Elektronische Signaturen für Online-Dienste an Universitäten und Fachhochschulen

Martin Wind

Universität Bremen
FB 3, Technologie-Zentrum Informatik
Institut für Software-Ergonomie und Informationsmanagement
wind@tzi.de
http://infosoc.informatik.uni-bremen.de

1 Ein Blick in die heutige Online-Welt

Das Internet beeindruckt nach wie vor durch die rasant steigende Zahl der angeschlossenen Rechner. Inzwischen ist aber deutlich geworden, dass längst nicht jeder Internetzugang auch tatsächlich genutzt wird [KW00]. Die jüngste Eurobarometer-Erhebung hat zudem nochmals bestätigt, dass Transaktionen (Homebanking, Bestellungen von Büchern oder CDs, Auktionen usw.) im Vergleich zu Anwendungen wie E-Mail, Downloads oder Computerspielen in der Gunst der Nutzerinnen und Nutzer einen deutlich geringeren Stellenwert einnehmen [In00].

Es gibt viele Gründe, warum das Internet im privaten Bereich bis heute bevorzugt für eher unverbindliche und wenig anspruchsvolle Dienste genutzt wird. Erschwerend kommt in jedem Fall hinzu, dass vor dem Eintritt in die Welt der Online-Transaktionen einige Hürden zu bewältigen sind. Betrachten wir als Beispiel einmal die Eröffnung eines Online-Kontos: Zwar können sich die zukünftigen Kundinnen und Kunden auf den Internet-Seiten einer Bank über deren Leistungen und Gebührensätze informieren, auch ein Antragsformular kann aufgerufen und am Bildschirm ausgefüllt werden, dann ist aber schon der Zeitpunkt gekommen, sich aus dem Internet zu verabschieden und den Rest der Formalitäten offline auf den Weg zu bringen: Das Formular muss unterschrieben und per Post an die Bank geschickt werden. Diese wird ihrerseits Mitteilungen über die Kontoeröffnung, Nutzerkennungen, Zugangscodes etc. auf dem Postweg versenden und in der Regel das Post-Ident-Verfahren in Anspruch nehmen, um sich Gewissheit über die Identität des Neukunden zu verschaffen. Das heißt: Der Briefträger klingelt, bittet um Vorlage des Personalausweises und bestätigt der Bank als Auftraggeber die persönlichen Daten des Kontoinhabers. Bis zur ersten Online-Buchung müssen die neuen Geschäftspartner also mehrmals postalisch miteinander korrespondieren, was durchaus einige Wochen in Anspruch nehmen kann.

Wie einfach wäre es, könnte der am Bildschirm ausgefüllte Antrag mit einer elektronischen Signatur als dem Pendant zur handschriftlichen Unterschrift versehen werden. Für die weiteren Angaben zur Person wäre noch eine Art elektronischer Identitätsnachweis beizufügen (entgegen manchen Verlautbarungen erfüllen elektronische Signaturen genau diese Funktion nämlich nicht!) und schon könnte der Antrag auf Kontoeröffnung komplett online abgewickelt werden. Die Bank würde den in elektronischer Form eingegangenen Antrag prüfen, weitere Formulare und Mitteilungen verschlüsselt übermitteln und den öffentlichen Signaturschlüssel des Neukunden im System hinterlegen. Dieser könnte sodann

seinen dazu passenden, auf einer Signaturkarte gespeicherten privaten Schlüssel für die Erledigung seiner Bankgeschäfte nutzen. Der Sprung von der Eröffnung eines Online-Kontos zur Online-Kontoeröffnung wäre geglückt!

Dieses Beispiel zeigt, dass der Internet-Geschäftsverkehr durch die Nutzung elektronischer Signaturen wesentlich vereinfacht werden kann. Ein einziges Schlüsselpaar könnte in vielen Feldern verwendet werden, statt einer Vielzahl an Karten und Zugangscodes wäre nur noch eine einzige Karte plus PIN erforderlich, Einbußen in Sachen Sicherheit oder Datenschutz sind nicht zu befürchten. Doch bis elektronische Signaturen so vielfältig genutzt werden können, ist noch ein weiter Weg zurückzulegen. Bislang mangelt es an signaturbasierten Diensten und ehrlicherweise muss zugestanden werden, dass der Erwerb einer Signaturkarte in den meisten Fällen mindestens so unkomfortabel und kompliziert ist wie die Eröffnung eines Online-Kontos.

