ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

INSTITUT FÜR INFORMATIK UND GESELLSCHAFT

Arbeitsgruppe Telematik

Prof. Dr. Günther Müller

eSign - Design und Implementierung eines Signierwerkzeugs auf einem mobilen Endgerät

Diplomarbeit

Michael Veeck

September 2002 – Mai 2003

Danksagung

An dieser Stelle möchte ich mich bei allen bedanken, die mich bei der Erstellung meiner Diplomarbeit unterstützt haben.

Besonders meinem Betreuer, Herrn Dr. Uwe Jendricke danke ich für die viele Zeit, die er sich für mich genommen hat. Er stand mir bei Fragen jederzeit hilfreich zur Seite und hat mich unterstützt, wo immer es ihm möglich war.

Ebenso möchte ich mich bei Prof. Dr. Günter Müller, Daniela Gerd tom Markotten und Sven Wohlgemuth für die vielen kleinen Tipps und die exzellente Arbeitsatmosphäre bedanken, sowie für ihr Engagement, mit der sie den CeBIT-Auftritt des Instituts zu einem Erfolg werden ließen.

Nicht zu vergessen meiner Freundin Kristina Wieland für ihre Verbesserungsvorschläge und ihre Geduld mit mir während der schriftlichen Ausarbeitung der Arbeit. Schließlich bedanke ich mich bei meiner Familie für die Unterstützung und Liebe, die sie mir nicht nur während meines Studiums entgegengebracht hat, und ohne die ich dies nicht hätte erreichen können.

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt und alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder unveröffentlichten Schriften entnommen wurden, als solche kenntlich gemacht habe. Außerdem erkläre ich, dass die Diplomarbeit nicht, auch nicht auszugsweise, bereits für eine andere Prüfung angefertigt wurde.

(Michael Veeck)
Freiburg, den 14. Mai 2003

Inhaltsverzeichnis

1 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 dabei die Auktionsplattform eBay mit zehn Millionen und der Onlineversender Amazon mit acht Millionen Kunden.[1]

Diese positiven Nachrichten für die Wirtschaft werden überschattet von einer ebenfalls stark ansteigenden Internet-Kriminalitätsrate, die sich laut des Jahresbericht des Internet Fraud Complaint Center im Jahre 2002 in den USA im Vergleich zum Vorjahreszeitraum verdreifacht hat [IFCC2003]. Von den über 48000 gemeldeten Vorfällen entfielen 46 Prozent auf Betrügereien bei Internetauktionen, 31 Prozent betrafen nicht ordnungsgemäß gelieferte oder nicht bezahlte Waren bei über das Internet getätigten Geschäftsabschlüssen.

Die den Konsumenten dabei entstandenen Schäden in Höhe von zusammengerechnet 54 Millionen Dollar rechtlich einzufordern ist oft nicht möglich, da der Geschäftspartner sich abgesetzt hat oder nicht mehr zu ermitteln ist. Die Anonymität, die das Internet bietet, ermöglicht Betrügereien, die beim Einkaufen im Laden nicht passieren können. Im Alltag ist es dem Kunden zwar möglich, 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 jederzeit zwecks Reklamationen zu ihm zurückkehren.

Wenn eine verlässliche Geschäftsbeziehung über das Internet aufgebaut werden soll, muss die 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 zur im Alltag gebräuchlichen handschriftlichen Unterschrift dar. Dennoch ist ihr 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 [GeJe2003]. Um die Akzeptanz der Digitale Signatur in der Bevölkerung zu erhöhen, ist eine neue Art von Anwendungen erfor-

1 http://www.heise.de/newsticker/data/see-10.04.03-000/

derlich. 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. Unter diesen Begriff der „Benutzbaren Sicherheit“ fällt auch die sichere Verwaltung der personenbezogenen Daten des Benutzer und eine abgesicherte Kommunikation bei Verbindungen in potentiell unsichere Netze.

Als solch eine Anwendung ist eSign konzipiert, das in dieser Arbeit vorgestellt wird. Sie verbirgt den Mechanismus der Digitalen Signatur, die im ersten Kapitel näher beschrieben wird, vor dem Benutzer und signiert automatisch für ihn die elektronischen Dokumente.

Um eine Digitale Signatur zu autorisieren, ist jedoch ein Zugangsschutz notwendig, der nur den berechtigten Benutzer eine Signatur erzeugen lässt. Im zweiten Kapitel werden deshalb verschiedene Authentifizierungsmechanismen diskutiert, angefangen von der PIN bis hin zu biometrischen Merkmalen, die auf der natürlichen Variation von menschlichen Eigenschaften basieren.

Im dritten und letzten Kapitel wird schließlich die Implementierung von eSign auf einem PDA im Rahmen des von der Deutschen Forschungsgemeinschaft (DFG) geförderten Schwerpunkt-Programms „Sicherheit in der Kommunikations-Technik“ [2] 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. Die Ziele der Programmierung von eSign sind dabei eine spätere leichte Erweiterbarkeit des Programm-Codes und eine für den Benutzer möglichst intuitiv bedienbare Oberfläche.

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

2 Die Digitale Signatur

Zu Beginn dieses Kapitels werden die handschriftliche Unterschrift und ihre Eigenschaften betrachtet. Danach werden neben den technischen auch die rechtlichen Grundlagen der digitalen Signatur eingeführt, sowie mögliche Anwendungsgebiete skizziert. Die Grenzen und Probleme des digitalen Signierens werden am Ende dieses Kapitels näher erläutert.

2.1 Die handschriftliche Unterschrift

Die handschriftliche Unterschrift unter einem Dokument bestätigt das Einverständnis des Unterzeichners mit den darin stehenden Sachverhalten. Dieses Dokument kann zum Beispiel ein Brief, ein Vertrag oder eine notariell bestätigte Urkunde sein. Neben dieser schriftlichen Willenserklärung wohnen der Unterschrift eines Menschen Schutzfunktionen inne, die ihre sichere Benutzung im alltäglichen Geschäftsverkehr erst ermöglichen. Diese werden von Roßnagel genauer ausgeführt [Ross94] und hier zusammengefasst präsentiert:

2.1.1 Schutzfunktionen der Unterschrift

Abschlußfunktion: Die Unterschrift kennzeichnet den Umfang des Dokuments und schließt den Signiervorgang ab. Durch sie wird ein Entwurf zu einem rechtskräftigen Dokument und somit für den Unterzeichnenden verbindlich.

Beweisfunktion: In einem Streitfall kann die Unterschrift als Beweismittel vor Gericht verwendet werden; dies ist durch Paragraph 415 der Zivilprozessordnung rechtlich verankert. Im Zweifelsfall können diese und das unterschriebene Dokument auch von einem Gutachter auf ihre Echtheit hin überprüft werden.

Echtheitsfunktion: Die Unterschrift gewährleistet die Unverfälschtheit des unterschriebenen Dokumentes, nachdem diese unter das Dokument gesetzt wurde und somit räumlich mit diesem verbunden ist. Veränderungen sind trotzdem nicht auszuschließen und können nur zum Teil durch besondere Vorkehrungen bei der Unterzeichnung ausgeschlossen werden, indem zum Beispiel ein Notar hinzugezogen wird, der als unabhängiger Dritter den gesamten Vorgang überwacht und bestätigt.

Identitätsfunktion: Die Unterschrift identifiziert den Unterzeichner eines Dokumentes und lässt eine spätere Zuordnung von Person und Dokument zu. Ein Unterzeichner kann somit nicht anonym auftreten, seine Identität verbergen oder eine andere Identität annehmen.

Warnfunktion: Der Akt des Unterschreibens setzt eine willentliche und bewusste Aktion des Unterzeichners voraus, die nicht ohne sein Wissen ausgeführt werden kann. Dies verdeutlicht für den Unterzeichner auch die Verbindlichkeit seiner Unterschrift.

2.1.2 Grenzen und Probleme

Ein Vertragsabschluss mit der handschriftlichen Unterschrift ist nicht auf elektronisch ausgeführte Geschäfte, wie zum Beispiel über das Internet, übertragbar, ohne dass die oben aufgeführten Schutzfunktionen verloren gehen.

Die Herangehensweise, an ein elektronisches Dokument eine weitere Datei anzuhängen, die zum Beispiel ein eingescanntes Bild der Unterschrift beinhaltet, berücksichtigt nicht die besonderen Eigenschaften dieses Mediums:

Elektronische Dokumente sind digitale Dateien und können mit geringstem Aufwand exakt kopiert werden, ohne dass ein Qualitätsverlust wie zum Beispiel bei einem Papierkopierer stattfindet. Das eingescannte Bild der Unterschrift kann von dem eigentlichen Dokument getrennt und an anderer Stelle wiederverwendet werden, ohne dass eine Fälschung erkennbar wäre. Somit ist auch die nachträgliche Änderung des Dokumentes jederzeit möglich, ohne dass die Unterschrift ihre Gültigkeit verliert.

Es muss also ein Mechanismus benutzt werden, der die von der handschriftlichen Unterschrift bekannten Abschluss-, Beweis-, Echtheits-, Identitäts- und Warnfunktion bereitstellt. Die Digitale Signatur bietet nicht nur diese Funktionalität sondern auch noch über dies hinausgehende Funktionen, die noch in Abschnitt 2.3 genauer ausgeführt werden.

2.2 Die Digitale Signatur

Die Digitale Signatur eines Dokumentes ist eine Prüfsumme, die in Verbindung mit dem signierten Dokument die Person identifizieren kann, die die Signatur erstellt hat. Diese Prüfsumme wird über eine mathematische Funktion berechnet, die als Parameter das zu signierende Dokument und nur dem Unterzeichner bekannte persönliche Daten erhält. Sie ist somit für jeden Unterzeichner und jedes Dokument unterschiedlich, so dass diese beiden anhand der Signatur eindeutig identifiziert werden können.

Die Schutzfunktionen der Echtheit und des Abschlusses werden durch die mathematischen Grundlagen der Digitalen Signatur gewährleistet, die im nächsten Abschnitt diskutiert werden; die Identitätsfunktion durch die Bereitstellung von Zertifikaten, die in Abschnitt 2.2.2 bespro-

chen werden. Die Beweisfunktion wird in Abschnitt 2.2.3 behandelt und die Erfüllung der Warnfunktion in Abschnitt 2.4.3.

2.2.1 Funktionsprinzip

Die Digitale Signatur basiert auf dem asymmetrischen Verschlüsselungsverfahren von Rivest et al., auch *Public-Key-Verfahren* genannt [RSA78]. Im Gegensatz zur symmetrischen Verschlüsselung, bei der zur Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird, besitzt jede Person X ein Schlüsselpaar bestehend aus einem öffentlichem C_x^{pub} und einem privaten Schlüssel C_x^{priv}.

Die Schlüssel sind bei diesem Verfahren komplementär zueinander, das heißt, dass eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht nur mit dem dazu passenden privaten Schlüssel wieder entschlüsselt werden kann. Der umgekehrte Weg ist ebenso möglich, jedoch kann eine Nachricht, die mit einem der beiden Schlüssel verschlüsselt wurde, nicht wie bei einem symmetrischen Verfahren mit demselben Schlüssel wieder entschlüsselt werden. Die Asymmetrie des Verfahrens bewirkt, das eine Datei *Doc*, die mit einem der beiden Schlüssel verschlüsselt wird, nur mit dem anderen Schlüssel des Paares entschlüsselt werden kann:

$$Doc = C_x^{priv}[C_x^{pub}[Doc]] = C_x^{pub}[C_x^{priv}[Doc]] \tag{2.1}$$

Eine Signatur *Sign* zu einem Dokument *Doc* wird erzeugt, indem dieses mit dem privaten Schlüssel verschlüsselt wird:

$$Sign = C_x^{priv}[Doc] \tag{2.2}$$

Ob nun ein Dokument von einer bestimmten Person X signiert wurde, wird überprüft, indem mit dem öffentlichen Schlüssel der Person die Signatur *Sign* dechiffriert wird. Als Ergebnis erhält man bei einer korrekter Signatur wieder das Originaldokument *Doc*:

$$Doc \stackrel{?}{=} C_x^{pub}[Sign] \stackrel{2.2}{=} C_x^{pub}[C_x^{priv}[Doc]] \stackrel{2.1}{=} Doc \tag{2.3}$$

Zu einem Dokument kann der Inhaber des privaten Schlüssel als einziger eine Signatur erstellen, die von seinem öffentlichen Schlüssel wieder entschlüsselt werden kann. Dieses Prinzip gewährleistet sowohl die Authentizität, was die Zuordnung von Signierendem und Dokument betrifft, als auch die Integrität, das heißt die Unverfälschtheit, eines digital signierten Dokumentes. Eine Veränderung der Daten verändert auch die Signatur, die aus diesen Daten erzeugt wird. Eine Manipulation des Dokumentes fällt somit durch Vergleich mit der Originalsignatur auf.

Diese asymmetrischen Verfahren setzen voraus, dass der private Schlüssel geheim bleibt und sich nicht aus dem öffentlich zugänglichen Schlüssel oder anderen Informationen wie zum Beispiel vorangegangenen Signaturen des Benutzers in überschaubarer Zeit berechnen lässt. Die

zugrunde liegenden asymmetrischen Kryptographiealgorithmen bauen auf komplexen mathematischen Problemen auf, wie zum Beispiel das zur Zeit noch am weitesten verbreitete Verfahren, das nach seinen Erfindern Rivest, Shamir und Adlemann benannte RSA-Verfahren. Es basiert auf dem Problem der Primfaktorzerlegung großer Zahlen [RSA78]. Bei den dort verwendeten Schlüssellängen von 1024 Bit wird für die Berechnung des geheimen Schlüssels selbst bei der Zusammenschaltung von großen Rechenzentren eine Dauer von mehr als 100 Jahren angenommen [Sc1996].

Je größer aber die Schlüssellänge ist, desto länger dauert es auch, bedingt durch die Komplexität der Algorithmen, die Signatur zu berechnen. Deshalb wird meist nicht das gesamte Dokument verschlüsselt, sondern nur eine Prüfsumme, die durch eine auf das Dokument angewandte, öffentlich bekannte Hashfunktion *Hash* berechnet wird. Diese Funktion verdichtet die Informationen des Dokumentes, wodurch Rechenzeit eingespart werden kann:

$$Sign = C_x^{priv}[Hash(Doc)] \tag{2.4}$$

Die Hashfunktion darf nicht umkehrbar sein, also aus einer Signatur darf nicht das ursprüngliche Dokument errechenbar sein, und sie muss möglichst kollisionsfrei sein, also zwei verschiedene Dokumente müssen möglichst immer zwei verschiedene Hashwerte haben. Diese Voraussetzungen an eine Hashfunktion sollen die nachträgliche Veränderung des Dokumentes und der Signatur verhindern.

