Automatische SSL-Zertifizierung

Henning Mohren

FernUniversität in Hagen
Universitätsrechenzentrum
58084 Hagen
henning.mohren@fernuni-hagen.de

Zusammenfassung: Die Akzeptanz und Verbreitung von PKI-Lösungen (Public Key Infrastructure) nimmt in den letzten Jahren zwar zu, ein Durchbruch ist jedoch bisher nicht gelungen. Ein Grund dafür ist das aufwändige und für den Endanwender schwer zu durchschauende Verfahren, um an ein SSL-Zertifikat zu gelangen.

Die hohen Sicherheitsanforderungen einer qualifizierten Zertifizierung stehen derzeit dem flächendeckenden Einsatz entgegen. Um die Akzeptanz von PKI-Lösungen zu erhöhen, bieten sich – sowohl im universitären als auch im außeruniversitären Umfeld – Zertifikate, das sind elektronische Identitätsbescheinigungen für Personen und Maschinen, die den Personen oder Maschinen eindeutig Signaturprüfschlüssel zuordnen, an. Solche Zertifikate können auch in automatisierten Verfahren ausgestellt werden.

Dieser Artikel beschreibt die zur automatisierten Vergabe von Zertifikaten erforderlichen Verfahrensweisen und Sicherheitsvorkehrungen.

1 Public Key Infrastrukturen

Das Internet ist – bedingt durch seinen Aufbau und die ihm zu Grunde liegenden Strukturen – unsicher. Einige Ursachen dafür sind

- unbefriedigende Sicherheitskonzepte der eingesetzten Betriebssysteme, Netzprotokolle und Middleware-Implementierungen,
- stark wachsende Funktionalität und Flexibilität und daher Komplexität auf allen Ebenen,
- fehlerbehaftete Implementierungen und natürlich
- menschliche Fehler und Sabotageversuche.

Um diese Fehlerquellen zu bekämpfen, werden zahlreiche Verfahren angewendet – alle mit dem Ziel, im Internet „mehr Sicherheit“ zu erzielen. In diesem Zusammenhang können als Beispiele Virenscanner, Firewalls, Verschlüsselungsverfahren, aber auch organisatorische Maßnahmen, wie schnelle Reaktionsweisen auf erkannte Probleme (CERT-Verbund[1], ...) aufgeführt werden.

Viele der schon seit langem bekannten Verfahren werden im Internet in einem neuen Kontext betrachtet. Dazu gehört unter anderem auch das Verlangen, seine Kommunikationspartner sicher zu identifizieren.

[1] Computer Emergency Response Team, http://www.cert-verbund.de

Diese „sichere Identifikation“ kann z.B. durch Verwendung einer „Public Key Infrastructure (PKI)“ gewährleistet werden. Eine PKI verhilft ihren Benutzern dazu, ein normalerweise unsicheres Medium, wie das Internet, sicher zu nutzen.

Vertraulichkeit[2], Datenintegrität[3], Authentizität[4] und die Nicht-Bestreitbarkeit von Aktionen, die auf PKI-Basis ausgeführt wurden, sind die Vorteile, die man durch PKI-Einsatz gewinnt.

2 Wie funktioniert eine PKI?

2.1 Private und öffentliche Schlüssel

Eine PKI setzt voraus, dass die Teilnehmer ein Schlüsselpaar bestehend aus einem öffentlichen („public key“) und einem privaten („private key“) Schlüssel besitzen. Der private Schlüssel ist dabei geheim – er befindet sich ausschließlich im Besitz und unter Kontrolle des Eigentümers des Schlüsselpaares. Der öffentliche Schlüssel hingegen kann und muss (als Teil eines digitalen Zertifikats) potenziellen Kommunikationspartnern zur Verfügung gestellt werden.

Der private Schlüssel dient dazu, Nachrichten, die mit dem zugehörigen öffentlichen Schlüssel *ver*schlüsselt wurden, zu *ent*schlüsseln, sowie zu versendende Nachrichten digital zu unterschreiben. Die Funktion des öffentlichen Schlüssels besteht neben der Verschlüsselungsfunktion darin, digitale Unterschriften zu verifizieren (Abbildung 1).

