E-Mail-Verschlüsselung mit S/MIME und Thunderbird

Für die Verschlüsselung mit S/MIME wird ein Schlüsselpaar benötigt, das von einer Stammzertifizierungsstelle[1] beglaubigt ist – der Beglaubigungsteil ist ein sogenanntes Zertifikat. Üblicherweise ist diese Beglaubigung kostenpflichtig. Einige wenige Stellen, bieten dies aber kostenfrei an. Für den **privaten Gebrauch** wird dies beispielsweise von Comodo angeboten. Unabhängig vom Einsatzgebiet bietet StartSSL[2] ebenfalls kostenfreie Zertifikate an.

U.a. bei diesen beiden Anbietern findet „nur“ eine sogenannte E-Mail-Validierung statt. Es wird also nur geprüft, ob der Antragssteller Zugriff auf das Mailkonto hat. Die Beglaubigung umfasst also auch nur diese Angabe.

Aufwändiger aber auch wesentlich vertrauenswürdiger, weil ein persönliches Treffen mit sogenannten Assuren erforderlich ist, ist CAcert[3].

Da Comodo das vergleichsweise einfachste Verfahren anbietet, wird hier für die ersten „Gehversuche“ dieser Anbieter einführend verwendet.

S/MIME-Zertifkat / Free Secure Email Certificate von Comodo[4]

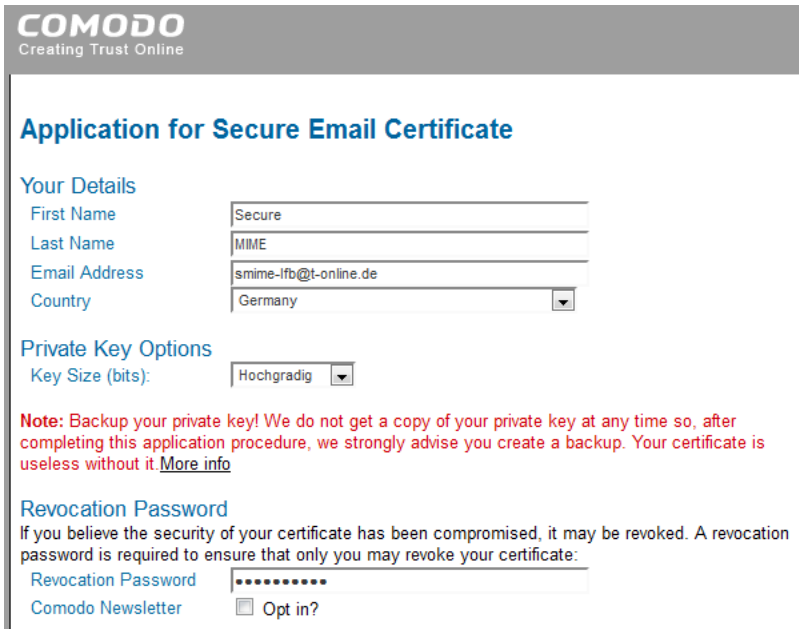
Unter der in der Fußnote angegebenen Adresse beginnt der Beantragungsprozess durch einen Klick auf die nebenstehende dargestellte Schaltfläche.

Im nachfolgenden Formular füllen Sie die Felder „Vorname“, „Nachname“, „E-Mail-Adresse“ und „Land“ aus.

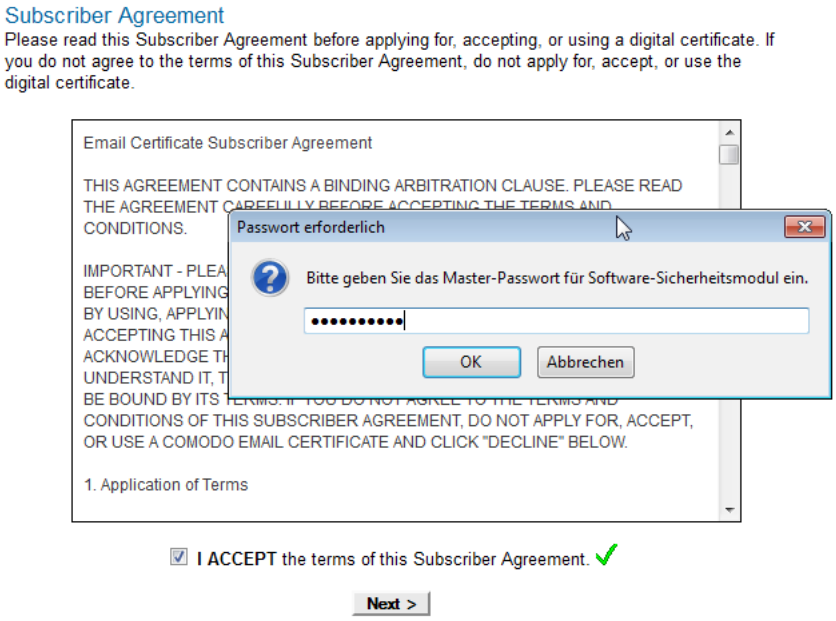
Die Schlüsseloption belassen Sie auf „Hochgradig“ oder „2048 (High Grade)“ - je nach Browser.