Der verschlüsselte Hashwert wird als Signatur zusammen mit dem Dokument veröffentlicht. Um die Echtheit der Signatur zu überprüfen, wendet man die Hashfunktion auf das Dokument an und vergleicht den Wert mit der entschlüsselten Signatur. Bei der Übereinstimmung der Werte ist gewährleistet, dass die Signatur echt und das Dokument seit der Signierung unverändert geblieben ist:

$$Hash(Doc) \stackrel{?}{=} C_x^{pub}[Sign] \stackrel{2.4}{=} C_x^{pub}[C_x^{priv}[Hash(Doc)]] \stackrel{2.1}{=} Hash(Doc) \tag{2.5}$$

Damit ist jedoch noch nicht gewährleistet, dass die Signatur und somit auch der benutzte öffentliche Schlüssel zu einer bestimmten Person gehören. Jeder kann sich sein eigenes Schlüsselpaar erzeugen und unter einem beliebigen Namen den öffentlichen Schlüssel zum Beispiel im Internet verbreiten. Dies erlaubt Man-In-The-Middle-Angriffe, bei denen die Gesprächsteilnehmer nicht bemerken, dass ein Angreifer sich heimlich in die Kommunikation der beiden eingeschaltet hat und die signierte Nachricht auf dem Übertragungsweg verändert.

Um die Identitätsfunktion der Digitalen Signatur zu gewährleisten und zweifelsfrei eine Signatur einer Person zuzuordnen, wird eine *Public-Key-Infrastruktur* (PKI) benötigt. Zu dieser gehören Zertifikate und Instanzen, die diese für die Benutzer ausstellen.

2.2.2 PKI

Die Authentizität eines öffentlichen Schlüssels und dessen Zuordnung zu einer bestimmten Person bestätigt ein Zertifikat. Dieses ist mit einem Personalausweis vergleichbar und wird von einer vertrauenswürdigen Instanz (Certification Authority *CA*) ausgestellt, die als unabhängige Dritte die Rolle eines überwachenden Notars übernimmt. Die Zertifizierung eines öffentlichen Schlüssels bestätigt die Identität der Person, auf die er ausgestellt ist.

Ein Zertifikat beinhaltet verschiedene Daten, darunter unter anderem den Namen der Person, ihren öffentlichen Schlüssel, den Typ der verwendeten Hashfunktion und die Gültigkeitsdauer der Signatur. Diese Daten werden von der CA mit ihrem privaten Schlüssel digital signiert:

$$Zertifikat = C_{CA}^{priv}[Name_x, C_x^{pub}] \tag{2.6}$$

Ob ein Schlüssel wirklich zu einer bestimmten Person gehört, wird dadurch überprüft, dass das Zertifikat der Person mit dem öffentlichen Schlüssel der CA entschlüsselt wird.

$$Name_x, C_x^{pub} \stackrel{?}{=} C_{CA}^{pub}[Zertifikat] \stackrel{2.6}{=} C_{CA}^{pub}[C_{CA}^{priv}[Name_x, C_x^{pub}]] \stackrel{2.1}{=} Name_x, C_x^{pub} \tag{2.7}$$

Die Zertifizierungsinstanz kann Zertifikate sperren, sollte der private Schlüssel eines Nutzer kompromittiert werden, das heißt verloren oder gestohlen werden. Solch ein Zertifikat wird in einer Sperrliste vermerkt und ähnlich der Sperrung einer verlorenen Kreditkarte ergibt eine Überprüfung des Schlüssels anhand des gesperrten Zertifikates, dass dieser nicht mehr gültig ist.

Doch eine Zertifizierungsstelle steht vor dem gleichen Problem wie ein Benutzer der Digitalen Signatur: Sie muss sicherstellen, daß ihr öffentlicher Schlüssel unter ihrem Namen im Internet bekannt ist und niemand sich für sie ausgeben kann. Um die Echtheit der CA-Schlüssel zu bestätigen, gibt es drei Modelle:

Zentralisierte CA In diesem Modell existiert nur eine Instanz, die alle Zertifikate für die Teilnehmer des Netzes ausstellt. Ein Beispiel dafür sind die früheren Versionen des Web-Browsers von Netscape, in denen die Firma VeriSign als alleinige Instanz vorgesehen war, um Zertifikate für SSL-Verbindungen zu verifizieren. Ein Benutzer musste somit nur das Zertifikat von VeriSign kennen, um alle anderen Benutzer sicher identifizieren zu können.

Web Of Trust Jeder kann in diesem Modell als Zertifizierungsinstanz auftreten und die Schlüssel anderer Teilnehmer in diesem Vertrauensnetz zertifizieren. Der Benutzer ist selbst für die Einschätzung von fremden Signaturen und Zertifikaten verantwortlich und kann bestimmen, wem er vertraut. Dieses Modell wird unter anderem von der Software „Pretty-GoodPrivacy“[1] verwendet.

1 http://www.pgpi.org/

Hierarchische CA Es existiert eine sogenannte Root-CA, die als höchste Zertifizierungsstelle weitere CAs zertifizieren kann. Diese können Benutzer oder wiederum andere CAs zertifizieren.

2.2.3 Rechtliche Grundlagen der Digitalen Signatur

Die mathematischen Grundlagen der Digitalen Signatur garantieren deren Fälschungssicherheit. Bis zum Jahre 2001 besaß diese jedoch vor Gericht keinerlei rechtlich garantierte Beweiskraft. Erst mit dem Erlass des Signaturgesetzes (SigG) [SigG2001] vom deutschen Gesetzgeber wurde der sogenannten elektronischen Signatur, die eine den Anforderungen des Gesetzes genügende Digitale Signatur ist, eine rechtliche Grundlage für ihre Verwendung in elektronischen Datennetzen wie zum Beispiel dem Internet geschaffen.

Das Signaturgesetz

Das Signaturgesetz definiert die Rahmenbedingungen der elektronischen Signatur und definiert die Umstände, unter denen eine elektronische Signatur der handschriftlichen juristisch gleichgestellt ist. Die konkreten technischen Anforderungen und Spezifikationen werden in der Signaturverordnung (SigV) beschrieben, da diese bei Bedarf schneller als das Gesetz verändert werden kann.

Neben den Begriffsdefinitionen von elektronischer Signatur und Zertifikaten legen die gesetzlichen Regelungen die Anforderungen an die Public-Key-Infrastruktur (PKI) fest, die die Gesamtheit von Zertifizierungsstelle, Anwendungen und Schlüsselspeicherung umfasst. Die Kriterien für die Lizenzvergabe an einen Zertifizierungsanbieter werden ebenfalls genau aufgelistet. Als Zertifizierungsmodell ist im Gesetz das der hierarchisch aufgebaute CAs bestimmt, in dem die Regulierungsbehörde für Telekommunikation und Post (RegTP) die Rolle der Root-CA einnimmt und auch die Einhaltung der in der Signaturverordnung definierten Sicherheitsvorgaben durch die CAs überwacht.

Begriffsdefinitionen

Das Signaturgesetz definiert die elektronische Signatur als „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“. Diese Formulierung beschreibt nur die Funktionalität der Digitalen Signatur ohne auf ihre Zertifizierung zu bestehen.

Die „fortgeschrittene elektronische Signatur“ verknüpft die Signatur mit einem Schlüsselinhaber und erfordert sowohl dessen Identifizierbarkeit als auch die Unveränderbarkeit der Signatur.

Erst die rechtliche anerkannte „qualifizierte elektronische Signatur“ erweitert die fortgeschrittene um die Anforderung nach einer „sicheren Signaturerstellungseinheit“ und vor allem nach

einem „qualifizierten Zertifikat“ zur Zuordnung von Person und Dokument.

„Qualifizierte Zertifikate“ dürfen nur von CAs ausgestellt werden, wenn diese die Mindestanforderungen in Bezug auf die Sicherheitsmaßnahmen erfüllen, die in der Signaturverordnung näher ausgeführt werden.

Praktische Umsetzung

Es existieren momentan mehrere Zertifizierungsinstanzen auf dem Markt. Zu den größten kommerziellen zählt die Firma „TC TrustCenter“[2]. Daneben haben sich einige nicht-kommerzielle Zertifizierungsstellen etabliert, darunter die Computer-Fachzeitschrift c’t[3], die ihre Dienste seit der CeBIT 1997 anbietet. Der Fokus ihrer Krypto-Kampagne liegt auf der Sensibilisierung der Allgemeinheit gegenüber Digitalen Signaturen und der Stärkung der Infrastruktur. Dies zeigt sich auch daran, dass keine qualifizierten Zertifikate ausgestellt werden, die dem Signaturgesetz genügen.

Die Abstufung der Zertifikatsklassen wird auch von den Zertifizierungsanbietern vorgenommen. TrustCenter bietet zum Beispiel 4 Klassen von Zertifikaten an. Die erste Klasse erfordert nur eine gültige E-Mailadresse, wohingegen für ein Zertifikat der Stufe 4 eine Überprüfung des Antragstellers anhand der Daten in der Meldebehörde stattfindet.

Durch das Signaturgesetz, die Signaturverordnung und eine Änderung verwaltungsverfahrensrechtlicher Vorschriften sind die handschriftliche und die elektronische Signatur gleichgestellt und Rechtsgültigkeit für letztere gewährleistet. Eine mit einer elektronischen Signatur vereinbarte Leistung kann somit vor Gericht eingeklagt werden, da die Authentizität der Signatur sehr einfach aufgrund der oben aufgeführten mathematischen Grundlagen bewiesen werden kann. Zweifelt eine Partei die Authentizität einer elektronischen Signatur an, die von einer dem Signaturgesetz genügende CA ausgestellt wurde, so hat sie die Beweise für diese Behauptung vorzulegen.

2.3 Eigenschaften der Digitalen Signatur

Das Unterschreiben eines elektronischen Dokumentes mit der Digitalen Signatur hat aufgrund der ihr innewohnenden Funktionen einige Vorteile, die die handschriftliche Unterschrift im normalen Geschäftsverkehr nicht besitzt.

Integrität des Dokumentes Eine nachträgliche Änderung des unterschriebenen Dokumentes ist nicht mehr möglich. Dies wird dadurch unterbunden, dass jede Änderung an dem Dokument zu einem anderen Hashwert und einer damit ungültigen Signatur führt. Solange

2 http://www.trustcenter.de/
3 http://www.heise.de/ct/pgpCA/

der private Schlüssel des Benutzers auch wirklich privat bleibt und nicht in die Hände unbefugter Dritter gelangt, kann sonst niemand eine neue Signatur im Namen des Benutzers erstellen.

Integrität der Signatur Das Fälschen der digitalen Unterschrift wird dadurch erschwert, dass in der digitalen Signatur keine Muster auftreten. Die handschriftliche Unterschrift sieht immer gleich aus und kann durch einen Fälscher einstudiert werden. Eine digitale Signatur wird immer neu aus dem unterzeichneten Dokument berechnet und weist deshalb jedes Mal einen anderen Wert auf.

Zeitstempel Im Gegensatz zur handschriftlichen Unterschrift können elektronische Signaturen Zeitinformationen enthalten. Diese verhindern zum einen die spätere Wiederverwendung einer Signatur, ermöglichen aber auch die Bereitstellung von Zeitstempeldiensten durch die Zertifizierungsinstanzen zur genauen Datierung von Digitalen Signaturen.

2.3.1 Anwendungsszenarien

Ihre spezielle Eignung für elektronische Medien eröffnet der digitalen Signatur eine Fülle von Anwendungsmöglichkeiten. Sie wird deshalb in einigen Projekten bereits eingesetzt:

Virtuelle Behördengänge Die Abwicklung von Behördengängen und das Abrufen von Informationen über das Internet bietet dem Bürger nicht nur einen erhöhten Komfort, sondern hilft auch dem Staat, seine Ausgaben zu senken.

Ziel der im Rahmen des „Bündnis für elektronische Signaturen“ gegründeten Bundesinitiative „BundOnline 2005“[4] ist es, die rund 400 onlinefähigen Dienstleistungen des Bundes bis zum Jahre 2005 im Internet zur Verfügung zu stellen. Dem Investitionsvolumen von rund 1,6 Milliarden Euro steht dabei laut der Bundesregierung nach der Umsetzung ein Einsparpotenzial von rund 400 Millionen Euro pro Jahr gegenüber.

Ende des Jahres 2002 waren 160 Dienstleistungen im Internet verfügbar, unter anderem das „DIGANT“-System der Bundesdruckerei[5], welches mit Hilfe der Digitalen Signatur die elektronische Abwicklung des Antragsverfahrens für Pässe und Ausweise ermöglicht.

Bankgeschäfte Beim Online-Banking kommen heutzutage zumeist Verfahren zum Einsatz, die zur Authentifizierung das PIN/TAN Verfahren über eine per SSL-gesicherte Verbindung einsetzen. Den meisten Benutzern sind diese Sicherheitsmaßnahmen aber unzureichend, da eine PIN geklaut oder vergessen werden kann. In einer Studie von Fittkau und Maas[6] gaben 69,8 Prozent derjenigen Befragten an, die bereits privates Online-Banking

4 http://www.bund.de/BundOnline-2005-.6164.htm
5 http://www.bundesdruckerei.de/de/behoerdenservice/index.html
6 http://www.heise.de/newsticker/data/jk-04.09.02-001/default.shtml

nutzen, dass durch weitere Sicherheitsmaßnahmen sich mehr Kunden für das Online-Banking gewinnen ließen. Erst an zweiter Stelle wurden günstigere Gebühren als bestes Mittel zur Kundenaquisition genannt.

Durch die Einbindung der Digitalen Signatur in diesen Prozess kann dieser sicherer und einfacher gestaltet werden und somit an Attraktivität für bisher unentschlossene Benutzer gewinnen.

Sicherer E-Commerce Wie schon in der Einleitung erwähnt wurde, ist die Kriminalitätsrate im Internet in den letzten Jahren stark angestiegen [IFCC2003]. Die Palette der Delikte reicht dabei von nicht gelieferten oder nicht bezahlten Waren bis hin zu sogenanntem Identitätsdiebstahl, bei dem die Betrüger unter falschem Namen Waren im Internet zu Lasten des Bestohlenen bestellen. Aufgrund dieser einfachen Betrugsmöglichkeiten und der bisherigen Unsicherheit bezüglich der Rechtsgültigkeit von im Internet geschlossenen Verträgen zögern viele Verbraucher noch, Geschäfte in diesem Medium zu tätigen.

Der Einsatz der Digitalen Signatur und von Zertifikaten erlaubt in diesem Bereich nicht nur die Identifikation des Vertragspartners, sondern auch die rechtliche Einforderung der Vertragssache. Im Internet geschlossene Verträge werden durch die elektronischen Signatur rechtskräftig und vor Gericht einklagbar.

