

# S/MIME-CA basierend auf OpenSSL

Nutzungsanleitung – erstellt von Gunnar Haslinger, 17.07.2020

Die „S/MIME-CA“ basierend auf OpenSSL stellt ein Stammzertifikat sowie S/MIME taugliche Benutzerzertifikate für die Verwendung mit E-Mail-Clients (Outlook, Thunderbird, ...) bereit.

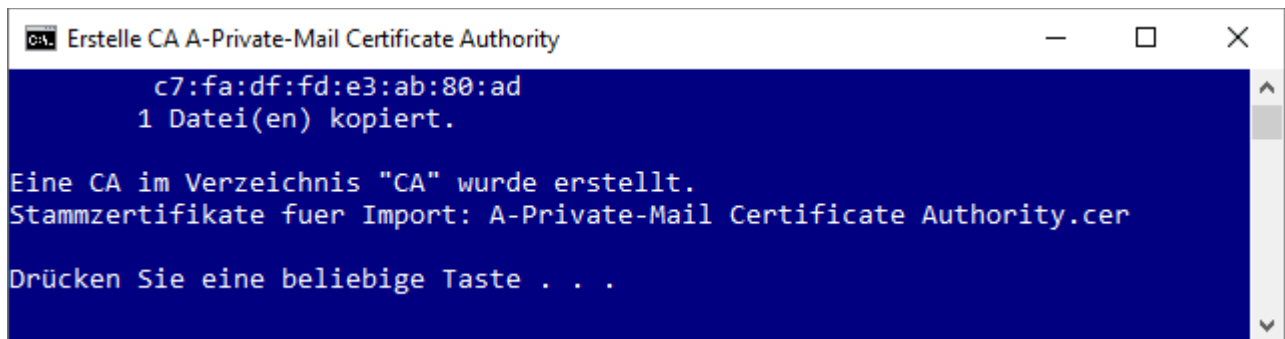
- Ordner „OpenSSL“ – enthält die Win64-Version von OpenSSL (portabel, muss nicht installiert werden)
- Die beiden BAT-Dateien sind in den nachfolgenden Kapiteln erläutert
- Datei „Stammzertifikat A-Private-Mail Certificate Authority.cer“ = das Demo-Stammzertifikat, wenn eine neue CA begonnen wird, kann dieses Zertifikat sowie der Ordner „CA“ gelöscht werden.
- Ordner „CA“ – enthält die Certificate Authority, um eine neue CA zu beginnen diesen Ordner löschen!

## 1 Neue CA erstellen (einmaliger Vorgang)

Nachdem die Demo-CA (der Ordner „CA“ und das Stammzertifikat) gelöscht wurden, kann eine neue CA generiert werden, hierzu:

Batch-Datei „**create\_CA.bat**“ starten

Anmerkung: Eine Anpassung der Attribute ist im BAT-File möglich, wird aber nicht uneingeschränkt empfohlen (siehe technische Informationen anbei).



```
Erstelle CA A-Private-Mail Certificate Authority

c7:fa:df:fd:e3:ab:80:ad
1 Datei(en) kopiert.

Eine CA im Verzeichnis "CA" wurde erstellt.
Stammzertifikate fuer Import: A-Private-Mail Certificate Authority.cer

Drücken Sie eine beliebige Taste . . .
```

Hinweise zum Inhalt des Ordners „CA“ sind im Kapitel „Technische Informationen zur CA“ zu finden.

## 2 Neues S-MIME Zertifikat für Anwender erstellen

Batch-Datei „**create\_SMIME-Certificate-for-User.bat**“ modifizieren, die nachfolgenden zwei Variablen sind in der Regel für jeden Benutzer anzupassen. Alle anderen Felder benötigen normalerweise keine Modifikation.

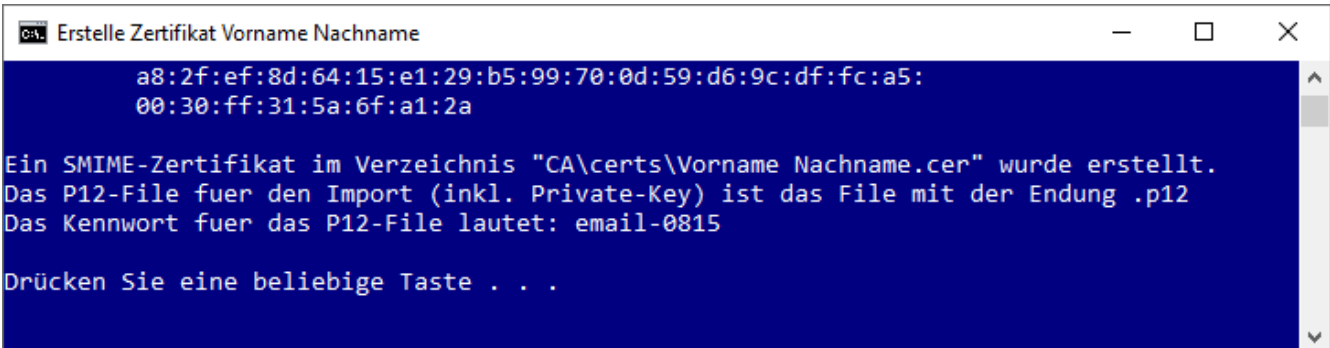
Beachte: Keine Sonderzeichen, keine Umlaute etc... (sonst hohe Chance für Fehlschlag / Inkompatibilität)

```
rem # USER = der Zertifikats-Common-Name, also z.B. Vorname Nachname
set USER=Vorname Nachname

rem # die E-Mail-Adresse fuer die dieses SMIME-Zertifikat gelten soll
set EMAIL=vorname.nachname@domain.demo

rem # Das Kennwort fuer das P12-File, keine Sonderzeichen verwenden!
set PASSWORD=email-0815
```

Batch-Datei „**create\_SMIME-Certificate-for-User.bat**“ starten



```
0x% Erstelle Zertifikat Vorname Nachname

a8:2f:ef:8d:64:15:e1:29:b5:99:70:0d:59:d6:9c:df:fc:a5:
00:30:ff:31:5a:6f:a1:2a

Ein SMIME-Zertifikat im Verzeichnis "CA\certs\Vorname Nachname.cer" wurde erstellt.
Das P12-File fuer den Import (inkl. Private-Key) ist das File mit der Endung .p12
Das Kennwort fuer das P12-File lautet: email-0815

Drücken Sie eine beliebige Taste . . .
```

Hinweis: Das Script „**create\_SMIME-Certificate-for-User.bat**“ konfiguriert die Umgebungsvariablen für USER, EMAIL und PASSWORD und startet anschließend „**create\_SMIME-Certificate.bat**“. Für eine Generierung mehrerer Zertifikate kann das „**create\_SMIME-Certificate-for-User.bat**“ somit einfach angepasst werden.

