Client-Zertifikate mit CAcert

Alexander Bahlo

Für das Signieren von E-Mails über S/MIME wird ein von einer Zertifizierungsstelle ausgegebenes Zertifikat benötigt, die meisten sogenannten CAs lassen sich dafür bezahlen. Nicht so CAcert. Dafür ist die Integration in den Client ein klein wenig aufwendiger.

Bewegt man sich im Internet, stößt man auf immer mehr Seiten, mit denen verschlüsselt kommuniziert wird. Solche Seiten mit der Kennung https verschlüsseln die Pakete per SSL. Damit sichergestellt ist, daß man auch mit der richtigen Domain in Kontakt ist und die Daten nicht kompromittiert werden, identifiziert sich der Server mit Zertfikaten beim Client. Aber nicht nur bei Seitenaufrufen im Web, sondern auch bei E-Mails bedient man sich heute immer häufiger der verschlüsselten Datenübertragung. Die Grundlage sind auch hier Zertifikate. Sie sind eine Art Beglaubigung und bestehen aus einem öffentlichen Teil, der verteilt werden darf, und einem privaten Teil, der ausschließlich dem Benutzer und seinen Programmen zugänglich sein darf. Aus Sicherheitsgründen empfiehlt es sich sogar, die privaten Zertifikate ausschließlich paßwortgeschützt abzulegen.

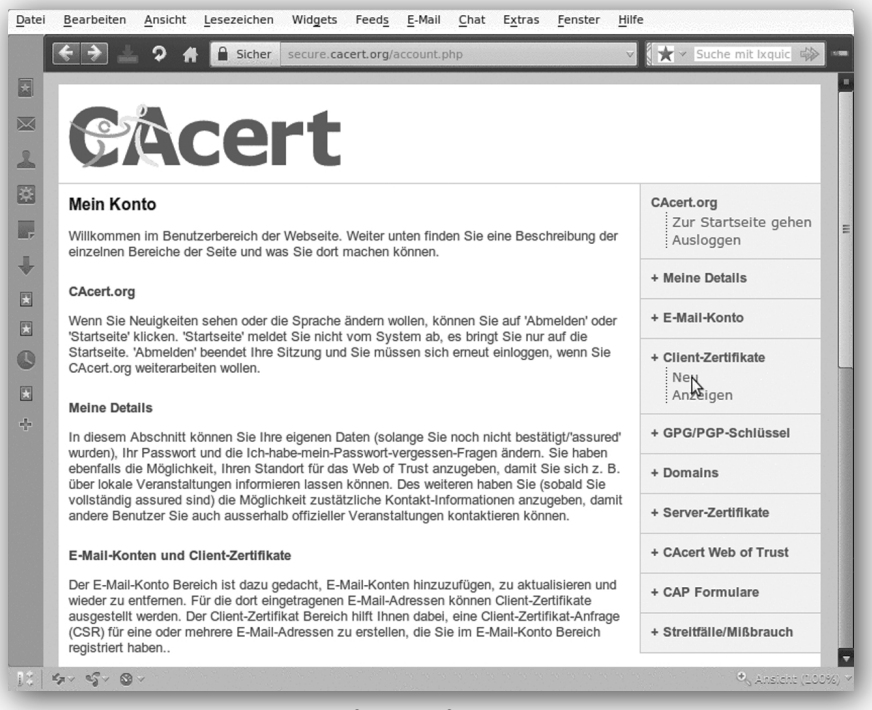

Bild 1: Auswahl des Client-Zertifikats auf der CAcert.org-Website

Die heute gebräuchlichen X.509-Zertifikate sichern die Authentizität, Integrität und Vertraulichkeit und bilden damit die Grundlage interner und externer Kommunikation. Doch in der Praxis scheitert eine unternehmensweite Verbreitung von digitalen Zertifikaten zur Absicherung von Servern und E-Mail-Kommunikation – gerade bei kleinen und mittelständischen Betrieben – aber häufig am begrenzten Budget der IT-Abteilung, denn bei den kommerziellen Zertifizierungsstellen fallen schnell jährliche Bereitstellungskosten von mehreren tausend Euro an, und auch für Privatanwender sind wenige hundert Euro Kosten im Jahr oft nicht tragbar.

