TECHNISCHE UNIVERSITÄT ILMENAU

Sicheres Homebanking in Deutschland 2001

Ein Vergleich mit 1998 aus organisatorisch-technischer Sicht

Christiane Hänseroth, Angelika Zobel, Rüdiger Grimm

Nr. 5 **November 2001**

Diskussionsbeiträge

INSTITUT FÜR MEDIEN- UND KOMMUNIKATIONSWISSENSCHAFT

Sicheres Homebanking in Deutschland 2001

Ein Vergleich mit 1998 aus organisatorisch-technischer Sicht

Christiane Hänseroth, Angelika Zobel, Rüdiger Grimm

Diskussionsreihe des IfMK der TU Ilmenau, Nr. 5, Nov 2001

Diskussionsreihe des IfMK der TU Ilmenau
Herausgeber: der Rektor der Technischen Universität Ilmenau
Redaktion: Institut für Medien- und Kommunikationswissenschaft,
Prof. Dr. Rüdiger Grimm
ISSN 1617-9048

Inhaltsverzeichnis

Einleitung

Banken und Sicherheit gehören von jeher untrennbar zusammen. Denn Sicherheit ist die Grundlage einer vertrauensvollen Beziehung zwischen der Bank und ihren Kunden. Die Banken, als Inbegriff der Vertraulichkeit, stehen nun vor einer neuen Herausforderung: die bestehende Beziehung zu dem Kunden muss über einen neuen, noch unsicheren Übertragungsweg, dem Internet, aufrecht erhalten werden.

Wie wird in den verschiedenen Institutionen das Homebanking realisiert? Welcher Standard hat sich bei den befragten Banken, im Vergleich zur Ausgangsumfrage der Zeitschrift „Capital" aus dem Jahr 1998 (Grimm, Kahlen; 1999), durchgesetzt? Ist das „moderne HBCI" bereits als Standard durchgesetzt? Welche Entwicklungen gab es hierzu in der letzten zweieinhalb Jahren? Ist das Homebanking auf die Bedürfnisse des Kunden zugeschnitten? Hat die Servicebereitschaft der Banken zugenommen? Ist die Bank für einen hilfesuchenden Kunden jederzeit erreichbar? Ist das Bewusstsein der Banken für die Gefahren des Internetbanking inzwischen stärker ausgeprägt?

Die Beantwortung dieser Fragen beschreibt die sich weiterentwickelnde Situation der Sicherheitsstandards der Banken, d.h. im speziellen die technisch-organisatorischen Entwicklungen einiger wichtiger Banken. Ziel dieser Arbeit war es auch, die Veränderungen und Neuerungen der Nutzerfreundlichkeit der Homebankingangebote zu verdeutlichen. Dabei stand im Mittelpunkt der Betrachtungen, welche Korrekturen bezüglich Beweissicherheit, Storno (Rückrufmöglichkeit von Aufträgen), persönlicher Betreuung und Verfügbarkeit stattgefunden haben.

Diese Arbeit ist aus einer studentischen Projektarbeit im Fachgebiet Multimediale Anwendungen der TU Ilmenau Mai bis September 2001 entstanden. Für die Unterstützung der Arbeit bedanken wir uns herzlich bei den beteiligten Banken. Sie haben unsere Fragen beantwortet und uns so bei der Suche nach Antworten auf obenstehende Fragen maßgeblich vorangebracht. Ein besonderer Dank gilt Prof. Rüdiger Grimm und Silvia Hessel für die Betreuung und Anja Koch für die organisatorische Unterstützung der Projektarbeit. Ein weiterer Dank gilt Rudolf Kahlen für die Bereitstellung von Material aus der „Capital"-Recherche von 1998.

1. Homebanking

1.1 Was ist Homebanking?

Unter Homebanking versteht man eine von der Bank angebotene Dienstleistung, die es dem Bankkunden ermöglicht, verschiedene Bankgeschäfte wie z.B. die Abfrage des Kontostandes oder das Tätigen von Überweisungen von zu Hause aus zu erledigen. Die Banken bieten verschiedene Formen des Homebanking (vgl. Algesheimer 2000, 59). Im Verlauf dieser Arbeit wird Homebanking als Synonym für Internetbanking verwendet.

1.2 Vorteile von Homebanking

Ein wesentlicher Vorteil für die Bank ergibt sich durch die Einsparung von Personalkosten mit einer gleichzeitigen Vergrößerung des Angebotes von Dienstleistungen. Mit Homebanking kann der Bankkunde bequem vom zu Hause aus verschiedene Bankgeschäfte erledigen und muß nicht persönlich bei der Bank vorbeikommen um diese zu erledigen. Zudem erweitert die Bank ihr Dienstleistungsangebot indem sie ihre Leistungen rund um die Uhr und quasi von überall anbietet. So kann der Kunde per Internet weltweit auf sein Konto zugreifen und Bankgeschäfte erledigen, z.B. kann man während eines Auslandaufenthaltes überprüfen ob bestimmte Überweisungen schon ausgeführt wurden. Zudem ermöglicht Homebanking eine größere zeitliche Flexibilität bei Bankgeschäften (vgl. BMWI 2001).

1.3 Sicherheitsanforderungen an Homebanking

Das Internet ist ein unsicheres Medium. Die Daten werden als kleine Pakete über verschiedene Leitungen und Server vom Sender zum Empfänger geschickt. Der Transportweg liegt im Allgemeinen außerhalb der Kontrolle von Sender und Empfänger. Bei diesem Transport gibt es viele Punkte, an denen es möglich wäre die Daten abzufangen, zu lesen, oder gar manipuliert an den Empfänger weiter zu schicken.

Um Homebanking sicher über das Internet betreiben zu können, müssen folgende Voraussetzungen erfüllt sein: zunächst einmal *Vertraulichkeit*.

Die Bank und ihr Kunde müssen sichergehen, dass die Informationen, die sie austauschen, nur von ihnen selbst gelesen und geändert werden können. Um dies zu erreichen ist es erforderlich die Daten mit einem sicheren Verfahren zu verschlüsseln.

Eine weitere Anforderung ist die *Integrität* der Daten. Der Empfänger muß sichergehen, dass die Daten, die er vom Sender erhält, unverändert angekommen sind. Sie dürfen weder durch Übertragungsfehler noch durch Angreifer verändert worden sein.

Mindestens genau so wichtig wie die beiden vorangegangenen Punkte ist die *Authentizität*. Bei der Kommunikation zwischen Bank und Kunde muß die wahre Identität beider Partner immer bekannt sein. Es darf keinen Zweifel daran geben, wer miteinander kommuniziert. Außerdem sollten alle Vorgänge jeder Zeit beweisbar sein. Zur Verifikation von Integrität und Authentizität kann die digitale Signatur verwendet werden (vgl. Jung 2000,7).

Weiterhin gehört die zuverlässige *Verfügbarkeit* der Dienste zu den grundlegenden Sicherheitsanforderungen. Dafür müssen die Dienstanbieter genügend Ressourcen bereitstellen, unberechtigte Massenanfragen abwehren und Notfalldienste vorhalten. (Zu IT-Sicherheitsanforderungen vgl. z.B. CC 2000)

Da eine hundertprozentige technische Sicherheit nicht zu erreichen ist, muss Homebanking - wie jedes andere technische Verfahren – die Möglichkeit enthalten, dass die betroffenen und verantwortlichen Menschen persönlich eingreifen können. Diese Anforderung kann man der Nutzerfreundlichkeit zuordnen.

1.4 Homebanking und Nutzerfreundlichkeit

Das Tätigen von Bankgeschäften soll dem Kunden so einfach wie möglich gemacht werden. Dabei ist die Nutzerfreundlichkeit ein nicht zu vernachlässigender Aspekt. Die einfache und problemlose Abwicklung von Geschäften steht im Vordergrund des Homebankings. Eine geeignete, übersichtliche Nutzerführung wird durch eine eindeutige und klar strukturierte Menüführung erzielt. Die Leistungsfähigkeit und Geschwindigkeit der Dienste müssen den Anforderungen der Kunden angepasst sein. Das beginnt schon bei der Anmeldung und Freischaltung von Homebanking, bei denen unnötige Verzögerungen auf jeden Fall vermieden werden sollten.

Ein weiterer wichtiger Punkt ist die Erreichbarkeit der Bank über eine Hotline und nicht zuletzt auch deren Kompetenz. Möglichkeiten zur persönlichen Ansprache und zum persönlichen Eingriff dienen der Vertrauensbildung für Online-Dienste. Sie ergänzen die technischen Sicherheitsmechanismen. Die Anbieter vermitteln ihren Kunden, dass sie Verantwortung für ihre Dienste übernehmen, indem sie die Probleme der Kunden annehmen (Hotline) und für eventuelle Schäden haften.