## 3 Technische Informationen zur CA

Die CA ist 20 Jahre lang gültig.

Die Zertifikate sind 15 Jahre lang gültig, man kann daher zumindest die nächsten 5 Jahre lang Zertifikate mit 15 Jahren Laufzeit ausstellen. Danach muss man die Laufzeit der SMIME-Zertifikate verkürzen, damit diese nicht über das Ende der CA-Gültigkeitsdauer hinausragen.

Die Gültigkeitsdauer der CA ist im Script „**create\_CA.bat**“ hinterlegt, siehe Argument „**-days**“.

Die Gültigkeitsdauer der SMIME-Zertifikate ist im Script „**create\_SMIME-Certificate.bat**“ hinterlegt.

Die Konfiguration der Zertifikate ist – soweit dies nicht in den BAT-Dateien parametrisiert wird – in der „**CA-openssl.cfg**“ vorbereitet hinterlegt, hier ist im Normalfall kein Anpassungsbedarf gegeben. Alle anpassbaren Werte sind im Header der BAT-Dateien dokumentiert hinterlegt.

Der Name „A-Private-Mail Certificate Authority“ der Firma „A-Private-Mail“ ist bewusst so gewählt, damit scheint die CA nämlich in den Ansichten von Thunderbird und Microsoft weit oben auf und man findet sie leicht zum Kontrollieren.

Die CA selbst hat ihren Private-Key unter „CA\private\ca-key.pem“ und dieser ist NICHT mittels Kennwort geschützt. Der Inhalt des Ordners ist daher gesichert aufzubewahren.

Die User-Zertifikate werden als CER-Files ausgegeben – wobei die CER-Files in der Regel nicht benötigt werden. Die Anwender benötigen tatsächlich das P12-File (PKCS#12, teils auch als PFX-File bezeichnet), dieses stellt einen importierbaren Zertifikatscontainer bestehend aus Zertifikat + Private Key inklusive dem CA-Zertifikat (also der Chain) dar. Das PKCS#12-Containerfile wird mit einem Kennwort geschützt, welches im Script „**create\_SMIME-Certificate.bat**“ oben in der Konfiguration vorkonfiguriert wird. Auch hier empfiehlt es sich auf Umlaute und Sonderzeichen zu verzichten.

Erkannte Stolpersteine im Zusammenhang mit Thunderbird:

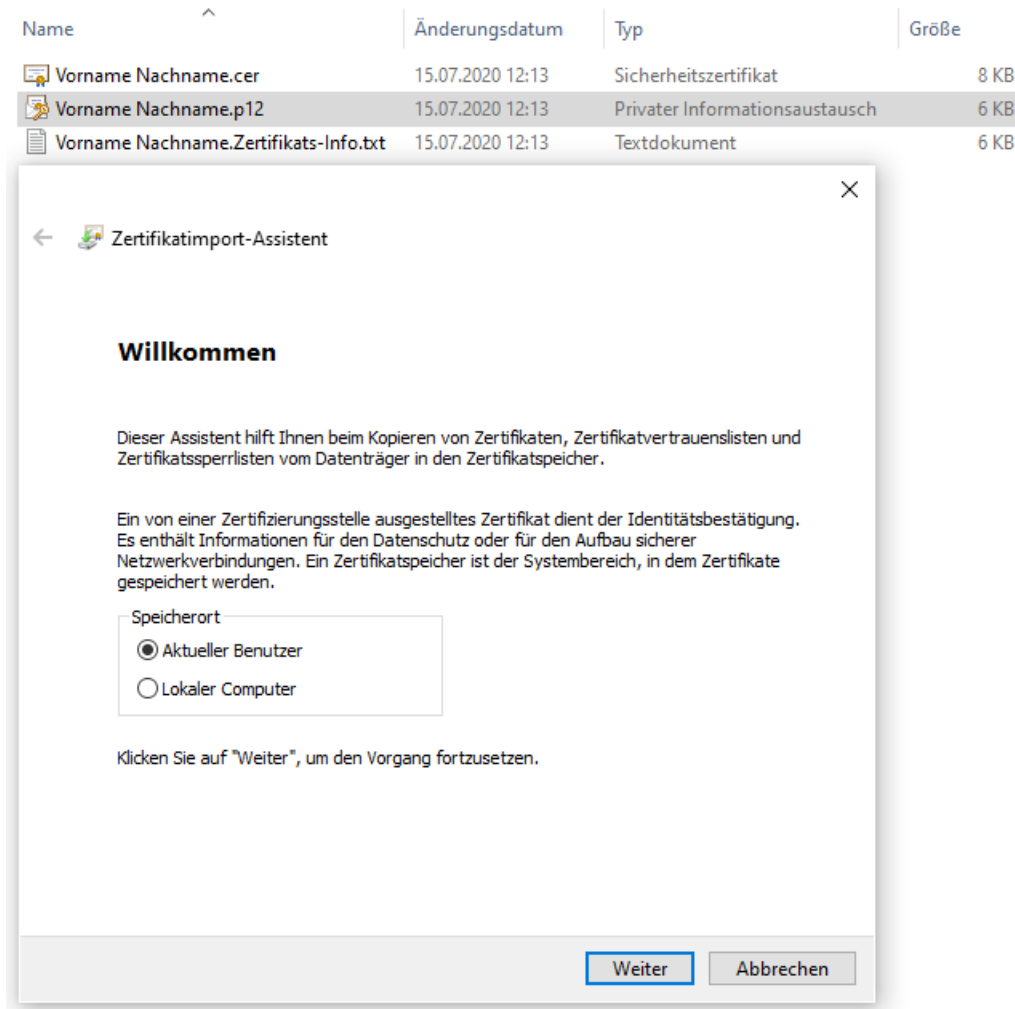
- Die Seriennummer des Stammzertifikates (CA-Zertifikats) muss für den Thunderbird offenbar unique sein, der Versuch das Stammzertifikat immer mit fixer Seriennummer „-set\_serial 0x01“ zu erzeugen führt zum kuriosen Effekt, dass der allererste Import eines solchen CA-Zertifikats klappt aber das Importieren weiterer SMIME-Zertifikate aus einer anderen CA mit gleicher Seriennummer dann aber mit einer generischen Fehlermeldung „*Die PKCS#12-Operation ist aus unbekannten Gründen fehlgeschlagen*“ blockiert wird. Abhilfe war hier, das CA-Zertifikat (Stammzertifikat) mit einer Random-Seriennummer zu generieren.
- Das Kennwort des PKCS#12 (.p12) Containers darf für Thunderbird nicht leer sein, daher jedenfalls ein Kennwort verwenden, selbst wenn keines benötigt wird.
- Auch wenn das Stammzertifikat bereits beim Import der p12-Datei mitimportiert wird, muss dieses dennoch für den Zweck des Mailings noch getrustet werden, siehe Kapitel „Vertrauenseinstellungen für das Stammzertifikat festlegen“

