SICHERE EMAIL MIT S/MIME UND THUNDERBIRD[1]

Gegeben / Voraussetzung:

Ein PC mit einem der folgenden drei Betriebssysteme: Windows, MacOS oder Linux,
und mit installiertem Firefox-Browser.

Vorgehensweise (durchführbar für jedermann):

In vier Schritten sichere Email einrichten:

1. Den kostenlosen Mail-Client Thunderbird installieren und dabei gleich einen Mail-Account einrichten (→ geht nahezu vollautomatisch).

2. Beantragen eines Zertifikats (im Firefox-Browser) und dieses als P12-Datei abspeichern
   (→ nicht schwer, aber umständlich durch viele Masken)
   - Kostenlose Class-1-Zertifikate gibt es z.B. von Comodo, StartSSL oder CAcert.
   - Die P12-Datei enthält dann das Zertifikat und das eigene Schlüsselpaar.

3. Installieren des Zertifikats in Thunderbird und Konfigurieren des Zertifikats für Email

4. Erster Kommunikationsteilnehmer sendet eine signierte Mail, der zweite kann schon verschlüsselt antworten.

5. Optional: Installation der Encrypt-if-Possible-Erweiterung für Thunderbird
   (https://addons.mozilla.org/de/thunderbird/addon/encrypt-if-possible/)

- Ein Artikel aus der Computerwoche vom 3.2.2013 dazu: „Mehr Sicherheit für Ihre E-Mails“:
  http://www.computerwoche.de/a/mehr-sicherheit-fuer-ihre-e-mails,2363681,8
- Ein Artikel vom 11.8.2014, der Mail-Clients mehr Sicherheit zubilligt: http://www.onlinekosten.de/news/artikel/59045/0/Datenschuetzer-warnt-vor-E-Mail-Abruf-im-Browser
- Anleitung in TB: http://www.thunderbird-mail.de/wiki/Mailverschl%C3%BCsselung_mit_S/MIME
- Wikipedia-Artikel zu S/MIME: http://de.wikipedia.org/wiki/S/MIME

[1] Dies ist das 1. Dokument in der Reihe "Sichere Email mit S/MIME" (© 2016).
Die meisten Screenshots stammen aus 2013/2014. Sie werden jeweils dann erneuert, wenn sich Inhalte oder die Masken ändern.

Inhaltsverzeichnis

SICHERE EMAIL MIT S/MIME UND THUNDERBIRD

Begriffserklärungen:

S/MIME	Protokoll für sichere Email
Thunderbird	Name des Mail-Clients, der auf den drei Betriebssystemen Windows, MacOS und Linux zur Verfügung steht.
Sichere Email	Mails, die signiert und verschlüsselt statt im Klartext verschickt werden.

Schreibweise: „E-Mail“ wird hier meist als „Email“ geschrieben.
Abkürzungen: **FF** = Firefox-Browser, **TB** = Thunderbird-Email-Client

Dokument-Status:

- Datum: 27.4.2016
- Version: 1.3.0
  (Todo für die nächste Version: auch den Umzug mit Thunderbird auf einen neuen Rechner behandeln: http://praxistipps.chip.de/thunderbird-konto-einstellungen-exportieren-und-umziehen_28209, http://www.at2907.net/tipps1/tipp15.php).
- Autor: Bernhard Esslinger, Uni Siegen
- Mit Unterstützung vom CrypTool-Projekt www.cryptool.org
- Dank an Michael Schober von der NOVOSEC AG und André Heller für ihre fachliche Expertise.
- Sprache: Deutsch
- Lizenz: Keine bzw. Public-Domain bzw. GNU Free Documentation License

- Benutzte Versionen:
  - Thunderbird 24.3.0 und 31.0 und 31.1.2 und 45.0;
  - Firefox 27.0.1 und 31.0 und 32.0 und 46.0.
- Aufbereitung: Schritt-für-Schritt mit vielen Bildschirmfotos (Screenshots)
- Zielgruppe: Jedermann, also
  Privat- und Heimanwender, die Ende-zu-Ende-verschlüsselt per Email kommunizieren wollen.

Dieses Dokument ist das **erste** in der Reihe „Sichere Email mit S/MIME“. Die gesamte Reihe besteht aus den 4 Dokumenten:

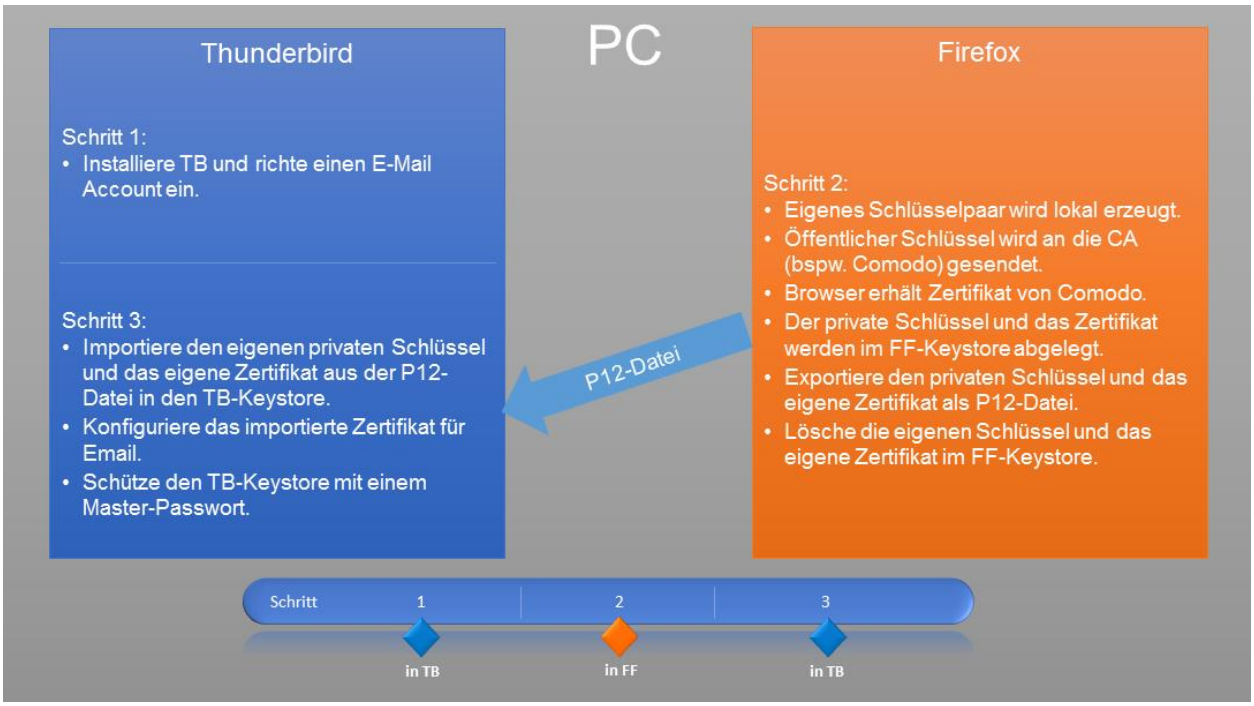
1. **Sichere Email mit S/MIME und Thunderbird (unter Windows, MAC und Linux)**
   Das 1. Dokument enthält die Theorie und erläutert, wie sichere S/MIME-Email mit dem Mail-Client „Thunderbird“ funktioniert.
2. **Sichere Email mit S/MIME und Outlook unter Windows**
   Das 2. Dokument zeigt, wie es unter Windows mit dem Mail-Client „Outlook“ geht (mit und ohne Virtual Smartcard).
3. **Sichere Email mit S/MIME unter Android**
   Das 3. Dokument zeigt, wie es unter Android mit dem Mail-Client „SMail“ geht.
4. **Sichere Email mit S/MIME unter iOS**
   Das 4. Dokument zeigt, wie es unter iOS mit dem Mail-Client „Mail“ geht.

Grafische Abfolge der Schritte in den beiden Programmen TB und FF

Auf Seite 1 wurden die Schritte kurz in Worten zusammengefasst.
Hier wird das Setup (ein PC mit Firefox und Thunderbird) in grafischer Form dargestellt, und welche Schritte (und Unterschritte) mit welchem Programm durchzuführen sind:

Installation / Setup:

- Schritt 1 mit Thunderbird
- Schritt 2 mit Firefox
- Schritt 3 mit Thunderbird



Anschließend kann man Thunderbird benutzen für das Senden und Empfangen von sicherer und natürlich auch weiterhin von unsicherer Email:

Benutzung / Anwendung:

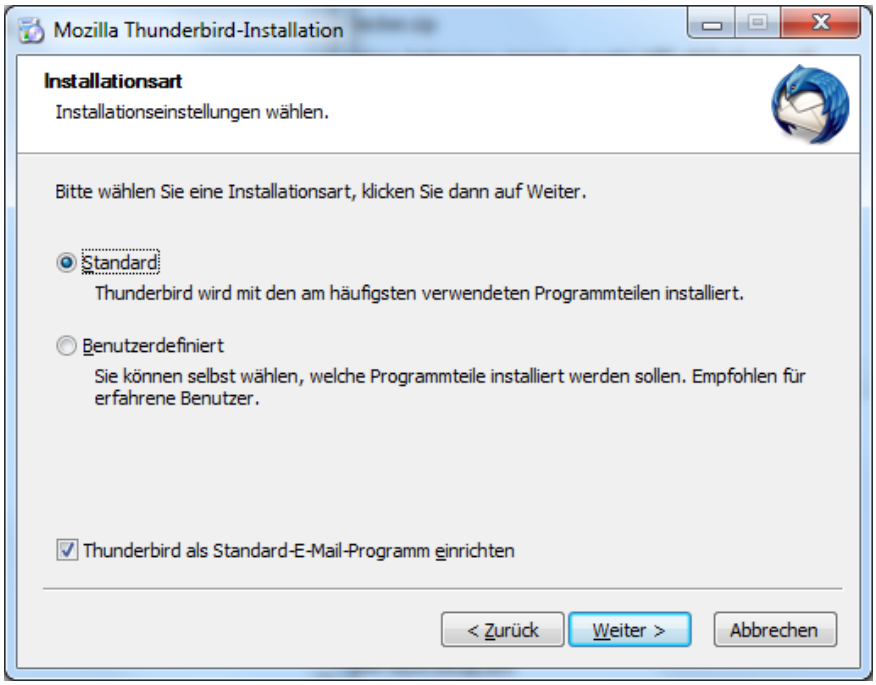
- Schritt 4 mit Thunderbird

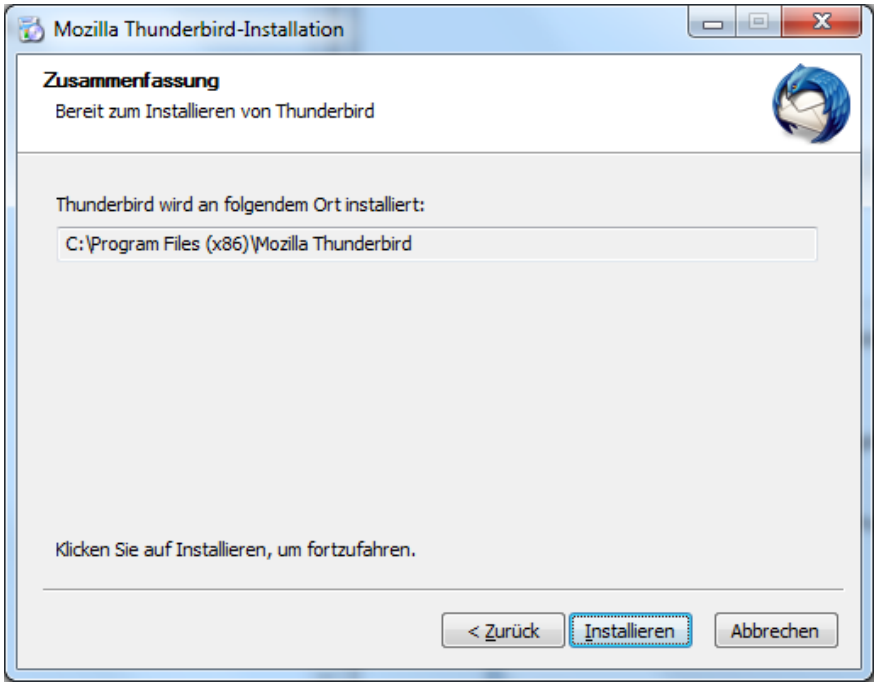
Schritt 1: Installiere Thunderbird (TB)

Thunderbird installieren und einen vorhandenen Mail-Account einrichten

→ Dies geht nahezu vollautomatisch.

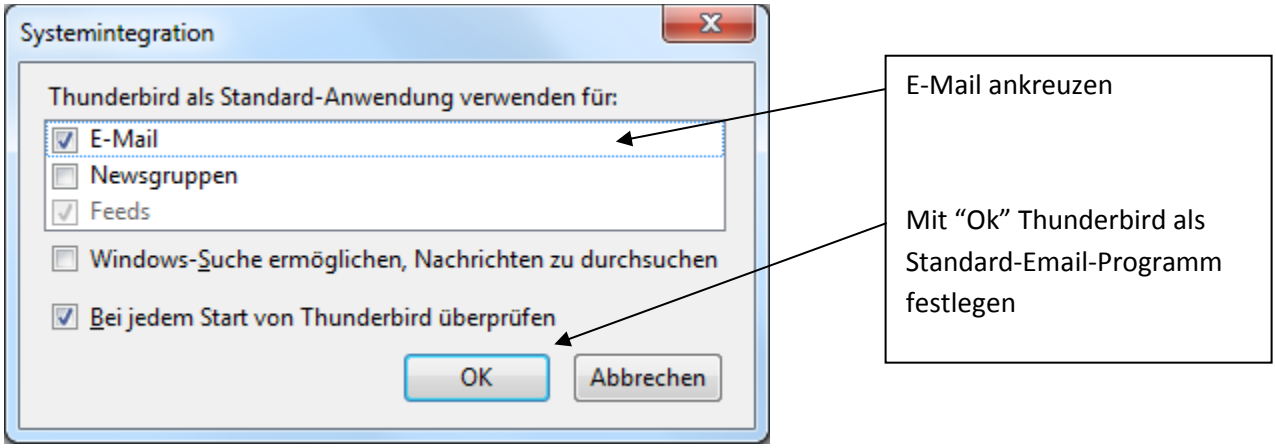
Download von Thunderbird: http://www.mozilla.org/de/thunderbird/

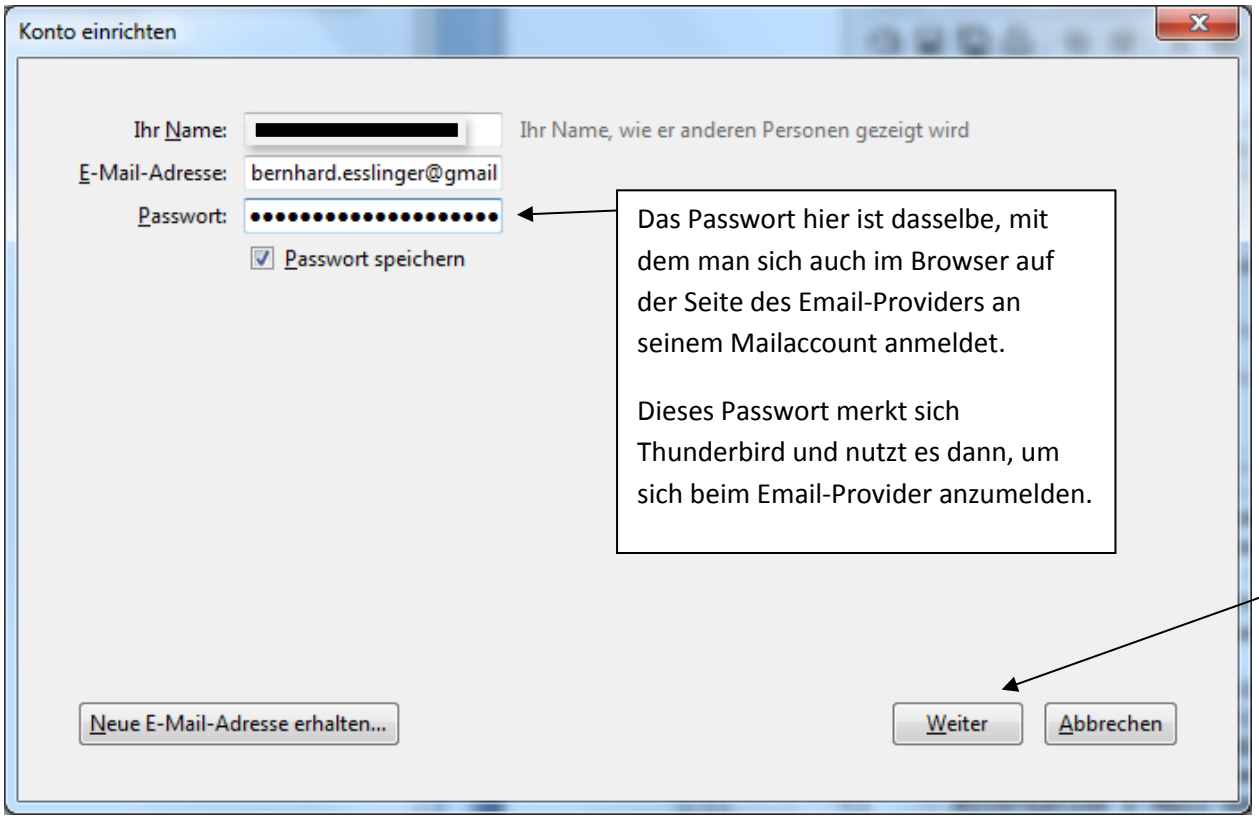


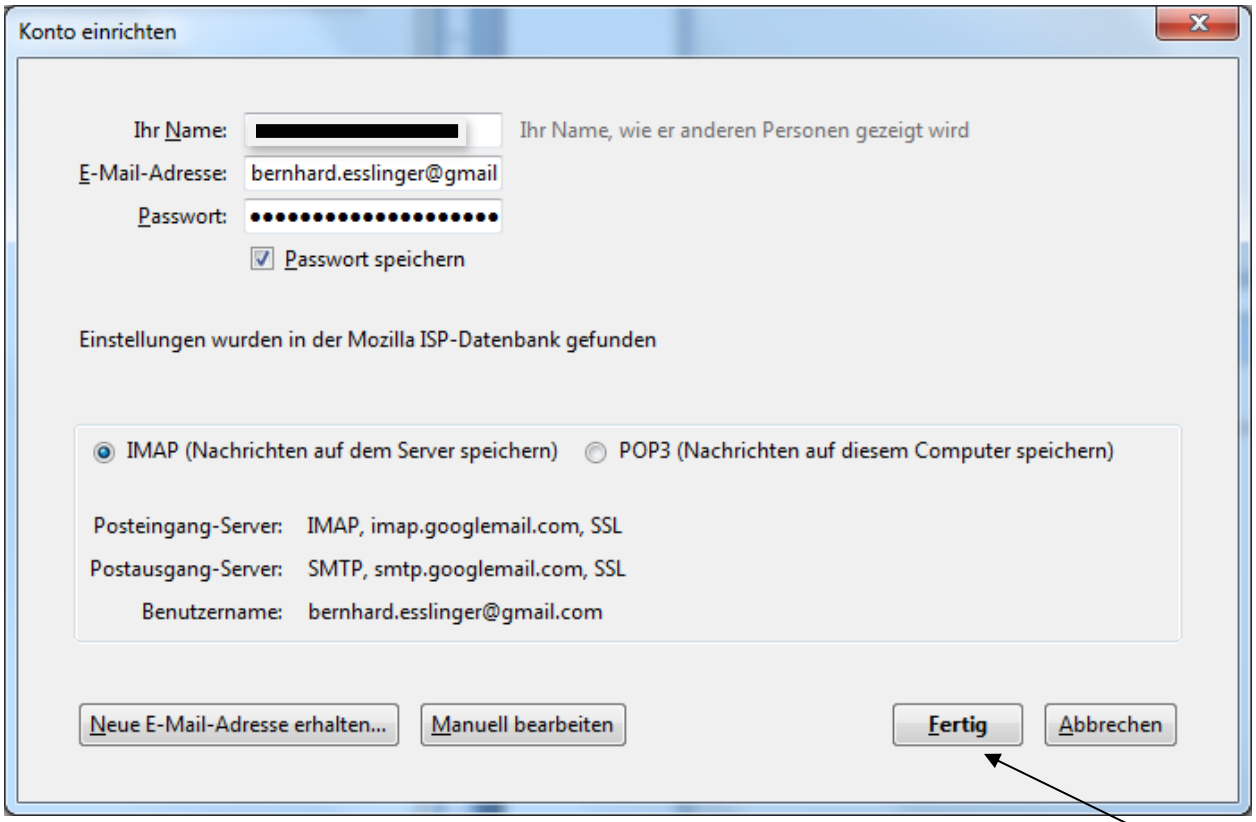


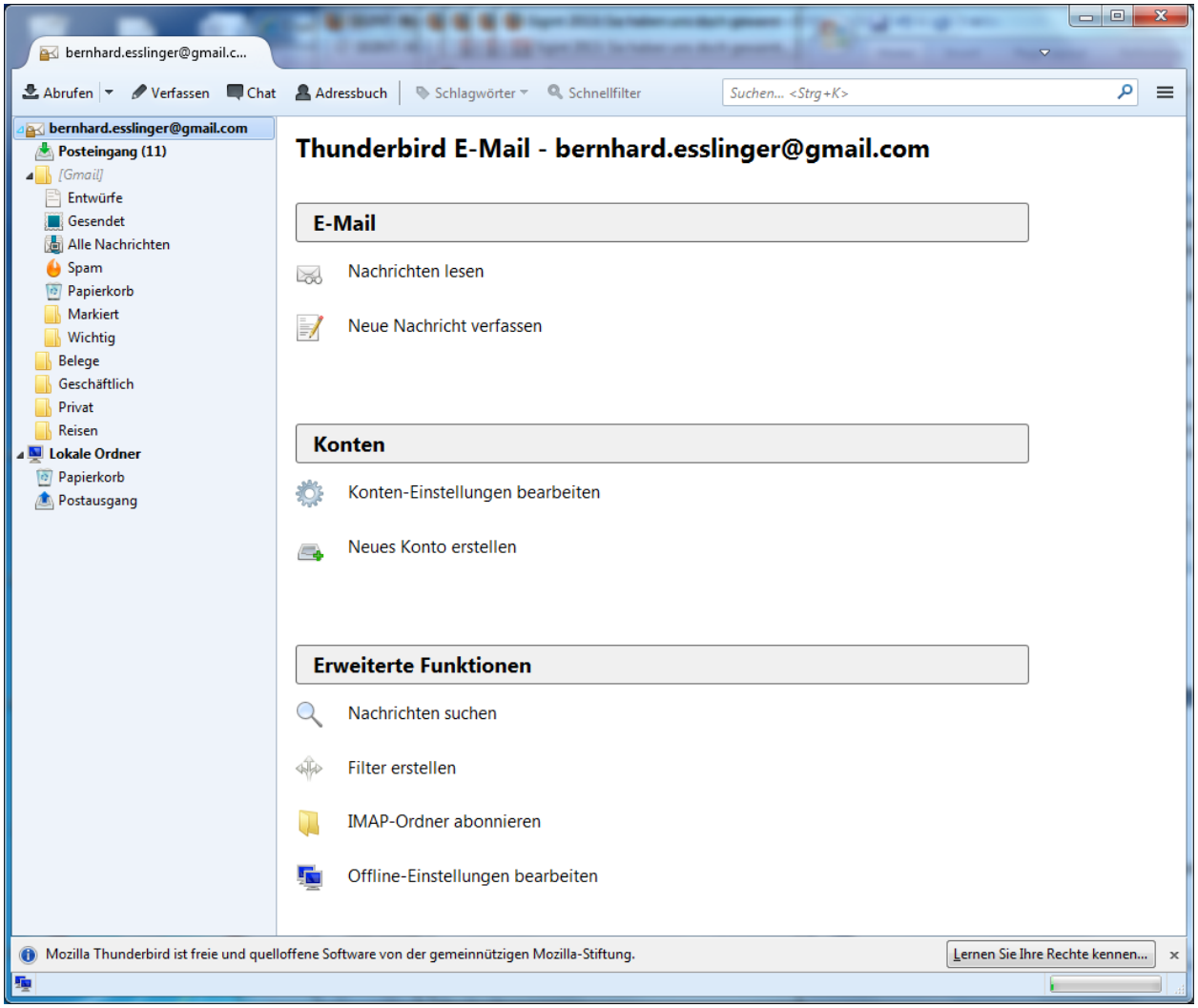
Drücken der Buttons „Installieren“ und am Ende „Fertigstellen“.