1.5 Homebanking – Verfahren

1.5.1 PIN/TAN

Das bis jetzt am häufigsten verwendete Homebankingverfahren ist das PIN/TAN-Verfahren, welches gleichzeitig auch das älteste ist. Die Persönliche Identifikationsnummer (PIN) dient dem Bankkunden als elektronischer Ausweis. Diese PIN kennt nur er. Die üblicherweise fünfstellige alphanumerische Zahlenfolge ist von dem Kunden frei wählbar. Sobald man sich mit dieser Identifikationsnummer authentifiziert hat, kann man seine Bankgeschäfte vornehmen. Möchte man beispielsweise eine Überweisung tätigen, benötigt man eine zweite Nummer, die sogenannte Transaktionsnummer (TAN).

Die TAN dient als einmalige elektronische Unterschrift zur Autorisierung der Aufträge. Diese meist sechsstelligen Zahlen werden von der Bank generiert und dem Bankkunden per Post zugesandt. Die Bank vergleicht die vom Auftraggeber verwendeten Zahlenfolgen und streicht diese nach der Durchführung der einzelnen Aufträge. Eine zusätzliche Verschlüsselungskomponente, wie zum Beispiel RSA- Verschlüsselung dient der sicheren Übertragung über das Internet (vgl. E-magine 2001).

1.5.2 HBCI

Der Homebanking Computer Interface- Standard ist momentan die modernste Form des Datenaustausches in der Finanzdienstleistung und bietet einen Schutzwall für Transaktionen im Internet. Dieser Standard dient zur Kommunikation zwischen intelligenten Kundensystemen und entsprechenden Bankrechnern.

Der Datentransfer wird dabei über eine Netto-Datenschnittstelle[1] abgewickelt, die auf einer flexiblen Trennzeichensyntax[2] basiert. Das plattform- und endgeräteunabhängige Verfahren HBCI bietet dem Kunden ein hohes Maß an Flexibilität. Zusätzlich werden hohe Sicherheitsanforderungen durch moderne kryptographische Verschlüsselungsverfahren erfüllt. Diese Verschlüsselungen können über die Chipkarte oder über auf einer Diskette gespeicherten Informationen zur Verfügung gestellt werden, der bedeutende Fortschritt ist dabei das elektronische Signaturverfahren (vgl. Zierl, 1999). HBCI hat vor allem den Vorteil für den Kunden, dass hier eine Umkehr der Beweislast vorliegt. Die Bank muß im Streitfall die Beweise erbringen und nicht mehr der Kunde. Dies wird dadurch ermöglicht, dass Bank und Kunde die ausgetauschten Nachrichten signieren und aufbewahren.

1.5.3 OFX

Unter dem Namen "OFX - Open Financial Exchange" entwickelt ein Konsortium der Firmen „Checkfree“, „Intuit“ und „Microsoft“ seit 1997 eine Spezifikation für Finanzdienstleistungen im Internet. Die neueste Version 2.0.1 wurde im Juli 2001 veröffentlicht. Anders als HBCI beschränkt es sich nicht auf Homebanking, sondern schließt andere Anwendungen mit ein, wie die Übermittlung von Rechnungen, die Bearbeitung von Kreditkarten und den Börsenhandel (Brokerage).
OFX orientiert sich an der Internet-Architektur. Das drückt sich insbesondere in der Verwendung der Web-nahen Sprache XML und in einer schichtenorientierten Sicherheit aus. OFX unterscheidet zwischen Kanalsicherung (SSL) und Anwendungssicherung. Die unterste Stufe der Anwendungssicherung beruht im Wesentlichen auf PIN/TAN zwischen Client und Server. Im Übrigen ist OFX offen für die Integration weiterer Sicherheitsmodule a la HBCI (vgl. OFX, 2001).
OFX wird nach eigenen Angaben im September 2001 von über 1400 Banken unterstützt. Allerdings ist es fast ausschließlich auf den amerikanischen Markt be-

[1]Sorgt lediglich dafür, dass die für den Geschäftsvorfall benötigten Daten von beiden Kommunikationspartnern richtig interpretiert werden können (vgl. Jung 2000,5).
[2]Datenblöcke werden durch bestimmte Trennzeichen separiert; aus den verwendeten Trennzeichen ergibt sich die Art des folgenden Datenblockes. Neben einer hohen Flexibilität lässt sich mit einer Trennzeichensyntax das Datenvolumen minimieren, denn Daten werden nur in der tatsächlich erforderlichen Länge übertragen, nicht benötigte Felder können bei der Übertragung weggelassen werden (vgl. Haubner 1999,5).

schränkt. In Deutschland spielt OFX bisher keine Rolle und wird daher in dieser Arbeit nicht weiter berücksichtigt.

2. Fragebogenentwicklung

2.1 Theoretische Annäherung

Neben der Beobachtung und der Inhaltsanalyse zählt die Befragung zu den Grundtechniken der Datenerhebung (vgl. Porst 1998, 13). Als Standardinstrument der empirischen Sozialforschung dient sie der Ermittlung von Fakten, Wissen, Einstellungen, Meinungen oder Bewertungen. Befragungen können schriftlich, mündlich oder telefonisch durchgeführt werden (vgl. Schnell 1999, 297).

Von einer schriftlichen Befragung spricht man, wenn Fragebögen in Anwesenheit eines Interviewers ausgefüllt werden oder Fragebögen an Befragte postalisch versandt werden, mit der Bitte, diese Fragebögen auszufüllen und an die Forschungsgruppe zurückzusenden („Mail Survey"). Hierbei ist entsprechend kein Interviewer anwesend. Deshalb erfordert die Konstruktion eines Fragebogens für eine postalische Befragung mehr Sorgfalt als bei jedem anderen Fragebogen, da der Befragte, ohne die Hilfe eines Interviewers, mit den Fragen allein gelassen wird (vgl. Schnell 1999, 335). Die Fragen sollten kurz, einfach, wertneutral, ausgewogen und eindeutig formuliert sein (vgl. Ikarus, Universität Dortmund 2001).

Bei einer Erhebung geht man in 3 Schritten vor. Zuerst wird der Fragebogen durch eine Literaturanalyse vorbereitet. Wichtige Begriffe müssen definiert werden, um im folgenden die Hypothesen aufstellen zu können (vgl. Kapitel 3.2). Im zweiten Schritt schließt sich die Befragung an, die Operationalisierung beinhaltet, d.h. die Variablen werden zueinander in Beziehung gesetzt und als Fragen formuliert (vgl. Kapitel 3.3 und 4). Als letzter Schritt erfolgt die Auswertung mit statistischen Auswertungsverfahren, hier zu finden in den Kapiteln 5 und 6 (vgl. Kromrey 1991, 276).

2.2 Analyse des Ausgangsfragebogens

Die erste Umfrage „Homebanking im Test" wurde 1998 von der Zeitschrift „Capital" (vgl. Grimm 1999, 138) verwirklicht. Getestet wurden 32 deutsche Banken, die nach Bekanntheitsgrad und Wichtigkeit ausgewählt wurden. Geprüft wurden

die Banken hierbei auf die Kriterien Wertpapierhandel, Zahlungsverkehr, Baufinanzierung und Nutzerfreundlichkeit. Das Merkmal der Nutzerfreundlichkeit umfasste die Unterkriterien Nutzerführung, Kommunikation, Sicherheit und Recht. Diese Unterkriterien wurden jeweils mit Schulnoten bewertet. Nach der jeweiligen Gewichtung der einzelnen Gebiete (Sicherheit ging zu 25% in die Bewertung ein) wurde eine Gesamtnote errechnet. Daraus ergab sich ein Ranking der Banken.
Die Grundlage dieser Arbeit bildete der Fragebogen zum Thema Sicherheit von Prof. Dr. Rüdiger Grimm, damals tätig im GMD- Forschungszentrum Informationstechnik. Ausgehend von der vorgegebenen Aufgabenstellung, den Sicherheitsaspekt, eingebettet in die Nutzerfreundlichkeit zu betrachten, wurde der „Capital-Fragebogen" überarbeitet.
Die Bereiche Funktionalität, Ausstattung, Versorgung und Verfügbarkeit wurden dementsprechend erweitert, um den Service der Banken zu überprüfen. Fragen, die in der ersten Befragung Mängel bei den Banken aufgedeckt hatten, wie z.B. im Gebiet des Storno, wurden ausführlicher betrachtet, um die Themen tiefgründiger zu bearbeiten. Teilweise war somit eine neue thematische Gliederung des Fragebogens nötig und auch eine neue Zuordnung verschiedener Fragen. Weiterhin wurde der Fragebogen an die aktuellen technischen Gegebenheiten angepasst, um den Entwicklungen im Bereich des Zahlungsverkehrs gerecht zu werden. Dies betraf z.B. die spezielle Hardware-Unterstützung für die Sicherheit. Ein Ranking bzw. eine Bewertung der einzelnen Banken ist in dieser Arbeit nicht vorgesehen.

