Die virtuelle Hochschulverwaltung?

Online-Dienstleistungen von Verwaltungen oder anderen Einrichtungen sind für uns mittlerweile selbstverständlich geworden. Wie kann die elektronische Signatur helfen, dieses Angebot zu erweitern und für welche Anwendungen ist der Einsatz einer elektronischen Signatur sinnvoll oder notwendig? Allgemeine Betrachtungen und spezielle Ansätze der HU vermittelt dieser Artikel.

Es gibt wohl kaum jemanden, der die Begriffe *E-Government*, *virtuelles Rathaus*, *E-Commerce* und *E-Business* nicht schon einmal gehört hat. Auch wenn sich die Bezeichnungen auf unterschiedliche Geschäfts- oder Verwaltungsfelder beziehen, ist allen eine möglichst vollständig elektronische Kommunikation zwischen den jeweiligen Partnern gemein. Im Falle einer Hochschulverwaltung heißt das, die Daten der Hochschulangehörigen werden über ein öffentliches Netz wie das Hochschulnetz oder das Internet übertragen und in den IT-Systemen der Verwaltung verarbeitet und archiviert. Dieser Prozess wird schon seit einigen Jahren vorangetrieben, kommt jedoch zum Stehen, wenn sensible Daten übertragen oder sensible Verwaltungsvorgänge angestoßen werden. Hier kommt der IT-Sicherheit eine besondere Bedeutung zu. Mit der Entwicklung der elektronischen Signatur ist es technisch möglich geworden, die Integrität und Authentizität von Daten zu gewährleisten. Eine ganz spezielle Art der elektronischen Signatur hat der Gesetzgeber rechtlich der handschriftlichen Signatur gleichgesetzt. Diese werden im Signaturgesetz und in der Signaturverordnung beschrieben. Doch in welchen Verwaltungsabläufen sind welche elektronischen Signaturen einzusetzen?

Warum „virtuelle“ Hochschulverwaltung?

Für die meisten Hochschulangehörigen ist die Benutzung moderner Kommunikationsmittel bereits eine Selbstverständlichkeit geworden. Sie verlangen Online-Angebote, welche die schnelle und unkomplizierte Nutzung von Dienstleistungen der Verwaltung ermöglichen. Dadurch sollten Verwaltungsvorgänge einfach zu verfolgen und nachzuvollziehen sein. Ziel ist es demnach, den Service und die Transparenz von *Verwaltungsdienstleistungen für Angehörige* zu mehren.

Das ist in der Tat ein hoher Anspruch, der aber mit Veränderungen im Verwaltungsablauf selbst durchaus erfüllt werden kann. So nützt es zum Beispiel nichts, den Hochschulangehörigen ein Front-End zum Online-Ausfüllen und Online-Versenden von Formularen anzubieten, wenn auf Verwaltungsseite dieses Formular ausgedruckt und auf dem Papierweg bearbeitet wird. Ziel muss es deshalb auch sein, *interne Verwaltungsabläufe* medienbruchfrei zu gestalten. Dieser Aspekt führt besonders in Hinblick auf eine dezentrale Verwaltung zu Zeitersparnis.

Die Medienbruchfreiheit weitet sich auf *externe Verwaltungsabläufe* mit der gleichen Möglichkeit zur Effizienzsteigerung aus. Damit sind speziell Geschäftsprozesse der Hochschule mit privaten Unternehmen, aber auch Prozesse mit Behörden gemeint.

Es sind durchaus weitere Beziehungen definierbar, aber dieser Artikel soll sich auf die oben genannten Beziehungen beschränken.

Das Signaturgesetz

Das „Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz, SigG)“ unterscheidet vier Arten von elektronischen Signaturen, deren Sicherheitsniveau mit jeder im Folgenden genannten Art steigt.

Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. Es gibt weiter keine gesetzlichen Regelungen und damit kein bekanntes Sicherheitsniveau bezüglich dieser elektronischen Signaturen, aber sie sind schon als Beweismittel zugelassen (Augenscheinbeweis). Als Beispiele können unpersonalisierte elektronische Signaturen und unpersonalisierte öffentliche Schlüssel genannt werden.

