Zertifikate im Einsatz – Ein Beitrag zu mehr Sicherheit

Steffen Platzer | Computer- und Medienservice, Hard- und Softwareservice | steffen.platzer@cms.hu-berlin.de

X.509-Zertifikate (im Weiteren Zertifikate) werden in asymmetrischen Kryptoverfahren verwendet. Dabei besitzt jede der kommunizierenden Parteien ein Schlüsselpaar, welches aus einem geheimen Teil (privater Schlüssel) und einem nicht geheimen Teil (öffentlicher Schlüssel) besteht. Der private Schlüssel ermöglicht es seinem Inhaber zum Beispiel, Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren. Der öffentliche Schlüssel ermöglicht es jedermann, Daten für den Schlüsselinhaber zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Ein Zertifikat ist der Nachweis, dass ein öffentlicher Schlüssel einer bestimmten Person, Einrichtung oder einem Server gehört.

Was beinhalten Zertifikate und wer stellt sie aus?

Herausgegeben werden Zertifikate durch vertrauenswürdige Instanzen, sog. Zertifizierungsstellen (Certificate Authority – CA). Zertifizierungsstellen sind hierarchisch aufgebaut. Das heißt es gibt eine Wurzelinstanz mit einem selbstsignierten Wurzelzertifikat (z. B. Deutsche Telekom Root CA 2) und eine oder mehrere durch diese zertifizierte sog. Zertifizierungsstellen, welche die Zertifikate für die Endteilnehmer ausgeben. Dabei wird der öffentliche Schlüssel des Inhabers mit dem Zertifikat der Zertifizierungsstelle signiert und das Zertifikat für den Schlüsselinhaber ausgestellt. Dem geht voraus, dass sich die Zertifizierungsstelle von der Identität des Inhabers des öffentlichen Schlüssels nach gewissen Regeln (CSP/CP) überzeugt. Bei positiver Prüfung wird ein Zertifikat ausgestellt.

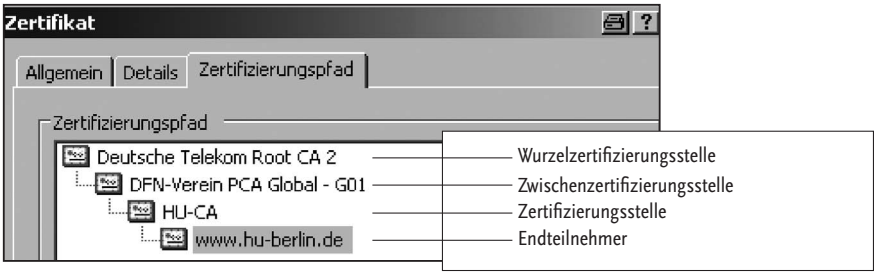

Abb.1: Zertifikatshierarchie

Zertifikate sind sozusagen digitale Identitäten von Personen, Servern oder möglicherweise auch von Einrichtungen (z. B. einer Poststelle). Es enthält u.a. folgende Informationen:

- Seriennummer des Zertifikates und Zertifikatsversion
- den Namen des Zertifikatausstellers (Zertifizierungsinstanz)
- den eindeutigen Namen des Eigentümers des öffentlichen Schlüssels (z. B. eine Person oder ein Webserver)
- Informationen zur Gültigkeitsdauer des Zertifikates
- zusätzliche Informationen zum Zertifikatinhaber
- Angaben zum Verwendungszweck des Zertifikates
- den öffentlichen Schlüssel des Zertifikatinhabers selbst
- Angaben zur Signatur der Zertifizierungsstelle

Zweck ist es also, einem öffentlichen Schlüssel zweifelsfrei eine Identität zuzuordnen. Diese eindeutige Verbindung wird durch die Zertifizierungsstelle durch Ausstellen des Zertifikates bestätigt, d.h., dass die Zertifizierungsstelle als Vertrauensanker für Identitäten dient.

Sollte ein privater Schlüssel zu einem Zertifikat nicht mehr sicher sein, wird das Zertifikat durch die Zertifizierungsstelle gesperrt. Dieses gesperrte Zertifikat wird auf einer Certificate Revocation List (CRL) veröffentlicht.Damit das ausgestellte Zertifikat in den Anwendungen auf Gültigkeit überprüft werden kann,

ist es erforderlich, dass die Zertifikate der Zertifizierungsstellen bekannt sind. Unter Umständen müssen die Zertifikate der Zertifizierungsstellen nachinstalliert werden.

Achtung: Gehen Sie mit der Installation von zusätzlichen Vertrauensankern (Stamm- oder Wurzelzertifizierungsstellen) sorgsam um. Allen durch diese Zertifizierungsstellen ausgestellten Zertifikaten wird somit vertraut.

