Automatischer X.509v3-Zertifizierungsdienst

Henning Mohren, Stephan Pieper

Zentrum für Medien und IT
FernUniversität in Hagen
58084 Hagen
Henning.Mohren@FernUni-Hagen.de
Stephan.Pieper@FernUni-Hagen.de

Abstract: Als erste Hochschule in Deutschland hat die FernUniversität in Hagen einen Server entwickelt, der den gesamten Vorgang einer X.509-Zertifizierung vom Antrag bis zum Empfang des Zertifikats durch den Nutzer innerhalb weniger Sekunden automatisch abwickelt. Es wurde bei der Entwicklung auf eine einfache und intuitive Bedienung Wert gelegt. Die Eingabemöglichkeiten des Nutzers wurden optimiert, um den Supportaufwand zu senken und das System besser etablieren zu können. Der Zertifikatsserver existiert mittlerweile in der Version 5.0. Seit dieser Version wird die sichere Speicherung der Signaturschlüssel auf einem Hardware Security Modul (HSM) unterstützt, darüber hinaus können digitale Zertifikate mit speziell definierten Attributen ausgestellt werden. Dadurch können z.B. Zertifikate generiert werden, die nur verschlüsseln oder digital signieren können. Der Zertifikatsserver der FernUniversität in Hagen wurde an Hochschulen in Nordrhein-Westfalen im Hostingbetrieb zur Verfügung gestellt und an zwei Hochschulen verkauft.

1 FernUniversität etabliert Zertifizierung im Massengeschäft

Bereits 1996 wurden an der FernUniversität in Hagen erste Überlegungen angestellt, die webgestützten Zertifizierungsdienste für den Nutzer so einfach wie möglich zu gestalten. Eine Automatisierung des bis dahin durch Administrationspersonal manuell zu bedienenden Verfahrens lag folglich nahe.

Bei der Planung des Zertifizierungsautomaten war die zentrale Frage, wie man eine sichere Identifikation der PKI-Teilnehmer gewährleisten kann, ohne dass persönliche Präsenz bei der Zertifizierungsstelle erforderlich ist. Grundlage dieser Identifikationsmethode sind die in der bestehenden Studierenden- und Mitarbeiterdatenbank vorhandenen Datensätze, die bereits beim Immatrikulationsvorgang (Studierende) bzw. beim Vorgang zur Einstellung eines Beschäftigten verifiziert wurden. Zu jedem dieser Adresssätze generiert das Identity Management System der FernUniversität automatisch das „Generalpasswort“. Dieses Passwort wird dem Adressaten auf Hydalam-Papier ausgedruckt und in den Postversand gegeben. Dabei wird die bereits verifizierte und in der Datenbank hinterlegte Adresse verwendet.

Um ein Zertifikat zu erhalten, muss der Student oder Mitarbeiter an einem von ihm selbst gewählten, beliebigen internetfähigen Arbeitsplatz die Website der Certification Authority (CA) der FernUniversität in Hagen aufrufen und seine Benutzerkennung in Kombination mit dem „Generalpasswort“ angegeben. Der Webserver sucht aus der Datenbank des Identity Management Systems den entsprechenden Datensatz heraus und stellt – bei positiver Prüfung – das Zertifikat aus.

Die kryptographischen Anforderungen werden durch die clientseitige Verwendung von modernen Browser-Technologien, wie Firefox, Internet Explorer, Mozilla, Netscape, Opera oder Safari erfüllt. Ein derartiges Online-Verfahren zum Beantragen eines Zertifikats ist auch für Studierende, die bis dahin keine Kenntnis auf dem Gebiet der PKI-Nutzung haben, einfach durchführbar. Dies können die Nutzer- und Supportstatistiken an der FernUniversität belegen.