2.4 Grenzen und Probleme der Digitalen Signatur

Die Probleme der Digitalen Signatur sind nicht nur technischer, sondern auch gesellschaftlicher Natur, was zum Beispiel die Akzeptanz innerhalb der Bevölkerung angeht. Im einzelnen tauchen folgende Probleme im Umgang mit der Digitalen Signatur auf:

2.4.1 Algorithmen

Die Sicherheit der Digitalen Signatur beruht auf den dabei verwendeten kryptographischen Signieralgorithmen. Diese verhindern durch ihre mathematische Komplexität, dass der private Schlüssel in einem zeitlich überschaubaren Rahmen aus den öffentlich verfügbaren Informationen berechnet werden kann. Zukünftige Forschungsergebnisse ermöglichen eventuell einen kryptoanalytischen Angriff auf den Algorithmus, der in vertretbarer Zeit den privaten Schlüssel einer Person errechnet oder das Erstellen von Signaturen ohne den dazugehörigen Schlüssel ermöglicht. Die Fälschungssicherheit einer Signatur wäre dann nicht mehr gegeben und alle auf diesem Verfahren basierenden Schlüssel müssten zeit- und kostenintensiv ausgetauscht werden.

Das Signaturgesetz schreibt keine speziellen Algorithmen zur Verwendung vor. Um jedoch das Risiko durch zu schwache Kryptographiealgorithmen zu vermindern, wird in der Signaturverordnung festgelegt, dass ein verwendeter Algorithmus ab seiner Bewertung durch das Bundes-

amt für Sicherheit und Veröffentlichung im Bundesanzeiger für mindestens sechs Jahre als fälschungssicher zu gelten hat.

2.4.2 Mobilität

Die Digitale Signatur bietet nicht die gleiche Mobilität wie die handschriftliche Unterschrift, mit der man jederzeit und überall einen Geschäftsabschluss tätigen kann. Sie ist immer auf ein elektronisches Medium zum Transport der Schlüssel und einen Computer oder ein ähnliches Gerät zum Erzeugen der Signatur angewiesen.

Der Verlust dieses Mediums und der darauf gespeicherten Schlüssel zwingt den Benutzer, seine alten Schlüssel und Zertifikate für ungültig erklären zu lassen und sich neue erstellen zu lassen. Außerdem sollte der private Schlüssel des Benutzers bei einem Signiervorgang das Transportmedium nicht verlassen müssen, damit dieser bei der Übertragung in ein Signiergerät nicht abgehört werden kann.

Ein mobiles Endgerät, wie zum Beispiel ein PDA, vereint in sich Transportmedium und Signiergerät. Somit müssen die privaten Schlüssel des Benutzers das Gerät nicht verlassen und die Digitale Signatur kann an jedem gewünschten Ort erbracht werden.

2.4.3 Warnfunktion

Zur Erfüllung der Warnfunktion darf die Signierung eines Dokumentes nur von dem berechtigten Benutzer freigeschaltet werden. Diese Funktion stellt ebenso wie die Mobilität eine Herausforderung an die praktische Umsetzung eines Signierwerkzeuges dar und muss von der verwendeten Hard- und Software zur Verfügung gestellt werden. Eine Möglichkeit ist die Verwendung eines biometrischen Merkmals zur Authentifizierung des Benutzers (siehe Kapitel 3).

2.4.4 Akzeptanz

Obwohl das Internet seinen Platz im alltäglichen Leben eingenommen hat, belegt eine Studie des britischen National Consumer Councils aus dem Jahre 2000 [NCC2000], dass es Vorbehalte gegenüber dem Einkaufen über das Internet gibt. Von den in der Studie befragten Internetnutzern sehen 55 Prozent diese Methode als die unsicherste Einkaufsart an und 45 Prozent geben an, daß sie mehr über das Internet einkaufen würden, wenn der Vorgang sicherer für sie wäre.

Die Digitale Signatur bietet dem Verbraucher diese erhöhte Sicherheit bei Geschäften aller Art über das Internet. Dennoch wurden bisher nur wenige Zertifikate von den offiziellen CAs ausgestellt, und dies trotz Investitionen von über 50 Millionen Euro seitens der Bundesregierung in den Aufbau einer PK-Infrastruktur.

2.4.5 Benutzbarkeit

Als der Hauptgrund für die mangelnde Akzeptanz von E-Commerce-Angeboten und somit auch der Digitalen Signatur durch den Anwender wird von Gerd tom Markotten und Jendricke die unzureichende Benutzbarkeit von bisherigen sicheren Anwendungen in diesem Sektor identifiziert [GeJe2003].

Die Forderung des Benutzers nach sicheren Anwendungen und informationeller Selbstbestimmung wird erfüllt, durch eine umständliche und unverständliche Benutzeroberfläche wird der Benutzer jedoch selbst zum Sicherheitsrisiko[Ge2003]. So ist das der Digitalen Signatur zugrunde liegende Konzept der asymmetrischen Kryptographie für viele der in Sicherheitsfragen unerfahrenen Benutzer nicht verständlich. Sicherheitslücken entstehen zum Beispiel, wenn sich der Benutzer nicht der Geheimhaltungspflicht seines privaten Schlüssels bewusst ist und diesen anstatt seines öffentlichen Schlüssels an Dritte weitergibt.

2.5 Zusammenfassung

Die Digitale Signatur ist der handschriftlichen Unterschrift ebenbürtig, was ihre Möglichkeiten bei der Signierung von Dokumenten angeht. Darüber hinaus besitzt sie weitere Vorteile, die über die Eigenschaften der handschriftlichen Unterschrift hinausgehen.

Dennoch hat die Digitale Signatur den von der Wirtschaft erhofften Durchbruch bisher nicht geschafft, wie er noch bei der Verabschiedung des Signaturgesetzes vorhergesagt wurde. Die Verbreitung in der Bevölkerung ist aufgrund der in Abschnitt 2.4 erläuterten Probleme hinter den Erwartungen der Industrie und des Staates zurückgeblieben.

Um die in Abschnitt 2.1.1 erläuterte Warnfunktion zu implementieren, muss der Benutzer eines mobilen Endgerätes den Signiervorgang explizit autorisieren, indem er sich diesem gegenüber authentifiziert. Dies schreibt auch die Signaturverordnung in Paragraph 15, Absatz 1 vor, so dass erst nach der Identifikation des Benutzers dessen private Schlüssel angewandt werden dürfen. Mehrere Verfahren zur Authentifizierung des Benutzers werden deshalb im nächsten Kapitel diskutiert.

3 Authentifikation

Diese Kapitel behandelt die verschiedenen Möglichkeiten, den Benutzer eines Computersystems zu authentifizieren, und basierend auf seiner Identität verschiedene Funktionen des Systems für ihn freizuschalten. Es werden verschiedene Authentifizierungsmethoden auf Sicherheit und Benutzbarkeit hin überprüft. Als Fazit wird eine biometrische Zugangskontrolle zur Freischaltung der Digitalen Signatur vorgeschlagen, wie sie auch in eSign verwendet wird.

3.1 Allgemeines zur Authentifizierung

Wann immer ein Rechnersystem sowie die darauf vorhandenen Daten und Funktionen geschützt werden müssen, lässt sich der Ablauf vor einem berechtigten Zugriff auf das System in zwei Teile gliedern:

Zuerst *identifiziert* sich der berechtigte Benutzer mit seinem Namen, einem eindeutigen Kennwort oder einer Chip-Karte und anschließend *authentifiziert* er sich mit einem Passwort, einer PIN-Nummer oder einer anderen geheimen Passphrase, die nur dem System und dem Benutzer bekannt ist.

Der erste Schritt kann unter Umständen entfallen, wenn die Identität des Benutzers allein anhand seines Authentifizierungsmerkmals durch einen Vergleich mit allen in einer Datenbank gespeicherten Identitäten festgestellt wird. Ebenso kann die Identifizierungsphase übergangen werden, wenn das System nur für einen Benutzer konzipiert ist, so wie es bei dem in der Einleitung beschriebenen PDA-Prototypen des SPPS-Projektes der Fall ist.

Es muss bei dem Zugriff auf den PDA und die eSign-Anwendung also nur die Authentifizierung des einzigen Benutzers vorgenommen werden. Dies dient der Autorisierung einer Digitalen Signatur durch den Benutzer, damit die in Abschnitt 2.1.1 beschriebene Warnfunktion der handschriftlichen Unterschrift auch bei der Digitalen Signatur gegeben ist. Eine automatische Signierung von Dokumenten durch die Software ohne Wissen des Benutzers ist somit ausgeschlossen.

3.2 Gängige Verfahren zur Authentifizierung

3.2.1 PINs und Chip-Karten

Die am gebräuchlichste Methode zur Authentifizierung des Benutzers ist die Personal-Identity-Number (PIN). Bankautomaten, Handys und Computer gestatten den Zugriff erst nach Eingabe der meist vierstelligen Geheimzahl, wobei sich der Benutzer zuvor dem System gegenüber meist mit einer Chip-Karte identifiziert.

3.2.2 Passwörter

Ebenso verbreitet wie die PIN sind Passwörter als Zugangsberechtigung zu einem System. Um sogenannte Wörterbuchangriffe, die alle Wörter aus einem Lexikon ausprobieren, auf einen durch ein Passwort geschützten Zugang zu vermeiden, sollten diese keinen Klartext oder erratbare Muster wie zum Beispiel Geburtsdaten enthalten.

3.2.3 Schwächen üblicher Authentifizierungsverfahren

Banken haben als Authentifizierungsmerkmal die PIN an ihren Geldautomaten eingeführt und somit den Gang zum Schalter durch einen Service rund um die Uhr ersetzen können. Die PIN hat sich in unserem Alltag so weit etabliert, dass die Bedienung solcher System allgemein bekannt und von jedem durchführbar ist. Sie ist aber mit generellen Schwächen behaftet, die die Benutzung erheblich erschweren. Diese Probleme lassen sich mit 3 Schlagwörtern zusammenfassen: Verlust, Vergessen und Diebstahl:

Verlust Eine Chipkarte kann verloren werden und eine Ersatzkarte muss dann zeitaufwendig nachgeliefert werden.

Vergessen PINs sind meistens nicht frei wählbar und somit sammeln sich für den Benutzer schnell mehrere verschiedene Nummern an. Mehr als ein Drittel der in einer Umfrage des BioTrust-Projektes[1] befragten Personen gaben an, sich nur bis zu 3 PIN-Nummern merken zu können. Mehr als fünf verschiedene Nummern können sich laut eigener Aussage nur 18 Prozent der Befragten einprägen [BeRo2000].

Durch diese PIN-Inflation wird die korrekte Zuordnung von Nummer und Verwendungszweck zu einem Problem, da zum Beispiel bei einem Geldautomaten maximal zwei falsche Eingaben erlaubt sind, bevor die Karte des Benutzers einbehalten wird.

Passwörter können zwar meist vom Benutzer frei gewählt werden. Wenn dieser statt erratbaren Klartextwörtern jedoch komplizierte Buchstabenfolgen benutzt, steht er damit wieder vor dem Problem, sich seine vielen Passwörter merken zu müssen.

1 http://www.biotrust.de

Diebstahl Es ist für einen Dieb möglich, die PIN-Eingabe an einem Terminal auszuspähen und somit in den Besitz der eigentlich geheimen Nummer zu gelangen. Unvorsichtige Benutzer schreiben ihre PIN auf oder benutzen leicht zu erratene Passwörter und gehen damit ein Risiko ein.

Der letztgenannte Fall ist der folgenschwerste: Wer in den Besitz einer fremden PIN und Chipkarte gelangt, kann im Namen deren rechtmäßigen Besitzers handeln. Vor Gericht zählt dann die Kenntnis der PIN als Authentifizierungsmerkmal, obwohl ein unberechtigter Dritter die Handlung durchführte.

3.2.4 Probleme durch Personengebundenheit und -bezogenheit

Die im vorherigen Abschnitt erläuterten Probleme entstehen dadurch, dass die dort vorgestellten gängigen Verfahren zur Authentifizierung, die auf Wissen und Besitz von geheimen Daten basieren, nicht *personengebunden*, sondern nur *personenbezogen* sind.

Der Unterschied zwischen diesen beiden Begriffen besteht darin, dass ein personenbezogenes Identifizierungsmerkmal wie zum Beispiel eine PIN gewollt oder ungewollt an eine andere Person weitergegeben werden kann, die damit im Namen der weitergebenden Person handelt.

Ein personengebundenes Merkmal kann nur von der Person benutzt werden, an die das Merkmal gebunden ist, wie zum Beispiel das Passbild im Führerschein nur den darauf Abgebildeten zum Fahren eines Autos berechtigt.

3.3 Biometrie zur Authentifizierung

Die genannten Schwächen der herkömmlichen Authentifizierungsverfahren in Bezug auf ihre Sicherheit und Benutzbarkeit lassen sie ungeeignet erscheinen, um sie in einem sicherheitskritischen Umfeld wie der Digitalen Signatur einzusetzen.

Als Alternative zu den diesen Authentifizierungsverfahren mittels PIN und Chipkarte bieten sich biometrische Erkennungssysteme an. Diese sollen eine höhere Sicherheit bei der Benutzerauthentifizierung aufweisen und werden im nächsten Abschnitt genauer vorgestellt. Im Anschluss daran wird die Frage diskutiert, welches biometrische Verfahren für die Autorisierung der Digitalen Signatur in eSign am besten geeignet ist.

3.3.1 Allgemeines zur Biometrie

Als biometrisches Merkmal wird eine messbare Eigenschaft oder eine Fähigkeit einer Person angesehen, die es erlaubt, diese von anderen Personen eindeutig zu unterscheiden. Im Gegensatz zu einer PIN ist das Merkmal *personengebunden*, also nicht übertragbar, da es dem Körper der

Person innewohnt. Es kann darüber hinaus auch nicht vergessen oder verloren werden. Beispiel dafür sind die Fingerabdrücke, die Gesichtsform, der Gang oder die Unterschrift einer Person.

Im Idealfall weist ein biometrisches Merkmal einer Person folgende Eigenschaften auf [BeRo2000]:

- *universell*, d.h es muss bei jeder Person vorhanden sein.
- *einzigartig*, d.h. es muss immer verschieden sein wie beispielsweise ein Fingerabdruck.
- *permanent*, d.h. es muss unabhängig von Zeit und Ort der Identifikation sein.
- *erfassbar*, d.h. Sensoren müssen es erfassen können.

Bewertungskriterien

Die Daten, die aus biometrischen Merkmalen gewonnen werden, unterscheiden sich nicht nur zwischen zwei Menschen, sondern sie weisen auch dann Variationen auf, wenn sie von derselben Person stammen, aber zu verschiedenen Zeitpunkten erfasst wurden. Im Falle der handschriftlichen Unterschrift kann jedermann bei der eigenen Signatur erkennen, wie sie sich in vielen kleinen Details immer wieder von der vorherigen unterscheidet und auch im Laufe der Zeit verändert. Schon eine veränderte Körperhaltung, Gesundheit oder auch die emotionale Verfassung lässt die eingeübte Unterschrift anders aussehen und wird deshalb eventuell von dem biometrischen Erkennungsalgorithmus als Fälschung zurückgewiesen.

Aufgrund dieser Variationen muss der einer biometrischen Authentifizierung zugrundeliegende Erkennungsalgorithmus eine gewisse Fehlertoleranz gegenüber den Daten aufweisen, die ihm zum Vergleich gegeben werden. Diese Toleranz schlägt sich in den zwei Werten False-Rejection-Rate (FRR) und False-Acceptance-Rate (FAR) nieder, anhand derer sich eine Bewertung von biometrischen Verfahren erstellen lässt.

