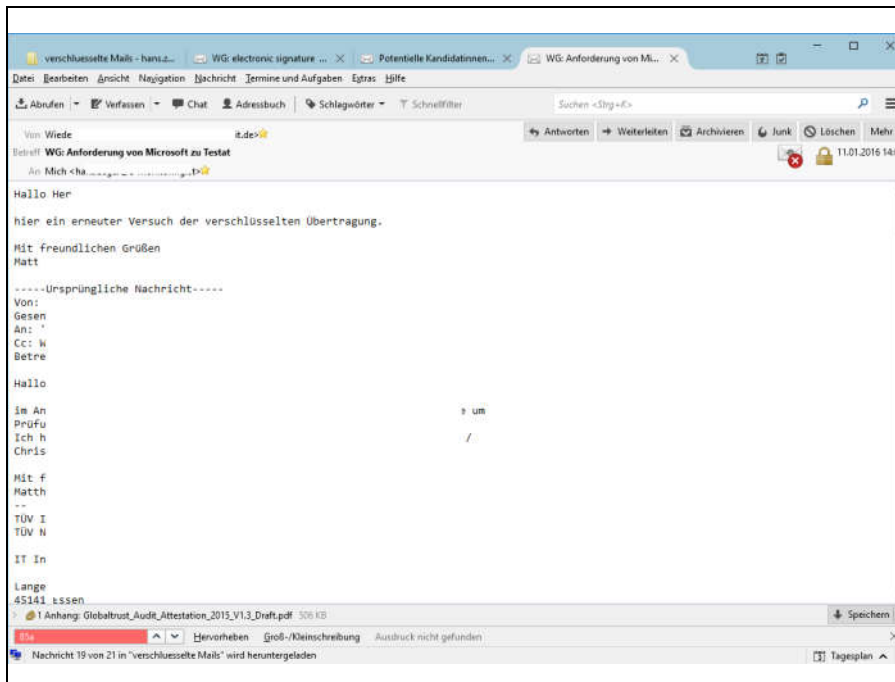
Die Nachricht kann auch gleichzeitig signiert werden. Dafür müssen Schlüssel und Zertifikat des Absenders installiert sein.

Hinweis III:

Der Betreff der E-Mail wird nicht verschlüsselt!

3.4 SIGNIERTE/VERSCHLÜSSELTE E-MAILS EMPFANGEN

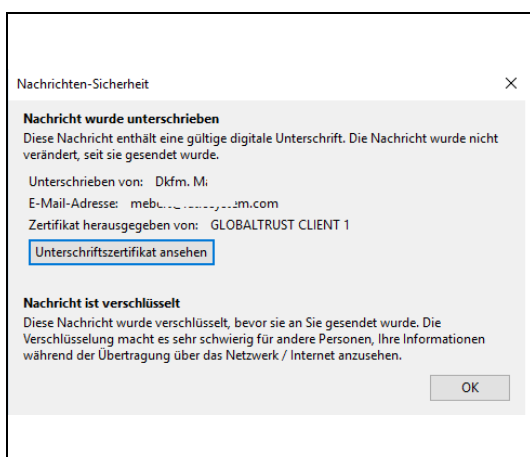
3.4.1 EMPFANGENE E-MAIL ÖFFNEN



Screen 21: Empfangene E-Mail öffnen

- Nach Doppelklick auf die empfangene E-Mail sind, im Falle der Signierung und Verschlüsselung, die entsprechenden Symbole (Kuvert mit Siegel und Vorhängeschloss) im rechten oberen Eck der E-Mail zu sehen.