Zertifikate an der HU

Die Zertifizierungsinstanz der HU „HU-CA“ ist in die Hierarchie des DFN-Vereins eingebettet, welcher das Wurzelzertifikat „Deutsche Telekom Root CA 2“, oder „DFN-Verein PCA Classic-G01“ zugrunde liegt (siehe Bild „Zertifikatshierarchie“). Sie stellt Endteilnehmer-Zertifikate für Angehörige der HU sowie für Server der HU aus.

Verwendet werden die ausgestellten Zertifikate an der HU zur sicheren Identifizierung von Webservern, Mailservern, VPN-Gateways und WLAN-Authentifizierungsservern. Diese werden von den jeweiligen Verantwortlichen/Administratoren über ein Webformular beantragt. Persönliche Zertifikate für elektronische Signaturen, Authentifizierungen und Verschlüsselungen werden für Angehörige der HU auf der HU-CA Smartcard zur Verfügung gestellt. Hierfür erfolgt die Beantragung über ein Webformular, wobei die Smartcard nach der Herstellung persönlich an den Inhaber übergeben wird. Dabei erfolgt dann auch die Identifizierung des Antragstellers. Mehr Informationen dazu finden Sie hier: http://www.cms.hu-berlin.de/dl/zertifizierung/SC/SC-Antrag_html

Einsatz für abhörsichere und authentische Verbindungen zu Webservern

Die HU setzt auf vielen Webservern Zertifikate ein, um die Kommunikation mit den anfragenden Webbrowsern sicher zu gestalten. Des Weiteren sollen sich diese auch als Webserver der HU authentifizieren (in Zeiten von Phishing-Attacken immer bedeutungsvoller). Insbesondere Webseiten, die die Eingabe von sensiblen Daten erfordern, müssen es ermöglichen, sichere und geschützte Verbindungen zu ihnen aufzubauen.

Geschützte Webseiten erkennen Sie an der Verwendung des HTTPS-Protokolls. HTTPS dient zur Verschlüsselung und zur Authentifizierung der Kommunikation zwischen Webserver und Browser. Zudem zeigt Ihnen Ihr Browser bei bestehender HTTPS-Verbindung ein geschlossenes Schloss in der Adress- und/oder Statusleiste an (Abb. 2).

Abb. 2: bestehende HTTPS-Verbindung

Dafür ist es erforderlich, dass die Zertifizierungsstelle, die das Zertifikat des Webservers ausgestellt hat, im Zertifikatsspeicher des Browsers als vertrauenswürdig eingetragen ist. Falls nicht, müssen Sie das Wurzelzertifikat nachinstallieren. Lesen Sie dazu auch den Beitrag: „Sicherheitseinstellungen für Webbrowser“.

Machen Sie sich deutlich: Wenn Sie kein HTTPS verwenden, werden Ihre Daten im Klartext übermittelt. Insbesondere bei der Nutzung offener Netze (z. B. WLAN) sind Ihre Daten lesbar.

Wenn Sie eine HTTPS-Verbindung zu einem Webserver aufbauen wollen, läuft ein sog. SSL-Handshake-Verfahren ab. Wie geschieht das nun?

1. Ihr Browser übermittelt eine Zufallszahl und die Verschlüsselungsverfahren, die er beherrscht, an den Server.
2. Der Server übermittelt sein Zertifikat (weist sich also aus), ebenfalls die Verschlüsselungsverfahren, die er kann, eine Zufallszahl und eine Session-ID.
3. Der Browser wählt das Verschlüsselungsverfahren (i.d.R. das Stärkste) für die weitere Kommunikation und er validiert das Zertifikat des Servers. Sollte dies fehlschlagen, kommt die Verbindung nicht zustande.
4. Ihr Browser berechnet unter Verwendung des gewählten Verschlüsselungsverfahrens und der übermittelten Zufallsdaten des Servers einen sog. Premaster-Schlüssel. Dieser Premaster-Schlüssel wird mit dem öffentlichen Schlüssel des Servers verschlüsselt und an den Server geschickt.
5. Der Server kann jetzt unter Verwendung seines privaten Schlüssels den Premaster-Schlüssel entschlüsseln.

Empfehlung:
Vergewissern Sie sich, mit wem Sie es zu tun haben. Vertrauliche Informationen sollten Sie nur preisgeben, wenn die Webseite auch die ist, die Sie wollen.

Vorgehen:
Überprüfen Sie dazu das Zertifikat der Gegenstelle. Klicken Sie auf das Schloss in oder neben der Adressleiste in Ihrem Browser. Sie erhalten dann die Sicherheitsinformationen über die bestehende Verbindung zu der Webseite. In Abb. 3 sehen Sie das verwendete Verschlüsselungsverfahren und den Namen der Webseite, wie er auch im Zertifikat beglaubigt ist.