Die FRR drückt den Anteil der Authentifizierungsversuche eines berechtigten Benutzers aus, die vom System respektive von dem zugrunde liegenden Algorithmus als gefälscht zurückgewiesen werden. Die FAR ist das Gegenstück zur FRR und verläuft entgegengesetzt zu dieser. Sie stellt den Fall der Akzeptanz eines unberechtigten Benutzers dar. Mit einer besseren Erkennung von berechtigten Zugriffen durch eine größere Fehlertoleranz handelt man sich also auch eine erhöhte Akzeptanz von gefälschter Unterschriften ein (siehe Abbildung 3.1).

Wenn man im Gegenzug die FAR jedoch so niedrig wie möglich halten will, indem die Toleranz gegenüber Variationen im biometrischen Merkmal sehr gering ansetzt, steigt im selben Moment die FRR an. Es muss bei der Entwicklung der Hard- und Software bei biometrischen Erkennungsverfahren ein Kompromiss gefunden werden, der sowohl den Benutzer nicht zu häufig abweist, als auch einem Fälscher den Zugang so selten wie möglich erlaubt. Dieser Wert liegt im Schnittpunkt der beiden in Abbildung 3.1 gezeigten Kurven und sollte möglichst niedrig liegen.

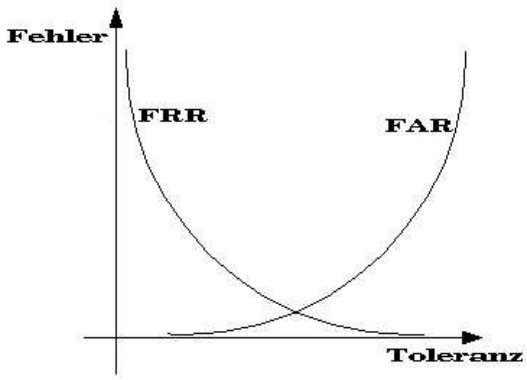

Abbildung 3.1: FAR und FRR Kurven

3.3.2 Biometrieverfahren

Die Forschung im Bereich der biometrischen Authentifikation (siehe dazu auch [AVBPA2001]) konzentriert sich auf mehrere Schwerpunkte. Eine ausführlichere Beschreibung geben Busch und Daum [BuDa2002], in dieser Arbeit werden nur die am häufigsten eingesetzten Merkmale vorgestellt.

Der Ablauf einer biometrischen Erkennung ist bei allen Verfahren ähnlich. Zuerst wird dem System in einer Enrollment-Phase das biometrische Merkmal des Benutzers antrainiert. Dabei wird das Merkmal durch Sensoren erfasst und das benutzte Muster extrahiert und gespeichert. Bei einer späteren Authentifizierung wird dann das Merkmal mit dem gespeicherten Muster verglichen.

In der Biometrie wird generell zwischen aktiven und passiven Erkennungsverfahren unterschieden [ScSt2000]. Eine passive biometrische Merkmalsextraktion wie zum Beispiel die Gesichtserkennung kann ohne Einwilligung der betreffenden Person stattfinden, während eine aktive Erkennung eine explizite Aktion des Benutzers erfordert und nicht unwissentlich erfolgen kann.

Iris

Durch die Wachstumsprozesse des menschlichen Körpers im Mutterleib bekommt die Iris ihre Charakteristika. Der auch Regenbogenhaut genannte Teil des Auges reißt durch das Wachstum auf und erhält so ein zufällig entstehendes Muster aus Furchen und Narben auf seiner Oberfläche (siehe Abbildung 3.2). Über 200 dieser Merkmale lassen sich in einem Bild der Iris ausmachen und mit einer Kamera aufnehmen. Diese hohe Anzahl und die sehr gute Unterscheidbarkeit, so-

gar von eineiigen Zwillingen, erlauben theoretisch den Einsatz dieses biometrischen Merkmals in sicherheitskritischen Gebieten.

Abbildung 3.2: Aufnahme einer Iris [Er2002]

Fingerabdruck

Authentifizierungssysteme, die sich am Fingerabdruck des Menschen orientieren, stellen den größten Teil der heutzutage erhältlichen Systeme dar. Dabei werden über Sensoren die sogenannten Minutien erfasst. Diese Punkte auf der Hautoberfläche sind die Stellen, an denen die Fingerlinien enden oder sich verzweigen (siehe Abbildung 3.3). Über optische oder elektrische Sensoren wird deren relative Lage zueinander gemessen und mit dem Referenzmuster verglichen [Kü2002].

Abbildung 3.3: Fingerabdruck mit Minutien [Er2002]

Gesicht

Im Gegensatz zum Fingerabdruck kommt die biometrische Gesichtserkennung ohne direkten Körperkontakt aus und kann somit unauffälliger als ein Fingerabdruckscanner in das Umfeld

der Anwender integriert werden. Die Erkennung einzelner Personen innerhalb von größeren Menschenmengen, wie sie zum Beispiel in Flughäfen vorzufinden sind, kann effektiver und schneller vorgenommen werden als bei Verfahren, die den Kontakt mit einem Sensor benötigen.

Eine Verarbeitungsmöglichkeit der erfassten Daten basiert dabei zum Beispiel auf den relativen Positionen charakteristischer Punkte des Gesichtes, wie zum Beispiel Nase, Stirn, Augen und Mundpartie. Diese bilden wie die Minutien des Fingerabdrucks ein Muster, welches nach der Messung durch Normalisierung von Einflüssen wie der Drehung des Kopfes befreit und anschliessend gespeichert wird.

Ein anderes Verfahren nähert das erfasste Gesicht durch Kombination aus mehreren vorher festgelegten Grundgesichtern an. Ähnlich einer Linearkombination von Vektoren bilden dann die Koeffizienten der Grundgesichter das Merkmal des erfassten Gesichtes [BuDa2002].

Stimme

Die von der Stimme erzeugten Frequenzen sind durch die körperlichen Variationen der Menschen unterschiedlich. Die Größe des Kehlkopfes, der ebenso wie der gesamte Rachenraum wie ein Resonanzkasten wirkt, verändert diese ebenso wie die Artikulation der Worte durch den Sprecher und dessen Dialekt und Akzent.

Unterschrift

Die handschriftliche Unterschrift ist durch ihre Einzigartigkeit und ihre rechtliche und gesellschaftliche Akzeptanz *das* Merkmal zur Identifizierung des Geschäftspartners bei Vertragsabschlüssen. Sie kann nicht zufällig und ohne Wissen des Unterzeichners abgegeben werden.

Bei der elektronischen Erfassung der Unterschrift wird nicht nur das von außen ersichtliche statische Schriftbild erfasst und analysiert, sondern auch die dynamischen Aspekte der Unterschrift berücksichtigt, die nicht so einfach ausgespäht werden können wie zum Beispiel die Zahlen bei einer PIN-Eingabe.

Zu diesen dynamischen Charakteristika, die mitunter unbewusst durch den Unterzeichner beeinflusst werden, zählen die Schreibgeschwindigkeit und -beschleunigung sowie der Anpressdruck des Stiftes. In Abbildung 3.4 ist eine Unterschrift und ihre vertikale Dichte dargestellt. Diese Dichte ist eins von über 50 statischen Merkmalen einer Unterschrift und drückt die Verweildauer des Stiftes bei der Abgabe der Unterschrift auf der x-Achse aus.

3.3.3 Anwendungsgebiete für Biometrie

Die speziellen Vorteile der Biometrie gegenüber anderen Identifizierungs- und Authentifizierungsverfahren prädestinieren sie für den Einsatz in vielen verschiedenen Anwendungsbereichen:

Abbildung 3.4: Unterschrift und Merkmal vertikale Dichte [SP2003]

- Wie in Abschnitt 3.2.3 gezeigt wurde, weisen die bisher zum Beispiel am Geldautomaten verwendeten Identifikations- und Authentifikations-Mechanismen mittels PIN und Chipkarte gravierende Mängel in Bezug auf Sicherheit und Benutzbarkeit auf. Eine Authentifizierung durch ein biometrisches Merkmal ist dazu eine Alternative, die auch von den Benutzern angenommen wird. In der schon erwähnten Umfrage des BioTrust-Projektes sagten zwei Drittel der befragten Personen, dass sie ein biometrisches Verfahren einer PIN vorziehen würden [BeRo2002].

- Aufgrund der Einzigartigkeit biometrischer Merkmale eignen sie sich, um Personalausweise fälschungssicherer zu machen. In einigen Ländern wie Brunei und Macau werden die Fingerabdrücke der Bürger mit in die Ausweise aufgenommen, um deren Echtheit zu verifizieren.[2]

- Pilotprojekte unter anderem auf den Flughäfen in Nürnberg, Sidney und Zürich, sowie an der deutsch-tschechischen Grenze sind im Jahre 2002 gestartet worden, um bei der Einreise mittels biometrischer Gesichtserkennung die Ausweise der Einreisenden zu überprüfen und gesuchte Personen in der Menge zu entdecken. Von Vorteil für die Gesichtserkennung ist dabei die Möglichkeit, größere Menschenmassen effizient und schnell mit Kameras zu durchsuchen.

- Die Freischaltung einer Digitalen Signatur durch ein biometrisches Merkmal ist laut der Signaturverordnung ausdrücklich erlaubt. Die Nutzung biometrischer Merkmale ist dabei nicht nur als Ergänzung, sondern als vollwertige Alternative zu den herkömmlichen Verfahren angesehen, die nur auf Wissen und Besitz von einer PIN oder Chipkarte basieren. Für qualifizierte elektronische Signaturen werden dabei Bedingungen an das biometrische System gestellt, welches eine unbefugte Benutzung der Signatur hinreichend auszuschließen hat [Al2002].

2 http://www.heise.de/newsticker/data/pmz-13.02.03-000/default.shtml

3.3.4 Grenzen der Biometrischen Authentifizierung

Trotz früherer positiver Prognosen werden biometrische Merkmalserkennungen bisher in der Praxis selten eingesetzt, da die Biometrie in der Praxis noch teilweise an ihre Grenzen stößt. Diese betreffen nicht nur die Ablehnung seitens des Benutzers, sondern sind auch technischer Natur, und werden in den folgenden Abschnitten genauer erläutert.

Aufgrund dieser Schwächen müssen Kompromisse gegenüber den in Abschnitt 3.3.1 postulierten Eigenschaften eines idealen biometrischen Merkmals eingegangen werden. Bei dem Design eines Systems zur biometrischen Erkennung müssen diese Einschränkungen bei der Auswahl des verwendeten biometrischen Merkmals berücksichtigt werden, um den Sicherheitslevel des Systems auf einem möglichst hohen Niveau zu halten.

Erkennungsrate

In der Theorie sind die biometrischen Merkmale wie zum Beispiel der Fingerabdruck bei jedem Individuum verschieden. In der Praxis ergeben sich jedoch Einschränkungen, die eine 100-prozentige Genauigkeit bei der Erkennung des Benutzers verhindern. Durch die analogen Sensoren wie zum Beispiel Kameras, die das Merkmal aufnehmen und verarbeiten, schleichen sich über die verwendeten Algorithmen Fehler in die Daten des Merkmals ein.

So werden bei der Gesichtserkennung die Videoaufnahmen und somit die Ergebnisse durch einige unwägbare Faktoren wie die Lichtverhältnisse oder die Kopfhaltung der Person beeinträchtigt. Laut einer Studie des US-amerikanischen Handelsministeriums ist trotz großen Verbesserungen des Verfahrens in den letzten zwei Jahren die Erkennungsrate immer noch nicht hoch genug, um die Gesichtsmerkmale als einziges Kriterium bei einer Entscheidung zu betrachten [FRVT2002].

Die besten der in der Studie getesteten Erkennungssysteme erkannten bei Aufnahmen in geschlossenen Räumen bei unterschiedlicher Beleuchtung 90 Prozent der vorgelegten Bilder korrekt, bei Außenaufnahmen jedoch nur 50 Prozent. Die FAR lag dabei bei einem Prozent, was für einen Einsatz in der Praxis noch als zu hoch angesehen wird.

Aufgrund dieser hohen Fehlerquote wurde auch das im Juli 2002 gestartete Pilotprojekt zur elektronischen Passbild-Überprüfung von Flugreisenden am Nürnberger Flughafen wieder eingestellt. Das System war weniger leistungsfähig als das geschulte Auge eines Polizeibeamten und konnte somit die in es gesteckten Erwartungen nicht erfüllen[3].

Temporäre Behinderung des Benutzers

Die Erkennungsrate hängt nicht nur maßgeblich von den Umwelteinflüssen, sondern auch von dem einzelnen Benutzer ab. Die Universalität und Permanenz des Biometriemerkmals ist nicht

3 http://www.heise.de/newsticker/data/jk-18.03.03-006/default.shtml

mehr gewährleistet, wenn der Benutzer durch körperliche Behinderungen, die zeitlich und örtlich begrenzt sein können, eingeschränkt ist.

So wird zum Beispiel die Identifikation des Benutzers durch dessen Stimme durch eine Erkältung erschwert, die die Tonlage verändert. Wenn eine Unterschrift in einem fahrenden Zug geleistet werden muss, verändert dies die Form signifikant.

Keine Fälschungssicherheit

In einem Test der Zeitschrift c't konnte jedes der getesteten biometrischen Erkennungssysteme mit einfachen Mitteln getäuscht werden [ThKrZi2002].

Die den Großteil der heute erhältlichen System ausmachenden Fingerabdrucksensoren wurden mit Latenzbildern überlistet. Diese sind Ablagerungen von früheren Fingerabdrücken, die sich noch auf der Oberfläche des Sensors befinden, und im Test teilweise schon durch einfaches Anhauchen des Sensors reaktiviert werden konnten. Die Gesichtserkennung konnte durch Abspielen eines Videos mit dem Gesicht eines berechtigten Benutzers über ein Notebook-Display getäuscht werden, teilweise sogar schon durch ausgedruckte Bilder.

Fälscher brauchen also bei dem heutigen Stand der Technik nicht auf extreme oder ausgefeilte Mittel zurückzugreifen, um diese Systeme zu überlisten. Die Täuschung mittels heimlich aufgenommener Aufnahmen eines Benutzers, die stattfinden können ohne Verdacht zu erregen, ist einfacher [DiMaVi2002].

Akzeptanz des Benutzers

Biometrische Verfahren müssen auch vom Benutzer akzeptiert werden, wenn sie als Authentifizierungsverfahren eine weite Verbreitung erlangen sollen. So hängt der Abgabe von Fingerabdrücken noch ihr Ruf als erkennungsdienstliche Maßnahme in der Polizeiarbeit an und wird deshalb von Benutzern als wenig vertrauenserweckend eingestuft.