2.3 Entwicklung des neuen Fragebogens

2.3.1 Kategorien

Wie bereits im vorhergehenden Abschnitt erwähnt, wurden die einzelnen Kategorien des Fragebogens überarbeitet. Durch die Korrektur der Zuordnung einiger Fragen wurde eine Kategorie überflüssig.
Andere Teile wurden in bestehende Kategorien aufgelöst oder in der Reihenfolge vertauscht, um die logische Folge der Fragen nicht zu unterbrechen. Damit ergab sich eine klarere Strukturierung des Fragebogens.
Die Kategorien 1 „Funktionalität, Ausstattung, Versorgung", 2 „Identifizierung und Kommunikationsintegrität" und 3 „Vertraulichkeit" wurden unverändert bei-

behalten. Auch die bisherige Reihenfolge wurde nicht geändert, da die Fragen aufeinander aufbauten. Die Kategorie 4 „Verantwortlichkeit und Haftung“ wurde vorgezogen (zuvor Kategorie 6), da sich die Fragen thematisch an die vorhergehende Kategorie anschlossen. Kategorie 5 „Persönliche Betreuung“ entstand aus der alten Kategorie 4 „Verfügbarkeit“. Die Umbenennung wurde erforderlich, da die Kategorie thematisch erweitert wurde. Die alte Kategorie 5 „Information und Beweise“ entfiel, da die Fragen, die hier enthalten waren, in den anderen Kategorien treffender zugeordnet werden konnten.

Im Kopf des Fragebogens wurden zum betreffenden Geldinstitut, dem Ansprechpartner und seiner Telefonnummer für Rückfragen noch ein weiterer Kontakt (E-Mail), die Abteilung und der Tätigkeitsbereich der ausfüllenden Person zugefügt. Dies war notwendig, um die Kompetenz des Ansprechpartners feststellen zu können. Die Änderungen in den einzelnen Kategorien werden im folgenden näher erläutert.

2.3.2 Funktionalität, Ausstattung, Versorgung

Die Fragen des ersten Punktes sollten klären, welche Grundvoraussetzungen sowohl der Bankkunde als auch die Bank selbst für das Homebanking erfüllen müssen.

Frage 1 „Welche Produkte (Software/Hardware) werden von Ihnen eingesetzt?“ wurde unverändert übernommen. Die folgende Frage „Was benötigt der Kunde?“ wurde vorgezogen (alte Frage 8), da sie die Zugangsvoraussetzungen beim Client abfragte und sich logisch an Frage 1 anschloss. Eine Antwortvorgabe wurde von „Modem-Anschluss“ auf „Analog-Anschluss“ berichtigt.

Frage 3 „Welche Zugangsmöglichkeiten bieten Sie an?“ entstand aus der zweiten Frage im alten Fragebogen. Die verschiedenen Zugangssysteme bieten dem Kunden unterschiedliche Software, Anwendungsmöglichkeiten und auch Sicherheitsstandards.

Diese Frage sollte Klarheit schaffen, welche Systeme von den Banken angeboten und damit als sicher bewertet werden. Ebenfalls wurden die Antwortvorgaben überarbeitet. „Direkte Telefonleitung“ wurde als Möglichkeit entfernt, da dies eher auf Telefonbanking abzielte und somit irreführend war. Frage 3 in der glei-

chen Kategorie des alten Fragebogens wurde mit diesen Korrekturen überflüssig und entfiel.

Frage 4 „Wie viel Prozent aller Ihrer Kunden nutzen die Möglichkeit des Homebanking?“ unseres Fragebogens wurde neu eingefügt um die Akzeptanz des Homebanking bei den Kunden in Erfahrung zu bringen.

Frage 5, ebenfalls neu, „Wie informieren Sie Ihre Kunden über die Sicherheitsstandards des Homebanking?“ zielte auf die Informationspolitik der Banken. Eine zu geringe Information seitens der Bank lässt eventuell auch Rückschlüsse über geringe Akzeptanz des Homebanking zu.

Frage 6, „Welche Standards bieten sie an?“, ging aus der Frage 5 „Welcher Standart wurde gewählt?“ des alten Fragebogens hervor. Diese Umformulierung war zweckmäßig, da die Banken ihren Kunden mittlerweile verschiedene Standards, meist HBCI und PIN/TAN, anbieten. Die Frage wurde darüber hinaus noch erweitert, um in Erfahrung zu bringen, seit wann HBCI eingesetzt wird und falls es nicht angeboten wird, warum nicht, bzw. ab wann der Einsatz geplant ist. HBCI ist in Deutschland als Standard für Homebanking vorgesehen. Bei der ersten Umfrage 1998 war dies allerdings noch nicht umgesetzt. Deshalb sollte mit dieser Frage geklärt werden, ob dieser Standard mittlerweile implementiert ist. Aufgrund der Umformulierung dieser Frage entfiel die Frage 6 der zweiten Kategorie im alten Fragebogen.

Frage 7 im neuen Fragebogen diente dazu, die Verteilung der Homebanking-Nutzer auf die verschiedenen Verfahren zu bestimmen. Nutzen die Kunden lieber das ihnen vertraute PIN/TAN- Verfahren oder das sicherere HBCI- Verfahren? Damit sollte erfasst werden ob der Standard auch seitens der Kunden akzeptiert wird. Die Frage ergab sich als Folge der Erweiterung der vorhergehenden Frage und wurde neu eingesetzt.

Frage 8 „Welche Geschäftsvorfälle kann der Kunde bei Ihnen online abwickeln?“ leitete sich aus den Fragen 4 und 6 des alten Fragebogens ab, die erweitert und nach 3 möglichen Antwortvorgaben (HBCI, PIN/TAN, bankspezifische Lösung) aufgeschlüsselt wurden. Entsprechend des HBCI- Standards 2.2 (vgl. Bundesverband deutscher Banken e.V. 2000, 195) wurden die einzelnen Geschäftsvorfälle, die mit HBCI zu verwirklichen sind, als Antwortvorgaben aufgeführt. Damit soll-

te überprüft werden, in welchen Maße die in Frage 6 angegebene Version implementiert wurde.

Frage 9 „Bieten Sie Ihren Kunden eine spezielle Hardware- Unterstützung für die Sicherheit bei Homebanking?“ war eine Überarbeitung der Frage 7 im alten Fragebogen. Sie wurde an die aktuellen Entwicklungen im Bereich der Sicherheitstechnik angepasst. So entfielen Me- und Mondex- Chip. Beibehalten wurden die DES- Karte und die Signaturkarte, die Verschlüsselungsalgorithmen RSA und DSA wurden eingefügt, ebenso Bankkundenkarte und Spezieller Chip. Diese Frage sollte das Sicherheitsinteresse der Bank überprüfen. Inwieweit bietet die Bank dem Kunden zusätzliche Sicherheitsmaßnahmen an?

2.3.3 Identifizierung und Kommunikationsintegrität

Beweisbarkeit war bei der ersten Befragung als zentrales Problem herausgestellt worden. Mit den nachfolgenden Fragen sollte analysiert werden, ob sich in den vergangenen zwei Jahren entscheidende Neuerungen/Änderungen ergeben haben. Im speziellen wird die Beweisbarkeit nach außen betrachtet. Das PIN/TAN- Verfahren dient, da PIN und TAN Bank und Kunden bekannt sind, lediglich zur inneren Beweissicherheit, aber nicht gegenüber Dritten. Bei HBCI hingegen ist jeder Schritt signiert und somit auch beweisbar. Die Fragen zielten ebenfalls auf Identifizierung der Beteiligten ab.

Frage 1 „Wie kann die Authentizität des Kunden bewiesen werden?“ war eine Überarbeitung der gleich positionierten Frage des alten Fragebogens. Die Antwortvorgaben wurden angefügt.

Frage 2 „Wie identifiziert sich der Bankserver gegenüber dem Kunden?“ des alten Fragebogens wurde erweitert um den Teil „Welche kryptographischen Verfahren und zugehörige Schlüssellängen werden eingesetzt?“ und um Antwortvorgaben. Diese Überarbeitung führte die Frage in Richtung Kryptographie und Verschlüsselung. Die Position wurde ebenfalls beibehalten, da diese Fragen logisch aufeinander aufbauten.

Im folgenden wurde eine neue, thematisch passende Frage eingefügt, um den Sicherheitsaspekt zu vertiefen: Frage 3, „In welchen Abständen wird die Identifizierung erneuert?“. Kann der Client also seinen Computer kurze Zeit unbeaufsichtigt

lassen, während er Bankgeschäfte online tätigt, ohne das eine Gefahr von Missbrauch durch Dritte entsteht?

Frage 4 „Wie prüft der Bank- Server die Berechtigung des einzelnen Auftrags?“ wurde aus dem alten Fragebogen übernommen. Ergänzt wurden lediglich die Aufteilung der Antwortmöglichkeiten nach HBCI, PIN/TAN und bankspezifischer Lösung.

Die Fragen 5 „Wie prüft die Bank, das der Auftrag unverletzt angekommen ist?“ und 6 „Wie prüft der Kunde, das der Auftrag angenommen wurde?“ sind aus der Frage 4 „Wie prüfen Bank bzw. Kunde, das Auftrag bzw. seine Erledigung unverletzt angekommen ist?“ des alten Fragebogens hervorgegangen. Eine Differenzierung war hier sinnvoll, um genauere Antworten zu erhalten. Erkennt die Bank Veränderungen des Auftrages durch Dritte? Können Daten auf Unverfälschtheit überprüft werden? Wird auch diese Sicherheitslücke von der Bank beachtet?