Um den Einsatz elektronischer Signaturen zu erproben und Erfahrungen sammeln zu können, wurde kurz nach Inkrafttreten des ersten deutschen Signaturgesetzes der Städtewettbewerb Multimedia MEDIA@Komm ins Leben gerufen. Aus einem dreistufigen Verfahren gingen die Städte Bremen und Esslingen sowie ein Verbund unter der Federführung Nürnbergs als Sieger hervor. Nachfolgend werden einige wesentliche Elemente des Bremer Konzepts und die in diesen Kontext eingebetteten signaturbasierten Online-Dienste für Studierende vorgestellt. Ausgehend von diesen Einblicken in die "Projektwerkstatt" wird abschließend diskutiert, welche Fortschritte und Probleme bei Verbreitung und Verwendung elektronischer Signaturen bislang deutlich geworden sind und welcher Handlungsbedarf zu konstatieren ist.

2 Kurzer Überblick über das Bremer MEDIA@Komm-Projekt

Nachdem die Freie Hansestadt Bremen im März 1999 vom Bundesministerium für Wirtschaft und Technologie als eine der drei Siegerstädte ausgezeichnet worden war, musste das eingereichte Konzept in einen förderfähigen Antrag für ein Forschungs- und Entwicklungsvorhaben umgewandelt werden. Die dreijährige Laufzeit begann im September 1999. Ein Jahr später präsentierte die in Public-Private-Partnership neu gegründete Entwicklungs- und Betriebsgesellschaft bremen online services GmbH & Co. KG (bos) auf dem MEDIA@Komm-Kongress in Bremen die ersten Online-Dienstleistungen mit integrierter Bezahlfunktion (Geldkarten-Zahlung übers Internet). In der Folgezeit wurde deutlich, dass der ursprüngliche Plan, auf Standards und Plattform-Lösungen aus dem Homebanking-Sektor aufzusetzen, aufgegeben werden musste. Der Hauptgrund bestand darin, dass der Nutzung elektronischer Signaturen ein anderes Rollenmodell zugrunde liegt als wir es vom Homebanking kennen. Im einen Fall kommunizieren zwei Partner, die sich kennen (eins-zu-eins-Beziehung), im anderen Fall soll mit der elektronischen Signatur der Zugang zu einer Vielzahl von Angeboten unterschiedlicher Anbieter (eins-zu-viele-Beziehung) eröffnet werden. Diese unterschiedlichen Rollenmodelle verlangen nach spezifischen technischen Lösungen. Folgerichtig wurde in der Zeit bis zum zweiten MEDIA@Komm-Kongress, der im Juni 2001 in Esslingen stattfand, die technologische Basis von Grund auf umgestellt.

Die in Bremen entwickelten Anwendungen verfolgen das Ziel, zwischen Bürgern, Verwaltung und weiteren Dienstleistern rechtsverbindliche Transaktionen vollelektronisch und

ohne Medienbrüche abwickeln zu können. Zu diesem Zweck wird in Abstimmung mit dem Projektträger, der wissenschaftlichen Begleitforschung zu MEDIA@Komm und einer Reihe weiterer Institutionen wie dem Bundesamt für Sicherheit in der Informationstechnik und den kommunalen Spitzenverbänden der Protokollstandard "Online Services Computer Interface" (OSCI) entwickelt. Nachdem die Version 1.0 der OSCI-Spezifikation vorlag, wurde ein Kernel programmiert, der anwendungsübergreifend benötigte Funktionen zum Signieren und Chiffrieren, zur Anbindung von Kartenlesegeräten, zur Visualisierung der zu signierenden Daten usw. zur Verfügung stellt.

Außerdem wurden im Zusammenhang mit der OSCI-Entwicklung Aktivitäten initiiert, um die mit einzelnen Geschäftsvorfällen verbundenen Inhaltsdaten in Form von XML-Dokumenten zu standardisieren. Sollte sich zumindest im öffentlichen Sektor OSCI als Standard für die Abwicklung rechtsverbindlicher Transaktionen mit elektronischen Signaturen durchsetzen und sollte es ferner gelingen, sich auf die Verwendung von XML und die Standardisierung von Datensätzen zu verständigen, wäre dies ein Meilenstein für Electronic Government in Deutschland. Bis heute gibt es beispielsweise keine Möglichkeit, bei einem Umzug in eine andere Stadt die Meldedaten elektronisch zu übermitteln. Standardisierung könnte in datenschützerisch unproblematischen Fällen wie diesem den Aufwand für die Verwaltungen senken und den Service für die Bürgerinnen und Bürger deutlich verbessern.

Das Bremer Konzept sieht vor, dass zwischen Bürgerinnen und Bürgern auf der einen und den öffentlichen und privaten Dienstleistern auf der anderen Seite ein Intermediär, in diesem Fall die Firma bremen online services, zwischengeschaltet wird, der zentrale Dienste wie die Abwicklung des Zahlungsverkehrs mit Systemen der Kreditwirtschaft, die Überprüfung von Signaturzertifikaten gegenüber den Servern der Trust Center etc. erbringt. Andernfalls wäre es erforderlich, dass jeder beteiligte Dienstleister selbst entsprechende Systeme vorhält, was wirtschaftlich nicht zu vertreten ist. Da OSCI mehrere Ebenen des Datenverkehrs unterscheidet, kann der Intermediär seine Dienste ohne Kenntnis der ausschließlich vom Empfänger dechiffrierbaren Inhaltsdaten erbringen.

