Bernhard Esslinger

Sichere E-Mail mit S/MIME

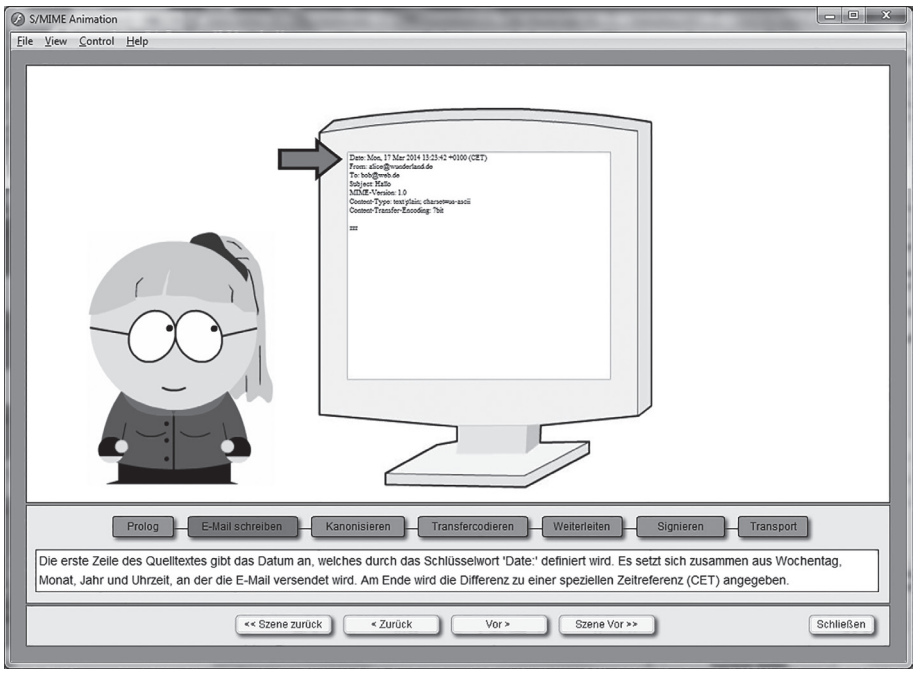
Eine Anleitung aus Anwenderperspektive

Lange Zeit war der eingeschränkte Bedienkomfort von E-Mail-Verschlüsselungslösungen eine populäre Ausrede für den Verzicht auf Schutzmaßnahmen. Dieser Beitrag zeigt ganz praktisch, wie man auf verschiedenen Plattformen sichere E-Mails nach dem S/MIME-Standard austauschen kann. Kryptographische Hintergründe werden dabei bewusst ausgeklammert.

E-Mail ist das verbreitetste Kommunikationsmedium im geschäftlichen Umfeld und wird vielfach auch im privaten Bereich eingesetzt – außer bei denjenigen, die nur (noch) über Facebook oder WhatsApp kommunizieren. Für sichere E-Mails braucht man Ende-zu-Ende-Verschlüsselung (Vertraulichkeit) und elektronische Signaturen (Integrität und Authentizität). „Verschlüsseln" bedeutet, dass der Absender den Inhalt so verschlüsselt, dass dieser nur vom gewünschten Empfänger wieder entschlüsselt werden kann. „Signieren" bedeutet, dass der Absender unterschreibt und der Empfänger nachprüfen kann, von wem die E-Mail wirklich stammt und ob diese unverändert empfangen wurde.

Schon seit den 90er Jahren des letzten Jahrhunderts gibt es zwei konkurrierende, nicht interoperable Standards: S/MIME [1] und OpenPGP [2]. Beide setzen auf nahezu dieselben kryptographischen Verfahren – aber das Modell, wie Vertrauen zwischen den Teilnehmern entsteht, ist verschieden. Bei OpenPGP gibt es ein Web-of-Trust; bei S/MIME die Zertifizierungsinstanzen (CAs). Ein anderer wesentlicher Unterschied ist, dass die meisten E-Mail-Clients von Hause aus S/MIME unterstützen, OpenPGP dagegen (per Plugin) nachinstalliert werden muss. Zusätzlich ist bei OpenPGP ein Programm (Gpg4win, GnuPG etc.) zu installieren, um die Schlüssel zu erzeugen und zu verwalten. Dafür müssen die Schlüssel nicht bei jedem beteiligten Programm (Firefox, Thunderbird) in den lokalen Zertifikatsspeicher importiert werden, sondern werden zentral in einem der o.g. OpenPGP-Programme verwaltet.[1]

Abb. 1 | S/MIME-Demo in CrypTool 1



Das kostenlose Lernprogramm CrypTool enthält eine Demo, die die Abläufe bei S/MIME visualisiert (Abb. 1).

Dieser Artikel orientiert sich am Anwender, der schnell sein Sicherheitsniveau steigern möchte. Kryptographische Details und rechtliche Grabenkriege (wie zur akkreditiert qualifizierten Signatur) werden ebensowenig diskutiert wie De-Mail (siehe [3]).

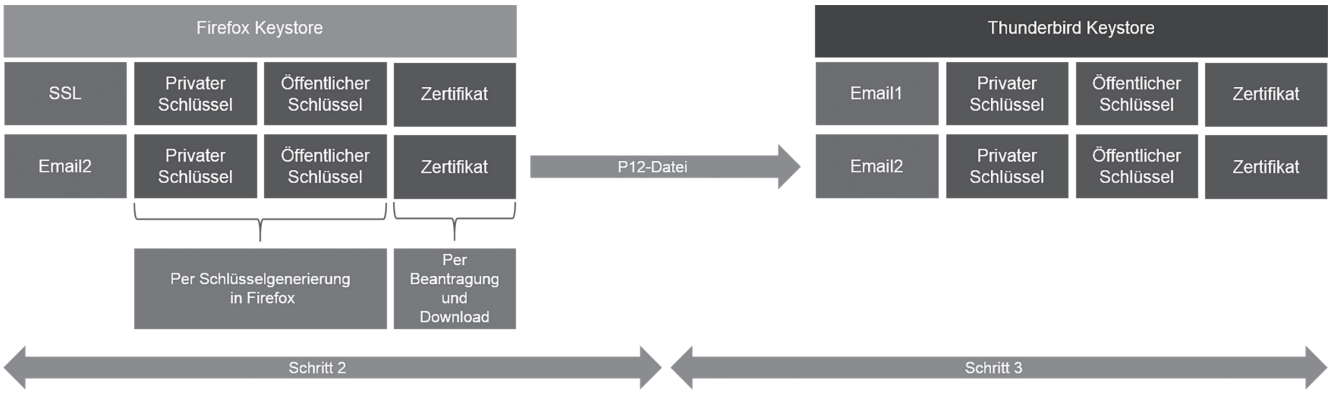
Prof. Bernhard Esslinger

Professor für IT Security und Kryptologie, Universität Siegen. Leiter des weltweiten Open-Source-Projektes CrypTool (www.cryptool.org).

E-Mail: esslinger@fb5.uni-siegen.de

1 In nahezu jeder Firma und Behörde werden für die Mitarbeiter Firmen-E-Mail-Adressen eingerichtet. Viele dieser Organisationen stellen für diese Firmen-E-Mail-Adressen auch S/MIME-Zertifikate aus. Diese Benutzer müssen selbst nichts mehr tun, um sichere E-Mail einzurichten – sie müssen nur lernen, diese zu nutzen. Wer kein Zertifikat für seine (z.B. private) E-Mail-Adresse hat, findet im Folgenden eine Anleitung dafür.

Abb. 2 | Zusammenspiel der Komponenten bei S/MIME



Sichere E-Mail in vier Schritten

Wenn Sie eine E-Mail-Adresse und einen PC (mit einem der drei Betriebssysteme Windows, MacOS oder Linux) besitzen, lässt sich sichere E-Mail in ca. 20 Minuten einrichten. Dieser initiale und einmalige Aufwand ist die wesentliche Hürde; die anschließende Benutzung unterscheidet sich kaum vom bisherigen Umgang mit E-Mails.