Thunderbird wird gestartet. Dabei erscheinen beim ersten Mal folgende Fenster:



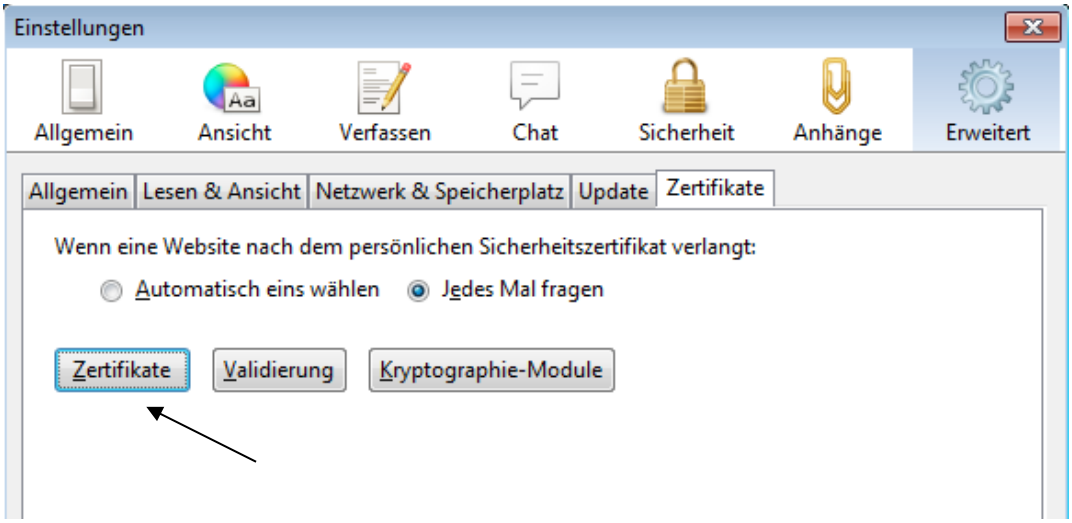

Konto einrichten
Ihr Name:
Ihr Name, wie er anderen Personen gezeigt wird
E-Mail-Adresse:
bernhard.esslinger@gmail
Passwort:
Passwort speichern
Das Passwort hier ist dasselbe, mit dem man sich auch im Browser auf der Seite des Email-Providers an seinem Mailaccount anmeldet.
Dieses Passwort merkt sich Thunderbird und nutzt es dann, um sich beim Email-Provider anzumelden.
Neue E-Mail-Adresse erhalten...
Weiter
Abbrechen

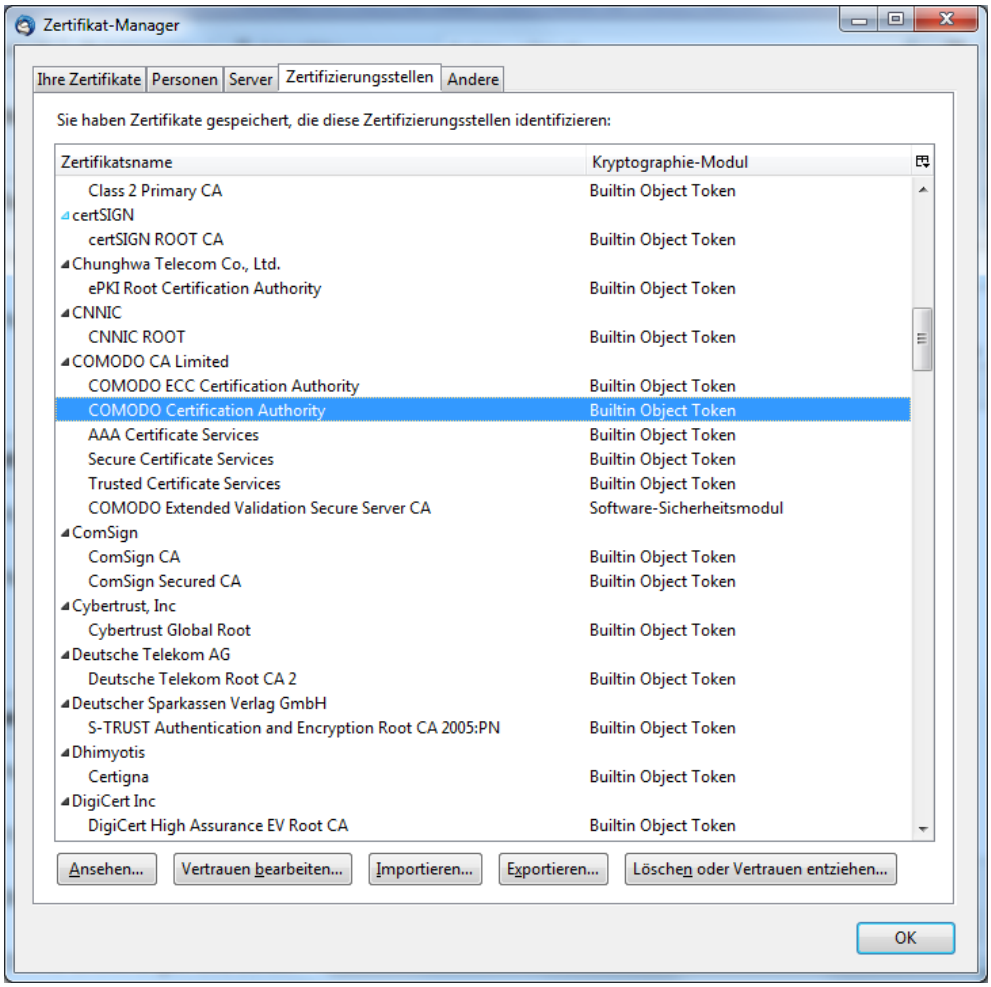

Konto einrichten
Ihr Name:
Ihr Name, wie er anderen Personen gezeigt wird
E-Mail-Adresse:
bernhard.esslinger@gmail
Passwort:
Passwort speichern
Einstellungen wurden in der Mozilla ISP-Datenbank gefunden
IMAP (Nachrichten auf dem Server speichern)
POP3 (Nachrichten auf diesem Computer speichern)
Posteingang-Server: IMAP, imap.googlemail.com, SSL
Postausgang-Server: SMTP, smtp.googlemail.com, SSL
Benutzername: bernhard.esslinger@gmail.com
Neue E-Mail-Adresse erhalten...
Manuell bearbeiten
Fertig
Abbrechen


bernhard.esslinger@gmail.c...
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
bernhard.esslinger@gmail.com
Posteingang (11)
[Gmail]
Entwürfe
Gesendet
Alle Nachrichten
Spam
Papierkorb
Markiert
Wichtig
Belege
Geschäftlich
Privat
Reisen
Lokale Ordner
Papierkorb
Postausgang
Thunderbird E-Mail - bernhard.esslinger@gmail.com
E-Mail
Nachrichten lesen
Neue Nachricht verfassen
Konten
Konten-Einstellungen bearbeiten
Neues Konto erstellen
Erweiterte Funktionen
Nachrichten suchen
Filter erstellen
IMAP-Ordner abonnieren
Offline-Einstellungen bearbeiten
Mozilla Thunderbird ist freie und quelloffene Software von der gemeinnützigen Mozilla-Stiftung.
Lernen Sie Ihre Rechte kennen...

Nur zur Information: Welche Zertifizierungsstellen (CAs) kennt TB schon automatisch?

Klick auf die Anwendungsmenü-Ikone → Einstellungen → Erweitert → Zertifikate (vgl. S. 23)



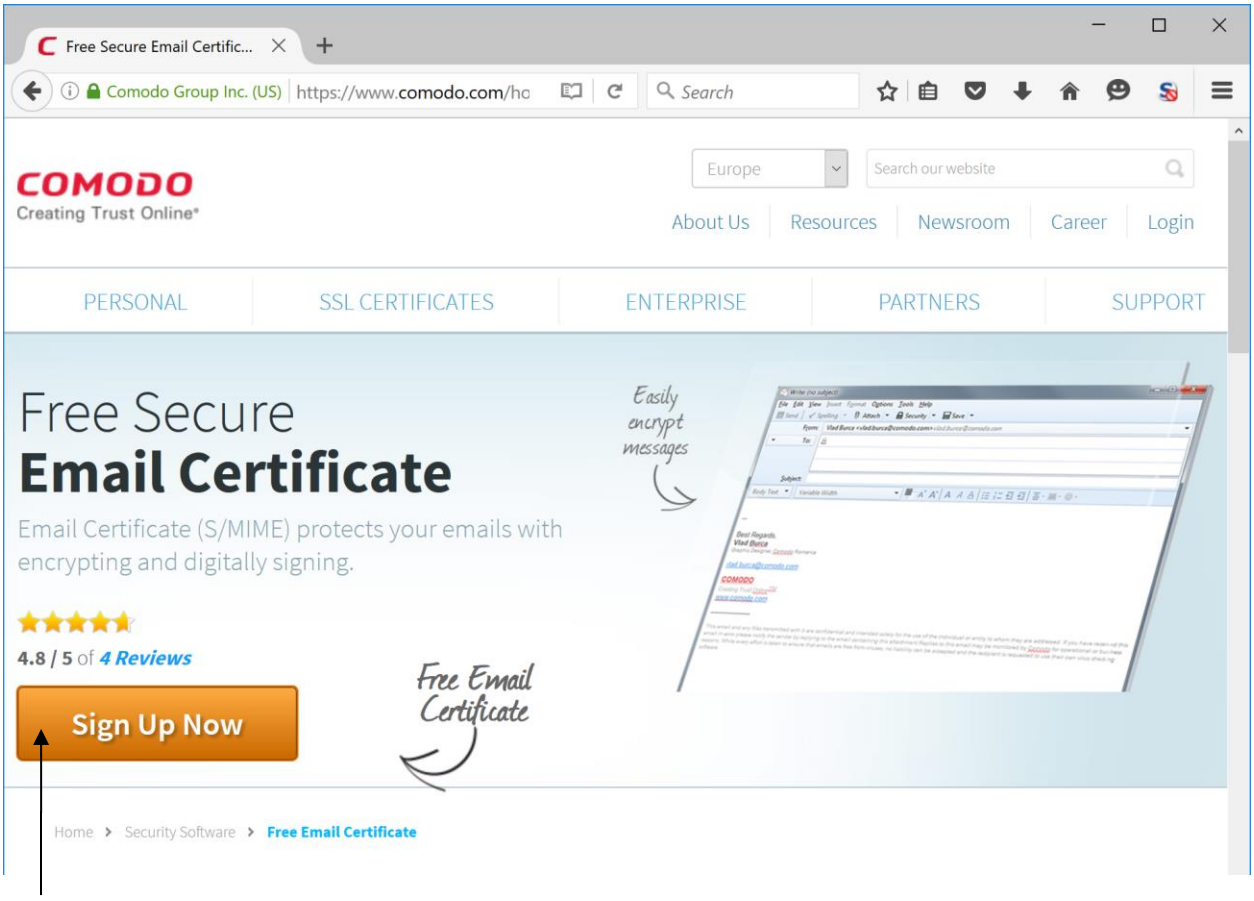


Schritt 2: Erzeuge ein Zertifikat (in Firefox)

Beantragen eines kostenlosen Zertifikats und Exportieren in eine P12-Datei (alles im Firefox-Browser)

Beantragen z.B. bei Comodo (gefunden per Google-Suchbegriff „s/mime zertifikat kostenlos“)

http://www.comodo.com/home/email-security/free-email-certificate.php



Anklicken

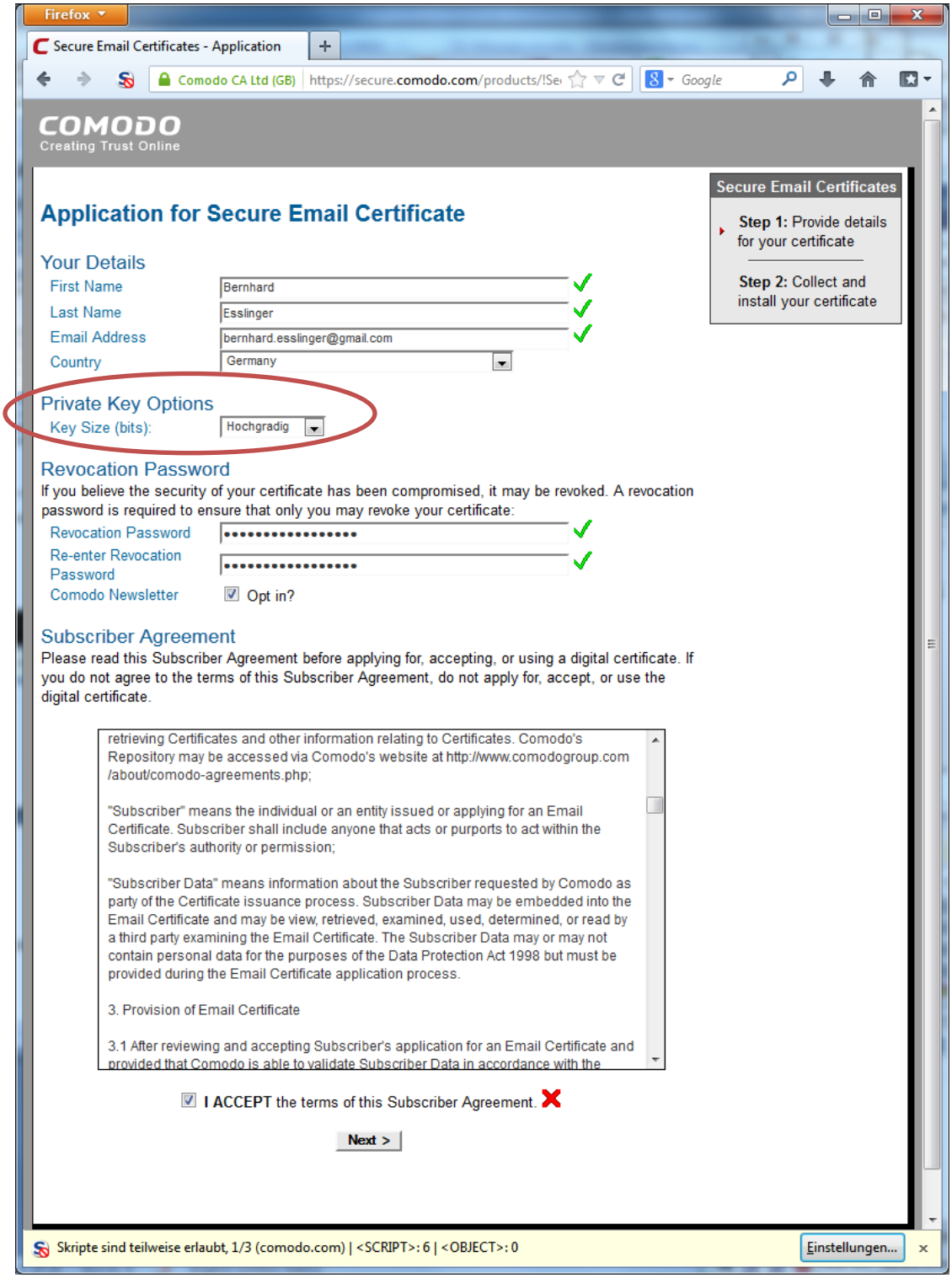
WICHTIG:

Private (Signatur-)Schlüssel sollten NIE außerhalb der eigenen Kontrolle erzeugt werden.

Firefox erzeugt das eigene Schlüsselpaar (den öffentlichen und den privaten Schlüssel) lokal.

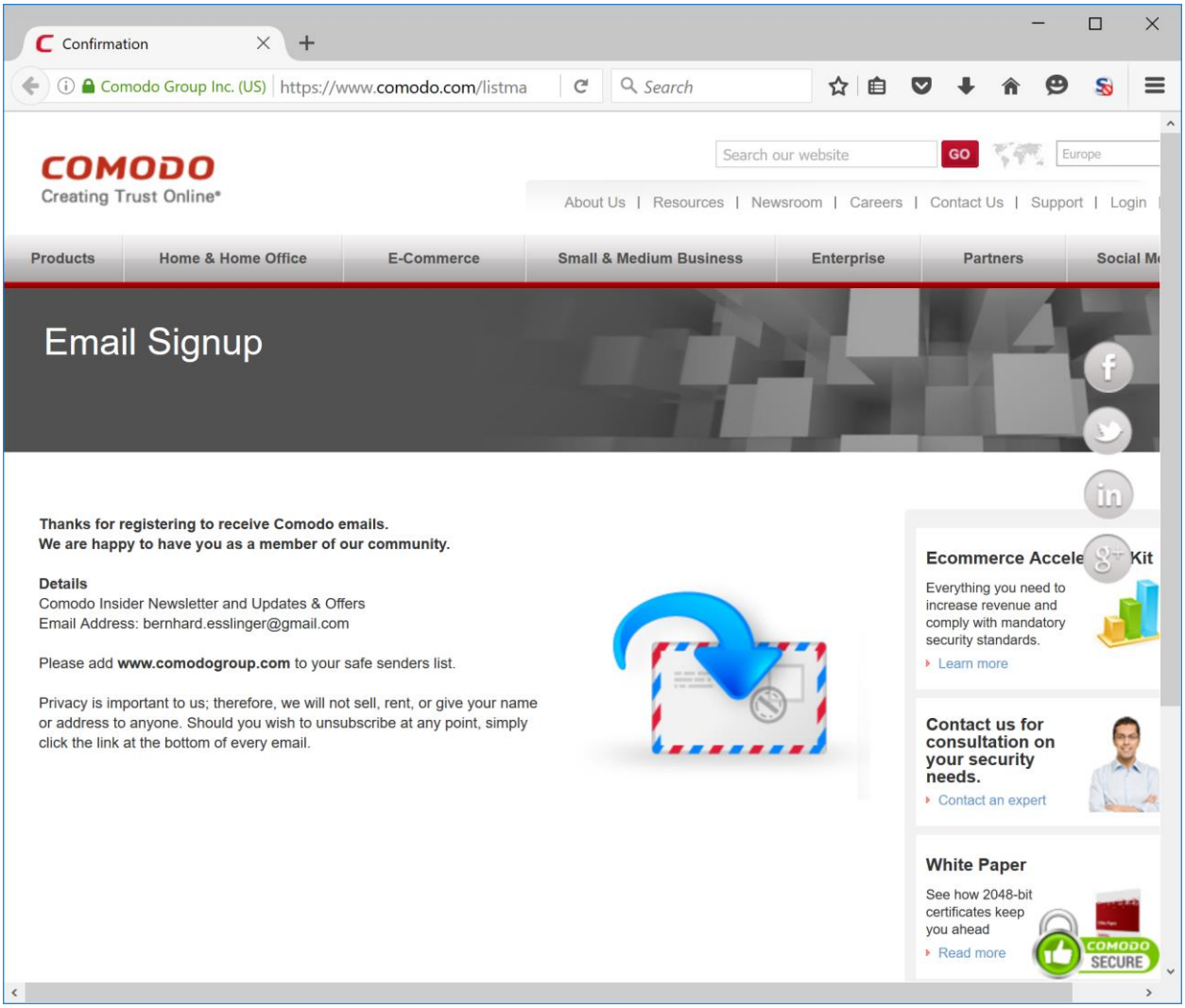
An die Zertifizierungsstelle (hier Comodo) wird nur der öffentliche Schlüssel gesandt.

Der Comodo-Seite muss man temporär erlauben, JavaScript auszuführen, sonst geht es mit dem „Next“-Button nicht weiter:

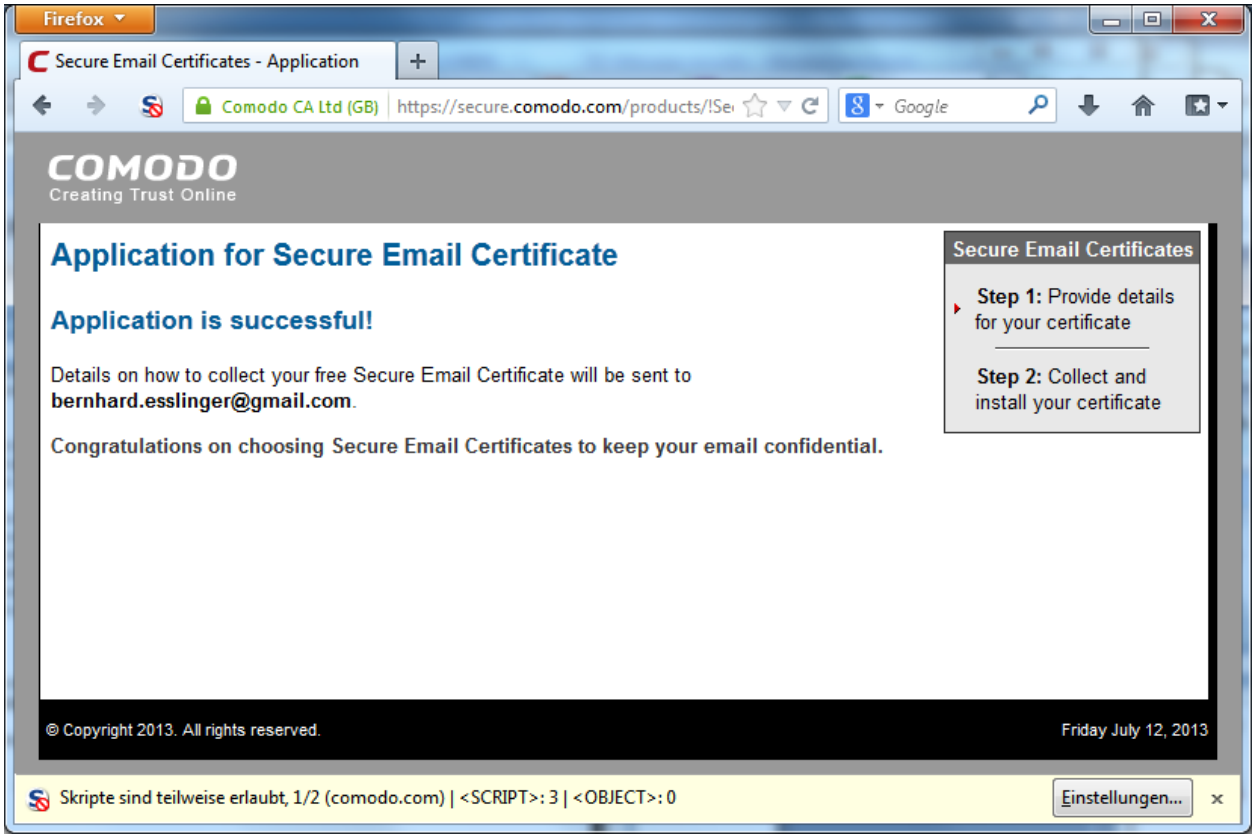


Der Haken bei „Opt-in“ führt dazu, dass man Newsletter bekommt.

http://www.comodo.com/listmanager/confirmation11.php?email=bernhard.esslinger@gmail.com



Außer der Schlüssellänge („hochgradig“) hatte man keine Wahl, irgendwelche Vorgaben zum Verfahren zu machen. Erzeugt wurde ein RSA-2048-Bit-Schlüsselpaar, was gängiger Standard ist.[2]



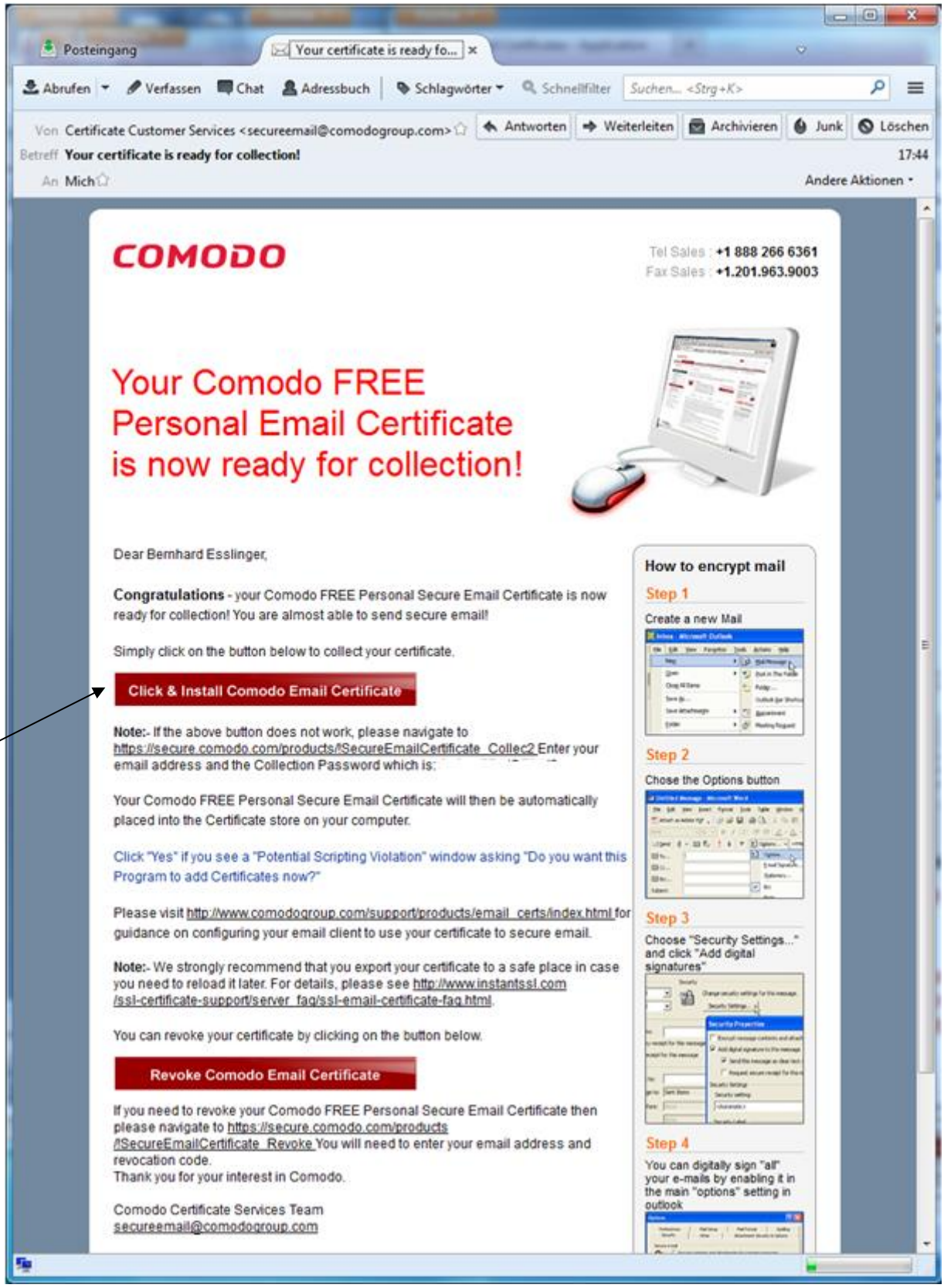
Zur Verifikation der Email-Adresse wird der Zugangslink zum Zertifikat als Email versendet. Diese Mail ist normalerweise in weniger als einer Minute in Ihrem Eingang.

