[RBLKPHSt+06] *Nicolas Repp, Rainer Berbner, Joerg Lenz, Christiane Kaplan, Alejandro Perez, Oliver Heckmann, and Ralf Steinmetz;* **Digitalisierte eigenhäendige Unterschrift im Online-Banking;** D-A-CH Security 2006, March 2006.

Beitrag eingereicht und akzeptiert auf D-A-CH Security 2006

Digitalisierte eigenhändige Unterschrift im Online-Banking

Nicolas Repp[1], Rainer Berbner[1], Alejandro Pérez[1], Jörg Lenz[2], Christiane Kaplan[2], Oliver Heckmann[1], Ralf Steinmetz[1]

[1]Multimedia Communications Lab KOM
Technische Universität Darmstadt
Merckstraße 25
64283 Darmstadt
[repp|berbner|perez|heckmann|steinmetz]@kom.tu-darmstadt.de

[2]SOFTPRO – Software Professional GmbH & Co. KG
Wilhelmstrasse 34
71034 Böblingen
[jle|csc]@softpro.de

Zusammenfassung

Online-Banking stellt eine einfache Methode dar, seine Bankgeschäfte von zu Hause aus erledigen zu können. Weitere Vorteile des Online-Bankings sind sowohl für Bankkunden als auch die anbietende Bank selbst die niedrigen Transaktionskosten, die im Rahmen des Online-Bankings anfallen. Allerdings sind in der letzten Zeit Online-Banking-Systeme wegen massiver Sicherheitsprobleme in Verruf geraten. Gerade Systeme, die auf PIN und TAN basieren, weisen eine Reihe von Sicherheits- und Akzeptanzproblemen auf.

Die Probleme im Online-Banking basieren zu einem nicht unerheblichen Anteil darauf, dass den Benutzern im Internet ein ausgeprägtes Sicherheitsbewusstsein fehlt. PIN und TAN stellen abstrakte Konstrukte zur Authentifizierung und Autorisierung dar, deren potentielles Missbrauchspotential den Benutzern oftmals nicht bewusst ist. Dieser Beitrag beschreibt einen Ansatz, die eigenhändige Unterschrift als Ergänzung oder Ersatz für Authentifizierung und Autorisierung im Online-Banking einzusetzen. Das Leisten einer Unterschrift ist dem Benutzer als Form der Autorisierung und Erklärung des Einverständnisses bekannt und die potentiellen Risiken bewusst. Weiterhin wird in diesem Beitrag ein Prototyp vorgestellt, der den Einsatz der eigenhändigen Unterschrift im Online-Banking realisiert.

Teile der Arbeit entstanden mit Unterstützung des E-Finance Lab e.V., Frankfurt am Main (http://www.efinancelab.de).

1 Motivation

Die Anzahl aller bei deutschen Kreditinstituten geführten Online-Konten lag Mitte 2004 bei knapp 35 Millionen [Deut04]. Zu diesem Zeitpunkt wurden rund 80 Prozent der Girokonten bei privaten Banken auch online geführt - bei den Sparkassen etwa die Hälfte. Nach Einschätzung der Branche werden allerdings nur ein Drittel der Online-Konten regelmäßig in Anspruch genommen [WüHa02]. Gründe für die schlechte Akzeptanz werden unter anderem in Sicherheitsbedenken gegenüber den existierenden Verfahren gesehen, so dass ein Teil der für das Online-Banking angemeldeten Konteninhaber für ihre Bankgeschäfte doch wieder auf papierbasierte Prozesse zurückgreifen. Sicher nicht zuletzt durch die Berichterstattung über „Trojaner", „Spoofing" oder „Phishing" (z.B. [Bach05], [Fina03], [Skud05]), speziell in Verbindung mit dem PIN/TAN-Verfahren, werden potentiellen Nutzer verunsichert. So lag beispielsweise im Jahr 2003 die Anzahl nicht online durchgeführter Transaktionen immer noch bei 1,6 Milliarden [Fies04].

Bereits im Jahr 2001 wurden von Bankenvertretern erste Bedenken an Finanzportalen geäußert, die auf dem PIN/TAN-Verfahren basieren. Sie wurden als Gefährdung der Beziehung zwischen Kunde und Kreditinstitut eingestuft und ihre baldige Ablösung gefordert [vonS01].

Bisher noch kaum in Erwägung gezogen wurde eine eigentlich nahe liegende Form der Authentifizierung: die eigenhändige Unterschrift kann, wenn sie direkt beim Schreiben digitalisiert wird, PIN und TAN ersetzen. Im Rahmen der Zusammenarbeit zwischen dem E-Finance Lab e.V., Frankfurt am Main, dem Multimedia Communications Lab[1] der Technischen Universität Darmstadt sowie des auf die Erkennung und Verarbeitung digitalisierter eigenhändiger Unterschriften spezialisierten Unternehmens Softpro[2] aus Böblingen entstand ein Prototyp, welcher die Machbarkeit einer solchen Lösung sowie die Akzeptanz potentieller Kunden im Rahmen des Online-Bankings nachweisen soll. Anhand des Prototyps wird den Kreditinstituten einerseits die technische Machbarkeit vorgeführt und andererseits die vertiefende Integration diskutiert. Der Prototyp beinhaltet eine Reihe von Funktionen einer traditionellen Online-Banking-Lösung, in welcher für Authentifizierung und Autorisierung auf die Verwendung der digitalisierten eigenhändigen Unterschrift zurückgegriffen wird.