Um ggf. das Zertifikat vorzeitig für ungültig zu erklären – eine Revocation – überlegen Sie sich für diesen Zweck ein Revocation-Passwort und tragen auch das ein.

Wenn Sie den Comodo Newsletter nicht abonnieren möchten, entfernen Sie diese Option die standardmäßig gesetzt ist.



1 Stammzertifizierungsstelle (engl. Certification Authority oder CA) ist so etwas wie ein Notar in der digitalen Welt. Die Stammzertifizierungsstelle, der digitale Notar, stellt Beglaubigungen aus.
2 http://www.startssl.com/
3 http://www.cacert.org/
4 http://www.comodo.com/home/email-security/free-email-certificate.php od. http://tinyurl.com/freecert



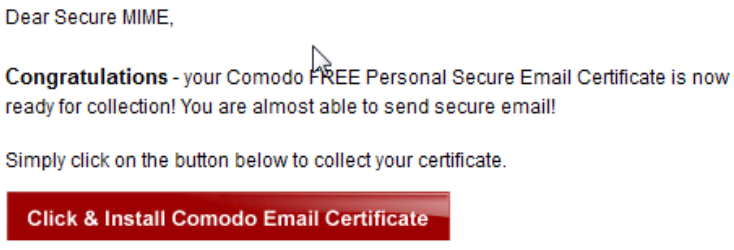
Im unteren Teil des Antragsformulars finden Sie den legalen Teil des Antrags – eine Einverständniserklärung / Vereinbarung zwischen Ihnen und Comodo. Diese Vereinbarung muss über das Setzen der ACCEPT-Option akzeptiert werden.

Nach dem **Anklicken der Schaltfläche „Next >“** sendet Comodo einen Funktionsaufruf an Ihren Browser, damit dieser über eine eingebaute Cryptofunktion ein Schlüsselpaar erzeugt.

Insbesondere der geheime Schlüssel (einer der beiden Schlüssel des Schlüsselpaars) verlässt Ihren Rechner dabei nicht! Nur der öffentliche Schlüssel wird anschließend automatisch an Comodo zur Beglaubigung übermittelt.

Da bei dieser Aktion das Schlüsselpaar in den Zertifikatsspeicher des Browsers geschrieben wird, müssen Sie diesen gegebenfalls über die Angabe des Master-Passworts freigeben. Sie haben doch hoffentlich ein Master-Passwort gesetzt? Falls nicht, machen Sie das unbedingt im Anschluss! Das Master-Passwort schützt unter anderem ihr persönliches Zertifikat und damit Ihre persönliche Identität.

Nach erfolgreicher Durchführung dieser Aktion, teilt Ihnen Comodo nun mit, dass die Antragsstellung durchgeführt wurde und Sie nun eine E-Mail erhalten.



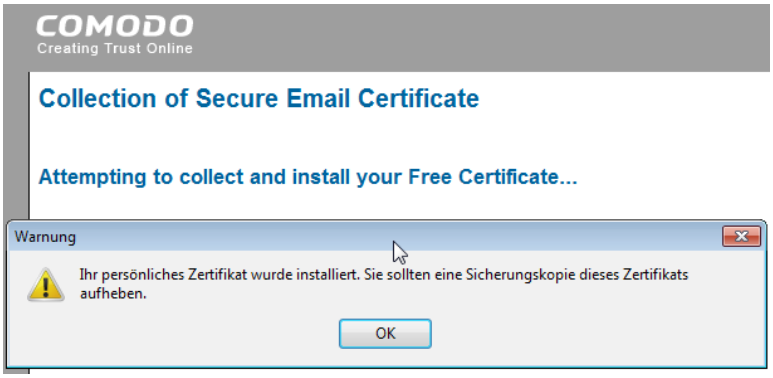
Mit dieser Mail, die Sie nach kurzer Zeit im Maileingang finden solllten, überprüft Comodo in einem Schritt, ob Sie das zugehörige Mailkonto abrufen können und teilt Ihnen mit, wo Sie die Beglaubigung abrufen können.