Fortgeschrittene elektronische Signaturen sind elektronische Signaturen, die ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind und die Identifizierung des Signaturschlüssel-Inhabers ermöglichen. Die Zertifizierungsinstanz *HU-CA* der Humboldt-Universität zu Berlin entspricht dieser Kategorie.

Qualifizierte elektronische Signaturen sind fortgeschrittene elektronische Signaturen, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen *qualifizierten Zertifikat* beruhen und mit einer sicheren Signaturerstellungseinheit wie Smartcard erzeugt werden. Qualifizierte Zertifikate können ausschließlich von *angemeldeten Zertifizierungsdiensteanbietern* ausgestellt werden. Die Anmeldung erfolgt mit Vorlage einer Deckungsvorsorge für Schadensfälle und einem Sicherheitskonzept bei der Regulierungsbehörde für Telekommunikation und Post (RegTP). Damit entsteht ein bekanntes Sicherheitsniveau mit einer *behaupteten Sicherheit* des Zertifizierungsdiensteanbieters. Als Beispiel ist das Trustcenter *D-Trust* der Bundesdruckerei GmbH zu nennen.

Der Zertifizierungsdiensteanbieter kann sich zusätzlich freiwillig akkreditieren lassen, was die Prüfung

von vorgeschriebenen Sicherheitsmaßnahmen durch Dritte erfordert (z. B. durch das Bundesamt für Sicherheit in der Informationstechnik, BSI). Damit entsteht ein bekanntes Sicherheitsniveau mit einer *nachgewiesenen Sicherheit* des Zertifizierungsdiensteanbieters. Man spricht von *qualifizierten elektronischen Signaturen akkreditierter Zertifizierungsdiensteanbieter.* Die Trustcenter *TeleSec* der Deutschen Telekom AG und *Signtrust* der Deutschen Post AG sind zum Beispiel solche Anbieter.

Mit dem „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr" wurde die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gleichgesetzt und als Beweismittel zugelassen (§ 126 Abs. 3 BGB-E). Der Inhaber des geheimen Signaturschlüssels zu einer qualifizierten elektronischen Signatur ist für geleistete Willenserklärungen mit dem geheimen Signaturschlüssel haftbar (§ 292 a ZPO-E). Im Streitfall muss demnach der Signaturschlüsselinhaber nachweisen, dass eine Willenserklärung ohne seinen Willen abgegeben worden ist. Dieser Nachweis ist bei der Verwendung zertifizierter Produkte und akkreditierter Zertifizierungsdiensteanbieter schwer zu führen. Diese *Vermutungsregel* schützt den Empfänger eines signierten Dokumentes und erhöht die Verantwortung des Signierers.

Die elektronische Signatur in der virtuellen Hochschulverwaltung

Die vorangegangenen Abschnitte haben unterschiedliche Arten von elektronischen Signaturen und von Geschäfts- und Verwaltungsbeziehungen gezeigt. In Abhängigkeit der Beziehung und einer Anwendung ergeben sich die Anforderungen an eine elektronische Signatur. Es wird im Folgenden nicht zwischen dem Signieren eines Dokumentes und dem Authentifizieren einer Person mittels einer elektronischen Signatur unterschieden, weil es technisch gleichartige Vorgänge sind. Prinzipiell sollte der Unterschied jedoch gemacht werden.

Im Falle der Beziehung *Verwaltungsdienstleistungen für Angehörige* einer Hochschule sind Online-Anwendungen denkbar wie:

- Prüfungsan- und abmeldung und Adressänderung für Studierende
- Elektronische Vergabe von Leistungsnachweisen für Studierende
- Online-Wahlen zum StuPa
- Sonstige Anmeldungen und Antragstellungen
- Dienstreiseantrag und -abrechnung für Mitarbeiter
- Urlaubs- und sonstige Anträge für Mitarbeiter
- Online-Wahlen zum Personalrat
- Leihfristverlängerungen bei der Bibliothek

Für alle genannten Anwendungen ist die Feststellung und Überprüfung der Identität eines Nutzers eine wesentliche Voraussetzung. Für sensible Anwendungen wie Prüfungsanmeldungen und Dienstreiseabrechnungen ist zum Zwecke der Authentifizierung ein Passwortverfahren nicht tragbar. Hier bietet sich die Benutzung einer fortgeschrittenen elektronischen Signatur an.