Ausgehend von einer Betrachtung der am Markt befindlichen Verfahren zur Authentifizierung von Nutzern und Autorisierung von Transaktionen werden im Folgenden die Grundlagen einer unterschriftsbasierten Online-Banking-Lösung beschrieben sowie ein entsprechender Prototyp vorgestellt. Weiterhin stellen wir potentielle Angriffszenarien auf unseren Ansatz dar und skizzieren Möglichkeiten zu deren Vermeidung.

2 Existierende Verfahren zur Authentifizierung und Autorisierung im Online-Banking

Das älteste und technologisch am wenigsten komplexe Verfahren ist das PIN/TAN-Verfahren. Im Rahmen dieses Verfahrens erfolgt die Authentifizierung eines Kunden im Online-Banking durch eine Benutzerkennung (z.B. die Kunden- oder Kontonummer) in Verbin-

[1] http://www.kom.tu-darmstadt.de

[2] http://www.softpro.de

dung mit einem nur dem Kunden bekannten Kennwort, der so genannten Persönlichen Identifikationsnummer (PIN). Die Benutzerkennung in Kombination mit der PIN muss einmalig pro Session eingegeben werden. Um nun eine einzelne Transaktion zu autorisieren, steht dem Kunden eine Liste zufällig generierter Transaktionsnummern (TAN) zur Verfügung, von denen pro Transaktion eine verwendet werden muss. Eine solche TAN kann nur einmal verwendet werden. Die TAN werden in Form einer Liste dem Kunden per Briefpost in speziell versiegelten Umschlägen zugestellt.

Der Vorteil des PIN/TAN-Verfahrens ist es, dass auf Seiten des Kunden keine zusätzlichen technischen Hilfsmittel eingesetzt werden müssen. Somit sind die Anschaffungs- bzw. Einführungskosten gering. Allerdings kostet die Erstellung und der Versand einer TAN-Liste rund 4,50 Euro [Mart04]. Über die Kosten vergessener PIN liegen aktuell keine Informationen vor. Ein Vergleich mit anderen Branchen lässt allerdings deren Höhe vermuten. Dort entstehen in der Systemadministration jährlich Kosten von bis zu 350 Euro pro Nutzer durch vergessene Passwörter [Hurl03]. Der Betreuungsaufwand bei vergessenen PIN und gesperrten Konten auf Grund von wiederholt falschen Eingaben von PIN oder TAN wird sich für diese Form der Authentifizierung nur kaum reduzieren lassen.

Ergänzend muss an dieser Stelle erwähnt werden, dass alle zurzeit aktuellen Angriffsverfahren auf Online-Banking-Systeme sich die Schwächen des PIN/TAN-Verfahren zunutze machen.

Auf Grund der schon im ersten Abschnitt dieses Beitrags angesprochenen Probleme des PIN/TAN Verfahrens haben verschiedene Online-Banking-Anbieter eigene Erweiterungen an dem Verfahren vorgenommen, um dessen Sicherheit und das Vertrauen in die jeweiligen Lösungen zu erhöhen. Eine Reihe Banken setzt mittlerweile das mit iTAN bezeichnete Verfahren ein, welches im Rahmen der Abfrage einer TAN nicht eine beliebige auf der Liste des Kunden noch verfügbare TAN akzeptiert, sondern ausschließlich eine zuvor für diese Transaktion indizierte TAN.[3]

Eine andere Erweiterung des traditionellen PIN/TAN Verfahrens stellt die eTAN dar. Im Rahmen des elektronischen TAN Verfahrens bekommt der Kunde von seinem kontoführenden Institut ein Gerät zur Verfügung gestellt (oder muss dieses käuflich erwerben), in welchem eine während der Transaktionsdurchführung erstellte Kontrollnummer eingegeben werden muss. Das Gerät erzeugt auf Basis der Eingabe ein gültige TAN, die vom Kunden dann im Online-Banking-System der Bank eingegeben werden kann, um die Transaktion zu autorisieren.[4]

Eine weitere Modifizierung des PIN/TAN-Verfahrens ist die so genannte mTAN. Die Mobile TAN integriert die Short Message Service (SMS) Technologie aus dem Mobilfunk mit dem Online-Banking. Ein Kunde bekommt zur Autorisierung eine einmal gültige, speziell der gestarteten Transaktion zugeordnete TAN per SMS auf sein Mobiltelefon zugestellt und kann diese dann analog einer TAN verwenden. Die Mobilfunknummer muss zuvor bei der kontoführenden Bank durch Eingabe einer normalen TAN freigeschaltet werden.

Eine Alternative zu den zuvor beschriebenen Varianten des PIN/TAN-Verfahrens ist das auf dem Einsatz von asymmetrischen Verschlüsselungsverfahren basierende Home Banking

---

[3] Erste Evaluierungen des Verfahrens durch die RWTH Aachen ergaben, dass auch dieses Verfahren eine Reihe von Schwachpunkten besitzt – vgl. http://www.redteam-pentesting.de/advisories/rt-sa-2005-014.txt

[4] http://www.gemoneybank.de/privatkunden/pcbanking/etan/index.shtml

Computer Interface (HBCI). HBCI stellt eine automatisiert nutzbare, multibankfähige Homebanking Schnittstelle dar, die auf einer Reihe von Plattformen und Technologien verfügbar ist. HBCI ist, im Vergleich zum PIN/TAN-Verfahren, nicht ausschließlich ein Verfahren zur Autorisierung und Authentifizierung, sondern beinhaltet darüber hinaus Funktionen wie beispielsweise ein Transaktionskonzept und Mandantenfähigkeit. HBCI wurde im Auftrag des Zentralen Kreditausschusses (ZKA) entwickelt, dem die wichtigsten der deutschen Bankenverbände angehören und stellt somit einen primär nationalen Standard dar.