Zum Einrichten brauchen Sie den E-Mail-Client[2] Thunderbird[3] und ein Zertifikat. Die Einrichtung umfasst lediglich vier Schritte, und lediglich die Schritte 2 und 3 sind etwas aufwändiger:

1. Den kostenlosen E-Mail-Client Thunderbird installieren (und dabei evtl. gleich einen E-Mail-Account einrichten).
2. Beantragen eines Zertifikats (im Firefox-Browser) und dieses als P12-Datei abspeichern; danach sind das Zertifikat und das Schlüsselpaar sowohl im Firefox-Keystore als auch in der P12-Datei verfügbar.
3. Installieren des Zertifikats in Thunderbird und Konfigurieren des E-Mail-Accounts zur Verwendung des Zertifikats.
4. Senden einer signierten E-Mail; der Empfänger kann darauf sofort verschlüsselt antworten.

Nach dem Einrichten ist die Benutzung nur einen Klick entfernt – sofern Ihr Kommunikationspartner auch in der Lage ist, sichere E-Mail zu nutzen.[4]

Wir werden diese vier Schritte des Einrichtens und die anschließende Nutzung von S/MIME anhand von Screenshots[5] erläutern. Weiter gehende Details (auch zu S/MIME mit Outlook und auf Smartphones) finden Sie in [4].

Abb. 3 | Hinzufügen eines E-Mail-Kontos in Thunderbird

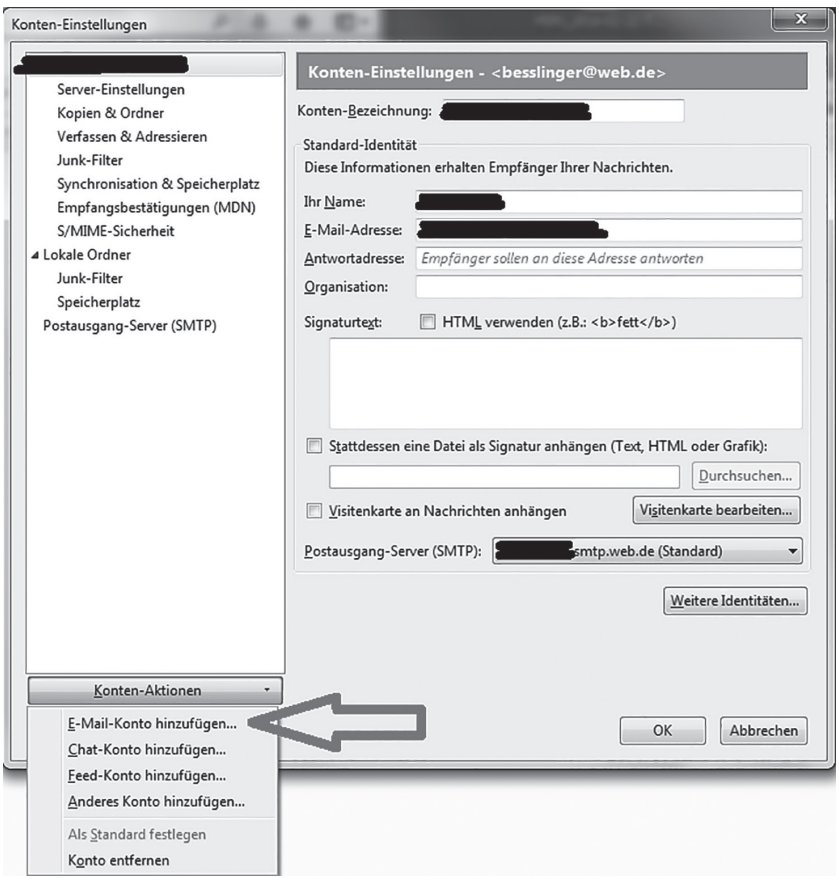


Abb. 2 zeigt, wie die beteiligten Schlüssel, das Zertifikat, die Zertifikatsspeicher (Keystores) der beteiligten Programme und die P12-Datei (zum Transport) zusammen hängen.

Schritt 1: Installiere Thunderbird

Thunderbird zu installieren und einen vorhandenen E-Mail-Account einrichten geht nahezu vollautomatisch. Wir verweisen diesbezüglich deshalb auf die Installationsanleitung von Mozilla.[6]

2 Sichere E-Mail per S/MIME braucht z. Zt. immer einen E-Mail-Client, ein Programm, mit dem man E-Mails besonders komfortabel empfangen und versenden kann. Direkt aus dem Browser heraus geht es noch nicht.

3 In den Dokumenten in [4] wird auch beschrieben, wie man sichere E-Mail mit dem E-Mail-Client Outlook und auf dem Smartphone machen kann.

4 Dass gerade Behörden bei der Unterstützung sicherer E-Mail gewaltigen Nachholbedarf haben, zeigt auch ff. Meldung aus dem April 2014: http://www.heise.de/newsticker/meldung/Firmen-und-Behoerden-schlampen-bei-Mail-Verschluesselung-2165319.html

5 Benutzt wurden dafür der Browser Firefox 27.0.1 und der E-Mail-Client Thunderbird 24.3.0 unter Windows 7.

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

Abb. 4 | Thunderbird mit mehreren E-Mail-Konten

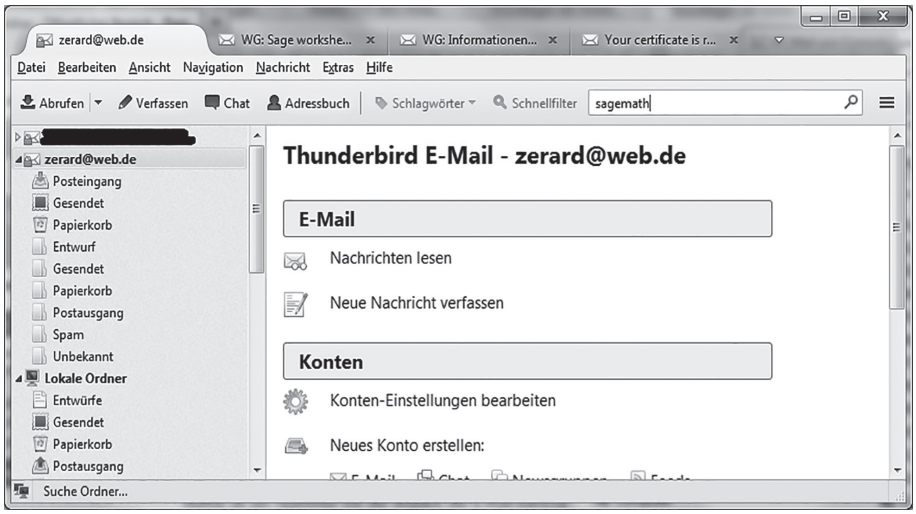
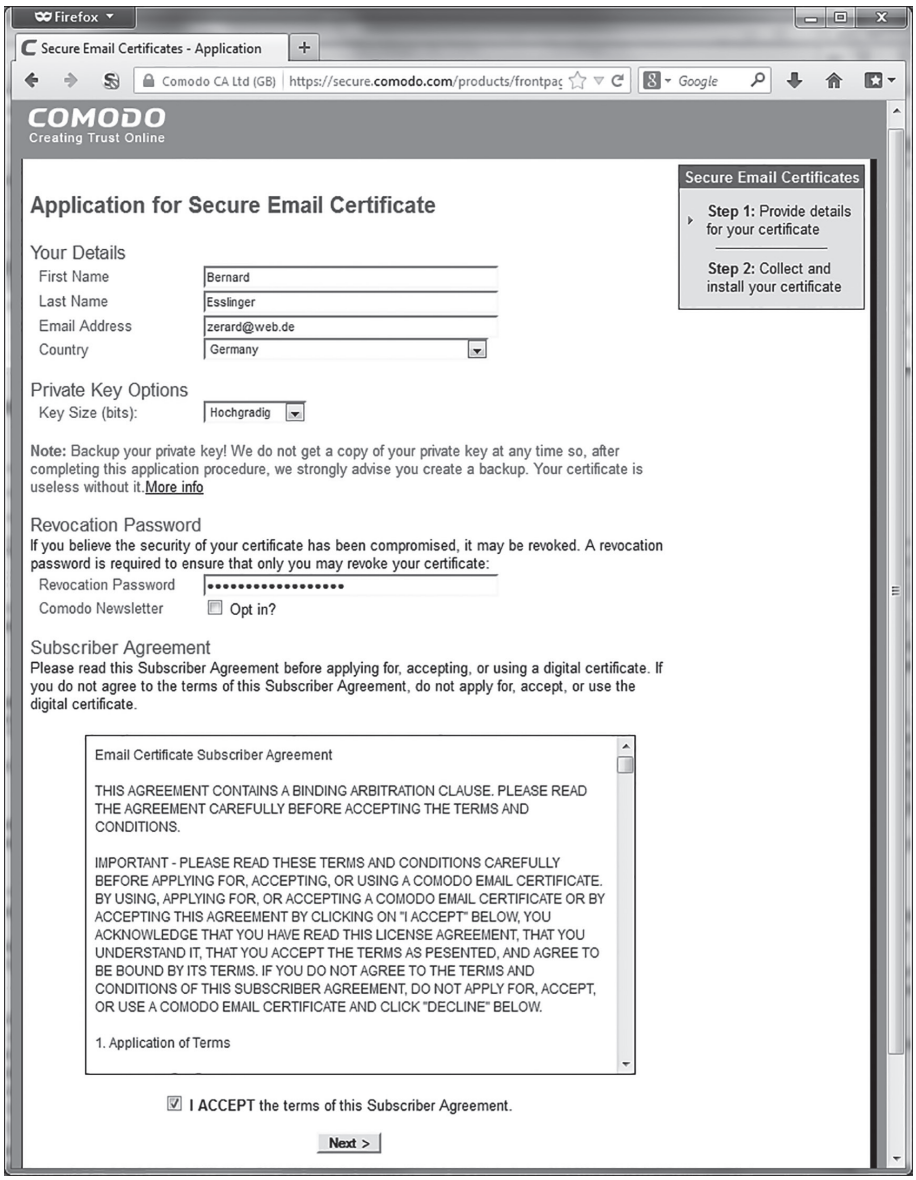


