WWW - Sichere Seiten

Bisweilen lösen sichere Webseiten in Ihrem Browser ein merkwürdiges Verhalten aus. Hier erfahren Sie einiges über die Hintergründe von HTTPS und Server-Zertifikaten.

Zertifikate der Uni FR CA

Bereits sehr viele geschützte Seiten im Web-Angebot der Universität Freiburg weisen sich dem Browser gegenüber mit einem Zertifikat aus, das von der **Zertifizierungsstelle der Universität Freiburg** (Uni FR CA) ausgestellt ist. Diese Zertifizierungsstelle wird im Rahmen der Public Key Infrastructure des Deutschen Forschungsnetzes (DFN) betrieben, das seine Zertifikate wiederum von der Wurzel-Zertifizierungsstelle (Deutsche Telekom Root CA2) der Deutschen Telekom AG beglaubigen lässt.

In der Liste der vertrauenswürdigen Zertifikatsanbieter im Internet Explorer ist diese Wurzelinstanz bereits eingetragen.

Das bedeutet, dass alle Zertifikate der Uni FR CA automatisch vom Internet Explorer (und Outlook / Express) als vertrauenswürdig eingestuft werden.

Beim Browser Mozilla Firefox ist die Deutsche Telekom in der Liste der vertrauenswürdigen Zertifikatsanbieter ab Version 3.0.12, bei Mozilla Thunderbird ab Version 2.0.0.23 ebenfalls eingetragen.

Falls Sie ältere Versionen betreiben, müssen Sie hier (falls noch nicht geschehen) die Wurzelzertifikate einmalig **importieren**, damit auch diese Programme alle Uni FR CA - Zertifikate auf Dauer für vertrauenswürdig halten.

Selbst erzeugte Zertifikate

Falls Sie eine Verbindung zu einem Server aufbauen wollen, der ein selbst generiertes Zertifikat übermittelt, können Sie den sich verweigernden Browser dazu „überreden“, das Zertifikat entweder nur für die laufende Sitzung (wenn z.B. keine späteren Verbindungen mehr geplant sind) oder auf Dauer als Vertrauenswürdig zu akzeptieren. Wie Sie das dürchführen, zeigen wir Ihnen an zwei Beispielen:

Für den Browser **Mozilla Firefox 3** und den **Microsoft Internet Explorer 7**.

Hintergrund

Sichere Webseiten beginnen mit **https:** und verwenden ein **digitales Zertifikat**, um die Authentizität der Webseite zu sichern. Die Sitzungsdaten laufen verschlüsselt über das Internet.

Beispiele:

https://ilias.uni-freiburg.de Lernplattform der Universität Freiburg

https://myaccount.uni-freiburg.de Die Seite der Benutzer-Selbstverwaltung des Rechenzentrums

Das digitale Zertifikat liefert beim Verbindungsaufbau u.a. Informationen über den Inhaber, die Internet-Adresse des Servers, die Gültigkeitsdauer des Zertifikates und den Aussteller mit.

Solche Zertifikate kann ein Dienstanbieter (z.B. das Rechenzentrum) entweder selbst erzeugen oder er kann die Echtheit der Zertifikate bei Zertifizierungsstellen kostenpflichtig bestätigen lassen. Viele dieser Zertfizierungsstellen sind in den verschiedenen Browsern in der Liste der vertrauenswürdigen Zertifizierungsstellen voreingetragen. Die Web-Browser akzeptieren nur solche Zertifikate automatisch, deren Herausgeber hier eingetragen sind. Zertifikate, deren Aussteller nicht in den Browser-Tabellen enthalten sind, werden nicht angenommen und für nicht vertrauenswürdig erklärt. Dies führt dazu, dass zahlreiche verschlüsselte Seiten von Servern (gerade auch von Universitäten) nicht sofort geöffnet werden, sondern eine Zwischenseite eingeblendet wird, die das Laden der gewünschten Seite zunächst verhindert.

Sicherheit - Artikelübersicht, Zertifikate - Artikelübersicht

From:
https://wiki.uni-freiburg.de/rz/ - **RZ**

Permanent link:
https://wiki.uni-freiburg.de/rz/doku.php?id=www_securepages

Last update: **2014/10/27 14:06**