Neben dem Aufbau einer technischen Plattform und der Entwicklung des OSCI-Protokolls besteht ein weiterer Schwerpunkt des Vorhabens in Maßnahmen, die den Zugang zu neuen Online-Diensten erleichtern sollen. Dazu werden beispielsweise an verschiedenen Stellen im Stadtgebiet betreute Nutzerplätze eingerichtet. Dort können Anwender Fragen klären oder bei Bedarf Hilfestellungen im Umgang mit der Signaturkarte oder der Abwicklung einzelner Geschäftsvorfälle in Anspruch nehmen. Während der Projektlaufzeit wird mit dem Trust Center der Telekom (TeleSec) kooperiert, aus einem begrenzten Kontingent an Fördermitteln können Signaturkarten stark verbilligt ausgegeben werden. Inzwischen sind ergänzend zu den Nutzerplätzen mehrere Registrierungsstellen eingerichtet worden, an denen Interessierte ihre Signaturkarte bestellen können. Dort sind auch spezielle Kartenlesegeräte erhältlich, die ebenfalls stark verbilligt ausgegeben werden. Diese Leser können nicht nur zum Signieren genutzt werden können, sondern sind von der Kreditwirtschaft für die Geldkarten-Zahlung übers Internet zugelassen worden.

Diese Form der vergünstigten Technikausstattung ist selbstverständlich nur im Rahmen eines Pilotprojektes tragbar. Das Bremer Konzept geht davon aus, dass in absehbarer Zeit eine Integration von Zahl- und Signierfunktionen auf den Karten der Kreditwirtschaft er-

folgt. Einzelne Institute haben dies bereits für die ab 2002 ausgegebene nächste Generation der EC-Karten angekündigt. Mit steigender Verbreitung entsprechender Angebote werden dann auch die benötigten Lesegeräte zu attraktiveren Konditionen erhältlich sein. Bremen setzt also auf marktgängige Produkte. Kein am Projekt beteiligter Dienstleister beabsichtigt, eine eigene Public-Key-Infrastruktur aufzubauen oder eigene Karten auszugeben. Die zentrale Herausforderung besteht vielmehr darin, über die Plattform des Intermediärs und die dem OSCI-Standard gehorchenden Anwendungen die Verarbeitung der von den kommerziellen Trust Centern verbreiteten Karten zu ermöglichen. Bislang können Produkte der TeleSec, der Deutschen Post (Signtrust) und der Datev genutzt werden. Diese Palette wird kontinuierlich ausgebaut.

Kernstück des Projekts sind natürlich die Anwendungen der beteiligten Dienstleister. Diese richten sich an unterschiedliche Zielgruppen: Direkt für die Bürgerinnen und Bürger sind Dienste wie Adressänderungen nach einem Umzug, die Bestellung von Urkunden beim Standesamt oder die Anwendungen der Hochschulen gedacht, auf die im nächsten Abschnitt noch näher einzugehen ist. Daneben gibt es eine Reihe von Angeboten, die sich an sogenannte Mittler wenden, womit Berufsgruppen gemeint sind, die regelmäßig im Auftrag Dritter Kontakte mit der Verwaltung unterhalten. Beispiele dafür sind Architekten, Rechtsanwälte, Notare, Steuerberater oder auch Kfz-Händler, die im Auftrag ihrer Kunden die Anmeldung eines Wagens übernehmen. An Unternehmen richten sich z.B. die derzeit in der Entwicklung befindlichen Angebote zur elektronischen Auftragsvergabe. Anwendungsübergreifend und für alle Nutzergruppen werden Zahlungsfunktionalitäten entwickelt. Neben der bereits mehrfach erwähnten Geldkartenzahlung sind Überweisungen, Lastschriftverfahren und Kreditkartenzahlungen vorgesehen. Die Anwendungen werden in der Regel als Signed Java Applications realisiert. Durch die Nutzung der neuen Java Web Start-Technologie von Sun (http://java.sun.com/products/javawebstart) wird Browser-Unabhängigkeit erreicht.

In der zurückliegenden Laufzeit konnten die drei Säulen des Bremer Pojekts – Zugang, Plattform, Anwendungen – so weit entwickelt werden, dass inzwischen ein ansehnliches Spektrum an Online-Diensten umgesetzt werden konnte (Einstieg über: http://www.bremer-online-service.de). Im Sinne des Projektmottos, Kundenorientierung durch Integration elektronischer Dienstleistungen für Bürger und Wirtschaft aus einer Hand, wird dieses Angebot kontinuierlich erweitert. Ein weiteres Ziel bestand in der Übertragbarkeit der Ergebnisse auf Anwendungsfelder außerhalb Bremens. Dem dient die frei abrufbare Spezifikation des OSCI-Standards (www.bos-bremen.de), zudem wird seit Mitte 2001 das Lizenzprodukt OSCAR (“OSCI-Architecture”) angeboten. Alle Spezifikationen und Lösungen setzen so weit wie möglich auf Open-Source-Produkte und ermöglichen es anderen Dienstleistern, ihren Kunden signaturbasierte Angebote zu unterbreiten, ohne das Rad neu erfinden, sprich: sich in die Grundlagen der Signaturtechnologie einarbeiten zu müssen.