Abb. 5 | Maske von Comodo zum Beantragen eines Zertifikats



Falls Sie Thunderbird schon nutzen und für sichere E-Mail eine zweite E-Mail-Adresse verwenden wollen, geht das ebenfalls relativ einfach: Menü Extras/Konten-Einstellungen und in der folgenden Maske unter „Konten-Aktionen“ den Eintrag „E-Mail-Konto hinzufügen“ (siehe Abb. 3 und 4) auswählen.[7]

Danach erscheinen zum Einrichten des neuen E-Mail-Kontos wieder dieselben Masken, die auch bei einer Neuinstallation von Thunderbird auszufüllen sind (siehe [4], S. 6 ff). Thunderbird funktioniert problemlos mit mehreren E-Mail-Konten.

Schritt 2: Erzeuge ein Zertifikat

Wir gehen davon aus, dass Sie den Firefox-Browser nutzen (wenn nicht, müssen Sie ihn installieren[8], was ebenfalls automatisch geht). In Firefox rufen Sie die Webseite einer Zertifizierungsstelle (CA) auf, beantragen ein (kostenloses[9]) Zertifikat und speichern alles ab. Dabei erzeugt Firefox genau genommen für Sie lokal auf Ihrem Rechner ein Schlüsselpaar, sendet den öffentlichen Schlüssel an die CA, und exportiert das erhaltene Zertifikat und Ihren privaten Schlüssel in eine P12-Datei.

Der Comodo-Seite muss man leider temporär Browser-Zugriff (JavaScript) erlauben, sonst geht es per ‚Next’-Button nicht weiter (Abb. 5).

Comodo untergliedert den zweiten Schritt in zwei Teilschritte. Der erste Teilschritt ist „Provide details for your certificate“ (nimmt man den Haken bei „Opt-in“ weg, abonniert man auch

7 Es gibt zwei Möglichkeiten, in Thunderbird an die Einstellungen zu kommen:
a) Man blendet sich durch Drücken der Alt-Taste die Menüleiste ein und klickt auf den Hauptmenüeintrag „Extras“.
b) Alternativ klickt man in der darunter liegenden Bedienzeile (sie heißt offiziell Funktionen-Symbolleiste bzw. Toolbar, http://www.thunderbird-mail.de/wiki/Die_Programm-Oberfl%C3%A4che) auf die ganz rechts liegende Ikone mit den drei waagrechten Balken (der Balloontext dazu besagt: „Anwendungsmenü von Thunderbird anzeigen“).

8 Man kann auch die portable Version nutzen: Diese braucht keine Administratorrechte.

9 Kostenlose Class-1-Zertifikate gibt es z. B. von Comodo (http://www.comodo.com/home/E-Mail-security/free-E-Mail-certificate.php), StartSSL oder CAcert. Die Gültigkeitsdauer beträgt normalerweise ein Jahr, bei CAcert zwei Jahre.

Abb. 6 | E-Mail-Aufforderung von Comodo zum Abholen des Zertifikats

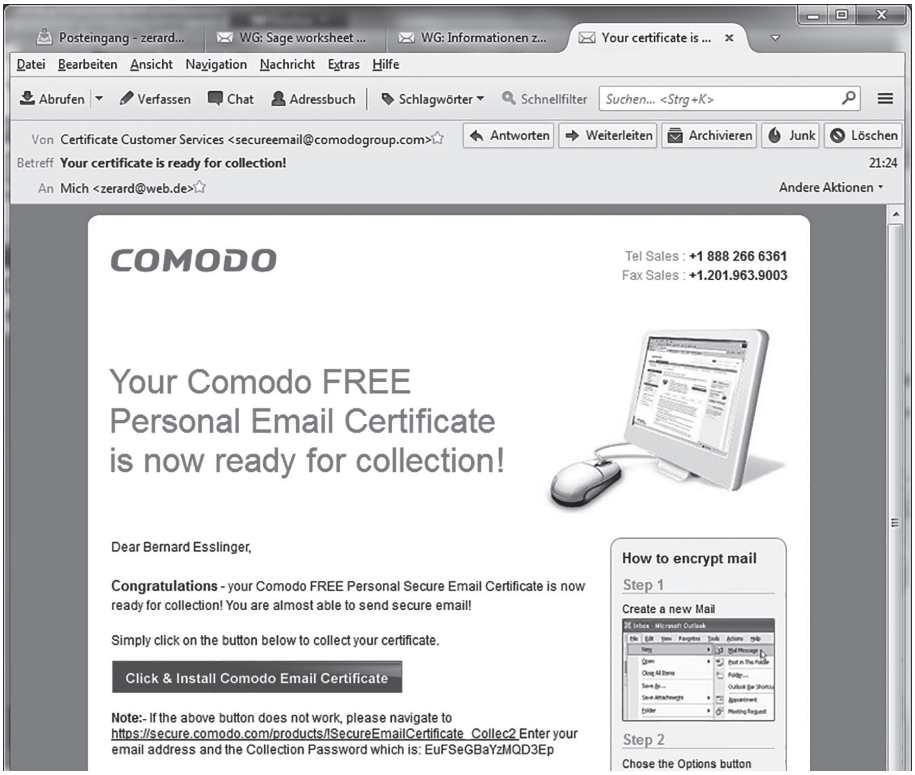


Abb. 7 | Zertifikat wurde in Firefox installiert

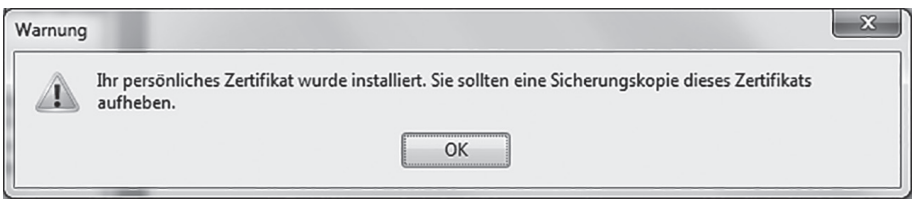


Abb. 8 | Fehlermeldung bei falschem Browser

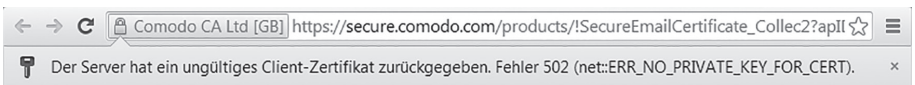
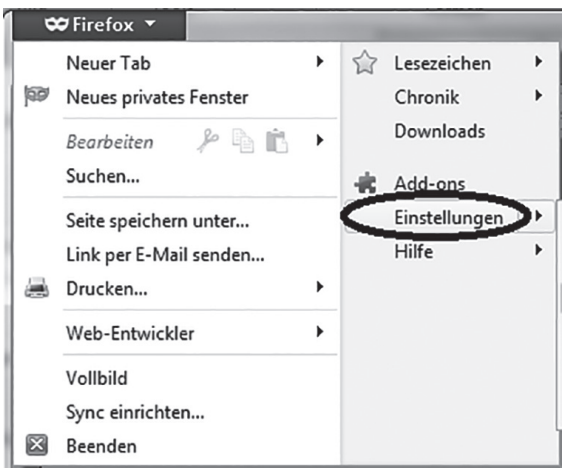