Gesichtserkennung durch Kameras erfordert keinerlei aktive Handlung des Benutzers und ist an jedem Ort möglich, der von einer Kamera überwacht wird. Dies wird von den meisten Benutzern als ein ungewollter Eingriff in die Privatsphäre angesehen und verstärkt das Misstrauen gegenüber solchen Verfahren. Diese Ängste vor einer ständiger Überwachung können dem Anwender durch einen konsequent betriebenen Datenschutz genommen werden. Dieser hat dafür zu sorgen, dass die Daten des Benutzers nicht zentral und außerhalb des Einflussbereiches des Benutzers gespeichert und nicht für andere Zwecke als die vom Benutzer erwünschte Authentifizierung missbraucht werden.

Ein weiteres Akzeptanzkriterium der Benutzer ist die Zeit, die zur Authentifizierung anhand eines biometrischen Merkmals einer Person gebraucht wird. Dies schließt sowohl die physische Messung mit Sensoren als auch die Verarbeitungsdauer und den Datenvergleich innerhalb des Systems mit ein. Neben Sicherheit, Einfachheit und Zuverlässigkeit ist in der Umfrage des

BioTrust-Projektes die Schnelligkeit des biometrischen Systems mit als eine der wichtigsten Eigenschaften von den befragten Personen genannt worden [BeRo2000].

Kosten

Eine Authentifizierung am Geldautomaten durch ein biometrisches Merkmal wird von den Banken hauptsächlich aus Kostengründen nicht in Erwägung gezogen [Si2002]. Neben der kostspieligen Umstellung der Geldautomaten muss die aufwändige Enrollment-Phase für alle Bankkunden durchgeführt werden. Da die FAR und FRR und damit die Zufriedenheit der Kunden maßgeblich von der Güte der in dieser Phase erstellten Referenzdatei abhängt, muss diese sehr sorgfältig und somit kosten- und zeitintensiv durchgeführt werden, was die Gesamtkosten in die Höhe treibt.

3.4 Anforderungen an ein geeignetes Biometriemerkmal

Wie im vorangegangenen Abschnitt aufgezeigt wurde, weist die Biometrie Schwachpunkte auf, so dass Kompromisse bei der Realisierung einer biometrischen Merkmalserkennung eingegangen werden müssen. Man stellt daher andere, realistischere Bedingungen und Bewertungskriterien an biometrische Merkmale. Dazu zählen *technische Umsetzbarkeit*, *Überlistungsresistenz* und die *Bereitschaft* der Zielgruppe, dieses Biometriemerkmal einzusetzen [BeRo2000].

Die einsetzbaren Verfahren und deren Effektivität werden auch durch das Umfeld bestimmt, in dem ein biometrisches Erkennungssystem arbeiten soll. Dazu zählt sowohl die Hard- und Software als auch die räumliche Umgebung, in der das System in einem gewissen Sicherheitsstandard laufen soll. Jedes Erkennungssystem stellt daher andere Voraussetzungen an das verwendete Merkmal.

In den folgenden Abschnitten werden die Anforderungen von eSign an ein biometrisches Merkmal diskutiert, welches auf dem Prototypen des SPP-Projektes die Digitale Signatur des Benutzers freischalten soll.

3.4.1 Technische Umsetzbarkeit

Da das eSign-Projekt für ein mobiles Endgerät konzipiert ist, ist eine einfache Integration in die schon vor dem Projektstart festgelegte Hardware notwendig.

Zwar sind auf mobilen Endgeräten meist Kartenschächte vorhanden, die die nachträgliche Erweiterung um Mikrofone oder hochwertigere Kameras erlauben. Diese zusätzlichen Module ermöglichen jedoch unter Umständen das Ausspähen der biometrischen Daten bei der Übertragung in das mobile Endgerät.

Kameras, die für heutige mobile Endgeräten vorhanden sind, sind technisch noch nicht ausgereift genug, um akzeptable Bilder für einen Gesichts- oder gar einen Irisvergleich zu machen.

Da die meisten PDAs über eine Stifteingabe verfügen, ist vom Standpunkt der technischen Umsetzbarkeit die Unterschriftseingabe als beste und kostengünstigste Möglichkeit zur biometrischen Erkennung anzusehen.

3.4.2 Überlistungsresistenz

Wie von Thalheim et al. [ThKrZi2002] demonstriert wurde, sind heutige Fingerabdruck-, Iris- und Gesichtserkennungssensoren noch relativ leicht zu überlisten. Durch die konstante Verbesserung der Soft- und Hardware wird es zunehmend schwerer, die Technik zu täuschen, obwohl bisher von einem alleinigen Einsatz eines biometrischen Merkmals abgeraten wird [FRVT2002].

Fälschungssicherheit ist ein wichtiger Faktor bei diesem Projekt, da mit der Digitalen Signatur von einem Fälscher rechtskräftige Verträge im Namen des Benutzers abgeschlossen werden könnten. Keine der vorgestellten Methoden kann sich in diesem Punkt einen Vorteil verschaffen, da sich alle noch in der Weiterentwicklung befinden und bedingt durch die natürliche Variation der biometrischen Merkmale keines eine 100-prozentige Klassifizierungsrate aufweisen kann.

3.4.3 Bereitschaft des Benutzers

Die Benutzerakzeptanz variiert je nach verwendetem Biometriemerkmal und ist von teilweise unbewussten Vorurteilen beeinflusst.

Die Abnahme von Fingerabdrücken erinnert viele Benutzer an die erkennungsdienstliche Behandlung durch die Polizei; Kameras erwecken den Anschein eines Überwachungsstaates, der den Benutzer jederzeit und überall unter Kontrolle hat. Bei der Iriserkennung denken die meisten Anwender, dass ihr Auge mit einem Laserstrahl abgetastet wird, obwohl dort eine Kamera benutzt wird. Die Frage nach der Hygiene spielt für die Benutzer ebenfalls eine Rolle, wenn mehrere hundert Personen im Laufe eines Tages einen Kontaktsensor berühren.

Die Unterschrift ist jedem Menschen aus dem Alltag als verlässliches Verfahren zum Beispiel zur Bestätigung von Geschäften bekannt und vertraut. Sie erscheint daher als geeignetstes biometrisches Merkmal, um die Akzeptanz durch den Benutzer zu erhöhen und wird deshalb auch von Johannes Kaiser zur Freischaltung der Digitalen Signatur vorgeschlagen [Ka2001].

3.4.4 Aktive Handlung des Benutzers

Das wichtigste Kriterium für eSign ist die aktive Handlung, die ein Benutzer ausführen muss, um sich mit seinem biometrischen Merkmal zu authentifizieren. Deshalb scheiden Verfahren wie die Gesichtserkennung, Fingerabdruck und Irisscan aus, da der Anwender sich zwar in den Erfassungsbereich eines Sensors begeben muss, dies aber nicht einer aktiven Handlung im Sinne

der handschriftlichen Unterschrift entspricht. Diese Handlung ist aber notwendig, damit das System sicher sein kann, daß der Benutzer seine Unterschrift willentlich abgegeben hat, und die Schutzfunktionen der Signatur gewährleistet bleiben.

Nur die Schrift- und Stimmerkennung bieten diese Sicherheit und können deshalb in Betracht gezogen werden. Das Tippverhalten des Benutzers ist eine dritte Möglichkeit, wird aber in diesem Projekt aufgrund der fehlenden Tastaturen bei mobilen Endgeräten ebenfalls nicht weiter berücksichtigt.

3.4.5 Alternative Authentifizierungsmöglichkeiten

Anstatt nur ein biometrisches Merkmal zu betrachten, kann im Falle einer Ablehnung ein zweites körperliches Charakteristikum zur Beurteilung hinzugezogen werden. Jedes weitere Merkmal muss aber wieder in Bezug auf seine Sicherheit und Umsetzbarkeit hin überprüft werden, um den Sicherheitsstandard des Systems nicht zu verringern. Dies erhöht den Hardwareaufwand und resultiert in höheren Kosten und einer längeren Enrollment-Phase, da alle Merkmale erfasst werden müssen.

Der erhöhte Hard- und Softwareaufwand zahlt sich aber bei geeigneter Wahl des zweiten Biometriemerkmals durch einen zumindest gleichbleibenden Sicherheitsstandard im Vergleich zu einer alleinigen Identifikation durch ein Merkmal aus. Außerdem werden so Benutzer nicht von dem System ausgeschlossen, die ein erforderliches Merkmal nicht vorweisen können.

Welcher Authentifizierungsmechanismus letztendlich eingesetzt wird, für alle Varianten ist festzuhalten, dass der Sicherheitsstandard des Systems lediglich so hoch sein kann, wie der des schwächsten Gliedes in der Kette der Authentifizierungsmerkmale. Wenn in dieser Kette aber eine PIN-Eingabe vorkommt, würden die Schwächen der PIN auch wieder in das System eingebracht werden, und der Benutzer wäre wieder das schwächste Glied. Die Vorteile einer biometrischen Erkennung kämen damit nicht mehr zum Tragen und das Konzept der biometrischen Erkennung auf einem mobilen Endgerät würde zu einem reinen Benutzungsmerkmal verkommen, welches keinerlei sicherheitsrelevanten Vorteile mehr für den Benutzer bietet.

3.5 Zusammenfassung

In der Arbeit von Kaiser wurde die Empfehlung ausgesprochen, als Ersatz für die Eingabe einer PIN ein biometrisches Merkmal zur Authentifizierung des Benutzers heranzuziehen [Ka2001b]. Diese auf der natürlichen Variation des menschlichen Körpers beruhenden Erkennungsverfahren ersetzen die bisher üblichen PIN-Authentifizierungen und erhöhen bei korrektem Einsatz den Sicherheitslevel des Gesamtsystems durch ihre Fälschungssicherheit beträchtlich, da ein biometrisches Merkmal nicht wie eine PIN verloren oder vergessen werden kann.

Auch diese Arbeit kommt zu dem Ergebnis, dass die Unterschrift als Authentifizierungsmerkmal

am besten geeignet ist, um die Digitale Signatur des Benutzers zu autorisieren. Die Unterschrift ist 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.

Diese Überlegungen werden nun in die Praxis umgesetzt. Dem Design und der Implementierung einer biometrischen Unterschriftseingabe auf einem mobilen Endgerät zur Freischaltung der Digitale Signatur widmet sich das nächste Kapitel.

4 Die Entwicklung von eSign

In diesem Kapitel wird beschrieben, wie das im Rahmen dieser Arbeit entwickelte Signaturwerkzeug auf einem mobilen Endgerät in die Praxis umgesetzt und auf einem PDA prototypisch implementiert wird. Dabei wird nach einem evolutionären Modell vorgegangen: Zuerst werden die Kern-Anforderungen definiert, bevor sie dann in der Praxis umgesetzt werden. Nach der Vorstellung des Programms auf der CeBIT und einem Benutzertest können dann die Anforderungen eventuell revidiert und neu implementiert werden.

Das Ziel des eSign-Projektes liegt in der prototypischen Entwicklung einer sicheren und gleichzeitig für den Nutzer einfach zu bedienenden Anwendung zur Erstellung digitaler Signaturen. Hauptmerkmal von eSign ist es, dass das Konzept der asymmetrischen Kryptographie vollständig vor dem Benutzer verborgen und die Schlüsselverwaltung und Signaturberechnung im Hintergrund für ihn erledigt wird.

Die Ziele der Implementierung sind dabei auf der Seite des Benutzers eine möglichst unkomplizierte Bedienung, sowie auf der Programmierebene die einfache spätere Erweiterbarkeit der Anwendung.

4.1 Stand der Wissenschaft

Die Idee, die handschriftliche Signatur zur Authentifikation des Benutzers heranzuziehen, ist in anderen Projekten bereits thematisiert worden, teilweise auf kommerzieller Basis [TÜV2002]. Dabei kann zwischen stationären und mobilen Lösungen unterschieden werden, wobei hier nur zwei ausgewählte Projekte vorgestellt und die Unterschiede zu dem Gesamtprojekt des SPP-Sicherheit verdeutlicht werden:

- Das Handschriften-Erkennungs-System HESY[1] ist als stationäres Gerät konzipiert. Es besteht aus einem Signiertablett, das die handschriftliche Unterschrift des Benutzers analysiert. Dabei werden auch die Druckstufen des Stiftes auf die Oberfläche mit in die Berechnungen mit einbezogen.

  Der Nachteil einer solchen stationären Lösung ist, dass der Benutzer an einen Ort und einen Computer gebunden ist, wenn er seine Unterschrift abgeben will. Außerdem ist

1 http://www.hesy.de/index.html

HESY als reines Authentifizierungssystem konzipiert, ohne dass auf die Benutzbarkeit der verwendeten Software eingegangen wird. Damit kann der Benutzer zu einem potentiellen Sicherheitsrisiko werden. Ebenso ist es möglich, die Übertragung der Daten zwischen Signiertablett und PC auszuspionieren und damit einen Angriff auf das System auszuführen.

Im Gegensatz dazu ist bei eSign kein Ausspionieren der Schlüssel- oder Unterschriftsdaten des Benutzers möglich, da diese sensiblen Daten nicht das Gerät verlassen müssen. Alle Anwendungen, auch die Erstellung der Digitalen Signatur, laufen auf dem PDA und sind auch auf ihre Benutzbarkeit hin optimiert.

- In dem im Jahre 2001 gestarteten Vernet-Projekt „Trusted Pocket Signer“[2] wird eine mobile, vertrauenswürdige Signatur-Plattform entwickelt. Als Zielgruppe ist dabei an Ärzte und andere Berufsgruppen gedacht worden, die im Laufe ihres Arbeitstages digitale Signaturen an wechselnden Orten erstellen müssen.

  Zur Authentifizierung des Nutzers ist eine Kombination aus SmartCard, PIN-Eingabe und Unterschriftsleistung vorgesehen. Der Anwender muss sich einmal pro Tag mit seiner SmartCard und PIN an einem beliebigen PDA einloggen und braucht dann alle Aktionen daran im Laufe des Tages nur noch mit seiner Unterschrift zu beglaubigen. Die Daten werden daraufhin drahtlos zu einem Computer übertragen und dort mit anderen Datenbanken im System synchronisiert.

  Genau wie bei dem HESY-System ist bei diesem Projekt ein stationärer PC nötig, der die Mobilität des Benutzers einschränkt. Die zu signierenden Daten werden lediglich auf verschlüsselten Kommunikationskanälen zu dem PDA übertragen, um dort nach Authentifizierung des Benutzers digital signiert zu werden. Es ist nicht vorgesehen, andere Anwendungen auf dem PDA laufen zu lassen. Daher ist ein zweiter PDA nötig, wenn der Benutzer weitere mobile Anwendungen benutzen möchte, was sich aufgrund der höheren Kosten negativ auf die Akzeptanz durch den Nutzer auswirkt.

4.2 Die Planungs- und Definitionsphase

Nach der Entscheidung, eine Biometriesoftware zur Freischaltung der Digitalen Signatur auf einem mobilen Endgerät zu entwickeln, besteht der nächste Schritt in der rechtzeitigen und möglichst detaillierten Planung und Definition des Projektes. Dabei steht die Erstellung eines Anforderungskatalogs und dessen Ausarbeitung in eine vollständige, konsistente, eindeutige und erfüllbare Produktdefinition im Vordergrund.