3 Signaturbasierte Online-Dienste für Studierende

Ein Anwendungsfeld im Rahmen der Bremer MEDIA@Komm-Aktivitäten, das sich direkt an die Bürgerinnen und Bürger richtet, ist der Teilbereich Studium. Entwickelt werden Angebote für Studierende der Universität Bremen sowie der (Fach)Hochschulen Bremen

und Bremerhaven. Damit wird einer überschaubaren Zielgruppe mit überdurchschnittlichen Medienkompetenzen angeboten, Signaturkarten zur Erledigung der studiumsbegleitenden Verwaltungsangelegenheiten zu nutzen.

Solche Online-Dienste entlasten die Hochschulverwaltungen von Routinearbeiten, ermöglichen die Konzentration auf die durch Internationalisierung und neue Studiengänge (Bachelor, Master) zunehmend anspruchsvollere Beratung von Studierenden und Studieninteressenten und entsprechen darüber hinaus der Erwartungshaltung der zukünftigen Generation von Studierenden: Junge Schulabgänger sind mit Handy, PC und Internet groß geworden. Sie informieren sich im Internet über Studienangebote und erwarten, später auch den unvermeidlichen "Verwaltungskram", der jedes Studium begleitet, online erledigen zu können. Moderne, technologisch aufgeschlossene und serviceorientierte Hochschulen nutzen das Internet also nicht nur zur Selbstdarstellung, sondern ebenso als Medium für die Kommunikation mit den Studierenden.

Analog zur Vorgehensweise in den übrigen Teilprojekten des Bremer MEDIA@Komm-Vorhabens bestand auch an Universität und Hochschulen der erste Schritt in einer Geschäftsprozessanalyse. Dies diente zum einen der hochschulübergreifenden Anpassung und Vereinheitlichung ausgewählter Verwaltungsprozesse, zum anderen wurden Prioritäten für die Online-Umsetzung gesetzt. Präferiert wurden Vorgänge, die keine zusätzlichen Anlagen auf Papier benötigen, bei denen aufgrund der Fallzahlen deutliche Entlastungen für die Verwaltungen zu erwarten sind, die einen erkennbaren Mehrwert für die Studierenden bieten (Zugewinn an Zeitsouveränität, Kontrolle über personenbezogene Daten, Transparenz über Verfahrensabläufe) und die technisch mit vertretbarem Aufwand umsetzbar erschienen. Die Liste der vorgesehenen Geschäftsvorfälle reicht von vergleichsweise einfachen Vorgängen wie der Mitteilung einer Adressänderung oder der Beantragung eines Urlaubssemesters bis zu komplexeren Anwendungen wie der An- und Abmeldung zu Prüfungen oder dem selbsttätig veranlassten Ausdruck von Leistungsnachweisen. Ergänzend werden Verfahren zur Online-Zulassung bzw. –Immatrikulation realisiert, bei denen parallel zu den elektronisch übermittelten Daten die erforderlichen Dokumente per Post eingereicht werden müssen. Bei diesen Anwendungen ist es auch nicht erforderlich, eine elektronische Signatur zu besitzen. Die Ergebnisse der Geschäftsprozessanalyse wurden anschließend in Form eines dv-technischen Feinkonzepts fortgeschrieben, das die Grundlage für die nachfolgenden Programmierungsarbeiten darstellt.

Die Ergebnisse der einzelnen Teilschritte mussten mit der zeitgleich an anderer Stelle stattfindenden Entwicklung des Protokollstandards OSCI und dem Aufbau der Plattform bei bremen online services als Intermediär abgestimmt werden. Dies stellte einige Zeit durchaus ein Problem dar, da Fragen zu den technischen Vorgaben, die von den Anwendungen zwingend einzuhalten sind, nicht immer unmittelbar geklärt werden konnten. Rückblickend erwies es sich aber als sehr hilfreich, dass die Anforderungen der einzelnen Teilprojekte noch in die Entwicklung der OSCI-Spezifikation 1.0 einfließen konnten und umgekehrt im Zuge der dortigen Entwicklungsarbeiten manche Ideen aufkamen, die von den mit der Anwendungskonzeption betrauten Gruppen dankbar aufgenommen wurden. Insofern profitierten beide "Baustellen" voneinander.