Die Fragen 7 „Erhält der Kunde eine digitale Quittung seines Auftrages?“ und 8 „Ist sie signiert?“ sind von der Frage 2 „Sind Quittungen beweissicher, z.B. mit Hilfe einer digitalen Signatur?“ der Kategorie 5 des alten Fragebogens abgeleitet worden. Diese Zuordnung erschien thematisch sinnvoller. In der siebten Frage wurde zusätzlich eine Filterführung zu Frage 9 eingebaut, um die Beantwortung zu erleichtern.

Frage 9 wurde neu eingefügt, um die Frage der Beweislast im Fall von Unstimmigkeiten zu klären. Um diesen Sicherheitsaspekt zu vertiefen, folgte Frage 10, „Was gilt als Beweis?“.

Die letzte Frage dieser Kategorie „Wie schützen Sie sich und Ihre Kunden vor Maskeraden?“ zielte ab auf das Bewusstsein das die Banken für die Gefahren der Kommunikation über das Internet entwickelt haben sollten.

Frage 5 „Wird eine digitale Signatur eingesetzt?“ im alten Fragebogen entfiel, da sie zu unspezifisch war.

2.3.4 Vertraulichkeit

Vertraulichkeit zwischen Kunden und Bank bei Bankgeschäften und im speziellen bei Homebanking ist unerlässlich. Von Interesse ist hier vor allem, welche Mittel eingesetzt werden, um dieses Vertrauen noch weiter zu stärken.

Frage 1 „Wird die Kommunikation zwischen Client und Server verschlüsselt?“ wurde aus dem alten Fragebogen übernommen und lediglich um eine Filterführung zu Frage 4 ergänzt. Frage 2 „Welche Verfahren?“ schließt sich logisch an und wurde deshalb vorgezogen (ehemals Frage 3 im alten Fragebogen). Ebenfalls wurden die Antwortvorgaben ergänzt. Um die Thematik noch zu vertiefen, wurde eine neue Frage eingefügt, „Welche Kommunikationsteile werden verschlüsselt?“.
In der sich anschließenden Frage 4 „Wer generiert Ihre Bankschlüssel?“ wurden die Fragen 3 „Wer generiert Bankschlüssel?“ der gleichen Kategorie und die Frage 7 „Welches Zertifizierungsmanagement?“ der Kategorie 2 zusammengefasst. Die Frage entsprach thematisch der Zuordnung in der Kategorie „Vertraulichkeit“.
Um das Thema auch aus Kundensicht zu behandeln, wurde eine neue Frage eingefügt: „Wer generiert die Kundenschlüssel?“.
Die Frage 2 des alten Fragebogens „Welche anderen Verfahren werden eingesetzt, um die Kommunikation vor unberechtigten Lauschern zu schützen?“ wurde weggelassen, da sie zu unspezifisch war. Ebenfalls entfiel ein Teil der Frage 3 „Welche Schlüssel werden wiederverwendet, welche Schlüssel sind einmalig?“, da die Beantwortung dieser Frage nicht im zentralen Feld unserer Betachtungen stand.

2.3.5 Verantwortlichkeit und Haftung

Serviceleistungen der Banken bei Störfällen und Problemen sind in diesem Abschnitt das zentrale Thema. Welche Möglichkeiten hat der Kunde und wie hilft ihm die Bank dabei?
Frage 1 „Bekommt der Kunde eine Übersicht über die ausgeführten Aufträge?“ entstand aus der Überarbeitung von Frage 1 „Bekommt der Kunde eine Orientierung seiner Aufträge?“ der Kategorie 5 des alten Fragebogens.
Frage 2 „Wie reagiert das Homebanking- System bei Unterbrechungen, wie z.B. bei Systemausfall oder Verbindungsabbruch?“ wurde aus der Kategorie 4 des alten Fragebogens ausgegliedert und überarbeitet, da sie ein zentraler Bestandteil des Themas Haftung darstellt.
Antwortvorgaben wurden eingefügt, um die Frage in den Kontext der Verantwortlichkeit einzubinden. Frage 3, eine Überarbeitung der ehemals dritten Frage der Kategorie 4 des alten Fragebogens, erweiterte das Themenfeld noch: „Erfährt der Kunde verbindlich, was bei einer solchen Unterbrechung ausgeführt worden

ist und was noch nicht?“. Die Frage wurde ergänzt durch eine Filterführung zur Frage 5, da sich die folgende Frage 4 ebenfalls noch mit der Thematik der Auftragsausführung beschäftigte. Frage 4 „Wie stellen Sie sicher, das in solchen Fällen Aufträge nicht doppelt durchgeführt werden?“ wurde neu eingefügt, um den Gegenstand umfassend zu beleuchten.
Die nun folgende Frage 5 „Wie gehen Sie mit Vertippen oder Verklicken seitens des Kunden um?“ leitet zum Teil der Stornierung hin, der sich in der ersten Umfrage als zentrales Problemfeld ergeben hatte. Dieser Teil wurde deshalb im Fragebogen stark erweitert, d. h. es wurden neue Fragen eingefügt, die Frage 7 „Welche Möglichkeiten der Stornierung räumt die Bank dem Kunden hierbei ein?“, die Frage 8 „Gibt es Vorgänge, die online vom Kunden selbst nicht storniert werden können?“ ‚die Frage 9 „Welche Vorgänge können vom Kunden selbst nicht storniert werden? (Begründung!)“ und 10 „Welche Fristen sind bei der Stornierung zu beachten?“. Die Frage 6 „Hat der Kunde die Möglichkeit einen Auftrag online zu stornieren (wie z.B. bei Lastschriftverfahren)?“ ist eine Überarbeitung der Frage 3 der gleichen Kategorie.

2.3.6 Persönliche Betreuung

Dieser Punkt setzte sich mit den persönlichen Serviceleistungen der Banken auseinander. Ist die Bank täglich 24 Stunden für den Kunden erreichbar?
Frage 1 „In welchen Zeitabständen werden die Kundenaufträge bearbeitet?“ wurde neu eingefügt, da sie auf ein interessantes Thema abzielt. Werden die Kundenaufträge genauso schnell bearbeitet, wie sie eingehen? Dies ist vor allem bei Wertpapiergeschäften von zentraler Bedeutung. Deshalb wurden in der Antwortvorgabe Taktzeiten eingefügt, so das zwischen Wochentagen und Wochenende und ebenfalls zwischen Geschäftszeiten und Zeiten, in denen die Bank geschlossen ist, unterschieden werden kann.

Die nächsten beiden Fragen behandelten die persönliche Beratung der Kunden durch die Bank, die auch in Zeiten des Homebanking noch nicht überflüssig geworden ist. Frage 2 „Hat der Kunde einen persönlichen Ansprechpartner bei der Bank?“ war eine Überarbeitung der Frage 1 der Kategorie 6 des alten Fragebogens. „Persönlich“ wurde eingefügt, um die Frage eindeutiger zu formulieren. Neu

eingefügt wurde hier die Frage 3 „Wann wird der Bankberater dem Kunden mitgeteilt?“, da sie eine sinnvolle Ergänzung darstellte.
Die letzten Fragen befassten sich mit dem Thema der Hotline, die eine zentrale Rolle bei der Kundenbetreuung einnimmt. Ist eine Soforthilfe rund um die Uhr gewährleistet? Zuerst war die Frage zu klären, ob die Bank über eine entsprechende Einrichtung verfügt: Frage 4 „Gibt es eine Hotline?“. Diese Frage wurde aus dem alten Fragebogen, Frage 1 aus der Kategorie 6, übernommen. Weiterhin interessant um die Serviceleistungen der Banken beurteilen zu können, war die Frage, ob die Hotline für den Kunden kostenpflichtig ist (Frage 5). Sie wurde deshalb neu eingearbeitet.
Wichtig ist auch die Verfügbarkeit der Hotline: Frage 6, „24 Stunden in Betrieb?“. Sie wurde ebenfalls aus der Kategorie 6, ehemals Frage 2, übernommen, da diese Fragen den Service der Bank beleuchteten und nicht die Haftung. Die Fragen 7 „Wie viele Anschlüsse stehen gleichzeitig zur Verfügung?“ und 8 „Wie viele Anrufe erhält die Hotline durchschnittlich im Monat?“ waren notwendig, um eine Auslastung der Hotline pro Anschluss zu beurteilen. Frage 7 war eine Überarbeitung der Frage 2 der Kategorie 6 des alten Fragebogens. Frage 8 wurde neu erstellt.
Frage 1 der Kategorie 4 des alten Fragebogens „Wie oft/wie lange hat es Systemausfälle und Systemunterbrechungen gegeben?“ wurde gestrichen, da hier keine validen Antworten zu erwarten gewesen wären.
Der Raum für zusätzliche Anmerkungen der ausfüllenden Person wurde beibehalten, um eventuell weiteres Feedback zu erhalten.