Eine zeitlich bindende Frist für das Projekt gab es nur insoweit, als dass der Beginn der CeBIT im März 2003 als Termin für die Fertigstellung der Software feststand. Da diese Arbeit im November 2002 begann, musste innerhalb von 4 Monaten das Projekt abgeschlossen sein. Der

2 http://www.sit.fraunhofer.de/english/SICA/sica_projects/TruPoSign/index.html

erste Monat wurde alleine mit der Planung und dem Design der Anforderungen verbracht, die übrigen drei Monate konnten zur Programmierung genutzt werden.

4.2.1 Ziele der Planungs- und Definitionsphase

Der Anforderungskatalog, der aus den meist ungenauen, vagen Projektangaben des Auftraggebers besteht, welche Funktionen das zu erstellende Modul zu besitzen hat, muss letztlich in eine Liste von exakten und unmissverständlichen Anforderungen und Zielen umgewandelt werden. Da eSign keine eigenständige Software, sondern in einem Gesamtprojekt eingebettet ist, muss bei der Festschreibung des Funktionsumfangs auf die anderen Teilprojekte Rücksicht genommen werden: Welche Erwartungen und Vorstellungen haben die anderen Gruppen, welche Leistungen werden von den anderen Modulen gefordert und welche Annahmen haben Entwickler und Programmierer selbst zu treffen und festzulegen? Je später im Projekt neue Funktionen hinzukommen, desto aufwändiger und kostspieliger sind diese zu implementieren.

4.2.2 Technische Grundlagen des Gesamtsystems

Zu Beginn dieser Diplomarbeit war das Gesamtprojekt schon weit fortgeschritten, die verwendete Hardware festgelegt und Teile der Software entwickelt. Diese Umstände mussten bei der Planung von eSign berücksichtigt werden.

Software

Die Oberfläche des PDA ist in Abbildung 4.1 zu sehen. Das Display ist dabei in drei Teile gegliedert: In die Titelleiste am oberen Rand, der Taskbar am unteren Rand sowie den für Programme nutzbaren Platz dazwischen. Als Programmiersprache wird projektweit Java benutzt, welches auf dem für PDAs angepassten Betriebssystem LucaOS[3] läuft und auf der Linux-Distribution Familiar[4] basiert.

Hardware

Bei dem in diesem Projekt prototypisch verwendeten PDA handelt es sich um einen Compaq iPAQ 3870 mit den im Anhang A aufgeführten technischen Spezifikationen. Von entscheidender Bedeutung für das Design der Software sind dabei die folgenden drei Punkte:

- Die Größe des PDA-Farbdisplays beträgt 240*320 Pixel, von denen effektiv für eine Anwendung lediglich 240*267 Pixel nutzbar sind. Der Rest des Displays wird von der Titelleiste und der Taskbar der Benutzungsoberfläche belegt. In letzterer werden essentielle

3 http://wwwspies.informatik.tu-muenchen.de/SPP/
4 http://familiar.handhelds.org/

Abbildung 4.1: Die Oberfläche des PDA

Informationen des Identitätsmanagements dargestellt, welches ein Sicherheitswerkzeug für die Verwaltung der persönlichen Daten des Benutzers ist [GeJe2001]. Da dort wichtige Informationen für den Benutzer zu sehen sind, wurde die Fläche der eSign-Anwendung nicht auf das gesamte Display ausgedehnt. Diese Einschränkung zwingt bei der Entwicklung von Programmen zu einem sorgsamen Umgang mit dem vorhandenen Platz.

- Der iPAQ besitzt nicht die Möglichkeit, verschiedene Druckstufen des Stiftes auf der Displayoberfläche zu unterscheiden. Die verwendete Programmiersprache Java bietet ebenfalls nicht die Möglichkeit, unterschiedliche Druckstufen des Eingabestiftes zu differenzieren. Somit kann eine Möglichkeit zur Erhöhung der Erkennungsrate des Verifikationsalgorithmus nicht genutzt werden, da genau wie die Geschwindigkeit der ausgeübte Druck des Stiftes auf das Display charakteristisch für einen Menschen und dessen Unterschrift sind.

- Der Prozessor des iPAQ ist eine mit 206 MHz getaktete Intel StrongARM CPU. Im Zusammenspiel mit der Sprache Java führt hier die relativ schwache Performance zu Problemen mit rechenintensiven Abläufen wie der digitalen Signierung von Daten und der Erfassung der Stiftbewegungen in Echtzeit.

4.2.3 Anforderungsanalyse

Der nächste Schritt nach der Analyse der bestehenden Hard- und Software besteht in der Bestimmung des genauen Funktionsumfangs des Signier-Moduls. Die Arbeitsgruppen des SPP-Projektes hatten im Vorfeld dieser Diplomarbeit bereits Drehbücher für die CeBIT entwickelt,

aus denen folgende zwei Szenarien bestimmt wurden, die zur Präsentation von eSign geeignet sind:

Szenario Geld abheben

Laut Drehbuch soll der Benutzer Geld von seinem Bankkonto abheben können. Dazu verlangt die auf dem PDA laufende Anwendung „Digitale Geldbörse“ von dem Benutzer zuerst die Bestätigung der Abbuchungsdaten und danach die Eingabe seiner PIN. Nach erfolgter Authentifizierung werden die Daten digital signiert und an die Bank übermittelt. Die Signatur der daraufhin zurückgelieferten digitalen Münzen wird auf ihre Richtigkeit hin überprüft. Die Quittung für die Bank wird wiederum digital signiert und an diese zurückgeschickt.

Die Digitale Geldbörse soll nun nicht mehr die PIN-Abfrage auf dem Schirm anzeigen (siehe Abbildung 4.4), sondern ruft sie eSign auf, welches vom Benutzer die Autorisierung der Abbuchung mit seiner Unterschrift verlangt. Nach erfolgreicher Authentifizierung signiert eSign die Daten digital und übergibt diese an die Digitale Geldbörse, die die Verschlüsselung und den Versand der Daten zur Bank vornimmt.

Szenario E-Ticket kaufen

Nachdem der Benutzer sich eine Zugverbindung ausgesucht hat und mit elektronischen Münzen die Zahlung durchführen möchte, wird die Digitale Geldbörse aufgerufen. Dort existierte bisher nur eine PIN-Abfrage zur Bestätigung der Zahlung, die durch eSign ersetzt werden könnte. Für die CeBIT wurde jedoch aus Zeitgründen entschieden, sich auf das erstgenannte Szenario zu beschränken.

Allgemeine Anforderungen

Ausgehend von diesen beiden Drehbuchszenarien wurden folgende allgemeinere Aufgabenstellungen konzipiert, die die eSign-Komponente zu erfüllen hat. Diese betreffen sowohl die Interaktion mit dem Benutzer, als auch die zugrundeliegenden algorithmischen Funktionen.

1. Auf Anfrage einer anderen Applikation wird der Benutzer aufgefordert, mit seiner Unterschrift ein Dokument auf dem Display zu signieren; eSign leitet ihn dabei durch diesen Vorgang.

2. Beim ersten Aufruf von eSign wird der Benutzer aufgefordert, dem zugrundeliegenden Algorithmus seine persönliche Unterschrift anzutrainieren.

3. eSign muss die Funktionalität bereitstellen, das zu unterschreibende Dokument digital mit dem privaten Schlüssel des Nutzers zu signieren.

4. eSign muss die Korrektheit eines empfangenen signierten Dokumentes mit dem öffentlichen Schlüssel des Absenders verifizieren können.

4.2.4 Ablaufsteuerung

Gemäß oben genannter Vorgaben wurden die Vorgänge innerhalb von eSign mittels eines Ablaufplans genauer spezifiziert. Dieser stellt die exakte Abfolge aus der Sicht des Benutzers innerhalb eines Signierprozesses dar. Diese Überlegungen beinhalten ebenso den Trainingsprozeß, um dem biometrischen Erkennungssystem Referenzdaten von der Unterschrift des Benutzers zur Verfügung stellen zu können. Je genauer dieser Ablauf spezifiziert ist, desto weniger Inkonsistenzen werden in der Benutzerführung im späteren Betrieb des Systems auftreten. Dies trägt sowohl zur Benutzbarkeit als auch zur Sicherheit des Gesamtsystems bei.

Trainingsphase

Damit der Benutzer anhand seiner Unterschrift identifiziert werden kann, sind Referenzdaten erforderlich, mit denen der Algorithmus die abgegebene Signatur vergleicht. Diese erforderliche Lernphase wird beim ersten Aufruf von eSign initiiert und besteht aus mehreren Durchläufen, von denen jeder folgendermaßen abläuft:

Der Benutzer bekommt zuerst auf dem Display einen in das Programm einführenden Text zu lesen. Da es erforderlich ist, dass er diesen sorgfältig durchliest, kann er erst fortfahren, wenn er bis zum Ende des Textes heruntergescrollt hat. Danach wird auf den Teil des Bildschirms umgeschaltet, auf dem die Referenz-Unterschrift abzugeben ist. Ein Screenshot des Trainingsprozesses ist auf Seite 45 abgebildet.

Diese Prozedur des *Lesens-Unterschreibens* wiederholt sich mehrere Male mit verschiedenen Hilfethemen, um dem Algorithmus die Verfeinerung der Trainingsdaten zu ermöglichen. Diese Trainingsphase, die das Handbuch von eSign darstellt, stellt somit gleichzeitig sicher, dass der Benutzer es gelesen hat.

Signieren eines Dokumentes

Greift eine Anwendung auf die Dienste von eSign zu, besteht der Ablauf stets aus den zwei Schritten *Präsentieren/Bestätigen* und *Unterschreiben*. Bevor der Benutzer ein Dokument unterschreiben kann, muss er dessen Korrektheit vorher bestätigen. Diese Bestätigung ist vor allem dann notwendig, wenn der Benutzer die zu signierenden Daten nicht vorher selber ausgewählt hat. Im Anschluss an diese Bestätigung gibt der Benutzer seine Unterschrift ab.

Der Benutzer signalisiert dabei durch einen Knopfdruck, dass er die gerade geschriebene Unterschrift verifizieren lassen möchte. Er hat aber auch die Möglichkeit, diese per Knopfdruck zu löschen und sie erneut zu schreiben. Diese Option ist erforderlich, da es denkbar ist, dass man

durch äußere Einflüsse beim Schreiben gestört wird, zum Beispiel durch das Rütteln in einem fahrenden Zug.

Zur Verifizierung der eingegebenen Unterschrift wird diese durch den Algorithmus mit der gespeicherten Referenz verglichen. Weist dieser die Unterschrift zurück, wird dies dem Benutzer mitgeteilt. Ruft eine Applikation eSign auf, muss ein Parameter mit übergeben werden, wie oft solch eine Zurückweisung möglich ist, bevor der gesamte Signiervorgang mit einer Fehlermeldung abgebrochen wird. In diesem Fall wird sowohl dies dem Benutzer durch einen Dialog mitgeteilt als auch eSign mit einer Fehlermeldung zur aufrufenden Anwendung geschlossen.

Stuft der Verifikations-Algorithmus die Unterschrift als korrekt ein, wird dem Benutzer die gelungene Authentifizierung in einem Dialog angezeigt und die Daten werden digital mit dem Schlüssel des Benutzers signiert. Die Berechnung der Digitalen Signatur wird nicht direkt von eSign durchgeführt, sondern durch den von der TU Darmstadt implementierten KeyStore-Manager[5], der eine auf elliptischen Kurven basierte Kryptographie-Bibliothek zur Verfügung stellt.

Die dazu notwendigen Schlüssel des Benutzers erhält eSign von der Klasse `idm.IDM.java` des im Prototypen implementierten Identitätsmanagers [GeJe2001b]. Dieser verwaltet die verschiedenen Identitäten des Benutzers und stellt die zur aktuell ausgewählten Identität passenden Schlüssel bereit.

Am Ende des Vorgangs werden alle Fenster von eSign geschlossen und die signierten Daten an die aufrufende Applikation zurückgeliefert.

Abbruch des Signier/Trainings-Vorgangs

Sollte der Benutzer mit den zu signierenden Daten nicht einverstanden sein, hat er jederzeit die Möglichkeit, den Vorgang abzubrechen. Durch das Betätigen des entsprechenden Buttons auf der Oberfläche des PDA wird der Signiervorgang nach einer weiteren Sicherheitsabfrage abgebrochen, die Fenster von eSign werden geschlossen und die aufrufende Applikation erhält eine Fehlermeldung über den Abbruch durch den Benutzer. Eine Unterscheidung zwischen einem gezielten Abbruch durch den Benutzer und einem Abbruch aufgrund eines Systemfehlers ist somit möglich.

Der schematische Ablaufplan des eSign-Programms ist in Abbildung 4.2 dargestellt. Der Ablauf der Trainingsphase ist aufgrund der Ähnlichkeit zu dem des Signiervorgangs nicht explizit aufgeführt.

4.3 Implementierung

Nach der Spezifikation der Anforderungen und dem Design des internen Ablaufs wurde mit der Implementierung von eSign begonnen. Auf eine detaillierte Darstellung aller Code-Segmente

5 http://www.informatik.tu-darmstadt.de/TI/Forschung/ECC

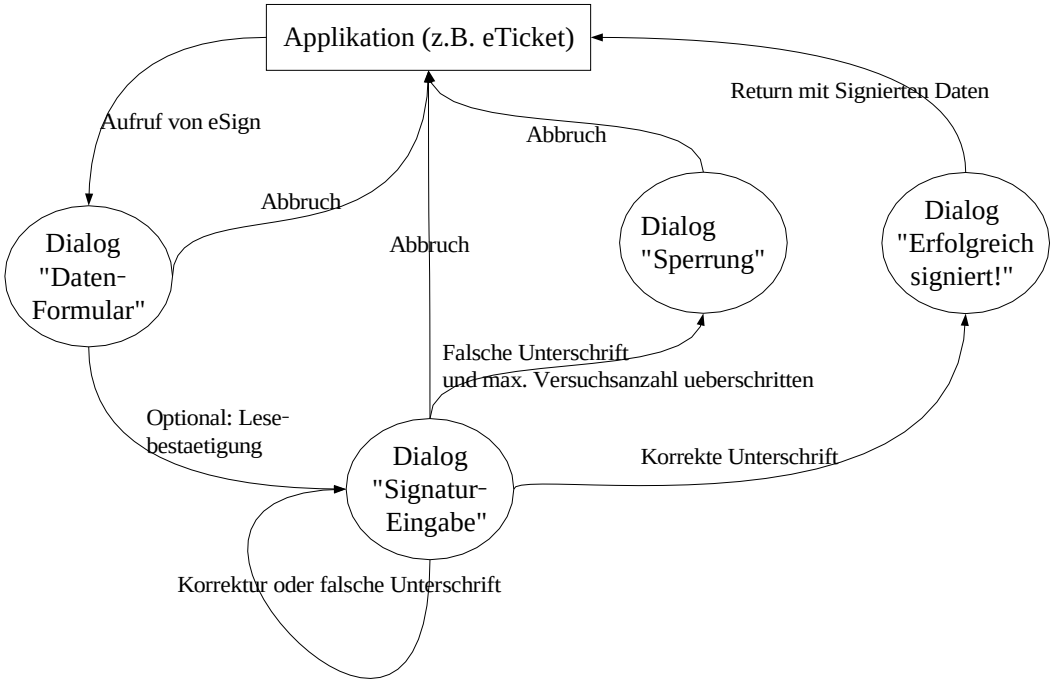

Abbildung 4.2: Der Ablaufplan von eSign

wird in dieser Arbeit verzichtet, der Inhalt dieses Abschnittes sind die drei Teilbereiche, auf die bei der Programmierung besonderen Wert gelegt wurde.