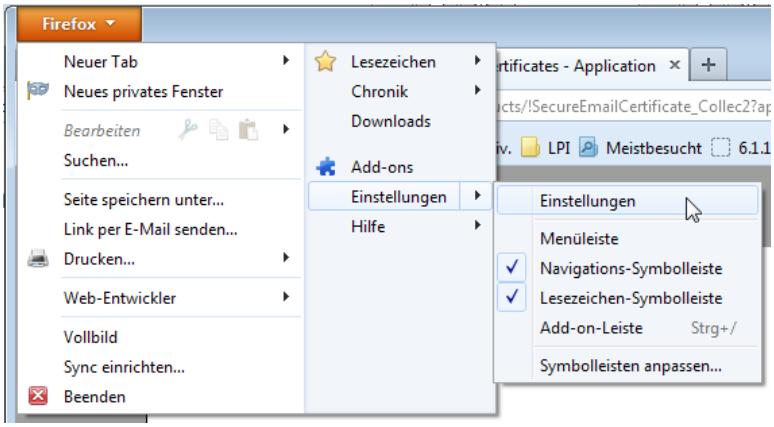
ACHTUNG: Es ist unbedingt erforderlich die nachfolgende Aktion mit dem gleichen Browser (hier war das Mozilla Firefox) durchzuführen, mit dem auch der vorige Schritt – die Beantragung des Zertifikats – durchgeführt wurde!!!

Klicken Sie zum Abruf des Zertifikats auf die Schaltfläche „Click & Install Comodo Email Certificate“. Die aufgerufene Seite auf der Comodo-Website übermittelt die Beglaubigung (das Zertifikat) und Ihr Browser fügt dies nun noch an Ihr bereits im Zertifikatsspeicher befindliches Schlüsselpaar an.

Die erfolgreiche Transaktion wird Ihnen durch eine kleine Dialogbox angezeigt.

Nehmen Sie das über „OK“ zur Kenntnis.





Das Zertifikat ist nun im Zertifikatsspeicher von Firefox enthalten. Leider hat Thunderbird, obwohl aus gleichem Haus, seinen eigenen Zertifikatsspeicher. Das Zertifikat muss also auf Firefox exportiert und in Thunderbird importiert werden.

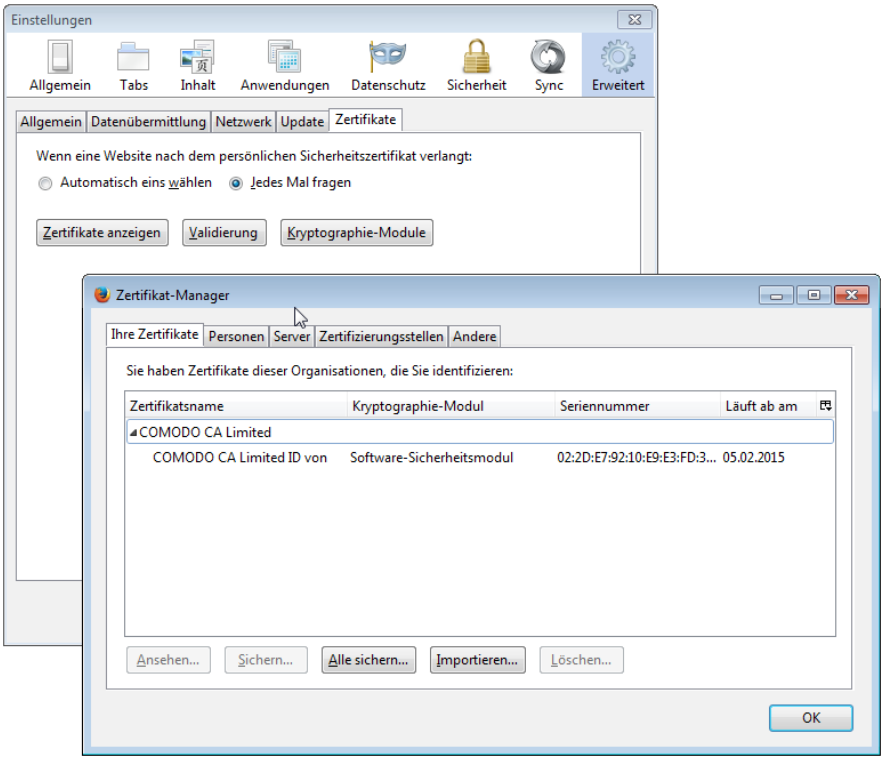
Rufen Sie nun die Einstellungen von Firefox auf – siehe Screenshot.

In den Einstellungen wählen Sie in der Icon-Leiste das Zahnrad-Icon → Erweitert.