Wo lauern Gefahren:
Verwenden Sie möglichst keine Links aus Ihnen zugesandten E-Mails. Oftmals verbergen sich dahinter Phishing-Attacken, mit denen versucht wird, Sie auf andere Webseiten „umzulenken“ und Ihnen dort Zugangsdaten und/oder TANs zu entlocken. Achten Sie darauf, dass tatsächlich eine HTTPS-Verbindung besteht

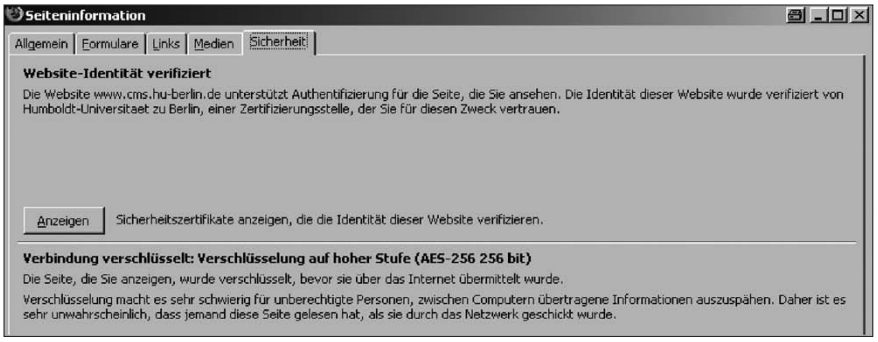

Abb. 3: Sicherheitsinformationen der Verbindung

(geschlossenes Schloss, meist eingefärbte Adressleiste). Sollte Ihrem Browser die Zertifizierungsinstanz, die das Zertifikat ausgestellt hat, nicht bekannt sein (Wurzelzertifikat ist nicht installiert oder nicht vertrauenswürdig), wird Ihnen angeboten, das Zertifikat zumindest für diese Sitzung zu akzeptieren. Klicken Sie nicht immer gleich auf „Akzeptieren“, sehen Sie sich das übermittelte Zertifikat an und überprüfen Sie den Aussteller des Zertifikates.

Einsatz zur sicheren Authentifizierung

Hierfür können Sie Ihre persönliche HU-CA Smartcard einsetzen. Der darauf vorhandene Krypto-Chip enthält Ihr persönliches Zertifikat, in dem u. a. Ihr Anmeldeaccount eingetragen ist, wenn Sie das bei der Beantragung Ihrer HU-CA Smartcard mit angegeben haben. Die Anmeldung erfolgt dann mittels Ihres auf der Smartcard befindlichen Zertifikates und des Nachweises der Berechtigung zur Nutzung des privaten Schlüssels, indem Sie die gültige PIN wissen.

Sie können sich an folgenden HU-Domänen mit Ihrer HU-CA Smartcard anmelden, wenn Sie darin einen gültigen Account haben: AGRAR, ASA, BIOLOGIE, CMS, EDUCAT, GEO, GERMAN, IFG, PSYCHOLOGIE, PUBLIC, SOWI, SPRACHEN, SPZ, STUDENT, SUB, UB, USER.

Voraussetzung ist ein Windows Client in den Versionen Vista, XP Professional oder Windows 2000 Professional, welcher sich in einer der o. g. HU-Domänen befindet, mit angeschlossenem Smartcard Reader und installiertem Treiber. Des Weiteren muss die HU-CA-Smartcard-Software einmalig installiert werden. Anleitungen finden Sie unter: http://www.cms.hu-berlin.de/dl/zertifizierung/SC/fertig/fertig_htm#2.0 Danach sieht Ihr Anmeldebildschirm so aus:

Abb. 4: mögliche Anmeldung mit HU-CA Smartcard

Wenn Sie dann Ihre HU-CA Smartcard in den Reader stecken, werden Sie zur Eingabe Ihrer PIN aufgefordert. Bei richtiger Eingabe werden Sie mit Ihrem Account angemeldet (siehe Abb. 5).

Abb. 5: Aufforderung zur PIN-Eingabe

An den Öffentlichen Computerarbeitsplätzen des CMS sind diese Voraussetzungen bereits erfüllt. Hier können Sie sich sofort mit Ihrer HU-CA Smartcard anmelden. Klicken Sie dazu auf das Icon „Anmelden mit Account/Smartcard“ auf dem Desktop und stecken Sie Ihre HU-CA Smartcard in den Kartenleser. Nach gültiger Eingabe Ihrer PIN erfolgt die Anmeldung mit Ihrem persönlichen Account. Wenn Sie die Smartcard aus dem Reader ziehen, werden Sie abgemeldet und Ihre Session wird beendet.

Vorteile:

- Erhöhung der Sicherheit in Bezug auf Authentifizierung durch 2-Faktor-Authentifizierung, d. h. Besitz der Smartcard und Wissen der PIN.
- Sichere Anmeldung an der Domäne, es wird kein Anmeldepasswort übermittelt.