1.1 Verfahrenstechnischer Vorteil

Ein Zertifikat kann online beantragt werden. Wurden in der Vergangenheit die Zertifikatsanträge durch Administrationspersonal im Zentrum für Medien und IT (ZMI) der FernUniversität manuell bearbeitet und die Zertifikate im Anschluss in eine Datenbank eingetragen, erfolgt dies nun automatisch. Das Zertifikat wird – im Gegensatz zu dem Verfahren in der Vergangenheit, wo das Zertifikat per E-Mail an die Antragsteller versandt wurde – nun unmittelbar nach dem Zertifikatsantrag der beantragenden Person zum Download angeboten. Hieraus ergeben sich erhebliche Zeitersparnisse bei den Studierenden, da unmittelbar nach Antrag auf ein Zertifikat sämtliche Anwendungen in personalisierter Form offen stehen und genutzt werden können. Durch organisatorische und kryptographische Maßnahmen wird Manipulation bei der Beantragung des Zertifikats verhindert.

1.2 Betriebswirtschaftlicher Vorteil

Durch den Betrieb einer eigenen Server-Lösung zum Erstellen von Zertifikaten entfallen für die Studierenden der FernUniversität die Zertifizierungskosten eines kommerziellen Trust-Centers. Sämtliche Planungs- und Programmierarbeiten am Zertifikatsserver wurden von Mitarbeitern des ZMI durchgeführt. Auch bei der Auswahl der verwendeten Softwareprodukte wurden Kosten minimiert: Die benötigten Softwareprodukte (Apache, PostgreSQL, PHP und OpenSSL) unterliegen der GNU General Public License (GPL). Alternativ kann auch eine Oracle-Datenbank zum Einsatz kommen. Dabei kommt die Sicherheit selbstverständlich nicht zu kurz: Geeignete Maßnahmen, wie z.B. der Einsatz eines Hardware Security Moduls (HSM) zum Schutz des Wurzelzertifikats, garantieren größtmögliche Sicherheit beim Betrieb der Zertifizierungsinstanz.

1.3 Organisatorischer Vorteil

Im Hochschulbereich gibt diese Neuentwicklung der Elektronischen Signatur, die von der Bundesregierung stark gefördert wird, einen kräftigen Schub:

Viele andere Universitäten nutzen den Server bereits jetzt durch vertragliche Verbindungen mit der FernUniversität, andere haben Interesse signalisiert, ihre eigene PKI über den Server abzuwickeln. Dabei lässt sich der Server über eine frei konfigurierbare Schnittstelle an beliebige Identity- und Accessmanagementsysteme, die in den jeweiligen Hochschulen vorhanden sind, ankoppeln. Sämtliche Kommunikation zwischen dem Identity- und Accessmanagementsystem sowie dem Zertifikatsserver ist dabei authentifiziert, verschlüsselt und integer.

Durch den Einsatz des an der FernUniversität in Hagen entwickelten Active Propagation Moduls (APM) ist es möglich, Zertifikate und Zertifikatsinformationen in beliebige Zielsysteme wie z.B. Verzeichnisdienste (LDAP, Active Directory), FTP-Servern, Datenbanken und eigene Anwendungen zu provisionieren. Der Einsatz des APM schaltet diese Anwendungen für die Benutzung mit Zertifikaten frei. Der Benutzer muss hierfür nur ein digitales Zertifikat auf dem Zertifikatsserver beantragen, im Hintergrund übernimmt das APM die nötigen Informationen und überträgt sie an die konfigurierten Zielsysteme. Das APM spart den administrativen Konfigurationsaufwand, der bei der manuellen Integration aufgewendet werden müsste.

1.4 Rahmenbedingungen

An der FernUniversität ist der Postversand der Passworte unabdingbar, da die Studierenden weltweit verteilt und damit nicht persönlich kontaktierbar sind. Ein Verfahren, mit dem eine obligatorische Personalausweiskontrolle verbunden war, wurde anfangs evaluiert, konnte sich jedoch aufgrund des hohen Aufwands in der Studierendenschaft nicht durchsetzen. Grundsätzlich ließe sich die Sicherheit des Versands noch durch delegierte Ausweiskontrolle erhöhen (Post Ident Verfahren), jedoch ist dies mit erheblich höheren Kosten für die FernUniversität verbunden. Zudem ist unklar, ob das Post Ident Verfahren in anderen Staaten den standardisierten Sicherheitsvorschriften, wie sie in Deutschland vorliegen, entspricht.

