

Überprüfung von Zertifikaten mit dem Mozilla Firefox

Zertifikate werden für die Überprüfung einer Identität oder andere sicherheitskritische Anwendungen benutzt. Woher wollen Sie wissen, dass dieses Zertifikat echt ist und nicht von einem Angreifer gefälscht wurde? Gewissheit erhalten Sie, indem Sie die eingetragenen Daten und den Fingerabdruck des Zertifikats überprüfen.

Die nachfolgende Anleitung soll Ihnen schrittweise helfen die Informationen sicher und schnell zu prüfen. Hierbei müssen Sie zwischen zwei Fällen unterscheiden:

1. Sie möchten das Zertifikat überprüfen, mit dem die Webseite geschützt ist.
2. Sie möchten das Zertifikat eines Ausstellers überprüfen.

Die Vorgehensweise wird exemplarisch am Zertifikat der RUBIcon-Download-Seite (Fall 1) und der CA der Ruhr-Universität Bochum (Fall 2) gezeigt. Für alle anderen Zertifikate können sie analog vorgehen.

Das Zertifikat „Ruhr-Universitaet Bochum CA“ ist von besonderer Wichtigkeit, da alle weiteren RUB-Zertifikate durch dieses generiert werden. Es bildet die Vertrauensbasis.

Fall 1 - Schritt 1

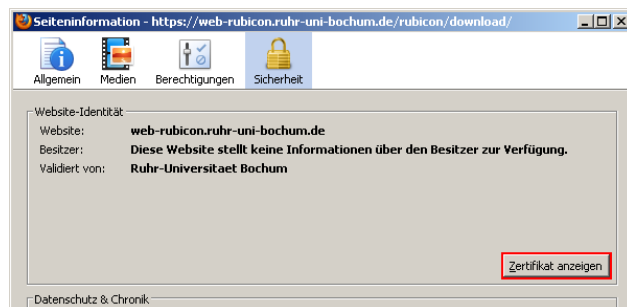
Sie befinden sich auf einer Seite, die durch ein Zertifikat gesichert ist (erkennbar z. B. durch das Präfix https).



Führen Sie einen Doppelklick mit der linken Maustaste auf das Schlosssymbol. Das Symbol befindet sich unten rechts im Browserfenster. Sie bekommen die Seiteninformationen zur Sicherheit angezeigt.

Schritt 2

Klicken Sie im oberen Drittel des Fensters auf Zertifikat anzeigen. Es öffnet sich die Zertifikat-Ansicht.



Schritt 3

Überprüfen Sie die Fingerabdrücke. In Ihren Unterlagen oder auf den Webseiten der Ruhr-Universität sollten die Fingerabdrücke zu diesem Zertifikat hinterlegt sein. Ist dies nicht der Fall, kontaktieren Sie bitte den jeweiligen Webseiten-Betreiber, um die Fingerabdrücke von einer vertrauenswürdigen Person zu erhalten.

Fingerabdrücke	
SHA1-Fingerabdruck	72:CE:04:54:62:38:11:37:D5:39:F8:1D:C5:DF:4D:47:18:46:AF:5C
MD5-Fingerabdruck	65:3A:8C:19:AE:AC:5E:80:AD:E3:75:A6:C5:13:02:E1

Zur Überprüfung müssen Sie den in der Zertifikat-Ansicht abgebildeten Fingerabdruck mit dem entsprechend angegebenen Abdruck (s. o.) vergleichen. Stimmen die Daten überein, können Sie der Webseite vertrauen. Stimmen die Fingerabdrücke nicht überein, verlassen Sie bitte nach Möglichkeit die Webseite. Geben Sie keine persönlichen Informationen ein und laden Sie keine Inhalte herunter!

Fall 2 - Schritt 1

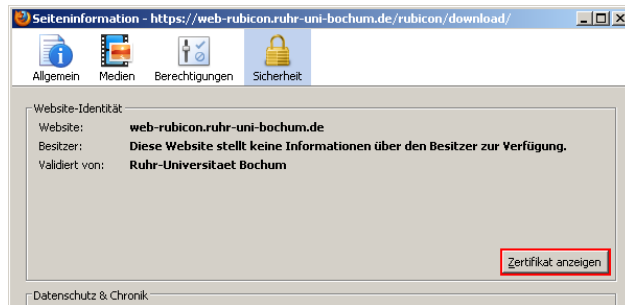
Sie befinden sich auf einer Seite, die durch ein Zertifikat gesichert ist (erkennbar z. B. durch das Präfix https). Sie möchten nun den Zertifikatsaussteller überprüfen.