Kostenintensiv

Um ohne entsprechende Investitionen eine deutliche Steigerung der Sicherheit der Internetkommunikation zu erreichen, kam im Jahr 2002 der Australier Duane Groth auf die Idee, bei X.509-Zertifikaten die zentralisierte Identitätsprüfung kommerzieller Anbieter durch ein Web of Trust zu ersetzen, wie man es in ähnlicher Form von PGP kennt. Er gründete CAcert als community-basierte, nicht-

kommerzielle Certification Authority (CA). Eine CA stellt Zertifikate an Anwender aus, wobei sie selbst ein Zertifikat besitzt, mit dem sie sich als CA, sozusagen als Wurzel von sicheren Client-Zertifikaten ausweist. Will jemand die Identität eines Dritten überprüfen – beispielsweise ob eine von diesem mit seinem Zertifikat unterschriebene E-Mail authentisch ist –, prüft er das Client-Zertifikat, stellt darüber hinaus fest, daß es von einer bekannten CA unterschrieben ist und kann auf diese Weise die Kette der Beglaubigungen nachvollziehen.

Damit bei CAcert [1] ein Interessent ein solches Zertifikat erhält, muß er sich auf der CAcert-Website [2] mit seiner E-Mail-Adresse und einigen persönlichen Daten wie Name und Geburtsdatum registrieren. Diese Daten werden später für eine Identitätsprüfung im Web of Trust benötigt. Danach erhält der Antragsteller eine zu bestätigende E-Mail, womit die Registrierung vollzogen ist.

Weil der Antragsteller sich für das Erlangen eines Zertifikats nur über eine Website identifizieren zu braucht und der CAcert-CA gegenüber nicht persönlich Dokumente vorlegen muß, enthält das Client-Zertifikat ohne Überprüfung seiner Angaben keinen Namen und ist nur sechs Monate gültig. Aus diesem Grund sollte er seine Identität von mehreren erfahrenen CAcert-Teilnehmern, sogenannten Assurern, in einem realen Vier-Augen-Gespräch anhand seiner Ausweisdokumente (Personalausweis, Reisepaß oder Führerschein) überprüfen lassen. Das Ergebnis dieser Überprüfung wird bei CAcert in Punkten ausgedrückt, die in das CAcert-Konto eingetragen werden. Nach einer erfolgreichen Überprüfung durch Assurer wird eine E-Mail mit dem Betreff »You've been Assured« zugesandt, dem die neue Gesamtpunktzahl auf dem CAcert-Konto zu entnehmen ist. Sobald der Antragsteller mindestens 50 Punkte besitzt, kann er benannte Zertifikate auf seinen Namen erzeugen und sein Zertifikat ist für den Zeitraum von zwei Jahren gültig. Alle E-Mail-Adressen, für die Zertifikate gelten sollen, müssen bei CAcert registriert werden. Eine davon gilt als Hauptadresse, die dem Assurer zur Punktevergabe mitgeteilt werden muß.

