Mac OS X Consoliero
Weiterführende Dokumentationen für Administratoren.

E-Mail verschlüsseln und signieren mit eigenen Zertifikaten

Christoph Müller, PTS

Mac OS X Consoliero:

E-Mail verschlüsseln und signieren mit eigenen Zertifikaten

Inhaltsverzeichnis

Mac OS X Consoliero:
E-Mail verschlüsseln und signieren mit eigenen Zertifikaten

Einleitung

E-Mails werden im Internet offen übertragen. E-Mails sind dadurch einer Postkarte im Postverkehr sehr ähnlich. Diese können beim Transport ebenfalls von vielen Personen gelesen werden. Im Internet kann Ihre E-Mail abgefangen, gelesen und sogar verändert werden. Auch ist es nicht auszuschließen, dass eine E-Mail einen falschen Adressaten erreicht.
Will man vertrauliche Inhalte in E-Mails vor fremden Augen schützen, muss man seine E-Mails verschlüsseln, dass heisst, so kodieren, dass sie für Unbefugte nicht lesbar sind. Verschlüsselungsverfahren eignen sich auch, um den Absender einer E-Mail eindeutig zu identifizieren und eine Manipulation auszuschließen. Dies kann man über verschiedene Wege realisieren. Zum Beispiel in dem man sich Zertifikate von einer Zertifizierungsstelle wie etwa Verisign kauft, oder in dem man sie selber erstellt. Verisign ist eine Vertrauensstelle für Zertifikate. Aber, wem trau ich am meisten? - genau mir selber! Zudem ist es erst noch am günstigsten.

Auch wenn die Grundprinzipien von Verschlüsselungstechniken komplex sind, ist die Nutzung im Alltag, sobald die Software installiert und die Schlüssel generiert und ausgetauscht sind, unkompliziert. Als einziges Problem erweist sich in der Praxis oft, dass die Kommunikationspartner auch das entsprechende Verschlüsselungsverfahren installiert haben müssen, was jedoch oft (noch) nicht der Fall ist.

Christoph Müller, www.pts.ch

Konventionen

Wenn im Text ein **^X** angezeigt wird, bedeutet das einen so genannten „control character". Eingegeben wird dieser mit „ctrl" + „X" Taste. Befehle sind in Courier und **fett** gehalten. Also in etwa:

```
vi testfile.txt
```

Ausgaben des Terminals werden in Courier gehalten, aber nicht fett gedruckt.

```
tcsh: was: Command not found
```

Pfade `/Library/Preferences` innerhalb des Fliesstextes werden ebenfalls in Courier gehalten.

1. Hintergrundwissen

Wenn wir also unseren E-Mail Verkehr sicher gestalten möchten, müssen wir den Inhalt verschlüsseln. Verschlüsselungsverfahren eignen sich auch, um den Absender einer E-Mail eindeutig zu identifizieren und eine Manipulation auszuschließen. Der Einsatz von Verschlüsselung ist damit, zum Beispiel in der Geschäftskommunikation, bei der Übertragung von internen Dokumenten oder Verträgen sehr zu empfehlen. Auch für die private Kommunikation ist Verschlüsselung sinnvoll.

1.1 Grundprinzipe der Verschlüsselung

Es gibt eine Anzahl verschiedener Verschlüsselungstechniken, die sich für den Einsatz bei E-Mails im Internet eignen. Die zwei verbreitetsten sind "Pretty Good Privacy" (PGP) und S/MIME. Das Grundprinzip ist bei beiden Verschlüsselungsverfahren gleich: Ein normaler Text wird mit Hilfe eines Verschlüsselungscodes in eine neue Form gebracht. Der Inhalt erscheint danach für unbefugte Leser als sinnloser "Buchstabenwirrwarr". Um den Text entziffern zu können, muss dem Empfänger ein so genannter "Schlüssel" vorliegen, der eine "Rückübersetzung" in den ursprünglichen Zustand erlaubt.

Soll ein Text von verschiedenen Personen ver- und entschlüsselt werden, wie es bei E-Mails der Fall ist, ist es sinnvoll, wenn zur Verschlüsselung und Entschlüsselung nicht derselbe Schlüssel benötigt wird. Hierzu wurde das so genannte "Public Key-Verfahren", das auch "asymmetrische Verschlüsselung" genannt wird, entwickelt. Es arbeitet mit unterschiedlichen "Schlüsselpaaren", einem "privaten Schlüssel" und einem "öffentlichen Schlüssel". Der private Schlüssel ist nur dem Besitzer bekannt und darf nicht weitergegeben werden. Er dient hauptsächlich dazu, Nachrichten zu entschlüsseln oder zu signieren. Der "öffentliche Schlüssel" dagegen ist allgemein bekannt und kann z.B. auf Websites veröffentlicht werden. Er dient hauptsächlich dazu, Nachrichten für eine Person zu verschlüsseln. Öffentlicher und privater Schlüssel gehören zusammen, können jedoch nicht von einander abgeleitet werden. Das Schlüsselpaar wird von der Verschlüsselungssoftware erzeugt bzw. bei S/MIME einem E-Mail-Programm, das S/MIME unterstützt. Um den öffentlichen Schlüssel eines anderen zu erfahren, muss er von diesem erfragt werden bzw. kann auf dessen Website oder speziellen Servern herunter geladen werden.

