E-Mail-Verschlüsselung mit S/MIME

17. November 2015

Inhaltsverzeichnis

In diesem Dokument wollen wir euch zeigen, wie ihr – am Beispiel von Firefox und Thunderbrid – ein S/MIME-Zertifikat erstellen könnt, mit dess Hilfe ihr und eure Freunde bequem verschlüsselte E-Mails austauschen könnt. Dazu sind drei Schritte notwendig:

1. Das Zertifikat erstellen.
2. Das Zertifikat aus Firefox exportieren.
3. Das Zertifikat in Thunderbrid importieren.

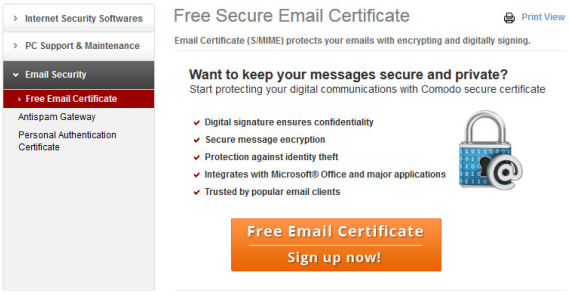
1 Zertifikat erstellen

Als erstes: Das Erstellen eines Zertifikates. Dabei wird ein privater und ein öffentlicher Schlüssel im Browser erzeugt. Der öffentliche Schlüssel wird zusammen mit einer E-Mail-Adresse, für die das Zertifikat gelten soll, an den Aussteller gesendet, der nun sicherstellen möchte, dass die E-Mail-Adresse auch der Person gehört, die die Anfrage stellt. Danach signiert der Aussteller – in unserem Beispiel Comodo – die Kombination aus E-Mail-Adresse und öffentlichem Schlüssel. Der private Schlüssel verlässt den Rechner nicht. Das Zertifikat von Comodo ist in der kostenlosen Variante ein Jahr gültig. Danach, kann ein neues, wiederum ein Jahr gültiges, erstellt werden.
Zum Erstellen dieses Zertifikats sind drei Schritte notwendig:

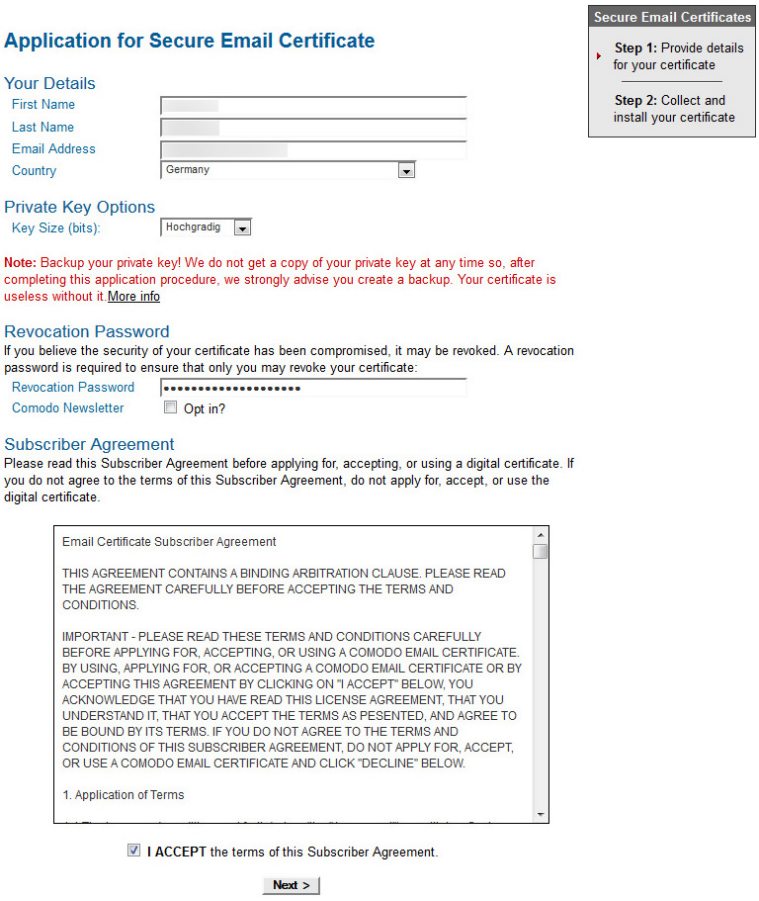
1. Besuchen Sie die Webseite

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

   und klicken Sie auf *Sign up now*:



2. Das Formularfeld muss mit Name, Nachname und E-Mail-Adresse ausgefüllt werden. Das Zertifikat wird für die hier eingetragene E-Mail-Adresse erstellt. In dem Feld *Key Size* ist es empfehlenswert, den höchstmöglichen Wert auszuwählen. Je länger der Schlüssel ist, desto sicherer ist die Verschlüsselung.

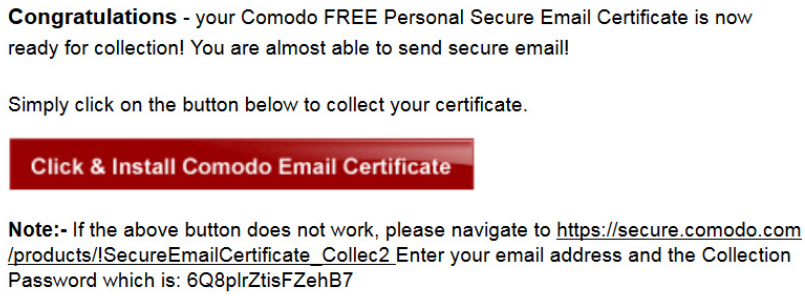


   Das *Revocation Password* dient dem Widerruf des Zertifikats, wenn der geheime Schlüssel beispielsweise durch einen Virus / Trojaner in die falschen Hände geraten sein sollte oder die Zertifikatserstellung fehlgeschlagen ist. Hier möglichst eine ausreichend lange zufällige Zeichenfolge angeben und für den Verlustfall des Zertifikats aufheben. Wir empfehlen für das Speichern einen Passwordmanager wie zum Beispiel *KeePass*. Widerrufen werden kann das Zertifikat unter der folgenden Adresse:

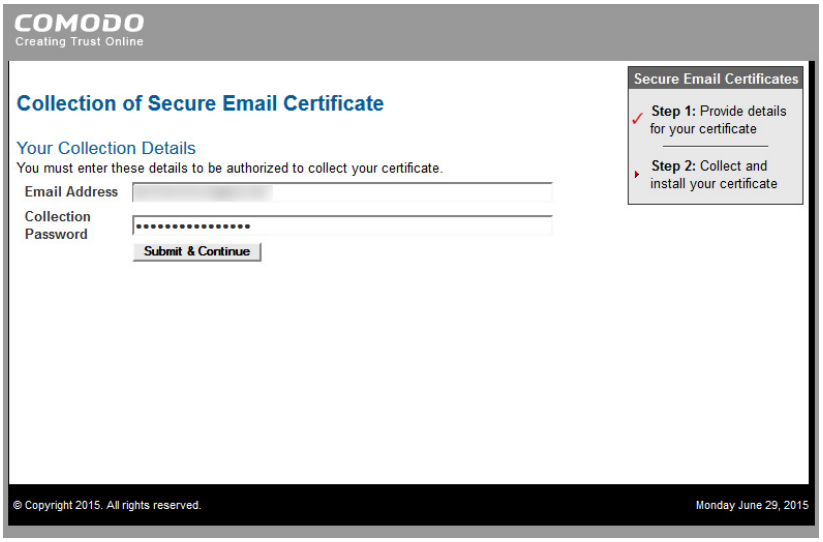
   `https://secure.comodo.com/products/!SecureEmailCertificate_Revoke`

   Alle Eingaben mit *Next >* bestätigen

3. Daraufhin schickt COMODO eine E-Mail an die in Schritt zwei angegebene Adresse. Im Zweifelsfall könnte diese im Spamordner gelandet sein. Die E-Mail enthält einen Button zum bestätigen, dass die angegebene tatsächlich Ihnen gehört.