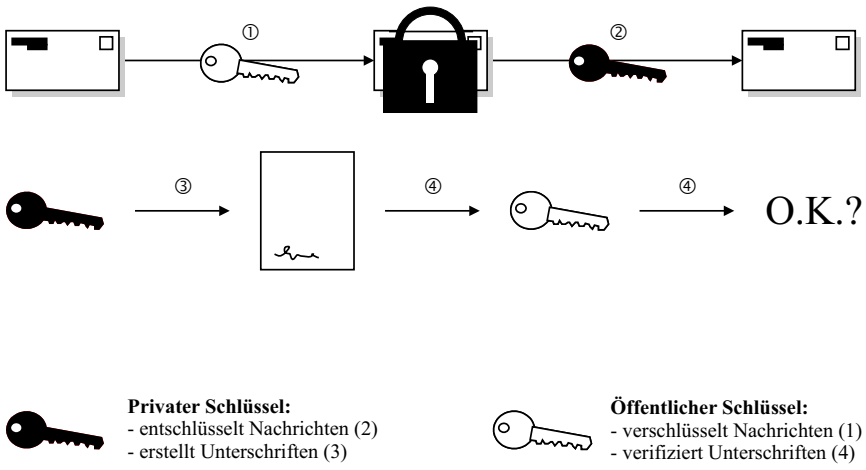


Abbildung 1: Private und öffentliche Schlüssel

[2] „Verschlüsselung“
[3] „Nicht-Veränderbarkeit“
[4] Gewährleistung der Identität der Kommunikationspartner

2.2 Die Rolle der Zertifizierungsinstanz

Um ein Schlüsselpaar zu erhalten, wendet man sich als Antragsteller an eine Zertifizierungsstelle (Certification Authority, CA). Diese Zertifizierungsstelle ist eine Instanz, die die Identität der Antragsteller genau prüft und durch Zertifikate bescheinigt.

Zertifikate (auch: digitale Zertifikate) sind „elektronische Kreditkarten“, die neben dem Namen des Inhabers weitere Eigenschaften, wie z.B. die Seriennummer des Zertifikats, das Ablaufdatum[5], den öffentlichen Schlüssel und die elektronische Unterschrift des Zertifikatsausstellers enthalten.

Nachdem der Antragsteller sein Zertifikat erhalten hat, ist er Teilnehmer oder Benutzer der PKI und sein Zertifikat wird durch die Zertifizierungsinstanz öffentlich zugänglich gemacht. Falls der Benutzer sein Zertifikat ungültig machen möchte[6], kann er sein Zertifikat bei der Zertifizierungsinstanz zurückrufen lassen – die Zertifizierungsinstanz vermerkt dann auf ihrer öffentlich zugänglichen Rückrufliste (Certificate Revocation List, CRL), dass das entsprechende Zertifikat ungültig ist.

2.3 Vertrauen gegen Vertrauen

Um einem vorgelegten Zertifikat Vertrauen schenken zu können, reicht es also aus, der Zertifizierungsinstanz zu vertrauen, die das vorgelegte Zertifikat unterschrieben hat[7] und nachzusehen, ob das vorgelegte Zertifikat auf der CRL der Zertifizierungsinstanz aufgeführt ist[8].

3 Zertifikate vs. Accounting

Dadurch, dass ein Zertifikat die Identität seines Inhabers bescheinigt, kann es auch dazu benutzt werden, Zugang zu schützenswerten Daten zu erhalten. In diesem Fall würde die Vertrauensprüfung z.B. durch einen Web-Server automatisch vorgenommen – der Web-Server verifiziert, dass die Unterschrift der Zertifizierungsinstanz unter dem vorgelegten Zertifikat gültig ist, und dass das Zertifikat auf keiner Rückrufliste der Zertifizierungsinstanz vermerkt ist. Bei positiver Prüfung erhält der Benutzer Zugang.

In der Regel kann ein solcher Zugang auch mit einem herkömmlichen Accounting-Verfahren (Angabe von Benutzername und Passwort) realisiert werden.

Durch Verwendung von Zertifikaten erreicht man jedoch zusätzlich Datenintegrität, Vertraulichkeit und Nicht-Bestreitbarkeit. Dieses „Plus“ an Sicherheit kann im universitären Umfeld ausgenutzt werden.