Hinweis Maileingang:

Wenn Sie bisher noch nie eine Mail von Comodo erhielten, kann es auch sein, dass die Mail in Ihrem Spam- oder Unbekannt-Ordner landet. Wenn der Eingang also länger dauert, schauen Sie bitte auch in diesen Ordnern nach.

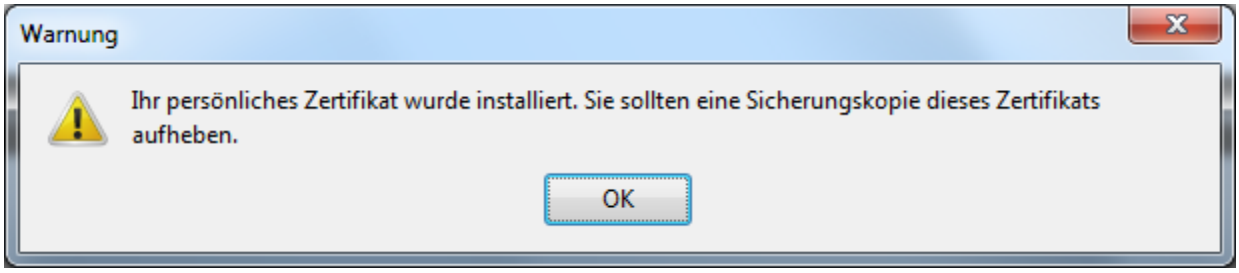
[2] Früher konnte man auch bei TC Trustcenter kostenlose Zertifikate bestellen. Das Vorgehen war im Grunde identisch zu dem bei Comodo, mit zwei kleinen Unterschieden:
- Voreingestellt war eine Schlüssellänge von 1536 Bit; diese war frei wählbar bis 8192 Bit.
- Das Stammzertifikat von TC Trustcenter war in Thunderbird nicht vorhanden. Deshalb muss man es von der Trustcenter-Homepage herunterladen und in TB hinzufügen. Dies geht analog zum Importieren des Zertifikats einer Firmen-Zertifizierungsstelle oder von CAcert (siehe Anhang, Teil B).
- Inzwischen bietet TC-Trustcenter kein kostenloses Zertifikat mehr an. Damit gibt es u.W. keine deutschen Trustcenter mehr, die in den Mozilla-Keystores drin sind und kostenlose Zertifikate erstellen (Stand April 2016).

Öffnen Sie die empfangene Verifikations-Mail:

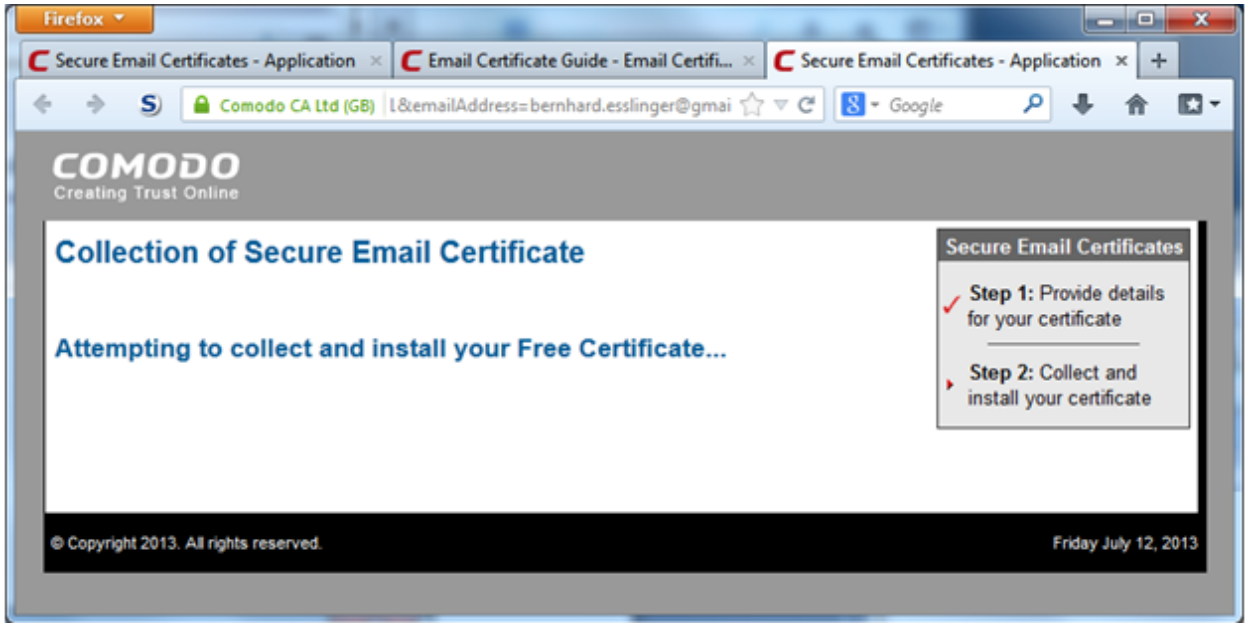


Der Import des Zertifikats in den Mozilla-Keystore für Firefox muss mit dem Firefox-Browser erfolgen (der Browser „Internet Explorer“ von Microsoft kann nicht auf einen Mozilla-Keystore zugreifen).[3]

Auch wenn „Warnung“ drüber steht, ist es eine Erfolgsmeldung: Das Zertifikat ist nun im Firefox-Keystore gespeichert. Eine Sicherungskopie von Zertifikat und privatem Schlüssel erzeugt man automatisch durch die im Folgenden für den Transfer zu benutzende P12-Datei.



Auf der Comodo-Seite erscheint im Browser leider kein Haken bei Schritt 2, obwohl alles geklappt hat.



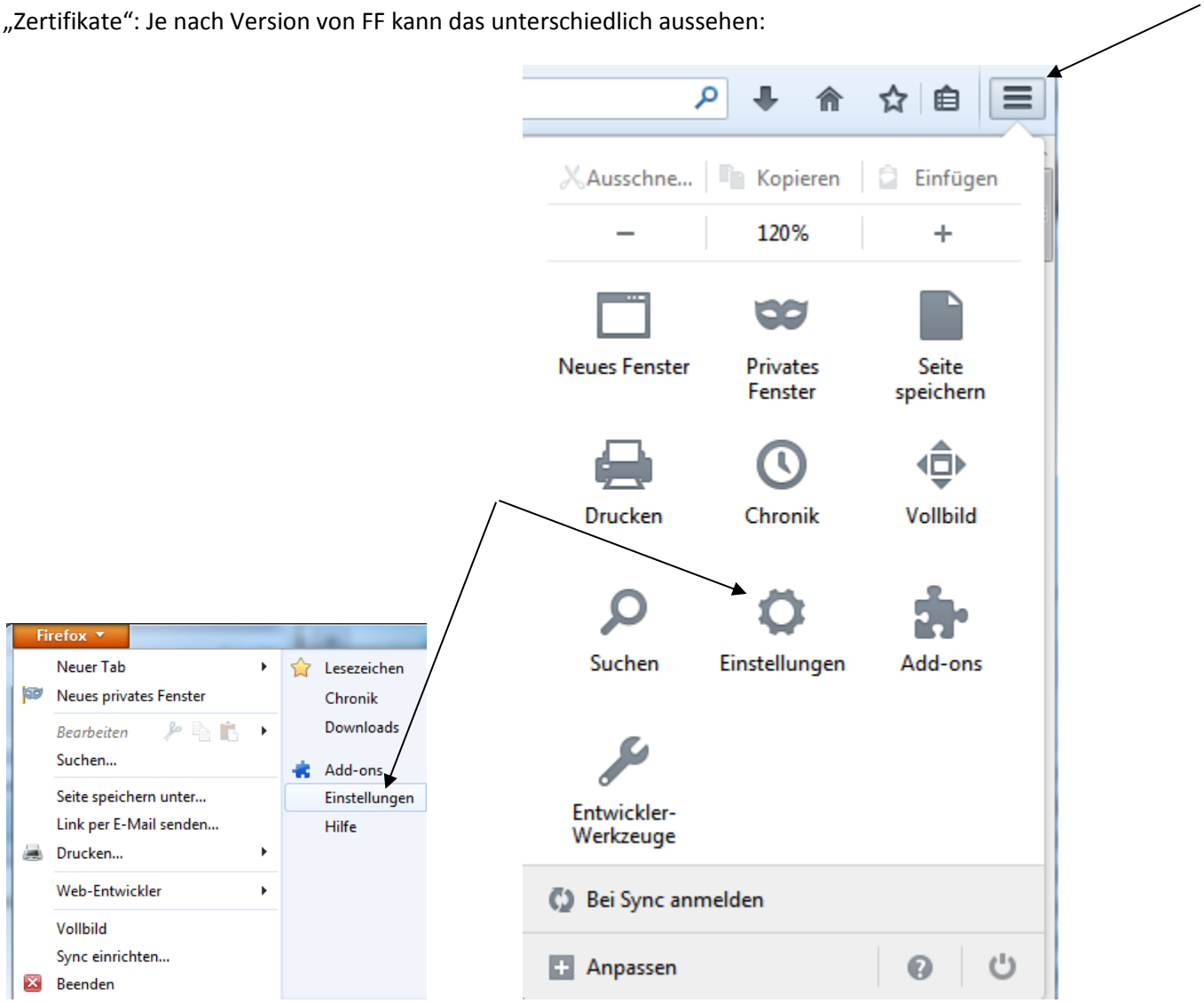
Info zur Fachsprache: Ich bin der „**Inhaber**“, Comodo ist der „**Aussteller**“ des Zertifikats.

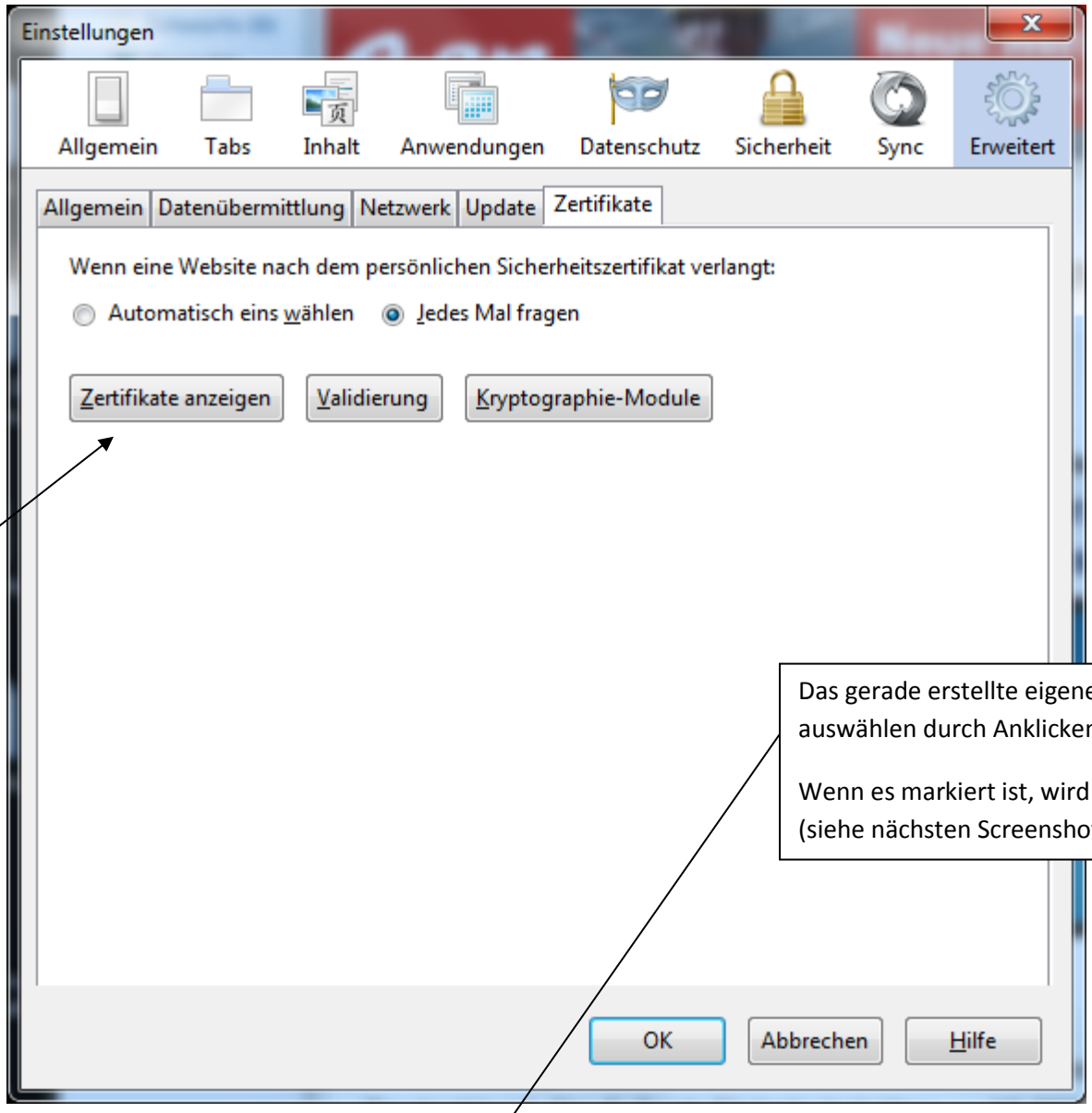
In Thunderbird sehe ich mein von Comodo ausgestelltes Zertifikat **noch** nicht, da es bisher nur im Mozilla-Keystore für Firefox abgespeichert ist. Das Konzept ist, dass man alle Infos unter der jeweiligen Installation (Firefox und Thunderbird) vorfindet. Firefox und Thunderbird basieren zwar auf dem gleichen Codebaum, sind aber jeweils eigenständige Produkte.

[3] Im Unterschied zum Windows-Betriebssystem-Keystore erfolgt hier beim Mozilla-Keystore korrekterweise kein "heimliches" Update (siehe http://www.heise.de/security/meldung/Windows-Dynamische-Zertifikat-Updates-gefaehrden-SSL-Verschluesselung-1925115.html).

Zum Transport von Zertifikat und eigenem privaten Schlüssel vom FF-Keystore in den Thunderbird-Keystore wird eine Datei in dem üblichen, Passwort-geschützten P12-Format benutzt.

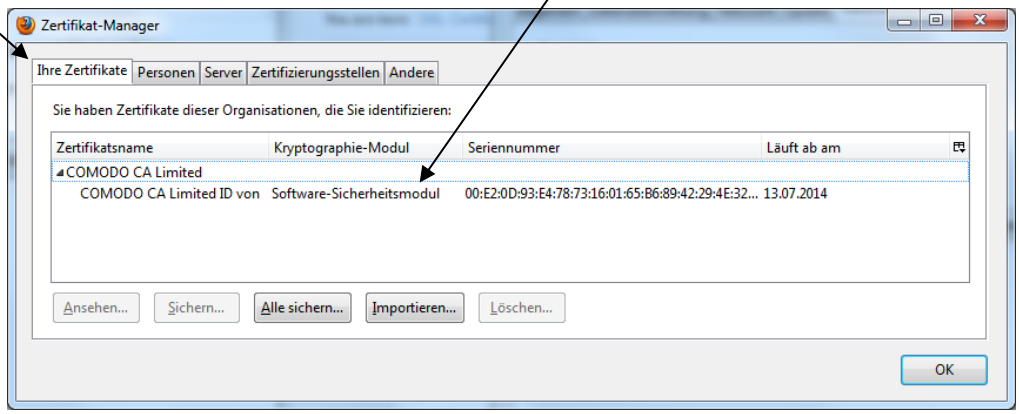
Das Zertifikat wird also in FF exportiert und als P12-Datei abgespeichert. Dazu ist zuerst in FF auf die „Menü öffnen“-Ikone zu klicken und dann auf „Einstellungen“, den Reiter „Erweitert“ und den Reiter „Zertifikate“: Je nach Version von FF kann das unterschiedlich aussehen:

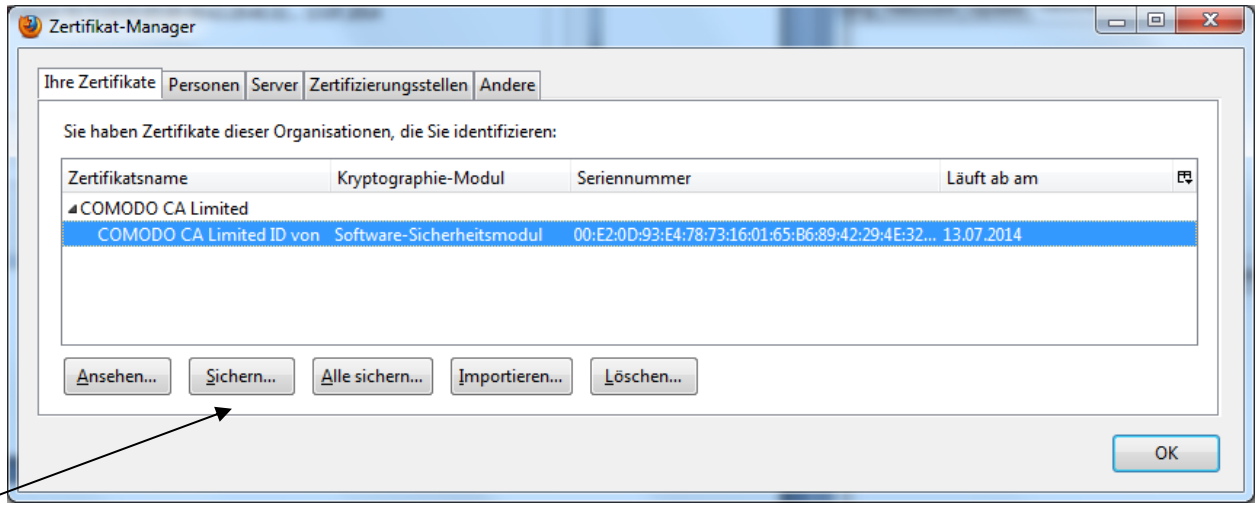




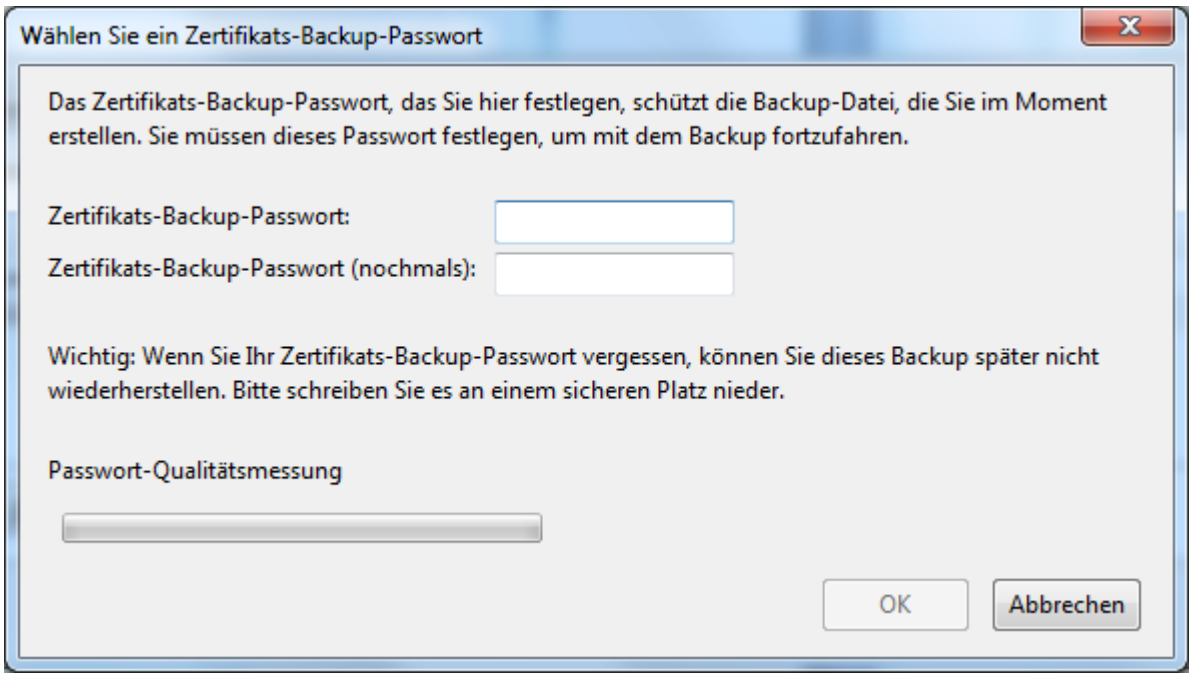
Das gerade erstellte eigene Zertifikat auswählen durch Anklicken.

Wenn es markiert ist, wird es blau (siehe nächsten Screenshot).





Dann den Button „Sichern“ (Backup) klicken und die P12-Datei an einen Ort eigener Wahl speichern (die P12-Datei enthält sowohl das Zertifikat als auch den zugehörigen privaten Schlüssel!). Weil sie auch den eigenen privaten Schlüssel enthält, wird ein Passwort zum Verschlüsseln der P12-Datei verlangt.



Nun „OK“ und Firefox (FF) schließen.

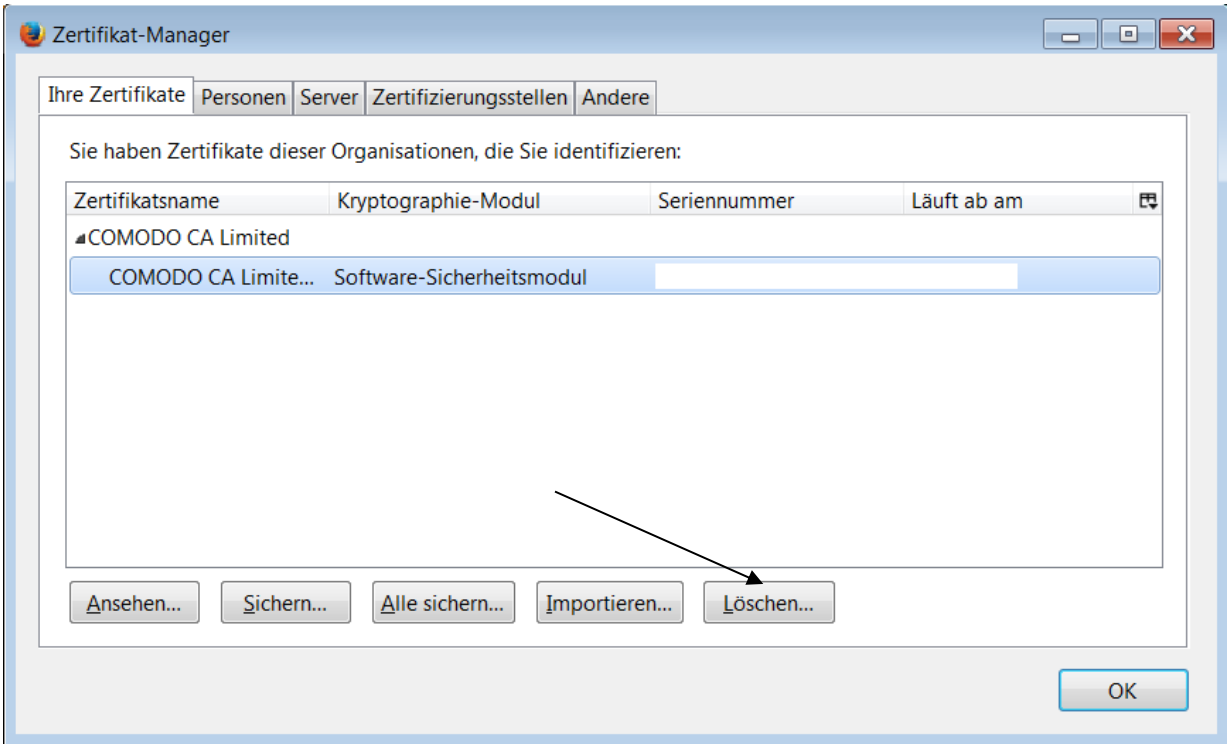
Auch das ist keine Warnung, sondern eine Erfolgs-meldung. Genaugenommen werden **ein** Zertifikat, **ein** öffentlicher Schlüssel und **ein** privater Schlüssel in die P12-Datei kopiert.

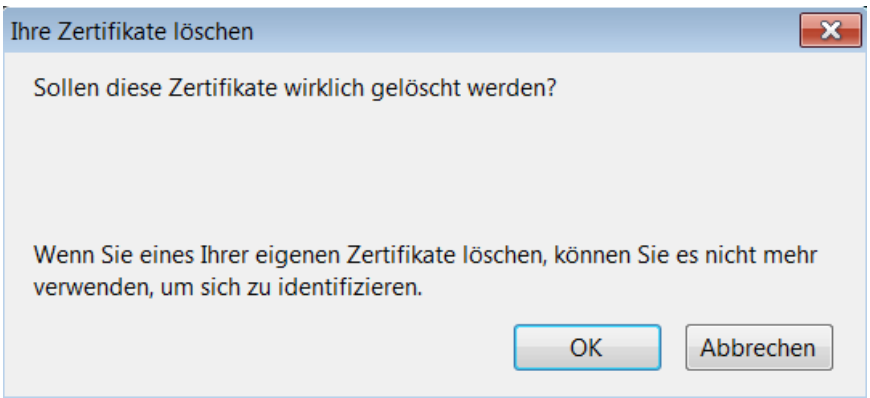
Hinweis zu FF-Keystore:

Wie Sie gesehen haben, konnte man ganz einfach einen privaten Schlüssel aus dem FF-Keystore exportieren. Damit nicht jeder an meinen privaten Schlüssel kommen kann, der Zugang zu meinem PC hat, gibt es zwei Möglichkeiten:

a) Auch den FF-Keystore mit einem Master-Passwort schützen.
b) Alternativ kann man in FF den privaten Schlüssel und das Zertifikat auch löschen, wenn man die P12-Datei erstellt hat, denn dort wird er nicht mehr gebraucht (sondern nur in Thunderbird).

