SSL-Zertifikate: Ein „Reisepass“ für Webseiten

Heute werden mehr und mehr Geschäfte via Internet abgewickelt – vom Reißnagel bis zur Weltreise kann man dort mittlerweile alles kaufen, verkaufen, tauschen oder versteigern. Dabei ist es von essentieller Bedeutung, dass diese Transaktionen sicher durchgeführt werden können. Und nicht nur, wenn es ums Geld geht, ist Sicherheit wichtig: Vertrauliche Daten werden ebenfalls zunehmend im bzw. über das Internet transportiert, und private eMails, Dokumente und Ähnliches sollen natürlich auch vertraulich bleiben und nicht von jedermann abgehört werden können.

Was sind SSL-Zertifikate?

Im WWW hat sich als Standard für sichere Datenverbindungen das Protokoll HTTPS auf Basis von TLS/SSL etabliert (siehe Artikel *WWW + SSL = HTTPS* auf Seite 46 und *Was ist TLS/SSL?* auf Seite 43). Ein wesentlicher Teil dieses Konzepts sind die so genannten SSL-Zertifikate, die nähere Angaben über die Server enthalten, mit denen man Verbindung aufgenommen hat.

Ein Zertifikat soll vor allem sicherstellen, dass der Eigentümer einer Webseite auch wirklich der ist, der er zu sein vorgibt. Jedes Zertifikat ist signiert; wie viel das Zertifikat wert ist, hängt natürlich davon ab, wer es signiert. Im Prinzip ist es auch möglich, ein Zertifikat selbst zu signieren. Ein solches Zertifikat ist als Nachweis der Identität allerdings ungeeignet, deshalb präsentieren Webbrowser und andere Klientenprogramme den BenutzerInnen jedesmal ein Pop-up-Fenster mit einer Warnung, wenn ein solcherart zertifizierter Server aufgerufen wird.

Aus diesem Grund lassen seriöse Anbieter von sicheren Webseiten ihre Zertifikate von „Vertrauenswürdigen Dritten“ erstellen, deren Signatur in den Webbrowsern verankert ist. Derartige CAs (*Certificate Authorities*) gibt es fast wie Sand am Meer, allerdings unterscheiden sie sich zum Teil sehr in der Qualität des Service, der Verifikation des Zertifikatsbestellers und damit der „Vertrauenswürdigkeit“ des Zertifikats. Nicht zuletzt unterscheiden sich die CAs auch beim Preis: Ein Zertifikat kann durchaus mit mehreren hundert Euro zu Buche schlagen.

Auch für eine Universität, die zwar nicht im eCommerce tätig ist, sehr wohl aber eine Unzahl von Services bietet, die ebenfalls mit Verschlüsselung angeboten werden (müssen), kann das schnell sehr teuer und sehr aufwendig werden.

SCS – Der Anfang

Da sich viele Universitäten in dieser misslichen Lage befinden, lag es nahe, sich gemeinsam um günstigere Zertifikate für die Bildungseinrichtungen zu bemühen. Unter der Schirmherschaft von TERENA (dem Dachverband der europäischen Wissenschaftsnetze, `www.terena.nl`) schlossen sich daher im Jahr 2004 acht Wissenschaftsnetze[1)] zusammen, um ein Service für „Pop-Up Free SSL Certificates“ für die europäischen Universitäten aufzubauen – das Projekt **SCS (*Server Certificate Service*)** war geboren.

Die Idee war, eine Certificate Autority zu finden, die imstande ist, mit der großen Zahl an potentiell benötigten Zertifikaten umzugehen und diese auf Basis der Gesamtmenge möglichst kostengünstig anzubieten. Die administrative Tätigkeit des Verifizierens der Anträge sollte dabei jedoch in der Hand der einzelnen Wissenschaftsnetze bleiben. Da das SCS-Projekt für die kommerziellen Zertifizierungsstellen Neuland war, musste für dieses Projekt einiges an Vorarbeiten geleistet werden. TERENA entschloss sich deshalb im Sommer 2005, eine Ausschreibung für dieses Service zu starten. Etliche Firmen haben auch Angebote eingebracht, sodass im Herbst mit allen interessierten Unternehmen konkrete Gespräche geführt werden konnten.

Im Dezember 2005 wurde schließlich die Firma Globalsign (`www.globalsign.com`) als „Bevorzugter Anbieter“ ausgewählt, und am 9. Jänner 2006 konnte der Vertrag zwischen TERENA und Globalsign unterzeichnet werden (siehe `www.terena.nl/activities/tf-emc2/scs.html`). Im Februar und März 2006 galt es dann, die technischen Rahmenbedingungen zu schaffen, um die neuen Zertifikate den einzelnen KundInnen möglichst unkompliziert zur Verfügung stellen zu können.

SCS – Status quo

Auch das österreichische Wissenschaftsnetz ACOnet hat im Laufe des März die nötigen Vorbereitungen getroffen, um das *Server Certificate Service* allen ACOnet-Teilnehmern zugänglich zu machen (Näheres siehe `www.aco.net`). Auf Basis dieses Service ist es nun für die ServerbetreiberInnen an Österreichs Bildungseinrichtungen erstmals möglich, SSL-Zertifikate ohne Lizenzkosten ausstellen zu lassen. Innerhalb der Universität Wien können wir das Service an Institute und Dienststellen weitergeben; dadurch profitieren auch jene Server von diesen Zertifikaten, die von den Instituten selbst betrieben werden.