Bleibt eine weitere Aufgabe: Um die Kommunikation wirklich sicher zu machen, muss gewährleistet sein, dass ein bestimmter Schlüssel auch zu einer bestimmten Person gehört. Andernfalls könnte sich jemand einfach als eine beliebige, andere Person ausgeben. Werden die Schlüssel nicht persönlich ausgetauscht, kann man nicht ohne weiteres sicher sein, dass hinter dem Schlüssel auch wirklich der gewünschte Absender steht. Man benötigt also eine Art "Authentifizierung" der Schlüsselinhaber. Hierzu werden bei PGP und S/MIME verschiedene Verfahren gewählt. PGP setzt auf ein so genanntes "Web of Trust", das heisst, Schlüsselinhaber können sich gegenseitig die Richtigkeit bestätigen. Auch anerkannte Institutionen können Schlüssel zertifizieren. Die Computerzeitschrift c´t zum Beispiel zertifiziert PGP-Schlüssel auf Messen, indem Sie den Inhaber anhand seines Personalausweises authentifiziert. Man kann jedoch auch ohne eine externe Zertifizierung schon mit seinem Schlüssel arbeiten. S/MIME dagegen setzt von vornherein auf ein formales Verfahren. Hier existieren spezielle Zertifizierungsstellen, von denen Zertifikate für den eigenen Schlüssel ausgegeben werden. Die Zertifizierung ist obligatorisch, ohne sie kann ein Schlüssel nicht eingesetzt werden.
Die Zertifzierungsstellen geben dabei verschiedene Klassen von Zertifikaten aus, die sich im Aufwand der Authentifizierung unterscheiden. In der Regel sind dies:

- Klasse 1: Verifizierung der E-Mail-Adresse über eine E-Mail. Ein Klasse 1-Zertifikat ist dementsprechend unsicher, da eine E-Mail-Adresse relativ leicht zu fälschen ist. Vorteil des Klasse 1-Zertifikates: Es ist meist kostenlos erhältlich, da es wenig Aufwand für die Zertifizierungsstelle verursacht. Oft werden Klasse 1-Zertifikate von den Zertifizierungsstellen auch als so genannte "Probe"- oder "Test-Zertifikate" ausgegeben.

- Klasse 2: Hierbei erfolgt die Verifizierung in der Regel anhand eines (amtlichen) Dokumentes. Beispielsweise muss der Personalausweis oder Führerschein vorgelegt werden. Solche Modelle werden aber bisher nur in Deutschland angeboten.

- Klasse 3: Hierbei handelt es sich um eine persönliche Authentifizierung. Der Zertifikatsantragsteller muss persönlich bei der Zertifizierungsstelle bzw. einem Stellvertreter wie etwa dem Postamt, (so genanntes PostIdent-Verfahren) erscheinen und sich ausweisen. Dieses Verfahren garantiert eine sehr hohe Sicherheit. Allerdings ist es oft nur eingeschränkt verfügbar, da viele Zertifizierungsstellen diese Form der Authentifizierung nur im näheren Umfeld ihres Institutssitzes vornehmen.

Je sicherer ein Zertifikat ist, desto aufwendiger und damit teurer wird es in der Regel. Die Preise variieren je nach Zertifizierungsstelle.

1.2 Absender identifizieren

Mit den vorgestellten Verschlüsselungsverfahren ist es auch möglich, den Absender einer E-Mail eindeutig zu identifizieren, wenn er seinen "privaten Schlüssel" wirklich geheim hält. Hierzu nutzt der Absender einer E-Mail die Verschlüsselungssoftware für eine an die E-Mail angehängte "digitale Signatur". Diese wird mit Hilfe des privaten Schlüssels erzeugt. Der Empfänger der E-Mail kann mit Hilfe des öffentlichen Schlüssels des Absenders überprüfen, ob die E-Mail wirklich von diesem gesandt wurde.

Ob man für diesen Zweck PGP oder S/MIME einsetzt, ist eine Frage der individuellen Präferenz. Von der zur Verfügung gestellten Grundfunktionalität und der Sicherheit her sind beide Verfahren gleich gut. S/MIME hat allerdings den Vorteil, dass dafür keine spezielle Software herunter geladen werden muss, sondern es schon in vielen verbreiteten Mailprogrammen wie zum Beispiel Outlook, Netscape Messenger, Apple Mail oder etwa Microsoft Entourage integriert ist. Allerdings muss für S/MIME ein Zertifikat bei einer Zertifizierungsstelle beantragt werden, das je nach Klasse kostenpflichtig ist.