Wir empfehlen, den privaten Schlüssel und das Zertifikat in FF zu löschen, nachdem man die P12-Datei erzeugt und erfolgreich in TB importiert hat. Dazu wieder in FF auf die „Menü öffnen“-Ikone klicken und dann auf „Einstellungen“, den Reiter „Erweitert“ und den Reiter „Zertifikate“. Nun auf „Zertifikate anzeigen“ und den Reiter „Ihre Zertifikate“.





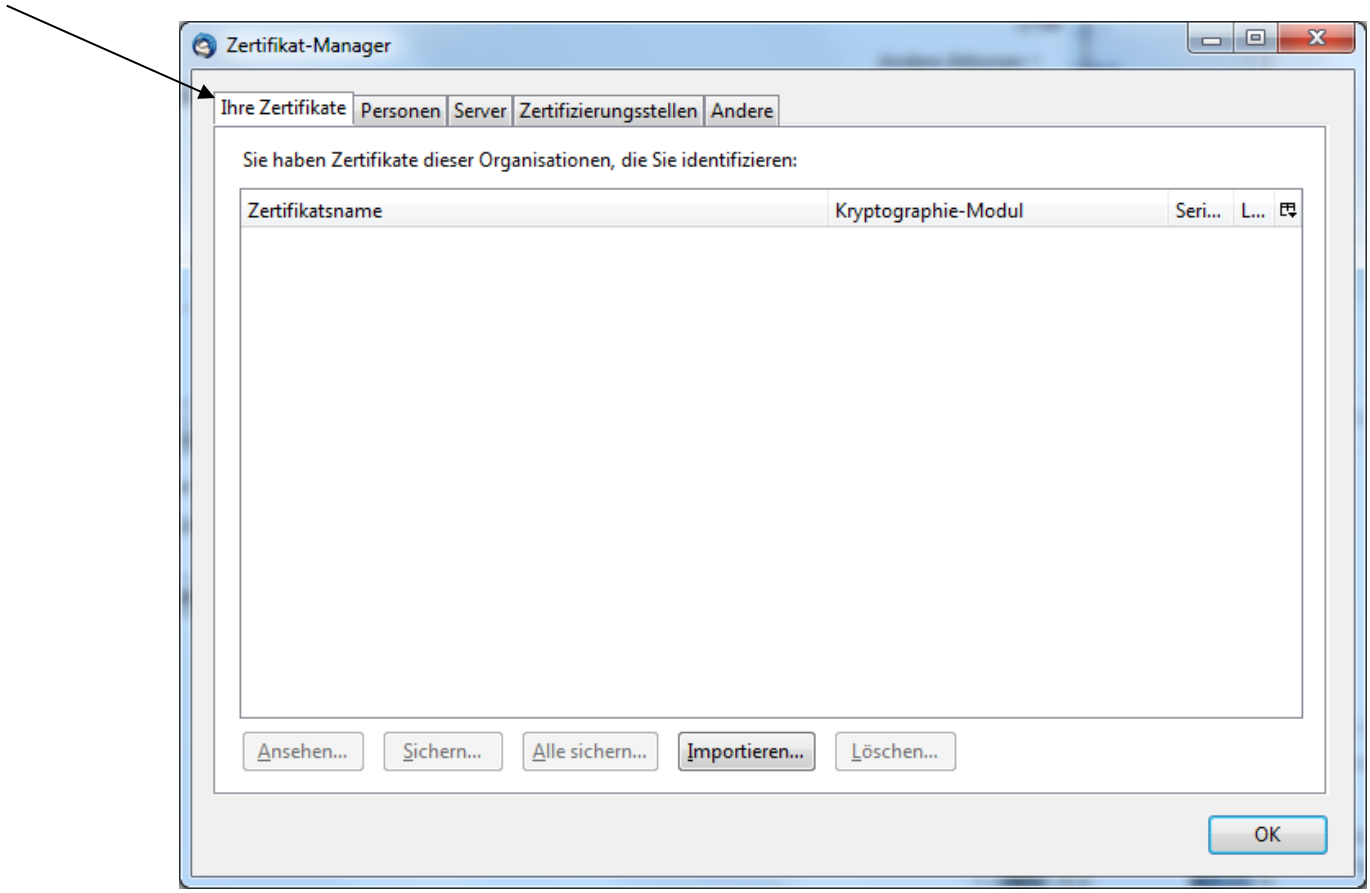
Mozilla spricht in FF und TB beim Inhalt des Keystores immer von „Zertifikaten“: Bei den eigenen Zertifikaten meinen sie damit aber nicht nur das Zertifikat, sondern auch den zugehörigen privaten Schlüssel !

Schritt 3: Installiere das eigene Email-Zertifikat in TB

Installieren des Zertifikats in TB und Konfigurieren des Zertifikats für Email

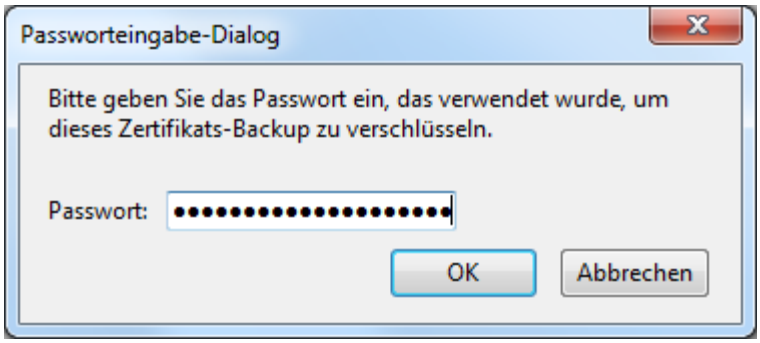
Nun also zurück zu Thunderbird (TB). Schritt 3 besteht aus 2 Teilschritten (3a und 3b):

Teilschritt 3a:



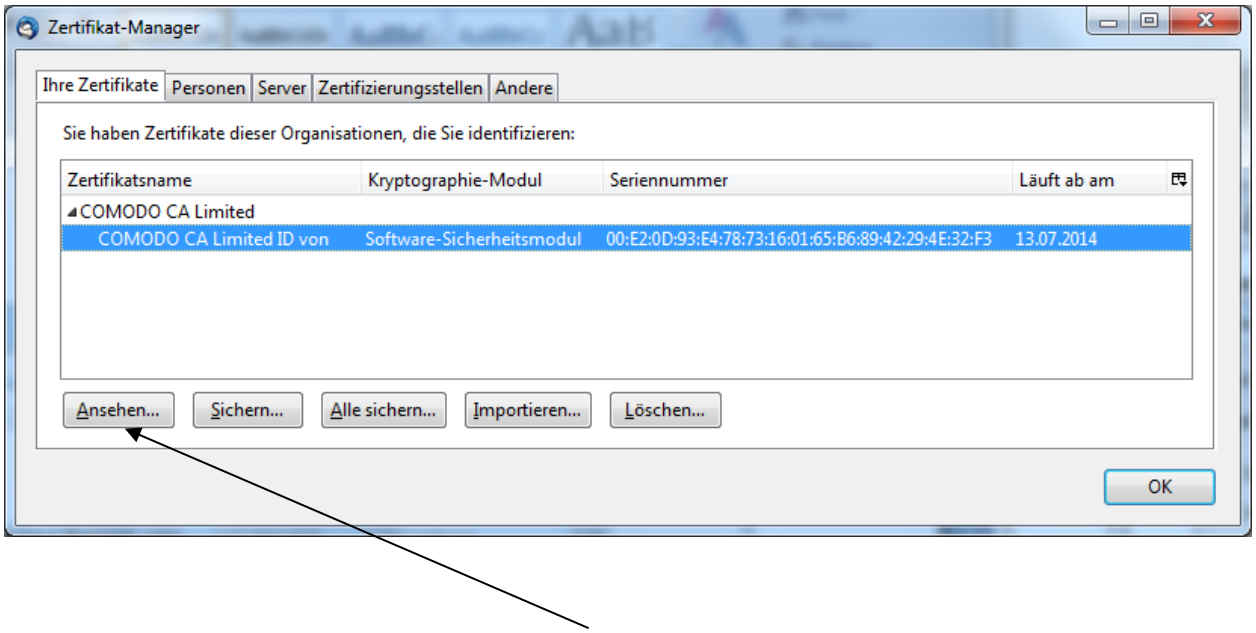
Importieren des Zertifikats aus der mit Firefox in Schritt 2 erzeugten P12-Datei.

Zum Öffnen der P12-Datei ist wieder das Passwort einzugeben:



Das Email-Zertifikat wurde erfolgreich in TB importiert:

Auch das ist keine Warnung, sondern eine Erfolgsmeldung. Genaugenommen werden **ein** Zertifikat, **ein** öffentlicher Schlüssel und **ein** privater Schlüssel im TB-Keystore gespeichert.



Teilschritt 3a ist nun erledigt. Mit dem Button „Ansehen“ kann man sich sein Zertifikat anzeigen lassen (siehe nächste Seite).

Hinweis zur P12-Datei:

Anschließend sollte das Backup-File wieder gelöscht oder zumindest an einen sicheren Ort gebracht werden.

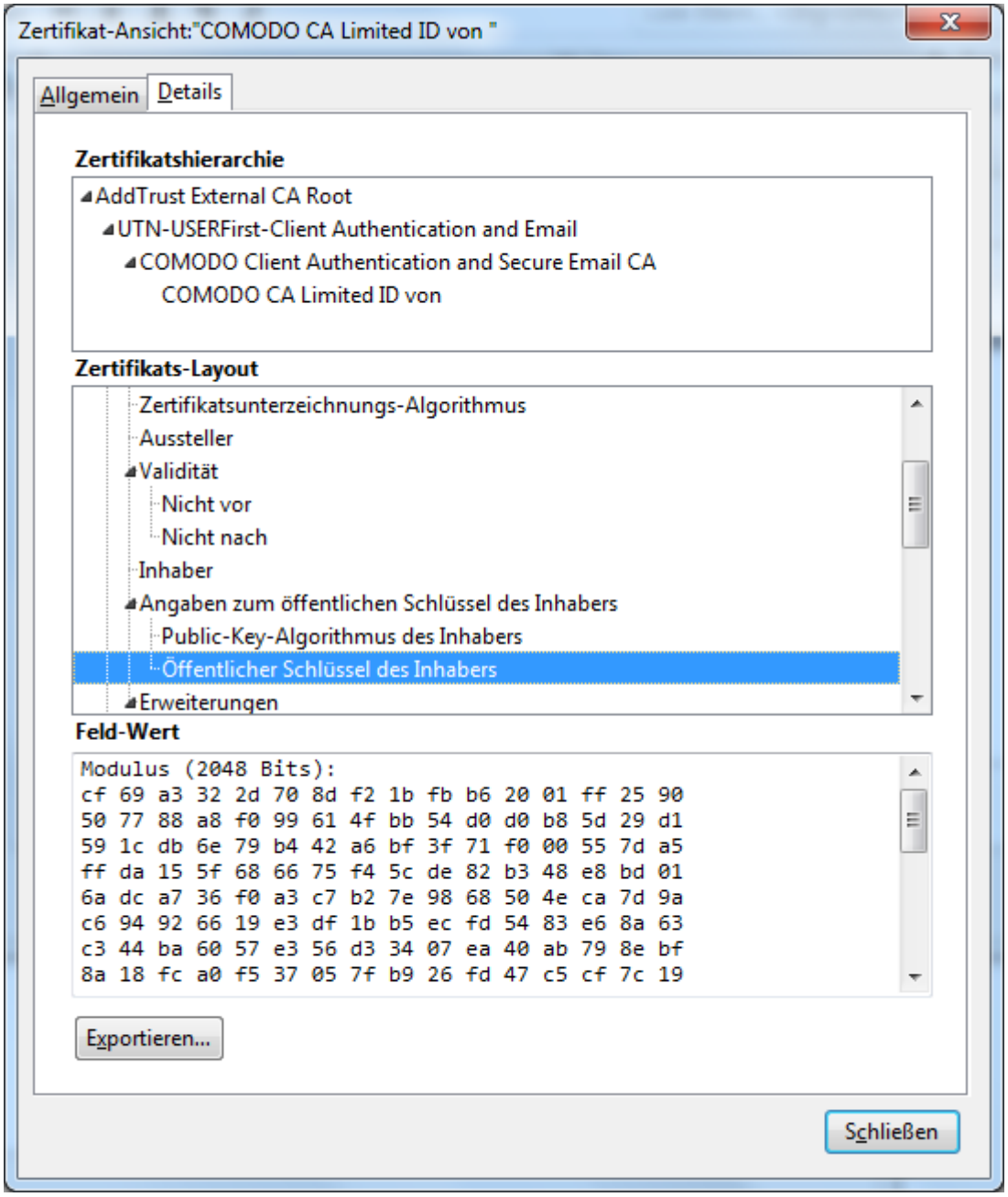
Dieser Hinweis bezieht sich auf das **Minimal-Exposure-Prinzip**, denn der Schlüssel liegt jetzt an drei Stellen vor: im FF-Keystore, als P12-Datei und im Thunderbird-Keystore [mit (verschiedenen) Passwörtern gesichert].

Technisch benötigt wird er nur im Mozilla-Keystore für Thunderbird, so dass man die beiden anderen entfernen kann (siehe den Hinweis am Ende von Schritt 2) und sich höchstens eine „sichere“ Offline-Kopie der P12-Datei (kein Internet-Access) irgendwo ablegt.

Nur zur Information:

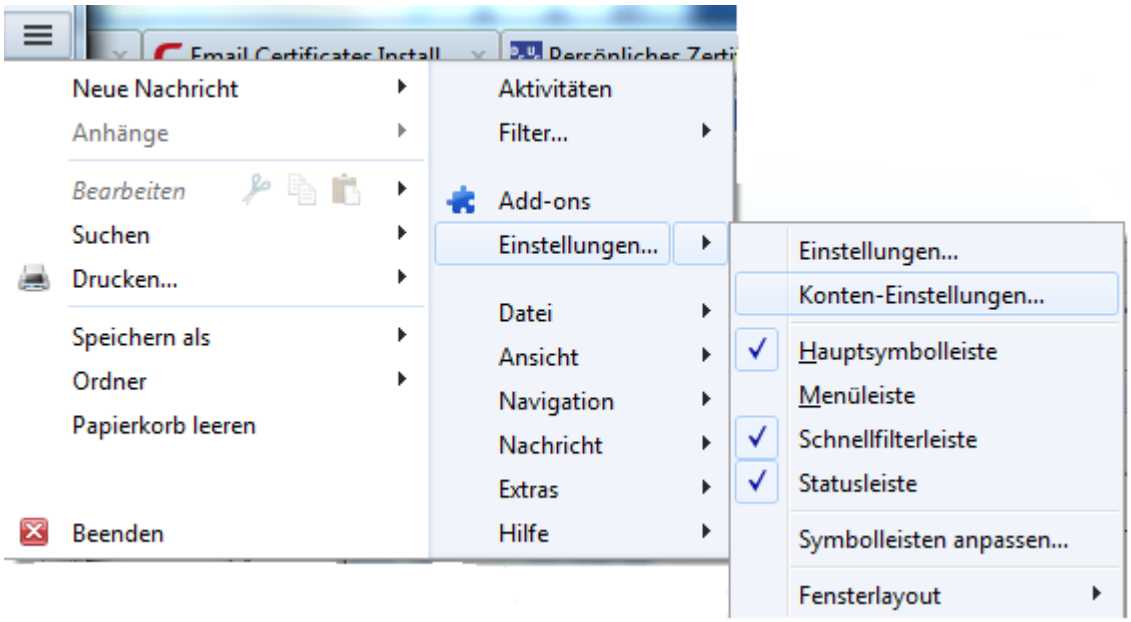
Falls man sehen will, was für ein Zertifikat man sich in TB installiert hat:

Klick auf den Reiter „Details“ → Unter den „Angaben zum öffentlichen Schlüssel des Inhabers“ sieht man, dass RSA mit 2048 Bit genutzt wird, was ok ist. (Würde das RSA-Verfahren geknackt, müssten die Trustcenter Zertifikate mit anderen Verfahren wie z.B. ECC anbieten).



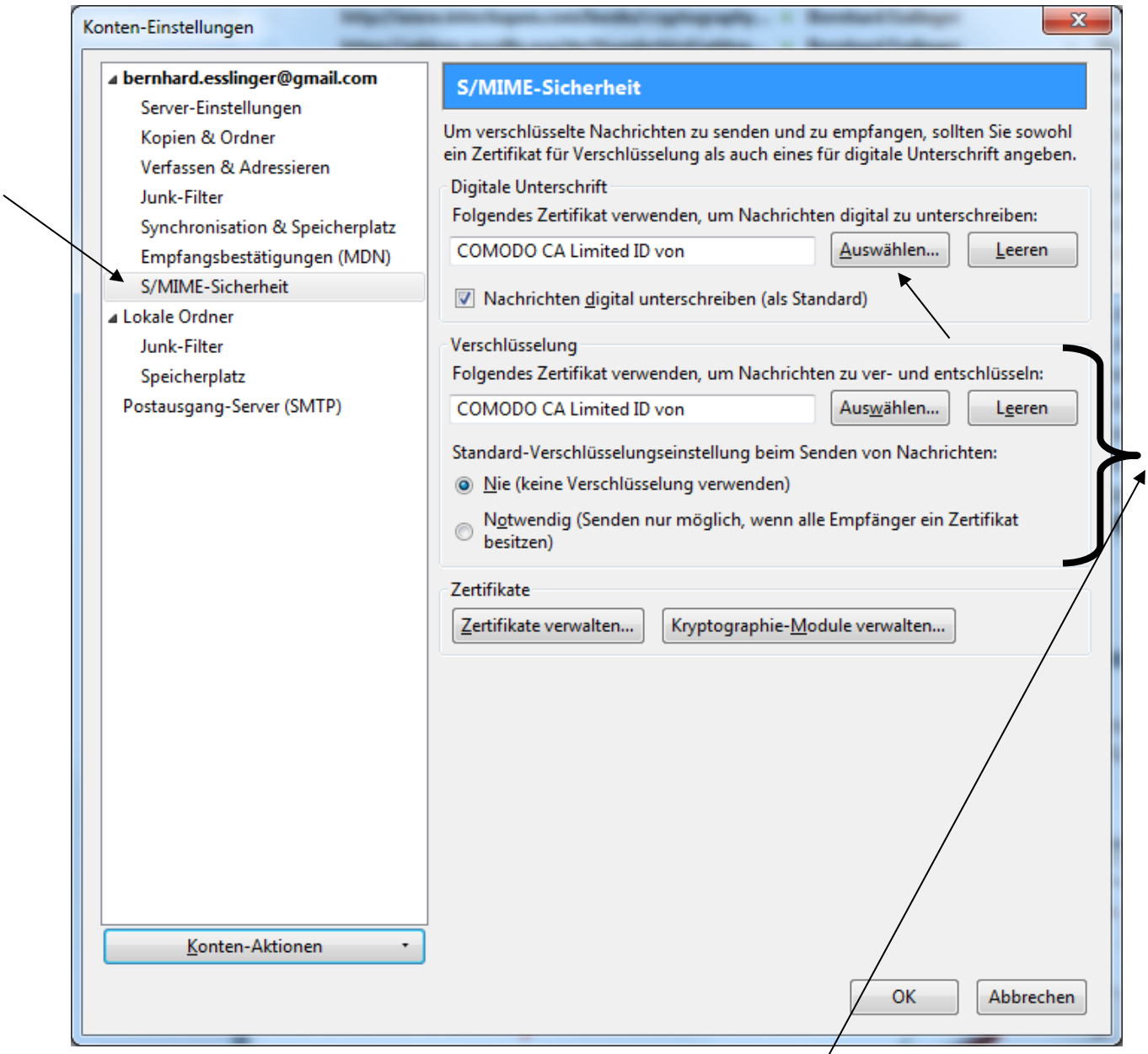
Teilschritt 3b:

Noch eine **letzte Aktion ist in Schritt 3** nötig: Das in TB installierte Zertifikat wird nicht automatisch beim Mailen verwendet, sondern muss in TB erst noch für den Email-Account konfiguriert werden:



Dazu ist im Dialog „Konten-Einstellungen“ unter „S/MIME-Sicherheit“ das eigene Zertifikat vorzusehen für:

- Signieren (Default)
- Verschlüsseln (**nicht** als Default)



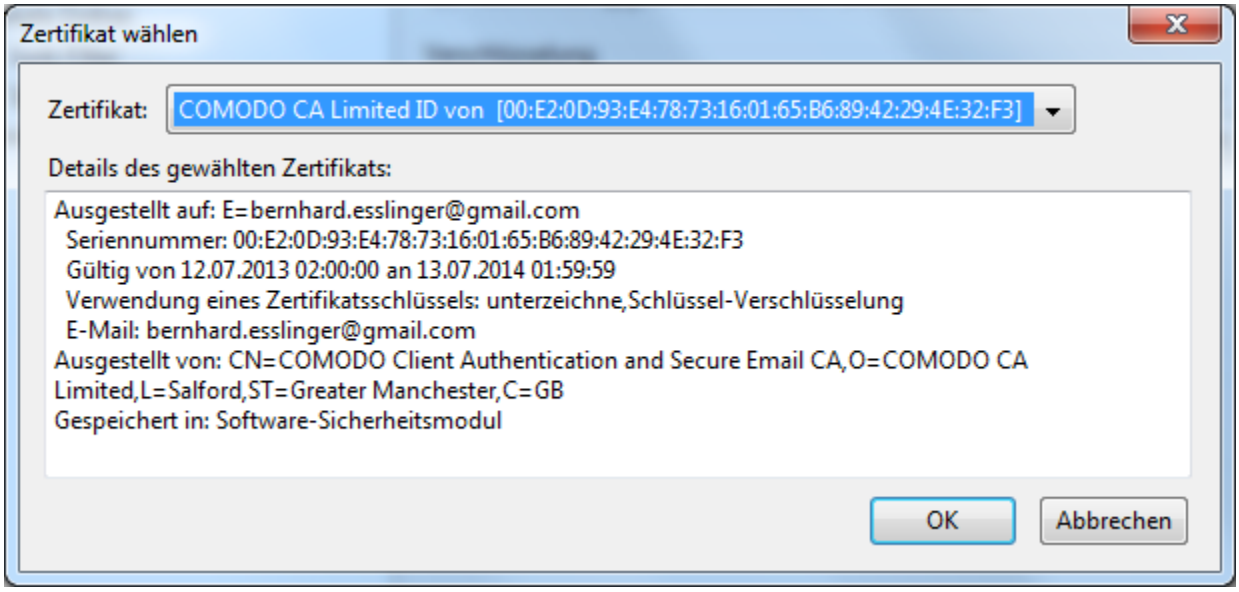
Hier oben in der Gruppierung „Digitale Unterschrift“ auf „Auswählen“ klicken.

Bemerkung zur Default-Einstellung beim verschlüsselten Senden:

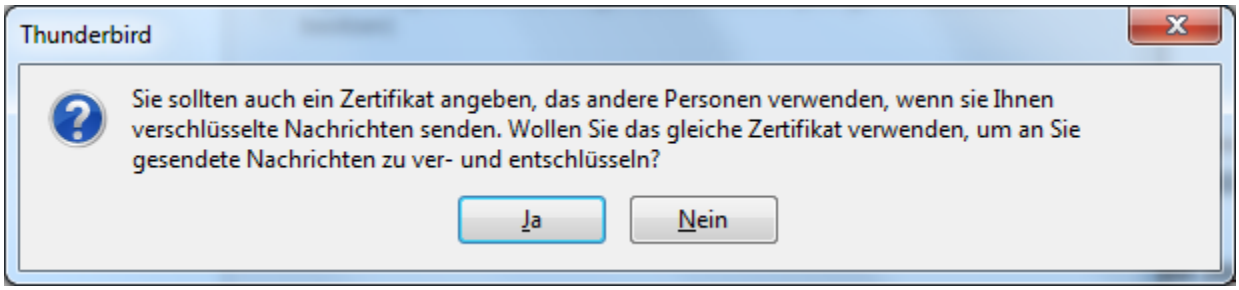
In der Gruppierung „Verschlüsselung“ gibt es nur zwei Auswahlmöglichkeiten: Nie oder immer verschlüsseln.

Sinnvoll wäre ein dritter Button: Dann verschlüsseln, wenn man von den Empfängern schon Zertifikate hat. Da dies TB standardmäßig noch nicht implementiert hat, wird in Schritt 5 gezeigt, wie man diese Funktionalität optional mit dem Plugin „Encrypt-if-possible“ nachrüstet.