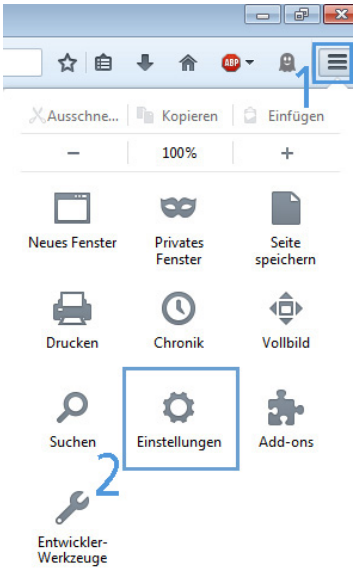
Alternativ kann die unter dem Button stehende Webseite besucht werden. Durch Eingabe der E-Mailadresse und des *Collection Password* kann die Erstellung des Zertifikats ebenfalls abgeschlossen werden:



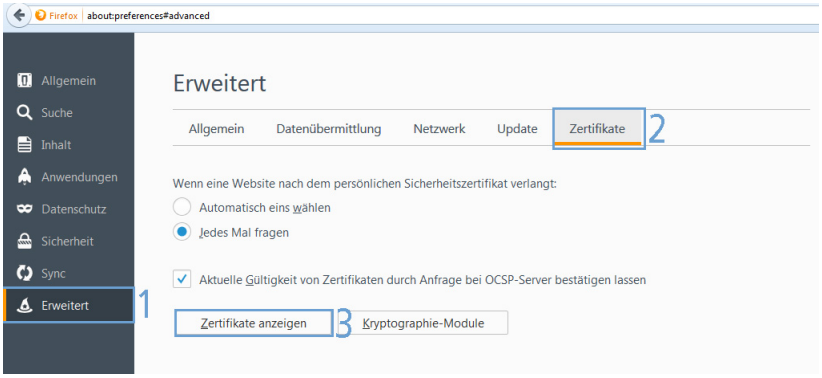
2 Zertifikat speichern

Das jetzt fertig erstellte Zertifikat ist in Ihrem Browser gespeichert. Von dort muss es so gespeichert werden, dass es in Thunderbird importiert werden kann:

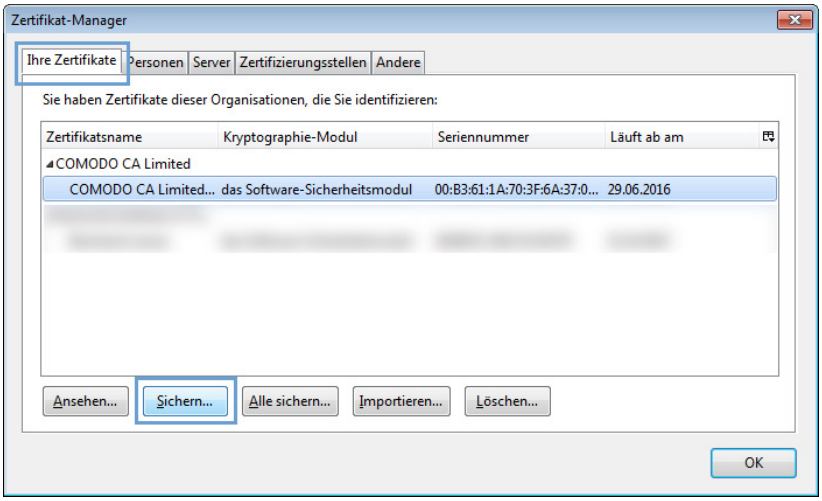
1. In Firefox (oben rechts) die Einstellungen öffnen:



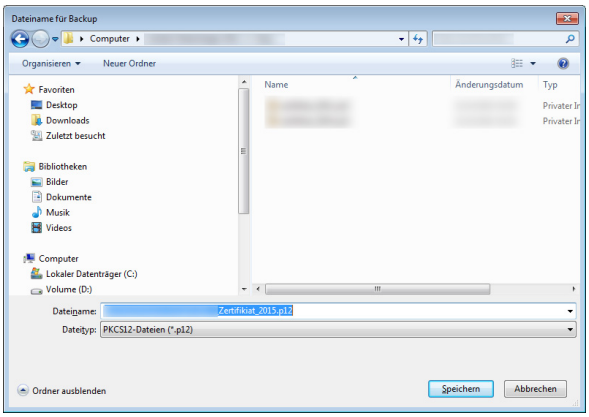
2. *Erweitert* → *Zertifikate* → *Zertifikate anzeigen*



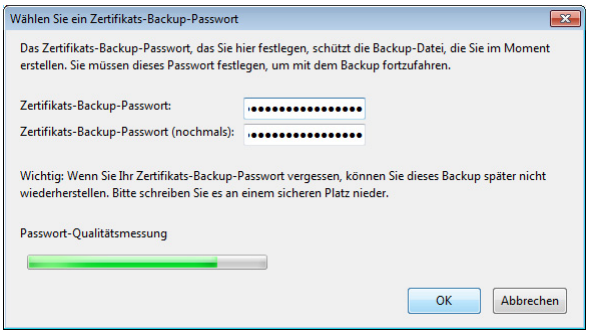
3. In das Register *Ihre Zertifikate* wechseln, das COMODO-Zertifikat auswählen und auf *Sichern...* klicken:



4. Im Speicherdialog den gewünschten Speicherort (z.B. in *Dokumente*) und Dateinamen (z.B. *E-Mail-Zertifikat-2015.p12*) wählen.



5. Ein Passwort vergeben, mit dem das Zertifikat verschlüsselt werden soll, damit der private Schlüssel nicht im Klartext auf der Festplatte liegt. Dieses Passwort wird später wieder beim Importieren in Thunderbird benötigt.