Geleitet wird das Teilprojekt zur Entwicklung signaturbasierter Online-Dienste für Studierende im Auftrag von bremen online services durch das Institut für Informationsma-

nagement und Software-Ergonomie des Technologie-Zentrum Informatik an der Bremen. Die fachlichen Anforderungen sind in Projektgruppen der Universität und der Hochschulen sowie in einer zur Anwendungsentwicklung eingerichteten hochschulübergreifenden Arbeitsgruppe benannt und spezifiziert worden. Hier hat es sich als hilfreich erwiesen, dass im Projektkontext sogenannte "Entlasterkräfte" mit befristeten Verträgen eingestellt werden konnten, um die durch das Projekt anfallende Mehrarbeit zu kompensieren. Die Koordination der Projektarbeit erfolgt durch eine Steuerungsgruppe, der Vertreter aller beteiligten Institutionen und ein Mitarbeiter des Landesbeauftragten für den Datenschutz angehören. An der Universität Bremen wurde außerdem eine Beratergruppe des Akademischen Senats eingerichtet. Mit der Durchführung der Geschäftsprozessanalysen und der Entwicklung des dv-technischen Feinkonzepts sind Fremdfirmen beauftragt worden, die Programmierung der Anwendungen erfolgt durch Mitarbeiter von bremen online services.

In der eigentlichen Realisierungsphase sind abermals mehrere Teilschritte vorgesehen.[1] Zunächst wurden einfache Formulare umgesetzt, die in elektronisch signierter Form von den Studierenden abgeschickt werden. Der Intermediär prüft die Gültigkeit des zugehörigen Signatur-Zertifikats, um auszuschließen, dass Unbefugte mit gestohlenen oder verloren gegangenen Karten Vorgänge im Namen anderer durchführen (wozu allerdings zusätzlich die geheime PIN erforderlich wäre). Im positiven Fall wird die Nachricht an die Verwaltungen weitergeschickt, wo sie per E-Mail eingeht. Der nächste Entwicklungsschritt besteht darin, in enger Zusammenarbeit mit den Herstellern der Fachverfahren, in Bremen und Bremerhaven ist dies in den meisten Fällen die Hochschul-Informations-System GmbH (HIS), Schnittstellen zu entwickeln, um den Direktzugriff auf das Fachsystem ohne Einschaltung der Sachbearbeitung zu ermöglichen. In anderen Fällen, insbesondere im Bereich der Prüfungsverwaltung, werden momentan noch vorläufige Varianten verfolgt, da an Universität und Hochschule die erforderlichen Prüfungsverwaltungssysteme zur Zeit erst eingeführt werden. Sobald diese verfügbar sind, soll auch hier ein signaturbasierter Zugriff eingerichtet werden.

Der Ablauf eines typischen Online-Geschäftsvorfalls erfolgt in den nachfolgend beschriebenen Schritten (s. Abb.), wobei die Daten ausschließlich in verschlüsselter Form zwischen den beteiligten Partnern übermittelt werden:

1. Die Studierenden rufen den gewünschten Geschäftsvorfall auf und erhalten zunächst ein Formular, in das sie ihre Matrikelnummer eintragen. Das Formular wird signiert und abgeschickt.
2. Der Intermediär prüft gegen den Server des Trust Centers, ob das Signatur-Zertifikat des Nutzers noch gültig ist.
3. Nach positiver Prüfung wird die Nachricht ans Fachverfahren weitergeleitet. Dort wird anhand der Matrikelnummer und des aus dem Zertifikat ausgelesenen Namens der erforderliche Datensatz des Studierenden aufgerufen.
4. In das für den speziellen Geschäftsvorfall benötigte Formular werden personenbezogene Angaben eingetragen, so dass der Nutzer sich diesen Erfassungsaufwand ersparen kann.

[1] Informationen über Projektverlauf und den aktuellen Stand der Dinge sind über www.signatur.uni-bremen.de abrufbar.