Bei der Auswahl zeigt TB gleich das installierte Zertifikat an:



TB fragt von selbst, ob man *dasselbe* Zertifikat zum Signieren und Verschlüsseln nutzen will – für Privatzwecke ist das ok:

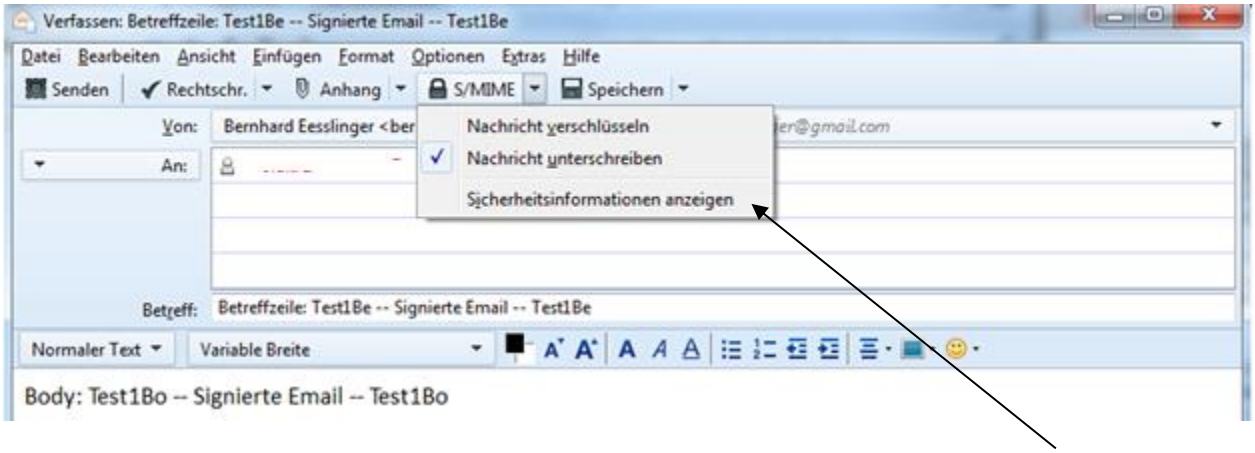


Schritt 4: Sende eine signierte Email

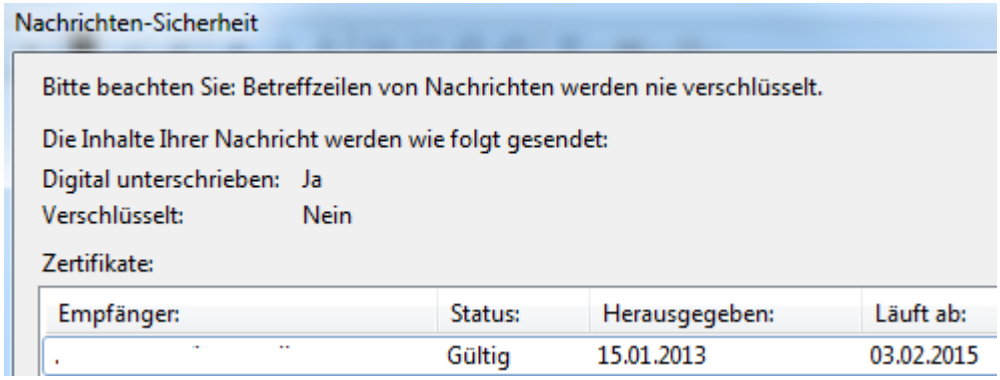
Erster Kommunikationsteilnehmer sendet eine signierte Mail, der zweite kann sofort verschlüsselt antworten.

Gehe in TB im Hauptfenster auf „Verfassen“.

Im Verfassen-Fenster ist unter dem S/MIME-Button bei „Nachricht unterschreiben“ schon ein Haken.



Den Status der Nachricht und des Empfängerzertifikats kann man **VOR** dem Senden im 3. Eintrag unter „S/MIME“ sehen:



Wichtige Info:

Hat man (als Sender) noch kein Zertifikat für den Empfänger, kann man ihm auch keine Email verschlüsselt senden.

Hat man selbst ein Zertifikat, kann man seine eigenen Nachrichten immer signieren (egal, ob der Sender ein Zertifikat hat oder nicht).

- ⇨ Der Empfänger erhält mit der **signierten** Email zugleich auch mein Email-Zertifikat (einfacher Austausch des Zertifikats).

Evtl. Bedienungsprobleme für neue Benutzer (Usability):

- Aktivieren des erhaltenen Zertifikats im Mail-Client (z.B. TB):
    - Das Zertifikat eines Kommunikationspartners wird automatisch im Mozilla-Keystore für Thunderbird gespeichert.
      Explizit Vertrauen aussprechen muss man einem anderen Zertifikat und dessen Zertifizierungsstelle nur dann, wenn die Zertifizierungsstelle nicht standardmäßig im Thunderbird-Keystore enthalten ist. Comodo ist standardmäßig vorhanden.
    - Leider werden die Zertifikate im Keystore, denen man das Vertrauen aussprach, von TB nicht extra geflaggt (grafisch gekennzeichnet), so dass man nicht optisch signalisiert bekommt, welches Vertrauen ausgesprochen ist.

- Der Menüeintrag unter „S/MIME“ lautet: „Nachricht unterschreiben“.
  Klarer wäre die Verwendung des Wortes „signieren“:
  → „Nachricht unterschreiben / signieren“

- Die Volltextsuche ist bei verschlüsselten Mails eingeschränkt: Über die Header- und Sender-/Empfangsinformationen kann man suchen, aber nicht über den Mail-Inhalt.
  → Das wäre eine gute Idee für ein weiteres Plugin.

- Wenn man TB neu installiert, kennt er noch keinen der Kommunikationspartner. Empfangene Emails landen also zuerst im Order „Unbekannt“. Verschiebt man sie mit der Maus einmal in den Ordner „Posteingang“, landen alle folgenden Mails dieses Absenders ab nun ebenfalls im Ordner „Posteingang“.

WICHTIG:

In beiden Richtungen verschlüsseln und signieren geht nur, wenn alle Kommunikationsteilnehmer (Sender und Empfänger) ein Zertifikat haben.

Solange man nur selbst ein Zertifikat hat, kann man
- signieren (und jeder andere Empfänger kann die Authentizität prüfen), und
- eine erhaltene verschlüsselte Mail auch wieder entschlüsseln.

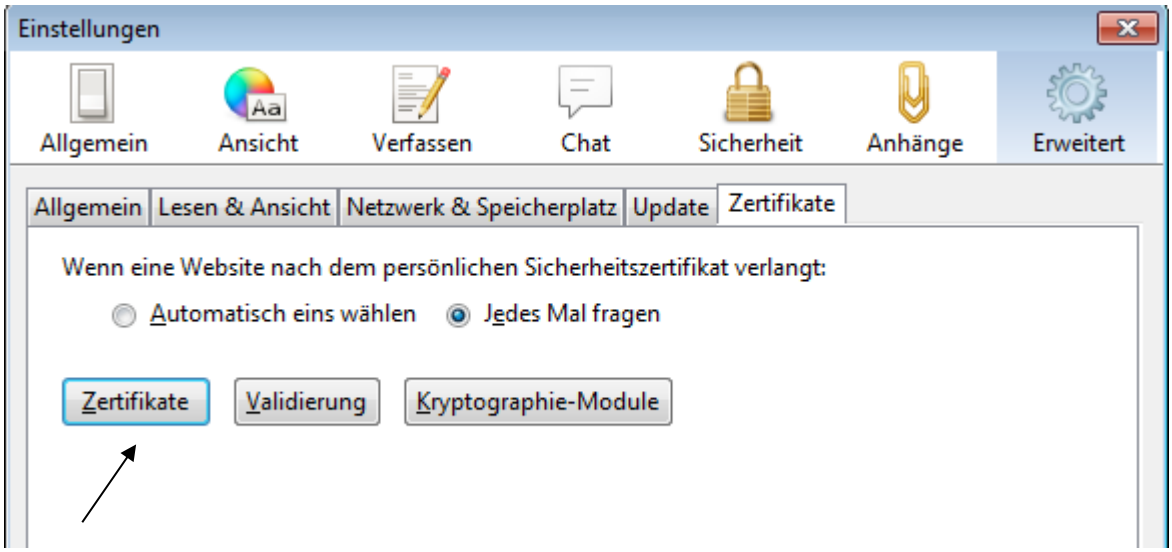
Was hat man davon?

- Mails werden verschlüsselt übertragen.
- Sie liegen auch lokal verschlüsselt vor, bis man TB seinen privaten Schlüssel zugänglich macht.
- Verschlüsselte Mails (erhaltene oder versandte) sind durch den privaten Schlüssel geschützt.

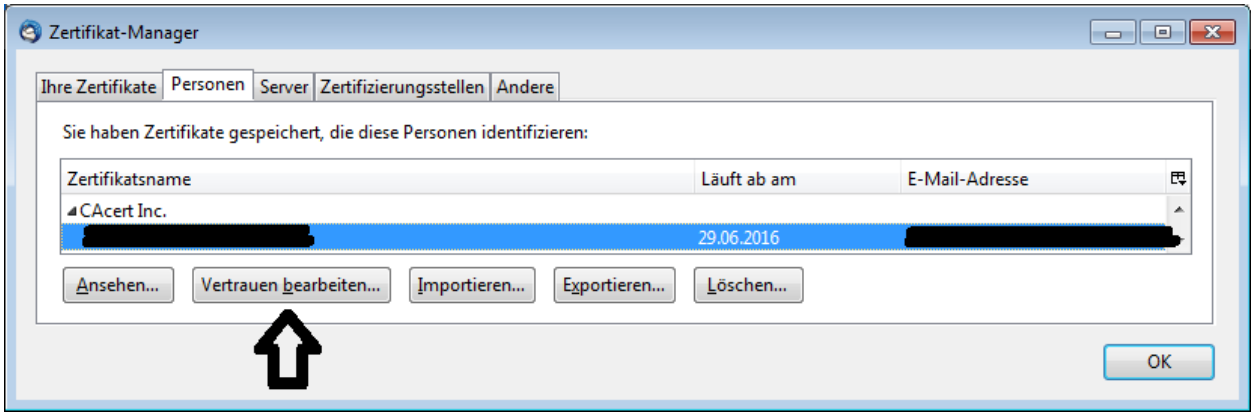
Explizit einem Zertifikat aus einer empfangenen Email das Vertrauen aussprechen

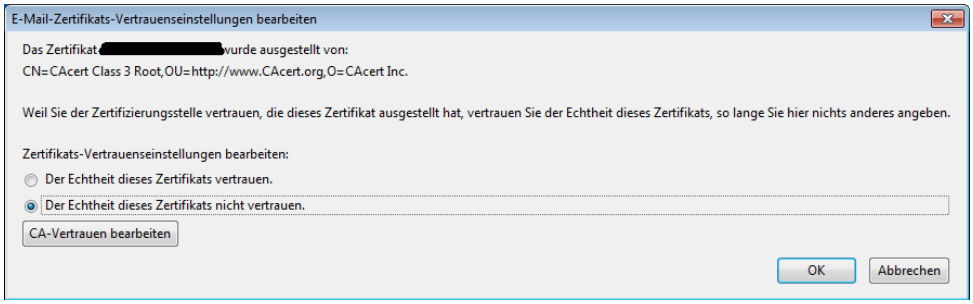
- Das ist nur nötig, falls der Zertifikats-Aussteller nicht im Thunderbird-Keystore enthalten ist (Comodo z.B. ist vorhanden; CAcert nicht). Vgl. Anhang B, S. 34 für CA-Zertifikate.

Klick auf Einstellungen → Zertifikate.



Im dann erscheinenden Zertifikat-Manager-Dialog auf den Reiter „Personen“ (Kommunikationspartner) und den Button „Vertrauen bearbeiten“ klicken.

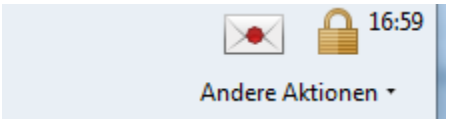




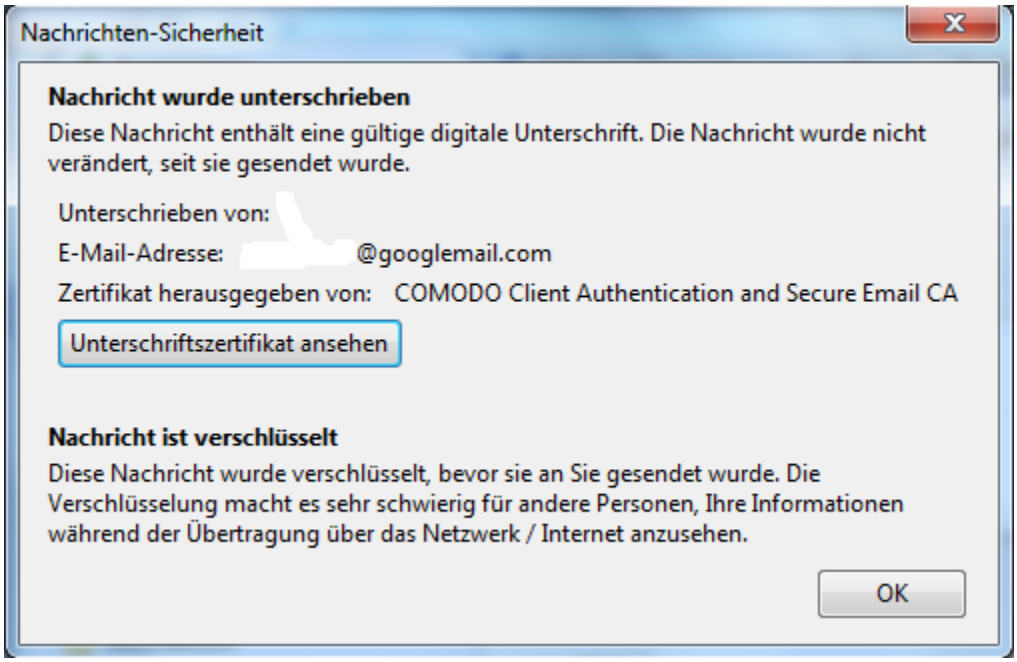
Das Vertrauen aussprechen, indem man den Radiobutton unter „Zertifikats-Vertrauenseinstellungen bearbeiten“ umsetzt. Nun kann ich an diesen Empfänger zurück verschlüsselt mailen.

Mailaustausch:

Hat man eine Mail erhalten, die verschlüsselt und signiert ist, zeigt TB die folgenden Ikonen (Buttons) an:



Beim Klick auf eine der beiden Ikonen, kommt jedes Mal dieselbe Dialogbox:

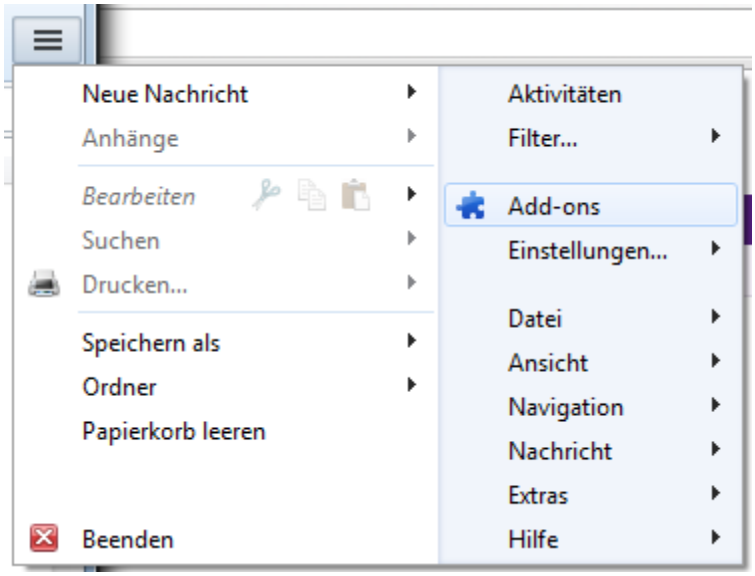


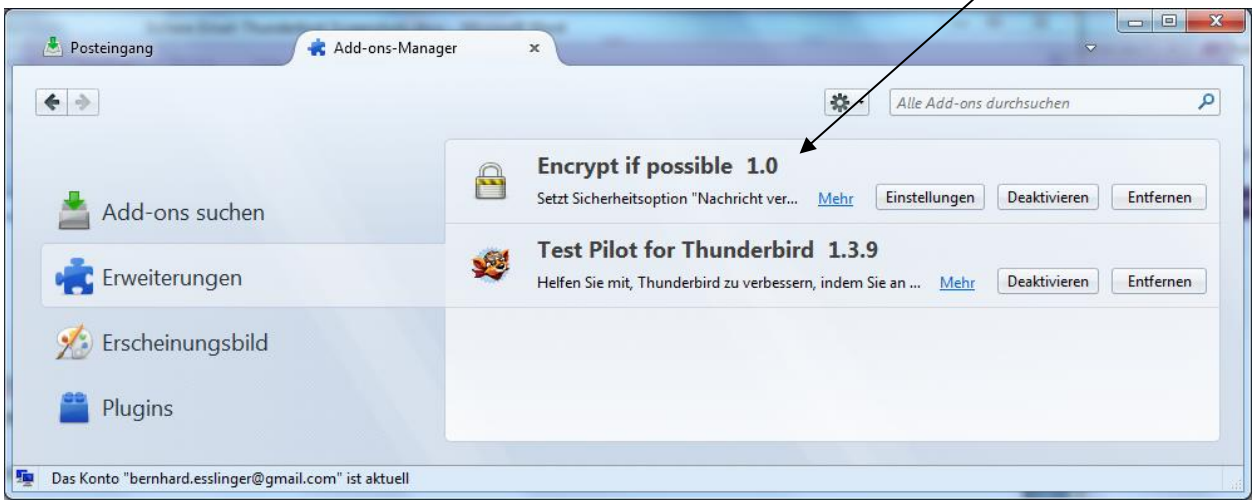
Schritt 5 (optional): Encrypt-if-Possible

Optional: Installation der Encrypt-if-Possible-Erweiterung

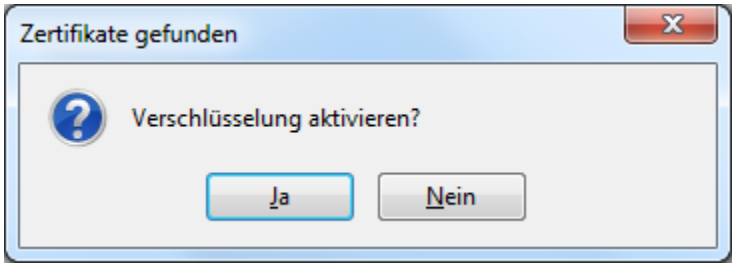
Installieren des Encrypt-if-Possible-Plugins in Thunderbird, damit TB immer verschlüsselt, wenn ich von allen in der Mail aufgeführten Empfängern (und auch selbst) ein gültiges Email-Zertifikat habe.

https://addons.mozilla.org/de/thunderbird/addon/encrypt-if-possible/





Das Plugin fragt beim Erstellen einer neuen Mail, ob man die Verschlüsselung aktivieren möchte:

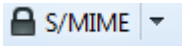


Wenn man auf Antworten geht und die Nachricht schon verschlüsselt war, fragt er nicht nochmal, sondern setzt es gleich auf Verschlüsseln (das ist das Standard-Verhalten von TB).

Anhang: Weitere Infos

Übersicht Anhang:

A) Was sollte man als Laie wissen?

1) Was man als normaler User (der sich nicht für Krypto interessiert) unbedingt über S/MIME-Nutzung wissen und tun sollte:
   Der Einstieg ist ganz einfach – man braucht nur vier Schritte:
   - Installiere Thunderbird,
   - Erzeuge ein Zertifikat (erhält man kostenlos von einem Trustcenter, macht man im Browser),
   - Installiere das Zertifikat in TB,
   - Sende eine signierte Email an alle, mit denen man sicher kommunizieren möchte; und nutze danach die S/MIME-Sicherheitseinstellungen 

   Dann sollte man seine Kommunikationspartner animieren, auch sichere Email zu nutzen !!!

2) Was man zusätzlich an Krypto-Wissen mitgeben könnte, z.B.:
   - Verschlüsselt wird nur der Mail-Körper, aber nicht die Titelzeile (der Betreff oder Subject).
   - Das Schlüsselpaar wird von Firefox **lokal** erzeugt, der private Schlüssel nicht weggeschickt.
   - Das Trustcenter (CA) erhält zum Erstellen des Zertifikats nur den öffentlichen Schlüssel.
   - Das Zertifikat enthält den öffentlichen Schlüssel und Metainformation zum Inhaber und Aussteller. Die PKCS12-Datei enthält den privaten Schlüssel und das Zertifikat.

3) WICHTIG:
   - Abgelaufene (eigene und fremde) Zertifikate, und den eigenen privaten Schlüssel muss man aufheben, sonst hat man keine Chance, seine früheren verschlüsselten Emails zu lesen!
   - Wenn einem der Kommunikationspartner eine signierte Email mit einem neuen Zertifikat schickt (weil sein altes abgelaufen war oder weil er es sperren ließ), nimmt TB automatisch für diese Person das neue Zertifikat (gut ist, dass man nichts dazu tun muss; etwas schlecht ist, dass TB einem nicht mal eine Meldung bringt, dass das Zertifikat ausgetauscht wurde).

4) Was darüber hinaus wissenswert ist?

1) Inhalt eines Benutzer-Zertifikats:
Das Enduserzertifikat enthält den öffentlichen Schlüssel des Eigentümers (Subject, Owner) und den Domain-Namen (DN) des Ausstellers (Issuer, CA) – das ausstellende Zertifikat ist also nur referenziert, aber nicht darin enthalten. Es liegt im Format X509v3 vor.
Vgl.: http://fusesource.com/docs/broker/5.3/security/i284538.html
Die Mail-Clients schicken aber oft die gesamte Zertifikatskette mit, so dass man die Aussteller- Zertifikate mit einer signierten Email auch gleich mit bekommt.
Das ist aber nicht zwingend (Outlook macht das so, Thunderbird (meist? – Ja macht auch Thunderbird, aber ohne das Root Zertifikat, was absolut Sinn macht. Antwort ist also ja ☺) auch.

2) Import eines erhaltenen Zertifikats in den Keystore:
- Thunderbird importiert Benutzer-Zertifikate automatisch, wenn er das Aussteller-Zertifikat schon getrusted hat. Ist das nicht der Fall, muss man erst das Aussteller-Zertifikat importieren (vgl. Anhang „B) Aufnehmen des Zertifikats einer weiteren Zertifizierungsstelle (CA) in den TB-Keystore“), dann noch extra das User Zertifikat (etwas umständlich über den Zertifikatsmanager, mit vorigem Exportieren der Zertifikate aus der Mail). Man kann auch das Aussteller-Zertifikat exportieren, sofern es in der Mail mit enthalten ist, ansonsten muss man das erst runterladen.
- Outlook ist da etwas nutzerfreundlicher und bietet die Optionen direkt aus der Mail heraus.

3) Inhalt einer P12-Datei:
In der P12-Datei sind normalerweise nur der eigene Schlüssel und das zugehörige Zertifikat enthalten.
Vgl.: http://fusesource.com/docs/esb/4.4/cxf_security/i298613.html
Es gibt aber auch die Möglichkeit, die gesamte zugehörige Zertifikatskette zum Aussteller mit abzuspeichern (optional).

B) Aufnehmen des Zertifikats einer weiteren Zertifizierungsstelle (CA) in den TB-Keystore

Dies kann nötig sein, wenn die CA nicht standardmäßig im Mozilla-Keystore von Thunderbird enthalten ist. Dies kann vorkommen, wenn man sein eigenes Zertifikat bei einer solchen CA beantragt, oder wenn man Kommunikationspartner hat, deren Aussteller-CA nicht standardmäßig im Thunderbird-Keystore enthalten ist. Falls das CA-Zertifikat nicht im TB-Keystore enthalten ist, aber im Zertifikat der empfangenen Email, kann man es leicht in dem TB-Keystore mit importieren (s. S. 28).

Heute haben viele Firmen eine eigene PKI (Public-Key-Infrastruktur). Diese können hochprofessionell betrieben und gesichert sein (mit regelmäßigem Key-Roll-over und Schlüsselverwahrung in HSMs [Hardware-Security-Modules]), und sich trotzdem nicht in den (teuer zu bezahlenden) Keystores der Browser-Hersteller befinden.

Auf den folgenden Seiten sind 4 Beispiel-Szenarien für vertrauenswürdige CA-Zertifikate, die nicht in Webbrowsern enthalten sind, erläutert:

1) Beispiel-Szenario anhand der Firmen-PKI der Deutschen Bank (DB), S. 35
2) Beispiel-Szenario anhand des Trustcenters CAcert, S. 43
3) Beispiel-Szenario anhand des Trustcenters CERT-Bund, S. 48
4) Beispiel-Szenario anhand des Verbundes vertrauenswürdiger PKIs der EBCA, S. 51

1. Beispiel-Szenario anhand der Firmen-PKI der Deutschen Bank (DB)

Der private TB-Benutzer (er könnte ein Mitarbeiter oder ein Kunde sein) hat eine signierte Mail an einen DB-Mitarbeiter gesandt. Der DB-Mitarbeiter antwortet signiert und verschlüsselt, der TB-Benutzer (Empfänger) enthält also eine signierte und verschlüsselte Email von einem DB-Mitarbeiter. Thunderbird kann (erstmal) die Signatur nicht validieren, weil er das Aussteller-Zertifikat der DB-CA nicht kennt.

TB zeigt in der Mail das Symbol für eine ungültige Signatur: 

Um der DB-CA das Vertrauen aussprechen, braucht der private TB-Nutzer mehrere Schritte:

1) Die direkt übergeordnete CA exportieren.
2) Diese CA in den Zertifikatsstore importieren und für Email vertrauen.
3) Dann die Email schließen und erneut öffnen.

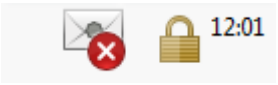
   Anschließend wird die Signatur korrekt angezeigt: 

Es ist wichtig, diese Reihenfolge einzuhalten. Welche Fehlermeldungen kommen, wenn man diese Reihenfolge nicht einhält, steht am Ende von Anhang B.