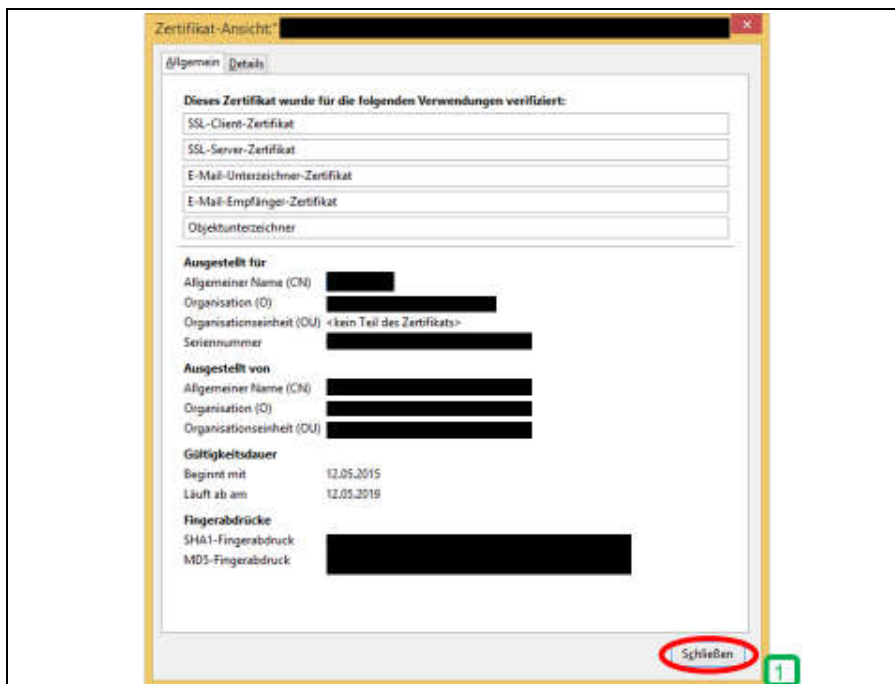
3.4.2 SIGNATUR PRÜFEN



Screen 22: Signierung prüfen

- Mit einem Klick auf die Symbole werden die Details zur Signierung und Verschlüsselung geöffnet. Mit einem Klick auf „Unterschriftszertifikat ansehen“ können die Details zum Zertifikat selber geöffnet werden.
- Mit „OK“ kann das Fenster geschlossen werden.

3.4.3 ZERTIFIKAT DETAILS ANZEIGEN



Screen 23: Zertifikat Details

Legende:

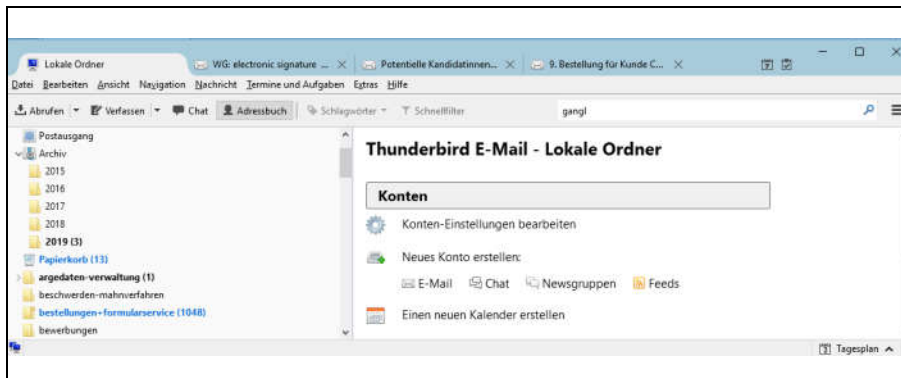
- 1** Nach Prüfung des Zertifikates kann das Fenster mit „Schließen“ wieder geschlossen werden. -> Fertig

4 MOZILLA THUNDERBIRD LDAP ADRESSBUCH

GLOBALTRUST stellt seinen Kunden ein LDAP Verzeichnis zur Verfügung. In diesem Verzeichnis sind alle von GLOBALTRUST ausgestellten Zertifikate zu finden. Somit ist es möglich an alle Personen mit einem GLOBALTRUST Zertifikat verschlüsselte E-Mails zu schicken. Es ist außerdem möglich dieses Verzeichnis in das Adressbuch von Mozilla Thunderbird zu integrieren.

