Einführung in CAcert

Sebastian Bötzl

19. März 2008

Inhaltsverzeichnis

Kapitel 1

Was ist CAcert

CAcert ist eine gemeinschaftsbetriebene, nicht-kommerzielle Zertifizierungsstelle (Certification Authority, Root-CA oder kurz CA), die kostenfrei X.509-Zertifikate für verschiedene Einsatzgebiete ausstellt. Damit soll eine Alternative zu den kommerziellen Root-CAs geboten werden, die zum Teil recht hohe Gebühren für ihre Zertifikate erheben.

1.1 Client-Zertifikate

Direkt nach einer Registrierung bei CAcert lassen sich sofort Client-Zertifikate ausstellen. Diese enthalten nur die durch eine automatische Testmail überprüfte E-Mail Adresse, als Name (CN) wird „CAcert WoT User“ eingetragen. Nach einer Bestätigung der eigenen Person durch andere Mitglieder des CACert-Web-of-Trust lassen sich auch personalisierte Zertifikate mit eingetragenem Namen ausstellen. Sie dienen zum Beispiel zum Verschlüsseln und Signieren von E-Mails und anderen Daten, aber auch Authentifikation an Servern oder zum Signieren von Softwarecode.

1.2 Server-Zertifikate

Server-Zertifikate sollen die Zugehörigkeit eines Servers zu einer Person oder Unternehmen bestätigen und dienen als Basis für verschlüsselte SSL/TLS-Verbindungen. Es gibt verschiedene Dienste, bei denen Server-Zertifikate zum Einsatz kommen. Dazu gehören u. a. HTTPS, FTP(S), SMTP(S), POP(S) und IMAP(S).

Kapitel 2

Wie funktioniert CAcert

Jede angemeldete Person kann sich sein selbst erstelltes Zertifikat von dieser Zertifizierungsstelle beglaubigen lassen. Hat er noch kein Zertifikat, so kann er sich ein Zertifikat austellen und gleich Signieren lassen. Das Zertifikat wird dann im Webbrowser erstellt und der Private Schlüssel lokal gespeichert. Die Zweite Möglichkeit ist es, ein Zertifikat mit Openssl zu erstellen und nur den CSR (Certificate Signing Request) zu Übertragen und diesen Zertifizieren zu lassen.

Jeder User kann sich „beglaubigen“ lassen. Hat eine User 50 Punkte erreicht gilt er als „assured“ und sein Richtiger Name wird ab diesen Zeitpunkt bei jedem neu ausgestellen Zertifikat hinterlegt. Desweiteren kann er nun auch ServerZertifikate mit einer Laufzeit von 24 Monaten erstellen.

Ab 100 Punkten könnennun Zertifikate zur Signiereung von Software erstellen werden und jeder kann nun selbst als Assuerer Tätig werden.

2.1 Der Ablauf der Assurance

Man erstellt einen Account unter www.cacert.org
Man vereinbart ein Treffen mit einen Assurer und lässt sich dort mit Personalausweis und Führerschein beglaubigen. Je nachdem welchen Rang der Assurer hat und wie Vertrauenswürdig wir man wirkt kann einen der Assurer 10-35 Punkte erteilen.
Eine Weitere Möglichkeit besteht sich bei einem Notar die Identität bestätigen zu lassen und diese Dokumente direkt an CAcert zu senden.
Nach dem Treffen mit dem Assurer trägt diese die Punkte in ein Formular ein und der User kann seinen Punkte kontrollieren.

Kapitel 3

Einsatzmöglichkeiten

Für was können Zertifikate eingesetzt werden: Email-Verschlüsselung
Email-Signierung
PC-Login
Website-Login
VPN-Login
SSH-Login
Dokumenten-Signierung
usw.

Kapitel 4

Mögliche Hardware

4.1 SmartCard

Die SmartCard ist mit einer Geldkarte zu vergleichen die einen Chip bestizt. Der Chip auf der Karte ist das Kernstück. Er ist veranwortlich für die Erzeugung, Speicherung und das Schützen von Zertifikaten sowie für das Signieren.

4.2 SmartCardReader

Es gibt verschieden SmartCardReader die je nach Aufbau in Verschieden Sicherheitssufen eingeteilt weren.

Class1 - Leser ohne Pinpad und ohne Display
Class2 - Leser mit Pinpad und ohne Display
Class3 - Leser mit Pinpad und Display

Der Kartenleser an sich ist hat nur die Aufgabe die Funktionen der SmartCard dem Computer zur verfügung zu stellen.

4.3 USB Token

Ein USB Token verbindet eine Smartcard mit einem Lesegerät. Es wird nur ein USB Port und die dazu nötigen Treiber benötigt. Der große Kartenlesen und die „große“ Smartcard entfallen. Alle beide kompentenen sind in einen kleine USB-Stick untergebracht.

4.3.1 Mit Flash

Es gibt verschiedene Hersteller die sogeannte eTokens mit integrierten Flasch Speicher anbieten.

Bsp.: Aladdin eToken NG-FLASH mit bis zu 1GB
http://www.aladdin.de/produkte/usbtoken_esecurity/etoken_ng_flash.html

4.3.2 Ohne Flash

USB-Smartcard

Bsp.: Aladdin eToken PRO USB
http://www.aladdin.de/produkte/usbtoken_esecurity/etoken_pro_usb.html
alternative
http://www.kobil.de/index.php?id=55&type=7&L=1

Kapitel 5

Beispiele mit dem Umgang mit openssl

Ein Client-Zertifikat (E-Mail) erstellen:

5.1 Erstellen

openssl genrsa -out myname.key 2048
openssl req -config user.config -new -key myname.key -out myname.csr

Tabelle 5.1: user.config

req

default_bits = 1024
distinguished_name = req_DN
string_mask = nombstr

req_DN

countryName = „1. Country Name (2 letter code)“
countryName_default = DE
countryName_min = 2
countryName_max = 2
stateOrProvinceName = „2. State or Province Name (full name) „

#stateOrProvinceName_default =
localityName = „3. Locality Name (eg, city) „
localityName_default = Chemnitz
0.organizationName = „4. Organization Name (eg, company) „
0.organizationName_default = Mustermann
organizationalUnitName = „5. Organizational Unit Name (eg, section) „
#organizationalUnitName_default =
commonName = „6. Common Name (eg, CA name) „
commonName_max = 64
commonName_default = Max Mustermann
emailAddress = „7. Email Address (eg, name@FQDN)“
emailAddress_max = 40
emailAddress_default = max@mustermann.de