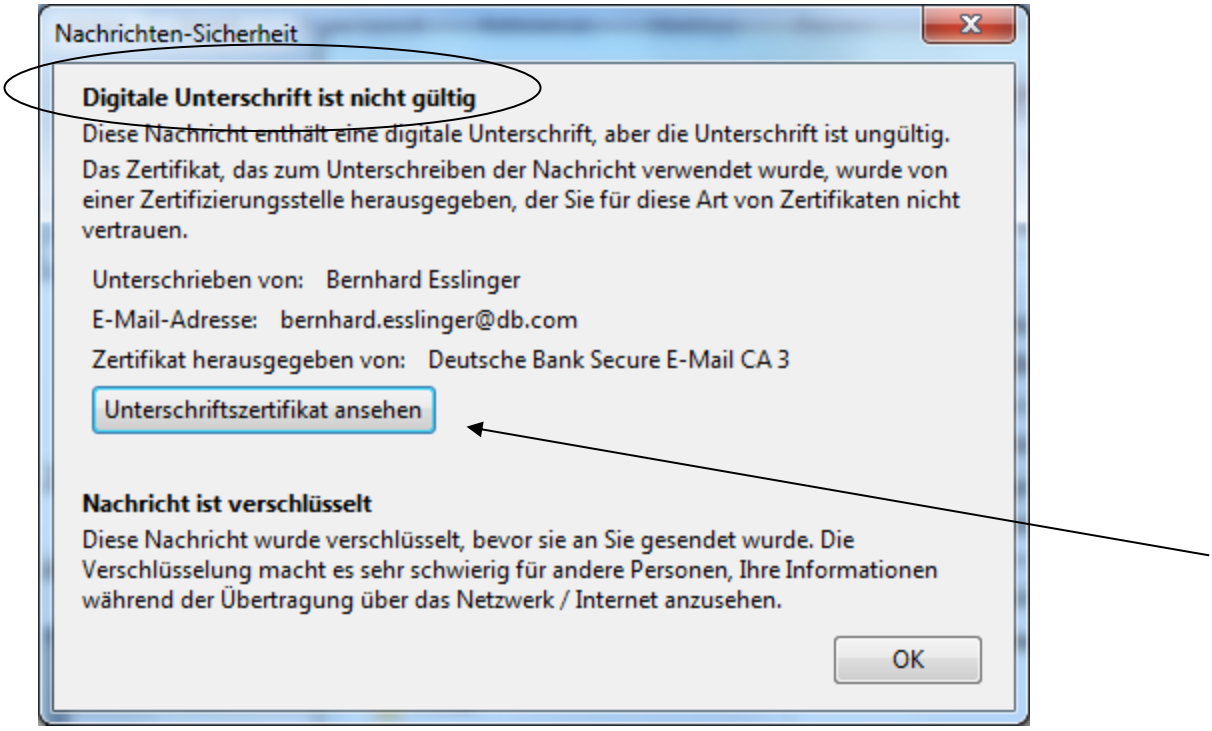
1) Direkt übergeordnete CA aus der Mail heraus exportieren

Mit der signierten Mail wurden das Zertifikat des Senders (und auch die Zertifikate der CAs, die das Zertifikat des Senders erstellten) mit geschickt. Aus der Kette der CA-Zertifikate ist erst einmal nur der direkt darüber liegenden CA (diese stellte das Sender-Zertifikat aus) das Vertrauen auszusprechen.

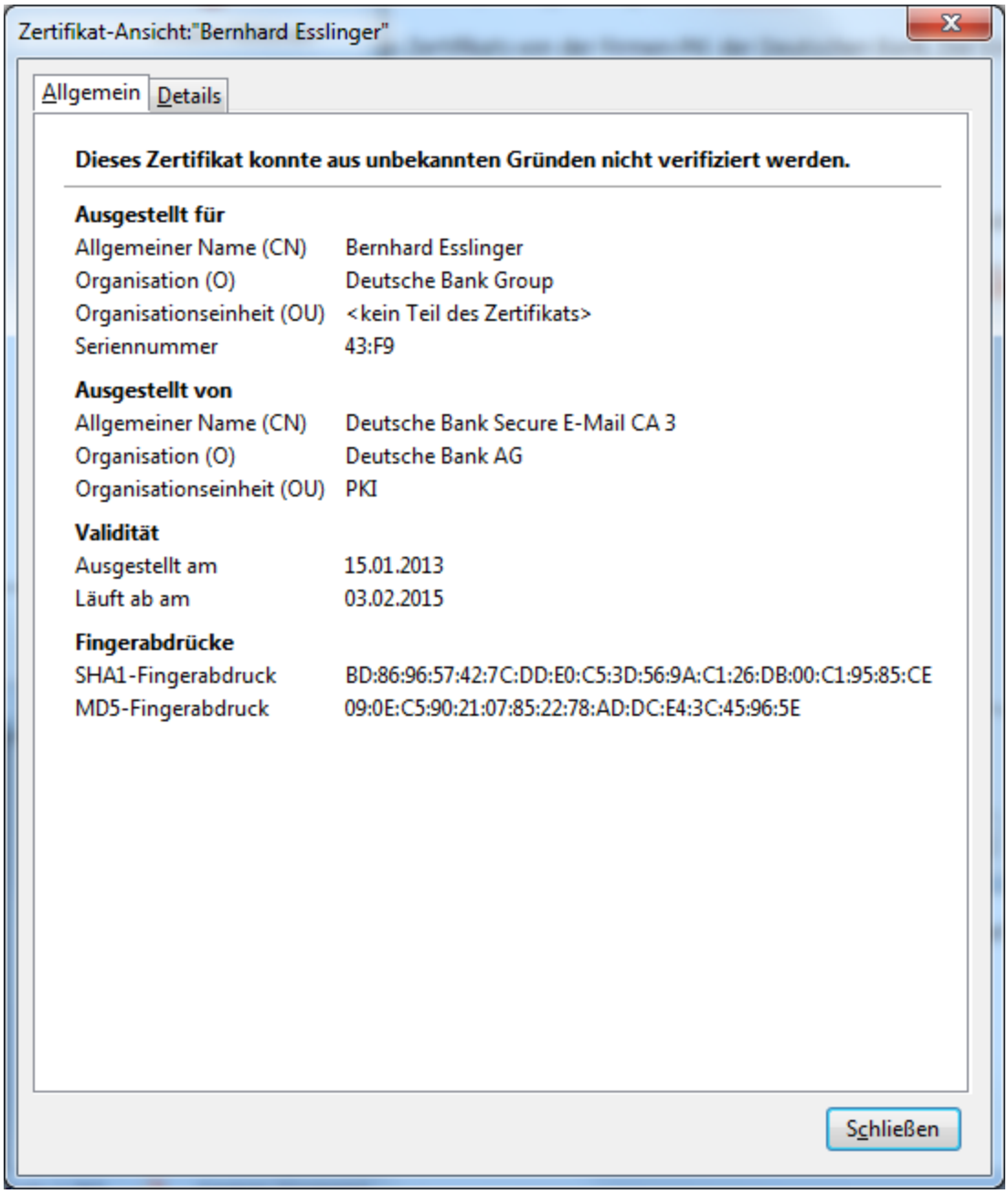
Zum entsprechenden Dialog kommt man am besten auf diesem Weg:

a) Anklicken des Signatur-Symbols in der Mail: 

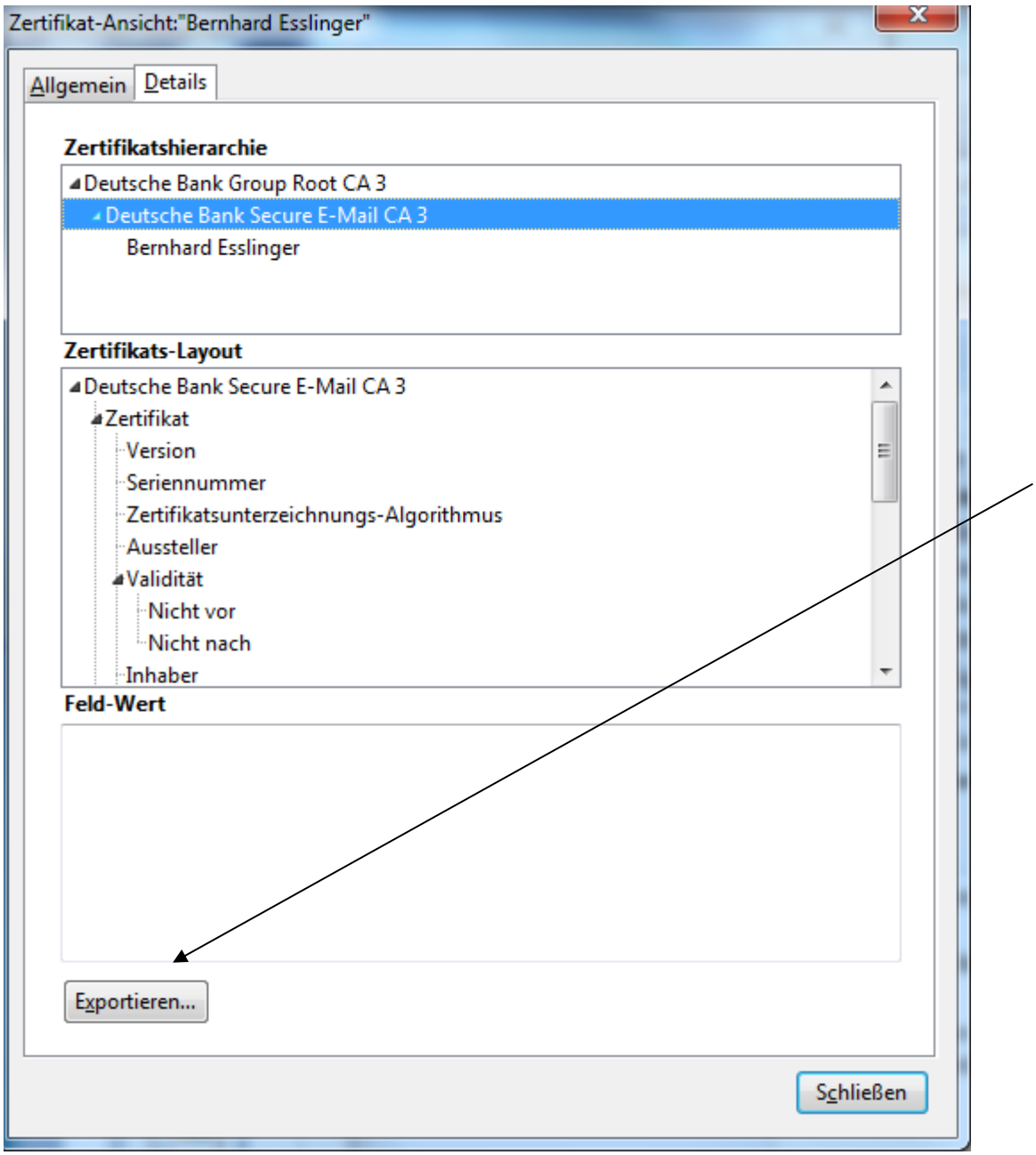
Somit erfährt man Genaueres: TB kennt die Aussteller-CA nicht.



b) Klick auf den Button „Unterschriftszertifikat ansehen“ bringt den ff. Dialog:


Zertifikat-Ansicht:"Bernhard Esslinger"
Allgemein
Details
Dieses Zertifikat konnte aus unbekannten Gründen nicht verifiziert werden.
Ausgestellt für
Allgemeiner Name (CN) Bernhard Esslinger
Organisation (O) Deutsche Bank Group
Organisationseinheit (OU) <kein Teil des Zertifikats>
Seriennummer 43:F9
Ausgestellt von
Allgemeiner Name (CN) Deutsche Bank Secure E-Mail CA 3
Organisation (O) Deutsche Bank AG
Organisationseinheit (OU) PKI
Validität
Ausgestellt am 15.01.2013
Läuft ab am 03.02.2015
Fingerabdrücke
SHA1-Fingerabdruck BD:86:96:57:42:7C:DD:E0:C5:3D:56:9A:C1:26:DB:00:C1:95:85:CE
MD5-Fingerabdruck 09:0E:C5:90:21:07:85:22:78:AD:DC:E4:3C:45:96:5E
Schließen

c) Wechsel in den Reiter „Details“, Auswahl der direkt über dem Sender liegenden CA (hier „Secure E-Mail CA 3“) und dann Klick auf den Button „Exportieren“.



Das Zertifikat wird in der Datei „DeutscheBankSecureE-MailCA3.crt“ abgelegt.

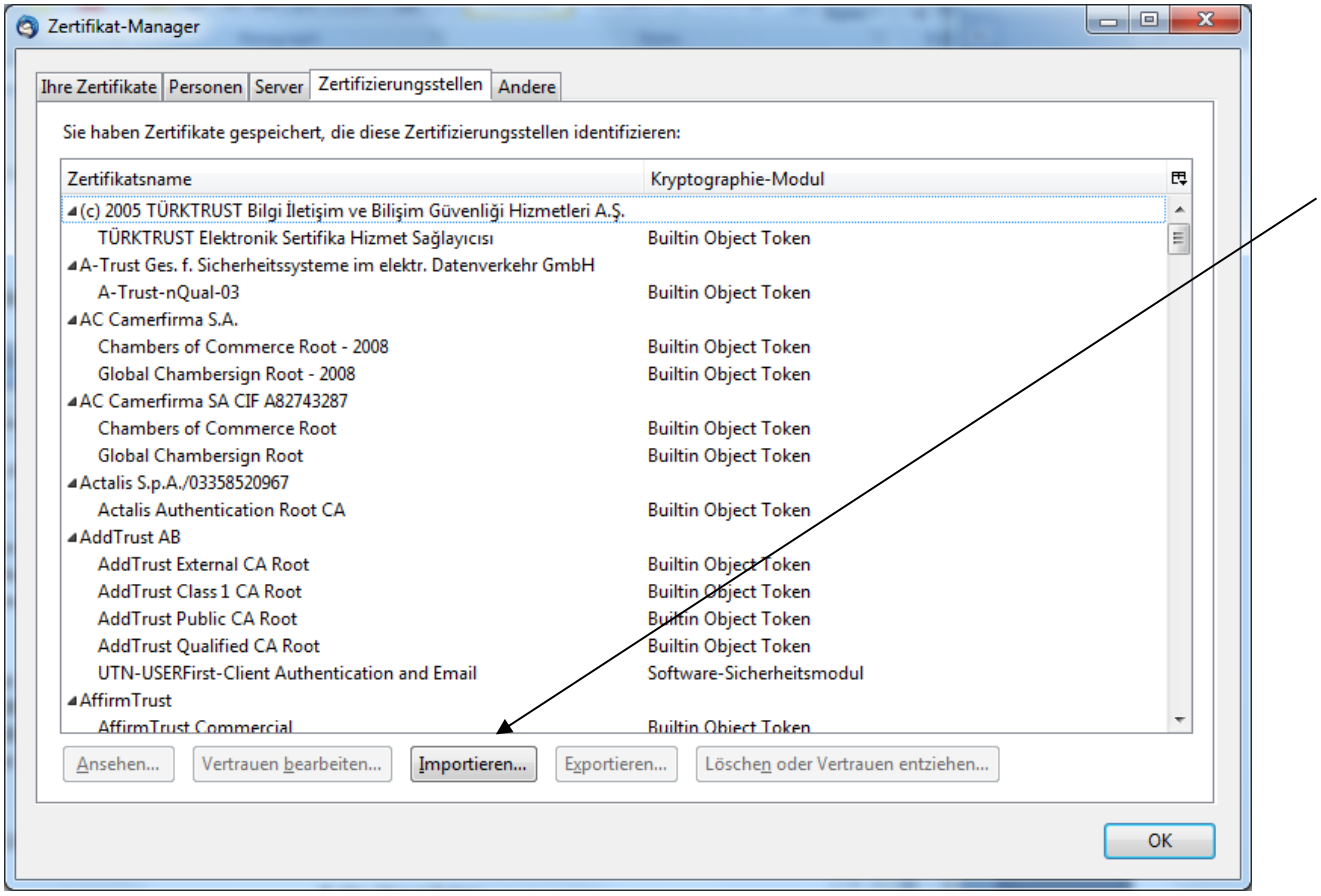
2) Diese CA in den TB-Zertifikatsstore importieren und für Email vertrauen

a) Klick auf die Ikone „Anwendungsmenü zeigen“

→ „Einstellungen“ → Tab oben „Erweitert“ → Tab „Zertifikate“

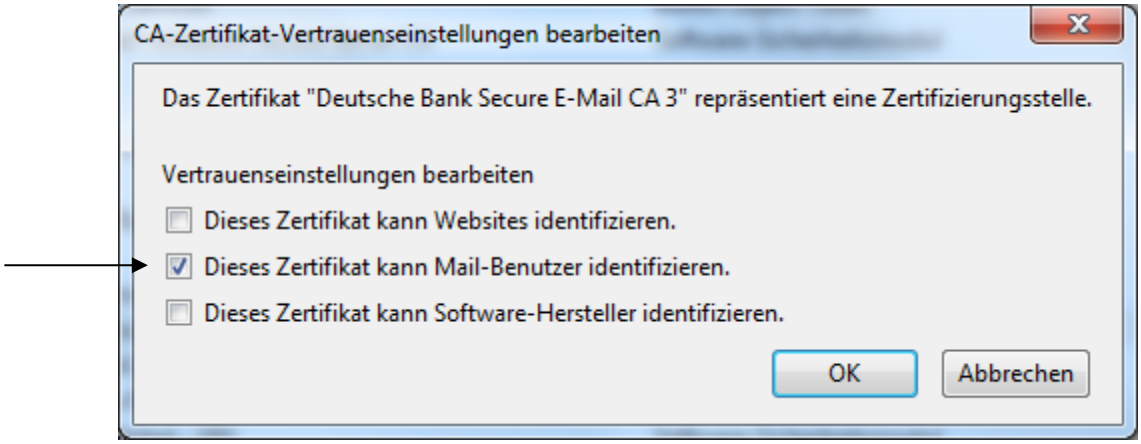
→ Button „Zertifikate“ → Tab „Zertifizierungsstellen“ (evtl. anderer Menüpfad in neueren TB)

Dann erhält man den Zertifikat-Manager:

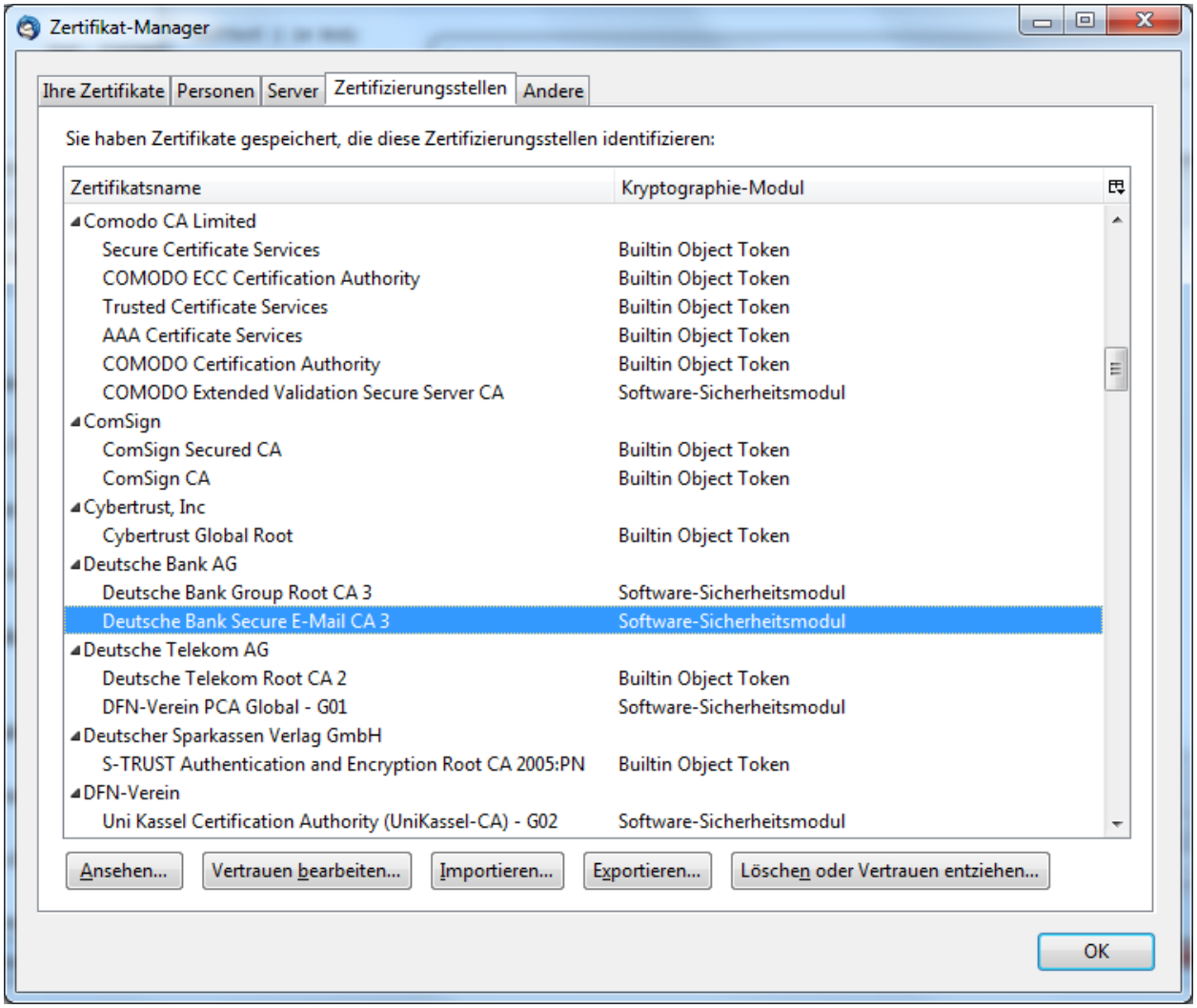


In diesem Dialog auf den Button „Importieren“ klicken – es wird gleich das Verzeichnis vorgeschlagen, in das die Datei „DeutscheBankSecureE-MailCA3.crt“ abgelegt wurde.

b) Im folgenden Dialog das Häkchen in der Mitte setzen:



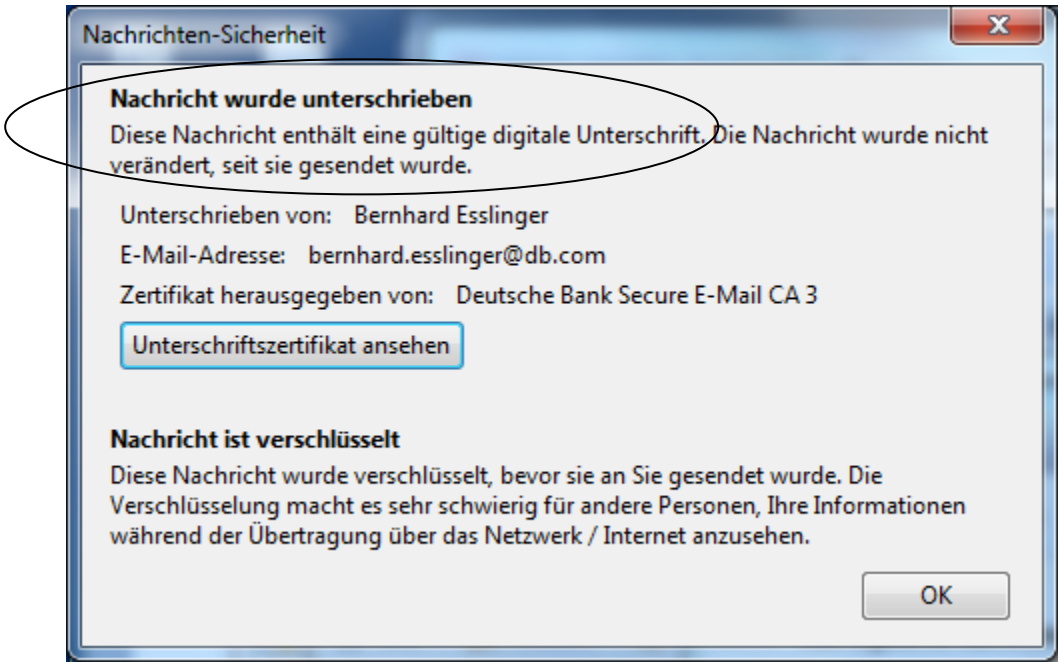
Nach Klick auf „Ok“ in diesem Dialog findet sich die DB-CA in der Liste der vertrauenswürdigen Zertifizierungsstellen:



3) Dann die empfangene Email schließen und erneut öffnen

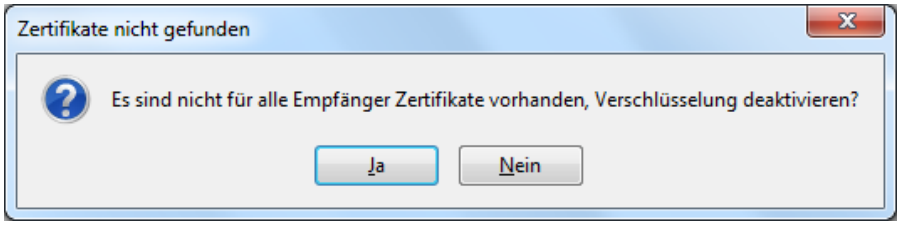
Anschließend wird die Signatur-Ikone korrekt angezeigt: 

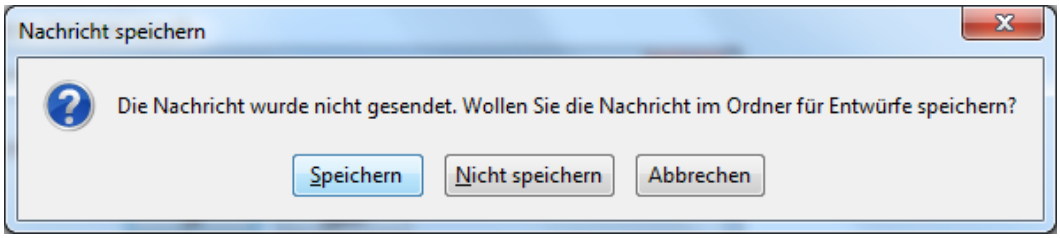
Klickt man auf die Signatur-Ikone, sieht man, dass die Signatur nun als gültig bewertet wird:



Den Sender von der DB findet man nun im Reiter „Personen“ unter „Deutsche Bank AG“.