[5] Zertifikate sind zeitlich begrenzt gültig.
[6] z.B. weil er die Kontrolle über seinen privaten Schlüssel verloren hat
[7] Wenn die Zertifizierungsinstanz vertrauenswürdig ist, hat sie auch Wert auf die Identitätsprüfung des Antragstellers gelegt und dessen Zertifikat mit korrekten Inhalten ausgestellt.
[8] Hoffentlich ist es das nicht...

4 Sicherheitsanforderungen im universitären Umfeld

An Universitäten und Hochschulen werden personenbezogene Daten verwaltet und bereitgehalten. Durch die Möglichkeiten der elektronischen Datenverarbeitung und das Internet steigen die Begehrlichkeiten, diese Daten – sowohl intern als auch extern – einzusehen und auch zu bearbeiten. Der interne Datenschutz kann dabei durch Firewalls und spezielle Zugriffsberechtigungen auf einfachem Wege gewährleistet werden. Externer Datenschutz erweist sich – bezogen auf diese Schutzmechanismen – jedoch als problematisch.

Hier bieten sich PKI-Lösungen an.

4.1 Welche Datenqualität wird an Universitäten gehandelt?

Den Schwerpunkt des universitären Geschäftbetriebs stellt das Verhältnis der Universität zu ihren Studierenden dar. Es stehen also personenbezogene Daten der Studierenden – Adressdaten, Prüfungsleistungen, etc. kurzum „Zeugnisdaten“ – im Vordergrund. Der Austausch dieser Daten zwischen Studierendem und Universität findet in der Regel durch persönliche Vorsprache und Austausch von Unterschriften statt.

Zu diesem Geschäftsvorgang definiert die europäische Signaturrichtlinie – ergänzt durch das deutsche Signaturgesetz und die Signaturverordnung – die „fortgeschrittene elektronische Signatur“ als Online-Äquivalent. Merkmale einer fortgeschrittenen elektronischen Signatur sind insbesondere die

- Identifizierung des Signierers durch seine Signatur, die
- ausschließliche Zuordnung der Signatur zum Signierer, die
- Bildung der Signatur durch den Signierer mit Mitteln, die dieser unter alleiniger Kontrolle hat, und die
- Verknüpfung mit den elektronischen Daten, so dass eine nachträgliche Veränderung erkennbar ist.

Die Definition der fortgeschrittenen elektronischen Signatur erlaubt automatische Verfahrensweisen zur Vergabe von Zertifikaten, mit denen Signaturen erstellt werden können, über Internetportale.

5 Automatische SSL-Zertifizierung

Mit automatisiert arbeitenden Internetportalen zur Zertifikatserstellung kann der administrative Aufwand auf ein Minimum reduziert werden. Die Identifikation der Person, die ein Zertifikat beantragt, sowie die Analyse des Zertifikatsrequests geschehen bei einem automatisiert arbeitenden Verfahren maschinell. Das Administrationspersonal kann sich daher auf Systemwartungsarbeiten konzentrieren und wird vom eigentlichen Prozess des Zertifikat-Ausstellens entlastet.

6 Fallstudie FernUniversität in Hagen

Bereits seit 1996 sind an der FernUniversität PKI-Lösungen im Rahmen von BMBF-geförderten Projekten[9] zum Deutschen Forschungsnetz (DFN) getestet und im Produktionsbetrieb eingesetzt worden.

Ursprünglich wurden dabei zwei technische Ansätze – PGP[10] und SSL[11] – in jeweils unterschiedlichen rechtlichen und organisatorischen Ausprägungen getestet. Jedoch zeichnete sich bereits zu Beginn der Projekte ein Trend zu Gunsten von Zertifizierungsdiensten ab, bei denen ein persönliches Erscheinen in Hagen nicht erforderlich ist[12]. Daher wurden im Universitätsrechenzentrum der FernUniversität Überlegungen angestellt, die webgestützten Zertifizierungsdienste für den Antragsteller so einfach wie möglich zu gestalten.

6.1 Wie erhält der Benutzer sein Zertifikat?

Bei der Planung eines Zertifizierungsautomaten ist die zentrale Frage, wie man eine sichere Identifikation der PKI Teilnehmer über das Internet sicherstellen kann, also eine Identifikation, die *ohne* persönliche Vorsprache bei der Zertifizierungsstelle erfolgen kann.