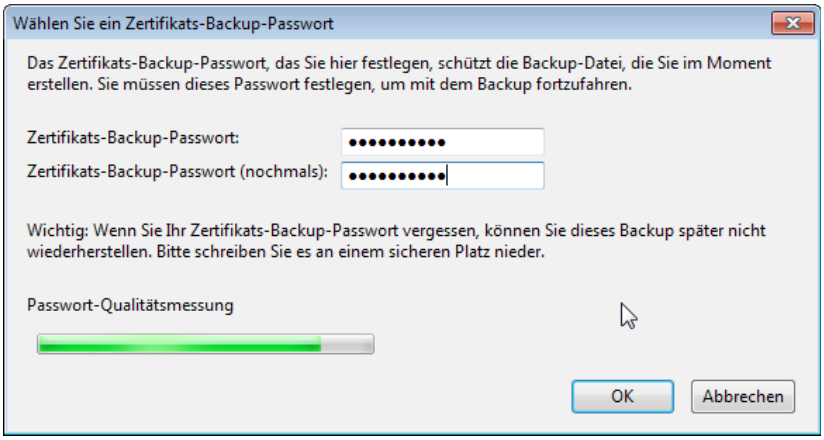
Klicken Sie dann auf den Reiter „Zertifikate“ und wählen Sie die Schaltfläche „*Zertifikate anzeigen*“.

Sie sehen dann den Zertifikat-Manager. Gehen Sie hier zum Reiter „*Ihre Zertifikate*“.

Wählen Sie Ihr Zertifikat durch einen Mausklick aus und klicken Sie danach die Schaltfläche „*Sichern ...*“ an.



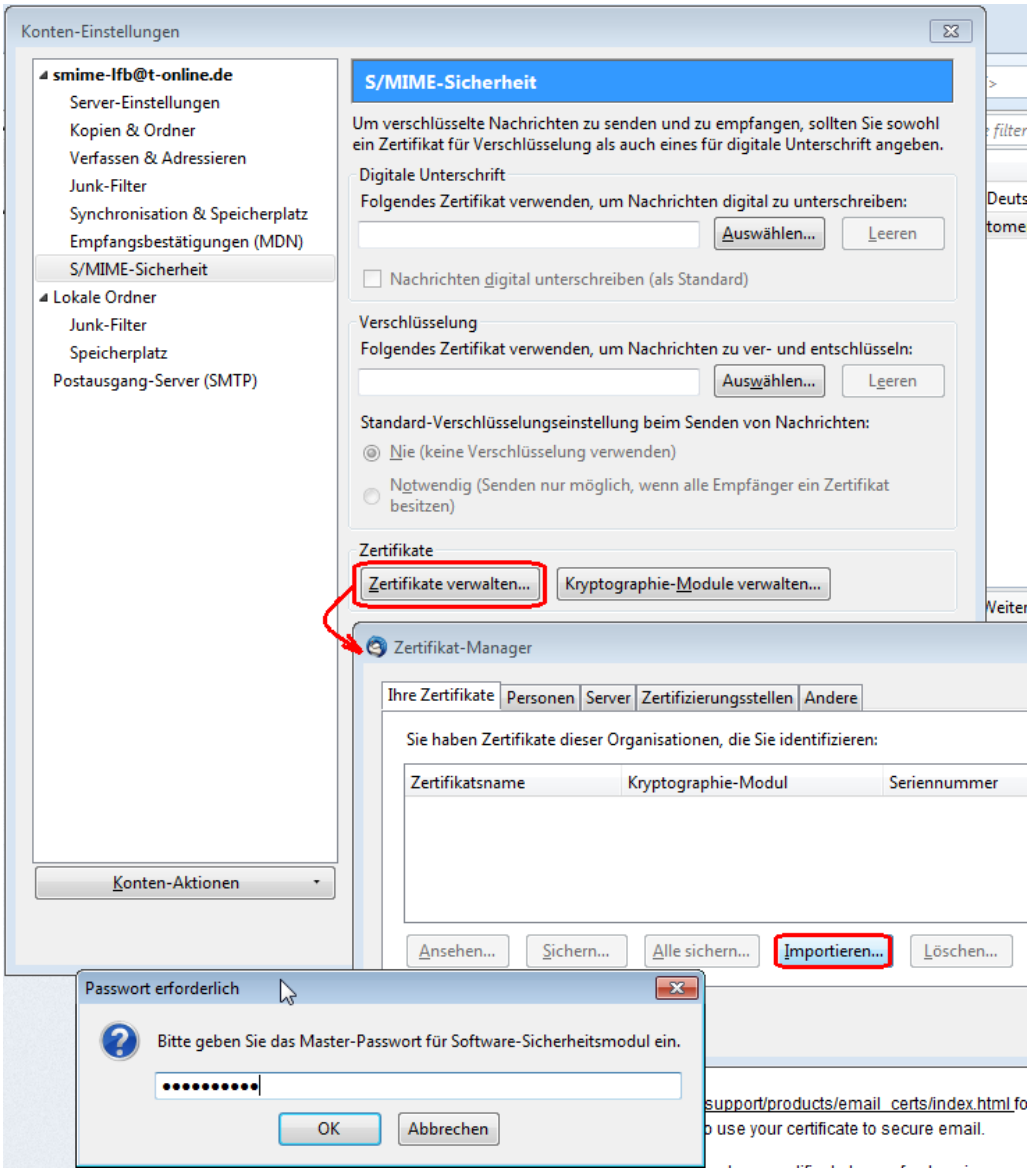
Gespeichert wird das Zertifikat im PKCS12-Format bei dem die Inhalte verschlüsselt gespeichert werden. Wählen Sie einen Speicherort für das Zertifikat und einen „sprechenden“ Dateinamen mit der Dateinamen-Erweiterung (Extension) ***.p12*** – ein mögliches Beispiel wäre in meinem Fall z.B.: ***mein-t-online-zertifikat.p12*** – denken Sie sich etwas Passendes aus.