PGP dagegen erfordert die Installation der PGP-Software, die jedoch kostenlos erhältlich ist. Es erzeugt seinen Schlüssel selbst, eine externe Zertifizierung kann vorgenommen werden, ist aber nicht zwingend.
Wichtig ist, dass, egal welches Verfahren Sie verwenden, Ihr Kommunikationspartner dasselbe Verfahren benutzt. Ein Verschlüsseln mit PGP und ein Entschlüsseln über S/MIME ist nicht möglich. Man kann aber beide Verfahren parallel nutzen. Sendet Ihnen jemand eine E-Mail mit PGP, können Sie diese mit Ihrem PGP-Schlüssel dechiffrieren. Wollen Sie dagegen jemanden erreichen, der über S/MIME verfügt, senden Sie ihm eine S/MIME verschlüsselte E-Mail.

1.3 Wie sicher sind Zertifikate

Ein Schüssel besteht beispielsweise aus 1024 Bit. Das entspricht einer 300-stelligen Dezimalzahl. Das "Knacken" einer Nachricht, also das unauthorisierte Entschlüsseln, ist bei solch großen Schlüsseln nur noch mit sehr hochleistungsfähigen Rechnerpools möglich. Im Alltag kann das Verfahren also als sicher gelten. Allerdings ist zu beachten, dass Sie Ihren privaten Schlüssel und Ihr zugehöriges Passwort auch wirklich geheim halten müssen. Ein weiteres Sicherheitsrisiko liegt in einem nicht-zertifizierten öffentlichen Schlüssel, bzw. einem mit einer niedrigen Verschlüsselungsklasse. Wenn keine Person oder Institution Ihres Vertrauens bestätigt, dass der Schlüssel auch wirklich von Ihrem Empfänger stammt, könnte es sein, dass dieser fälschlicherweise von jemand anderem als solcher ausgegeben wird.

2. Zertifikate selber erstellen

Wollen wir also für uns und unsere E-Mail Partner Zertifikate haben, welche uns eindeutig identifizieren, können wir diese selber erstellen und an alle die sie benötigen, verteilen. Mit diesen Zertifikaten können wir auch den Inhalt eines E-Mails verschlüsseln.

Mac OS X verwendet für das lesen, überprüfen und speichern von Zertifikaten den so genannten Schlüsselbund. Die entsprechende Applikation findet sich unter `/Applications/Utilities` (Abbildung 1).

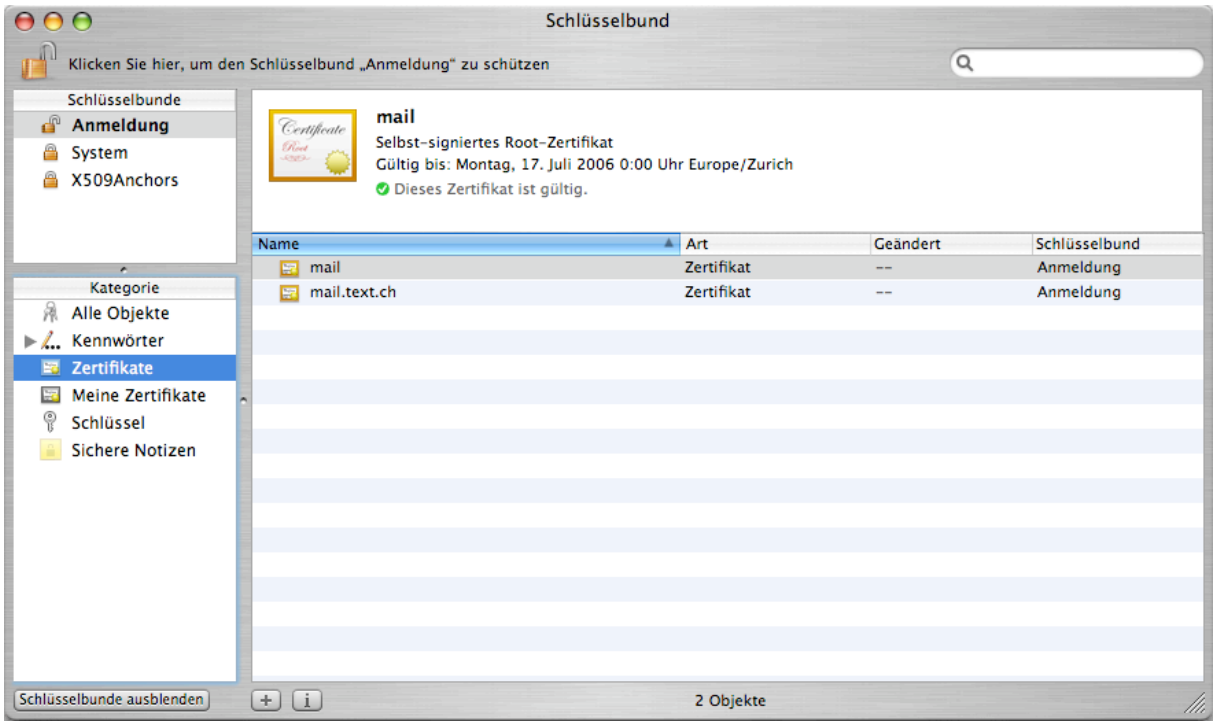

Abbildung 1 – Applikation Schlüsselbund

Über die Schaltfläche unten links, kann ich mir alle drei vorhandenen Schlüsselbunde in der linken Spalte anzeigen lassen. In der Regel ist nur der Schlüsselbund „Anmeldung" geöffnet. Öffnen Sie nun zusätzlich den Schlüsselbund „X509Anchors", in dem Sie ihn anklicken und dann in der Symbolleiste auf das Schloss-Symbol klicken. Um das zu tun, benötigt man ein Administratorkennwort.