Abb. 9 | Erzeugung der P12-Datei



keinen Newsletter). Außer der Schlüssellänge (‚hochgradig') hat man keine Möglichkeit, irgendwelche Vorgaben zum Verfahren zu machen. Firefox erzeugt ein RSA-2048-Bit-Schlüsselpaar, was gängiger Standard ist.

Man muss nun in seinen (im Zertifikat angegebenen) E-Mail-Account schauen, um auf den Zugangslink zum Zertifikat zu klicken. Damit stellt Comodo sicher, dass der E-Mail-Account auch tatsächlich existiert und der Antragsteller darauf Zugriff hat. Erstaunlicherweise ist die Mail von Comodo nicht signiert… Comodo nennt den zweiten Teilschritt auf seiner Webseite „Collect and install your certificate". Dazu muss man auf der im E-Mail-Client angezeigten HTML-Seite auf den Button „Click & Install Comodo E-Mail Certificate" klicken (Abb. 6).

Abb. 7 zeigt die Erfolgsmeldung, dass das Zertifikat im Firefox-Keystore liegt.

Erstaunlicherweise ist die Erfolgsmeldung mit „Warnung" überschrieben. Achtung: Klickt man im E-Mail-Client auf den Button und ist Firefox nicht als Default-Browser eingestellt, funktioniert die Installation nicht, denn ein anderer Browser kann mit dem Zertifikat nichts anfangen, da er nicht das zugehörige Schlüsselpaar kennt und auch nicht auf den Mozilla-Keystore zugreifen kann. Die Meldung, die z. B. Chrome in diesem Fall anzeigt, ist ziemlich unverständlich (Abb. 8).

Ähnliches passiert auch, wenn man den Firefox-Browser schließt, bevor man das Zertifikat importiert – dann muss man den Prozess wiederholen.

In Thunderbird sieht man das von z. B. Comodo ausgestellte Zertifikat noch nicht, da es bisher nur im Firefox-Keystore abgespeichert ist. Das Mozilla-Konzept ist, dass man alle Infos eigenständig unter der jeweiligen Installation (Firefox und Thunderbird) vorfindet, denn Firefox und Thunderbird basieren zwar auf dem gleichen Codebaum, sind aber jeweils eigenständige Produkte.

Um das Schlüsselpaar samt Zertifikat vom Firefox-Keystore zum Thunderbird-Keystore zu transportieren, muss man eine Datei im Passwort-geschützten P12-Format erzeugen. Dazu werden mit Firefox das Zertifikat und der private Schlüssel in eine P12-Datei exportiert (Abb. 9).

Anschließend muss man im Dialog „Einstellungen", Ikone „Erweitert", Reiter „Verschlüsselung" auf den Button „Zertifikate anzeigen" klicken, dann im Firefox-Fenster im Tab „Ihre Zertifikate" das Comodo-Zertifikat auswählen (Zeile wird blau), auf den Button „Sichern" klicken (Abb. 10) und die P12-Datei – mit ei-

Abb. 10 | Sichern des Zertifikats in Firefox

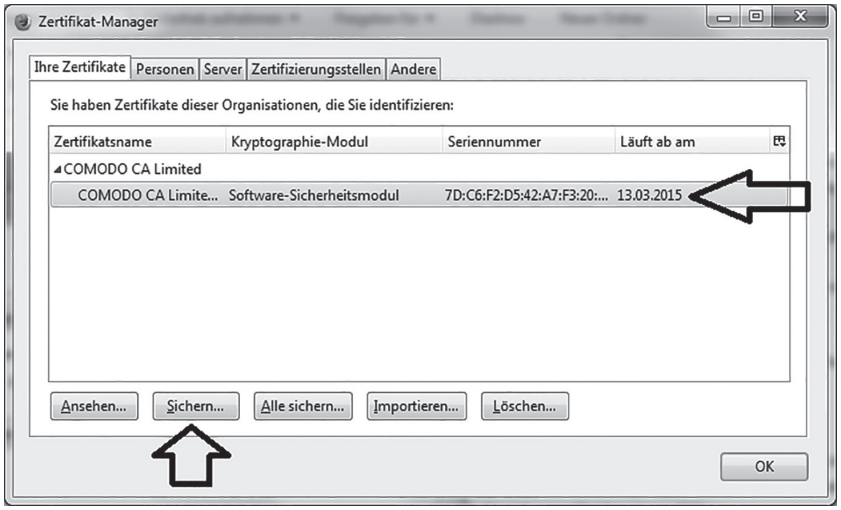
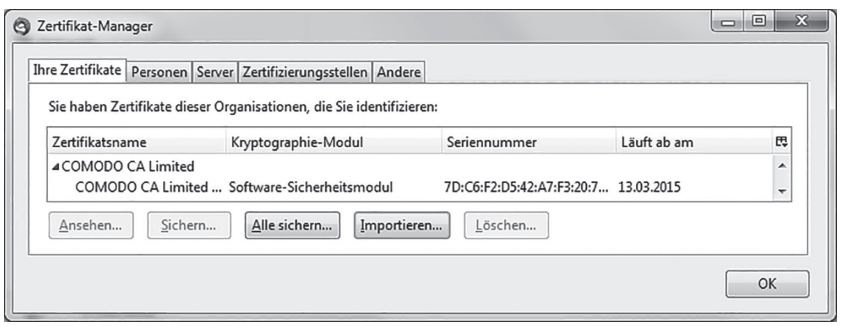


Abb. 11 | Zertifikats-Backup

Abb. 12 | Zertifikat-Manager in Thunderbird



nem guten Passwort geschützt – an einem geeigneten Ort abspeichern (Abb. 11).

Nun hat man also in Firefox erfolgreich sein Schlüsselpaar erzeugt, ein Zertifikat bei Comodo für seine E-Mail-Adresse beantragt, alles in den Firefox-Keystore abgelegt und das Zertifikat samt den Schlüsseln als P12-Datei abgespeichert. Etwas vereinfacht: Ihr privater Schlüssel und Ihr Zertifikat befinden sich nun in der P12-Datei. Diese kann nun in den Thunderbird-Keystore importiert werden.

Schritt 3: Installiere das Benutzer-Zertifikat in Thunderbird

Während sich Schritt 2 nur in dem Browser Firefox abspielte, findet Schritt 3 komplett im E-Mail-Client Thunderbird statt. Auch Schritt 3 besteht wiederum aus zwei Teilschritten: Dem Installieren des Zertifikats in Thunderbird und der Konfiguration des E-Mail-Accounts zur Verwendung des Zertifikats.

Zuerst muss das Zertifikat aus der mit Firefox in Schritt 2 erzeugten P12-Datei geladen werden: Hier ist – wie in Schritt 1 – das Menü „Extras“ zu öffnen. In dem folgenden Dialog „Einstellungen“, Ikone „Erweitert“, Reiter „Zertifikate“ muss man auf den Button „Zertifikate“ klicken.