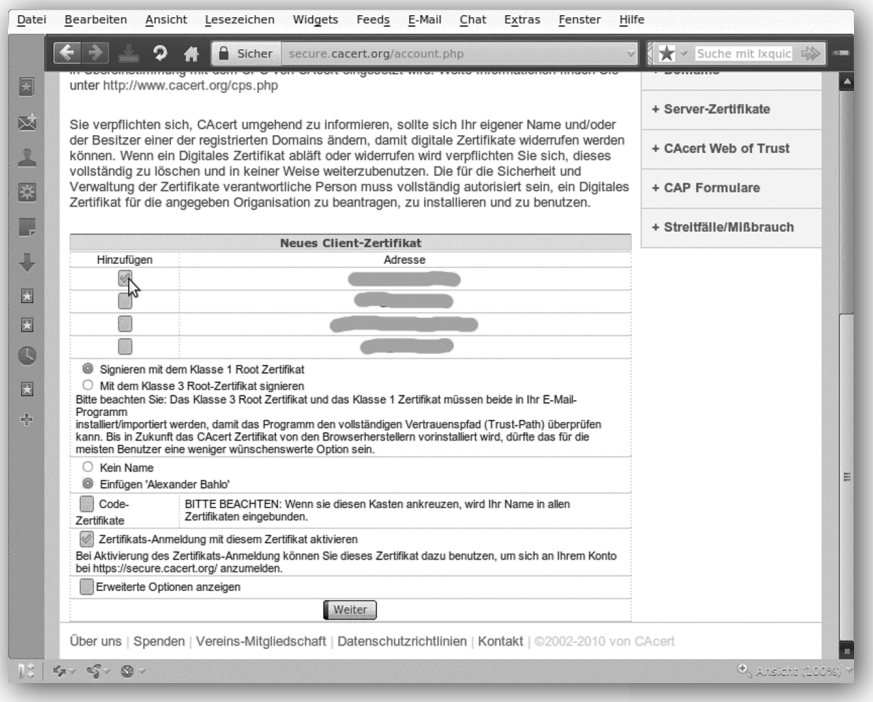

Bild 2: Welche Daten sollen in das Zertifikat aufgenommen werden

Das Web of Trust

Auch wenn ein Client-Zertifikat in der Praxis mehrere E-Mail-Adressen enthalten kann, ist es praktischer, für jede E-Mail-Adresse ein eigenes Client-Zertifikat zu beantragen. Sollte einmal eine E-Mail-Adresse nicht mehr gültig sein, müßte es, wenn sich alle E-Mail-Adressen in einem Zertifikat befinden, als ungültig erklärt werden und ein neues mit den noch übrig gebliebenen E-Mail-Adressen angelegt werden. Bei getrennten Zertifikaten pro Adresse kann das Zertifikat einfach auslaufen und man spart sich viel Arbeit. Auch ist manche Software fehlerhaft und schaut nur nach der ersten Adresse.

Durch die Assurance entsteht bei CAcert das Web of Trust, ein Vertrauensnetzwerk zwischen allen Beteiligten. Stand November 2010 gibt es über 4000 Assurer weltweit. Wo man sich durch Assurer überprüfen lassen kann, ist im CAcert-Portal [3] unter dem Menüpunkt CAcert-Web of Trust oder, im Fall von CAcert-Messebesuchen, direkt auf der Startseite einsehbar.

Um ein X.509-Client-Zertifikat bei CAcert anzulegen, um einfachen und gleichzeitig sicheren Zugang zum Beispiel zu entsprechend gestalteten Websites oder auch zur E-Mail-Signierung zu haben, muß auf dem CAcert-Portal [4] der Menüpunkt *Client-Zertifikate* | *Neu* aufgerufen werden, siehe Bild 1. Hierbei können die E-Mail-Adressen ausgewählt werden, für die das Zertifikat gelten sollen (Bild 2).

Die X.509-Norm

Ein populärer Verschlüsselungsalgorithmus neben GPG/PGP ist X.509. Ein X.509-Zertifikat [8] ist ein Schlüssel, der von einer Certification Authority, wie beispielsweise CAcert oder S-Trust, beglaubigt und unterschrieben ist. Mit einem gültigen Zertifikat übermittelte Daten belegen zunächst, daß die enthaltene Information unverändert übertragen worden ist. Ist im Zertifikat ein Name oder eine E-Mail-Adresse enthalten, gehört es wirklich zur angegebenen Person oder zur angegebenen Adresse. Das Zertifikat ist deshalb mit einem elektronischen Ausweis vergleichbar.

Bild 3: Exportieren des Client-Zertifikats aus dem Web-Browser

Ein Klick auf *Weiter* führt auf ein Fenster, in dem die Länge des erzeugten Schlüssels angegeben werden kann. Voreingestellt ist er auf 2048 Bit, was gemeinhin als ausreichend sicher gilt. Möglich sind Schlüssellängen bis 4096 Bit. Anschließend wird über den Button *Erstellen einer Zertifikatsanfrage (CSR)* das Client-Zertifikat erzeugt und für den Webbrowser direkt zum Import in den Zertifikatspeicher des Browser bereitgestellt. Wird das Zertifikat in einem Mail-Client wie dem Thunderbird benötigt, der keine eigene Download-Möglichkeit vorsieht, muß es auf die lokale Festplatte heruntergeladen und über diesen Umweg in den Mailclient importiert werden.

Aufnahme in den Zertifikatspeicher

Zu finden ist der Zertifikatspeicher in SeaMonkey im *Bearbeiten*-Menü unter *Einstellungen* | *Datenschutz & Sicherheit* | *Zertifikate*, dort verbergen sich hinter der Schaltfläche *Zertifikate verwalten* die Speicher für die Zertifikate. Der Reiter *Ihre Zertifikate* enthält das soeben bezogene persönliche Client-Zertifikat. SeaMonkey-Anwender haben es ab nun sehr einfach, denn es mit der Speicherung im Browser zugleich im Mail-Client verfügbar.