Um nun ein eigenes Zertifikat zu erstellen, kann man sich auf das gute alte Terminal stützen, oder eine fast nicht dokumentierte Funktion des Programms Schlüsselbund benutzen. Im Menü „Schlüsselbund" findet sich der Zertifikatsassistent (Abbildung 2).

Mit diesem Assistent können wir für uns und für alle die ein Zertifikat benötigen, Zertifikate erstellen. Aber nun Schritt für Schritt:

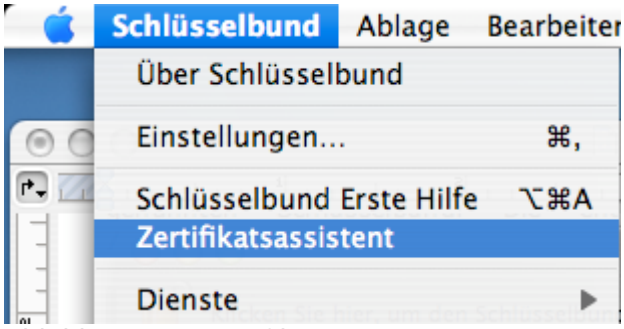

Abbildung 2 – Zertifikatsassisent

Klicken Sie sich durch den Assistenten bis Sie zu dem Punkt „Optionen" kommen. Dort wählen Sie „Ein eigenes Zertifikat erstellen" aus (Abbildung 3).

Abbildung 3

Danach müssen Sie die Details des Zertifikates angeben. Was man dort eingibt, ist nicht entscheidend. Wichtig ist nur, dass die E-Mail Adresse genau der E-Mail Adresse entspricht, für den das Zertifikat beabsichtigt ist (Abbildung 4). Natürlich kann man die

Gültigkeit auch verlängern, damit ein Zertifikat länger als ein Jahr gültig ist. Ganz nach Geschmack. Prüfen Sie zudem ob der Hacken bei „Zertifikat wird selbst signiert" gesetzt ist.

Der Assistent warnt uns nun, dass ein selbst signiertes Zertifikat nicht die gleiche Sicherheit bietet wie ein öffentliches Zertifikat. Klicken Sie die Warnung weg und fahren Sie weiter.

Abbildung 4

Die Länge des Schlüssels und der Algorithmus lassen wir auf der Standardeinstellung (2048 Bit, RSA).

Nun müssen wir definieren für was das Zertifikat verwendet werden kann (Abbildung 5). Um hier eine Auswahl treffen zu können, müssen wir die Option „Erweiterung „Schlüsselverwendung" verwenden", aktivieren. Danach wählen wir alle Verwendungszwecke aus, welche wir mit diesem Zertifikat verwenden. Zumindest aber „Signatur" und „Datenverschlüsselung" und gehen weiter.

Im nächsten Feld können wir weitere Optionen definieren, welche wir mit diesem Zertifikat planen. Für unsere Zwecke genügen aber die Einstellung aus Abbildung 5 völlig, so dass wir bei „Verschiedene Erweiterungen" alle inaktiv lassen können.

Danach definieren wir noch den Schlüsselbund, in dem unser Zertifikat gespeichert werden soll. Wir lassen das in der Standardeinstellung (Anmeldung) und das Zertifikat wird generiert.