An Randbedingungen sind hier ggf. mehrere Teilnehmergruppen (Studierende, Mitarbeiter, Organisationseinheiten) zu berücksichtigen, aber auch unterschiedliche Qualitäten von Zertifikaten (persönliche Zertifikate „Client-Zertifikate“, maschinell einsetzbare Zertifikate „Server-Zertifikate“). Aufgrund der Heterogenität der Rahmenbedingungen ergeben sich hier verschiedene Möglichkeiten zur Identifizierung der Benutzer:

Bei Client-Zertifikaten können die Benutzer anhand von Daten identifiziert werden, die der FernUniversität aufgrund des Geschäftsbetriebs bereits vorliegen: Studierende können durch die beim Immatrikulationsvorgang durch Personal der FernUniversität verifizierte Adresse identifiziert werden – Mitarbeiter und Organisationseinheiten z.B. durch ihre Dienst- oder Behördenadresse.

Server-Zertifikate sind im Internet auch außerhalb des eigenen PKI-Verbunds sichtbar. Sie unterliegen also einer gewissen Außenwirkung. Daher werden Serverzertifikate an der FernUniversität stets nur bei persönlicher Vorsprache und Identifikation des Antragsstellers durch seinen Personalausweis ausgestellt.

Für das Beispiel der Studierenden der FernUniversität sieht der Ablauf – wie folgt – aus:

Zunächst wird der Studierende durch Personal der FernUniversität beim Immatrikulationsvorgang identifiziert. Dabei werden seine Adressdaten – gemeinsam mit der Matrikelnummer – in einer „Authentisierungs-Datenbank“[13] abgelegt. Falls sich der Studierende

[9] Bundesminister für Bildung und Forschung

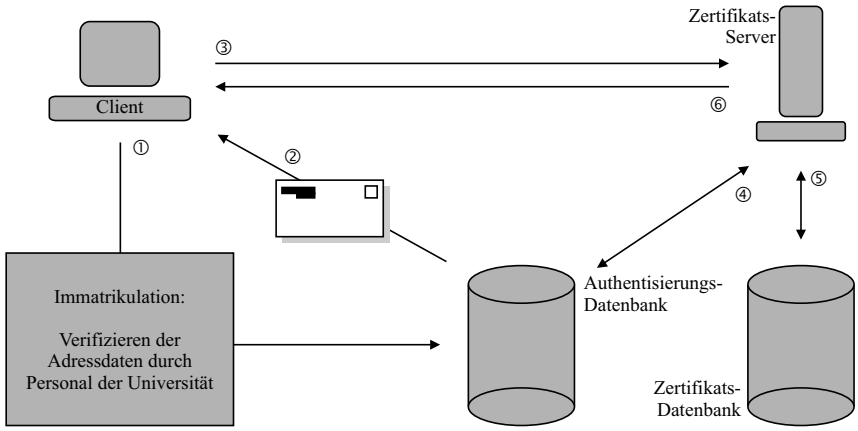
[10] Pretty Good Privacy

[11] Secure Socket Layer

[12] Das ist auch nicht verwunderlich, denn im Normalfall arbeiten die Studierenden der FernUniversität zu Hause – der an „normalen“ Universitäten stattfindende Studienbetrieb wird an der FernUniversität ersetzt durch Postversand von Studienmaterialien oder Online-Zugriffe („virtuelle Universität“).

[13] Das ist an Universitäten üblicherweise eine von der Firma HIS gelieferte Datenbank.

dazu entschließt, an der PKI der FernUniversität teilzunehmen, bekundet er sein Interesse durch Angabe seiner Matrikelnummer (und *nur* der Matrikelnummer) in einem Web-Formular. Der Zertifikatsserver generiert dann ein Identifikations-Passwort, sucht die zu der Matrikelnummer gehörende Adresse aus der Authentisierungs-Datenbank und schickt das Passwort an die passende Adresse. In einem weiteren Arbeitsschritt wird das Passwort automatisch der Authentisierungs-Datenbank hinzugefügt. Nachdem der Studierende das Passwort per Post erhalten hat, kann er über ein weiteres Web-Formular ein Zertifikat beantragen. Dort muss er sich mit Matrikelnummer und Passwort anmelden. Aufgrund der Datenbasis, die dem Zertifikatsserver nun vorliegt, wird dann das Zertifikat erstellt, im selben Arbeitsschritt dem Studierenden zugestellt und in der Zertifikats-Datenbank hinterlegt. Dieser Ablauf wird in Abbildung 2 schematisiert.