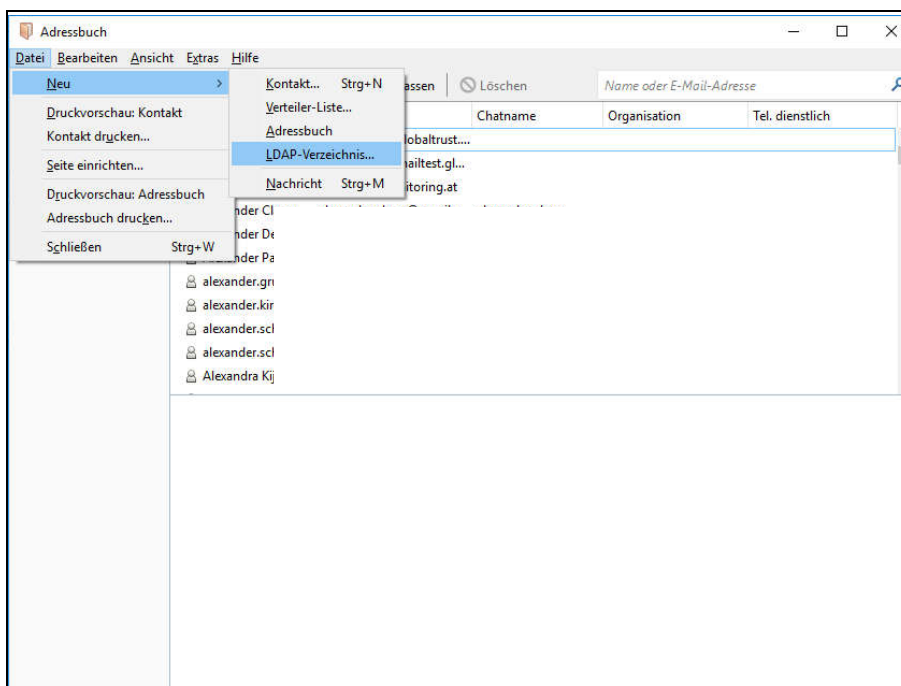
4.1 DETAILDOKUMENTATION LDAP

4.1.1 ADRESSBUCH ÖFFNEN



Screen 24: Adressbuch öffnen

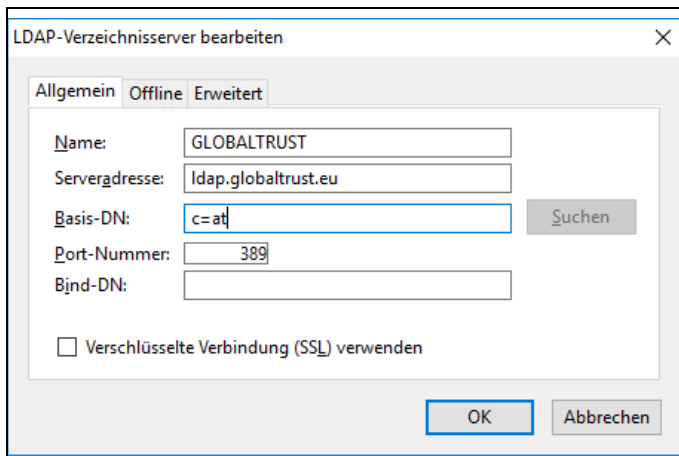
- Im Hauptfenster auf „Adressbuch“ klicken



Screen 25: Adressbuch öffnen

- Im Adressbuch unter „Datei“ und „Neu“ auf „LDAP-Verzeichnis...“ klicken.