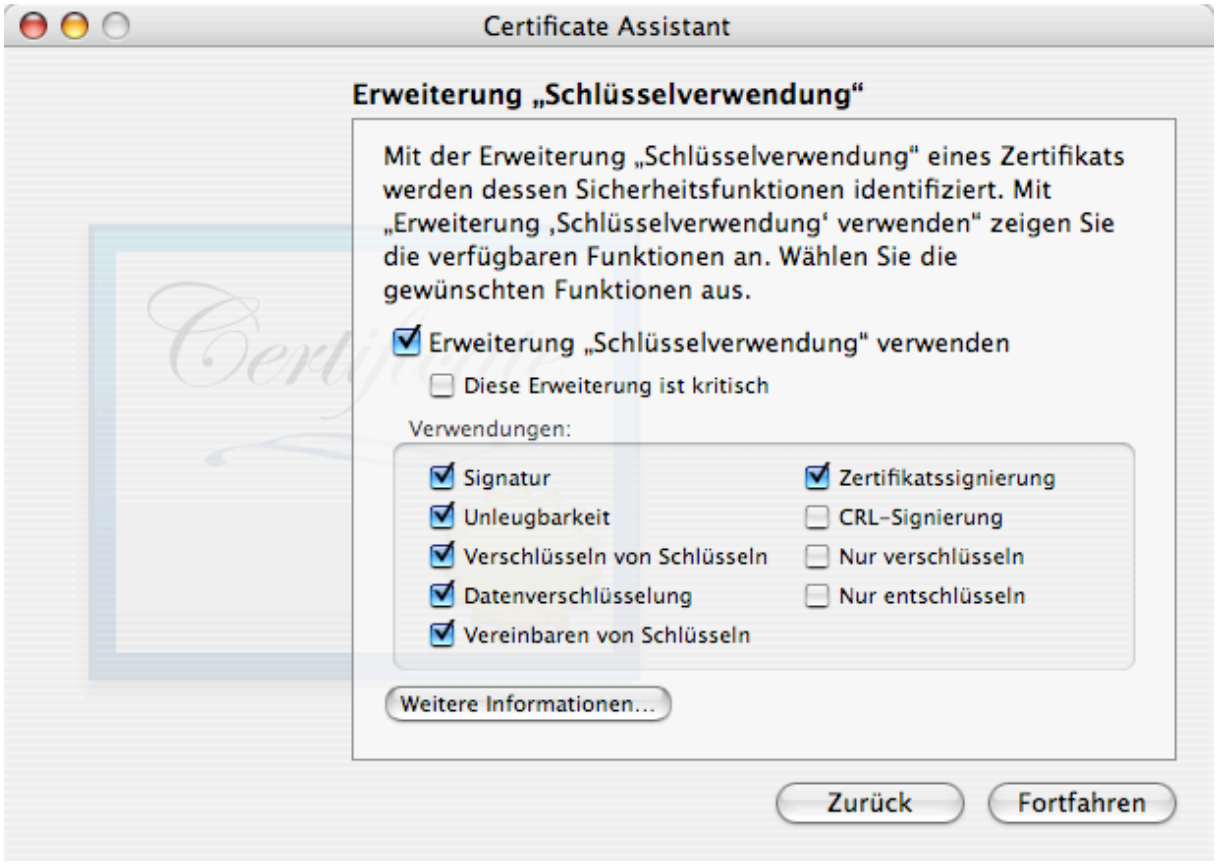

Abbildung 5

Wenn Sie alles richtig gemacht haben, erscheint das Zertifikat nun im Schlüsselbund „Anmeldung“ unter „Meine Zertifikate“ (Abbildung 6).

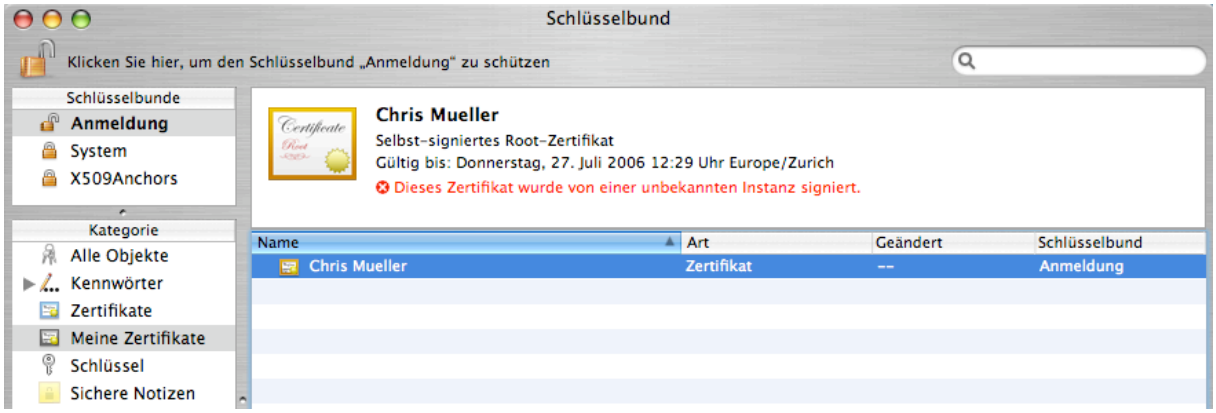

Abbildung 6

2.1 Uns selber vertrauen

Das Programm Schlüsselbund zeigt es uns an: das Zertifikat wurde von einer unbekannten Instanz signiert. Die Instanz sind wir selber und wir trauen uns ja. Allerdings weiss das unser Macintosh noch nicht. Deswegen müssen Sie das Zertifikat in den Schlüsselbund „X509Anchors“ importieren. Dort werden die bekannten

Zertifizierungsstellen gespeichert. Um das zu tun, müssen wir unser frisch erstelltes Zertifikat exportieren und in den Schlüsselbund „X509Anchors" importieren.