Das HBCI-Verfahren befindet sich sowohl mit Schlüsseldiskette als auch mit Smartcard im Einsatz, wobei die höchste Sicherheit nur unter Verwendung der kostspieligen Smartcard mit entsprechendem Lesegerät erreicht wird. In jedem Fall muss der Kunde zur Autorisierung und Authentifizierung eine PIN eingeben, die dann den privaten Schlüssel des Kunden freischalten, welcher sich auf Diskette oder Smartcard befindet. Der Schlüssel wird dann für die Erstellung einer digitalen Signatur der Transaktionen verwendet. Der Bankserver auf der Gegenseite kennt den öffentlichen Schlüssel des Kunden und kann auf diese Weise die Signatur der Transaktion verifizieren. Die Verbindung mit der Bank wird ihrerseits unter Einsatz eines symmetrischen Verschlüsselungsverfahrens verschlüsselt.

Die Entwicklung von HBCI wird seit 2002 im Rahmen des Financial Transaction Services Frameworks (FinTS) fortgeführt. FinTS integriert die Verfahren PIN/TAN und HBCI innerhalb eines gemeinsamen Frameworks, welches weiterhin zu den Verfahren auch Geschäftsvorfälle und Finanzdatenformate definiert [Zent05]. Aktuell liegt die Version 4 vor, die 2004 vom ZKA verabschiedet wurde.

3 Die Digitalisierung der eigenhändigen Unterschrift

Unter den biometrischen Merkmalen weist die Unterschrift eine Sonderstellung auf. Als gewohnte Form der Autorisierung und der Erklärung des Einverständnisses bei Transaktionen und Verträgen braucht ihre Anwendung nicht erklärt zu werden. Die eigenhändige Unterschrift wird nicht vergessen und kann auch nicht ohne den Einsatz komplexer Verfahren ausgespäht werden.

Im Gegensatz zur passiven Aufnahme von Körpermerkmalen wie dem Auge, der Hand oder Finger erfordert das Unterschreiben immer einen aktiven Vorgang. Authentifizierungsmethoden, die auf Körpermerkmalen basieren, wie z.B. dem Fingerabdruck, werden im Finanzbereich nur vereinzelt akzeptiert. Ihre Einführung ist zumeist komplex und erklärungsbedürftig. Dabei geht es häufig nicht um technische, sondern um kulturelle oder organisatorische Aspekte.

3.1 Rechtlicher Rahmen

Weder die Eröffnung eines Kontos noch die Autorisierung von Transaktionen erfordern per Gesetz Schriftform gemäß BGB §126a. Es handelt sich hierbei um so genannte „formfreie Vereinbarungen". Somit können, parallel zum PIN/TAN-Verfahren, grundsätzlich auch beweiskräftig digitalisierte eigenhändige Unterschriften die Authentizität und Integrität sicherstellen. Die Unterschrift wird dazu während des Schreibens in vergleichsfähiger Qualität digitalisiert und es wird ein Integritätswert für Dokument und Unterschrift gebildet. Dieser Integritätswert wird verschlüsselt im Dokument abgelegt. Die Unterschrift selbst kann mit einem Referenzwert bei der Ablage in das Dokument oder zu einem späteren Zeitpunkt verglichen

werden. Hierfür kommt im Prototyp eine Softwarelösung des Unternehmens Softpro zum Einsatz.

Die digitalisierte eigenhändige Signatur darf an dieser Stelle nicht mit der elektronischen Signatur gemäß den Richtlinien des Signaturgesetzes aus 2001 (SigG – siehe [SigG01], [SigV01], [SigÄ05] sowie [Euro99]) verwechselt werden. Im Signaturgesetz werden drei Formen von elektronischen Signaturen beschrieben. Diese werden mit "einfacher elektronischer Signatur", "fortgeschrittener elektronischer Signatur" sowie „qualifizierter elektronischer Signatur“ bezeichnet, wobei nur die letztgenannte Form aus juristischer Sicht zum Nachweis von Authentizität und Integrität in allen Anwendungsfällen zulässig ist. Die qualifizierte elektronische Signatur wird nochmals unterschieden in qualifizierte elektronische Signatur mit und ohne Anbieterakkreditierung. Der qualifizierten elektronischen Signatur mit Anbieterakkreditierung wird vom Gesetzgeber eine erhöhte Beweiskraft zugemessen, die in einer Umkehrung beim Anscheinsbeweis resultiert. Vereinfacht gesprochen kann sich der Empfänger eines Dokumentes mit qualifizierter elektronischer Signatur mit Anbieter-Akkreditierung zunächst auf dessen mutmaßliche Authentizität und Integrität berufen. Die Authentizität derartiger Signaturen wird nach heute gängiger Praxis durch eine Verbindung der personenbezogenen Faktoren Besitz (Smartcard) und Wissen (PIN) gewährleistet. Ihre Beweiskraft wäre jedoch ungleich höher, wenn zur Authentifizierung ein personengebundener Faktor wie die eigenhändige Unterschrift verwendet werden würde.