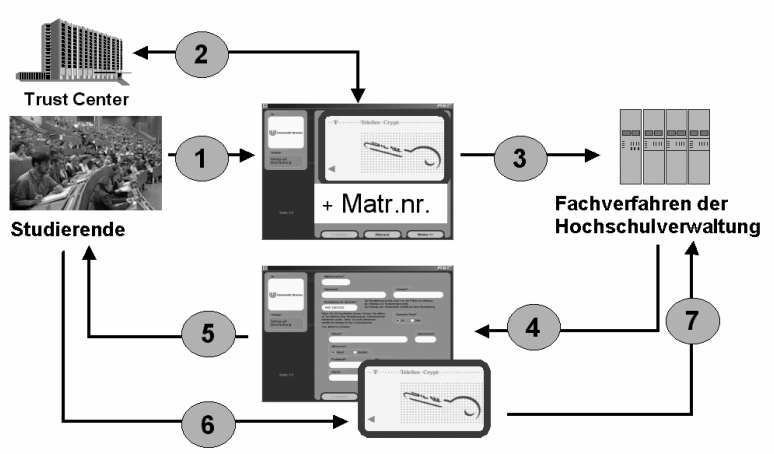

Abbildung 1. Ablauf eines signaturbasierten Online-Geschäftsvorfalls

5. Das Formular wird über die Plattform des Intermediärs an den Studierenden übermittelt.
6. Der Nutzer trägt die zusätzlich erforderlichen Angaben ein, signiert abermals und schickt das Formular ab.
7. Im Hochschulverfahren werden die entsprechenden Änderungen vorgenommen, die Studierenden können später online kontrollieren, ob die von ihnen online angestoßenen Vorgänge wunschgemäß abgeschlossen worden sind.

Die zu Beginn jeder Transaktion vorgesehene Authentifizierung gegenüber der Hochschul-Datenbank hat u.a. den Vorteil, dass geschäftsvorfallspezifische Daten ausgelesen und mitgeliefert werden können, die über die Durchführbarkeit eines Online-Geschäftsvorfalls entscheiden: Zum Beispiel geben die in Prüfungsverwaltungssystemen hinterlegten Prüfungsordnungen Auskunft über die Voraussetzungen, die erfüllt sein müssen, damit sich Studierende für weitere Leistungsnachweise anmelden können. Ein weiteres Beispiel: Das Bremische Hochschulgesetz regelt in §40, dass Beurlaubungen erst nach Abschluss des ersten Fachsemesters möglich sind und insgesamt zwei Semester nicht überschreiten sollen. Nur wenn vorab geprüft wurde, dass sich jemand mindestens im zweiten Fachsemester befindet und bislang höchstens ein Urlaubssemester in Anspruch genommen hat, kann der Vorgang vollständig online abgewickelt werden. In allen anderen Fällen wird es auch zukünftig erforderlich sein, Rücksprache mit der Studierendenverwaltung zu halten.

Abschließend lässt sich das Projekt an Universität und Hochschulen im Land Bremen durch folgende Besonderheiten charakterisieren:

– Mit der Verwendung elektronischer Signaturen, die mindestens den Anforderungen an qualifizierte elektronische Signaturen (§2 Nr. 2 SigG) entsprechen müssen, momentan aber sogar von akkreditierten Anbietern (§15 SigG) stammen, wird eine Technik genutzt, die Rechtssicherheit gewährleistet. Zugegeben: Dies ist bei den meisten, vermutlich sogar bei allen Geschäftsvorfällen im Kontext eines Studiums nicht zwingend

erforderlich. Doch angesichts der möglicherweise weitreichenden Konsequenzen von Transaktionen im Prüfungswesen ist es mindestens wünschenswert, eine Technik zu nutzen, der bei gerichtlichen Auseinandersetzungen hohe Beweisqualität zukommt. Viele Prüfungsordnungen schreiben zudem die Schriftform bei An- und Abmeldungen vor. Die Verwendung gesetzeskonformer Signaturen erleichtert es erfahrungsgemäß, für eine befristete Zeit zu Erprobungszwecken von dieser Vorschrift abweichen zu dürfen und im Erfolgsfall die erforderlichen Änderungen der Prüfungsordnung durchzusetzen.

- Es wird ausdrücklich darauf verzichtet, hochschulspezifische Karten auszugeben und eine eigene Infrastruktur (Terminals, Geräte zur Kartenpersonalisierung usw.) aufzubauen. Die bisherige Form der Studierendenausweise wird beibehalten, für den Zugang zum Online-Service werden marktgängige Produkte genutzt. Diese Form des Online-Angebots mag weniger prestigeträchtig sein als eine Multifunktionskarte mit dem Logo der jeweiligen Hochschule. Sie ist aber ungleich kostengünstiger, zumal auch die semesterweise Aktualisierung als traditionelle Schwachstelle vieler hochschulspezifischer Kartensysteme umgangen wird.
- Es handelt sich um ein offenes System ohne Bindung an (und Abhängigkeit von) einzelnen Karten- oder Systemlieferanten.
- Signaturkarten vereinheitlichen den Zugang zu Selbstbedienungsangeboten. Dies ist auch an Hochschulen keine Selbstverständlichkeit, werden doch in Studierendenverwaltungen auf der einen und den Prüfungsverwaltungen auf der anderen Seite gelegentlich schon Systeme unterschiedlicher Anbieter genutzt. Dies könnte zur Folge haben, dass für einen Urlaubsantrag der elektronische Studierendenausweis genügt, für eine Prüfungsanmeldung aber PIN und Transaktionsnummern erforderlich sind. Einheitliche, signaturbasierte Lösungen schaffen Abhilfe.
- Durch die hochschulübergreifende Entwicklungsarbeit und die Kooperation mit Anbietern der an Hochschulen eingesetzten Fachsysteme sind die im Rahmen des Bremer MEDIA@Komm-Vorhabens entwickelten Anwendungen durch ein hohes Maß an Übertragbarkeit gekennzeichnet.

