Zertifikate (SSL-Zertifikate)

Definition SSL

SSL steht für *Secure Sockets Layer* und ist ein Verschlüsselungsprotokoll im TCP/IP-Protokollstapel.
Dabei soll ein SSL-Zertifikat als Identitätsnachweis dienen, da in diesem Zertifikat Informationen enthalten sind, mit dem ein Webbrowser und ein Server eine verschlüsselte Verbindung aufbauen können.
Es sei angemerkt, dass heutzutage der Nachfolger TLS (*Transport Layer Security*) verwendet wird, aber der alte Name weiterhin benutzt wird.

Das SSL Zertifikat

Was ist ein SSL-Zertifikat

Das Zertifikat enthält zahlreiche Informationen, wie unter anderem, den Namen des Ausstellers, Seriennummer oder aber auch den Fingerabdruck für die Verschlüsselung.
SSL-Zertifikate müssen von den Webseitenbetreiber auf dem Server installiert werden, damit ein Hoster ein Zertifikat erhält, muss dieser bei einer Zertifizierungsstelle anfragen. Diese Organisationen sind zur Ausstellung von SSL-Zertifikate berechtigt und verlangen auch für ihre Dienste Gebühren.

Wie funktioniert die Verschlüsselung

Es wird ein Public Key und ein Private Key, also ein öffentlicher und privater Schlüssel generiert. Diese werden verwendet, um den Datenverkehr zwischen Browser und Server zu verschlüsseln.

Arten von SSL-Zertifikaten

SSL-Zertifikate werden durch die Gründlichkeit der Überprüfung des Antragstellers und der Reichweite des Zertifikates unterschieden.

Überprüfung

Es wird zwischen drei Arten von Überprüfungen unterschieden, diese Kategorien unterscheiden sich auch stark an den Kosten des Zertifikates.
So sind Domain Validation Zertifikate teilweise kostenlos zu haben, so können z.B. Privatpersonen und kleinere Unternehmen die Kosten für ein Extended Validation Zertifikat oft nicht stemmen.

- Domain Validation (DV)

Überprüft, ob ein Webserver auch wirklich zu einer Domain gehört, das SSL-Zertifikat gibt Auskunft über eine E-Mail-Adresse des Hosters.
Der Überprüfungsvorgang kann vollständig automatisiert werden und wird deshalb von vielen nicht als sicher angesehen. Manche Browser markieren ein DV-SSL-Zertifikat als gering Sicher im Vergleich zu den anderen Zertifikat-Arten.

- Organization Validation (OV)

Bei der Ausstellung eines OV-Zertifikates fordert die Zertifizierungsstelle Unterlagen vom Besitzer der Webseite an. Diese angeforderten Unterlagen können unter anderem einen Handelsregisterauszug beinhalten. Dadurch ist die Identität besser sichergestellt, als bei einem DV-Zertifikat.

- Extended Validation (EV)

Bei diesem Zertifikat wird die Domain und die Organisation hinter der Domain, aber auch der Antragsteller selbst kontrolliert. Dabei wird überprüft, ob der Antragsteller bei der Organisation arbeitet und überhaupt die Berechtigung hat, ein solches Zertifikat anzufragen. Außerdem muss die Stelle, die die Zertifikate ausstellt, eine Überprüfung des CA/Browser-Forums standhalten.

Digitale Signatur (RSA)

Was ist RSA?

Rivest-Shamir-Adleman, ein viel benutztes Verschlüsselungssystem für den sicheren Datenverkehr. RSA ist auch nebenher das älteste Verfahren.
Der Name kommt von den Nachnamen, der Personen, die das entwickelt haben. Sie heißen: Ron Rivest, Adi Shamir und Leonard Adleman.

Wann wurde RSA das erste mal Veröffentlicht?

1973 wurde geheim ein äquivalentes System von GCQH von Clifford Cocks entwickelt (the british signals intelligence agency). 1977 ist RSA jedoch erst veröffentlicht worden.

Wie funktioniert RSA?

In einem Public-Key-Kryptosystem ist der Verschlüsselungsschlüssel öffentlich und unterscheidet sich vom Entschlüsselungsschlüssel (decryption key), der geheim gehalten wird (privat). Ein RSA-Benutzer erstellt und veröffentlicht einen öffentlichen Schlüssel (public key) basierend auf zwei großen Primzahlen zusammen mit einem Hilfswert. Die Primzahlen werden geheim gehalten. Nachrichten können von jedem über den öffentlichen Schlüssel verschlüsselt werden, können aber nur von jemandem dekodiert werden, der die Primzahlen kennt. Die Sicherheit von RSA beruht auf der praktischen Schwierigkeit, das Produkt zweier

großer Primzahlen zu faktorisieren, dem "Factoring-Problem". Das Brechen der RSA-Verschlüsselung wird als RSA-Problem bezeichnet. Ob es so schwierig ist, wie das Factoring-Problem, ist eine offene Frage. Es gibt keine veröffentlichten Methoden, um das System zu besiegen, wenn ein ausreichend großer Schlüssel verwendet wird.

Nachteil RSA

RSA ist ein relativ langsamer Algorithmus, weshalb er nicht wirklich für Benutzer-Daten Entschlüsselung verwendet wird. RSA wird meist benutzt um einen Shared-Key für eine symmetrische Kryptografie zu benutzen.