Die Fingerprints unserer SSL-Zertifikate

Verschiedene Nutzer waren verwundert darüber, dass wir auf unserer Webseite nicht die „**Fingerprints**“ (also den **Hashwert**) unserer SSL-Zertifikate von SwissSign veröffentlichen. Manche Webseiten machen das - wir jedoch nicht. Wenn man die Fingerprints von SSL-Zertifikaten überprüfen will, so macht man dieses, um ausschließen, dass sich ein Dritter („**Man-in-the-Middle**“) in die Verbindung eingeschaltet und die gesichert erscheinende Verbindung mit gefälschten Zertifikaten manipuliert hat.

Ein „**Man-in-the-Middle**“, dem solch eine Manipulation gelingen würde, könnte jedoch im gleichen Moment auch die Inhalte der Webseite verändern und dadurch auch den veröffentlichten SSL-Fingerprint gegen einen eigenen SSL-Fingerprint austauschen. Würde dann ein Benutzer die SSL-Fingerprints überprüfen, dann würden Ihm die manipulierten SSL-Fingerprints zu dem manipulierten Zertifikat passend erscheinen. Dieser Anwender würde darauf schließen, dass die Webseite authentisch ist und sich einer trügerischen (und darum gefährlichen) Sicherheit hingeben.

Wir von mailbox.org veröffentlichen unsere SSL-Fingerprints daher auf einem sicheren, dritten Kanal. Die dafür verwendete Technik heißt „**DANE**“ und veröffentlicht SSL-Fingerprints direkt im DNS-System der Domain. Damit hier ein „**Man-in-the-Middle**“ keine Möglichkeit hat, Manipulationen vorzunehmen, sind die dort veröffentlichten Daten über das „**DNSsec**“**-System** mittels eigener kryptographischer Signaturen geschützt. „**DANE / DNSsec**“ stellt darum ein sicheres, zweites und unabhängiges Medium dar, mit dem die Fingerprints der SSL-Zertifikate veröffentlicht werden können.

Moderne Browser - oder entsprechend moderne Plug-ins - können die „**DANE**“-Einträge einer Webseite überprüfen und den Nutzer z.B. durch eine farbliche Markierung über die Au-then-ti-zi-tät des SSL-Zertifikats informieren. Alternativ können Sie auf einen unabhängigen Dienst zur Verifikation des SSI Zertifikats zurückgreifen, der den entsprechenden DNS-Eintrag für Sie auslesen kann - zum Beispiel: https://www.huque.com/bin/danecheck.

Verwandte Artikel

- E-Mail-Adressen der eigenen Domain nutzen
- SSL-TLS-Verschluesselung bei mailbox.org
- Wird der Versand meiner E-Mail verschluesselt
- Die Fingerprints unserer SSL-Zertifikate
- Welche Daten wir speichern