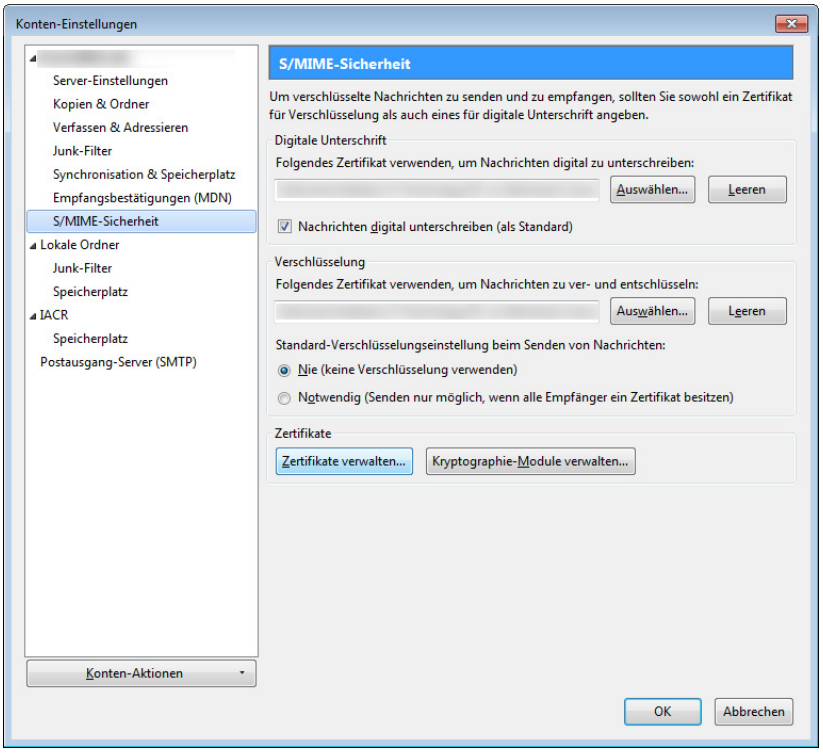


6. Nun sollte das Zertifikat aus dem Browser gelöscht werden, da es hier unverschlüsselt abgelegt ist.

3 Zertifikat in Thunderbird importieren

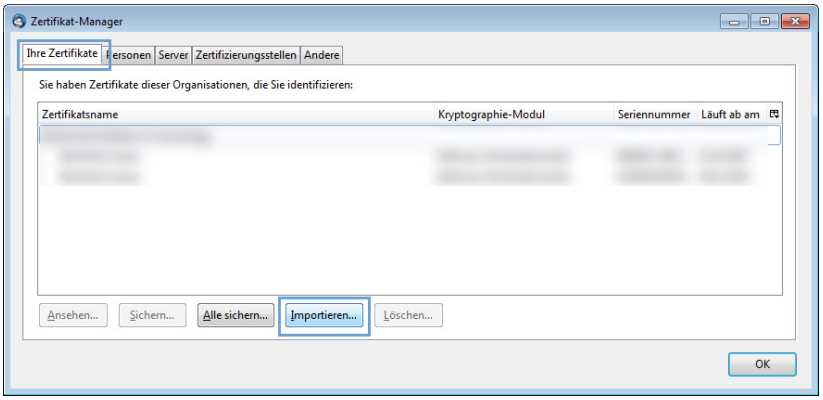
Das in Firefox exportierte (gesicherte) Zertifikat muss nun in Thunderbird importiert werden.

1. Konto-Einstellungen öffnen (in der Windows-Version im Menü Extras zu finden):

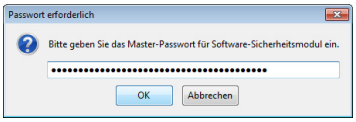


   Hier das entsprechende Konto (linke Spalte) und darin den Unterpunkt *S/MINME-Sicherheit* auswählen. Auf der rechten Seite *Zertifikate verwalten...* klicken

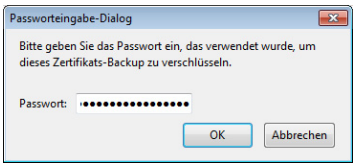
2. In dem sich öffnenden Dialogfeld den Reiter *Ihre Zertifikate* wählen und *Importieren...* anklicken und anschließend die Datei auf der Festplatte aussuchen, die in Schritt 4 beim Speichern des Zertifikats erstellt wurde:



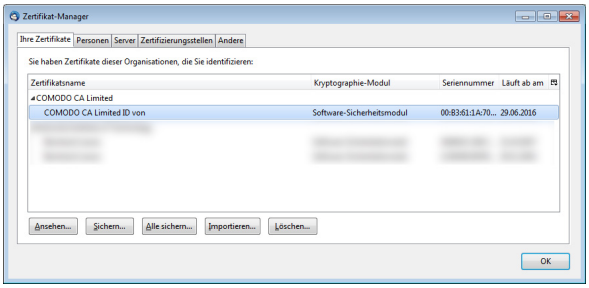
3. Wenn die Passwörter für die E-Mailkonten mit einem zentralen Master-Passwort verschlüsselt sind, muss dieses nun evtl. eingegeben werden. Sonst kommt direkt das nächste Dialogfeld.