Mit dem Hinzufügen von neuen Verifikations-Algorithmen befasst sich der erste Bereich, der zweite mit dem von unbekannten Dokumenten. Der dritte Teil beschreibt die Schnittstellen, mit denen eSign anderen Applikationen wie zum Beispiel der Digitalen Geldbörse seine Funktionalität zur Verfügung stellt.

4.3.1 Einbindung neuer Verifikations-Algorithmen

Ein theoretisch optimaler Verifikations-Algorithmus weist eine Klassifizierungsrate von 100 Prozent auf, das heißt, er könnte eine gefälschte Unterschrift immer vom Original unterscheiden. Wie der Report des National Institute of Standards and Technology gezeigt hat, ist trotz Fortschritten in der Forschung selbst eine Erkennungsrate von über 90 Prozent für andere, weiter entwickelte biometrische Verfahren schon schwer zu erreichen [FRVT2002]. Ein Schwerpunkt dieser Diplomarbeit ist die Erstellung standardisierter Schnittstellen für die einfache Einbindung von Verifikations-Algorithmen in das Programm, nicht jedoch die eigentliche Entwicklung solcher Algorithmen. Neue, effizientere Verfahren können aber problemlos in eSign integriert werden

Zu implementierendes Interface

Um dem Programm einen neuen Algorithmus hinzuzufügen, muss dessen Implementierung das Interface `VerificationAlgorithm.java` aus dem Package `idm.standardapps.signature.algorithm` überschreiben. Folgende Methoden sind dabei zu implementieren:

- `void trainAlgorithm (Vector signature) throws SignatureException`:
  Der Parameter dieser Methode beinhaltet die einzelnen Punkte einer Unterschrift, die der Algorithmus in seine Referenzdaten aufnehmen soll. Die Punkte sind dabei als `SignaturePoints` gespeichert, welche sowohl die Raum- als auch die Zeitkoordinaten beinhalten.
- `boolean testSignature (Vector signature)`:
  Diese Methode vergleicht die übergebene Signatur mit der gespeicherten Referenz und gibt bei Übereinstimmung den Wert `true` zurück, andernfalls `false`.
- `String getName()`:
  Dies liefert einen beschreibenden Name für den Algorithmus zurück und ist nur notwendig, wenn mehrere Algorithmen im System registriert sind und eine Auswahl zwischen diesen stattfinden soll.

Eingebundene Verifikations-Algorithmen

Verschiedene Firmen befassen sich mit der Entwicklung von kommerziellen Lösungen für die Erkennung von Unterschriften. Die Doktorarbeit von Christiane Schmidt hat sich ebenfalls mit dem Thema von Online-Unterschriften-Analyse beschäftigt [Schmidt1998].

Da die von Christina Schmidt entwickelten Algorithmen nicht rechtzeitig für die CeBIT zur Verfügung gestellt werden konnten, wurde ein einfacher Algorithmus zur Verifikation der Unterschrift implementiert. Dieser klassifiziert die Unterschriften anhand der Zeit, die der Stift während der Unterschrift auf dem Display verbleibt, relativ zu der Zeit, in der er das Display verlässt. Ein Toleranzwert wird dazu gerechnet, um die Varianz der Unterschrift zu berücksichtigen.

$$\frac{Time_{OnDisplay}}{Time_{OffDisplay}} * Toleranz \tag{4.1}$$

Für die Präsentation des Gesamtsystems auf der CeBIT war dieser Algorithmus mehr als ausreichend. Da er aber unter anderem keinerlei Informationen über das Aussehen der Unterschrift berücksichtigt, ist er denkbar ungeeignet, sollte das Gesamtprojekt bis zur Marktreife weiterentwickelt werden. Dazu ist die Einbindung eines leistungsfähigeren Algorithmus erforderlich, der die Zeit-, Orts- und Druckinformationen in seine Berechnungen miteinbezieht.

4.3.2 Signieren verschiedener Dokumente

Die speziellen Anforderungen dieses Projekts verlangen, dass eine Abbuchungsbestätigung vom Benutzer mit seiner Unterschrift signiert wird, wobei seine Unterschrift in einem Trainingsprozeß dem Algorithmus zuvor anzulernen ist. Aus diesem Grund kann eSign zwei Dokumenttypen von dem Benutzer signieren lassen: Ein „HelpFile“ und eine „Withdrawel“. Der erste Typ präsentiert die schon im Abschnitt 4.2.4 beschriebenen Hilfetexte und die Referenzspeicherung, der zweite modelliert eine Abhebung von einem Bankkonto.

Neue Dokumenttypen, die eSign dem Benutzer zum Unterschreiben präsentieren soll, können dem Programm einfach hinzugefügt werden. Dokumenttypen sind generell in XML codiert und enthalten neben ihrem Namen weitere Informationen, im Falle einer Abbuchung unter anderem den abzuhebenden Geldbetrag und die Kontonummer des Benutzers.

Damit das System einen neuen Dokumenttypen erkennen kann, muss die Klasse `idm.standardapps.signature.DocumentParser.java` diesen XML-String parsen können. Sie generiert dann aus den darin enthaltenen Informationen ein neues Objekt, welches sowohl die graphische Repräsentation der Daten als auch die Logik zur Unterschriftseingabe enthält. Im Falle des Hilfetextes wird ein Objekt der Klasse `jdpHelpText.java` erzeugt, bei der Abhebung eines des Typs `jdpWithDraw.java`. Durch diese Modularität ist eine individuelle Anpassung der Oberfläche und des Ablaufs möglich.

Zu implementierendes Interface

Ein GUI-Objekt zur Repräsentation eines Dokumenttyps, wie es im vorherigen Abschnitt beschrieben wurde, muss unter anderem diese Methoden des Interfaces `idm.standardapps.signature.gui.jdpAbstract` überschreiben:

- `void specialInit(Object obj) throws Exception`:
  Dies initialisiert die Oberfläche des Dokumenttyps. Der Parameter enthält die zusätzlichen Informationen, die von dem `DocumentParser.java` aus dem XML-String ausgelesen wurden.

- `Vector getSignaturePoints()`:
  Wenn sich das Dokumenten-Fenster schließt, muss diese Methode die Punkte der geleisteten Unterschrift zurückliefern. Damit ein Abbruch des Signiervorgangs durch den Benutzer erkannt werden kann, muss in diesem Fall ein leerer Vektor zurückgeliefert werden.

- `void tryAgain()`:
  Wenn die Unterschrift zurückgewiesen wurde, wird diese Methode aufgerufen. Das Objekt setzt sich auf den Zustand vor der Unterschriftseingabe zurück, eventuelle Veränderungen seit der Initialisierung der GUI bleiben somit erhalten.

- `JPanel getShortForm()`:
  Nach der erfolgreichen Signierung wird dieses Panel angezeigt, zusammen mit dem Mitteilung, dass diese Daten signiert wurden. Hier sollten also nur die essentiellen Daten enthalten sein (siehe Abbildung 4.6).

4.3.3 Aufruf durch andere Applikationen

Um auf eSign zugreifen zu können, benötigt eine Applikation eine Referenz auf das eSign-Objekt. Diese erhält sie durch Aufruf der statischen Klassenmethode `Idm.getSignatureManager()`. Zur Signatur von Daten und zur Verifikation von erhaltenen digitalen Signaturen stellt dieses Objekt folgende Methoden zur Verfügung:

- `byte[] signDocument(String XMLdocument, int triesLeft, boolean showError) throws SignatureException`:
  Diese Methode initiiert eSign mit dem übergebenen XMLdocument. Daraus erzeugt das System ein von `jdpAbstract.java` abgeleitetes GUI-Objekt. Die beiden anderen Parameter geben an, wie oft die Unterschriftseingabe versucht werden kann und ob eSign eine Fehlermeldung bei Überschreitung dieser Anzahl anzeigen soll. Zurückgeliefert wird bei erfolgreicher Authentifizierung des Benutzers die elektronische Signatur des XMLdocuments in Byteform.

- `boolean verifyDocument(String doc, byte[] signature, ECPublicKey pub) throws SignatureException`:
  Hiermit wird anhand der Signatur `signature` überprüft, ob das Dokument `doc` von dem Benutzer mit dem öffentlichen Schlüssel `pub` signiert wurde. Bei einer erfolgreichen Verifizierung wird `true` zurückgegeben, ansonsten `false`.

4.4 Oberflächengestaltung

Geldautomaten benutzen einen Authentifizierungsmechanismus mit PIN und Chip-Karte. Die Bankkunden haben sich an die Bedienung dieser Automaten mittlerweile gewöhnt und sind mit deren Umgang vertraut. Um diesen Verbreitungsvorsprung aufzuholen, muss der Umstieg auf eine unterschriftsbasierte Lösung mit zusätzlichen Anreizen für den Benutzer erleichtert werden. Den Vorteil, sich keine PIN mehr merken zu müssen, darf eine Software nicht durch eine komplizierte und unverständliche Oberfläche verspielen. Außerdem können dadurch zu Sicherheitsrisiken führende Bedienungsfehler des Benutzers vermieden werden.

4.4.1 Die Passwort-Lösung der Digitalen Geldbörse

Bevor eSign in das Gesamtprojekt aufgenommen worden war, existierte bereits eine Authentifizierungslösung durch ein Passwort beim Abheben von digitalem Münzen. Wie bei eSign muss dabei der Benutzer des PDAs zuerst die Richtigkeit der Daten bestätigen (Abbildung 4.3), bevor er sein Passwort mit Hilfe des virtuellen Keyboards eintippen kann (Abbildung 4.4).

Benutzbarkeitsprobleme der Passwort-Lösung

Abgesehen von den schon vorher in Abschnitt 3.2.3 diskutierten prinzipiellen Schwächen einer Authentifizierung mittels PIN oder Passwort weist die Lösung der Digitalen Geldbörse noch darüber hinaus Design-Fehler in ihrer Oberfläche auf:

- Obwohl die Daten der Abbuchung, wie man später bei eSign sehen wird, auch auf einer Bildschirmseite untergebracht werden könnten, werden diese auf zwei Seiten verteilt. Dies vermindert die Übersichtlichkeit und weitere Probleme entstehen, die in den folgenden Punkten noch näher ausgeführt werden.

- Auf der zweiten Seite des Bestätigungsdialogs stehen wichtige Informationen der Abbuchung wie zum Beispiel der abzuhebende Geldbetrag. Der Benutzer muss erst gar nicht auf diese Seite umschalten, sondern kann sofort auf den OK-Button klicken und zur Passwort-Eingabe gelangen. Eine Warnfunktion vor einem falschen Betrag ist hier nicht gegeben.

Abbildung 4.3: Bisheriger Bestätigungsdialog in der Digitalen Geldbörse

Abbildung 4.4: Die Passwort-Eingabe der Digitalen Geldbörse

- Die Beschriftung der Buttons zum Wechseln auf die jeweils andere Seite sind nicht klar beschriftet. ”Weiter” könnte hier auch als Bestätigung der Daten interpretiert werden, um zur Passwort-Eingabe zu gelangen. Der OK-Button ist nicht sofort als solcher zu identifizieren, da er kein besonderes Design gegenüber den anderen Schaltflächen aufweist.

4.4.2 Die eSign-Oberfläche

Bei der Entwicklung der Oberfläche von eSign wurden die Schwächen der bisherigen Authentifizierungsmethode berücksichtigt, um die Benutzbarkeit der Software zu erhöhen. Folgende Veränderungen wurden in dem eSign-Modul vorgenommen, die die Benutzbarkeit erhöhen, und die sich an Leitfäden für das Oberflächendesign speziell von Handhelds orientieren.[6]

- Da keine projektweiten Design-Richtlinien gelten, was Farbe, Form und Lage von Buttons und anderen GUI-Elementen auf der Oberfläche angeht, wurde das Design von eSign an das der Digitalen Geldbörse angepasst, um zumindest in dem auf der CeBIT präsentierten Szenario ”Geld abheben” ein durchgängiges Design zu bewahren.

  Dazu wurden die Buttons, die nicht von der momentan gezeigten Seite abhängig sind, wie zum Beispiel der Hilfe-Button, wie in der Geldbörse in einer Leiste am oberen Rand des Displays gruppiert.

  Alle Buttons der eSign-Anwendung wurden in dem Stil der graphischen Buttons der Geldbörse gestaltet, um sich von den Standard-Buttons der Java-Laufzeitumgebung abzusetzen. Diese Buttons wurden konsequent in allen Dialogen verwendet und tragen zu einer einheitliche Oberfläche bei.

- Alle Anwendungen auf dem PDA haben als Farbe für ihre Titelleiste die voreingestellte blaue Standardfarbe gewählt. Um eSign und die Wichtigkeit der Unterschriftsleistung von den anderen Anwendungen abzuheben, ist deren Standardfarbe gelb, da diese eine größere Signalwirkung besitzt. Der Hintergrund der Anwendung wird auch in dieser Farbe dargestellt und trägt ebenfalls zu einem einheitlichen Design des Moduls bei.

- Die Darstellung der Abbuchungsbestätigung passt nun auf eine Bildschirmseite (siehe Abbildung 4.5(a)). Auf dieser erfährt der Benutzer, dass er jeden einzelnen der aufgeführten Posten wie Kontonummer, Betrag etc, bestätigen muss, um die Korrektheit der Daten zu garantieren. Dieses Konzept einer Checkliste ist dem Benutzer bekannt und vertraut, wird aber zusätzlich noch einmal auf dem Display erklärt. Der Button zum Scrollen des Bildschirms ist auf der Abbildung noch deaktiviert, da noch nicht alle Punkte der Checkliste abgehakt sind.

6 http://www.mobilecoders.com/Articles/mc-01.asp

(a) Bestätigung der Daten **(b)** Unterschriftseingabe

Abbildung 4.5: Bestätigung der Abbuchung und anschließende Signierung in eSign

Abbildung 4.6: eSign-Dialog bei erfolgreicher Verifi kation der Unterschrift

Erst nach Bestätigung aller Daten scrollt der Bildschirm zum oberen Rand hinaus. Es erscheint von unten das Unterschriftseingabefeld, auf dem der Benutzer wie bei einem Papierdokument unterhalb der zu signierenden Daten unterschreibt (vgl Abbildung 4.5(b)).