Wie schon erwähnt, wird das Zertifikat verschlüsselt gespeichert. Grundlage ist ein gutes Passwort.

Geben Sie hier also ein Passwort ein, dem Sie erneut Ihre digitale Identität anvertrauen.

Sie erhalten anschließend eine kurze Erfolgsbestätigung. Nun muss das Passwort in Thunderbird importiert werden. Rufen Sie dazu in Thunderbird über die **Konten**-Einstellungen im betreffenden Konto → „*S/MIME-Sicherheit*“ ebenfalls den Zertifikats-Manager (→ „*Zertifikate verwalten*“) auf.

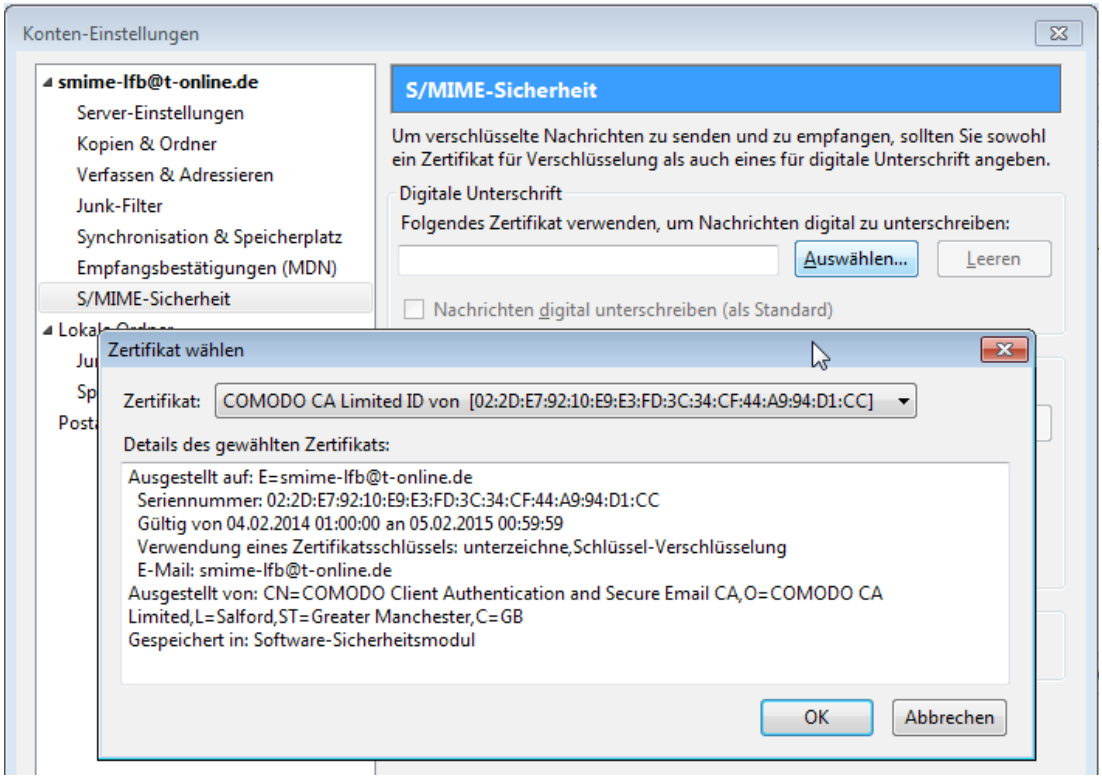


Starten Sie den Import Ihres Zertifikats durch einen Klick auf „Importieren ...“. Wählen Sie dann die im vorigen Schritt gespeicherte P12-Datei. Sie werden nun

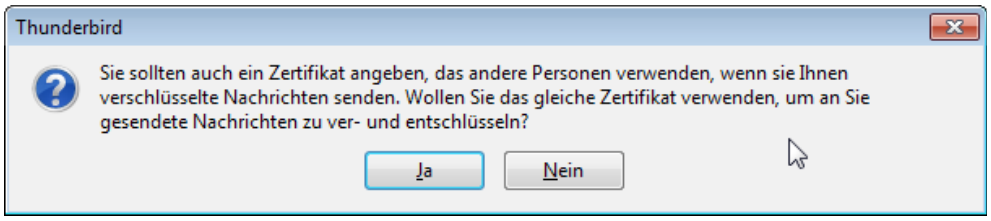
- nach dem Master-Passwort von Thunderbird gefragt (Sie haben doch eins – oder?)
- und nach dem Backup-Passwort des Zertifikats um dieses zu entschlüsseln.