In einem Rechtsstreit wird der Beweis durch die physische Vorlage des Originaldokuments vor Gericht angetreten. Dies gilt nach § 371 der Zivilprozessordnung (ZPO) auch für elektronische Dokumente. Sofern ein elektronisches Dokument vorgelegt wird, ist grundsätzlich dessen Beweiswert in den Bereichen Authentizität und Integrität zu hinterfragen. Eine erhöhte Beweiskraft kann dem Dokument nur zugesprochen werden, wenn die in ihm enthaltenen Merkmale der Authentizität und Integrität einen nachvollziehbaren und wiederholbaren Prüfprozess ermöglichen [Geis03].

In [Hoer04] wird die Beweiskraft digitaler Versicherungsverträge analysiert, die durch die digitalisierte eigenhändige Unterschrift abgesichert wurden. Das Gutachten kommt zu dem Schluss, dass „das beschriebene Verfahren der handgeschriebenen elektronischen Unterschrift ein funktionsäquivalentes Surrogat zur herkömmlichen Unterschrift auf einem Papierdokument darstellt“ [Hoer04].

3.2 Aufnahme vergleichsfähiger Unterschriften

Um die Unterschrift eines Kunden zuverlässig und in der gewünschten Qualität zu erhalten, muss man ein Schreibtablett verwenden, welches entweder an den Rechner angeschlossen wird (Pen Pad) oder ein Teil des Rechners darstellt (Tablet PC). Die am Markt befindlichen Geräte erlauben die Digitalisierung der Unterschrift während des Schreibvorganges (z.B. [Klee05]). Diese können neben dem statischen Unterschriftenbild auch dynamische Merkmale des Schreibvorgangs ermitteln und dokumentieren. Wichtige Kriterien bei der Unterschriftsgewinnung stellen die folgenden qualitativen Aspekte dar:

- Auflösung der digitalisierten Unterschrift: Um charakteristische Details einer Unterschrift nicht zu verlieren, gilt es eine ausreichend hohe Auflösung bei der Digitalisierung zu wählen (der Erfahrungswert liegt bei rund 300 dpi).
- Optische Rückkopplung beim Schreiben: Der Mensch ist es gewohnt, sein Schriftbild während des Schreibvorgangs zu sehen. Eine Aufnahme mit einem Schreibtablett

muss sicherstellen, dass der Unterzeichner seine Unterschrift zeitnah und positionsgenau zu sehen bekommt.

- Analyse der Druckintensitäten: Ein wichtiges Merkmal bei der Analyse von Unterschriften ist die Auswertung der Druckintensitäten, die beim Unterschreiben auftreten. Das Aufnahmesystem muss diese Merkmale entsprechend messen können.

Weiterhin muss gewährleistet sein, dass sich ändernde Unterschriften von Kunden im System abgebildet werden können. Eine Unterschrift ist nicht statisch, sondern entwickelt sich über die Jahre mit ihrem Besitzer.

In diesem Bereich kommen Schwellenwert-basierte Verfahren zum Einsatz ([KlKL05a], [KlKL05b]). Mit ihrer Hilfe kann die Analyse verschiedener Merkmale, wie z.B. die Akzeptanz unberechtigter Personen (False Acceptance Rate) sowie die Ablehnung berechtigter Personen (False Rejection Rate) bzw. die Equal Error Rate, gesteuert werden ([ViSt03], [Viel04]).

3.3 Merkmale von Unterschriften

Eine Unterschrift besteht aus statischen und dynamischen Merkmalen [Schm99]. Hierunter fallen z.B. neben dem Bild der Unterschrift auch Beschleunigungs- und Drucksignale, die beim Schreiben ermittelt werden können. Ein Ansatz zur vollständigen Beschreibung einer Unterschrift ist in [HaSe95] zu finden.

Eine Unterschrift besteht meist aus mehreren Schriftzügen, wobei ein Schriftzug als ein ununterbrochener Kontakt des Stiftes mit der Schreibfläche definiert ist. Die Anfangs- und Endpunkte dieser Schriftzüge stellen charakteristische statische Merkmale einer Unterschrift dar. Sie können aus der Analyse einer einzigen Unterschrift wie auch aus dem Vergleich verschiedener Unterschriften gewonnen werden. Statische Merkmale lassen sich z.B. durch Häufigkeits- oder Korrelationsparameter beschreiben.

Ergänzend zu den statischen Merkmalen kann man bei der Beschreibung einer Unterschrift auf dynamische Merkmale zurückgreifen. Zu ihnen zählen unter anderem die Schreibgeschwindigkeit sowie die Variation des Schreibdrucks während des Schreibvorgangs [GeGH96]. Durch die Auswertung der dynamischen Merkmale kann sichergestellt werden, dass das Unterschriftsbild nicht nur identisch mit dem Original ist, sondern auch mit hoher Wahrscheinlichkeit durch dieselbe Person erstellt wurde.

4 Eigenhändige Unterschrift im Online-Banking

Im vorherigen Abschnitt wurden die Grundlagen für die Umsetzung der digitalisierten eigenhändigen Unterschrift im Online-Banking vorgestellt. Um den Beweis zu führen, dass dieses Konzept nicht nur theoretisch möglich, sondern auch mit der aktuellen Technik realisierbar ist, wurde am Multimedia Communications Lab der Technischen Universität Darmstadt in Zusammenarbeit mit dem E-Finance Lab sowie Softpro ein Prototyp einer solchen Lösung für eine fiktive Online-Bank implementiert.