Für die FernUniversität entfällt zudem die „Wohnheimsproblematik“ – Studierende der FernUniversität wohnen in der Regel nicht in einer Umgebung, in der „aus Spaß“ das Passwort abgefangen werden und dann missbraucht werden kann. An Hochschulen, die diesem Problem durch persönliche Aushändigung des Passworts entgegnen können, lässt sich das Verfahren der FernUniversität jedoch ohne Änderung des zugrunde liegenden Workflows adaptieren.

Zum Passwortversand wird das Hydalam-Verfahren eingesetzt. Die Nachteile des Hydalam-Verfahrens ([5]) in Bezug auf Angreifbarkeit der Hydalam Technologie sind dabei durchaus bekannt: Trotzdem eignet es sich in Verbindung mit einem Kaltklebeverfahren, mit dem die Passwortbriefe unmittelbar nach Ausdruck verschlossen werden (Sealerformular). Das Formular verhindert dabei den Zugriff auf das durch Hydalam gesicherte Passwortfeld und damit die bekannten Angriffsmöglichkeiten auf das Passwort. Das Kaltklebeverfahren wird üblicherweise auch bei Banken oder Versicherungen eingesetzt, um PIN-Briefe sicher zu versenden.

1.5 Verfahrensvergleich

Das durch die FernUniversität etablierte Verfahren gehört organisatorisch zu den „PKI Self-Services“, denen gemeinsam ist, dass der Nutzer selbst sein Zertifikat verwalten, d.h. beantragt, erneuert, revoziert und suspendiert. Diese Verfahren sind in unterschiedlichsten Formen im Hochschul-, Verwaltungs- aber auch im privatwirtschaftlichen Umfeld im Einsatz. Sie bergen ganz allgemein die Gefahr, dass unbedarfte Nutzer bei der Bedienung des Zertifizierungsautomaten „Fehler machen“. Genau hier liegt der Ansatz der FernUniversität: Nach Einloggen auf dem Server erhält der Nutzer bereits nach bis zu sieben Mausklicks (das entspricht ca. 30 Sekunden) sein funktionsfähiges Zertifikat. Dabei sind keine weiteren Eingaben erforderlich – sämtliche Daten provisioniert das Identity- und Accessmanagementsystem. Das Verfahren ist daher nicht fehleranfällig.

Im Vergleich zu Verfahren, bei denen das Zertifikat durch Administrationspersonal ausgestellt wird, schneidet die Lösung der FernUniversität in bezug auf Administrationskosten besser ab: Eine Erhebung der Hansestadt Hamburg belegt, dass ein zusätzlicher administrativer Aufwand von 30 Sekunden pro Jahr und Student dazu führen würde, dass an den Hochschulen dieses Bundeslandes zusätzlich 45 Planstellen eingerichtet werden müssen. Ein manuell im Dialog zwischen Nutzer und Administrator zu erstellendes Zertifikat verursacht einen höheren Aufwand.

Beim PKI Self-Service muss man sich jedoch der Gefahr von Angriffen aus dem Internet bewusst sein und daher den Server durch bekannte Techniken (Intrusion Prevention / Detection, …) gegen Übernahmen schützen.

1.6 Interesse im außeruniversitären Umfeld

Auch außerhalb des universitären Bereichs ist der Server auf Interesse gestoßen: Die Certification Authority (CA) steht in Verhandlungen mit Unternehmen der Privatwirtschaft. In mehreren Gutachten wurde dem Verfahren der FernUniversität in Hagen die Konformität zum Signaturgesetz (SigG) bescheinigt ([1, 2, 3]): Die FernUniversität stellt fortgeschrittene Zertifikate aus.

Der X.509v3 Zertifizierungsdienst der FernUniversität hält sich an internationale PKI-Standards wie z.B. PKCS, MS/CAPI, so dass die in Hagen erzeugten Zertifikate auch in Anwendungen von Anbietern zum Einsatz kommen können, die nicht in Kontakt zur FernUniversität stehen. Mit dem Ziel das Sicherheitsniveau weiter zu erhöhen und die Nutzung der Zertifikate zu flexibilisieren, kann auch jede beliebige Smartcard mit einem Zertifikat des Hagener Zertifikatsservers versehen werden.