Nach erfolgreichem Import schließen Sie den Zertifikats-Manager.

Im Bereich „Digitale Unterschrift“ müssen Sie nun Ihr persönliches Zertifikat hinterlegen. Klicken Sie dazu auf „*Auswählen ...*“ und ...



… wählen Sie Ihr vorher importiertes Zertifikat aus. Thunderbird fragt anschließend sofort nach, ob das gleiche Zertifikat auch für das Entschlüsseln verwendet werden soll – klicken Sie hier „Ja“ an.



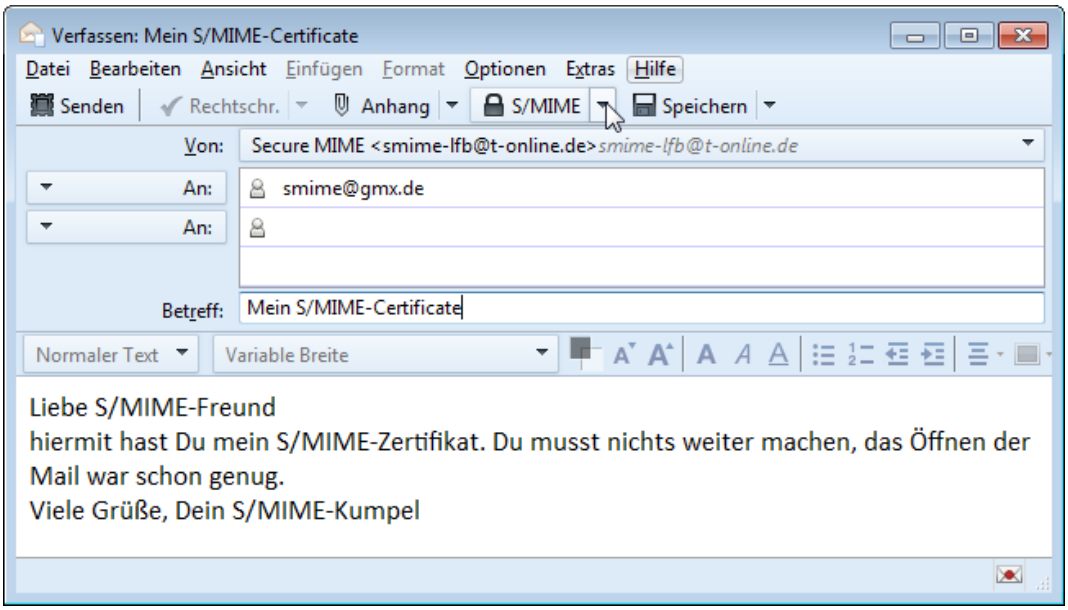
Damit haben Sie es eigentlich geschafft. Thunderbird ist nun für digitale Unterschriften und für verschlüsselten Mailverkehr vorbereitet.

Sie können nur noch überlegen, ob Sie an dieser Stelle auch gleich einstellen wollen, dass Ihre Mails zukünftig automatisch digital unterschrieben werden sollen. Falls Ihnen das hier schon zusagt, setzen Sie vor dem Schließen des Konten-Einstellungs-Fensters noch die Option „*Nachrichten digital unterschreiben (als Standard)*“. Sie können natürlich jederzeit in den Konten-Einstellungen wieder Änderungen vornehmen.

Kommen wir zur Anwendung im Alltag.