In Mozilla Firefox ist das importierte Zertifikat im *Extras*-Menü unter *Einstellungen* | *Erweitert* auf dem Tab *Verschlüsselung* und hinter der Schaltfläche *Zertifikate anzeigen* | *Ihre Zertifikate* zu finden. Firefox-Anwender müssen nun noch etwas arbeiten und das Zertifikat in Thunderbird oder einen anderen Mail-Client exportieren.

Gleichzeitig versendet CAcert eine E-Mail mit dem Betreff »[CAcert.org] Your certificate« mit weiteren Hinweisen zum Download des Client-Zertifikats sowie zu den CAcert-Root-Zertifikaten und den Fingerprints. Ein Fingerprint bildet eine lesbare, weil halbwegs kurze, Prüfsumme über das Zertifikat. Der in der E-Mail angegebene Fingerprint muß mit dem Root-Zertifikat und dem Class-3-Zertifikat der Zertifizierungsstelle verglichen werden.

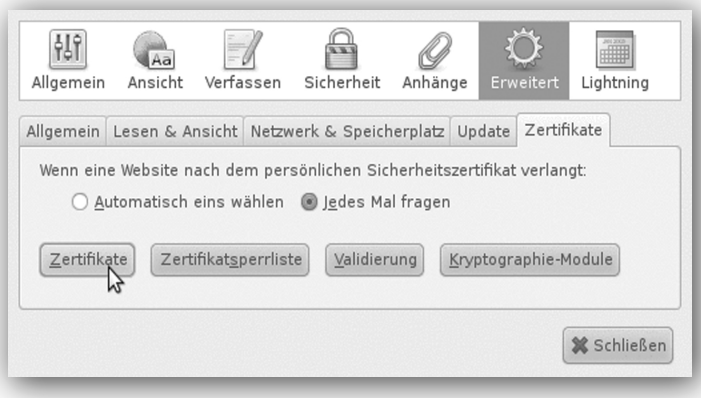

Bild 4: Aufruf des Zertifikat-Managers im Mailprogramm Thunderbird

Um in E-Mail-Programmen wie Mozilla Thunderbird mit dem Client-Zertifikat arbeiten zu können, muß das Zertifikat erst aus dem Browser im sogenannten PKCS#12-Format in eine Datei exportiert werden, wie Bild 3 zeigt. Dazu muß das Zertifikat im Zertifikatspeicher angeklickt und dann die Schaltfläche *Exportieren* (oder *Sichern*) betätigt werden. Dabei wird zusätzlich ein privater, geheimer Teil exportiert, der mit einem Paßwort gesichert werden sollte. Die exportierte Datei darf niemals weitergegeben werden, da sie den privaten Schlüsselteil enthält. Wenn dieser bekannt werden würde, könnten andere Personen die verschlüsselten und somit sicher geglaubten Daten lesen und selbst auch E-Mails signieren, die den Anschein erwecken, als stammten sie von der im Zertifikat angegebenen Person. Nur der öffentliche Schlüssel(teil) darf und soll – zum Beispiel durch das standardmäßige Signieren in E-Mails – weitergegeben werden.

Mit der Eingabe des Paßworts des privaten Schlüssels kann das E-Mail-Programm die Nachricht signieren und bei Bedarf verschlüsseln – letzteres ist nur möglich, wenn der öffentliche Schlüssel des Empfängers bekannt ist. Der Empfänger prüft dann die Unterschrift mit dem öffentlichen Schlüssel des Unterzeichners und entschlüsselt die Nachricht mit seinem eigenen geheimen Schlüssel. Um die Automatik mit privatem und öffentlichem Schlüssel kümmert sich in der Regel das E-Mail-Programm. Es fragt auch selbständig nach dem Paßwort für den privaten Schlüssel, um eine empfangene E-Mail zu dekodieren.

Die aus dem Browser exportierte Datei kann nun in den Zertifikat-Manager von Thunderbird, Evolution, Claws-Mail, Outlook und vielen weiteren

Mailprogrammen, die mit Zertifikaten umgehen können, importiert werden. In diesen Mail-Clients (mit Ausnahme von Claws-Mail) ist das Verschlüsselungsprotokoll S/MIME, das die Verschlüsselung über Zertifikate steuert, bereits enthalten, es muß nichts extra nachinstalliert werden.