Die Subfolder im Ordner „CA“:

- „certs“ – hier landen die erstellten Zertifikate als .cer-Datei (PEM/Base64-kodiert, ohne Private-Key) sowie als p12-Datei (PKCS#12 / PFX Format mit Private-Key). Zusätzlich wird stets noch eine „Zertifikats-Info.txt“ mitgeneriert, die Infos zum Zertifikat und dem Kennwort das für den Import der p12-Datei benötigt wird enthält.
- Unterordner „crl“ bleibt leer, es werden keine Revocation-Lists geführt bzw. erstellt
- Unterordner „newcerts“ – hier legt die CA die erstellten Zertifikate nach Seriennummer sortiert chronologisch zur Dokumentation ab. Wird im täglichen Gebrauch nicht benötigt.
- „private/ca-key.pem“ – der Private-Key der CA, zu schützen!
- „ca-cert.cer“ ist das Stammzertifikat selbst (Public-Teil)
- index.txt protokolliert alle ausgestellten Zertifikate mit
- serial zählt die nächste freie Seriennummer für das nächste auszustellende Zertifikat mit
- index.txt.attr sowie die .old Dateien benötigen OpenSSL für seine Abläufe

## 4 Import des S/MIME-Zertifikats unter Windows (z.B. für Outlook)

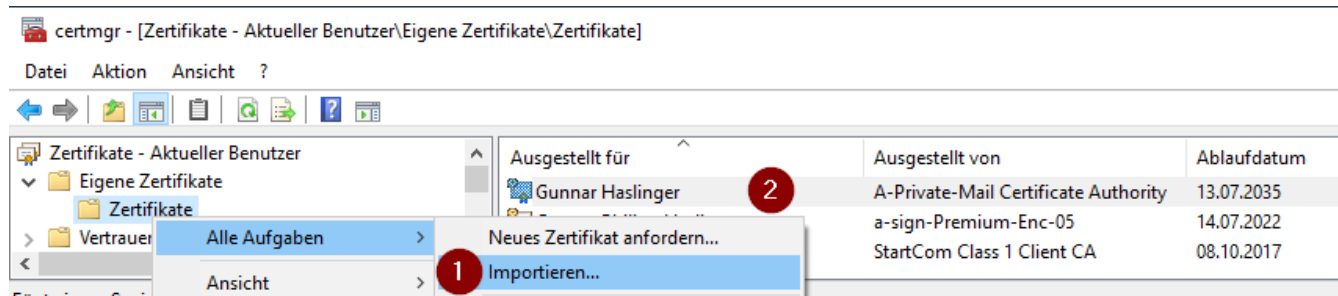
**Variante 1, direkt aus dem Explorer:** die p12-Datei doppelklicken und dem Wizzard folgen:



**Variante 2, über den Zertifikatsmanager:** Windowstaste + R => **certmgr.msc** starten

Eigene Zertifikate => Zertifikate => Rechtsklick => Alle Aufgaben => Importieren

Mit [1] (siehe Screenshot) die p12-Datei des eigenen SMIME-Zertifikats importieren. Danach F5 drücken, das Zertifikat muss nun (siehe [2], als Beispiel wurde Gunnar Haslinger importiert) aufscheinen.



Empfohlen wird beim Import folgendes (Default-Konfiguration) beizubehalten.

Das Kennwort zum Import der p12-Datei ist in der zugehörigen „... Zertifikats-Info.txt“ Datei zu finden.

**Schutz für den privaten Schlüssel**

Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

---

Geben Sie das Kennwort für den privaten Schlüssel ein.

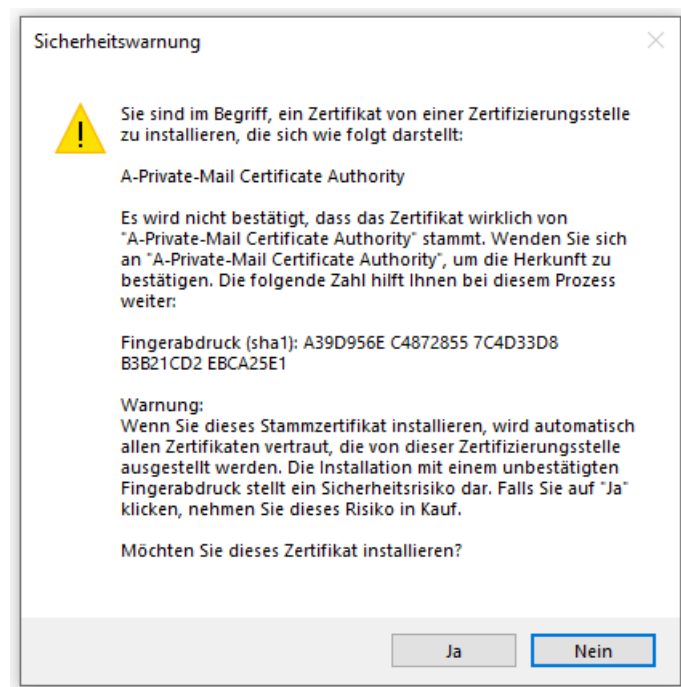
Kennwort:

☐ Kennwort anzeigen

Importoptionen:

- ☐ Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.
- ☐ Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.
- ☐ Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar)
- ☒ Alle erweiterten Eigenschaften mit einbeziehen

Da beim ersten Import eines Zertifikates aus der CA auch das Stammzertifikat mitimportiert wird, ist hierzu folgende Sicherheits-Warnung zu bestätigen:



## 5 Stammzertifikats-Import unter Windows (z.B. für Outlook)

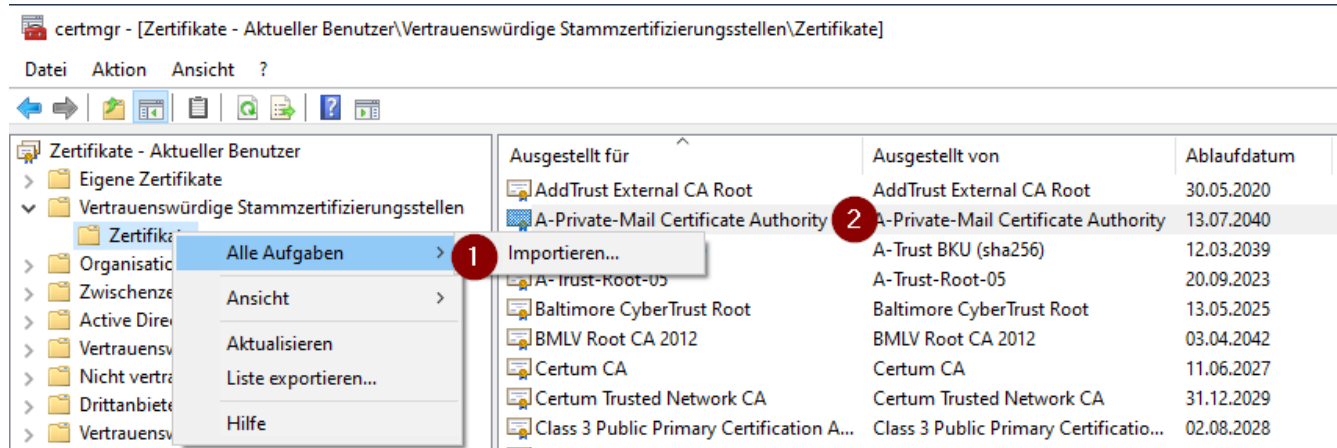
Hinweis: Dieser Vorgang ist nicht erforderlich, wenn ein p12-File importiert wird, das p12-File das aus dieser CA generiert wird enthält das Stammzertifikat bereits, dieser Abschnitt kann daher (wenn ohnehin das p12-File importiert wurde) übersprungen werden.

Windowstaste + R => **certmgr.msc** starten

Vertrauenswürdige Stammzertifizierungsstellen => Zertifikate => Rechtsklick => Alle Aufgaben => Importieren

Mit [1] (siehe Screenshot) die Datei des Stammzertifikats importieren.

Danach F5 drücken, diese muss nun in der Liste (siehe [2]) aufscheinen.



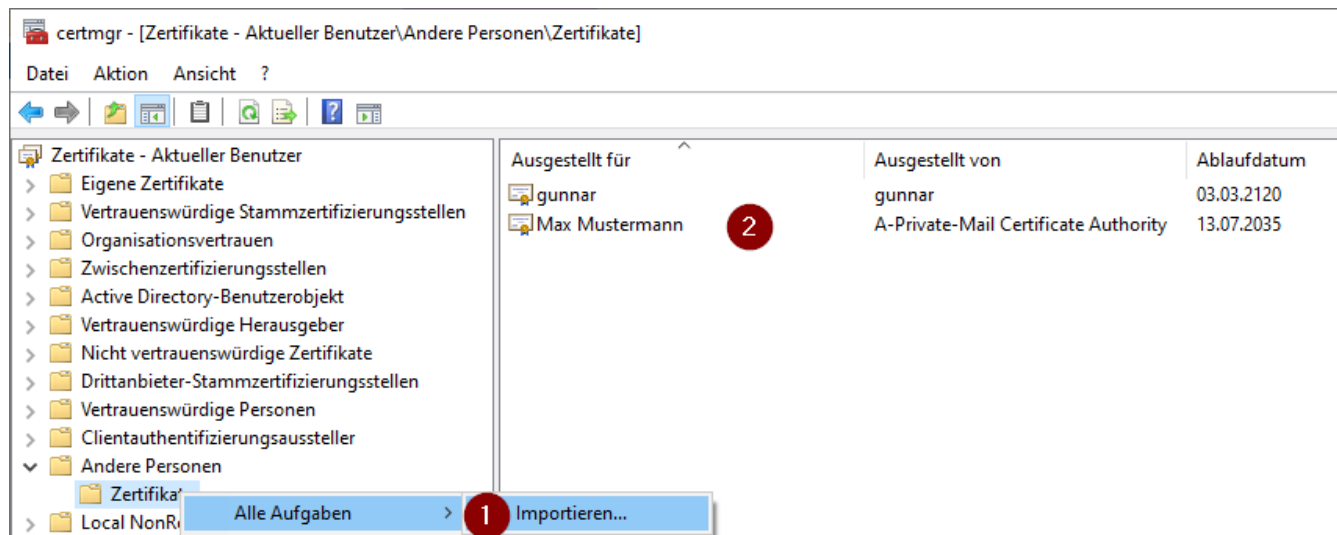
## 6 Import „fremder“ SMIME-Zertifikate ohne PrivateKey unter Windows

Zu importieren ist für gewöhnlich nur das eigene SMIME-Zertifikat in Form der p12-Datei (also inkl. Private-Key). Die „anderen“ SMIME-Zertifikate fremder Personen müssen nicht importiert werden, da man diese trusted kann sobald man die erste signierte E-Mail von diesen erhält. Will man diesen aber verschlüsselte E-Mails senden, noch bevor man von diesen eine signierte E-Mail erhalten hat, so können auch diese importiert werden.