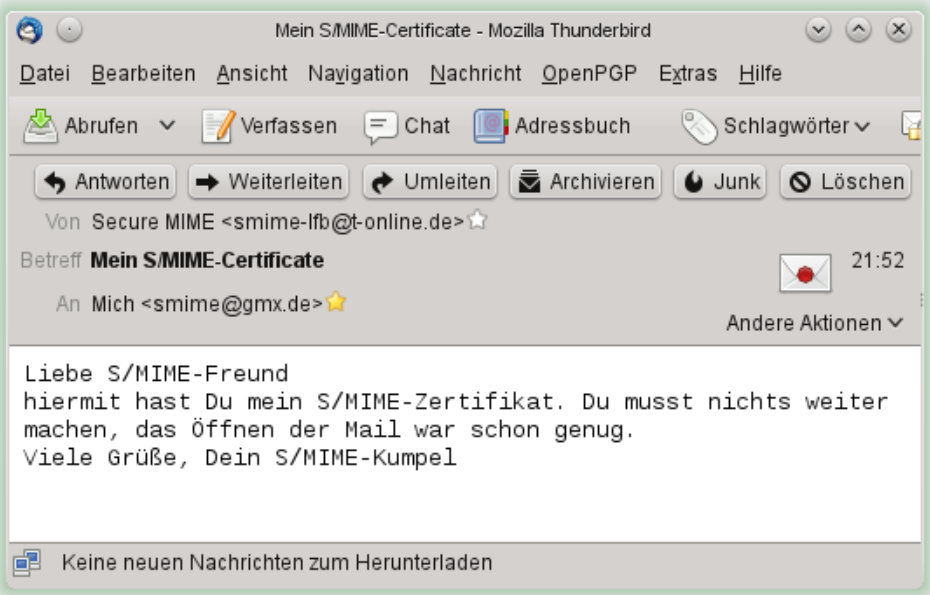
Praktische S/MIME-Anwendung

Versenden einer digital unterschriebenen Mail: Klicken Sie auf S/MIME und wählen Sie die Option „*Nachricht unterschreiben*“ aus – mehr ist dafür nicht zu machen. Sie verfassen einfach Ihren Mailtext, fügen evtl. noch Anhänge hinzu, und senden die Mail dann einfach ab.



Ein Nebeneffekt von S/MIME ist übrigens, dass damit auch gleich das eigene Zertifikat (nur der für die Öffentlichkeit bestimmte Anteil) an den Empfänger übermittelt wird[5].

Der Empfänger sieht die gültige Signatur am „versiegelten Briefumschlag“ - ein Mausklick darauf zeigt nähere Informationen an. Wurden von irgendjemanden Änderungen am Mailinhalt vorgenommen, ist die Unterschrift ungültig und es wird ein anderes Icon zur Warnung angezeigt.



5 Für die Profis: Der lästige Schlüsselaustausch bei GnuPG ist hier doch wesentlich eleganter gelöst.

Wie im obigen Beispiel-Mailtext beschrieben, ist als Nebeneffekt das Zertifikat des Absenders **automatisch** im Zertifikatsspeicher des Empfängers gespeichert. Eine Nachfrage dazu erfolgt nicht.

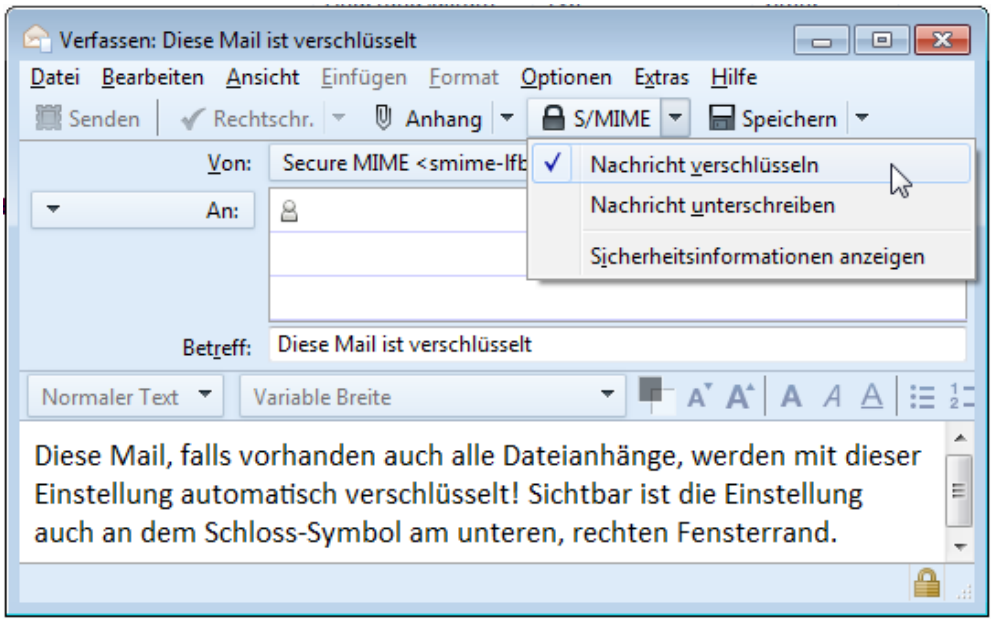
Sie müssen jedem Kommunikations-Partner, der auch in der Lage sein soll Ihnen verschlüsselte Informationen zu mailen, einmal eine unterschriebene Mail senden. Damit hat das Gegenüber, wie gerade beschrieben, Ihr öffentliches Zertifikat. Genau dieses Zertifikat von Ihnen wird für verschlüsselte Mails benötigt.