Für den Import in beispielsweise Mozilla Thunderbird muß wieder der bereits bekannte Zertifikatspeicher geöffnet werden, er befindet sich im *Bearbeiten*-Menü im Punkt *Mail- und Newsgroup-Account-Einstellungen*, dort unter *[Name des E-Mail-Accounts] | Sicherheit* hinter der Schaltfläche *Zertifikate verwalten*. Hier muß der Reiter *Ihre Zertifikate* angeklickt werden, darauf die Schaltfläche *Importieren*. Im folgenden Dateiauswahldialog werden die auf der Festplatte befindlichen Dateien des Typs PKCS 12 angezeigt, es muß die richtige geöffnet werden. Nach einer Paßwortabfrage befindet sich das Zertifikat in der Liste von *Ihre Zertifikate* und ist fast betriebsbereit.

Jetzt muß noch in den Benutzerkonto-Einstellungen des jeweiligen Mail-Clients (in SeaMonkey im *Bearbeiten*-Menü unter *Mail- und Newsgroup-Account-Einstellungen*, dort unter *[Name des E-Mail-Accounts] | Sicherheit*; in Thunderbird im *Extras*-Menü im Punkt *Konten-Einstellungen | S/MIME-Sicherheit*) in der rechten Spalte jeweils das Zertifikat ausgewählt werden, mit dem digital unterschrieben und verschlüsselt werden soll, siehe Bild 6. Allerdings sollte das Konto nicht mehr »Identitäten« (im Sinne von Mozilla) aufweisen, als im Zertifikat vorhanden, weil es sonst passieren kann, daß plötzlich hier gar nichts mehr auswählbar ist.

Root-CA importieren

Soll eine E-Mail signiert oder verschlüsselt werden, muß im E-Mail-Programm des Verfassers das Root-Zertifikat der zertifikat-ausstellenden Stelle gespeichert sein. Ist auf seinem Client nicht das CA-Zertifikat seines Zertifikats installiert, gelingen die Verschlüsselung und das Unterschreiben nicht. Es erscheint die Fehlermeldung

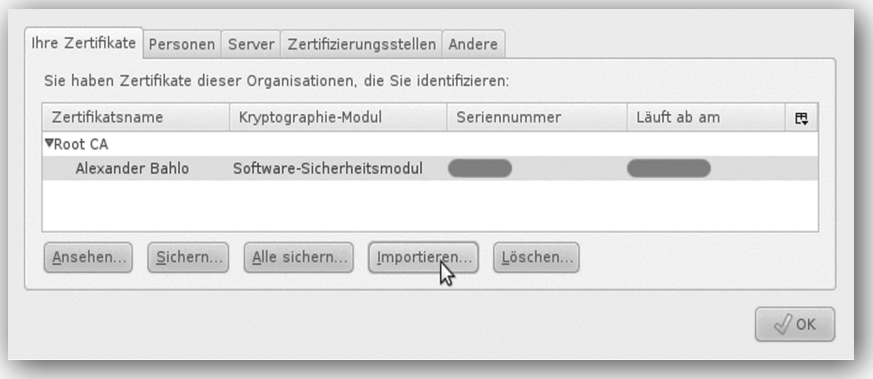

Bild 5: Importieren des Client-Zertifikats in Thunderbird

»Senden der Nachricht fehlgeschlagen. Kann Nachricht nicht signieren. Bitte überprüfen Sie, ob die Zertifikate, die für dieses Konto in den Konten-Einstellungen angegeben sind, gültig und vertrauenswürdig sind.« Das gleiche gilt für das Entschlüsseln oder Verifizieren einer signierten Nachricht beim Empfänger, damit die Authentifizierungskette nachvollzogen werden kann.

Die CAcert-Root-Zertifikate sind nicht in den Anwendungen der Mozilla-Suite eingebettet und müssen selbst importiert werden. Um die beiden CAcert-Root-Keys [7] zu beziehen, wird im Webbrowser *cacert.org* aufgerufen. Auf der rechten Seite der Homepage befindet sich im ersten Bereich *Join CACert.org* der Punkt *Root-Certificate*. Er wird nun angeklickt. Auf der nun erscheinenden Webseite muß unter der Überschrift *Class 1 PKI Key* der darunter befindliche Punkt *Root-Certificate (PEM Format)* angeklickt werden. Es öffnet sich eine Dialogbox, auf der angekreuzt werden muß, für welchen Zweck das CA-Zertifikat vorgesehen ist: zum Identifizieren von Webseiten, für Mail-Nutzer oder Software-Entwickler. Nach dem Ankreuzen von mindestens *Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren* wird mit Ok abgeschlossen. Danach muß unter der Überschrift *Class 3 PKI Key* der Vorgang wiederholt werden. Der Browser kann dann geschlossen werden.