1. Beim Immatrikulationsvorgang wird die Adresse des Studierenden verifiziert und in der Authentisierungs-Datenbank hinterlegt.
2. Client (Studierender) erhält Authentisierungsdaten per Post.
3. Client (Studierender) beantragt ein Zertifikat.
4. Zertifikatsserver verifiziert die Authentisierungsdaten gegen die Authentisierungs-Datenbank.
5. Zertifikatsserver stellt Zertifikat aus und schreibt den öffentlichen Schlüssel in die Zertifikats-Datenbank.
6. Zertifikatsserver schickt den öffentlichen Schlüssel zum Client (Studierenden).

Abbildung 2: Schematischer Ablauf einer automatisierten Zertifizierung

Der Vorgang der Zertifizierung kann bei solchen Verfahren also vom persönlichen Arbeitsplatz erfolgen (im Gegensatz zu herkömmlichen Verfahren ist eine persönliche Vorsprache bei der Zertifizierungsinstanz nicht erforderlich) und geschieht unmittelbar (Antrag und Abrufen des Zertifikats ist ein verfahrenstechnischer Vorgang). Der Studierende muss also, um ein Zertifikat zu erhalten, folgende Schritte durchführen:

- durch Angabe seiner Matrikelnummer bekundet er seinen Willen zur Teilnahme an der universitären PKI,

- durch Ausfüllen eines Web-Formulars erhält er sein Zertifikat.

6.2 Technische Realisierung

Die Daten, die dem Zertifikatsserver zu Grunde liegen, sind sämtlich schützenswert und liegen daher auf Datenbankservern innerhalb der Firewall. Einzig die Web-Formulare, die der Studierende bedienen muss, liegen auf einem Server außerhalb der Firewall. Diese Serveranordnung wird durch Abbildung 3 verdeutlicht.

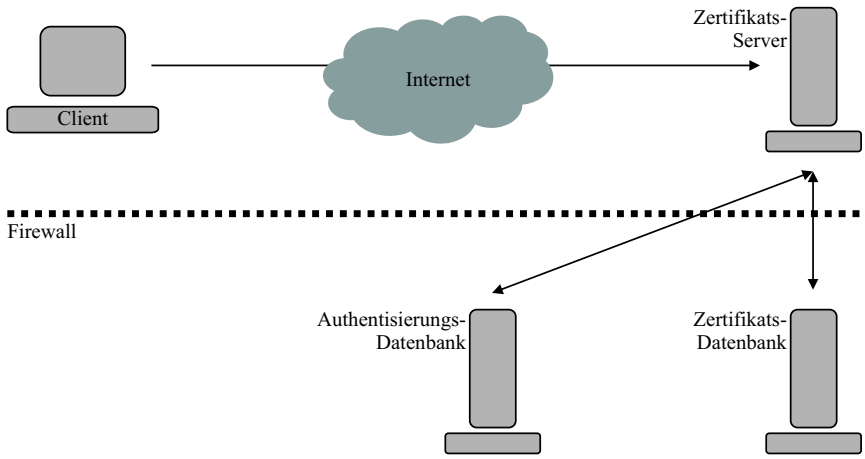


Abbildung 3: Topologie, Server- und Netzaufbau mit Firewall

Die Anwendung selbst wurde in einer mehrschichtigen Architektur realisiert. Für die Datenhaltungsschicht wird ein Oracle-Datenbanksystem[14] eingesetzt. Die Programmierebene wird in PHP[15] realisiert und als Web-Server dient ein Apache[16]. Um maximale Flexibilität und Unabhängigkeit vom Datenbanksystem zu erreichen, kommuniziert die Datenbankabstraktionsklasse Pear::DB[17] mit der Oracle-Datenbank. Diese Datenbankabstraktionsklasse arbeitet jedoch auch mit anderen Datenbankprodukten, wie etwa MySQL, Informix, ODBC, ... zusammen. Designunabhängigkeit, also die Trennung von Designelementen von der Programmierlogik wird durch den Templategenerator Smarty[18] erreicht. Diese Fünf-Schichten-Architektur verdeutlicht Abbildung 4.