Durch das Ziehen der Smartcard erfolgt entweder die Abmeldung vom oder die Sperrung des Rechners.

Nachteil:
Die Anmeldung dauert etwas länger als gewöhnlich, ca. 20 Sekunden.

Einsatz zur Verschlüsselung von Daten

Das Zertifikat der HU-CA Smartcard kann für die Verschlüsselung von Daten verwendet werden. Da die Verwendung der windowseigenen Dateiverschlüsselung EFS (Encrypting File System) sehr kompliziert ist und nur auf Ordnerebene funktioniert, haben wir nach anderen Möglichkeiten gesucht.

Als Verschlüsselungssoftware, die sich auf Notebooks in der Verwaltung im Einsatz befindet, haben wir uns für „Safe Guard Private Disk“ von Utimaco entschieden. Hierbei wird nach Einstecken der HU-CA Smartcard ein verschlüsseltes Laufwerk gemountet, auf dem die Daten verschlüsselt gespeichert werden. Zur Vereinfachung kann ein konstanter Laufwerksbuchstabe z. B. S: vergeben werden und nach Anpassung des Standard-Speicherpfades werden Daten immer auf dem verschlüsselten Laufwerk gespeichert.

Eine Anleitung zur Installation und Konfiguration finden Sie hier: http://www.cms.hu-berlin.de/dl/zertifizierung/SC/Anwendungen/Verschluesseln_html Eine Übersicht über ein konfiguriertes verschlüsseltes Laufwerk finden Sie in der Abb. 6.

In Ihrem Explorer haben Sie dann ein zusätzliches Laufwerk mit den angegebenen Parametern zur Verfügung. Hier können Sie die Daten ablegen, die Sie vor fremdem Zugriff schützen wollen (siehe Abb. 7).

Einsatz in der E-Mail-Kommunikation

Die Anonymität der Internetbenutzer ist in vielen Bereichen sicher gern willkommen. Im E-Mail-Verkehr allerdings möchte man schon wissen, mit wem man kommuniziert. Spam- und Phishingmails, bei denen die Absenderadresse gefälscht ist, belästigen uns heute schon zur Genüge. Beim Einsatz von elektronischen Signaturen mittels vertrauenswürdiger Zertifikate weiß man, mit wem man „spricht“.

Normalerweise werden E-Mails mit der Vertrautheit von Postkarten übertragen, wenn dann noch die Netze offen sind, wie das Internet, gibt es überhaupt keine Vertraulichkeit mehr. Unverschlüsselte E-Mails können an jedem Punkt auf dem Übertragungsweg gelesen werden. Inhalte können verändert werden.

Deshalb sollten Sie E-Mails mit vertraulichen Informationen unbedingt verschlüsselt übermitteln. Dazu benötigen Sie das Zertifikat Ihres Kommunikationspartners. Damit die E-Mail auch unverfälscht ihren Empfänger erreicht und dieser auch weiß, von wem sie kommt,

Abb. 6: Konfigurationsübersicht PrivateDisk

Abb. 7: verschlüsseltes Laufwerk

sollten Sie Ihre E-Mail auch signieren. Setzen Sie dafür Ihre HUCA Smartcard ein. Lesen Sie dazu den Artikel „Sichere Konfiguration von Mailclients“.

Einsatz in der Dokumentensignatur/ -verschlüsselung

Ein bisher leider unterschätztes Einsatzfeld ist die Signatur von elektronischen Dokumenten. Mit dem Zertifikat der HU-CA Smartcard können Dokumente in MS-Word (ab Version 2003) und Adobe Acrobat (ab Version 6) digital signiert werden.

Ein Vorteil liegt in der medienbruchfreien Weiterverarbeitung von Dokumenten, die unterschrieben oder von mehreren Bearbeitern bearbeitet bzw. unterschrieben werden müssen. So ist es z. B. möglich, ein PDF-Dokument mehrfach zu signieren und so lange Postwege auszuschließen.

Des Weiteren besteht die Möglichkeit, ein PDF-Dokument unter Verwendung des Zertifikates des oder der Empfänger zu verschlüsseln. Das Dokument kann dann nur durch die berechtigten Empfänger unter Einsatz ihrer HU-CA Smartcard geöffnet werden.

Eine Anleitung zum Einsatz der HU-CA Smartcard in Adobe Acrobat finden Sie hier: http://www.cms.hu-berlin.de/dl/zertifizierung/SC/Anwendungen/acrobat_html

Ausblick

Es ist vorgesehen, Zertifikate auch für sichere Authentifizierungen von mobilen Endgeräten wie z. B. PDAs am WLAN der HU einzusetzen. Dabei sollen diese Geräte, mit einem Zertifikat ausgestattet, im 802.1X WLAN authentifiziert werden.