Vom Browser zum Maildienst

Jetzt wird in den Mail-Client Thunderbird gewechselt und *Extras | Einstellungen | Erweitert* aufgerufen, dort der Tab *Zertifikate* und die Schaltfläche *Zertifikate*. Auf dem Tab *Zertifizierungsstellen* muß nun auf die Schaltfläche *Importieren* geklickt werden. Man landet im Dateiauswahldialog. Weil

Bild 6: Konteneinstellungen zur Aktivierung des Zertifikats in Thunderbird

Bild 9: Website-Login per Client-Zertifikat

für die Auswahl *Zertifikat-Dateien* voreingestellt ist, werden die soeben gespeicherten Dateien *class3.crt* und *root.crt* automatisch angezeigt. Man wählt die erste aus, klickt auf *Öffnen* und landet im Zertifikat-Manager. Dort klickt man wieder auf *Importieren* und wählt im Dateiauswahldialog die zweite Datei an. Zurückgekehrt im Zertifikat-Manager befindet sich dann der Punkt *Root CA* mit den beiden Unterpunkten *CA Cert Class3 Root* und *CA Cert Signing Authority* in der Listbox. Das ist das erfolgreich importierte CA-Zertifikat. Abgeschlossen wird mit Ok.

Nicht nur E-Mail

Wurde beim Erzeugen des Client-Zertifikats die Option *Zertifikats-Anmeldung mit diesem Zertifikat aktivieren* gewählt und ist es im Browser gespeichert, ist es auch für Website-Logins nützlich, siehe Bild 9. Wenn die Website neben der üblicherweise angebotenen Anmeldung über ein Paßwort auch den Login mit einem Client-Zertifikat ermöglicht, ruft der Webserver an dieser Stelle das im Browser gespeicherte Zertifikat ab. Er gleicht dann die darin gespeicherte Benutzerkennung mit seiner eigenen Benutzerliste ab und erlaubt bei Übereinstimmung die Anmeldung. Das Client-Zertifikat selbst kann zuvor anhand der CAcert-Root-Keys auf korrektes Anlegen und über den OCSP-Server auf Gültigkeit geprüft werden.

Eine weitere nützliche Anwendung ist zum Beispiel ein öffentlicher Blog, auf den jeder Benutzer mit einem CAcert-Client-Zertifikat automatisch Schreibzugriff hat. Spam und vergessene Paßwörter sind für den Admin der Website kein Thema mehr. Auch Votings sind auf diese Weise sehr einfach. Bei CAcert selbst sind diese und weitere Anwendungen tägliche Praxis.

Ebenso können mit Zertifikaten beliebige Dokumente signiert werden, um sicherzustellen, daß sie nach dem Anlegen nicht mehr geändert worden sind; dies ist laut Steuergesetz insbesondere beim Vorsteuerabzug elektronischer Rechnungen wichtig. Für OpenOffice/LibreOffice gibt es auch entsprechende Plugins, die die Anwendung vereinfachen.

Zum Schluß sei auf die Code-Signing-Zertifikate hingewiesen, die gerade in Zeiten der App-Entwicklung immer interessanter werden: Die Endgeräte oder deren Betriebssysteme verlangen nämlich oft, daß die zu installierenden Programme signiert sind. Auch wenn dies zwar noch keinen Qualitätsstandard für das Programm selbst darstellt, so erfährt man doch zumindest den Autor des Programms.

Immer unterschreiben

Sollen E-Mails standardmäßig signiert werden, schaltet man in Thunderbird in den Konto-Einstellungen zur S/MIME-Sicherheit die Option *Nachrichten digital unterschreiben (als Standard)* ein, dann braucht man nicht extra beim Versand daran zu denken, der spätere Austausch verschlüsselter E-Mails wird dadurch deutlich vereinfacht. In der gleichen Dialogbox kann auch das Verschlüsseln der Nachrichten voreingestellt werden.