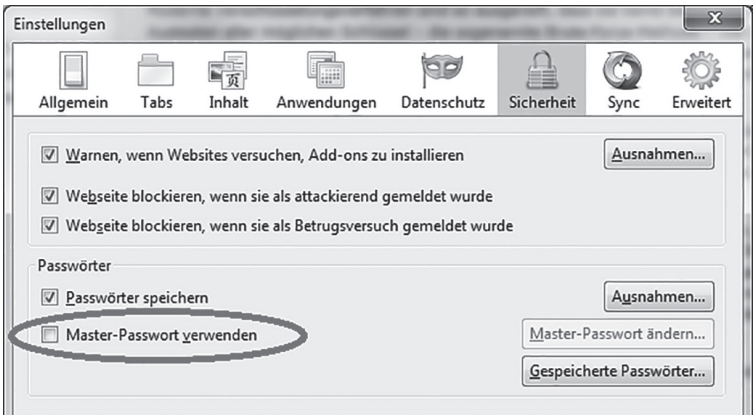
Im darauffolgenden Dialog „Zertifikat-Manager“ kann man dann im Tab „Ihre Zertifikate“ unten den Button „Importieren“ klicken. Zum Importieren müssen Sie zuerst die P12-Datei im Dateisystem auswählen und dann zum Öffnen das Passwort der P12-Datei eingeben. Nach dem erfolgreichen Import zeigt der Thunderbird-Zertifikat-Manager das Commodo-Zertifikat an (Abb. 12).

Details des Zertifikats kann man sich im Zertifikat-Manager (eine Maske, die sowohl von Firefox wie von Thunderbird verwendet wird) ansehen: Aussteller ist Comodo, Ihre E-Mail-Adresse im Zertifikat finden Sie unter „Inhaber“.

Ein Hinweis noch zur P12-Datei. Der private Schlüssel liegt jetzt an drei Stellen vor: im Firefox-Keystore, als P12-Datei und im Thunderbird-Keystore. Nur die P12-Datei ist mit einem Passwort gesichert. Technisch benötigt werden das E-Mail-Zertifikat und der zugehörige private Schlüssel nur im Thunderbird-Keystore, so dass man die beiden anderen entfernen kann (Minimal-Exposure-Prinzip). Die P12-Datei sollte man als Backup auf ein ‚sicheres' Offline-Medium kopieren (kein Internet-Zugang). In Firefox sollte man dann das Zertifikat und den zugehörigen privaten Schlüssel unbedingt löschen (alternativ kann man auch ein Master-Passwort für den Firefox-Keystore vereinbaren).

Standardmäßig ist Firefox so konfiguriert, dass jeder, der physisch Zugang zu Ihrem Rechner hat und Firefox starten kann, und jedes Malware-Programm, das Firefox steuern kann, Zugriff auf den Firefox-Keystore hat und daraus Ihre Schlüssel mit Hilfe des Firefox-Zertifikat-Managers exportieren („sichern“) kann. Dass Firefox hier nach dem Generieren von privaten Schlüsseln weder eine Warnung bringt noch gleich auf die vorhandene Möglichkeit verweist, die privaten Schlüssel im Firefox-Keystore per Master-Passwort zu sichern, ist nicht nur ein Sicherheitsproblem, sondern ebenso mangelnde Qualität bei der Implementierung von Sicherheitsfeatures und ein Verstoß gegen Usability-Regeln. Die folgenden Screenshots zeigen – als Alterna-

Abb. 13 | Master-Passwort in Firefox setzen



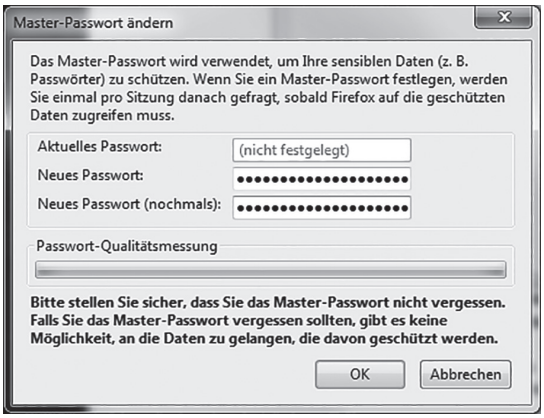


Abb. 14 | Master-Passwort in Thunderbird setzen

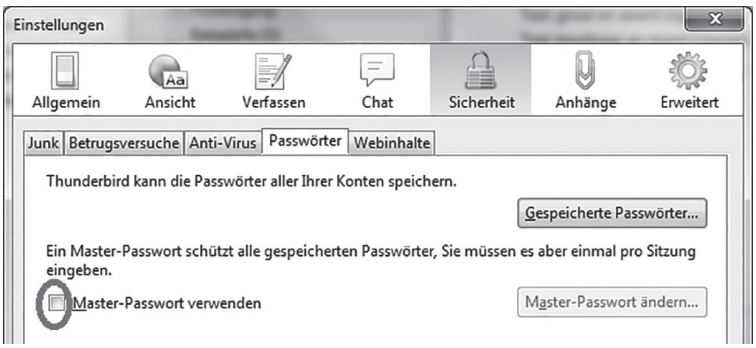
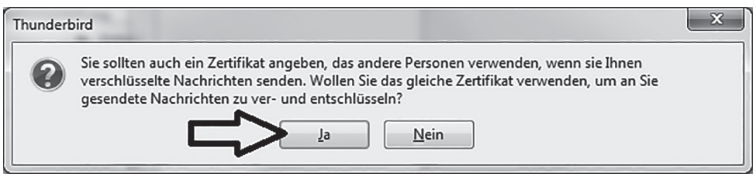
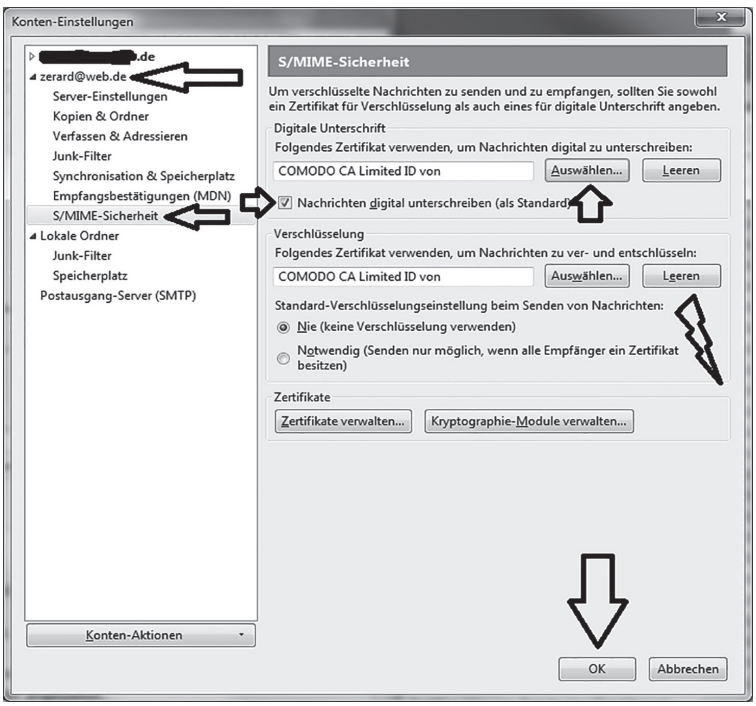


Abb. 15 | Nutzung des Zertifikats konfigurieren





tive zum Löschen – wie man das Masterpasswort setzt: In Firefox im Dialog „Einstellungen", Ikone „Sicherheit", einen Haken setzen bei „Master-Passwort verwenden" (Abb. 13).

Offenbar verlangt Firefox nur dann von sich aus ein Master-Passwort, wenn man Web-Passwörter (also die auf manchen Webseiten verlangten Passwörter) benutzt. Wenn man ein Master-Passwort setzt, ist der Firefox-Keystore verschlüsselt. Darin liegen die Zertifikate, evtl. generierte private Schlüssel und Web-Passwörter.[10] Es ist ein Fehler, generierte Keys nicht für mindestens so sensibel zu erachten wie Webseiten-Passwörter. Auch für den Thunderbird-Keystore ist es dringend zu empfehlen, ein Master Passwort zu setzen (Abb. 14).