Mittels SCS lässt sich im Prinzip jedes Service zertifizieren, das TLS/SSL nutzt; allerdings muss der Domain-Name, unter

1) ACOnet (Österreich), CARNet (Kroatien), CESNET (Tschechien), RENATER(CRU) (Frankreich), RedIRIS (Spanien), SURFnet (Niederlande), SWITCH (Schweiz) und UNI-C (Dänemark)

dem der Server läuft, auf die Universität Wien registriert sein. Jeder Serverbetreiber kann die benötigten Zertifikate selbst beantragen. Nach einer Bestätigung des Antrags durch den von der Universität authorisierten Ansprechpartner – den so genannten *Proxy* – wird das Zertifikat von der im ACOnet angesiedelten *Registration Authority* (RA) freigegeben und dann sofort vom Globalsign-System ausgestellt.

Eine genaue Beschreibung der Voraussetzungen und des Anmeldevorgangs finden Sie im Artikel *Der Weg zum SSL-Zertifikat für Uni-Server* auf Seite 44.

Fazit

Nachdem die Frage der Zertifizierungskosten dank SCS keine ausschlaggebende mehr ist, entfällt der wichtigste Grund, SSL nicht zu verwenden. TLS/SSL – bzw. ganz allgemein der Einsatz verschlüsselter Übertragungsprotokolle – ist heute im Interesse der Security schon fast ein Muss, und dieses Service bietet die Gelegenheit, im universitären Bereich eine möglichst flächendeckende Verschlüsselung einzuführen.

Ulrich Kiermayr ■

Was ist TLS/SSL?

Bei TLS (*Transport Layer Security*) oder SSL (*Secure Sockets Layer*) handelt es sich um ein Verschlüsselungsprotokoll zur Datenübertragung im Internet bzw. um eine verschlüsselte Netzverbindung zwischen Server und Client, über die auch unverschlüsselte Anwendungsprotokolle (z.B. HTTP, POP3, IMAP, SMTP, NNTP, SIP, ...) sicher transportiert werden können.

TLS/SSL sorgt also dafür, dass die Daten verschlüsselt über das Netz geschickt werden und somit vor unerwünschten Zugriffen und Manipulationen geschützt sind. Es sichert jedoch nur den Übertragungsweg zwischen Server und Client; auf alles, was davor oder danach mit den Daten geschieht, hat TLS/SSL keinen Einfluss.

Warum zwei Namen?

SSL Version 1.0 wurde 1994 von der Firma Netscape entwickelt. Als SSL 3.0 schließlich 1999 vom Standardisierungs-Gremium IETF (*Internet Engineering Task Force*) im RFC 2246[1)] als *Proposed Standard* festgelegt wurde, benannte man es auf TLS um. Die Unterschiede zwischen SSL 3.0 und TLS sind minimal; umgangssprachlich wird daher meistens weiterhin der Begriff SSL verwendet.

Wie funktioniert SSL?

Bei SSL kommen verschiedene kryptographische Methoden[2)] zum Einsatz:

- **Symmetrische Verschlüsselung**: Hierbei wird für die Ver- und Entschlüsselung der Daten derselbe Schlüssel (*Key*) verwendet.
- **Asymmetrische Verschlüsselung**: Asymmetrische Verfahren benutzen zwei verschiedene Schlüssel zum Ver- und Entschlüsseln – einen öffentlichen (*Public Key*) und einen geheimen (*Private Key*).
- **Hash-Funktion**: Damit wird ein „digitaler Fingerabdruck" mit einer konstanten Länge (128 bis 512 Bit, abhängig vom verwendeten Algorithmus) erstellt, anhand dessen kontrolliert werden kann, ob die übermittelten Daten am Weg zum Empfänger verändert wurden.

Das SSL-Protokoll selbst besteht aus zwei übereinanderliegenden Schichten:

- Auf der unteren Schicht befindet sich das ***SSL Record Protocol***. Dieses prüft, ob die übertragenen Daten vollständig und unverändert ihren jeweiligen Empfänger erreichen und verschlüsselt, sofern dies gewünscht wird, die Daten mit einem symmetrischen Verfahren. Der dabei verwendete Schlüssel wird über das *SSL Handshake Protocol* vereinbart.
- Die obere Schicht enthält unter anderem das ***SSL Handshake Protocol***.[3)] Dieses baut auf dem *SSL Record Protocol* auf und wird einerseits zum Aushandeln der verwendeten kryptographischen Algorithmen und Schlüssel benötigt, andererseits zur Identifikation und Authentifizierung der Kommunikationspartner mit Hilfe asymmetrischer Verschlüsselungsverfahren (in der Regel authentifiziert sich zumindest der Server gegenüber dem Client).

Susanne Kriszta ■

1) siehe `www.ietf.org/rfc/rfc2246.txt` (mittlerweile abgelöst durch RFC 4346, `www.ietf.org/rfc/rfc4346.txt`)

2) Detailliertere Informationen zu den einzelnen Methoden finden Sie z.B. im Artikel *Grundbegriffe der Kryptographie* in *Comment 00/3*, Seite 20 bzw. unter `www.univie.ac.at/comment/00-3/003_20.html`.

3) Neben dem *SSL Handshake Protocol* umfasst die obere Schicht auch noch das *SSL Application Data Protocol*, das *SSL Alert Protocol* und das *SSL Change Cipherspec. Protocol*, die ebenfalls ihr Scherflein zu einer sicheren Datenübertragung beisteuern, hier jedoch nicht näher beschrieben werden.