4.1 Anforderungsanalyse und Entwurf

Vor der Implementierung des Prototyps wurden die verschiedenen Merkmale identifiziert, die innerhalb dieser Online-Bank durch das neuartige Autorisierungs- und Authentifizierungsver-

fahren unterstützt werden sollten. Hierfür wurden die Prozesse bestehender Online-Banking-Systeme auf die Verwendung des PIN/TAN-Verfahrens hin analysiert. Die identifizierten Prozesse sollen im nächsten Schritt durch die digitalisierte eigenhändige Unterschrift ersetzt werden. Die folgenden drei Prozesse wurden für eine prototypische Umsetzung ausgewählt:

- Login im Web Portal der Online-Bank
- Ausfüllen eines Überweisungsformulars mit darauf folgender Autorisierung der Überweisung
- Autorisierung der Veränderung von Personaldaten.

Die Umsetzung des Prototyps erfolgte unter Verwendung der Java-Technologie für Front- und Back-end. Das Web Portal wurde mit einem Apache Tomcat 5.5 Server realisiert. Die Daten der Kunden werden in einer MySQL-Datenbank verwaltet.

Die Unterschriftserkennung wurde mit der Java API des SignWARE SDK von Softpro implementiert. Das SDK erlaubt die Entwicklung von Anwendungen, die von Tablet PCs oder anderen Schrifterfassungsgeräten aufgenommenen Unterschriften erkennen und mit in einer Datenbank gespeicherten Referenzen vergleichen können.

Sowohl die Referenzen als auch die zu vergleichende (erfassende) Unterschrift haben nicht nur statische Information (das Bild), sondern auch dynamische Information über die Ausführung der Unterschrift. Innerhalb des SDK kann man auswählen, welcher Übereinstimmungsgrad (zwischen 1 und 100 Prozent) zwischen Referenz und zu vergleichender Unterschrift ausreichend ist, um den Benutzer zu authentifizieren. In unserem Prototyp wurde ein Übereinstimmungsgrad von 80 Prozent für beide Fälle (statisch und dynamisch) benutzt.

Die in diesem Beitrag beschriebene Version des Prototyps speichert und verwaltet die Referenz der jeweiligen Kundenunterschrift auf dem Server einer fiktiven Bank. Eine zukünftige Version des Systems soll als Speichermedium der persönlichen Referenz eine Smartcard verwenden. Diese Smartcard kann weiterhin als Speicher für einen privaten Schlüssel dienen, welcher durch die erfolgreiche Authentifizierung auf Basis der digitalisierten eigenhändigen Unterschrift freigeschaltet wird.

4.2 Beschreibung des Prototyps

Nach dem Aufruf unserer fiktiven Online-Bank (KOM Bank) findet der Benutzer eine zu anderen Online-Banken ähnliche Startseite. Nach Angabe des Benutzernamens kann man sich zwischen der Eingabe eines Passwort bzw. einer PIN (wie gewohnt) oder der Benutzung der digitalisierten eigenhändigen Unterschrift entscheiden. Hierfür existiert eine entsprechende Schaltflache („LoginSecure"), die ein separates Fenster öffnet, in welchem die Unterschrift über ein Schrifterfassungsgerät (in unserem Fall ein Tablet PC) erfasst werden kann (siehe Abbildung 1).

Nach Eingabe der Unterschrift und dem erfolgreichen Abgleich mit der gespeicherte Referenz wird der Benutzer auf eine neue Seite geführt, auf welcher die verschiedenen zur Verfügung stehenden Transaktionen ausgewählt werden können. Zur Auswahl stehen im Prototyp die Möglichkeit, sich den aktuellen Kontostand von Konten und Kreditkarten anzeigen zu lassen, eine Überweisung durchzuführen oder die gespeicherten persönlichen Informationen zu editieren. Für die letzten beiden Transaktionsformen kann man als Alternative zur TAN bei der Autorisierung die digitalisierte eigenhändige Unterschrift verwenden.