Es muss an dieser Stelle auf eine noch nicht erwähnte Beziehung der Hochschulangehörigen untereinander aufmerksam gemacht werden. Als Beispielanwendungen für diese Beziehung sind der signierte oder verschlüsselte Austausch von E-Mails sowie der Zugang zu Rechnern und Netzwerken zu nennen.

Ganz ähnlich gestalten sich die Anwendungen in der Beziehung *interne Verwaltungsabläufe*, für die aufgrund des internen Charakters fortgeschrittene elektronische Signaturen Verwendung finden können. Als Anwendungen sind zu nennen:

- Signieren und Verschlüsseln von E-Mails und Dateien
- Signieren und Bearbeiten von elektronischen Akten, z. B. von Studienbüchern
- Elektronische Archivierung von elektronischen Akten und sonstigen Dokumenten
- Zugang zu Rechnern und Netzwerken

In der Beziehung *externe Verwaltungsabläufe* werden alle Kommunikationsprozesse zusammengefasst, bei denen ein Partner nicht Angehöriger der Hochschule ist. Die wichtigsten Anwendungen sind:

- Versand von Ausschreibungsunterlagen
- Eingehende Angebote nach einer Ausschreibung
- Einkauf/Bestellung von Sachmitteln
- Zugriff auf amtliche Verzeichnisse (z. B. Grundbuch)

Für alle das Privatrecht berührenden Prozesse – wie den Einkauf von Sachmitteln – ist die Verwendung von qualifizierten elektronischen Signaturen gemäß Signaturgesetz zwingend erforderlich, wobei das für die Kommunikation mit Behörden zurzeit nicht klar festgelegt ist. Eine Änderung des Verwaltungsverfahrensgesetzes ist zurzeit in Arbeit. Nach heutigem Stand wird ebenfalls die Verwendung einer qualifizierten elektronischen Signatur notwendig werden.

Die ersten Schritte an der HU

Es wurde bis jetzt viel über Möglichkeiten und Potentiale der virtuellen Hochschulverwaltung geschrieben. Doch gibt es das Prinzip der elektronischen Signatur und der Zertifikate seit etwa zehn und das Signaturgesetz seit fünf Jahren, und trotzdem mangelt es noch immer an konsequenten Umsetzungen dieser Technologie. Das liegt zum einen an notwendigen tiefgreifenden organisatorischen Veränderungen in Verwaltung und Organisation selbst und zum anderen am Fehlen einheitlicher Standards. Viele – wie auch die HU

– gehen den schrittweisen Weg, einzelne Dienstleistungen online zur Verfügung zu stellen, um Erfahrungen zu sammeln.

Es ist zum Beispiel für Studierende und Mitarbeiter schon heute möglich, die Einschreibung zu einem Kurs des Hochschulsports oder des Sprachenzentrums online zu erledigen. Diese Einschreibung hat vorerst reservierenden Charakter und erhält erst nach erfolgter Bezahlung der Kursgebühr ihre Gültigkeit. In diesem Szenario würde die Verwendung einer elektronischen Signatur keinen Gewinn bringen.

Weiterhin können sich Studierende und Mitarbeiter über ein Benutzername-/Passwortsystem unter anderem einen Überblick über ihre bei der zentralen Universitätsbibliothek ausgeliehenen medialen Objekte sowie einen eventuell vorhandenen Gebührenstand verschaffen. Der Einsatz einer elektronischen Signatur würde in dieser Anwendung die Vertraulichkeit der Daten erhöhen, indem ein Nutzer sich mit Hilfe seiner Signatur gegenüber dem Bibliotheksserver identifiziert und authentifiziert. Außerdem würde der Nutzer von dem erneuten Merken eines Passwortes entbunden werden.