3. Projektverlauf

3.1 Auswahl der Banken

Da es sich bei dieser Arbeit um eine Anschlussumfrage handelt, sollten die damals beteiligten Unternehmen erneut integriert werden. 1998 wurden 32 deutsche Banken, die nach Bekanntheitsgrad und Wichtigkeit ausgewählt wurden, befragt. Bei diesem Projekt wurde allerdings mit einer Stichprobe von nur 31 Banken gearbeitet, da die Frankfurter Sparkasse und die Frankfurter Sparkasse 1822 direkt als ein Unternehmen angesehen wurde. Bei den 31 Banken handelte es sich um folgende

Unternehmen: Advance Bank, Allgemeine Direktbank, Apotheker- und Ärztebank, Augsburger Aktienbank, Badische Beamtenbank, Bank 24, Bank Girotel, Citibank, Comdirekt, Commerzbank Frankfurt, Consors, Deutsche Bank Frankfurt, Direkt Anlage Bank, Dresdner Bank, Entrium, Fimatex, Frankfurter Sparkasse, Hypo/Vereinsbank, Nassauische Sparkasse Frankfurt, Norisbank Frankfurt, Postbank, SEB Bank, Spardabank Hamburg, Spardabank Köln, Sparkasse Norden, Stadtsparkasse Magdeburg, Stadtsparkasse München, Vereins- und Westbank Hamburg, Volksbank Mainz und Volksbank Leipzig.

Zu Beginn des Projektes war geplant, neben den 32 durch die Zeitschrift „Capital" befragten Banken, auch neue Banken in die Befragung einzubeziehen. Jedoch wurde festgestellt, dass bereits bei der damaligen Umfrage alle bekannten Bankinstitute aufgenommen wurden. Eine sinnvolle Stichprobenziehung weiterer Banken war auf dieser Basis somit nicht möglich. Eine Erweiterung der Bankenliste würde das Ergebnis verfälschen und unbrauchbar machen. Aus diesem Grund wurde die Erhebung lediglich an den oben erwähnten Institutionen durchgeführt.

Da es hier nicht um eine Beurteilung einzelner Banken, sondern um eine Beschreibung des Verhaltens deutscher Banken im Allgemeinen geht, wobei leider nur eine kleine Anzahl wichtiger Banken zur Verfügung stand, wurde die Auswertung anonymisiert. Eine Benennung der Banken war nicht erforderlich, da diese Arbeit nicht auf ein Ranking abzielt. Im nachfolgenden Teil wurden die befragten Banken mit Nummern versehen. Die Nummernvergabe erfolgte nicht in der hier aufgeführten Reihenfolge.

3.2 Recherche der Telefonnummern

Ausgangspunkt der Recherche war eine Adressliste der Zeitschrift „Capital", die freundlicherweise von Herrn Kahlen, Redakteur bei „Capital", für dieses Projekt zur Verfügung gestellt wurde. Diese Liste enthielt die Namen der damals befragten Banken und teilweise bereits Telefonnummern der Geschäftsstellen. Die noch fehlenden Nummern wurden den Homepages der einzelnen Unternehmen entnommen.

Größere Probleme bei der Suche nach einer Kontaktnummer traten bei Bank 8 auf. Eine Kontaktaufnahme war offensichtlich nur per e-Mail möglich, was in diesem Fall allerdings nicht weitergeholfen hätte. Erst nach intensiver Suche konnte

die Nummer einer Hotline für Homebankingkunden gefunden werden. Die Telefonnummer der Geschäftszentrale war nicht auf den Internetseiten vorhanden.

3.3 Kontaktaufnahme mit den Banken

3.3.1 Telefonrecherche nach Ansprechpartnern

Der größte Teil der vorliegenden Telefonnummern waren Telefonzentralen und Hotlines der Unternehmen. Die erste Telefonaktion wurde am Donnerstag, dem 14.06.2001 von 9.00 bis 12.30 Uhr durchgeführt. Dieser Zeitpunkt wurde gewählt, um möglichst viele Banken während ihrer Geschäftszeiten zu erreichen. Allerdings gelang dies nur bei 19 von 31 Instituten. Deshalb wurde ein zweiter Termin am Montag, dem 18.06.2001 zur gleichen Zeit, angesetzt. Ziel dieser ersten Telefonrecherche war es einen kompetenten Ansprechpartner zu finden, der sich bereit erklärte den Fragebogen entgegenzunehmen und zu bearbeiten.

Die Suche nach dieser Person erwies sich bei fast allen Banken als sehr schwierig, meist mussten mehrere Abteilungen durchlaufen werden, bevor sich ein Mitarbeiter angesprochen fühlte. Häufig wurde man von den Zentralen an die Hotline weitergeleitet, sobald das Wort Homebanking fiel. Die Hotlines konnte jedoch am wenigsten weiterhelfen, da sie lediglich für Kunden mit technischen Fragen und Problemen zuständig waren. Bereits bei dieser Aktion wurde festgestellt, dass nicht alle Banken rund um die Uhr erreichbar sind, z.B. ist die Hotline der Bank 14 nur Montag bis Freitag von 11.00-19.00 Uhr besetzt.

Die Hotlines waren meist mit Telefonansagen zur Überbrückung der Wartezeit ausgestattet. Bei Bank 5 und 26 wurde über ein Tastenmenü die Verbindung zur zuständigen Hotline hergestellt. Am schnellsten fanden sich Ansprechpartner in den Presseabteilungen, die den Fragebogen gern in Empfang nahmen und für dessen Bearbeitung bzw. Weiterleitung an die zuständigen Stellen sorgten. Allerdings wurde bei Bank 25 deutlich, dass deren Pressestelle sehr schwierig zu erreichen war, entweder war niemand unter dieser Telefonnummer zu erreichen oder die Leitung war besetzt. Erst nach mehreren Versuchen gelang es einen Bankangestellten zu sprechen.

Die Freundlichkeit und Hilfsbereitschaft in den Zentralen und Hotlines war bei fast allen Banken sehr angenehm, mit Ausnahme der Bank 20, wo man lediglich

mit dem Hinweis „Wir bearbeiten nur schriftliche Anfragen." abgewiesen wurde. Es war weder möglich die zuständige Abteilung noch einen Ansprechpartner zu erfahren. Nur die Postadresse wurde mitgeteilt.

3.3.2 Versenden der Fragebögen

Durch die einzelnen Telefonate wurde, mit Ausnahme von Bank 20, in jeder Institution ein kompetenter Ansprechpartner gefunden, der den Fragebogen entgegen nahm. Am 14.Juni und am 18.Juni, jeweils direkt nach den Telefonaktionen, wurden der sechsseitige Fragebogen zusammen mit dem Anschreiben und einem offiziellen Schreiben von Herrn Prof. Dr. Grimm an 31 Unternehmen versendet. 20 der Banken bzw. Bankangestellten erhielten den Fragebogen per e-Mail, 10 Unternehmen per Fax und zwei per Post. Bank 27 bekam die Unterlagen auf Wunsch per Fax und per Mail.

3.4 Das Erinnerungsschreiben

Nachdem die für den 10.Juli 2001 angesetzte Antwortfrist verstrichen war, lagen erst vier ausgefüllte Fragebögen vor. Bank 13 sendete bereits am 28.06.01 den ausgefüllten Fragebogen zurück. Danach folgten die Bögen der Banken 4, 6 und 8 sowie eine Absage von Bank 26.

Der Aussand des Erinnerungsschreibens fand am 15.Juli wieder per Post, Fax und e-Mail statt. Bereits am 16.Juli reagierte Bank 2 mit der Aussage:

„Ihre Unterlagen wurden an den Vorstand weitergeleitet, sollten Sie keine Reaktion erhalten, hat er sich gegen eine Beantwortung Ihrer Fragen entschieden.". Da keine Reaktion des hier erwähnten Vorstandes erfolgte, wurde dies als Absage gewertet. Eine weitere Absage kam von Bank 18. Fünf ausgefüllte Fragebögen von den Banken 1, 12, 14, 21 und 23 wurden auf Grund des Schreibens zurückgefaxt. Außerdem hatten sich zwei weitere Banken gemeldet, dass ihre Fragebögen noch in Bearbeitung seien (Bank 17 und Bank 19). Weiterhin teilte der Mitarbeiter der Bank 28 den Namen der Person mit, an welche er die Unterlagen mit der Bitte um Bearbeitung weitergeleitet hatte.

4.5 Erneute Telefonaktion

Da einige Banken noch keinerlei Reaktion gezeigt hatten, wurde noch einmal telefonisch am Montag, dem 06.08.2001 von 14.00 bis 17.00 Uhr, nach dem Verbleib der übrigen 17 Bögen geforscht.

Bei Bank 3 war selbst nach mehreren Versuchen an verschiedenen Tagen niemand zu erreichen, weder der Ansprechpartner noch ein anderer Mitarbeiter der Bank. Durch einen Personalwechsel war der Fragebogen in Bank 5 und ebenso in Bank 30 verloren gegangen. Wir sendeten die Unterlagen erneut per e-Mail an die entsprechenden Nachfolger. Aufgrund der Urlaubszeit waren die Ansprechpartner der Banken 7, 9, 15, 25, 28 und 31 nicht erreichbar und deren Kollegen konnten keine Aussagen über den Verbleib des Fragebogens machen. Bank 10 und Bank 11 erkundigten sich nochmals bei Personen, an welche sie den Bogen weitergeleitet hatten. Allerdings sagten diese per Rückruf am darauf folgenden Tag aus Kapazitätsgründen ihre Teilnahme ab. Bei den Banken 16, 24 und 27 wurde nur mit Kollegen gesprochen, welche versprachen, dem jeweiligen Ansprechpartner eine Mitteilung zu hinterlegen und diesem um Rückruf zu bitten, welche bis zum heutigen Tage nicht erfolgten.