Als zweiter Teilschritt von Schritt 3 muss in Thunderbird der E-Mail-Account noch für das installierte Zertifikat konfiguriert werden, da es nicht automatisch für E-Mails verwendet wird. Dazu ist im Menü „Extras"der Dialog „Konten-Einstellungen" zu wählen (Abb. 15). Dort ist dann der eigene E-Mail-Account und darunter (unter „S/MIME-Sicherheit") das eigene Zertifikat auszuwählen – sowohl für Signieren (Haken setzen, dann werden ausgehende Mails immer signiert) als auch für Verschlüsseln. Setzt man den Radiobutton auf „Nie", muss man beim Senden im Menü explizit „Verschlüsseln" auswählen, wenn man verschlüsseln will. Da dies umständlich ist, findet sich hier ein Blitz-Symbol im Screenshot. Das Plugin „Encrypt-if-possible" (siehe den optionalen Schritt 5) richtet es so ein, wie es sein soll: Weder „nie" noch „immer" verschlüsseln, sondern immer dann, wenn man von allen Empfängern ein Zertifikat hat. Dies ist eine absolute Muss-Funktionalität für Einsteiger.

10 Unter Windows werden die Schlüssel und Passwörter im Verzeichnis C:\Users\USERPROFILE\AppData\Roaming\Mozilla\Firefox\Profiles\PROFILENAME in den drei folgenden Dateien gespeichert: key3.db, signons.sqlite und cert8.db. Siehe https://support.mozilla.org/de/kb/Wiederherstellen-wichtiger-Daten-aus-einem-alten-Profil und http://kb.mozillazine.org/Master_password.

Abb. 16 | Signierte E-Mail verfassen

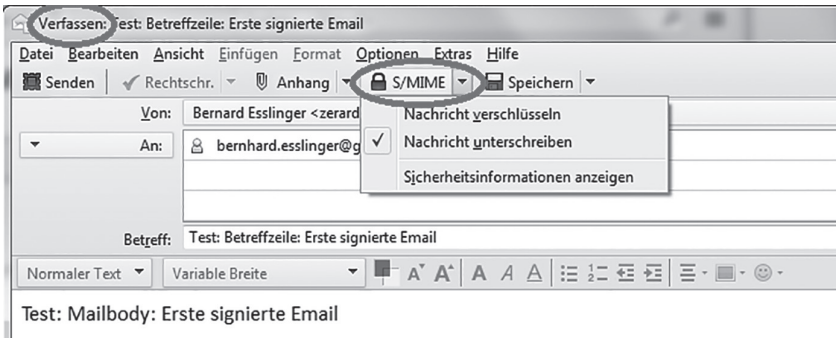


Abb. 17 | Statusabfrage vor E-Mail-Versand

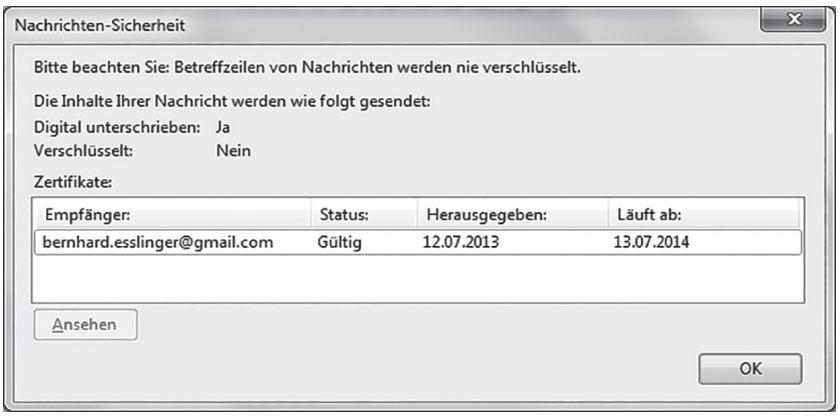


Abb. 18 | Icons einer verschlüsselten & signierten E-Mail

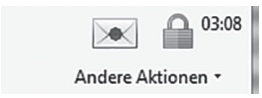
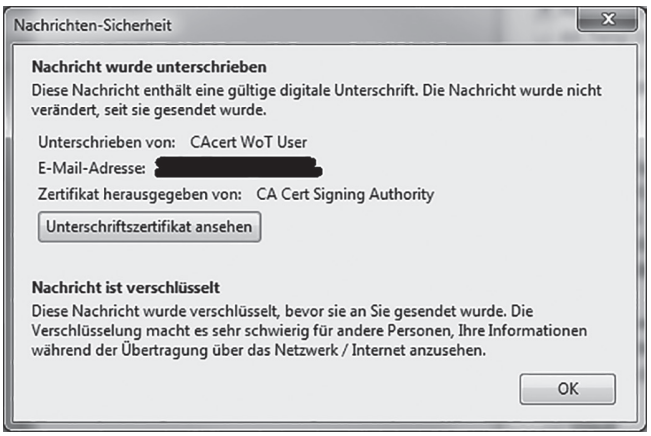


Abb. 19 | Status der empfangenen Nachricht



Schritt 4: Sende eine signierte E-Mail mit Thunderbird

Nun ist die Einrichtungsphase vorbei und wir können die erste signierte E-Mail versenden. Der Empfänger kann dann darauf sofort verschlüsselt antworten. Dazu muss man im Thunderbird-Hauptfenster auf „Verfassen" drücken – entweder oben in der Funktionen-Symbolleiste oder im Konto-Fenster.[11] Im Verfassen-Fenster ist unter dem S/MIME-Button bei „Nachricht unterschreiben" schon ein Haken gesetzt (Abb. 16).

Den Status der Nachricht und des Empfängerzertifikats kann man sich *vor* dem Senden durch einen Klick auf den dritten Eintrag unter S/MIME sehen (Abb. 17).

Hat man selbst ein Zertifikat, kann man seine eigenen Nachrichten immer signieren (egal, ob der Sender ein Zertifikat hat oder nicht).[12] Der Empfänger erhält mit der signierten E-Mail zugleich auch das E-Mail-Zertifikat des Absenders – was einen einfachen Austausch der Zertifikate bewirkt, denn das Zertifikat aus einer empfangenen E-Mail wird automatisch im Thunderbird-Keystore aufgenommen.

In beide Richtungen kann man allerdings erst dann verschlüsseln und signieren, wenn alle Kommunikationsteilnehmer (Sender und Empfänger) ein Zertifikat haben und diese untereinander ausgetauscht sind.

Was gewinnt man nun damit, dass beide Seiten sichere E-Mail verwenden? Erstens werden die E-Mails Ende-zu-Ende-verschlüsselt übertragen. Und zweitens liegen die E-Mails auch lokal verschlüsselt vor, bis man Thunderbird seinen privaten Schlüssel zugänglich macht.

Hat man eine E-Mail erhalten, die verschlüsselt und signiert ist, zeigt Thunderbird zwei Ikonen (Buttons) an (Abb. 18).

Beim Klicken auf eine der beiden Ikonen sieht man die Dialogbox aus Abb. 19.

Schritt 5 (optional): Installation der Erweiterung „Encrypt-if-possible"

Es empfiehlt sich, die Erweiterung „Encrypt-if-possible" in Thunderbird zu installieren, damit Thunderbird immer verschlüsselt, wenn man von allen in der Mail aufgeführten Empfängern ein gültiges E-Mail-Zertifikat hat.[13] Erweiterungen werden in Thunderbird über das Menü „Extras", „Add-ons", „Add-ons suchen" installiert (Abb. 20).

Aufnehmen eines CA-Zertifikats in den Thunderbird-Keystore

Wenn man eine Nachricht empfängt, die eine „ungültige" Signatur aufweist, bedeutet dies meist nicht, dass die Signatur nicht korrekt ist, sondern dass Thunderbird der ausstellenden Zertifizierungsstelle (CA) nicht vertraut, weil deren Zertifikat nicht im Thunderbird-Keystore enthalten ist. Dann muss man explizit einer solchen CA das Vertrauen aussprechen.[14]

Das Vertrauen selbst aussprechen ist im Thunderbird-Zertifikat-Manager unter dem Reiter „Personen" möglich, indem man

11 http://www.thunderbird-mail.de/wiki/Erste_Schritte_mit_Thunderbird

12 Der Menüeintrag unter „S/MIME" lautet: „Nachricht unterschreiben". Klarer wäre die Verwendung des Wortes „signieren": „Nachricht unterschreiben / signieren".