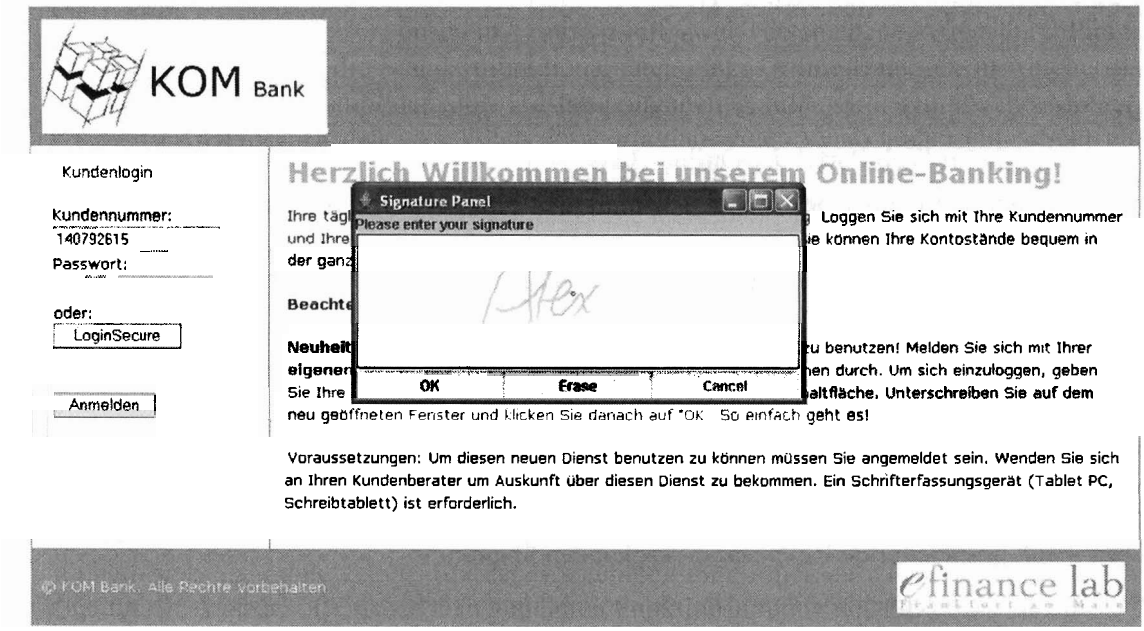

Abbildung 1: Anmeldung durch digitalisierte eigenhändige Unterschrift

Überweisungen lassen sich in unserem Prototyp auf zwei verschiedene Arten durchführen. Die erste Methode bildet die Standardfunktionalitäten einer Online-Bank ab, in welcher das Überweisungsformular traditionell über Tastatureingaben gefüllt wird. Die zweite Methode unterstützt das handschriftliche Ausfüllen des Formulars unter Verwendung eines Schrifterfassungsgeräts sowie Funktionen des Microsoft Tablet PC SDK. Unabhängig davon, wie das Überweisungsformular ausgefüllt wurde, bekommt der Kunde danach eine Seite angezeigt, auf welcher die eingegebenen Informationen bestätigt werden müssen. Zur Bestätigung kann wiederum eine TAN benutzt werden oder die digitalisierte eigenhändige Unterschrift. Auch in diesem Fall öffnet sich ein gesondertes Fenster, in welchem sich die Unterschrift erfassen lässt. Falls der Vergleich mit den Referenzen ein positives Ergebnis ergibt, werden die Daten in der Datenbank mit den neuen Werten aktualisiert. Die Änderung der Personaldaten sowie deren Bestätigung werden analog durchgeführt.

4.3 Sicherheitsanalyse des Prototyps

Die in den vorherigen beiden Abschnitten beschriebene Lösung wird nun einer Analyse ihrer Sicherheitsmerkmale unterzogen. Bei der Betrachtung unterscheiden wir (soweit angebracht) nach aktueller Ausbaustufe sowie dem geplanten Funktionsumfang des Prototyps.

Angriffe auf eine Online-Banking-Lösung können sowohl rein rechnergestützt als auch ohne Rechnerunterstützung durchgeführt werden. Wir haben die folgenden Szenarien als relevante Angriffsszenarien identifiziert, die es im Rahmen einer sicheren Online-Banking-Lösung zu beachten gibt:

> Man-in-the-Middle-Attacke: die Kommunikation eines Kunden mit seiner Bank wird durch einen Dritten auf Ebene des Netzwerks abgefangen und mitgelesen. Auf Basis der so erhaltenen Informationen können z.B. Transaktionen verändert und wieder in das Banksystem eingespielt werden. Weiterhin ist die Verwendung

der so erhaltenen Daten im Rahmen einer Replay-Attacke möglich, bei welcher die Daten zu einem erneuten Durchführen von Transaktionen gegenüber der Bank verwendet werden können, auch wenn der eigentliche Kunde in dem Moment nicht angemeldet ist.

- Phishing: Im Rahmen eines Phishing-Angriffs wird ein Benutzer im Online-Banking dazu gebracht, auf einem Server, der nicht zur Bank des Benutzers gehört, seine Authentifizierungsinformationen zu hinterlassen. Diese können dann von Dritten zur Durchführung eigener Transaktionen genutzt werden. Ausgangsbasis für diese Form des Angriffs sind zumeist gefälschte E-Mails, die von Dritten im angeblichen Auftrag der Bank an den Benutzer versendet werden.
- Trojaner: Trojaner, d.h. Schadprogrammen, die auf dem Rechner eines Opfers installiert werden, können die Authentifizierungs- und Autorisierungsinformationen eines Benutzers auf einem System mitschneiden und einem Dritten zur Verfügung stellen. Die Informationen können wiederum für unberechtigte Transaktionen eingesetzt werden.
- Social Hacking und weitere nicht rechnerbasierte Angriffsszenarien: in diese Kategorie von Angriffsszenarien fallen z.B. bei aktuellen Online-Banking-Lösungen das Erspähen von PIN oder der Diebstahl von TAN-Listen. Auch zählen hierzu z.B. das Ermitteln von Unterschriften und weiteren sensiblen Informationen durch die Durchsuchung von Abfällen, die Unterschriftensammlung an der Haustür oder der Beobachtung eines Opfers bei der Leistung seiner Unterschrift.

Grundsätzlich sollte eine Online-Banking-Lösung alle der identifizierten Bereiche hinreichend absichern. Die aktuelle Version des Prototyps bietet noch nicht für alle Angriffsszenarien einen ausreichenden Schutz. Der Prototyp wurde mit Hinblick auf den Bereich des Social Hackings und anderer nicht rechnerbasierter Angriffszenarien entwickelt. Der Vorteil einer Unterschrift ist hierbei die erhöhte Sensibilität des Benutzers bei der Leistung einer Unterschrift. Eine Unterschrift ist weniger abstrakt als eine PIN oder TAN und wird vom Benutzer bewusster geleistet. Die Digitalisierung der eigenen Unterschrift bei gleichzeitiger Messung von Merkmalen wie dem Druck oder der Geschwindigkeit beim Schreiben (auf Basis spezialisierter Hard- und Software) verhindert den einfachen Diebstahl der Unterschrift in vielen der vorher beschriebenen Szenarien.