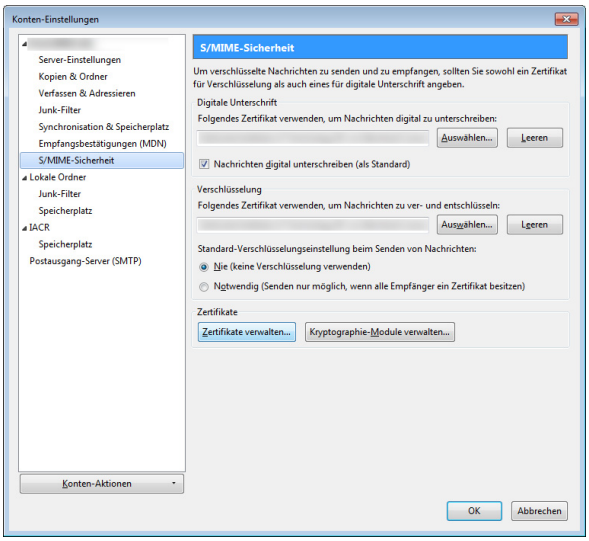
In das Dialogfeld *Passworteingabe-Dialog* muss das Passwort eingegeben werden, das beim sichern aus Firefox vergeben wurde (Siehe Zertifikat speichern, Schritt 5).



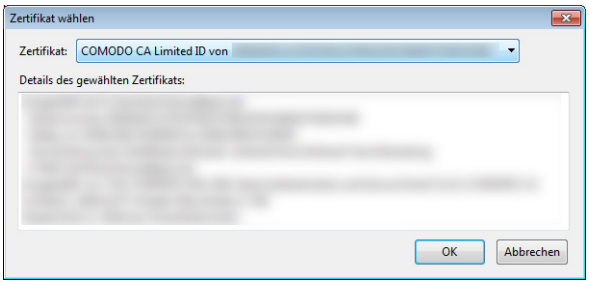
4. Das Zertifikat taucht nun unter *Ihre Zertifikate* auf.



5. Um E-Mails signieren und entschlüsseln zu können, muss das Zertifikat noch für diese Nutzung ausgewählt werden. Sowohl bei *Digitale Unterschrift* als auch bei *Verschlüsselung* über den Button *Auswählen...*



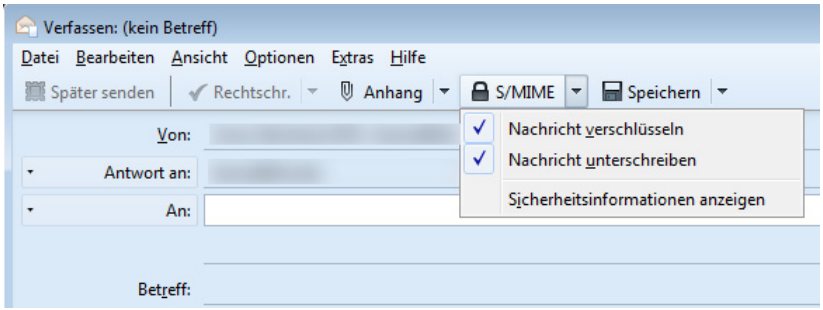
und das darauf hin erscheinende Dialogfeld



das COMODO-Zertifikat auswählen.

4 Verschlüsselte Mail senden

Ob eine Mail signiert und / oder verschlüsselt werden soll, kann nun beim Erstellen der Mail ausgewählt werden.



Nur an Empfänger, zu denen der private Schlüssel bekannt ist, können Mails auch verschlüsselt werden. Der einfachste Weg den eigenen privaten Schlüssel zu übertragen ist dem Kommunikationspartner eine signierte E-Mail zu schicken.

5 Verschlüsselte Mail empfangen

Ob eine Mail nun signiert und / oder verschlüsselt wurde, können Sie den Symbolen entnehmen die im Kopf der E-Mail angezeigt werden: Um die Nachricht lesen zu können, müssen Sie nichts weiter tun. Thunderbird zeigt ihnen die Mail automatisch entschlüsselt an.