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

14 Bei Comodo-Zertifikaten passiert das nicht, weil das CA-Zertifikat von Comodo „ab Werk" im Thunderbird-Keystore enthalten ist.

Abb. 20 | Installation des Add-ons „Encrypt-if-possible"

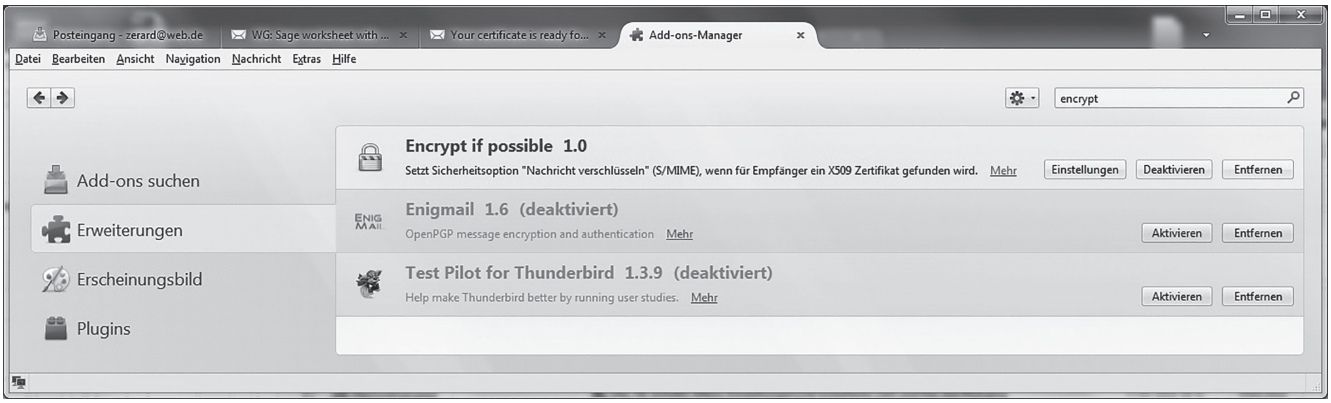
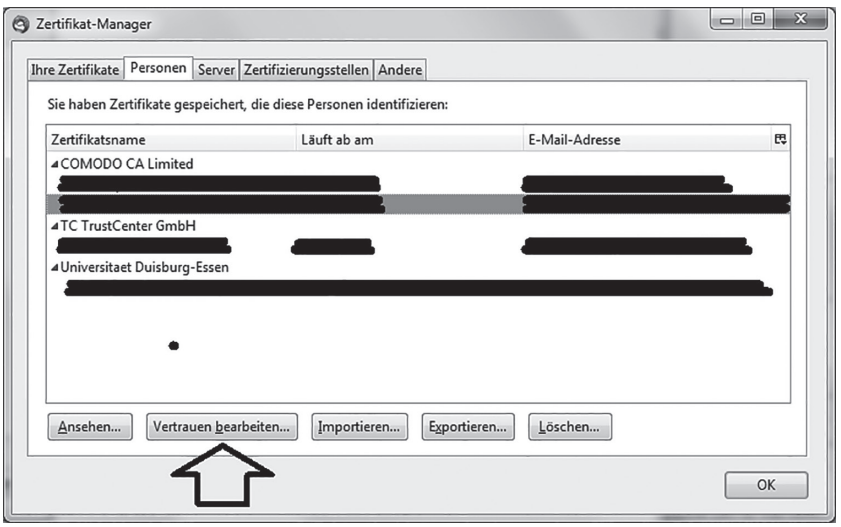


Abb. 21 | Empfänger-Zertifikate im Zertifikat-Manager



nach dem Empfangen der E-Mail das Zertifikat des Senders markiert und auf den Button „Vertrauen bearbeiten" klickt. Anschließend kann man an diesen Empfänger verschlüsselte E-Mails schicken (Abb. 21).

Da in einem S/MIME-Zertifikat normalerweise die gesamte Zertifikatskette bis zum CA- oder Root-Zertifikat enthalten ist, können daraus die übergeordneten Zertifikate entnommen, manuell importiert und diesen dann – nach einer Überprüfung des Hashwerts – das Vertrauen ausgesprochen werden.

Achtung (vgl. Kasten): Thunderbird importiert aus signierten empfangenen E-Mails Benutzer-Zertifikate nur dann automatisch, wenn das Aussteller-(CA-)Zertifikat schon im Keystore vorliegt. Ist ein Zertifikat nicht als ‚vertrauenswürdig' erklärt, lässt Thunderbird es nicht zu, es zu benutzen – man kann also z.B. nicht verschlüsselt auf eine erhaltene signierte E-Mail antworten. Auch das Abspeichern und manuelle Importieren geht nicht (Fehlermeldung: "*Certificate can't be verified and will not be imported. Certificate issuer might be unknown or untrusted….*"). Man muss – sehr umständlich – das E-Mail-Zertifikat des Senders öffnen und unter dem Reiter „Zertifikatskette" das ROOT-CA-Zertifikat in eine Datei exportieren und es danach in Thunderbird unter „Zertifizierungsstellen" importieren und zumindest das Vertrauenslevel „*Trust this CA to identify E-Mail users*" auswählen. Erst danach speichert Thunderbird das E-Mail-Zertifikat des Senders unter „Personen" automatisch, wenn man die signierte E-Mail erneut öffnet.[15]

Also: Ist das Aussteller-(CA-)Zertifikat (noch) nicht im Thunderbird-Keystore, muss man es erst importieren, und anschließend, separat, das Zertifikat des Senders. Deshalb empfiehlt es sich, verbreitete CA-Zertifikate, die nicht im Keystore sind (wie z. B. das von CAcert (www.cacert.org)), vorsorglich in den Keystore aufzunehmen.

Was man sonst noch wissen sollte

- Verschlüsselt werden der E-Mail-Inhalt (*Body*) und eventuelle Anhänge, nicht aber die Titelzeile (das Betreff bzw. Subject).
- Auch abgelaufene eigene Zertifikate (und die zugehörigen privaten Schlüssel) muss man aufheben, sonst hat man keine Chance mehr, seine eigenen, alten, verschlüsselten E-Mails zu lesen.
- Wenn der Kommunikationspartner einem eine signierte E-Mail mit einem neuen Zertifikat schickt (weil sein altes abgelaufen ist oder weil er es sperren ließ), nimmt Thunderbird automatisch für diese Person das neue Zertifikat. Gut daran ist, dass man nichts dazu tun muss; unbefriedigend ist, dass Thunderbird nicht durch eine Meldung informiert, dass das Zertifikat ausgetauscht wurde.
- Wenn Ihr Zertifikat abläuft, müssen Sie sich ein neues ausstellen lassen. Das funktioniert genauso wie beim ersten Mal.
- Bei CAcert kann man als authentisierter User nicht nur für sich, sondern auch für andere kostenlose Zertifikate ausstellen.

Literatur

[1] Wikipedia: S/MIME. http://de.wikipedia.org/wiki/S/MIME
[2] Wikipedia: OpenPGP. http://de.wikipedia.org/wiki/OpenPGP
[3] Stiftung Warentest, März 2014: „Sichere Post -- E-Mail-Verschlüsselung", S. 56-59
[4] http://www.anti-prism-party.de/cms/downloads/sichere%20E-Mail%20am%20pc%20und%20mit%20dem%20smartphone-anleitung.zip; und darin speziell das Dokument: Schritt-für-Schritt-Anleitung_Sichere E-Mail mit SMIME und Thunderbird unter Windows, MAC und Linux_v1.1.0.pdf

15 Das ist eine schlechte Usability von Thunderbird; Outlook ist an dieser Stelle eingängiger.

Appell zur Förderung eines umfassenden Projektes „Benutzerfreundliche sichere E-Mail"

Sichere E-Mail funktioniert technisch, hat sich aber nicht verbreitet. Hauptgrund ist, dass die Einstiegshürden (sowohl bei OpenPGP wie bei S/MIME) zu hoch sind und dass die Bedienung zu wenig benutzerfreundlich ist. Ansätze und Aufrufe, das zu verbessern, gibt es viele. Leider sind all diese Ansätze – auch in Deutschland – stecken geblieben (z. B. CryptoBird, Mynigmail, IDB-Encryption). Zu viele Miniprojekte, keine Nachhaltigkeit, keine akzeptierten Produkte.