Um das zu tun gibt es nur einen Weg der genau eingehalten werden muss. Wechseln Sie im Schlüsselbund „Anmeldung" in die Ansicht „Alle Objekte" und wählen Sie dort Ihr Zertifikat aus (Abbildung 7). Stellen Sie sicher, dass Sie das Zertifikat und nicht einer der beiden Schlüssel ausgewählt haben. Danach exportieren wir das Zertifikat über das Menü „Ablage" mit dem Menüeintrag „Exportieren".

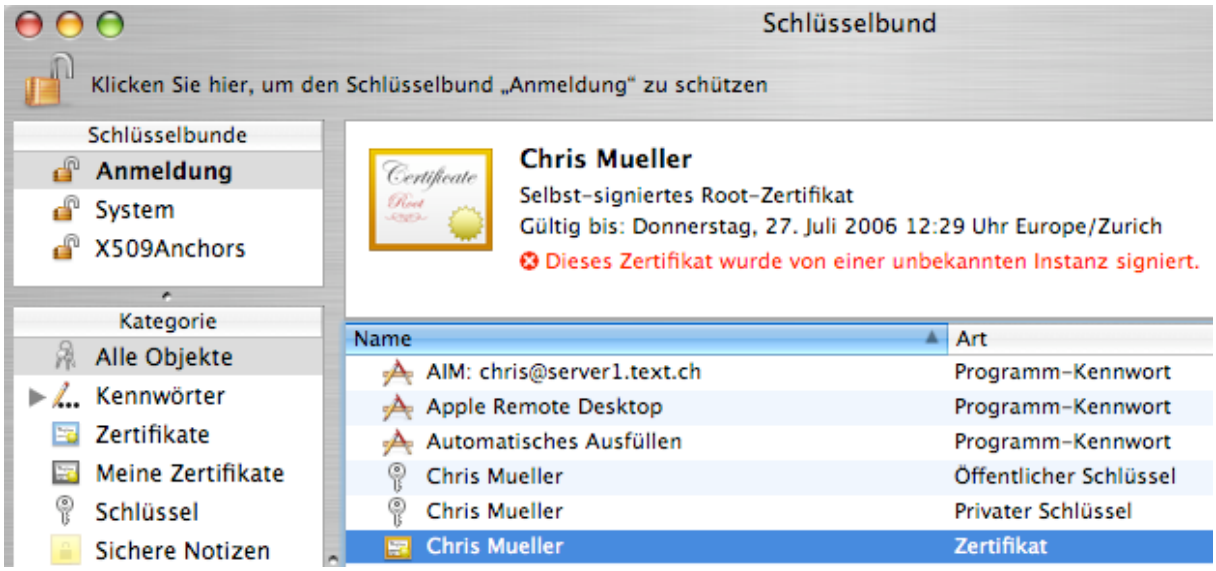

Abbildung 7

Exportiert wird das Zertifikat als Format „.cer" (Abbildung 8).

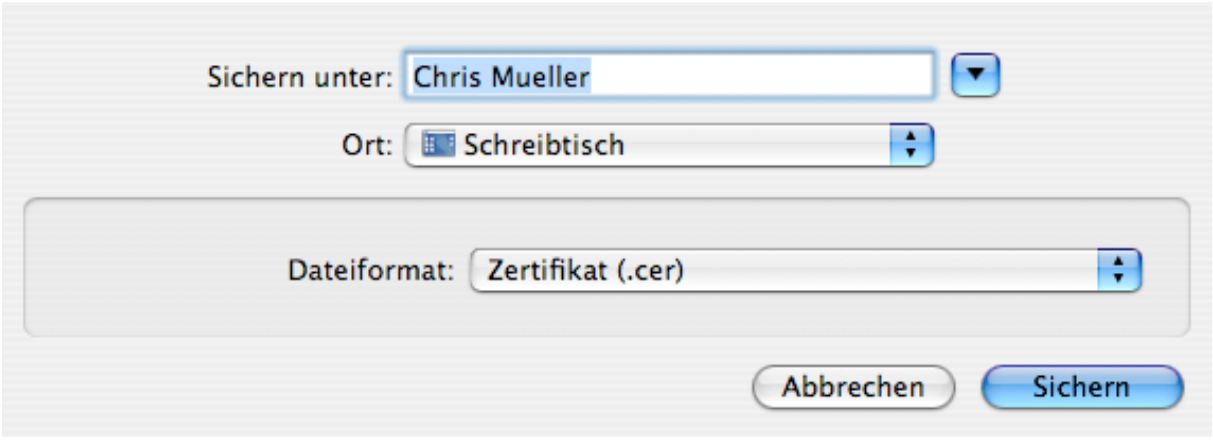

Abbildung 8

Danach importieren wir wiederum über das Menü Ablage das soeben exportierte Zertifikat in den Schlüsselbund „X509Anchors" (Abbildung 9).