Der Empfänger erkennt eine gültige E-Mail-Signatur in Thunderbird daran, daß das geöffnete E-Mail ein Bildchen mit einem versiegelten Brief enthält, wie Bild 7 zeigt. Sollte die Prüfung dagegen fehlschlagen, etwa weil die Signatur nicht verifiziert werden kann oder gar die E-Mail nach dem Verfassen und Versand geändert wurde, erscheint am Brief ein rotes Kreuz (siehe Bild 8). Eine Meldung über die Ursache befördert ein Klick auf den Briefumschlag zutage. Auf die gleiche Weise kann man sich auch bei einer gültigen Signatur das Zertifikat für die Unterschrift ansehen.

Andere E-Mail-Programme funktionieren letztendlich entsprechend, beispielsweise erscheint in Claws-Mail in der Attachment-Liste auf der rechten Seite einer E-Mail ein Brief mit einem grünen Haken, wenn die Signatur erfolgreich geprüft werden konnte, und ein Brief mit einem roten

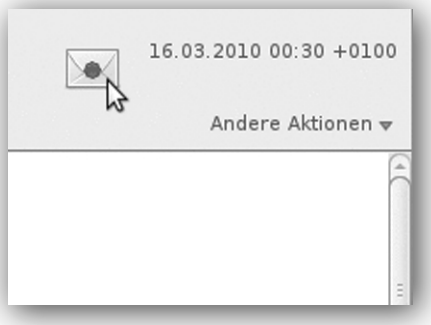

Bild 7: Darstellung einer erfolgreich geprüften Mail-Signatur in Thunderbird

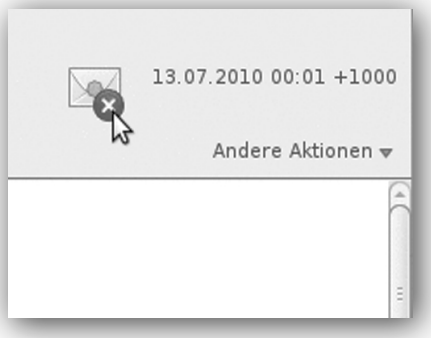

Bild 8: Thunderbird konnte die Signatur nicht verifizieren

Kreuz, wenn die Prüfung fehlschlug. Allerdings unterscheidet sich die Handhabung der Zertifikatseinbindung von Programm zu Programm. Informationen zu weiteren Browsern und E-Mail-Programmen finden sich im CAcert-Wiki unter [5], Hinweise speziell für Claws-Mail stehen in den Claws-Mail-FAQ[6].

Sollen Nachrichten dagegen nur in Einzelfällen unterschrieben beziehungsweise verschlüsselt werden, muß jedesmal vor dem Absenden in Thunderbirds *Einstellungen*-Menü der Punkt *Nachricht unterschreiben* beziehungsweise *Nachricht verschlüsseln* angeklickt werden.

Was CAcert (noch) nicht kann...

So praktisch Zertifikate auch sind – das Root-Zertifikat von CAcert ist zwar bereits in einigen Linux-Distributionen integriert, nicht jedoch standardmäßig in den verbreiteten Browsern, was die Anwendung erleichtern würde. Aktuell werden die durch das letzte Audit der Mozilla Foundation angestoßenen Maßnahmen umgesetzt. Nach dem Abschluß eines weiteren Audits wird die Integration in die Browser angestrebt. Bis dahin ist zur Nutzung der CAcert-PKI in aller Regel eine einmalige Prüfung und Aufnahme der Class-1- und Class-3-Root-Keys in den Zertifikatspeicher vonnöten, die über die CAcert-Website [7] heruntergeladen werden können.

Insbesondere in Unternehmen, die Dokumente unterschreiben wollen/müssen, ist zu beachten, daß es sich bei den Zertifikaten von CACert derzeit um zwar fortgeschrittene, aber nicht um qualifizierte Zertifikate im Sinne des deutschen Signaturgesetzes (SigG) handelt. ◆

Links

[1] http://www.cacert.org/
[2] https://www.cacert.org/index.php?id=1
[3] https://secure.cacert.org/wot.php?id=12
[4] https://secure.cacert.org/account.php?id=3
[5] http://wiki.cacert.org/EmailCertificates
[6] http://www.claws-mail.org/faq/index.php/S/MIME_howto
[7] http://www.cacert.org/index.php?id=3
[8] http://de.wikipedia.org/wiki/X.509