Wir halten eine konkrete Förderung eines Projektes mit klaren Prioritäten für wichtig – nicht jeder Ansatz und jede „Excellenzeinrichtung" sollte „ein wenig" gefördert werden. Das Gesamt-Projekt sollte in mehreren Schritten ablaufen:

- **Schritt 1 (Verbesserung des Bisherigen)**: Thunderbird und die entsprechenden Open-Source-Plugins benutzerfreundlich machen, und eine in Deutschland ansässige CA etablieren, die kostenlose Zertifikate ausstellt (sie muss unter einer schon in den Browsern vorhandenen CA stehen).
- **Schritt 2 (Neue Cloud-basierte Ansätze marktreif machen)**: Hier sollte E-Mail mit SMS und Chat verbunden sein und auch auf Smartphones laufen. Grundlage dafür sind Projekte wie TextSecure[1] oder die neue sehr sichere Kommunikationsplattform vom Prof. Roth.[2]

Hiermit ergeht also ein Appell an die federführenden Ministerien der „Digitalen Agenda", ein solches Projekt zu finanzieren. Die „Digitale Agenda 2014-2017" wurde von den drei Bundesministerien für Wirtschaft, Inneres sowie Verkehr und Internet auf der CeBIT 2014 vorgestellt.

Auch Stiftungen könnten diese Finanzierung für ein Open-Source-Projekt leisten, damit allen (sowohl den Endnutzern als auch der Wirtschaft) sichere E-Mail in einer benutzerfreundlichen Form zur Verfügung steht und weiterentwickelt wird. Erforderlich sind konkrete gemeinsame Planungen mit einem ausreichenden Budget. Die Anforderungen und die technische Machbarkeit wurden vom Autor und mehreren Kollegen schon evaluiert.

1 https://whispersystems.org
2 http://www.volkerroth.com/proj-secure-mail.html

Usability-Probleme

S/MIME funktioniert technisch gut und lässt sich in vier Schritten schnell einrichten, aber es ergeben sich etliche Usability- und Interoperabilitäts-Probleme – sowohl generell bei S/MIME als auch speziell mit Thunderbird. Dazu zählen insbesondere:

- Leitet man von Outlook empfangene E-Mails mit Thunderbird weiter, so wird der Inhalt aus dem E-Mail-Körper entnommen und zusammen mit den Anhängen als p7m-Datei angehängt.
- Der ebenfalls verbreitete E-Mail-Client „TheBat!" (z.B. in Version 6.2.14) komprimiert standardmäßig vor der Verschlüsselung (nach RFC-3274) – was eigentlich gut ist. Leider hat diese Option noch eine andere Funktion (für die es eine extra Option geben sollte): Die Signatur wird als eigenständiger E-Mail-Teil dazu gepackt. Wenn ein Benutzer mit TheBat! an einen Benutzer mit Thunderbird eine signierte und verschlüsselte E-Mail sendet, zeigt Thunderbird einen leeren E-Mail-Körper an, meldet aber, dass die Signatur in Ordnung ist. In umgekehrter Richtung funktioniert es allerdings korrekt.
- Im E-Mail-Körper eingefügte Screenshots werden beim Versenden aus dem Text herausgenommen und als PNG-Datei angehängt – mit seltsamen Namen (wie aigajeef.png). Sie sollten zumindest in der richtigen Reihenfolge durchnummeriert werden (mit einer Referenz im Text).
- Sind Screenshots in einer E-Mail enthalten und man antwortet auf diese Mail, kann Thunderbird endlos eine ‚Anhängen'-Messagebox zeigen. Dann muss man die verstümmelten Reste alter Bilder in der alten E-Mail löschen.
- Die Volltextsuche ist bei verschlüsselten Mails eingeschränkt: Über die Header- und Sender-/Empfangsinformationen kann man weiterhin suchen, aber nicht über den E-Mail-Inhalt.
- Wenn man noch keinen Empfänger eingegeben hat, kommt die Meldung, „Es sind nicht für alle Empfänger Zertifikate vorhanden." Die Meldung ist überflüssig und sie erweckt den falschen Eindruck, als ob die Verschlüsselung nicht möglich wäre.
- Beim Antworten auf eine verschlüsselte E-Mail wird nicht automatisch signiert.
- Statt von Hand Schlüsselpaar und Zertifikat per P12-Datei vom Firefox-Keystore zum Thunderbird-Keystore zu transportieren, sollten die S/MIME-Funktionen der Mozilla-Produkte den normalen Benutzer so unterstützen, dass dieser Zwischenschritt über die P12-Datei nicht mehr notwendig ist.
- Die Zertifikate, denen man das Vertrauen selbst aussprach, werden von Thunderbird im Keystore nicht extra gekennzeichnet.
- Die Meldung „Ungültige Signatur" kann sehr irreführend sein. Es wird nicht unterschieden zwischen den möglichen Gründen: a) Das Aussteller-Zertifikat ist unbekannt, die Signatur aber technisch korrekt, und b) Das Aussteller-Zertifikat ist bekannt, die Signatur hat technisch aber einen falschen Wert (d. h. die E-Mail wurde zwischen dem Versenden und dem Empfang geändert). Fall a) tritt auch bei den Bürger-CERT-E-Mails des BSI so.[1] Wie man das CERT-Bund-Zertifikat oder Zertifikate anderer CAs direkt importiert (weil man es vorsorglich so machen will, oder weil das CA-Zertifikat nicht in der E-Mail-Signatur enthalten ist), ist ausführlich beschrieben im 3. Szenario im Anhang B von [4].
- Wenn man in Thunderbird sowohl OpenPGP (per Gpg4win und Enigmail) als auch S/MIME installiert, funktioniert das leidlich. Probleme ergeben sich jedoch z. B. dadurch, dass sich die Ikonen unten (ob Signieren oder Verschlüsseln aktiv ist) unterschiedlich verhalten, dass die Menüs unterschiedlich sind, dass Begriffe unterschiedlich benutzt werden und dass Einstellungen in Thunderbird (wie HTML-Mail verbieten) nur ‚immer' oder ‚nie' gelten.
- Setzt man den Haken nur auf „Verschlüsseln" (und nicht auch auf „Signieren"), kann der Sender die Mail später bei S/MIME noch lesen, bei OpenPGP nicht mehr. Ein bei OpenPGP nicht gesetzter Signieren-Haken sollte nicht bewirken, dass nicht auch noch an einen selbst verschlüsselt wird.

1 http://www.heise.de/newsticker/meldung/Sicherheitswarnung-zur-Signatur-von-Buerger-CERT-Mails-2145053.html (Meldung vom 14.3.2014)

Kritik an S/MIME aus Sicht von OpenPGP

Wie sehr kann man zentralen Instanzen (CAs) vertrauen?[1]

OpenPGP ist mit dem Web-of-Trust unabhängiger aufgestellt, da hier jeder Teilnehmer eine „CA" darstellt und so etwas wie eine dezentralisierte PKI aufgebaut wird. Jeder kann einen Schlüssel (Public Key) signieren und damit die Identität bestätigen. Je mehr dies tun, desto glaubwürdiger ist ein öffentlicher Schlüssel.

Das Vertrauensmodell bei S/MIME kennt nur zwei Stufen: volles Vertrauen oder kein Vertrauen. OpenPGP erlaubt mehrere Stufen. Wobei gerade dies aus Usability-Perspektive wieder kontraproduktiv sein kann.

Ein persönliches S/MIME-Zertifikat verifiziert den Nutzer *nur* anhand der E-Mail-Adresse. Wie zuverlässig und vollständig aber werden die Daten von der CA geprüft?

S/MIME kann ausschließlich im E-Mail-Client benutzt werden. Mit OpenPGP kann z. B. auch einen Anhang verschlüsseln und diesen Anhang dann auch außerhalb des E-Mail-Clients austauschen und entschlüsseln.

1 http://www.openpgp-schulungen.de/kurzinfo/openpgp-smime/