4.1.2 SERVERDATEN EINGEBEN



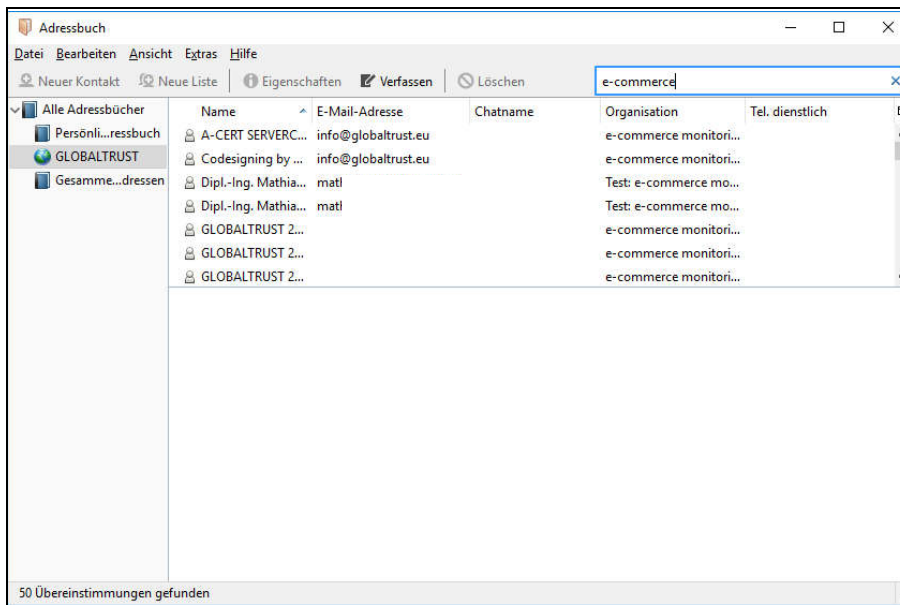
Screen 26: Serverdaten eingeben

Legende:

- Im neu erschienen Fenster die Informationen für das Verzeichnis eingeben.
- Name: „GLOBALTRUST“
- Serveradresse: „ldap.globaltrust.eu“
- Basis-DN: „c=at“
- Port-Nummer: „389“

Wenn alle Daten eingegeben wurden auf „OK“ klicken.

4.1.3 NACH EINTRÄGEN SUCHEN



Screen 27: Nach Einträgen suchen und anzeigen

- Auf der linken Seite das entsprechende Adressbuch auswählen. Hier: „GLOBALTRUST“
- Rechts oben den gesuchten Namen/ die gesuchte E-Mail Adresse eingeben. In der Ergebnisliste den gewünschten Eintrag auswählen. -> Fertig

5 ABBILDUNGEN

Screen 1:	Download Root CA	4
Screen 2:	Einstellungen öffnen	5
Screen 3:	Zertifikat importieren	6
Screen 4:	Zertifikatseigenschaften festlegen	6
Screen 5:	Eigenes Zertifikat installieren	7
Screen 6:	Passwort vergeben	8
Screen 7:	Kryptographie-Modul installieren I	9
Screen 8:	Kryptographie-Modul installieren II	10
Screen 9:	Kryptographie-Modul installieren III	10
Screen 10:	Kryptographie-Modul installieren IV	11
Screen 11:	eMail-Konto auswählen	11
Screen 12:	Einstellungen konfigurieren	12
Screen 13:	Nachrichten verfassen und signieren I	12
Screen 14:	Nachrichten verfassen und signieren II	13
Screen 15:	Nachrichten verfassen und signieren III	13
Screen 16:	Empfänger Zertifikat importieren I	14
Screen 17:	Empfänger Zertifikat importieren II	14
Screen 18:	Empfänger Zertifikat importieren III	14
Screen 19:	Empfänger Zertifikat importieren	15
Screen 20:	Neue E-Mail verfassen + verschlüsseln	15
Screen 21:	Empfangene E-Mail öffnen	16
Screen 22:	Signierung prüfen	16
Screen 23:	Zertifikat Details	17
Screen 24:	Adressbuch öffnen	18
Screen 25:	Adressbuch öffnen	18
Screen 26:	Serverdaten eingeben	19
Screen 27:	Nach Einträgen suchen und anzeigen	19