Solange man nicht alle diese Schritte durchführte, kommen beim Erstellen einer Mail an diesen Empfänger immer wieder die folgenden Fehlermeldungen:

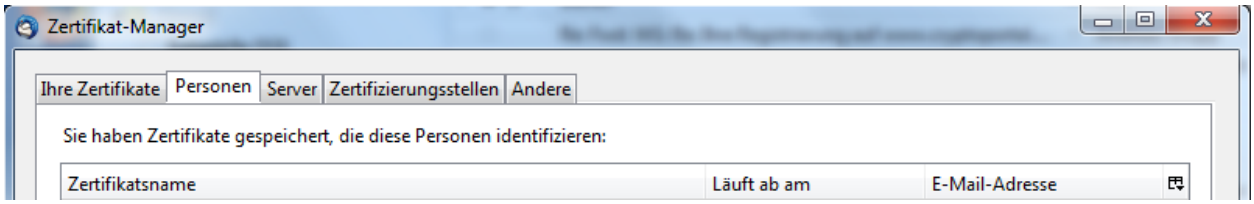




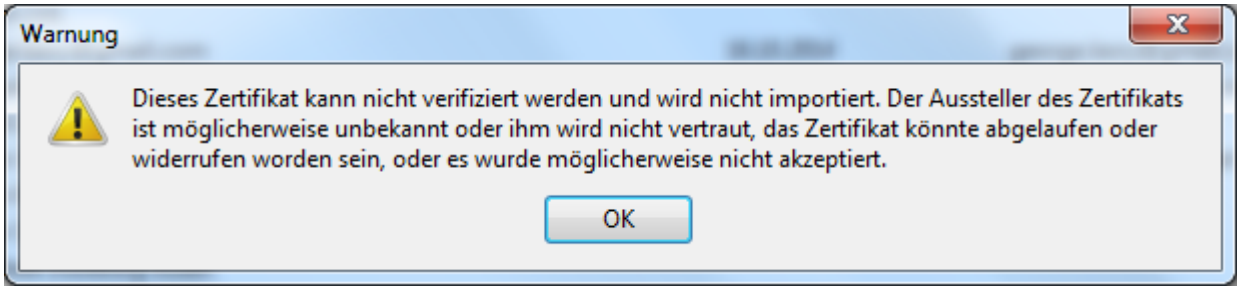
4) Es ist wichtig, die oben beschriebene **Reihenfolge** beim Import eines noch nicht im Keystore enthaltenen CA-Zertifikates einzuhalten.

Welche Fehlermeldungen kommen, wenn man diese Reihenfolge nicht einhält, wird im Folgenden dokumentiert:

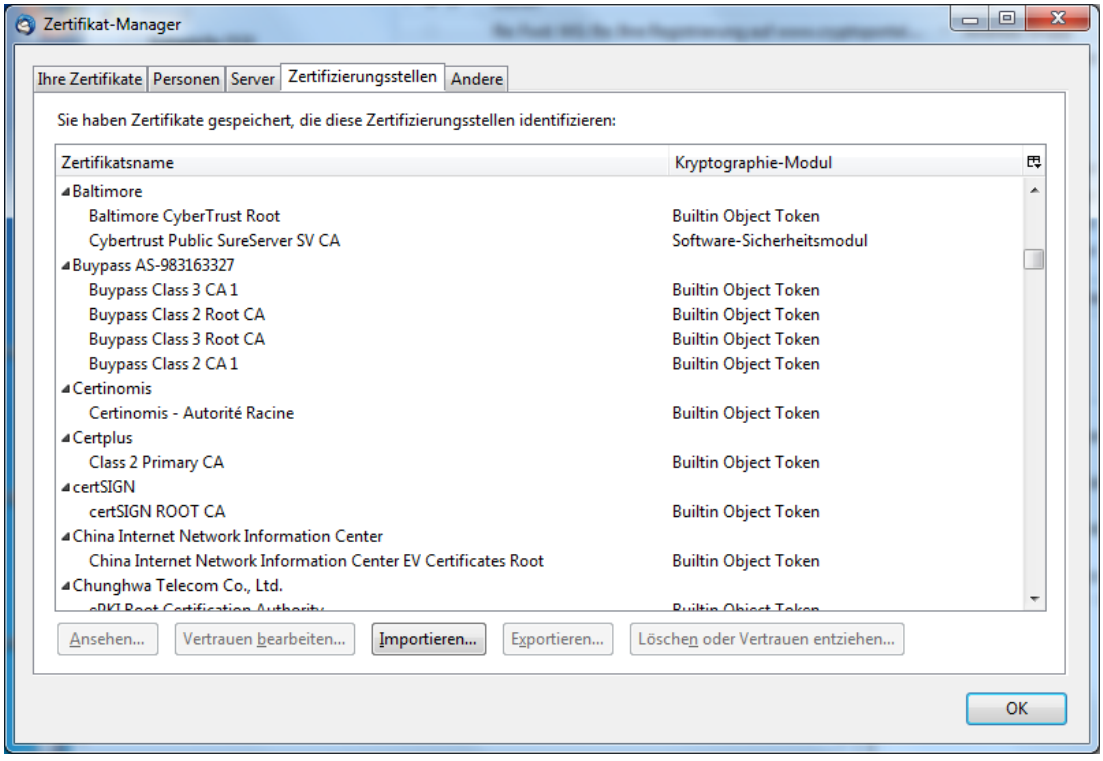
a) Versuch, das User-Zertifikat in TB im Zertifikatsmanager-Dialog im Tab "Personen" direkt zu akzeptieren (obwohl dessen Aussteller-Zertifikat unbekannt ist):



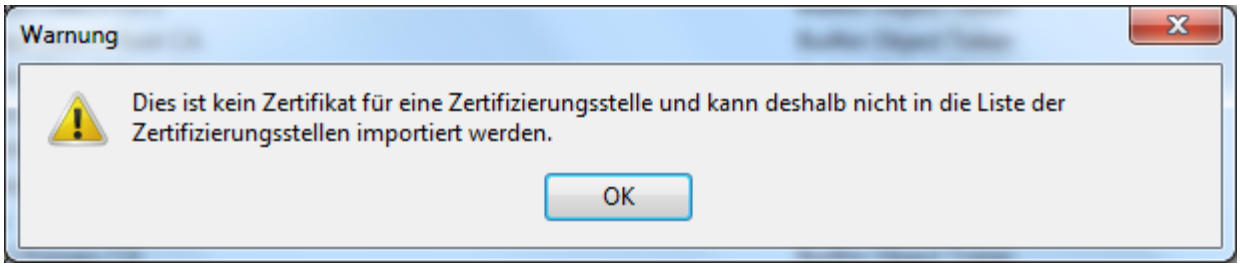
Nach Klick auf "Importieren" kommt die korrekte Fehler-Meldung



b) Versuch das User-Zertifikat zu benutzen, um dessen Aussteller-Zertifikat zu importieren:



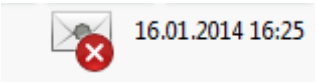
Nach erneutem Klick auf "Importieren" kommt die Fehler-Meldung:



Dies liegt daran, dass das Aussteller-Zertifikat nicht im Benutzer-Zertifikat enthalten ist.

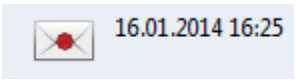
2. Beispiel-Szenario anhand des Trustcenters CAcert

Sie nutzen TB und haben eine signierte Email von einer anderen Person erhalten. Das Zertifikat der anderen Person ist von dem Trustcenter „CAcert“ ausgestellt worden. Da CAcert standardmäßig **nicht** im Mozilla-Keystore enthalten ist, kann Ihr Thunderbird die Signatur (erstmal) nicht validieren.

TB zeigt in der Mail das Symbol für eine ungültige Signatur: 

Damit TB das Root-Zertifikat von CAcert kennt und ihm damit vertraut, braucht man mehrere Schritte:

1) Das CAcert-Root-Zertifikat von der Webseite herunterladen.
2) Das CAcert-Root-Zertifikat mit dem TB-Trustmanager importieren und diesem für Email vertrauen.
3) Dann die Email schließen und erneut öffnen.

   Anschließend wird die Signatur korrekt angezeigt: 

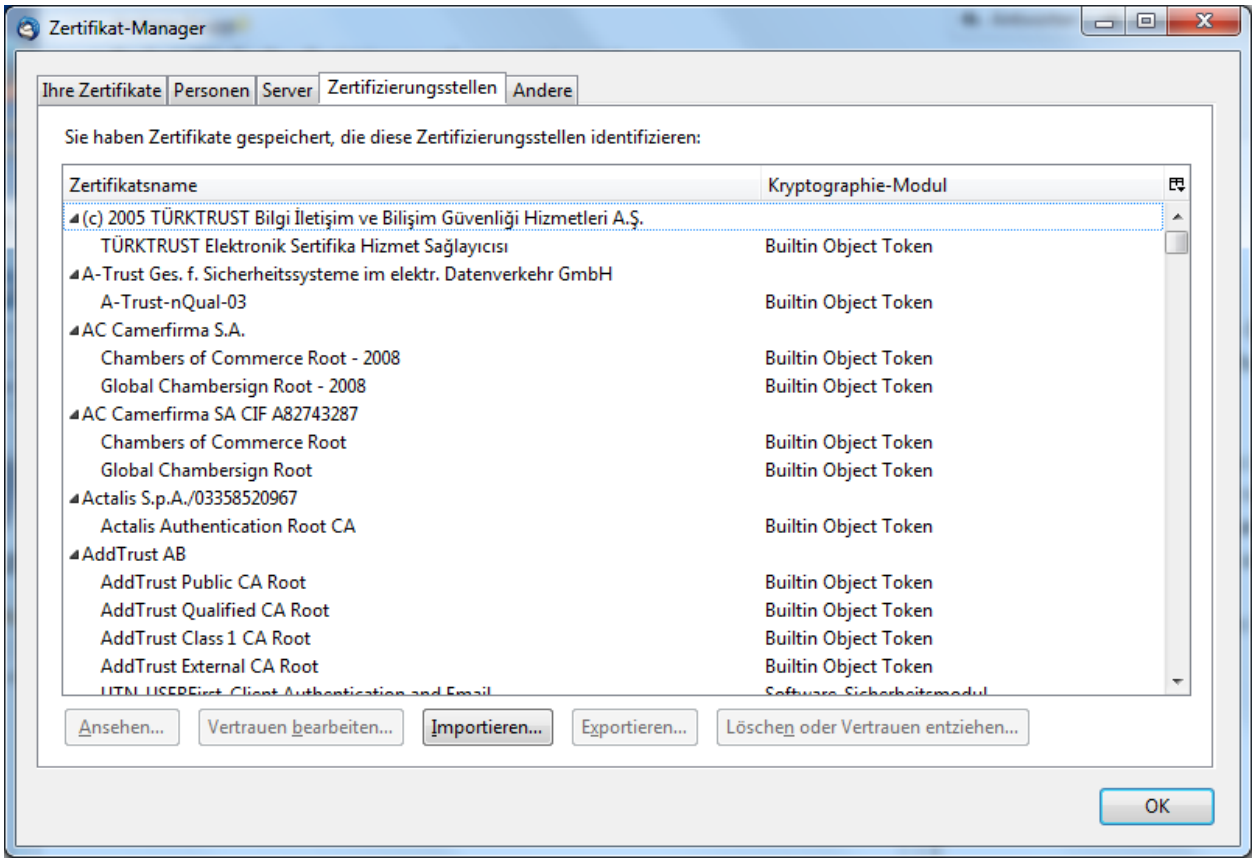
Es ist wichtig, diese Reihenfolge einzuhalten.

1) Das CAcert-Root-Zertifikat von der Webseite herunterladen

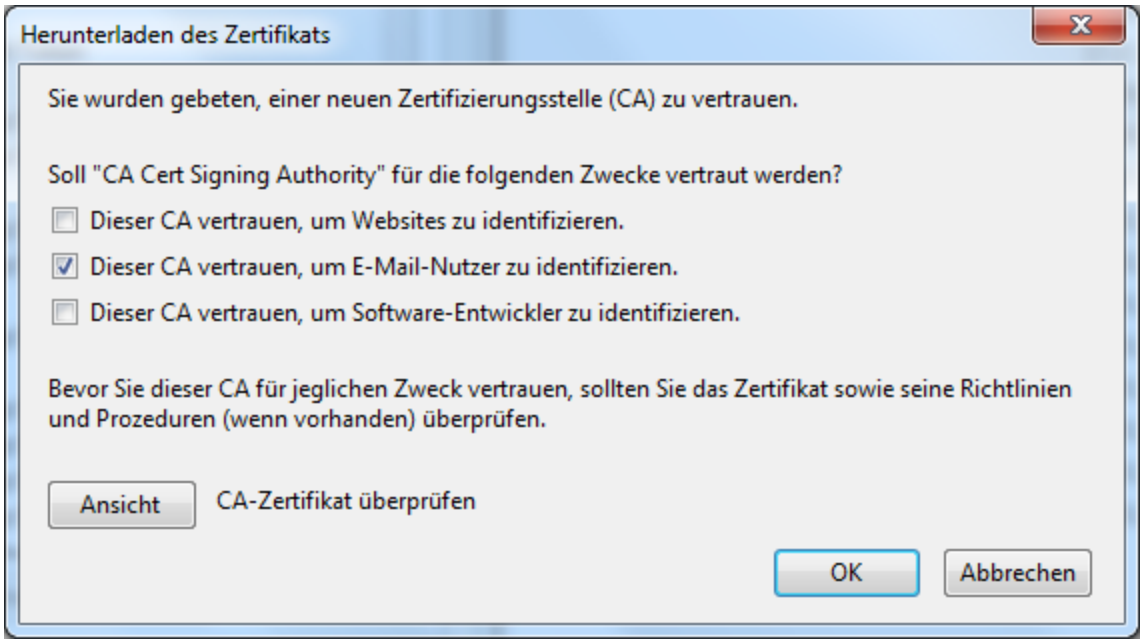
Von der entsprechenden Trustcenter-Webseite www.cacert.org erhält man dessen Root-Zertifikat in Form der Datei „root.der“.

2) Das CAcert-Root-Zertifikat mit dem TB-Trustmanager importieren und diesem für Email vertrauen.

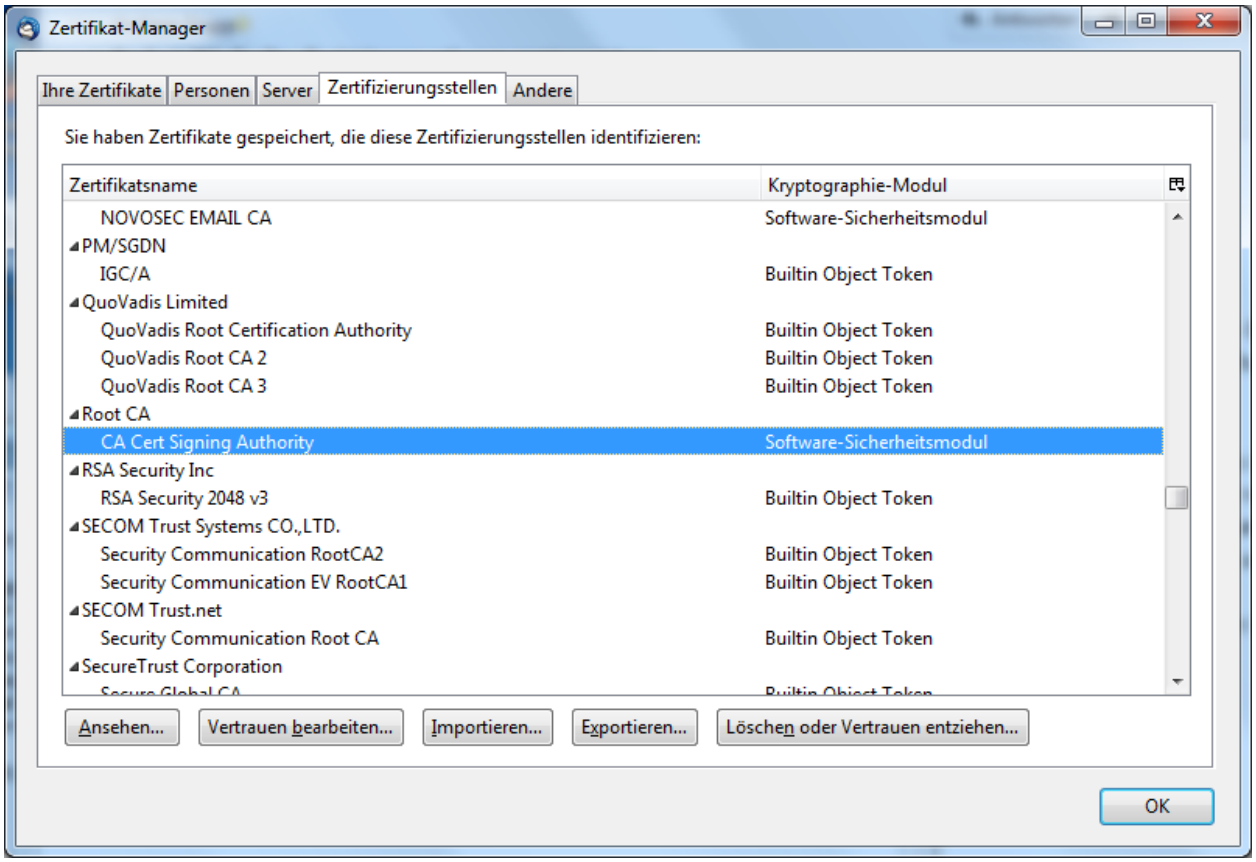
Aufruf des Tabs für Zertifizierungsstellen (CAs) im TB-Zertifikats-Manager:



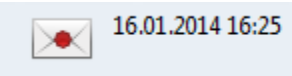
Klick auf „Importieren“ (mit Angabe des Verzeichnisses, wo die DER-Datei mit dem Root-Zertifikat liegt):



Bemerkung: Macht man hier gleich die Liste der Zertifizierungsstellen auf, muss man erst suchen – leider wird die Liste nicht von allein an der Stelle angezeigt, wo die neue hinzu gefügte CA eingefügt wurde:



3) Die erhaltene Email schließen und erneut öffnen.

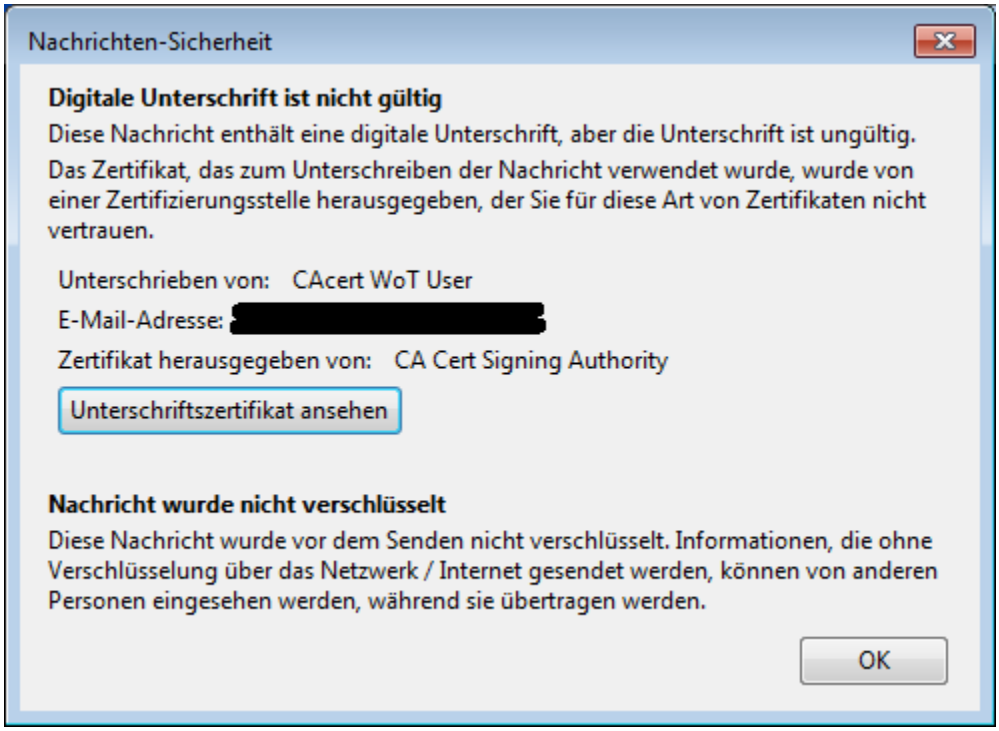
Anschließend wird die Signatur korrekt angezeigt: 

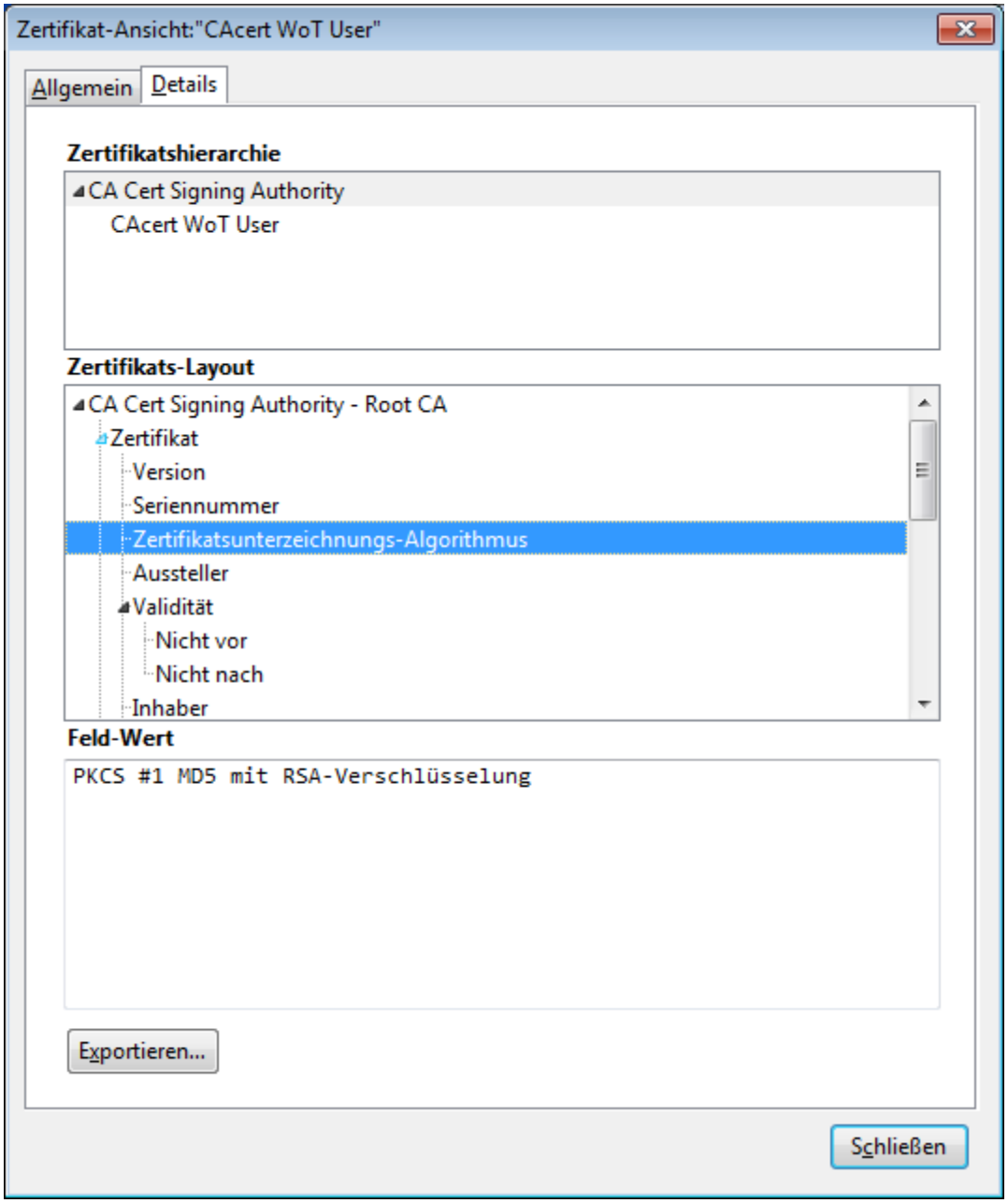
Dieses Procedere war nötig, weil das CA-Zertifikat (**im Gegensatz zu Szenario 1**) nicht in der Zertifikatskette des Benutzers enthalten war. Vergleiche auch http://wiki.cacert.org/ThunderBird.

Anmerkung zum bei CAcert verwendeten Hashverfahren:

Ab Version 24.6.0 (Juli 2014) wurde TB strenger bezüglich seiner Anforderungen an Hashverfahren (der Wechsel weg von SHA-1 wurde notwendig, da Zertifikate, die nach dem 31.12.2013 ausgestellt werden und SHA-1 nutzen, vom National Institute of Standards and Technology (NIST) als unsicher eingestuft werden). Siehe http://blog.cacert.org/tag/zertifikate/.

Mit der neuen TB-Version wurden von der alten CAcert-Root ausgestellte Zertifikate und die damit verbundenen Mail-Signaturen als ungültig erklärt. Inzwischen verwendet CAcert ein neues Root-Zertifikat mit einem neueren Hashverfahren zum Self-Signing, was das Problem behebt.