Bank 20 fiel auch bei dieser Telefonaktion auf. Auf die Frage der Bankmitarbeiterin an welche Abteilung der Fragebogen geschickt worden sei, konnte keine Auskunft geben werden, da bei der Adressrecherche kein Ansprechpartner bzw. die zuständige Abteilung genannt wurde. Daraufhin erfolgte die Auskunft, dass der Verbleib des Bogen so nicht nachvollziehbar wäre und somit kein Interesse an der Teilnahme bestünde.

Der Mitarbeiter der Bank 22 hatte die Unterlagen an den Vorstand weitergeleitet und noch keine Reaktion erhalten, jedoch wollte er sich erkundigen und sich telefonisch melden, was allerdings ausblieb. Bank 29 erhielt den Fragebogen erneut per Fax, da die Unterlagen aus nicht geklärten Gründen verschwunden waren. Sie reagierte einige Tage später mit Bedauern über den ungeklärten Verbleib und sagte aus zeitlichen Gründen ihre Teilnahme ab.

Somit lagen 11 ausgefüllte Fragebögen zur Auswertung vor. Dies entspricht einer Rücklaufquote von rund 35,5 Prozent. Ebenfalls sagten 6 Unternehmen ihre Teilnahme ab. Dies entsprach 19,4 Prozent der befragten Banken. Ein Anteil von 45,1 Prozent (14 Banken) musste als Ausfall gewertet werden.

4. Auswertung

Dieser Auswertung lagen die ausgefüllten Fragebögen der Banken 1, 4, 6, 8, 12, 13, 14, 17 19, 21 und 23 zugrunde. Die Auswahl der Banken wurde nach Bekanntheit und Wichtigkeit in der deutschen Bankenlandschaft getroffen. Die Umfrage entsprach keiner repräsentativen Stichprobenziehung, da sie einen zu geringen Umfang hatte. Es wurde mit einer Stichprobe von nur 31 Banken gearbeitet. Dies schränkte die Auswertung von vorn herein auf tendenzielle Aussagen über die größten Banken in Deutschland ein. Aufgrund der sehr geringen Beteiligung (35,5%) der kontaktierten Unternehmen, ist es nicht möglich, allgemeingültige Aussagen über den momentanen Stand der Entwicklungen bei den Sicherheitsstandards zu treffen. Es können lediglich Tendenzen aufgezeigt werden. Dies ist bei den folgenden Ausführungen zu beachten.

Die Fragebögen wurden immer von kompetenten Mitarbeitern der einzelnen Banken ausgefüllt. Meist waren sie im Bereich Internet Banking Service zu finden (8 Abteilungen). Darunter waren 2 Abteilungsleiter und 2 Produktmanager. Zwei weitere Ansprechpartner waren die Leiter von IT- Abteilungen. Ein Bogen wurde von einem Mitarbeiter einer Presseabteilung, tätig bei der Online- Redaktion, ausgefüllt.

4.1 Funktionalität, Ausstattung, Versorgung

Als Grundvoraussetzung für das Homebanking muss der Kunde über einen Personalcomputer sowie einen Internetanschluss (ISDN/Analog Anschluss) verfügen, so waren sich alle Banken einig.

Bei 57 Prozent der Banken reicht bereits ein höherwertiger Standardbrowser, wie Netscape ab Version 4.x oder Microsoft Internet Explorer ab Version 5.x aus. Ein HBCI- Client oder ein kryptographischer Browser wird bei den restlichen 43 Prozent benötigt. Da diese Frage nur von wenigen Banken beantwortet wurde, kann man keine Tendenz ableiten. Nutzt ein Bankkunde HBCI, benötigt er meist noch ein Kartenlesegerät, denn 80 Prozent der befragten Banken die HBCI anbieten, bieten dies in Verbindung mit einer Chipkarte. Lediglich 20 Prozent speichern den Kundenschlüssel auf einer Diskette ab.

Als Zugangsmöglichkeit werden in 91 Prozent das Internet, in 82 Prozent T-Online und in 57 Prozent AOL angeboten. Darüber hinaus bieten einzelne Ban-

ken Zugänge über DGN, DZN, aponet[3], Telebanking via Direkteinwahl, FTAM[4] per ISDN für Firmenkunden und WAP/SMS- Banking an. Die Zugangsmöglichkeit ist demzufolge weitgehend offen. Der Kunde kann selbst entscheiden, über welchen Zugang er sich einwählt. Er ist somit von keinem bestimmten Zugang oder Provider abhängig.

Die Angaben der Banken über verwendete Soft- und Hardware lassen darauf schließen, dass es keine allgemeine Standardsoftware bzw. -hardware gibt. Die Banken nutzen Produkte verschiedener Firmen sowohl im Soft- als auch Hardwarebereich, z.B. von „Omikron", „Towitoko" oder „DataDesign".

Banken	Anteil der Gesamtkunden
1	10%
2	20%
1	22%
1	25%
2	30%
1	92%
3	Keine Angabe
Gesamt 11	

Tab.1: Auf Frage I.4: „Wie viel Prozent aller Ihrer Kunden nutzen die Möglichkeit des Homebanking?" ergab sich nebenstehende Verteilung.

Die großen Unterschiede ergeben sich daraus, dass sich an der Umfrage sowohl Filialbanken als auch Direktbanken und Broker beteiligt haben. Bei den Direktbanken ist die Nutzung des Homebanking wesentlich höher als bei den Filialbanken. Nur 20 bis 30 Prozent der Kunden von Filialbanken nutzen die Möglichkeit des Homebanking.

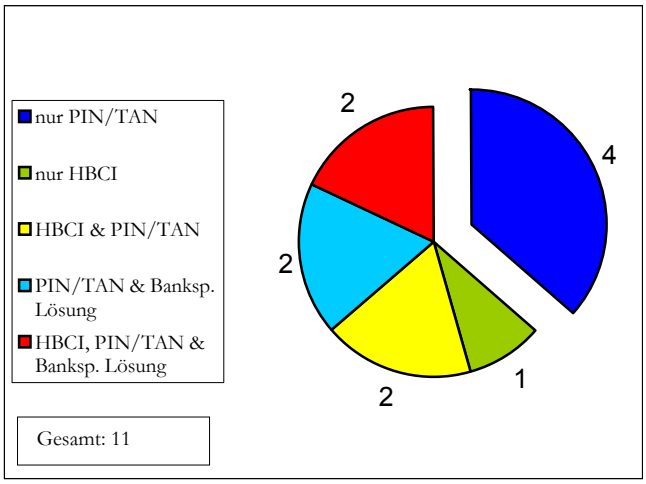
Alle Banken bieten nähere Informationen über Sicherheitsstandards im Bereich Homebanking auf ihren Internetseiten an. Ein Großteil der befragten Banken in-

[3]DGN, DZN und aponet sind spezielle Netzwerke für Ärzte und Apotheken.

[4]FTAM- Verfahren = File Transfer Access Method. FTAM ist ein branchenübergreifendes und international eingesetztes Protokoll zur Datenübertragung, das auf internationalen Standards be-

formiert ihre Kunden zu diesem Thema mit Broschüren. Ebenso werden die Bankmitarbeiter und die Verteilung von Infopost genutzt, um den Kunden das Thema näher zu bringen. Informationsmedien, wie Newsletter, Kontoauszüge, Hotlines, Plakate und Pressemitteilung werden eher selten von den Banken diesbezüglich gewählt.

Abb.1: Auswertung der Frage I.6: „Welche Standards bieten Sie an?“.



Die Verteilung in Abb.1 lässt vermuten, dass viele Banken den HBCI- Standard noch nicht umgesetzt haben, und lediglich über das PIN/TAN- Verfahren verfügen. Hingegen bieten Banken mit HBCI, diesen als Zusatz neben dem PIN/TAN- Verfahren und/oder einer eigenen bankspezifischen Lösung an. Ein möglicher Grund könnte sein, dass die Nutzung des HBCI- Verfahrens bei diesen Banken unter 10 Prozent liegt. Nur Bank 4 besitzt neben HBCI kein weiteres Verfahren. Sie plant jedoch das PIN/TAN- Verfahren noch im 4.Quartal 2001 für seine Kunden zu realisieren, da das PIN/TAN- Verfahren die größte Akzeptanz bei den Kunden findet. Sie führte HBCI bereits 1998 ein. Die weiteren vier Banken, die über HBCI verfügen, boten ihren Kunden diesen Standard hingegen erstmals 1999 bzw. 2000 an. Die Banken bieten den Usern die Versionen 2.01 oder 2.1 an. Ein Trend in Richtung HBCI- Standard scheint sich in den nächsten

---

ruht. Die Sicherung der Datenübertragung erfolgt hierbei durch die Elektronische Unterschrift (vgl. Glossar s-online 2001).