- Der Durchlauf einer Trainingseinheit für den Benutzer folgt einem ähnlichen Prinzip: Der Benutzer muss zuerst bis ans Ende des Textes scrollen, bevor der Knopf aktiviert wird, der den Bildschirm nach oben wegscrollen lässt.

  Das Design ähnelt dem einer Abbuchungsbestätigung, jedoch sind die Texte und Buttons der veränderten Situation angepasst (siehe Abbildung 4.7).

- Während des gesamten Vorgangs bleibt die Taskbar am unteren Ende gesperrt, da sonst der Benutzer eventuell andere Vorgänge ausführt, die ihn von seiner eigentlichen Aufgabe ablenken. Somit könnte er mit einer anderen Anwendung ein zweites Signierfenster öffnen, was zu einer Verwechslung der zu unterschreibenden Daten führt.

- Der Benutzer kann zwar jederzeit sowohl das Training als auch den Authentifizierungs-Vorgang abbrechen, jedoch findet zuvor immer eine Sicherheitsabfrage statt, so dass keine unbeabsichtigte Beendigung des Programms veranlasst werden kann.

(a) Einführungstext **(b)** Referenzeingabe

Abbildung 4.7: Hilfetext und anschließende Referenzeingabe in eSign

4.5 Vorführung von eSign auf der CeBIT

Während der CeBIT vom 12. bis zum 19. März 2003 in Hannover gab es viele interessierte Besucher, die sich an dem Stand des Schwerpunktprogramms „Sicherheit“ der DFG einem Benutzertest des eSign-Moduls unterziehen wollten (siehe Abbildung 4.8). Dabei reichte die Zeit nicht aus, um einen ausführlichen Benutzertest mit einem standardisierten Versuchsaufbau und -ablauf durchzuführen. Vielmehr wurden die Teilnehmer durch einen verkürzte Einführung in das Programm angelernt, um anschliessend einen Geldtransfer aus der Digitalen Geldbörse heraus mit ihrer vorher eintrainierten Unterschrift zu signieren. Anschließend wurden die Teilnehmer nach ihrer Meinung zu dem Programm befragt.

Abbildung 4.8: Projektpräsentation auf der CeBIT

4.5.1 Anpassungen an eSign für die CeBIT

Für die Präsentation vor Publikum mussten einige Veränderungen an dem Code von eSign vorgenommen werden. So wurde die einleitende Trainingsphase von drei auf einen Durchlauf verkürzt und die Bestätigung der Daten wurde dahingehend vereinfacht, dass der Scroll-Button am oberen Displayrand immer aktiviert ist. Es wurde ebenfalls die Möglichkeit implementiert, das Training manuell zu starten, ebenso wie die Option, die vorhandenen Referenz-Daten zu löschen. Diese Optionen sind aber nur über eine gesonderte Anwendung auf dem PDA veränderbar, welche in einem serienreifen Betrieb des PDA für den Benutzer nicht zugänglich ist.

4.5.2 Reaktionen des Publikums

Aus den Gesprächen mit den Besuchern auf der CeBIT ergab sich, dass viele der Benutzer die Authentifizierung durch die eigene Unterschrift sicherer und auch einfacher fanden als eine PIN-Abfrage. Durch die Ähnlichkeit zu einer handschriftlichen Unterzeichnung wurde auch die aktive Willenserklärung als deutlicher als bei einer PIN-Eingabe empfunden.

Dennoch waren die Benutzer teilweise immer noch mit der Oberfläche überfordert oder haben selbst die kurz gehaltenen erklärenden Texte auf dem Display nicht gelesen. Aber erst mit einem standardisierten und mit genügend Teilnehmern durchgeführten Benutzertest dürfte ersichtlich werden, wo noch Verbesserungen an der Oberfläche vorgenommen werden müssen.

4.6 Zusammenfassung

Dass das primäre Ziel von eSign erfüllt wurde, auf Benutzerebene die Komplexität der Digitalen Signatur vor dem Benutzer zu verbergen und durch einen vertrauteren und sicheren Mechanismus zu ersetzen, konnte auf der CeBIT nachgeprüft werden.

Die Autorisierung der Digitalen Signatur durch die handschriftliche Unterschrift überträgt die Willenserklärung, die dieser innewohnt, auf die Digitale Signatur. Für die befragten Zuschauern, die eSign auf der CeBIT ausprobierten, drückte sich diese Willenserklärung, die sie mit ihrer Unterschrift unter ein digitales Dokument auf das Display des PDA abgaben, deutlicher aus als bei einer PIN-Eingabe.

Insgesamt war das Echo des Publikums auf die Unterschriftseingabe bei eSign trotz der vielleicht noch verbesserungswürdigen Oberfläche durchweg positiv und es kann davon ausgegangen werden, dass eine unterschriftsbasierte biometrische Authentifizierung die PIN-Eingabe in der Gunst der Benutzer überholen könnte.

Auf Programmierebene gestaltet sich die zukünftige Erweiterung des Codes von eSign aufgrund des modularen Aufbaus sehr einfach, so dass neue und bessere Verifikationsalgorithmen und mehr Dokumenttypen mit individuellen Oberflächen hinzugefügt werden können.

5 Zusammenfassung und Ausblick

Biometrische Authentifizierung wird zu einem Bestandteil der Gesellschaft. Sie ist jetzt schon an einigen Flughäfen und Grenzen im Einsatz und weitere Systeme, die bisher die herkömmlichen Verfahren wie PIN oder Passwörter benutzt haben, werden diesem Trend folgen.

Auch wenn die Erkennungsrate von heutigen biometrischen System noch verbesserungswürdig ist, so ist doch abzusehen, dass auf längere Sicht die Biometrie die Authentifizierung durch PIN oder Passwort ablösen wird. Um keine Zwei-Klassen Gesellschaft entstehen zu lassen, die die Leute außen vor lässt, die biometrische System nicht nutzen wollen oder können, wird die PIN aber nicht völlig verschwinden.

Eine Ausweg bietet der Vorschlag im Face Recognition Vendor Test, mehrere biometrische Merkmale zur Authentifizierung des Benutzers heranzuziehen [FRVT2002]. Somit steigt nicht nur die Erkennungsrate, es werden auch die Leute nicht mehr benachteiligt, deren biometrisches Merkmal nicht ausgeprägt genug ist, als dass es durch das System eindeutig identifiziert werden könnte.

Für eine spätere Marktreife von eSign wäre der Umstieg auf einen leistungsfähigeren PDA wie beispielsweise den Compaq iPAQ h5450 angebracht. Dieser besitzt neben einem schnelleren Prozessor, der die Zeit zur Datenerfassung und -verarbeitung verkürzt, einen eingebauten Fingerabdruckscanner, der zur Identifizierung des Benutzers mit hinzugezogen werden kann. Eine auf den Prozessor abgestimmte Programmiersprache wie zum Beispiel C++ würde weitere Geschwindigkeitsoptimierungen erlauben. Wünschenswert für eine marktreife Version ist außerdem ein Display, welches die unterschiedlichen Druckstufen des Stiftes erkennt und an die Software übermittelt.

Auf der Seite der Software sind durch die Programmierung von eSign alle Möglichkeiten gegeben, um problemlos neue, effizientere Verifikationsalgorithmen einzubinden. Weitere Dokumenttypen, die vom Benutzer signiert werden sollen, können genauso einfach eingebunden werden. Eine weitere sinnvolle Erweiterung für das Gesamtprojekt wäre in diesem Zusammenhang die Einführung eines Dateimanagers, der beliebige Dokumente an eSign zum Signieren übergeben könnte.

In der kurzen Zeit konnte kein standardisierter Benutzertest durchgeführt werden, um die Oberfläche und den Ablauf des Unterschreibens zu verbessern. Eventuell könnten Geräusche wie das Kratzen eines Stiftes während des Digitalen Signierens dem ganzen Prozess eine größere Alltags-Vertrautheit geben und somit die Akzeptanz bei den Benutzern erhöhen.

Trotz des prototypischen Charakters des Gesamtsystems bleibt festzuhalten, dass die hier vorgestellte Lösung einer unterschriftsbasierten Benutzerauthentifizierung als eine der besten Lösung anzusehen ist, um die Verwendung der Digitale Signatur für den Benutzer einfach und dennoch sicher zu gestalten. Die Benutzung eines vertrauten Merkmals und die Verbergung von komplexen technischen Zusammenhängen vor dem Benutzer sind die Grundlage für die einfache Bedienbarkeit von eSign.

A Technische Daten des Compaq iPAQ 3870

Abbildung A.1: Der Compaq iPAQ 3870

Parameter	Wert
Prozessor	206 MHz Intel StrongARM SA-1110 32-bit RISC Processor
Speicher	64-MB SDRAM + 32-MB Flash ROM Memory
Maße (H x B x T)	133 mm x 80 mm x 16 mm
Gewicht	180 g, einschließlich Akku
Display-Typ	Touchscreen TFT-Reflektions-Farb-LCD
Anzahl der Farben	65.536
Auflösung (Breite x Höhe)	240 x 320 pixel
Pixelabstand	0,24 mm
Sichtbare Bildgröße	57,6 mm breit x 76,82 mm hoch

Abbildung A.2: Datenblatt des Compaq iPAQ 3870

Abbildungsverzeichnis

Literaturverzeichnis

[Al2002] Astrid Albrecht. *Biometrie und Recht*, Kapitel II-2, Seiten 97–114. Lothar Leger, Veronika Nolde, 2002.

[AVBPA2001] Josef Bigün und Fabrizio Smeraldi, Herausgeber. *Third International Conference, Audio- and Video-Based Biometric Person Authentication*, Band 2091 von *Lecture Notes in Computer Sciene*. Springer, 2001.

[BeRo2000] Michael Behrens und Richard Roth. Sind wir zu vermessen, die PIN zu vergessen? *DuD - Datenschutz und Sicherheit*, 6/2000(24):327–331, 2000.

[BeRo2002] Michael Behrens und Richard Roth. *BioTrusT: Untersuchung der Akzeptanz und Nutzung biometrischer Identifikationsverfahren*, Kapitel V-4, Seiten 399–419. Lothar Leger, Veronika Nolde, 2002.

[BuDa2002] Henning Daum Dr. Christoph Busch. Frei von Zweifel? Biometrische Erkennung: Grundlagen, Verfahren, Sicherheit. *c't magazin für computertechnik*, 5/2002:156–161, 2002.

[DiMaVi2002] Astrid Mayerhöfer und Claus Vielhauer Dr. Jana Dittmann. *Praktische Angriffsmöglichkeiten auf biometrische Systeme*, Kapitel III-4, Seiten 192–200. Lothar Leger, Veronika Nolde, 2002.

[Er2002] Sabine Ertl. Biometrie: Der Körper als Schlüssel? Technischer Bericht, Wiener Zeitung, 2002. http://www.wienerzeitung.at/aktuell/2002/biometrie/default.htm.

[FRVT2002] National Institute of Standards und Technology. The Face Recognition Vendor Test 2002. Technischer Bericht, National Institute of Standards and Technology, 2002. http://www.frvt.org/FRVT2002/documents.htm?tag=nl.

[Ge2003] Daniela Gerd tom Markotten. USE - Usable Security Evalution. *Eingereicht zur CHI 2003*, 2003.

[GeJe2001] Daniela Gerd tom Markotten und Uwe Jendricke. Identitätsmanagement im E-Commerce. *it+ti Informationstechnik und Technische Informatik*, 43(5):236–245, October 2001. http://www.iig.uni-freiburg.de/telematik/atus/publications/GeJe2001.pdf.

[GeJe2001b] Daniela Gerd tom Markotten und Uwe Jendricke. Identitätsmanagement: Einheiten und Systemmanagement. *Verlässliche IT-Systeme - Sicherheit in komplexen Infrastruktur*, Seiten 77–85, September 2001.

[GeJe2003] Daniela Gerd tom Markotten und Uwe Jendricke. Erfolgsfaktor für E-Commerce: Benutzbare Sicherheit. *Eingereicht für Wirtschaftsinformatik*, 2003.

[IFCC2003] Internet Fraud Complaint Center. IFCC Annual Internet Fraud Report 2002. Technischer Bericht, Internet Fraud Complaint Center, April 2003. http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf.

[Kü2002] Frak Künzer. *Kann sich die Fingerabdruck-Technologie durchsetzen?*, Kapitel IV-9, Seiten 281–291. Lothar Leger, Veronika Nolde, 2002.

[Ka2001] Johannes Kaiser. Vertrauensmerkmal Unterschrift - Gestaltungskriterien für sichere Signierwerkzeuge. In *Informatik 2001 - Tagungsband der GI/OCG-Jahrestagung, 25.- 28. September 2001*, Seiten 500–504, 2001.

[Ka2001b] Johannes Kaiser. Integration vertrauter Merkmale als Gestaltungsprinzip für sichere Systeme. *Informationstechnik und Technische Informatik (it+ti)k*, 5/2001(43):264–269, 2001.

[NCC2000] National Consumer Council. E-commerce and consumer protection. A report by the National Consumer Council, August 2000. http://www.ncc.org.uk/pubs/pdf/ecomm_full.pdf.

[Ross94] A. Roßnagel. *Die Simulationsstudie Rechtspflege: eine neue Methode zur Technikgestaltung für Telekooperation*. sigma-Verlag. 1994.

[RSA78] A.Shamir R.L.Rivest und L.Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, Februar 1978.

[Sc1996] Bruce Schneier. *Angewandte Kryptographie*. Addison Wesley (Deutschland) GmbH. 1996. ISBN 3-89319-854-7.

[Schmidt1998] Christiane Schmidt. *On-line Unterschriftenanalyse zur Benutzerverifikation*. PhD thesis, TH Aachen, 1998.

[ScSt2000] Dirk Scheuermann und Bruno Struif. Usability of Biometrics in Relation to Electronic Signatures. Technischer Bericht, GMD- Forschungszentrum Informationstechnik, November 2000.

[Si2002] Richard Sietmann. Hype verflogen. *c't magazin für computertechnik*, 9/2002:48–49, 2002.

[SigG2001] Bundesregierung. Gesetz über Rahmenbedingungen für elektronische Signaturen. BGBl. I 2001, 876, 2001. http://jurcom5.juris.de/bundesrecht/sigg_2001/gesamt.pdf.

[SP2003] Softpro GmbH & Co. KG., Wilhelmstraße 34, 71034 Böblingen. *Das sichere Doppel - Wissenswertes über Unterschriften-Prüfung und biometrische Authentifikation*, März 2003. http://www.signplus.com/e/download/fachinfo_klassische_und_digitale_unterschrift.doc.

[ThKrZi2002] Peter-Michael Ziegler Lisa Thalheim, Jan Krissler. Körperkontrolle. *c't magazin für computertechnik*, 11/2002:114–123, 2002.

[TÜV2002] TÜVit. Mobile elektronische Signatur : eine Übersicht. Technischer Bericht, TÜV Informationstechnik GmbH, Dezember 2002. http://www.mediakomm.net/documents/forschung/mobile—signatur.pdf.