Albert-Ludwigs-Universität Freiburg
Institut für Informatik und Gesellschaft
Arbeitsgruppe Telematik, Prof. Dr. Günter Müller

eSign - Design und Implementierung eines Signierwerkzeugs auf einem mobilen Endgerät

Kurzfassung der Diplomarbeit von Michael Veeck, September 2002 – Mai 2003

Einleitung: In den letzten Jahren ist das Internet zu einem festen Bestandteil des alltäglichen Lebens geworden. Immer mehr E-Mails werden verschickt und immer mehr Waren werden über das Internet bestellt. Allein im letzten Jahr hat jeder fünfte Deutsche regelmäßig online eingekauft. Marktführer sind in diesem Geschäftsfeld die Auktionsplattform eBay mit zehn Millionen und der Onlineversender Amazon mit acht Millionen Kunden.[1]

Diese positiven Nachrichten für die Wirtschaft werden von der stark ansteigenden Internet-Kriminalitätsrate überschattet, die sich laut Jahresbericht des amerikanischen Internet Fraud Complaint Center im Jahre 2002 in den USA im Vergleich zum Vorjahreszeitraum verdreifacht hat[2]. Von den über 48.000 gemeldeten Fällen entfielen 46 Prozent auf Betrügereien bei Internetauktionen, 31 Prozent betrafen nicht ordnungsgemäß gelieferte oder nicht bezahlte Waren bei über das Internet getätigten Geschäftsabschlüssen. Die dabei für den Konsumenten entstandenen Schäden belaufen sich auf insgesamt 54 Millionen Dollar.

Diese Schäden rechtlich einzufordern ist oft nicht möglich, da der Geschäftspartner nicht mehr zu ermitteln ist. Die Anonymität, die das Internet bietet, ermöglicht Betrügereien, die beim Einkaufen in einem Ladengeschäft nicht passieren können, da es dort dem Kunden zwar möglich ist, anonym aufzutreten und zu bezahlen. Der Verkäufer kann dies aber nicht tun. Er ist dem Kunden bekannt, übergibt diesem die Ware sofort und der Kunde kann eine Reklamation jederzeit geltend machen.

Das Ziel dieser Diplomarbeit und der prototypischen Implementierung der Software „eSign“ ist ein sowohl einfaches als auch sicheres Werkzeug zu entwickeln, welches es dem Benutzer ermöglicht, in elektronischen Medien zuverlässig Geschäfte tätigen zu können. Bestehende Sicherheitswerkzeuge zeichnen sich oft durch eine komplizierte Benutzeroberfläche aus, die den Benutzer bei der Erledigung seiner Aufgaben mehr verwirren als ihn unterstützen und somit mehr Sicherheitslücken öffnen als schliessen. Deshalb wird besonderer Wert auf eine intuitive Benutzerführung gelegt, unter der versteckt Mechanismen arbeiten, die dem Benutzer die Sicherheit seiner Daten und Aktionen gewährleisten können. In den folgenden Abschnitten wird der Inhalt der Arbeit in Kürze zusammengefasst, um einen ersten Einblick in selbige zu geben.

Die Digitale Signatur: Zu einem verlässlichen Geschäftsaufbau über das Internet muss die

1 http://www.heise.de/newsticker/data/see-10.04.03-000/
2 http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf

Identität des Gegenübers feststellbar und später vor einem Gericht als Nachweis einbringbar sein. Eine Lösung dafür existiert schon seit mehreren Jahren, die Digitale Signatur. Diese stellt im elektronischen Datenverkehr das Äquivalent zu der im Alltag gebräuchlichen handschriftlichen Unterschrift dar. Das erste Kapitel dieser Diplomarbeit erläutert sowohl die funktionalen Grundlagen der Digitalen Signatur als auch ihre Vorteile im elektronischen Geschäftsverkehr und ihre Grenzen.

Wie die handschriftliche Unterschrift unter einem Dokument bestätigt die Digitale Signatur das Einverständnis des Unterzeichners mit den darin stehenden Sachverhalten. Neben dieser schriftlichen Willenserklärung wohnen der Unterschrift eines Menschen Schutzfunktionen inne, die ihre sichere Benutzung im alltäglichen Geschäftsverkehr erst ermöglichen: Dies sind die Abschluß-, Echtheits-, Identitäts-, Warn- und Beweisfunktionen.