Jahren jedoch nicht abzuzeichnen, da alle befragten Banken ohne HBCI momentan nicht planen diesen Standard einzuführen.

Nach Aussage der Banken sei keine Akzeptanz auf Seiten der Kunden vorhanden. Das Verfahren wird für zu kompliziert und für den Kundenbereich als ungeeignet eingeschätzt. Daher seien die Chancen für eine Marktdurchdringung sehr gering. Wenn dann würden künftig nur Signaturkarten mit weitem Einsatzbereich eine Chance haben, so Bank 13. Ebenfalls äußerte der Mitarbeiter dieser Bank: „Die Sicherheit mittels PIN/TAN ist seit 1982 im Einsatz und bis heute ist noch kein Missbrauchsfall bekannt geworden. Auch Stiftung Warentest, die die verschiedenen Systeme untersucht hat, stellt dem PIN/TAN- Verfahren eine Vertrauensbescheinigung aus."

Ein weiteres Problem ist die Umsetzung des HBCI- Standards. Die Antwortvorgaben zu Frage I.8 wurden auf Basis des aktuellsten HBCI- Standards, Version 2.2 (vgl. Bundesverband deutscher Banken e.V. 2000, 195) ausgearbeitet, um alle möglichen Geschäftsvorfälle zu berücksichtigen. Wie in der Tabelle 2 zu sehen ist, bieten die Banken im Rahmes des PIN/TAN- Verfahrens eine größere Breite an Geschäftsvorfällen bei Homebanking an. Zum Beispiel haben die Kunden bei keiner der befragten Banken die Möglichkeit mit HBCI Unterkonten zu erstellen oder Elektronisches Geld zu nutzen. Allerdings hat auch keine der befragten Banken die Version 2.2 des HBCI- Standards bisher implementiert. In den von den Banken verwendeten Versionen 2.1. und 2.01 sind diese Geschäftsvorfälle noch nicht enthalten. Kunden der Bank 19 können mit PIN/TAN über 19 verschiedene Geschäftsvorfälle verfügen, mit HBCI hingegen nur über 15. Eine noch geringere Auswahl an Geschäftsvorfällen sowohl bei HBCI, PIN/TAN als auch bei Bankspezifischen Lösungen haben die Kunden der restlichen Banken. Bank 23 bietet lediglich 8 Geschäftsvorfälle über HBCI und 9 über PIN/TAN an. Bank 1 plant beispielsweise, Wertpapierorder ab Oktober 2001 via PIN/TAN- Verfahren zu realisieren. Dies erweckt den Anschein, das die Banken eher daran interessiert sind die Breite der Geschäftsvorfälle des PIN/TAN- Verfahrens zu erweitern, als den aktuellen HBCI- Standart vollständig zu implementieren.

Geschäftsvorfälle	HBCI	PIN/TAN	Bankspez. Lösg.
Kontenabfrage	5 Banken	10 Banken	3 Banken

Kontoauszüge	5	9	3
Einzelüberweisungen	5	10	3
Sammelüberweisungen	3	8	1
Terminierte Überweisungen	3	9	2
Auslandsüberweisungen	2	5	2
Euroüberweisungen	2	9	2
Sonderform der Überweisung	2	1	0
Daueraufträge	5	10	1
Lastschriften	1	6	1
Scheckbestellung	2	4	2
Vordruckbestellung	1	4	2
Reisescheckbestellung	1	2	2
Kartenbestellung	1	4	2
Kartensperre	2	2	1
Unterkontenerstellung	0	1	1
Sorten-/Devisenkurse	3	2	2
Wertpapierinformationen	3	6	2
Wertpapiertransaktionen	3	7	1
Depotauszüge	4	7	2
Festgeld/Termineinlagen	1	6	0
Elektronisches Geld	0	1	0
Kreditrechnungen	0	2	0
Banken, mit diesem Standard	5	10	3

Tab.2: „Welche Geschäftsvorfälle kann der Kunde bei Ihnen online abwickeln?“
(Häufigkeitsverteilung der umgesetzten Geschäftsvorfälle)

Dies führt zu der Vermutung, das sich ein Spiralprozess in Gang setzen könnte. Die Banken bieten wenig Service im HBCI- Bereich, der Kunde hat mehr Möglichkeiten mit PIN/TAN als mit HBCI und nutzt deshalb eher ersteres. Demzufolge besteht keine Nachfrage nach HBCI und die Banken sehen keine Notwendigkeit, diesen Standard weiter auszubauen. Eine Verallgemeinerung über die Umsetzung und Serviceleistungen in bezug auf das Angebot der möglichen Geschäftsvorfälle ist auf Grund der geringen Beteiligung allerdings nicht möglich.

Sechs der elf befragten Banken bieten den Kunden zusätzliche Sicherheitsmaßnahmen. Bank 8 hält sowohl RSA[5], DSA[6]-Signaturkarte als auch DES- Karte[7] für

[5]RSA = Rivest, Shamir und Adleman. RSA kann mit Schlüsseln variabler Länge arbeiten und teilt die zu verschlüsselnden Daten in Blöcke auf, deren Länge der Schlüssellänge entspricht. Aktuelle

ihre Kunden bereit. Die anderen 5 Banken verfügen jeweils über eine weitere Sicherheitsmaßnahme, welche in den meisten Fällen die RSA, DSA- Signaturkarte ist.

5.2 Identifizierung und Kommunikationsintegrität

Wie bereits im vorhergehenden Abschnitt festgestellt, nutzen 4 Banken die RSA, DSA- Signaturkarte mit einem 1024- Bit Schlüssel und 2 Banken die DES- Karte mit 128- Bit Schlüssel, um die Kunden zu authentifizieren. Eine weitere Bank nutzt dafür RSA/Triple DES. Diese Verfahren werden allgemein als sicher bewertet. Beim PIN/TAN- Verfahren dient zur Authentifizierung die PIN in Verbindung mit der Kontonummer. Die Identifizierung des Kunden findet jeweils zu Beginn einer Session, sowie bei einem Großteil der Banken nach 5, bzw. 10 Minuten Inaktivität des Users statt. Der Bankserver prüft zusätzlich noch die Berechtigung jedes einzelnen Auftrages. Bei HBCI geschieht dies durch Signaturverifikation oder UPD (vgl. Baschny 2001,6).

Beim PIN/TAN- Verfahren erfolgt ein Abgleich der TAN mit der Datenbank des Bankservers, um die Berechtigung des Auftrages sicherzustellen. Die meisten der hier analysierten bankspezifischen Lösungen arbeiten mit einem Abgleich der Schlüsselpaare und des Kennworts.

Auf die Frage „Wie prüft die Bank, das der Auftrag unverletzt angekommen ist?“ antworteten viele Banken nicht. Bei den 6 Banken, die geantwortet haben, erfolgt eine Prüfung entweder durch eine syntaktisch- semantische Eingangsprüfung oder durch eine Hash- Wert- Berechnung. Jedoch sind diese Informationen nicht ausreichend, um allgemeine Aussagen treffen zu können.

Prüfkriterium	Häufigkeit

Tab.3: Die nebenstehende

Implementierungen unterstützen derzeit Schlüssellängen zwischen 512 und 2048 Bit. Es gilt als sehr sicher, wenn auch sehr langsam (vgl. Cryptovision, 2000).

[6]DSA = Digital Signature Algorithm. DSA ist eine Variante zur Erstellung digitaler Signaturen basierend auf dem Diskreten Logarithmus- Problem in endlichen Körpern. Für Anwendungen finden gegenwärtig Zahlen mit 1024 Bit Verwendung (vgl. Cryptovision, 2000).

[7]DES = Data Encryption Standard. DES verschlüsselt immer 64- Bit Blöcke. Die Bits 8, 16, 24,..,64 des externen Schlüssels dienen dabei als Paritätsbits, so dass die tatsächlich wirksame Schlüssellänge nur 56 Bit beträgt. Der kurze Schlüssel von DES macht das Verfahren sehr leicht angreifbar. Diese Schwäche kann durch die Verwendung von Triple- DES umgangen werden. Dabei wird das DES- Verfahren in drei Stufen mit zwei unterschiedlichen Schlüsseln verwendet (vgl. Cryptovision, 2000).