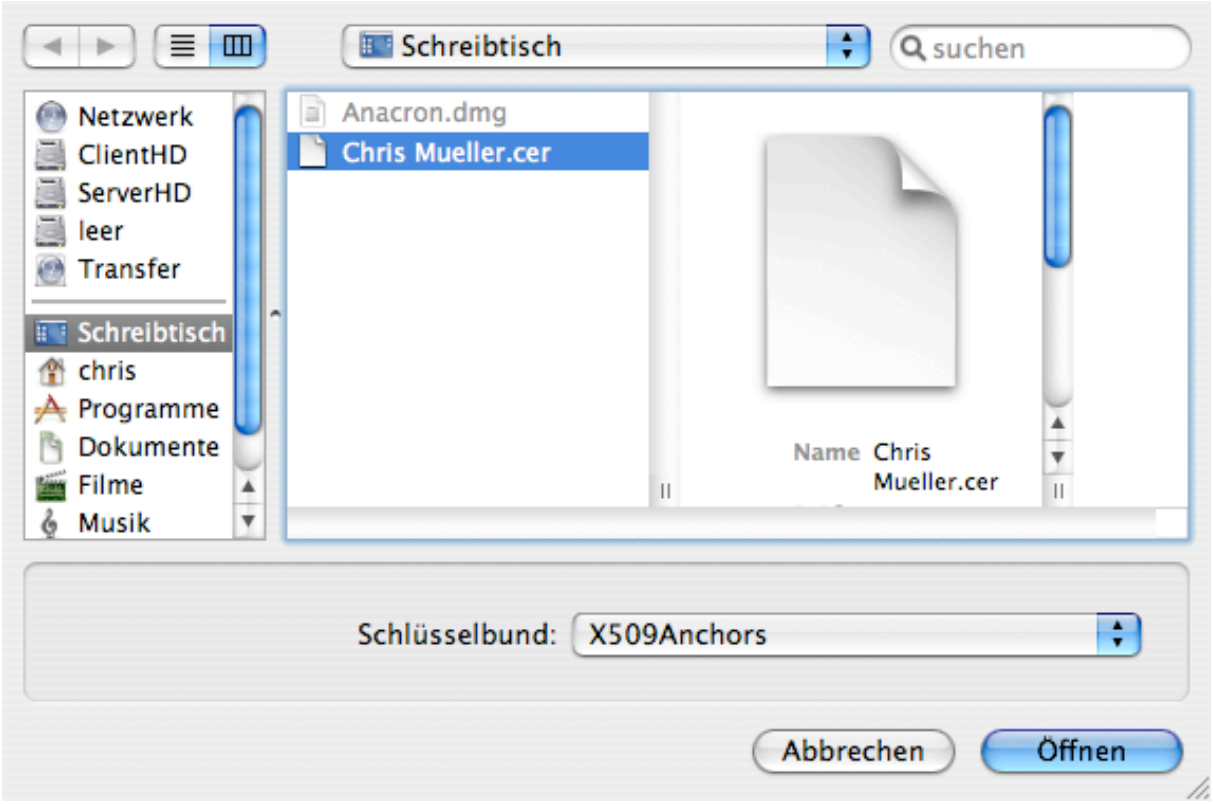

Abbildung 9

Nun gilt also unser Zertifikat als vertrauenswürdig. Wenn wir nun das Programm Schlüsselbund beenden und wieder starten, wird das auch dementsprechende angezeigt (Abbildung 10).

Abbildung 10

Damit diese Vertrauensstellung allen Programmen die dieses Zertifikat verwenden werden auch klar ist, und sie nicht immer zurückfragen, ob sie dieses Zertifikat benutzen dürfen, definieren wir das noch genauer.

Doppelklicken Sie auf Ihr Zertifikate und scrollen bis zum Eintrag „Einstellungen bestätigen" herunter (Abbildung 11). Dort stellen Sie alle Verwendungszwecke auf „Immer vertrauen". Diese Einstellungen müssen Sie nur in einem Schlüsselbund

vornehmen. Die Einstellungen gelten dann automatisch für das Zertifikat zum Beispiel im Schlüsselbund „X509Anchors".

Abbildung 11

2.2 Apple Mail und die digitale Identität

Starten Sie nun das Apple E-Mail Programm. Erzeugen Sie eine neue E-Mail, so als ob Sie eine E-Mail schreiben möchten. Wenn Sie alles richtig gemacht haben, erscheinen nun zwei neue Symbole unterhalb des Betreffs (Abbildung 12).