Bei der Programmierlogik wurde strikt darauf geachtet, dass der Server durch eine einzige Konfigurationsdatei im XML-Format konfigurierbar ist. Dennoch besitzt er aus Sicherheitsgründen separate Verzeichnisse für die Funktionen der Administrationsebene und der für den Benutzer zugänglichen Ebene.

[14] http://www.oracle.com
[15] http://www.php.net
[16] http://www.apache.org
[17] http://pear.php.net
[18] http://smarty.php.net

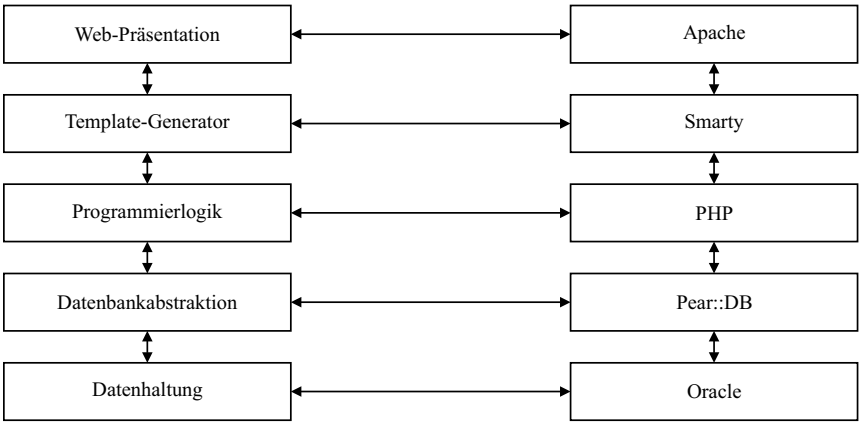


Abbildung 4: Schichtenarchitektur

6.3 Support für die Client-Seite

Grundsätzlich ist es für jeden Studierenden möglich, ein Zertifikat zu erhalten. Vom Universitätsrechenzentrum der FernUniversität werden jedoch nur Browser der Hersteller Microsoft, Netscape, Mozilla, Konqueror und Opera auf den Betriebssystemen Windows und Linux unterstützt[19].

Für den Fall, dass ein Benutzer eine Supportanfrage stellen möchte, gibt es auf jeder aufrufbaren Web-Seite ein kontextsensitives Hilfeformular. Dieses Formular fängt aufgrund der Kombinationen verschiedener Eingaben typische Fehlerfälle ab und leistet dann sofortige Hilfestellung. Weiter gehende Anfragen, die nicht automatisiert bearbeitet werden können, werden an eine zentrale First-Level-Supportstelle des Universitätsrechenzentrums der FernUniversität weitergeleitet. Dieser First-Level-Support wird durch einen Second-Level-Support verstärkt.

Neben dem Supportformular erhält der Studierende auf jeder Web-Seite des Zertifikatsservers eine Anleitung im Film-Format (Flash-PlugIn erforderlich). In einem kurzen Video kann er sich die Bedienung der aktuellen Web-Seite ansehen.

6.4 Akzeptanzsteigerung

Ein derartiges Online-Verfahren zum Beantragen eines Zertifikats ist auch für Studierende, die bis dahin keine Kenntnisse auf Gebieten der PKI-Nutzung haben, einfach durchführbar – alle vom Studierenden durchzuführenden Aktionen konzentrieren sich auf das Ausfüllen von zwei Web-Formularen. Dass die Zertifizierung nach diesem ablauforganisatorischen Verfahren an der FernUniversität auch angenommen wird, kann anhand von Statistiken belegt werden.

[19] Immerhin machen diese Betriebssystem/Browser-Kombinationen einen Anteil von ca. 98% aus.

Während von 1996 – also der Aufnahme von Zertifizierungstätigkeiten an der FernUniversität – bis 2001 ca. 4500 Zertifikate ausgestellt wurden[20], hat das Universitätsrechenzentrum von Februar 2002 bis einschließlich März 2003 nach dem hier beschriebenen Verfahren 3800 Zertifikate ausgestellt.