2 Anwendungen

Grundsätzlich kann dabei jede Web-Anwendung (z.B. Kundenportale, Selbstauskunftfunktionen, Bereitstellung kostenpflichtiger Informationen, eShopping-Portale, Abruf kostenpflichtiger Software) abgesichert werden.

Anwendungen sind vor allem denkbar im Bereich von eEntry-Funktionen (Eingangs- und Zugangskontrollen, die in diesem Sinne nicht nur räumliche Zugänge (Türen, Parkplätze etc.), sondern auch organisatorische Zugänge (Datenverbindungen, Server-Log-On, SSH, VPN) und Systemzugänge (Starten von Autos, Maschinen etc.) ermöglichen. Im Bereich des eProcurement steht hingegen die für Menschen auswertbare Signatur im Vordergrund. Neben E-Mails und PDF-Dokumenten können Webformulare mit dem Zertifikat digital signiert werden. Die FernUniversität in Hagen hat für diesen Zweck ein Portal entwickelt. Mit Hilfe dieses Portals können Kurse und Informationsmaterial urheberrechtlich geschützt werden. Nach der eindeutigen Authentifizierung eines Benutzers mit dessen digitalem Zertifikat, wird das angeforderte Dokument digital signiert und einem personalisierten 2D-Barcode versehen. Das so erstellte Dokument ist folglich personalisiert, vor Manipulationen geschützt und eine Identifizierung des Benutzers ist bei unberechtigter Weitergabe möglich.

Allgemein können natürlich sämtliche Komponenten im Bereich des eBusiness durch Zertifikate abgesichert werden. eEducation und eGovernment sind Bereiche, in denen schon jetzt der flächendeckende Einsatz möglich ist (BundOnline 2005).

An der FernUniversität in Hagen werden eine Reihe von zertifikatsbasierenden Anwendungen gleichermaßen im Bereich der Hochschulverwaltung und im Bereich Forschung und Lehre eingesetzt: Studierende können sich mit einem Zertifikat zu Prüfungen und Praktika anmelden und ihre Klausurergebnisse online abrufen. Lizenzpflichtige Software (Campuslizenzen) kann ebenfalls nur nach Vorlage eines gültigen Zertifikats herunter geladen werden. Beschäftigte der FernUniversität können sich mit ihrem Zertifikat an ihrem Arbeitsplatzrechner (Active Directory Login) oder an Unix Servern anmelden. Sensible Daten wie Beleg- oder Leistungsdaten werden mit dieser Methode vor unbefugten Zugriff geschützt, damit wird eine erhöhte Sicherheit gewährleistet. Eine Anzahl von Standardanwendungen, wie Signieren/Verschlüsseln von E-Mails sowie Login-Prozess am VPN-Gateway runden die Einsatzmöglichkeiten ab.

Literaturverzeichnis

[1] Modellvergleich zur Vergabe fortgeschrittener Signaturen nach §2 Nr. 2 Signaturgesetz, Prof. Dr. Hoeren, Forschungsstelle Recht im DFN, Münster

[2] Begutachtung des Zertifizierungsverfahrens der FernUniversität in Hagen und Einordnung in einen Level für digitale Signaturen gemäß Signaturgesetz, Johannes Bleker, CI-SA, Düsseldorf

[3] Gutachten zur Sicherheit der Plattform 2003 der FernUniversität Hagen, Prof. Dr. Schwenk, Ruhr-Uni Bochum

[4] Gesetz über Rahmenbedingungen für elektronische Signaturen, http://www.gesetze-im-internet.de/sigg_2001/index.html

[5] Laser-printed PIN Mailer Vulnerability Report, Bond, Murdoch, Clulow, University of Cambridge, http://www.cl.cam.ac.uk/~sjm217/papers/cl05pinmailer-vuln.pdf