jetzt digital signiert auch aus Lotus

Published Dezember 1st, 2009 in Allgemein.

Seit wir auf Lotus migriert sind, konnten aus Lotus keine digital signierten E-Mails mehr ins Internet verschickt werden, weil nicht klar war, wie die Zertifikate, welche die Client Certificate Authority der UZH ausstellt, im Lotus Client importiert werden müssen. Nachem jetzt die gesamte Lotus Umgebung auf 8.5.1 gehoben wurde, wurde die Sache nochmals analysiert. Es klappt. Nicht, weil sich mit Lotus 8.5.1 etwas geändert hätte gegenüber 8.5. Aber weil klar wurde, weshalb die an der UZH ausgestellten Zertifikate nicht importiert werden konnten.

Lotus Notes importiert S/Mime Zertifikate nicht, wenn das ROOT-Zertifikat nicht vorhanden ist. Egal, von welcher Certificate Authority ein Zertifikat bezogen wrd. Die Zertifikate, welche die UZH ausstellt, enthalten aber die Chain zum ROOT-Zertifikat nicht und enthalten auch das ROOT-Zertifikat nicht. ROOT-Zertifikate können aber von Endusern nicht importiert werden. Es gelingt aber, ein ROOT Zertifikat in ein persönliches Zertifikat zu importieren und so die Kette zu schliessen. Lotus Notes findet dann das ROOT Zertifikat während dem Import und das Zertifikat kann importiert und benutzt werden.

Und wie ist das Vorgehen, wenn wie an der UZH ein Zertifikat im PKS12-Format vorliegt um ein importfähiges Zertifikat zu erzeugen? Nebst dem eigenen Zertifikat, welches auch den privaten Schlüssel verschlüsselt enthält, benötigt man dafür auch das ROOT-Zertifikat der ausstellenden Behörde respektive falls notwendig auch die Zwischenzertifikate um die Zeritifkatskette zu schliessen. Und openssl, was unter Mac OS X und Linux-Distributionen vorhanden ist.

Zuerst gilt es, das eigene Zertifikat im PKS12-Format in ein PEM-Format umzuwandeln. Da das resultierende Zertifikat nur temporär gebraucht wird, verschlüsseln wir den Private Key des Zertifikates im PEM-Format nicht. Das wird, wenn das Zertifikat `MyCert.pfx` heisst, mit folgendem openssl-Befehl erreicht.

```
#
# bestehendes pkcs12 Zertifikat in PEM-Format konvertieren
# OHNE den private key zu verschlüsseln
#
openssl pkcs12 -in MyCert.pfx -out MyCert.pem -nodes
#
```

Das Passwort/Passphrase des bestehenden privaten Schlüssels wird abgefragt.

Jetzt gilt es, das ROOT-Zertifikat (in diesem Fall im File `CAClientRoot.crt` abgelegt) diesem Zertifikat beizufügen, wobei wir den Privaten Schlüssel wieder verschlüsseln:

```
#
# entschlüsseltes Zertifikat mit ROOT-Zertifikat respektive
# mit weiteren Intermediate-Zertifikaten ergänzen.
#
openssl pkcs12 -export \
-in MyCert.pem \
-inkey MyCert.pem -out MyCert-Chained.p12 \
-CAfile CAClientRoot.crt \
-caname "University of Zurich, Client Certificate Authority" \
-chain
#
```

Nach Eingabe des Befehls wird wieder das Passwort (ihr wählt da natürlich wieder eine lange Passphrase) für das neue Zertifikat abgefragt.

Und jetzt unbedingt das Zertifikat, in welchem der Private Key unverschlüsselt abgelegt ist, löschen!

```
rm MyCert.pem
```

Das neue Zertifikat `MyCert-Chained.p12` kann jetzt als Internet-Zertifikat in die Notes-ID importiert und aktiviert werden.

Und für alle jene, denen das doch etwas zu viel des Guten ist, es gibt für Thunderbird-Benutzer, die Ihr Zertifikat und die notwendigen ROOT-Zertifikate in Thunderbird importiert haben, einen einfacheren Weg. Ein aus Thunderbird exportiertes Zertifikat kann in Lotus Notes ohne weiteres importiert werden!

Und was lehrt uns die Übung? Wir verfolgen seit geraumer Zeit die Optionen, die Client- und Server-CA an der UZH abzulösen aber weiterhin für Angehörige der UZH kostenlos Zertifikate anbieten zu können. Mit Thawte gab es bis Mitte November einen Anbieter, der gratis Zertifikate anbot, bei welchen es mögliche war, nicht nur die E-Mail-Adresse, sondern auch Name und Vornamen ins Zertifikat hineinzubringen. Mann oder Frau musste sich durch andere Mitglieder des Web of Trust (WOT) lediglich notifizieren zu lassen. Die Thawte Zertifikate konnten gebraucht werden, **OHNE** dass die Zertifikate von den Empfängern einer signierten E-Mail akzeptiert werden mussten oder ein ROOT Zertifikat eingebaut werden musste. Der Dienst wurde leider von VeriSign eingestellt.

Die UZH hat sich daraufhin bei CACert.org, zusammen mit der ETHZ, als Organisation anerkennen lassen und wir prüfen jetzt, welche Optionen für uns bei CACert offen stehen respektive wie Angehörige auch in Zukunt Zertifikate erhalten können, welche Ihnen nicht auf der

Geldbörse liegen. Damit für signierte und verschlüsselte E-Mail aus Lotus ins Internet auch in Zukunft eine Option besteht, bei welcher ohne openssl Befehle oder Umwege über Thunderbird E-Mail digital signiert werden kann. Gerade bei den immer wieder laufenden Pishing-Attacken bieten digitale Unterschriften doch eine Gewähr für einen korrekten Absender. Bei CACert.org kann auch mitmachen, wer nicht Angehöriger der UZH oder ETHZ ist und jedermann kann sich beim Web of Trust von CACert bestätigen lassen. Macht doch jetzt schon mit!

0 Responses to “jetzt digital signiert auch aus Lotus”

No Comments