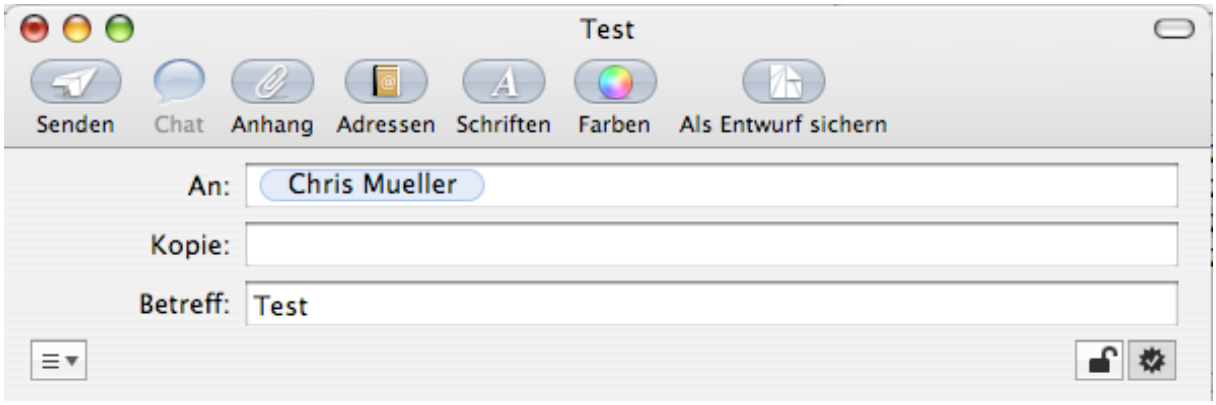

Abbildung 12

Das Symbol das einer Sonne ähnlich scheint, symbolisiert dabei die digitale Identität. Wenn der Hacken gesetzt ist, wird Ihre Identität über das Zertifikat sichergestellt. Das Symbol mit dem Schloss symbolisiert die Verschlüsselung. Wenn das Schloss geschlossen ist, wird das die E-Mail verschlüsselt, wenn es offen ist konsequenterweise nicht. Die Möglichkeit eine E-Mail zu verschlüsseln erscheint nur dann, wenn das Programm Mail auch in der Lage ist, mit Hilfe des Zertifikates des Empfängers dieses zu verschlüsseln. Ansonsten bleibt das Schloss grau.

3. Mehr Benutzer einrichten

Interessant und sinnvoll wird dieses System erst wenn mehrere Benutzer an einem solchen System beteiligt sind. Erstellen Sie also für jeden Benutzer ein eigenes Zertifikat gemäss Anleitung, Abschnitt 2.

Wenn Ihnen ein neuer Benutzer im System mit einer neuen digitalen Identität eine E-Mail sendet, fragt der Schlüsselbund nach, ob dieses Zertifikat gespeichert werden soll. Wenn das geschehen ist, kann das Programm Mail ab sofort dieses Zertifikat benutzen um den Inhalt des Mails zu verschlüsseln (Abbildung 13) und die Identität in Zukunft anhand der gespeicherten digitalen Identität zu überprüfen.

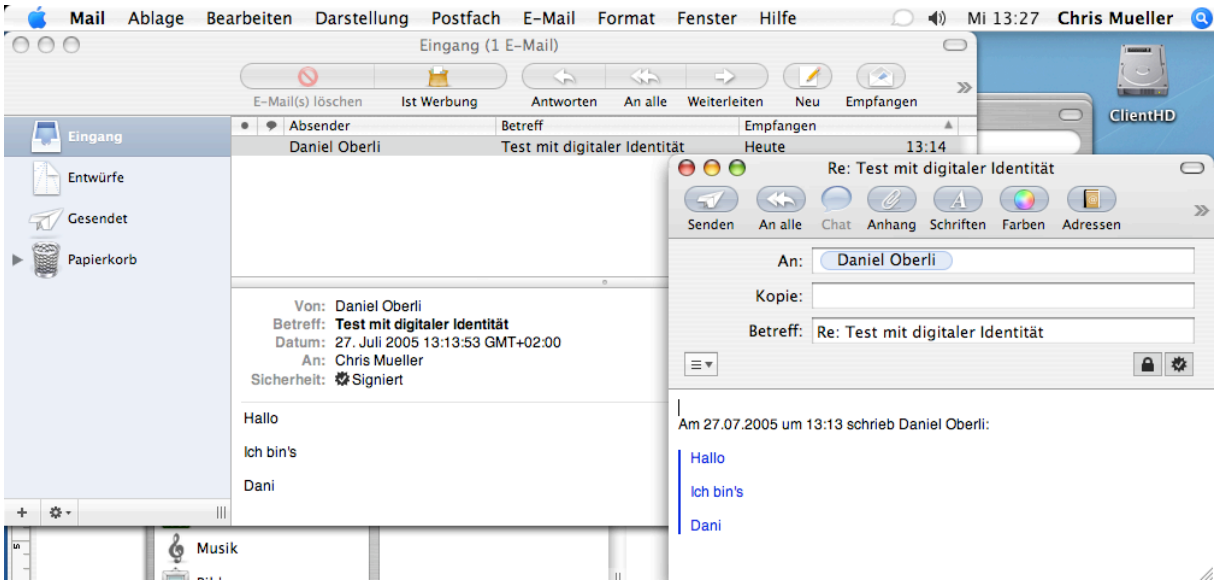

Abbildung 13

Christoph Müller - www.pts.ch

Publishing Tools Support
Rüschlikon, 30.8.2005

Bei Fragen oder Anmerkungen, kontaktieren Sie mich bitte unter chm@pts.ch

Weitere detaillierte Informationen erhalten Sie aus meinem Buch: **„Mac OS X „Consoliero-Client" Praxis Handbuch"**: ISBN-Nr. 3-905647-17-6.