Es ist aber nicht ohne weiteres möglich, diese Funktionen auf die Digitale Unterschrift zu übertragen. Zum Beispiel wurde erst durch die Verabschiedung des Signaturgesetzes durch den Gesetzgeber im Jahre 2001 die Digitale Signatur der handschriftlichen in einem Gerichtsverfahren gleichgestellt und somit dieser die Beweisfunktion übertragen. Aber vor allem die Umsetzung der Warnfunktion, die den Benutzer vor übereilten Aktionen schützt, im Ablauf der Digitalen Signatur erfordert eine besondere Betrachtung und wird deshalb im zweiten Kapitel dieser Arbeit genauer ausgeführt..

Die Digitale Signatur bietet aber Möglichkeiten, die über die der handschriftlichen Unterschrift hinaus gehen. Sie garantiert zum Beispiel durch ihre mathematischen Grundlagen die Integrität des unterzeichneten Dokuments, welches somit nicht verändert werden kann, ohne die Signatur ungültig zu machen.

Jedoch ist der Digitalen Signatur der von Wirtschaft und Politik erhoffte Durchbruch bisher nicht gelungen. Die mangelnde Benutzbarkeit von aktuell verfügbaren Sicherheitswerkzeugen wie zum Beispiel der von der Deutschen Post entwickelten Signaturanwendung „Signtrust Mail“ und deren komplexen Funktionsweisen wurden von Gerd tom Markotten und Jendricke als Haupthindernis für eine weite Verbreitung der Digitalen Signatur identifiziert[3].

Um die Akzeptanz der Digitale Signatur in der Bevölkerung zu erhöhen, ist eine neue Art von Anwendungen erforderlich. Deren Aufgabe ist es, die komplexen Sicherheitsmechanismen, wie zum Beispiel die der Digitalen Signatur zugrundeliegenden asymmetrischen Kryptographie, mit einer für den Benutzer intuitiv bedienbaren Oberfläche zu kombinieren. Als solch eine Anwendung ist „eSign“ konzipiert. Sie verbirgt den Mechanismus der Digitalen Signatur vor dem Benutzer und signiert automatisch elektronische Dokumente für diesen. Für den Anwender besteht somit keine Veranlassung mehr, sich mit den komplexen mathematischen Algorithmen und verwirrenden Programmabläufen auseinandersetzen zu müssen.

Benutzerauthentifizierung: Die im vorherigen Abschnitt erwähnte und in der handschriftlichen Unterschrift implizit vorhandene Warnfunktion setzt eine willentliche und bewusste Aktion des Unterzeichners voraus, die nicht ohne sein Wissen ausgeführt werden kann, und ihn dadurch vor Fälschungen und übereilten Handlungen schützt. Um diese Schutzfunktion auch im Prozess des Digitalen Signierens zu implementieren, muss der Benutzer eines mobilen Endgerätes diesen Vorgang explizit autorisieren, indem er sich dem System gegenüber au-

3 Daniela Gerd tom Markotten und Uwe Jendricke: „Erfolgsfaktor für E-Commerce: Benutzbare Sicherheit“, Eingereicht für WI 2003, Dresden

thentifiziert. Im zweiten Teil dieser Diplomarbeit werden deshalb verschiedene Authentifizierungsmechanismen diskutiert.

Neben den gebräuchlichsten Methoden zur Authentifizierung durch Passwörter und PINs werden biometrische Verfahren betrachtet. Diese Erkennungsverfahren basieren auf dem Vergleich von körperlichen Charakteristika und können die eben genannten PIN-Authentifizierungen ersetzen, die allgemein als unzuverlässig und unsicher gelten. Ein biometrisches Merkmal kann aufgrund der natürlichen Variation des menschlichen Körpers nicht ohne weiteres dupliziert werden und auch nicht wie ein Passwort verloren, vergessen oder von Dritten kopiert werden. Bei korrektem Einsatz kann Biometrie somit den Sicherheitslevel des Gesamtsystems beträchtlich erhöhen.