Windowstaste + R => **certmgr.msc** starten

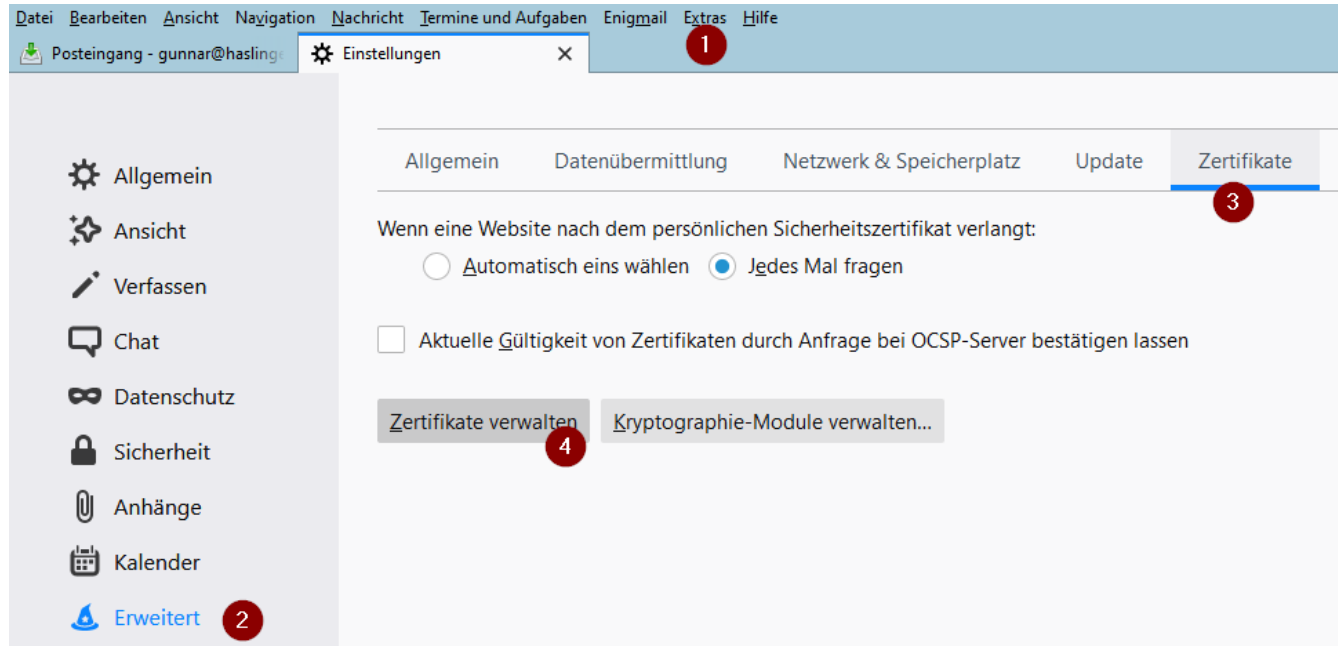
Andere Personen => Zertifikate => Rechtsklick => Alle Aufgaben => Importieren

Mit [1] (siehe Screenshot) die cer-Datei des fremden SMIME-Zertifikats importieren. Danach F5 drücken, das Zertifikat muss nun (siehe [2], als Beispiel wurde Max Mustermann importiert) aufscheinen.

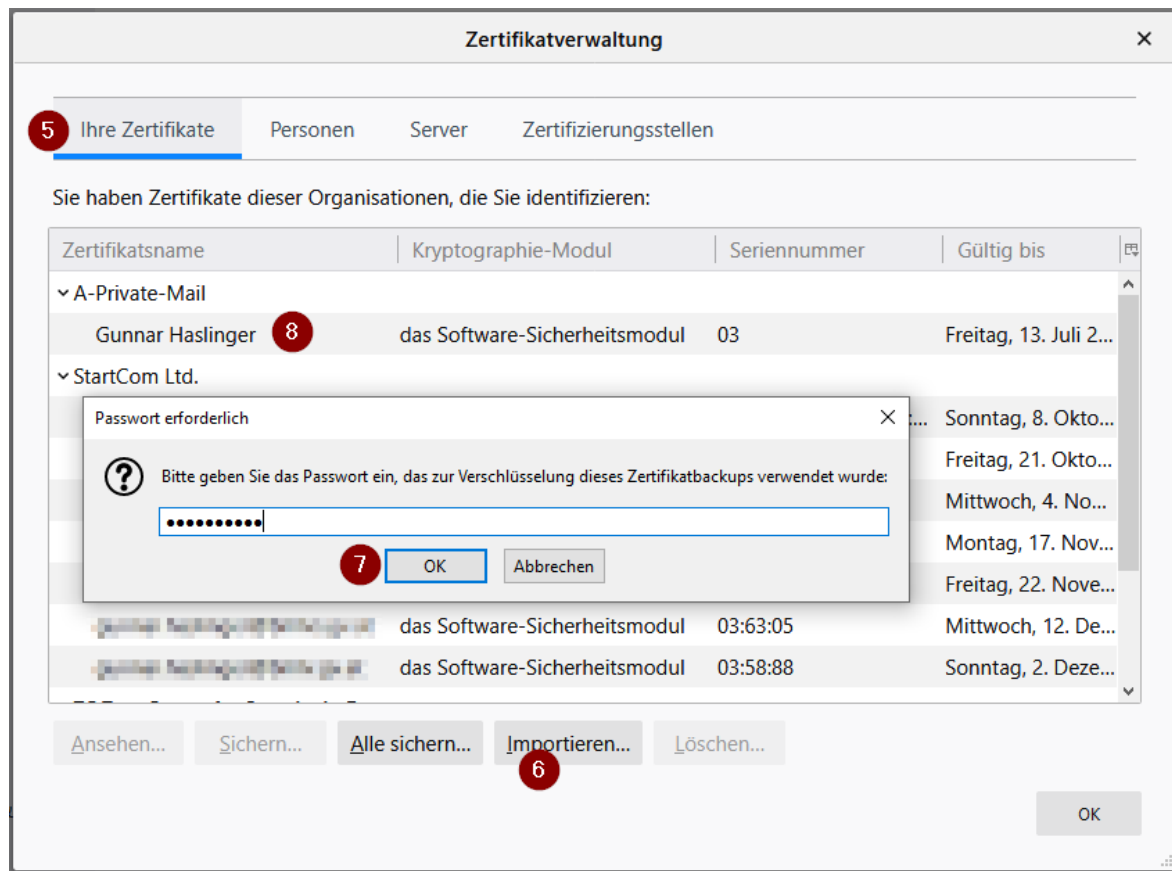


## 7 Import des S/MIME-Zertifikats unter Thunderbird

Thunderbird Menü „Extras“ [1] => „Einstellungen“ => Erweitert [2] => Zertifikate [3] => Zertifikate verwalten [4]