So gesehen ist es grundsätzlich eine gute Idee, die digitale Signatur Ihrer Mails als Standard einzustellen. Empfänger die nur einen Webmailer verwenden, sind allerdings dann oft etwas verwirrt, da bei ihnen die digitale Signatur als Mailanhang in einer P7-Datei erscheint.

Verschlüsselte Mails

Grundvoraussetzung für verschlüsselte Mails: Der Empfänger muss Ihnen vorab sein öffentliches Zertifikat per Mail übermittelt haben. Dazu muss er, wie im vorigen Abschnitt beschrieben, einmal eine digital unterschriebene Mail an Sie gesandt haben.

Danach geht es ganz einfach → neue Mail verfassen und im S/MIME-Menü die Option „*Nachricht verschlüsseln*“ setzen. Beachten Sie auch den Mailtext.



Das kann nicht so einfach sein …

Oh doch …, wenn Sie bis hierher gekommen sind, dann ist das nachfolgend sooooo einfach. Wenn Sie es nicht glauben, schauen Sie sich doch mal den Quellcode einer verschlüsselten Mail an – die Sie dazu einfach mal verschlüsselt an sich selbst mailen. Klicken Sie die Mail an und drücken Sie dann „Strg“ + „U“ auf der Tastatur. Sie sehen dann den Quellcode der Mail.

```
X-Seen: false
X-ENVELOPE-TO: <smime-lfb@t-online.de>

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHFMIIBwQIBADCBqDCBkzELMAkGA1UEBhMCR0IxGzAZ
BgNVBAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UEBxMHU2FsZm9yZDEaMBgGA1UEChMR
Q09NT0RPIENBIExpbWl0ZWQxOTA3BgNVBAMTMENPTU9ETyBDbGllbnQgQXV0aGVudGljYXRp
b24gYW5kIFNlY3VyZSBFbWFpbCBDQQIQAi3nkhDp4/08NM9EqZTRzDANBgkqhkiG9w0BAQEF
AASCAQB5kRxnvWGOnRM6c3rmxC2ehniOtIJEjKiDOq83heiP6nMlsxsMK7SvOethgeqOnaMK
```

Dieser „Zeichensalat“ ist der verschlüsselte Mailinhalt, ggf. incl. Dateianhänge.

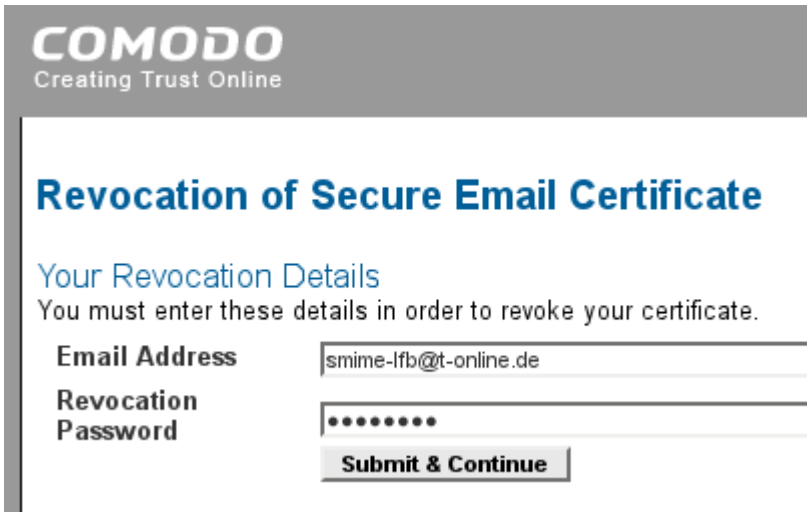
Anhang A – Comodo-Zertifikate für ungültig erklären

Gründe für das Zurückziehen eines Zertifikats / ein Zertifikat für ungültig erklären:

- Das Zertifikat / Teile des Zertifikats gingen verloren
- Es besteht der Verdacht, dass das Zertifikat in falsche Hände gelangt ist

In solchen Fällen benötigen Sie ein neues Zertifikat und müssen das bisherige Zertifikat möglichst für ungültig erklären / zurückziehen, oder im englischen Fachbegriff → eine Revocation durchführen.

Am Beispiel von Comodo-Zertifikaten gehen Sie dazu auf https://secure.comodo.com/products/!SecureEmailCertificate_Revoke, tragen die E-Mail-Adresse und das Revocation Passwort (wurde bei der Beantragung des Zertifikats festgelegt) des betroffenen Zertifikats ein.



Betätigen Sie dann die Schaltfläche „Submit & Continue“. Bei korrekter Angabe des Revocation Passworts erhalten Sie die nachfolgende Rückbestätigung.

Anhang B – CAcert – Vertrauen – aber richtig!

Inhalt folgt noch