Die Angriffsszenarien „Man-in-the-Middle-Attacke“ und „Phishing“ können in der vorliegenden Version unseres Prototyps nicht ohne Anpassungen des Systems ausgeschlossen werden. Sie basieren auf dem Sachverhalt, dass Online-Banking auf Interaktionen vernetzter Systeme basiert, welche über potentiell unsichere bzw. nicht vertrauenswürdige Netze geleitet werden. Die hieraus resultierenden Probleme können aber auf Basis der asymmetrischen Verschlüsselung gelöst werden [Ecke01]. Hierfür sollte ein zum SigG konformes Verfahren zum Einsatz kommen. Die Erweiterung unseres Prototyps sieht deshalb auch den Einsatz einer Smartcard vor, welche einen benutzerspezifischen privaten Schlüssel beinhaltet, der durch Leistung der Unterschrift aktiviert werden kann. Dieser Ansatz wird auch benötigt, um die TAN endgültig ablösen zu können. Der traditionelle TAN-Ansatz hat den Vorteil, dass eine TAN nur einmalig verwendbar ist. Die Kompromittierung einer einzelnen TAN zieht somit nicht automatisch die Kompromittierung der anderen TAN sowie der gesamten Bankverbindung mit sich, was durch die reine Leistung der Unterschrift noch der Fall wäre.

Auch die erweiterte Ausbaustufe des Prototyps, welche eine Smartcard sowie elektronische Signaturen einsetzt, kann das Problem der Trojaner, die auf dem Rechnersystem des Opfers installiert werden, nicht vollständig beheben. Um hier Sicherheit zu erreichen, müsste den Anwendern Hardware zur Verfügung gestellt werden, welche Unterschriftserkennung sowie Kartenlesen integrieren kann (beispielsweise vergleichbar mit den Kartenlesern Klasse 3 bei HBCI).

5 Fazit und Ausblick

Parallel zur Weiterentwicklung des Systems in Richtung Smartcard-Unterstützung und Einbindung der asymmetrischen Kryptografie ist in einem nächsten Schritt geplant, die Anwendbarkeit der hier beschriebenen prototypischen Implementierung mit Hilfe unserer Partner im E-Finance Lab zu evaluieren. Des Weiteren werden Szenarien zum Einsatz digitalisierter eigenhändiger Unterschriften im Front-Office-Bereich (z.B. Kontoeröffnung oder Freistellungsaufträge) der Banken untersucht, welche die Reduzierung von Medienbrüchen ermöglichen können. Sucht beispielsweise ein Kunde eine Bankfiliale auf, um dort ein neues Konto zu eröffnen, so werden seine persönlichen Daten vom Sachbearbeiter in das System eingegeben. Dann wird unter Berücksichtigung dieser Daten ein Ausdruck erstellt, auf dem der Kunde unterschreiben muss. Die Verwendung der digitalisierten eigenhändigen Unterschrift würde einen solchen Medienbruch vermeiden. Ziel ist hierbei die weitere Flexibilisierung und Optimierung der Geschäftsprozesse in Banken (z.B. [BHMS05], [BeMS04]). Im Zuge des Multi-Channel-Banking bietet eine Referenzhandschrift, auf die von mehreren Kanälen aus zugegriffen werden kann, ein zusätzliches Einsparpotential für die Banken (Abbildung 2). So kann beispielsweise die Unterschrift, die bei der Kontoeröffnung in der Filiale (PoS - Point-of-Sale) als Referenz angegeben wurde, später im Online-Banking oder am Geldautomaten (im Self-Service-Center) eingesetzt werden.

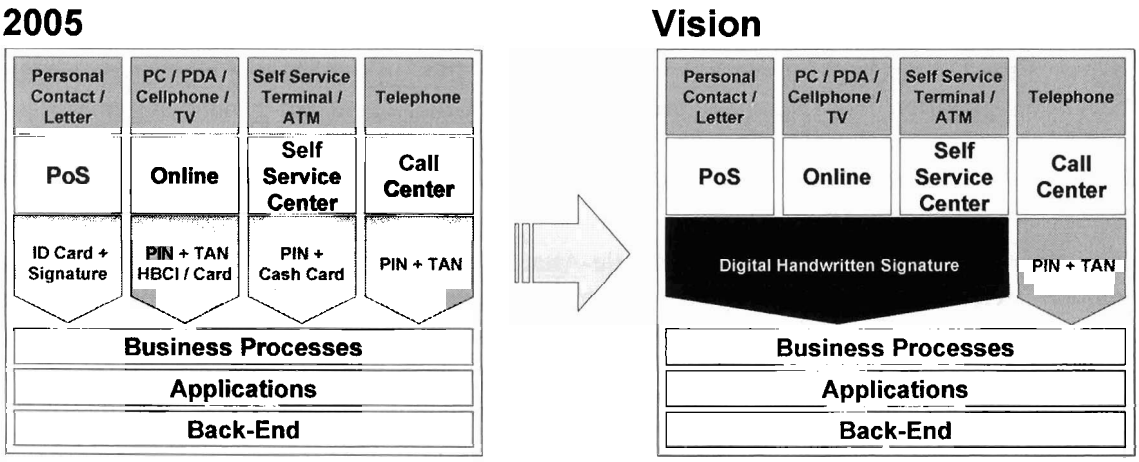

Abbildung 2: Multi-Channel-Integration mit Hilfe digitaler Unterschriften

Abschließend soll hier erwähnt werden, dass die hier beschriebene Lösung zwar ein erhöhtes Maß an Benutzerkomfort, eine hohe Benutzerakzeptanz und auch ein Plus an Sicherheit bietet, sowie helfen kann, Bankprozesse zu harmonisieren. Dies kann aber nur unter Einsatz spezieller Hardware für die Unterschriftserkennung sowie Chipkartenlesern erreicht werden, welche von der Bank oder den Kunden angeschafft werden muss.