6.5 Anwendungen für Zertifikate

Studierenden und Mitarbeitern der FernUniversität stehen zahlreiche Anwendungen für Zertifikate zur Verfügung:

Studierende erhalten über das Internet einen Ausdruck ihres Studienkontos: Dort sind alle an der FernUniversität abgelegten Prüfungsergebnisse verzeichnet, sie können sich zu Prüfungen und Praktika anmelden; Software, die einem Campuslizenz-Modell unterworfen ist, kann mit Hilfe eines SSL-Zertifikats von Servern der FernUniversität heruntergeladen werden, Studierende und Mitarbeiter können sich mit einem Zertifikat am VPN-Gateway der FernUniversität anmelden, Mitarbeiter können Belegerdaten von Studierenden herunterladen und Leistungsdaten ihrer Studierenden in die Studierendendatenbanken einpflegen. Natürlich steht jedem Inhaber eines Zertifikats die Möglichkeit offen, seine E-Mails zu signieren und verschlüsseln.

7 Einsatz von eToken

SSL-Zertifikate sind naturgemäß von ihrem Einsatz her unflexibel. Dies liegt an der „festen Integration“ in die jeweilige Browserumgebung. Die Verwendung eines Zertifikats in mehreren Browsern (oder auch auf mehreren Computern) ist daher nur schwierig möglich[21]. Dies ist insbesondere für FernStudierende von Nachteil, da FernStudierende oftmals sowohl vom Arbeitsplatz, als auch aus ihrer Wohnung auf die Services der FernUniversität zugreifen möchten.

Das Universitätsrechenzentrum der FernUniversität begegnet diesem Problem – derzeit in einer Testphase – durch die Ausgabe von „eToken“. eToken sind kleine Stecker (Abbildung 5)[22], die in den USB-Port des Computers eingeführt werden. Auf einem eToken kann das Zertifikat auf einem darin eingebrachten Crypto-Chip erstellt und abgespeichert werden. Durch Installation eines Gerätetreibers für den eToken steht das darauf befindliche Zertifikat jedem auf dem Betriebssystem installierten (Microsoft-, Netscape- oder Mozilla-) Browser zur Verfügung. Wird der eToken aus dem USB-Port entfernt, ist das Zertifikat in der Computer-Umgebung nicht mehr vorhanden und kann daher auch nicht missbraucht werden.

[20] In diesem Zeitraum wurde ein manuell zu bedienender, kommerzieller Zertifikatsserver eingesetzt, bei dem das Administratorpersonal durch die manuelle Bedienung erheblich mehr Aufwand betreiben musste und falsche Eingaben durch den Studierenden nicht unmittelbar abgefangen werden konnten.

[21] Um ein Zertifikat „mehrfach“ zu nutzen, muss es in der Regel erst umständlich aus einer Browserumgebung exportiert und in eine andere Browserumgebung importiert werden.

[22] http://www.ealaddin.com

Abbildung 5: eToken der Firma Aladdin

Durch Installation des Gerätetreibers auf mehreren Computern und Mitnahme des eToken ist das Zertifikat nun auch in den verschiedensten Umgebungen verfügbar.

Bei gleicher Leistung ist der Einsatz von eToken auf mehreren Rechnern praktischer als eine SmartCard Lösung, bei der jeweils der SmartCard-Reader mitgenommen (oder mehrfach angeschafft) werden muss.

Der eToken ist daher ein „Schlüssel“ zu schützenswerten Daten der FernUniversität.

8 Bewertung des Verfahrens

Das automatisiert arbeitende Verfahren zur Ausstellung von Zertifikaten an der FernUniversität ist naturgemäß nicht so sicher, wie ein Verfahren, bei dem die Antragsteller ihr Zertifikat bei ihrer Zertifizierungsinstanz persönlich abholen müssen. Gefährdungspunkte für mögliche Sabotageversuche liegen insbesondere im Postversand des Identifikationspassworts und in der automatisch stattfindenden Analyse des Zertifikatsrequests.

Vergleicht man jedoch das Zertifizierungsverfahren mit einem „herkömmlichen“ Accountingverfahren, so stellt man fest, dass insbesondere bei der Verwendung von eToken durch dieses Verfahren ein nachhaltiger Sicherheitsgewinn erzielt werden kann. Trotz des Zugewinns an Sicherheit, leidet jedoch die Benutzerfreundlichkeit eindeutig nicht.

Daher scheint das automatisiert arbeitende SSL-Verfahren an der FernUniversität langfristig zum Ersatz von Accounting-Verfahren zu werden. Bei der stets wachsenden Anzahl von Anwendungen ist dies zudem als ein Schritt in Richtung Single-Sign-On zu bewerten.