3.1 Elektronische Signaturen – Fortschritte und Probleme

Die Diffusion elektronischer Signaturen ist sicherlich kein Selbstläufer. Dies wird allein schon durch den Umstand belegt, dass zwischen Inkrafttreten des ersten deutschen Signaturgesetzes im Jahr 1997 und den ersten signaturbasierten Anwendungen mehrere Jahre verstrichen sind. Bis heute reicht die Verbreitung von Signaturkarten kaum über einen kleinen Insiderkreis und die MEDIA@Komm-Regionen hinaus. Ohne entsprechende Online-Angebote gibt es für die Bürgerinnen und Bürger auch gar keinen Grund, sich eine Signaturkarte zu besorgen. Umgekehrt ist es für die Anbieter von Online-Diensten denkbar unattraktiv, ohne ein Mindestmaß an Verbreitung der Signaturkarten Anwendungen zu deren Nutzung zu entwickeln – obwohl solche Angebote im eigenen Interesse wären. Dieses "Henne-Ei-Problem" wird auch nicht durch den Städtewettbewerb MEDIA@Komm allein gelöst werden können.

Gleichwohl ist festzustellen, dass viele Punkte, die vor einiger Zeit noch als gestaltungsbedürftig angesehen wurden [Wi00] inzwischen angegangen worden sind. Folgende Fort-

schritte dürften sich förderlich auf die Verbreitung und Verwendung elektronischer Signaturen auswirken:

- Die zunehmende Zahl von Trust Centern wird die Phase der prohibitiven Gebührengestaltung hoffentlich bald beenden und sicherlich auch den Wettbewerb um nutzerfreundliche Produkte befördern.
- Lockerungen bei den gesetzlichen Schriftformerfordernissen eröffnen weitere Anwendungsfelder für elektronische Signaturen.
- Mit der Entwicklung des OSCI-Kernels steht eine Technik zur Verfügung, die mit Karten verschiedener Trust Center umgehen und Lesegeräte unterschiedlicher Anbieter ansprechen kann. Parallel dazu wurden die Bemühungen um die Interoperabilität der von Trust Centern angebotenen Leistungen und Produkte intensiviert.[2]
- Das neue Signaturgesetz erlaubt es den Trust Centern, Aufgaben an Dritte zu delegieren, sofern diese ins Sicherheitskonzept eingebunden sind (§4 Abs. 5 SigG). Dies eröffnet neue Wege, um den Bürgerinnen und Bürgern die Bestellung einer Signaturkarte zu erleichtern.
- Wie an anderer Stelle bereits erwähnt, planen erste Banken und Sparkassen, die neuen EC-Karten mit einer Signaturfunktionalität auszustatten.
- Last not least wurden im Umfeld von MEDIA@Komm wertvolle Entwicklungsarbeiten geleistet und Erfahrungen gesammelt. Dieses Wissen bleibt nicht ungenutzt, Vertreter der Preisträgerregionen arbeiten in einschlägigen Gremien mit und referieren ihre Ergebnisse auf Kongressen und Workshops.
- Auf der "Haben-Seite" ist also einiges zu verbuchen. Die Rahmenbedingungen wurden verbessert und werden sich weiterhin verbessern, die Anwendung der Technik durch Dienstleister und innerhalb von Organisationen muss nun folgen. Ausgelöst vielleicht auch durch das im Mai 2001 verabschiedete neue Signaturgesetz hat sich das Interesse an der Thematik spürbar erhöht. Dennoch sind noch einige Probleme auszuräumen:
- Das neue Gesetz hat mit der Unterscheidung unterschiedlicher Signaturarten einige Unsicherheiten hervorgerufen. Es sollte nun möglichst bald Klarheit herbeigeführt werden, wann qualifizierte Signaturen ausreichen und in welchen Fällen Produkte akkreditierter Anbieter verwendet werden müssen.
- Nach wie vor besteht erheblicher Aufklärungs- und Informationsbedarf. Funktion und Nutzen elektronischer Signaturen müssen erklärt werden, wobei die äußerst gewöhnungsbedürftige und in manchen Fällen schlicht unverständliche Terminologie des Gesetzestextes ("sichere Signaturerstellungseinheiten") nach Möglichkeit vermieden werden sollte. Gefordert sind alle Beteiligten – vom Bundesministerium für Wirtschaft und Technologie über die Trust Center bis hin zu Dienstleistern, die – wie die Freie Hansestadt Bremen – zukünftig rechtsverbindliche und sichere Transaktionen übers Internet abwickeln wollen.

