LU07a - Zertifikate: Einführung

Grundlagen

Mit einem digitalen Zertifikat kann ein Rechner seine Identität beweisen. Wenn Sie eine gesicherte Webseite aufrufen, verlangt Ihr Browser das Zertifikat des Servers. Verfügt der Server über kein gültiges Zertifikat, so wird der Browser eine Warnung anzeigen.

Dadurch soll verhindert werden, dass sich ein Server für einen anderen Server ausgibt.

Analogie

Im täglichen Leben müssen Sie bei verschiedenen Gelegenheiten Ihre Identität angeben oder sogar beweisen. Betrachten wir einmal verschiedene Möglichkeiten.

Visitenkarte

Jeder kann eigene Visitenkarten erstellen. Dabei steht es Ihnen frei, welche Angaben Sie auf der Visitenkarte machen.

Ob die Angaben auf der Visitenkarte korrekt sind oder nicht, lässt sich nicht feststellen. Somit kann eine Visitenkarte nicht als Beweis der Identität (Authentifikation) dienen.

Kundenkarte

Viele Organisationen (Banken, Fitness-Studio, Detailhändler, ...) geben ihren Kunden eine Kundenkarte. Diese Kundenkarte wird von der jeweiligen Organisation erstellt.

Wer im Besitz der Kundenkarte ist, kann sich als Kunde dieser Organisation ausweisen. In einigen Fällen muss der Kunde zusätzlich einen Code (z.B. PIN) kennen.

Identitätskarte / Reisepass

Wenn Sie ins Ausland reisen möchten, müssen Sie Ihre Identität beweisen können. Eine Identitätskarte oder ein Reisepass wird vom Staat ausgestellt.

Eine Identitätskarte ist nur deshalb gültig, weil der Zollbeamte dem Aussteller (Schweizerische Eidgenossenschaft) vertraut. Er vertraut darauf, dass der Ausstellen die Identität der Person auf dem Ausweis geprüft hat.

Digitale Zertifikate

Vergleichen wir nun die digitalen Zertifikate mit den Beispielen aus dem Alltag. Ein Zertifikat besteht aus:

- Angaben zur Identität des Servers bzw. der Organisation.
- Informationen zur Zertifizierungsstelle, welche das Zertifikat ausgestellt hat.
- Angaben zum Schlüssel, welcher vom Server eingesetzt wird.

Self-signed Certificate

Ein „selbst-unterzeichnetes“ Zertifikat wird vom Ersteller unterschrieben. Wie bei einer Visitenkarte gibt es keine Garantie, dass die Angaben im Zertifikat stimmen. Es ist daher ein Kinderspiel, ein self-signed Certificate mit beliebigen Angaben zu erstellen.

Ein solches Zertifikat kann nur zwischen Rechnern der gleichen Organisation genutzt werden. Bei einem öffentlich zugänglichen Webserver führen solche Zertifikate immer zu Warnungen.

Zertifizerungsstellen

Jedes Zertifikat muss von einer Zertifizierungsstelle unterschrieben werden. Der Fachbegriff lautet „Certificate Authority“ oder kurz „CA“.

Es gibt weltweite eine grosse Anzahl von Firmen, die Zertifikate ausstellen oder unterschreiben. Damit ein solches Zertifikat von Ihren Browser akzeptiert wird, muss es von einer bekannten Zertifizierungsstelle unterschrieben sein. Dazu kennt jeder Browser eine Reihe von Zertifizierungsstellen, deren Unterschrift er vertraut. Zum Beispiel:

- https://www.swisssign.com/de / Dieses Unternehmen gehört zur Schweizerischen Post.

Sie können auch nachschauen, welchen Zertifizierungsstellen Ihr Browser vertraut.

Google Chrome

Einstellungen ⇒ Erweiterte Einstellungen ⇒ Zertifikate verwalten ...

Mozilla Firefox

Einstellungen ⇒ Erweitert ⇒ Zertifikate ⇒ Zertifikate anzeigen

---

m114-A0G