Nun unter „Ihre Zertifikate“ [5] auf „Importieren ...“ [6] und die P12-Datei auswählen. Das für den Import benötigte Kennwort der P12-Datei eingeben [7]. Danach scheint das Zertifikat auf (siehe [8] im Screenshot, als Beispiel wurde „Gunnar Haslinger“ importiert)

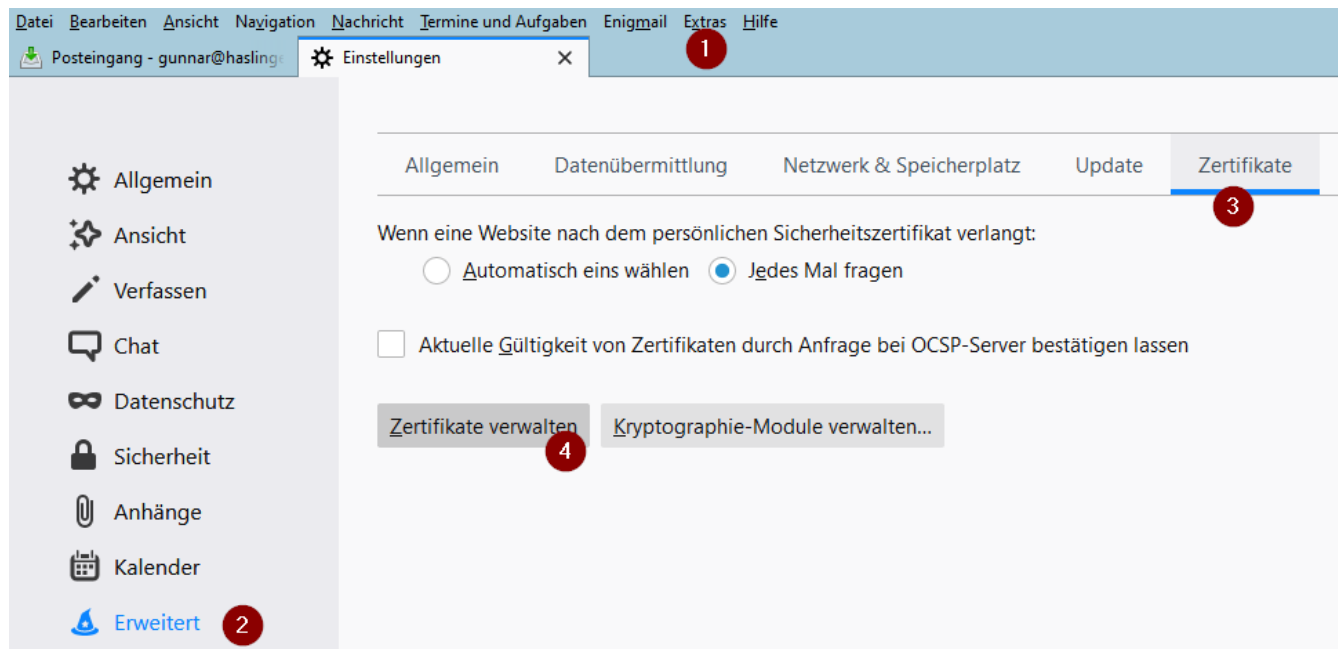




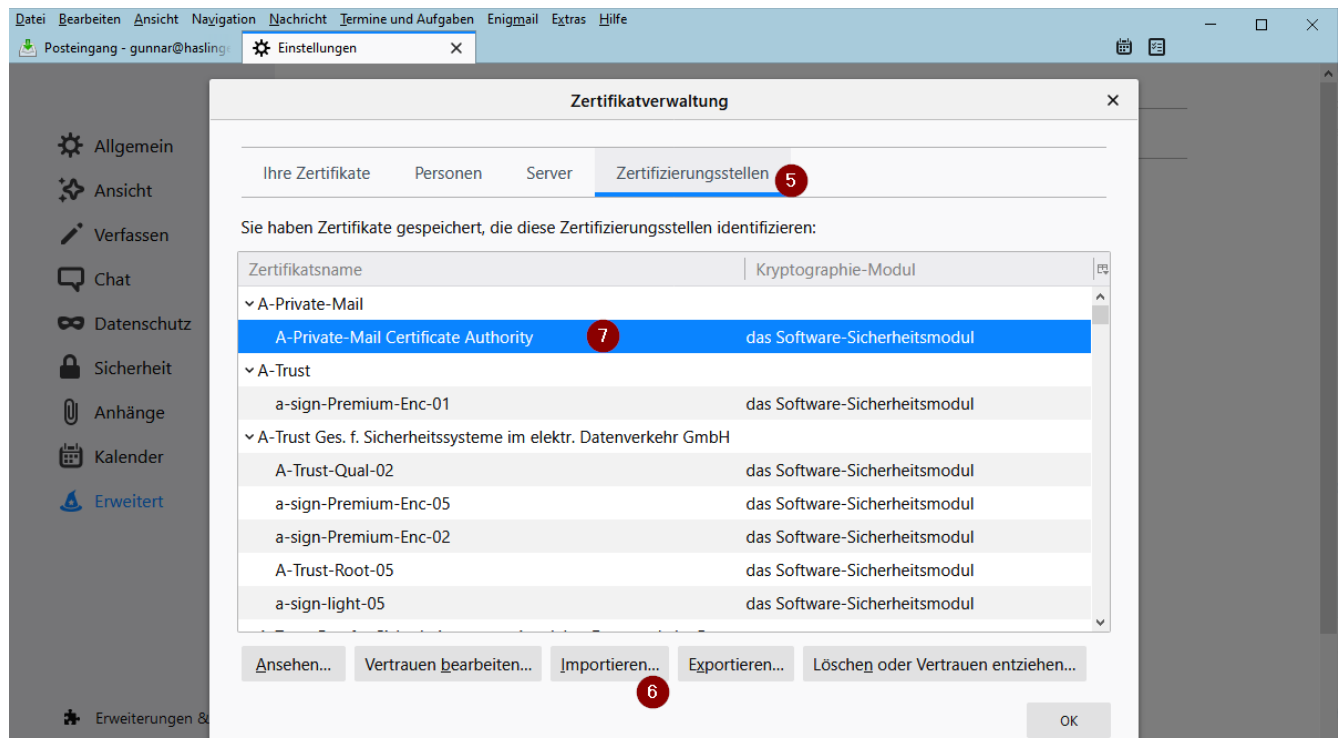
## 8 Stammzertifikats-Import unter Thunderbird

Hinweis: Dieser Vorgang ist nicht erforderlich, wenn ein p12-File importiert wird, das p12-File das aus dieser CA generiert wird enthält das Stammzertifikat bereits, dieser Abschnitt kann daher (wenn ohnehin das p12-File importiert wurde) übersprungen werden.