Diese Technik könnte weitere Passwortsysteme ablösen und somit die Passwortflut eindämmen. Dieser Versuch wird zurzeit in dem neu entstehenden „Informations- und Kommunikationszentrum Adlershof (IKA)“ unternommen, indem der Zugang zu den öffentlichen Computerarbeitsplätzen und damit zu Dienstleistungen des RZ und der Universitätsbibliothek zertifikatbasiert, d. h. mit Hilfe einer elektronischen Signatur erfolgen soll. Da mit dieser Methode ein Nutzer erheblich sicherer authentifiziert werden kann, wird es möglich, bestimmte Dienstleistungen wie das Drucken von Dokumenten nutzerbezogen abzurechnen. Mit einem Passwortverfahren würde immer die Gefahr des Ausspähens eines Passwortes und damit die Möglichkeit der Fremdabrechnung eines Druckauftrages bestehen.

In dem Pilotprojekt *UVsec* wird die Anwendung der fortgeschrittenen elektronischen Signatur für interne Verwaltungsabläufe getestet. Im Zuge der Dezentralisierung von Verwaltungsaufgaben müssen Fakultäten, Institute und Zentraleinrichtungen auf sensible Finanz- und Personaldaten in dem durch eine Firewall geschützten Verwaltungsnetz über das offene Universitätsnetz zugreifen können. Ein solcher Dienst erfordert eine starke Authentifizierung über eine fortgeschrittene elektronische Signatur der berechtigten Nutzer sowie die Verschlüsselung der Daten. Dazu wird der zertifkatbasierte dezentrale Zugriff über ein Virtual Private Network (VPN) über IPsec realisiert werden. Als erste konkrete Anwendungen sind hier die folgenden vorgesehen:

- Dezentrale Bearbeitung der Adreßdatenbank
- Dezentrale Bearbeitung der Gehaltsdaten im LOGA-System
- Dezentrale Bearbeitung der Forschungsdatenbank
- Dezentraler Zugriff auf einzelne Komponenten des Facility Management Systems

Neben dem dezentralen Zugriff auf sensible Daten ist die E-Mail-Kommunikation zwischen den zentralen und dezentralen Bereichen der Verwaltung abzusichern. Dazu soll den Mitarbeitern die Möglichkeit gegeben werden, ihre E-Mails elektronisch signieren und verschlüsseln zu können. Schon 1997 begann die HU die Zertifizierungsinstanz HU-CA zu betreiben, die ihrerseits von der Zertifizierungsinstanz des DFN-Vereins DFN-PCA zertifiziert ist. Die HU-CA stellt Zertifikate im Format S/MIMEv2 aus, das von den E-Mail-Programmen MS Outlook (Express) und Netscape Messenger standardmäßig unterstützt wird. Das Signaturschlüsselpaar und das zugehörige Zertifikat werden auf einer Smartcard gespeichert, was das Ausspionieren des geheimen Signaturschlüssels erheblich erschwert. Somit sind Vertraulichkeit, Integrität und Authentizität der Daten in einer verschlüsselten und signierten E-Mail realisiert.

Es soll abschließend noch erwähnt werden, dass ein Nutzer prinzipiell alle genannten Anwendungen mit einer einzigen Smartcard und Schlüsselpaar(en) mit zugehörige(m/n) Zertifikat(en) bedienen könnte. Doch leider erlauben es die bis heute entwickelten Standards und Anwendungen nicht, zum Beispiel ein Zertifikat für die E-Mail-Signierung gleichzeitig für den Aufbau ein IPsec-Verbindung zu benutzen. Hier gibt es noch erheblichen Entwicklungsbedarf, der unter anderem durch Projekte verschiedener Bundesministerien wie MEDIA@Komm, DOMEA, SPHINX, eVergabe und Elster gedeckt werden soll.

Matthias Schwan
matthias.schwan@rz.hu-berlin.de