[2] Dies betrifft insbesondere die Arbeiten an der "Industrial Signature Interoperability Specification" (ISIS; ausführlich dazu: www.t7-isis.org/ISIS/isis.html) sowie die Bemühungen um die Verknüpfung bestehender Sicherheitsinfrastrukturen durch eine sogenannte "Bridge-CA" (CA: Certification Authority; weitere Informationen unter: www.bridge-ca.org).

- Vor der ersten Online-Transaktion sind aufwändige Vorbereitungen seitens der Nutzer erforderlich, die sich eine Karte besorgen, Software installieren und einen Kartenleser anschließen müssen. Daran wird sich so schnell auch nichts ändern. Der damit verbundene Aufwand und ebenso die anfallenden Kosten werden sich nur lohnen, wenn möglichst viele Angelegenheiten mit dem einmal angeschafften und installierten Equipment genutzt werden können. Dies erfordert eine Konvergenz der für E-Banking, E-Commerce, E-Government usw. benötigten Technik.
- Aufgrund der Rechtsverbindlichkeit elektronisch signierter Dokumente werden hohe Sicherheitsanforderungen an Anwendungen und eingesetzte Komponenten gestellt. Dies ist sicherlich sinnvoll, geht in Teilen aber auf Kosten der Benutzerfreundlichkeit [Ku2001]. Hier sind sicherlich noch einige Diskussionen zwischen Sicherheits- und Usability-Experten erforderlich, bevor akzeptable Lösungen vorliegen.
- Bisweilen bereitet es Probleme, eine Person anhand ihres Signaturzertifikats zuverlässig zu identifizieren. Hier zeichnen sich unterschiedliche Lösungswege ab: In den allermeisten Fällen würde es bereits genügen, Geburtsdatum und -ort in ein zusätzliches Attributzertifikat aufzunehmen, das bei Bedarf vom Nutzer erfragt und von diesem zur Übermittlung freigegeben werden müsste. Einen eigenen – und damit leider proprietären – Weg hat die Bundesdruckerei mit ihrer "bCard" geplant: In Zusammenarbeit mit den Meldestellen ausgewählter Kommunen soll den Bürgerinnen und Bürgern eine Karte angeboten werden, auf der ergänzend zu den Signaturkomponenten die üblicherweise im Meldedatensatz enthaltenen Angaben gespeichert sind. Letztlich wird sich früher oder später auch in Deutschland die Frage stellen, ob der Personalausweis in seiner jetzigen Form eigentlich noch zeitgemäß ist oder in Richtung "Internet-Tauglichkeit" weiterentwickelt werden sollte. Hitzige Debatten werden bei diesem sensiblen Thema sicherlich nicht ausbleiben.

Bei so viel Licht und Schatten fällt es schwer, die Frage zu beantworten, ob sich elektronische Signaturen auf dem Weg zum Erfolgsmodell befinden. Versuchen wir es optimistisch mit einer dreigeteilten Antwort: Ja, elektronische Signaturen werden ein Erfolg, da mit zunehmender Häufigkeit elektronischer Transaktionen der Bedarf nach Sicherheit und Rechtsverbindlichkeit steigen wird. Ja, elektronische Signaturen werden ein Erfolg, da es unakzeptabel sein wird, den Nutzern für jeden neuen Online-Dienst eigene Zugangslösungen anzubieten. Ja, elektronische Signaturen werden ein Erfolg, aber wir sollten nicht vergessen, dass wir uns erst am Anfang eines komplizierten Diffusionsprozesses befinden.

Literatur

[In00] INRA Europe: Measuring Information Society. A Eurobarometer survey carried out for the European Commission (EB 53.0). Spring 2000.
http://europa.eu.int/ISPO/basics/measuring/eurobaro/eurobaro53/i_eurobaro53.html

[Ku01] Kubicek, H.: Die digitale Signatur zwischen Bürger und Verwaltung – Erleichterung oder Erschwernis? In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): 2001 – Odyssee im Cyberspace? Sicherheit im Internet. Tagungsband zum 7. Deutschen IT-Sicherheitskongress des BSI. Bonn/Ingelheim 2001, S. 11-22.

[KW00] Kubicek, H.; Welling, S.: Vor einer digitalen Spaltung in Deutschland? Annäherung an ein verdecktes Problem von wirtschafts- und gesellschaftspolitischer Brisanz. In: Medien & Kommunikationswissenschaft 4/2000, S. 497-517.

[Wi00] Wind, M.: Erfolgsmodell digitale Signatur? Rahmenbedingungen und Gestaltungsanforderungen. In: Lüttich, H.-J./Rautenstrauch, C. (Hrsg.): Verwaltungsinformatik 2000. Verwaltungsinformatik in Theorie, Anwendung und Hochschulausbildung. 3. Internationale Fachtagung "Verwaltungsinformatik" der Gesellschaft für Informatik. Halle (Saale), S. 340-352.