Thunderbird Menü „Extras“ [1] => „Einstellungen“ => Erweitert [2] => Zertifikate [3] => Zertifikate verwalten [4]



Auf „Zertifizierungsstellen“ [5] => Button „Importieren ...“ [6] die Stammzertifikatsdatei importieren, sodass diese anschließend in der Liste (siehe [7] im Screenshot) aufscheint.



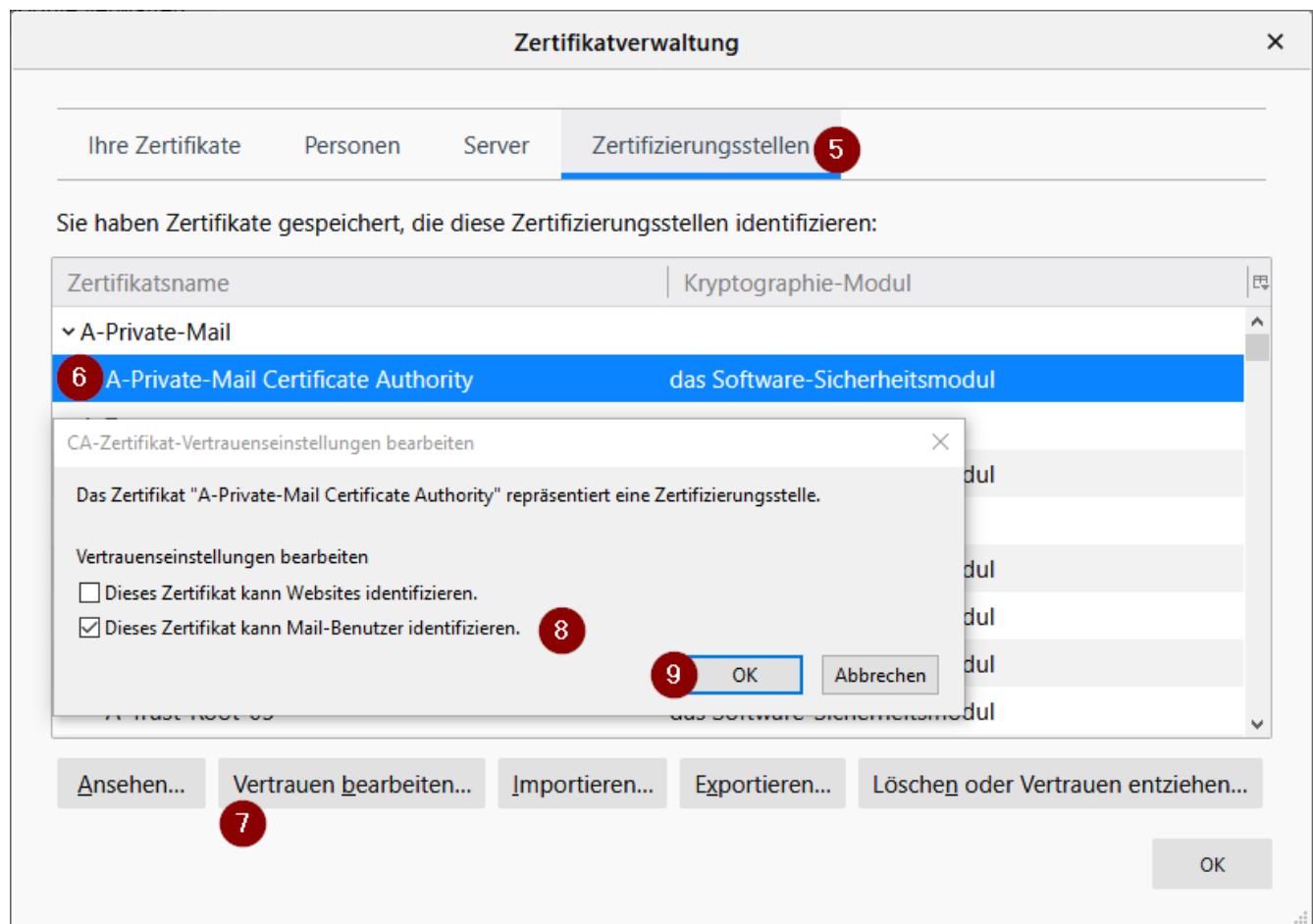
## 9 Vertrauenseinstellungen für das Stammzertifikat festlegen

Auch wenn der vorangegangene Punkt „Stammzertifikats-Import unter Thunderbird“ übersprungen werden konnte, weil das Stammzertifikat automatisch mittels p12-Datei mit-importiert wurde, so muss dennoch die Vertrauensstellung des Zertifikats aus dieser CA Mail-Benutzer identifizieren dürfen manuell getätigt werden:

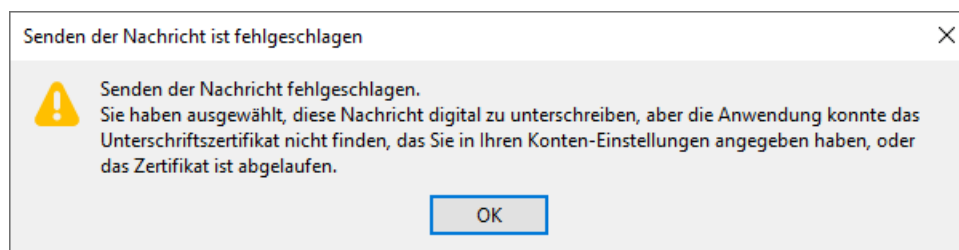
Wie im vorangegangenen Kapitel beschrieben unter:

Thunderbird Menü „Extras“ [1] => „Einstellungen“ => Erweitert [2] => Zertifikate [3] => Zertifikate verwalten [4]

Auf „Zertifizierungsstellen“ [5] => Die „A-Private-Mail Certificate Authority“ auswählen [6] und mittels „Vertrauen bearbeiten“ [7] den Haken bei „Dieses Zertifikat kann Mail-Benutzer identifizieren.“ [8] setzen. Mit OK [9] bestätigen:



Hinweis: Wird dieser Schritt vergessen, kommt es zu folgender Fehlermeldung beim Senden von signierten Mails:

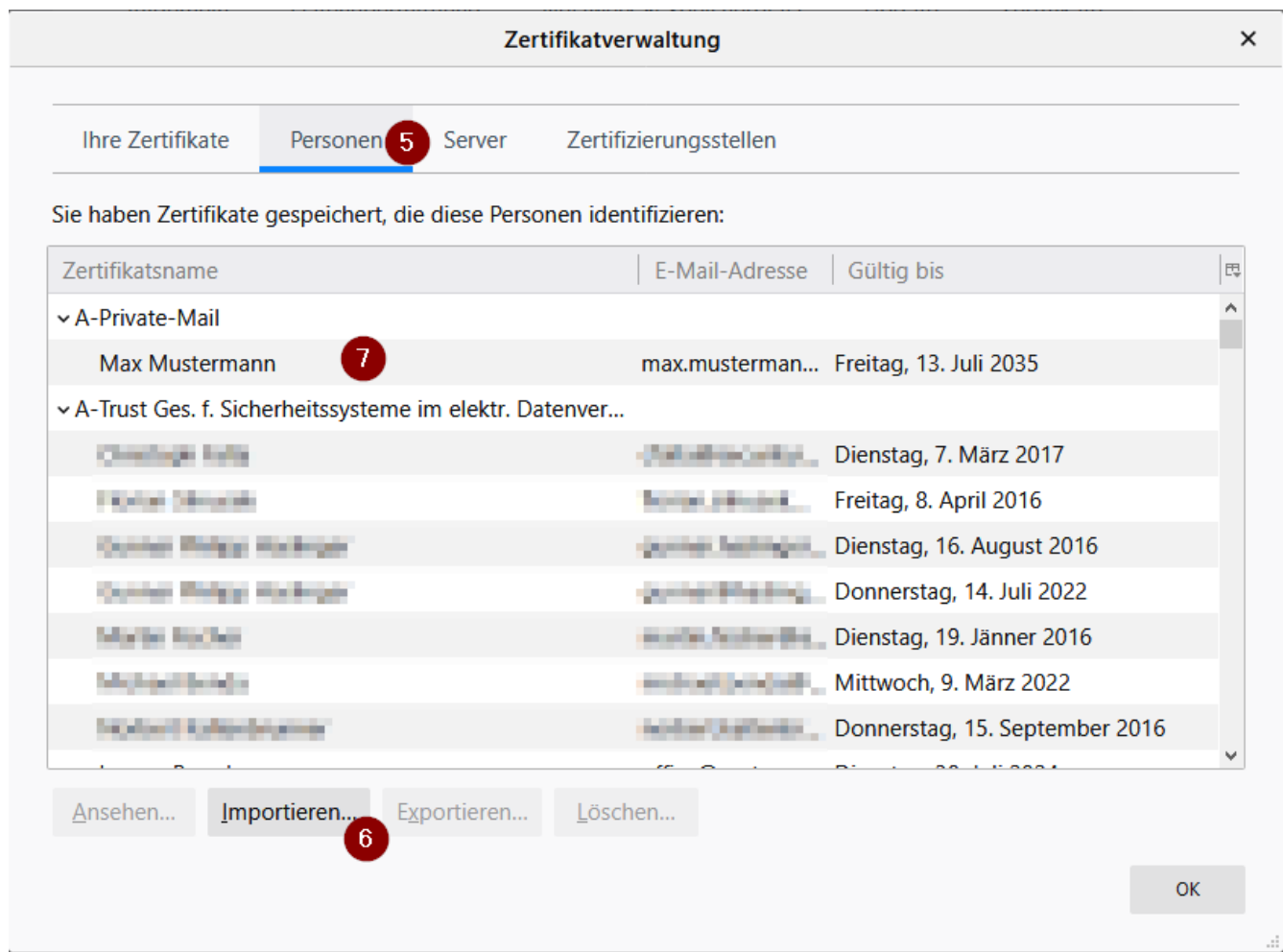


## 10 Import „fremder“ SMIME-Zertifikate ohne PrivateKey unter Thunderbird

Zu importieren ist für gewöhnlich nur das eigene SMIME-Zertifikat in Form der p12-Datei (also inkl. Private-Key). Die „anderen“ SMIME-Zertifikate fremder Personen müssen nicht importiert werden, da man diese trusten kann sobald man die erste signierte E-Mail von diesen erhält. Will man diesen aber verschlüsselte E-Mails senden, noch bevor man von diesen eine signierte E-Mail erhalten hat, so können auch diese importiert werden.

Wie im vorherigen Abschnitt bereits erläutert, im Thunderbird im Menü „Extras“ [1] => „Einstellungen“ => Erweitert [2] => Zertifikate [3] => Zertifikate verwalten [4]

Nun unter „Personen“ [5] mittels Button „Importieren“ [6] die CER-Datei des Kommunikationspartners importieren, diese scheint anschließend in der Liste (siehe [7] im Screenshot, es wurde Max Mustermann als Beispiel importiert) auf.



## 11 Konfiguration des zu verwendenden Zertifikats im Thunderbird Konto

Das S/MIME-Zertifikat ist zuletzt noch im Thunderbird-Konto zu konfigurieren:

Thunderbird-Menü: „Extras“ => „Konteneinstellungen“

Hier beim betreffenden E-Mail-Konto unter [1] S/MIME-Sicherheit das Zertifikat für die Digitale Unterschrift [1] und für die Verschlüsselung [2] konfigurieren. Wenn das zuvor importierte Zertifikat hier nicht zur Auswahl angeboten wird, dann passt die E-Mail-Adresse die im Zertifikat hinterlegt ist nicht zur im Konto konfigurierten E-Mail Adresse.