Literatur

[Bach05] D. Bachfeld: Nepper, Schlepper, Bauernfänger - Risiken beim Online-Banking. In: c't Ausgabe 22, Heise-Verlag (2005) 148.

[BeMS04] R. Berbner, A. Mauthe, R. Steinmetz: Unterstützung dynamischer eFinance-Geschäftsprozesse. In: P. Horster: Elektronische Geschäftsprozesse 2004, syssec (2004) 44-54.

[BHMS05] R. Berbner, O. Heckmann, A. Mauthe, R. Steinmetz: Eine Dienstgüte unterstützende Web Service-Architektur für flexible Geschäftsprozesse. In: Wirtschaftsinformatik Ausgabe 4, Vieweg-Verlag (2005) 268-277.

[Deut04] Deutscher Sparkassen- und Giroverband: Sparkassen-Finanzgruppe führt fast jedes zweite Online-Konto in Deutschland. Pressemitteilung vom 6. Juli 2004.

[Ecke01] C. Eckert: IT-Sicherheit – Konzepte, Verfahren, Protokolle. Oldenbourg Verlag (2001).

[Euro99] Europäisches Parlament und Europäischer Rat: Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. In: Amtsblatt EG 2000 Nr. L 13 (1999) 12-20.

[Fies04] B. Fieseler: Die Marktverteilung jetzt gestalten. In: Die Sparkassenzeitung, Deutscher Sparkassen Verlag (2004) 13.

[Fina03] Finanztest: Sicherheit beim Online-Banking. In: Finanztest Ausgabe 9, Stiftung Warentest (2003) 24-27.

[GeGH96] A. van Gemmert, G. van Galen, H. Hardy: Dynamical features of disguised handwriting. In: Proceedings 5th European Conference for Police and Handwriting Experts (1996).

[Geis03] I. Geis: Recht und Praxis des elektronischen Geschäftsverkehrs. AWV-Verlag (2003).

[HaSe95] K. Han, I. Sethi: Signature identification via local association of features. In: Proceedings of the Third International Conference on Document Analysis and Recognition (1995) 187-190.

[Hoer04] T. Hoeren: Gutachten zur Rechtssicherheit bei der Verwendung von mittels Schreibtabletts eigenhändig unterzeichneten elektronischen Dokumenten für Versicherungsdienstleistungen (2004).

[Hurl03] J. Hurley: Passwords are gobbling up your profits. In: Ask the Analysts, Aberdeen Research (2003).

[Klee05] T. Kleemann: Beweiskräftige Patientenaufklärung mit dem Tablet PC und digitalen Unterschriften. In: 5. Schweizer eHealthCare Kongress, eHealthCare.ch (2005).

[KlKL05a] T. Kleemann, C. Kaplan, J. Lenz: Eigenhändige Unterschrift als elektronische Signatur. In: P. Horster: D-A-CH Security 2005, syssec (2005).

[KlKL05b] T. Kleemann, C. Kaplan, J. Lenz: Elektronisch signieren mit eigenhändiger Unterschrift – Erfahrungsbericht aus dem Klinikum Ingolstadt. In: 9. IT-Sicherheitskongress des BSI (2005).

[Mart04] A. Martin: TAN auf Tastendruck. In: Geldinstitute, Holzmann-Verlag (2004) 22ff.

[Schm99] C. Schmidt: Online Unterschriftenanalyse zur Benutzerverifikation. Dissertation, RWTH Aachen (1999).

[SigÄ05] Erstes Gesetz zur Änderung des Signaturgesetzes (2005), http://217.160.60.235/BGBL/bgbl1f/bgbl105s0002.pdf, abgerufen am 10.10.2005.

[SigG01] Signaturgesetz (2001), http://bundesrecht.juris.de/bundesrecht/sigg_2001/, abgerufen am 08.10.2005.

[SigV01] Signaturverordnung und Begründung zur Signaturverordnung (2001), http://www.iid.de/iukdg/aktuelles/verordnung_es.pdf, abgerufen am 08.10.2005.

[Skud05] H. Skudelny: Phishing und Pharming den Kampf ansagen. In: Bankmagazin Ausgabe 10, Gabler-Verlag (2005) 48f.

[Viel04] C. Vielhauer: Handwritten Biometrics for User Authentication. Dissertation, TU Darmstadt (2004).

[ViSt03] C. Vielhauer, R. Steinmetz: Handschriftliche biometrische Signaturen. In: P. Horster: D-A-CH Security 2003, syssec (2003) 344ff.

[vonS01] A. von Stülpnagel: Beyond HBCI - von der HBCI-Standardisierung zur Multi-Channel-Integration. In: Euroforum Konferenz (2001).

[WüHa02] G. Wübker, P. Hardock: Online Banking - Weit verbreitet, doch kaum genutzt?. In: Die Bank Ausgabe 6, Bank-Verlag (2002) 376-378.

[Zent05] Zentraler Kreditausschuss: FinTS – Standard für sicheres Online-Banking v4.0 (2004), http://www.hbci-zka.de/spec/4_0.htm, abgerufen am 12.10.2005.