Zertifikat-Ansicht:"CAcert WoT User"
Allgemein
Details
Zertifikatshierarchie
CA Cert Signing Authority
CAcert WoT User
Zertifikats-Layout
CA Cert Signing Authority - Root CA
Zertifikat
Version
Seriennummer
Zertifikatsunterzeichnungs-Algorithmus
Aussteller
Validität
Nicht vor
Nicht nach
Inhaber
Feld-Wert
PKCS #1 MD5 mit RSA-Verschlüsselung
Exportieren...
Schließen

3. Beispiel-Szenario anhand des Trustcenters CERT-Bund

Dies ist in weiten Teilen dasselbe Szenario wie das des 2. Beispiel-Szenarios mit CAcert, da auch hier die Root-CA standardmäßig nicht im Mozilla-Keystore enthalten ist.

Das CERT ist ein Warn- und Informationsdienst der Bundesregierung zur Förderung von Cybersecurity. Alle per E-Mail versendeten Meldungen sind digital signiert.

Das dahinter stehende Trustcenter nutzt das „Wurzelzertifikat der Verwaltungs-PKI des Bundes“ (also die oberste Root-CA der bundesdeutschen Behörden).

Um die Authentizität einer signierten Email, die Sie vom CERT-Bund oder auch z.B. einem Mitarbeiter des BSI erhalten, zu überprüfen, muss Thunderbird die gesamte Zertifikatskette bekannt sein. Es ist also das Wurzelzertifikat der Verwaltungs-PKI in den Thunderbird-Keystore aufzunehmen.[4]

Um dem Root-Zertifikat der Verwaltungs-PKI das Vertrauen aussprechen, braucht man drei Schritte:

1) Das Root-Zertifikat von der Webseite herunterladen.

2) Das Root-Zertifikat in den Trustmanager importieren und für Email vertrauen.

3) Dann die Email schließen und erneut öffnen.
   Anschließend wird die Signatur korrekt angezeigt.

Es ist wichtig, diese Reihenfolge einzuhalten.

[4] Siehe auch die Meldung vom 14.3.2014 auf Heise, dass man die PKI der Verwaltung selbst in seinen Email-Client importieren muss, dass man das im Browser aber nicht kann und dass das BSI bewusst keine in den Browsern installierten CA-Zertifikate nutzt: http://www.heise.de/newsticker/meldung/Sicherheitswarnung-zur-Signatur-von-Buerger-CERT-Mails-2145053.html

1) Das Root-Zertifikat der Verwaltungs-PKI von der Webseite herunterladen

Das Root-Zertifikat erhält man von der Webseite https://www.cert-bund.de/wid-sig unter dem Eintrag „Digitale Signatur“ in Form der Datei „PCA-1-Verwaltung-11_zip.zip“ (diese enthält die Datei „PCA-1-Verwaltung-11.cer“).

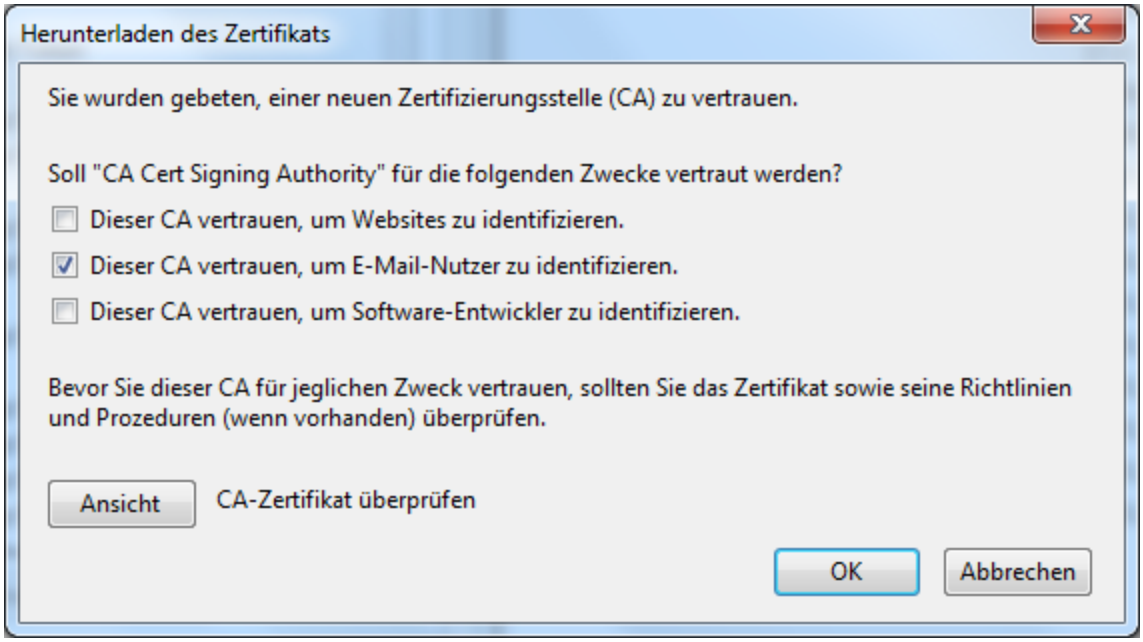
Es ist wichtig, die ZIP-Datei vor dem Import zu entpacken (dies ist der Hauptunterschied zu Scenario 2)! Es gibt gute Gründe, dass die Zertifikate auf der BSI-Webseite als Zip-Dateien bereitgestellt und damit ein zusätzlicher Schritt nötig wird [In FF funktioniert der Download (also Speichern als Datei) nur per Rechtsklick, Linksklick führt direkt zur Aufnahme in den Mozilla-Zertifikatsspeicher. Microsoft Browser warnen vor dem Download oder verhindern ihn. Firewalls sind oft so konfiguriert, dass Zertifikatsdateien blockiert werden].

Man kann die Zertifikate der Wurzel-CA und weiterer Bundesbehörden auch ungezippt (im CER-Format) bekommen vom X500-Verzeichnis Bund im Reiter "Service-Zertifikate" (oben): http://x500.bund.de/

2) Das Root-Zertifikat in den Trustmanger importieren und für Email vertrauen.

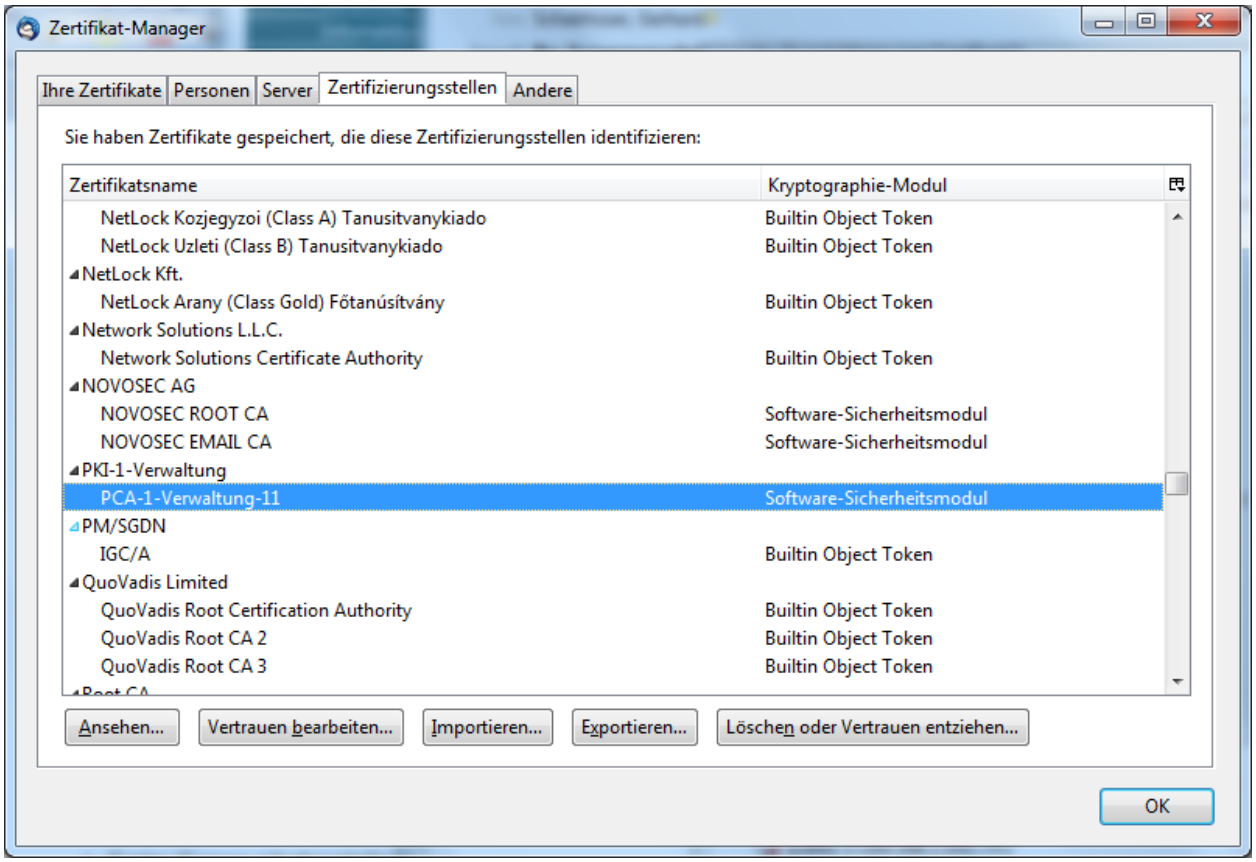
Vorgehen (nachdem man das Zertifikat aus dem ZIP-Archiv entpackte):

- Aufruf des Tabs für Zertifizierungsstellen (CAs) im TB-Zertifikats-Manager:
- Klick auf „Importieren“ (und Eingabe des Verzeichnisses, wo die CER-Datei liegt):



- Ok drücken.
  Das Fenster schließt sich ohne Rückmeldung, ob der Import erfolgreich war oder nicht.
  (Hinweis: Falls man die ZIP-Datei selbst statt der entpackten CER-Datei zum Import anbietet, gibt TB – genauso wie im Erfolgsfall -- keine Rückmeldung, obwohl nichts importiert wurde.)

Bemerkung: Macht man die Liste der Zertifizierungsstellen auf, muss man den neuen Eintrag („PKI-1 Verwaltung“) erst suchen – leider zeigt TB die Liste nicht von allein an der Stelle an, wo die zuletzt neue hinzu gefügte CA eingefügt wurde:



3) Die erhaltene Email schließen und erneut öffnen. Anschließend wird die Signatur korrekt angezeigt.

Dieses Procedere war nötig, weil das CA-Zertifikat (**im Gegensatz zu Szenario 1**) nicht in der Zertifikatskette des Senders enthalten war.

4. Beispiel-Szenario anhand des Verbundes vertrauenswürdiger PKIs der EBCA

Dies ist in weiten Teilen dasselbe Szenario wie das des 3. Beispiel-Szenarios mit dem CERT-Bund, da auch hier die Root-CAs standardmäßig nicht im Mozilla-Keystore enthalten sind.

Die European Bridge-CA (EBCA) ist ein Projekt des TeleTrusT-Vereins, in dem sich etliche große Firmen- und Behörden-PKIs zusammen fanden, die jeweils ein hohes Sicherheitsniveau haben, aber nicht in den Webbrowsern enthalten sind, und so schnell untereinander Vertrauen schaffen können.

„Die TeleTrusT European Bridge CA (EBCA) ist ein Zusammenschluss einzelner, gleichberechtigter Public-Key-Infrastrukturen (PKIen) zu einem PKI-Verbund. Sie ermöglicht eine sichere und authentische Kommunikation zwischen den beteiligten Unternehmen, Institutionen und öffentlichen Verwaltungen."

Partner und Teilnehmer sind z.B.

- Cassidian Cyber Security GmbH
- Deutsche Bank AG
- Deutsche Bundesbank
- E.ON Business Services GmbH
- Net at Work Netzwerksysteme GmbH
- SECARDEO GmbH
- Siemens AG
- PKI-1 der Bundes-Verwaltung
- Regulierungsgesellschaft Österreich (RTR)
- Unify GmbH & Co. KG

https://www.ebca.de/ebca/

https://www.ebca.de/nutzung-der-ebca/vertrauen-herstellen/

Anleitungen zur Installation der Zertifikate finden sich z.B. unter

https://www.ebca.de/nutzung-der-ebca/anwender/vertrauen-herstellen/anleitung-ctl-installation/

https://www.bundesdruckerei.de/de/2834-d-trust-softtoken-class-ii

https://www.bundesdruckerei.de/de/2875-installationsanleitungen

C) Was tun, wenn das eigene Zertifikat abläuft?

Trustcenter wie Comodo stellen Zertifikate aus, die 1 Jahr gültig sind. Ist ein Zertifikat abgelaufen, behandelt TB es so, als würde es nicht existieren. Obwohl es technisch ginge, bieten sie keine Zertifikatsverlängerung (d.h. ein neues Zertifikat, aber derselbe öffentliche Schlüssel), sondern verlangen die Neuausstellung eines Zertifikats, so dass man – wie in Schritt 2 – wieder in FF ein Schlüsselpaar generieren und ein Zertifikat beantragen muss.

Hinweis Gültigkeitsende beim eigenen Zertifikat:

Hat man das **neue** eigene Zertifikat per P12-Datei wieder in TB importiert, wird es von TB automatisch verwendet.

Leider gibt es keine Funktion, die automatisch alle Kommunikationspartner auflistet, denen man schon einmal eine signierte Mail sandte, so dass man sofort allen sein neues Zertifikat senden kann (Usability).

Wichtig ist auch, die alten Zertifikate und Schlüssel NICHT zu löschen.

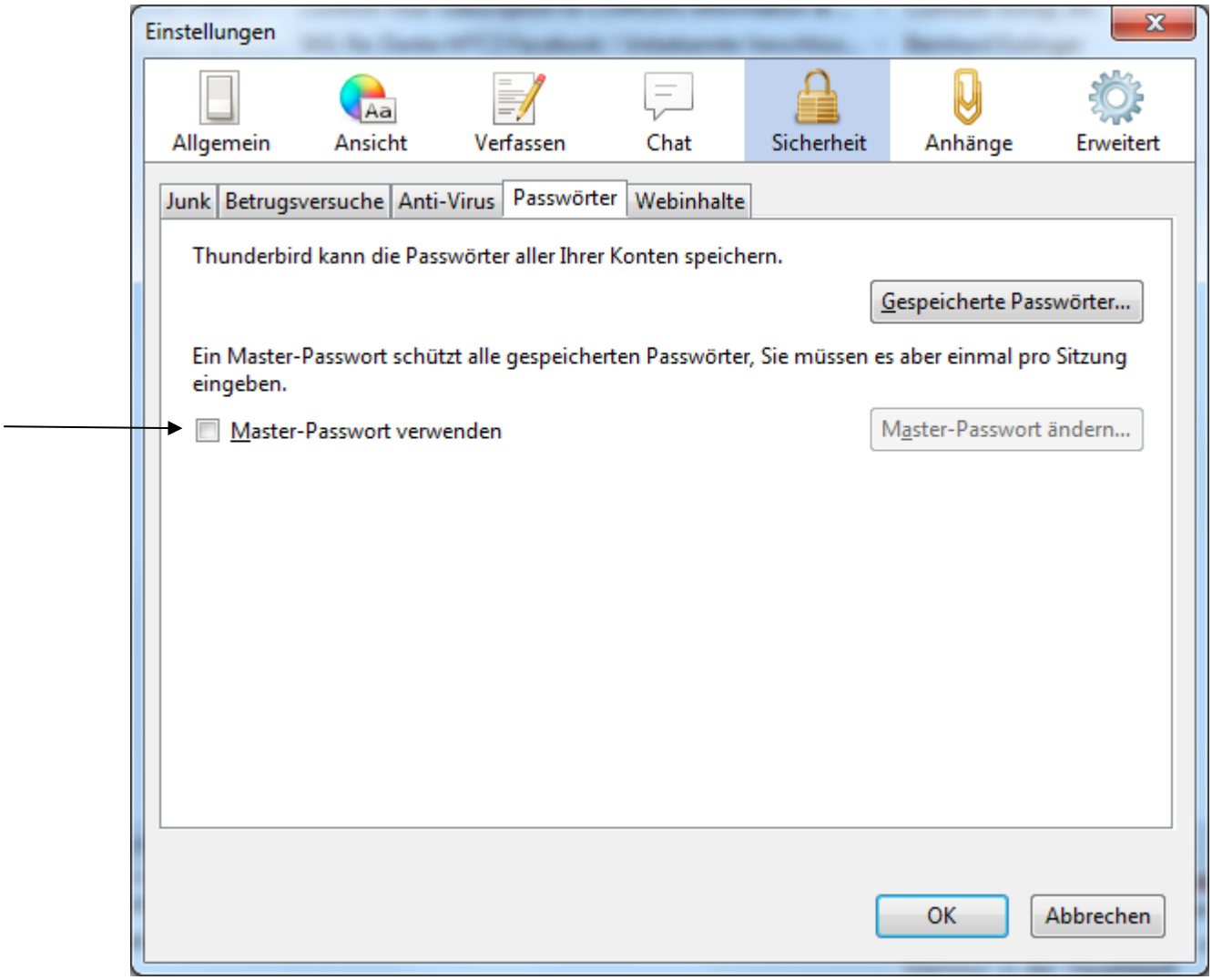
Hinweis Gültigkeitsende beim Zertifikat eines Kommunikationspartners:

Läuft das Zertifikat eines Kommunikationspartners aus, hat das zwei unschöne Folgen (solange Sie von ihm kein neues bekommen):

- TB erlaubt Ihnen nicht, das abgelaufene Zertifikat zum Verschlüsseln zu verwenden, sondern behauptet, er hätte keines oder es seien nicht alle vorhanden (Usability).
- Mails, deren Signatur gestern noch als gültig bewertet wurden, werden von TB nun als ungültig bezeichnet (ohne zu sagen, warum; denn zum Erstellungszeitpunkt und gestern war die Signatur noch in Ordnung; heute ist sie formal nur aufgrund des Ablaufdatums ungültig) (Usability!).

D) Verwendung eines Master-Passworts für den TB-Keystore

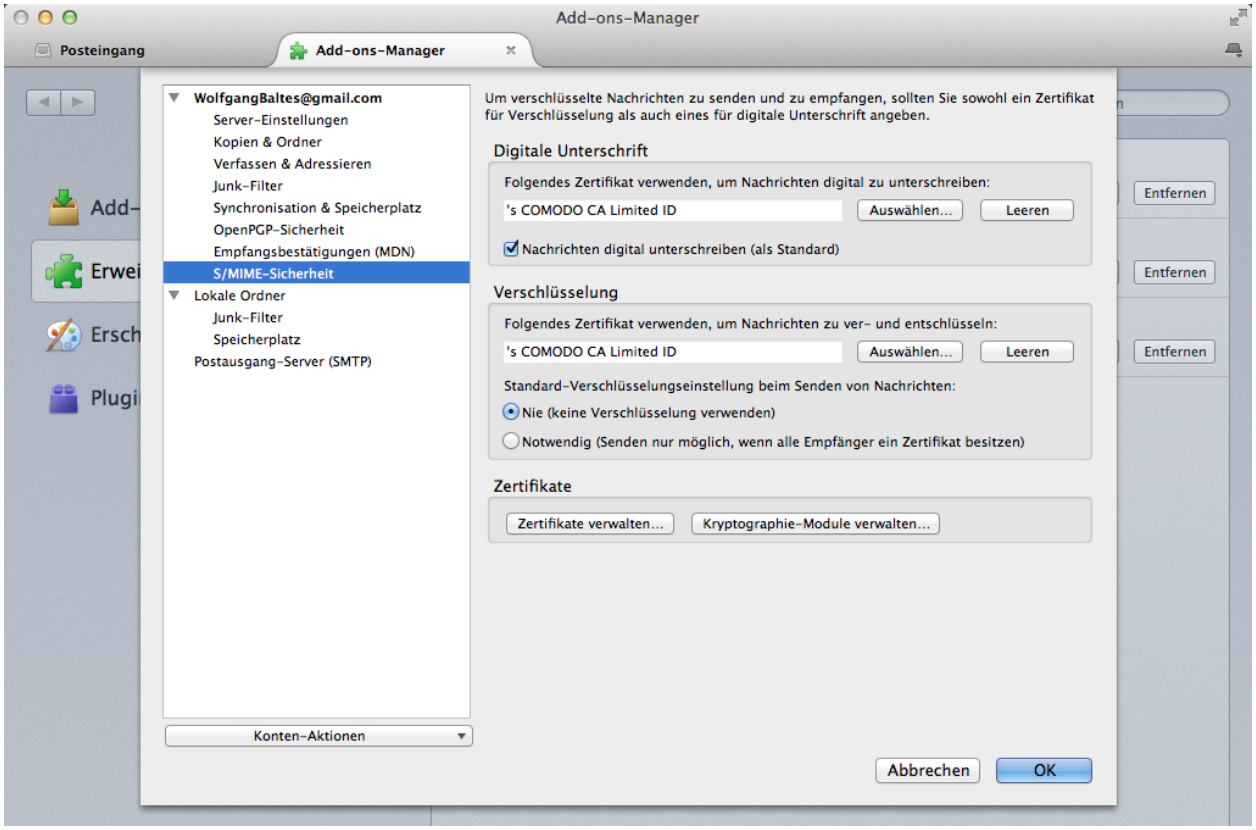
Wenn man nicht sicherstellen kann, dass niemand anderes evtl. Zugriff auf den Rechner mit TB bekommen kann (also eigentlich immer), sollte man für den Keystore ein Master-Passwort setzen, denn sonst kann jeder die eigenen privaten Keys exportieren.



Nachteil: Beim Neustart von Thunderbird ist das Masterpasswort jeweils neu einzugeben.

E) Screenshots von Thunderbird unter Mac

Die bisherigen Screenshots waren unter Windows gemacht. Da Thunderbird aber auf Mac, Linux und Windows gleichartig läuft, sehen auch die Screenshots auf dem Mac gleich aus. Hier zwei Beispiele:



F) Weitere Informationsquellen

http://www.thunderbird-mail.de/wiki/Mailverschl%C3%BCsselung_mit_S/MIME

http://kb.mozillazine.org/Message_security

- Hier steht, dass man ein Master-PW setzen soll:
  You are asked to set a master password to protect your own certificates stored in Thunderbird. If you do not set a master password, then someone who has access to your computer might be able steal and use your certificates.
  You might choose different security measures to protect your stored certificates instead of a master password—for example, if you work in an environment where you could be observed typing a master password. However, leaving your stored certificates unprotected is probably a bad idea. Das Master-PW muss man bei jedem Neustart von TB eingeben.
- Expired Zertifikate behalten! (um seine alten verschlüsselten Mails weiterhin lesen zu können).

http://www.instantssl.com/ssl-certificate-support/server_faq/ssl-email-certificate-faq.html

- Hier steht, dass man seine Zertifikate und seinen privaten Schlüssel sichern soll (Backup):
  How do I back up my email certificate?
  bei Verwendung von Internet Explorer, Firefox/IceDragon , Chrome / Dragon

http://www.uni-due.de/zim/services/e-mail/konfigurationsanleitungen/zertifikat-exportieren.shtml

http://www.comodo.com/support/products/email_certs/thunderbird.php?key5sk1=824de56d24cefccf1b3cfc3d558591f948ad255d&key5sk2=&key5sk3=1373645014000&key5sk4=&key5sk5=1373645077000&key6sk1=&key6sk2=FF220&key6sk3=7&key6sk4=de-de&key6sk5=DE&key6sk6=1&key6sk7=http%3A%2F%2Fwww.comodo.com%2Fsupport%2Fproducts%2Femail_certs%2Findex.php&key6sk8=117700&key6sk9=19201200&key6sk10=false&key6sk11=0a8cc25d908d03bbdc4a21b3cb00220c37e3689b&key6sk12=2034&key7sk1=57&key1sk1=dt&key1sk2=http%3A%2F%2Fwww.comodo.com%2Fsupport%2Fproducts%2Femail_certs%2Findex.php

- **Installing and Using your Secure Email Certificate with Thunderbird**

http://www.blafusel.de/files/quis_custodiet_custodes.pdf

- Sehr gute und umfangreiche Anleitung zu sicherer Email etc (Sept. 2014, V 5.0, 300 Seiten)
- „Quis custodiet custodes? (Wer bewacht die Wächter?) oder Eine einfache, praxisorientierte Anleitung, wie Sie Emails und Dateien mit PGP oder S/MIME schützen können und warum es sich lohnt, dies zu machen“.

https://bugzilla.mozilla.org/show_bug.cgi?id=1243449

- 40 seitiges Dokument in Bugzilla von Mozilla TB mit Verbesserungsvorschlägen (Usability Issues) zur Bedienung der Email-Verschlüsselung und zur Interoperabilität von S/MIME und PGP.

http://www.spiegel.de/video/daten-verschluesseln-einfach-erklaert-video-1656682.html

- Animation: Daten verschlüsseln einfach erklärt (19.03.2016)

http://www.spiegel.de/video/edward-snowden-goes-techno-video-1666161.html

- Videoclip mit Jean-Michel Jarre: Snowden wird Pop (15.04.2016)

http://www.spiegel.de/video/edward-snowden-film-citizenfour-portraet-von-whistleblower-video-1527801.html

- Snowden-Film "Citizenfour": Porträt eines Gejagten (11.10.2014)

http://zkm.de/event/2015/10/globale-global-control-and-censorship

- Ausstellung im ZKM in Karlsruhe: GLOBALE: GLOBAL CONTROL AND CENSORSHIP
  Weltweite Überwachung und Zensur, Beginn Sa, 03.10.2015, Ende So, 01.05.2016