Führen Sie einen Doppelklick mit der linken Maustaste auf das Schlosssymbol. Das Symbol befindet sich unten rechts im Browserfenster. Sie bekommen die Seiteninformationen zur Sicherheit angezeigt.



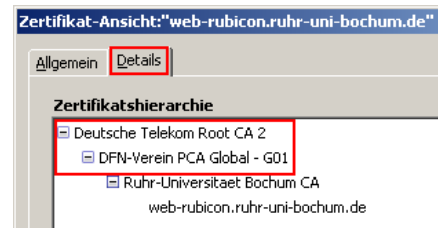
Schritt 2

Klicken Sie im oberen Drittel des Fensters auf Zertifikat anzeigen. Es öffnet sich die Zertifikat-Ansicht.



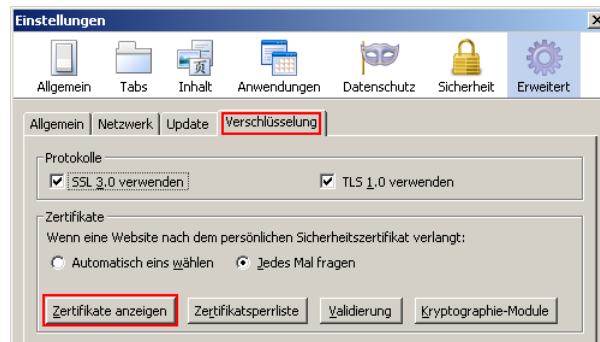
Schritt 3

Rufen Sie in der Zertifikat-Ansicht die Karte Details auf. Im oberen Drittel finden Sie die gesamte Zertifikatshierarchie. Lassen Sie das Fenster geöffnet oder notieren Sie sich die Hierarchie bis zu dem Zertifikat, das Sie überprüfen möchten. (In unserem Beispiel bis zur CA der Ruhr-Universität Bochum.)



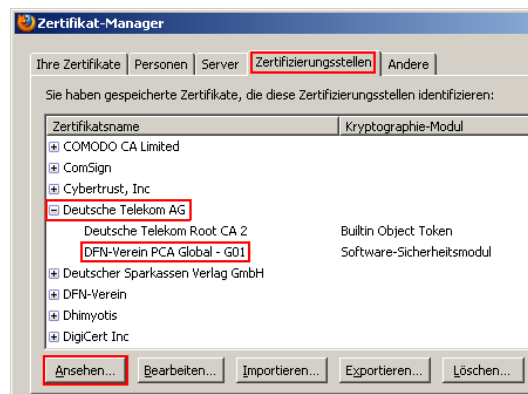
Schritt 4

Gehen Sie im Hauptfenster des Firefox auf Extras → Einstellungen. Wählen Sie das Symbol Erweitert aus, dann die Karte Verschlüsselung. Klicken Sie auf den Button Zertifikate anzeigen.



Schritt 5

In diesem Beispiel möchten Sie das Zertifikat des DFN-Verein überprüfen (s. Bild Schritt 3). Daher müssen Sie in der Karte Zertifizierungsstellen des Zertifikat-Manager nach der Deutschen Telekom AG suchen (s. Bild Schritt 3). Die Aussteller sind alphabetisch geordnet. Unter dem Eintrag der Deutschen Telekom sollten Sie dann den DFN-Verein finden.



Wählen Sie den DFN-Verein aus und klicken Sie auf Ansehen.

Schritt 6

Sie erhalten eine Ansicht über die Zertifikat-Informationen. Überprüfen Sie die Fingerabdrücke. In Ihren Unterlagen oder auf den Webseiten der Ruhr-Universität sollten die Fingerabdrücke zu diesem Zertifikat hinterlegt sein. Ist dies nicht der Fall, kontaktieren Sie bitte den jeweiligen Webseiten-Betreiber, um die Fingerabdrücke von einer vertrauenswürdigen Person zu erhalten.

Fingerabdrücke	
SHA1-Fingerabdruck	F0:28:8F:DA:C6:3A:F7:9A:31:9A:E9:72:F3:95:09:0E:A3:EF:E9:45
MD5-Fingerabdruck	CA:5A:00:CF:78:D1:4B:A7:E1:7F:DE:59:67:71:3A:BC

Zur Überprüfung müssen Sie den in der Zertifikat-Ansicht abgebildeten Fingerabdruck mit dem entsprechend angegebenen Abdruck (s. o.) vergleichen. Stimmen die Daten überein, können Sie der Webseite vertrauen. Stimmen die Fingerabdrücke nicht überein, verlassen Sie bitte nach Möglichkeit die Webseite. Geben Sie keine persönlichen Informationen ein und laden Sie keine Inhalte herunter!