Auch wenn die Erkennungsrate von heutigen biometrischen Systemen noch verbesserungswürdig ist, so ist doch abzusehen, dass auf längere Sicht die Biometrie die PIN bzw. Passwörter ablösen wird. Es lässt sich bereits jetzt beobachten, dass sich die biometrische Authentifizierung zu einem festen Bestandteil der Gesellschaft entwickelt. Sie ist zum Beispiel an einigen Flughäfen und Landesgrenzen im Einsatz und weitere Systeme, die bisher die herkömmlichen Verfahren wie PIN oder Passwörter benutzt haben, folgen dieser Tendenz.

Diese Arbeit kommt zu dem Ergebnis, dass eine biometrische Zugangskontrolle in Form der handschriftlichen Unterschrift zur Freischaltung der Digitalen Signatur am besten geeignet ist, um die Digitale Signatur des Benutzers zu autorisieren. Nicht nur ist die Unterschrift sehr fälschungssicher, da sie unsichtbare Daten beinhaltet, die nicht einfach ausgespäht werden können. Sie ist außerdem dem Anwender aus dem Alltag vertraut, was die Akzeptanz und die Benutzbarkeit erhöht, und sie kann ohne zusätzlichen Hardwareaufwand auf den meisten mobilen Endgeräten eingesetzt werden, da diese häufig eine Stifteingabe besitzen.

Implementierung und Ausblick: Im dritten und letzten Kapitel dieser Diplomarbeit wird die Implementierung von eSign auf einem PDA im Rahmen des von der Deutschen Forschungsgemeinschaft (DFG) geförderten Schwerpunkt-Programms "Sicherheit in der Kommunikations-Technik"[4] beschrieben. Der in dem SPP-Projekt verwendete PDA ist als Prototyp eines mobilen sicheren Endgerätes konzipiert, auf dem ein Referenzszenario mit sicheren und benutzbaren Anwendungen läuft. In diesem Szenario laufen die verschiedenen Einzelprojekte zusammen, wie zum Beispiel der Kauf eines Bahntickets mit digitalem Geld aber auch formale Methoden, die zur Sicherheit des Gesamtsystems beitragen. Unter den in dem Projekt geprägten Begriff der „Benutzbaren Sicherheit" fallen auch die sichere Verwaltung der personenbezogenen Daten des Benutzer und eine abgesicherte Kommunikation bei Verbindungen in potentiell unsichere Netze.

Die Ziele der Programmierung von eSign sind dabei eine spätere leichte Erweiterbarkeit des Programmcodes und eine für den Benutzer möglichst intuitiv bedienbare Oberfläche. Durch den modularen Aufbau von eSign sind dem Programmierer alle Möglichkeiten gegeben, um problemlos neue, effizientere Verifikationsalgorithmen zur Unterschriftserkennung einzubinden. Neue Dokumenttypen, die vom Benutzer signiert werden sollen, können genauso einfach hinzugefügt werden.

Auf den folgenden Bildschirmfotos ist der prinzipielle Ablauf bei der Benutzung von eSign zu sehen. Zuerst hat der Anwender die Daten eines Überweisungsauftrags an seine Bank zu be-

4 http://www.iig.uni-freiburg.de/telematik/spps/

stätigen, bevor er wie bei einem, ihm aus dem Alltag vertrauten, Überweisungsformular mit seiner Unterschrift den Überweisungsvorgang an die Bank starten kann.

Ohne eine weitere Aktion des Benutzers zu verlangen, vergleicht dann eSign die Unterschrift gegen eine gespeicherte Referenz und bei einer erfolgreichen Verifikation der Unterschrift werden die Überweisungsdaten automatisch digital signiert und an die Bank verschickt.

Trotz des prototypischen Charakters der Implementierung in das Gesamtsystem bleibt abschliessend festzuhalten, dass die hier vorgestellte Lösung einer unterschriftsbasierten Benutzerauthentifizierung als eine sehr gute Lösung anzusehen ist, um die Verwendung der Digitalen Signatur in der Gesellschaft zu fördern, da sie für den Benutzer intuitiv und dennoch sicher gestaltet wurde. Die Benutzung eines vertrauten Merkmals und die Verbergung von komplexen technischen Zusammenhängen vor dem Benutzer sind die Grundlage für die einfache Bedienbarkeit von eSign, während durch die Einbettung in das Gesamtprojekt die Sicherheit der biometrischen Daten und der Digitalen Signatur vor unberechtigtem Zugriff durch Dritte gewährleistet ist.