IT Services IT

Was ist eine X509-Zertifizierung?

X.509-Zertifikate werden von Rechnern zur Authentifizierung bei einer verschlüsselten Übertragung von Daten (per SSL, Secure Socket Layer) verwendet, z. B. von WWW-Servern (https-URLs).

Prinzipiell kann jeder Server-Betreiber sich selbst ein Zertifikat ausstellen und selbst signieren. Eine CA bestätigt durch ihre digitale Signatur, dass der Zertifikatsinhaber auch wirklich der ist, für den er sich ausgibt. Auf welche Art und Weise eine CA das überprüft, steht in ihrer Policy.

Was ist eine Policy?

Ein Vertrauen in eine CA setzt voraus, dass die CA gewissenhaft arbeitet und sich an gewisse Vorschriften hält. Diese Vorschriften beinhalten zu Beispiel, wer wen wann und wie lange zertifizieren darf und auf welche Art er sich von dessen Identität überzeugen muss. Die Sammlung dieser Vorschriften nennt man Policy, und diese ist bindend für die Mitarbeiter einer CA.

Policies ändern sich im Laufe der Zeit, aber meistens nur geringfügig. Da man aus einem Zertifikat stets den Zeitpunkt der Zertifizierung erkennen kann, wird eine Historie der Policies mitgeführt, um erkennen zu können, unter welchen Bedingungen eine Zertifizierung durchgeführt wurde.

Was ist der Unterschied zwischen SSL und SMIME?

Man möge die etwas ungenaue Formulierung entschuldigen. Es geht hier nicht um die detailgetreue Wiedergabe diverser RFCs, sondern um eine einfache Erklärung.

SSL steht für Secure Socket Layer und beschreibt ein Verfahren, dass verwendet wird, um eine sicherere Verbindung zwischen einem Client und einem Server herzustellen. X.509 beschreibt ein Format, welches für Zertifikate verwendet wird. SSL verwendet wiederum solche Zertifikate für die Autentifizierung beim Verbindungsaufbau.

SMIME ist eine Erweiterung des MIME-Standards für Emails und arbeitet ebenfalls mit X.509-Zertifikaten. Eine CA stellt also genaugenommen keine SSL-Zertifikate aus (obwohl die immer wieder so genannt werden), sondern Zertifikate nach dem X.509-Standard, die für SSL-Verbindungen (Server-Certs) oder SMIME-Emails (Client-Certs) verwendet werden können. Genau genommen sind das X.509v3-Zertifikate, aber das sind schon wieder Feinheiten. Alles klar?

Was sind öffentliche und private Schlüssel?

Bei der sogenannten asymmetrischen Verschlüsselung besitzt jeder Teilnehmer einen öffentlichen und einen privaten Schlüssel. Ohne jetzt hier ins Detail zu gehen, sollen nur zwei grundlegende Eigenschaften genannt werden:

1. Zu jedem öffentlichen Schlüssel gibt es genau einen privaten Schlüssel und umgekehrt.
2. Was mit dem einen der beiden verschlüsselt wurde, kann nur mit dem anderen entschlüsselt werden.

Was sich hier ganz harmlos anhört, hat weitreichende Konsequenzen und die Entdeckung stellte in der Geschichte der Kryptographie (und der Nachrichtendienste) eine wahre Revolution dar.

Während der öffentliche Schlüssel für jeden zugänglich gemacht wird (je mehr, desto besser), beruht die Sicherheit des Verfahrens auf der Geheimhaltung des privaten Schlüssels. Dieser darf niemals (weil es so wichtig ist, noch mal: niemals!) irgend jemandem zugänglich gemacht werden. Auch nicht der CA. Die bekommt nur den öffentlichen Schlüssel zu sehen.

Alle öffnen Alle schließen