Signierte Auftragsbestätigung	1 Bank
Bestätigungsnummer	2
Serverrückmeldung	3
ZVDFÜ[8]/FTAM	1
Sendebestätigung	2
Keine Angabe	2
Gesamt	11

Tabelle zeigt die Verteilung der Häufigkeiten bei Frage II.6: „Wie prüft der Kunde, dass der Auftrag angenommen wurde?“

Wie in Tabelle 3 ersichtlich, erhält der Kunde in allen angegeben Fällen nach Auftragseingang eine Rückmeldung von der Bank. Von den 11 befragten Banken gaben 6 Institute an, dass ihre Kunden eine Quittung über die ausgeführten Aufträge erhalten. Jedoch sind diese nur bei zwei Banken signiert. Demzufolge ist es für die Banken noch nicht selbstverständlich, dass der Kunde eine Quittung erhält. Der Kunde hat also nur in 2 von 11 Fällen einen gültigen Beweis in Form einer signierten Quittung, sollte es zu Unstimmigkeiten zwischen Bank und Kunde kommen. Bei 3 Banken trägt der Kunde die Beweislast und nur in 2 Fällen die Bank. Bei den restlichen sechs Banken wird jeder Sachverhalt einzeln abgewägt. Eine pauschale Aussage sei nicht möglich, gaben die Unternehmen an. Als Beweise dienen, neben den signierten Quittungen, die Statusprotokolle der Bankserver. Jedoch entscheiden viele Banken hauptsächlich einzelfallabhängig, was als Beweis angesehen wird. Eine weitere Frage beschäftigte sich mit dem Bewusstsein, das die Banken für die Gefahren, die das Internet als Kommunikationsmedium, bzw. Kommunikationskanal mit sich bringt. Eine Sicherheitslücke stellen z.B. Scheinhomepages dar. Als zusätzlichen Schutz vor Maskeraden[9] betrachten 9 von 11 Banken SSL- Verschlüsselung mit Bankzertifikat. Für SSL ist ein Serverzertifikat zwingend erforderlich. Dies haben auch alle ausfüllenden Institute erkannt. Bank 6 kaufte zur Sicherung vor Scheinhomepages ähnliche URLs auf.

[8] ZVDFÜ = Zahlungsverkehrsdatenfernübertragung. Verfahren zur Übertragung von Daten im Rahmen der DFÜ. Die per ZVDFÜ übertragenen Daten werden vor ihrer Übertragung einer syntaktischen Prüfung unterzogen. Der eigentliche Datentransfer ist durch Kontrollmitteilungen, die während der DFÜ zwischen Kreditinstitut und Kunde ausgetauscht werden gegen Manipulation gesichert (vgl. Glossar s-online 2001).

[9] Maskerade = Scheinhomepage, bzw. Scheinidentität. Man gibt sich als etwas aus, was man nicht ist. Durch Irreführung des Clients können Dritte PINs und TANs abfangen und anschließend gegenüber der Bank mit einer falschen Identität auftreten.

5.3 Vertraulichkeit

Die Kommunikation zwischen Client und Server wird bei allen befragten Banken verschlüsselt, was zeigt, dass die Banken in hohem Maße auf Vertraulichkeit achten. Die Verteilung der einzelnen angewendeten Verfahren zeigt Tab.4.

Verschlüsselungsverfahren	Häufigkeit
RSA- Verschlüsselung	6 Banken
SSL	8
andere Hybridverfahren	1
HBCI- Spezifikation	1

Tab.4: Verteilung der Häufigkeiten der angewandten Verschlüsselungsverfahren der Banken. (Mehrfachnennungen)

Um die Kommunikation zwischen Bank und Kunde zu verschlüsseln, benötigen beide Seiten einen Schlüssel. Diese können durch verschiedene Personen bzw. Institutionen erzeugt werden. Bei den elf Banken ergab sich folgende Verteilung.

Schlüsselgenerator	für Bank	für Kunde
Bank	5 Banken	1 Bank
Trustcenter	4	2
Kunde	-	4
Bank & Trustcenter	1	1
Rechenzentrum SDV	1	1
Kartenhersteller	-	1
Standardbrowser	-	1
Gesamt	11	11

Tab.5: „Wer generiert den Bank- bzw. den Kunden-schlüssel?“

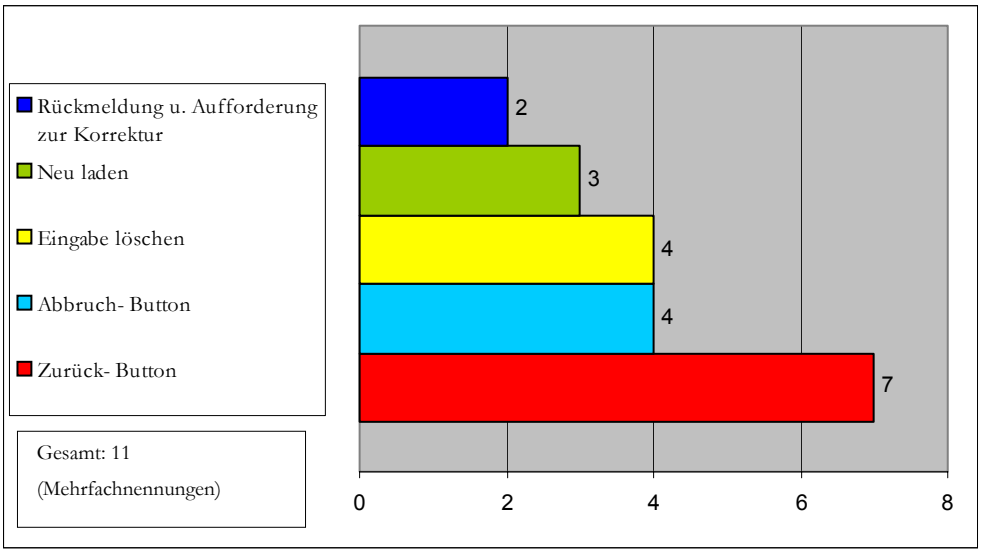
5.4 Verantwortlichkeit und Haftung

Bei allen für die Auswertung zur Verfügung stehenden Banken erhält der Kunde eine Übersicht über die von ihm ausgeführten Aufträge.

Sollte es zu Systemausfällen oder Verbindungsabbruch kommen während der Kunde Transaktionen tätigt, erscheint bei allen Banken eine Fehlermeldung beim Kunden. Allerdings werden nur 7 der 11 Bankserver in einem solchen Fall benachrichtigt. Bei den restlichen vier Banken geht keine Meldung über eine Störung ein. Erhält ein Bankserver eine Fehlermeldung fordert dieser die erneute Authentifizierung des Clients. Die Sicherung, bzw. Speicherung oder Löschung der gerade durchgeführten Transaktionen ist in den meisten Fällen abhängig vom Zeitpunkt der Störung.

Der Kunde erfährt bei sieben der elf Banken durch einen Abgleich mit dem Auftragsbuch der Bank, oder der Doppelkontrolle durch PIN/TAN verbindlich vom Bankserver ob der Auftrag ausgeführt wurde oder nicht. Durch diese Bestätigung werden Doppelbuchungen vermieden. Die vier anderen Banken gaben an, dass der Kunde eine verbindliche Information über den Auftragseingang im Fall einer Unterbrechung erhält. Somit sei eine weitere Kontrollfunktion für den Kunden nicht notwendig.

Abb.2: Auswertung zu Frage IV.5: „Wie gehen Sie mit Vertippen oder Verklicken seitens des Kunden um?“



Nur zwei der befragten Banken unterstützen den Client durch eine Serverrückmeldung mit einer Aufforderung zur Korrektur der eingegebenen Daten. Der Kunde muss also bei den meisten Banken selbst darauf achten, seine Angaben exakt einzutragen. Bei sieben Banken hat er die Möglichkeit, durch einen Zurück-Button in der Anwendung seine eingegebenen Daten zu korrigieren. Weitere Möglichkeiten können der Abbildung 2 entnommen werden.
Falls der Auftrag bereits abgeschickt wurde, bieten 5 der 11 Banken die Möglichkeit den Vorgang online zu stornieren. Eine Stornierung ist allerdings nur möglich, solange der Auftrag noch im Auftragsbuch des Kunden enthalten ist, d.h. noch nicht von der Bank ausgeführt wurde. Bei den restlichen 6 Banken kann eine Stornierung nur über einen Berater in der Geschäftsstelle ausgeführt werden, z.B. per Telefon, Fax oder TAN- gesicherten Auftrag. Zu beachten ist, dass die Online- Stornierungen nur in einem begrenzten Umfang möglich sind. Die einzige Bank, bei der laut Fragebogen sämtliche umgesetzte Vorgänge ohne Einschränkung online storniert werden können, ist Bank 13. Die Servicebereitschaft der einzelnen Banken unterscheidet sich auch im Fall der Stornierung von Bank zu Bank. Jedoch ist bei allen Banken die Stornierung eines Online- Auftrages, wenn zum Teil auch offline, möglich.

5.5 Persönliche Betreuung

Wie gut die Serviceleistungen einer Bank sind, zeigt auch eine regelmäßige Bearbeitung der vorliegenden Aufträge. Hier variieren die Leistungen der Banken auffallend stark. Die Bearbeitungsintervalle reichen von einer Sekunde bis zu 15 Minuten nach Auftragseingang bei dem Bankserver. Allerdings haben nicht alle Banken die Bearbeitungsabstände angeben. Die meisten Angaben bezogen sich auf die Buchungszeiten, zu denen die Kundenaufträge bearbeitet werden. Bank 13 führt die Aufträge nur von Montag bis Freitag bis 13:00 Uhr aus. Neben Bank 13, bearbeitet auch Bank 19 die Kundenaufträge nur an Werktagen. Die Ausführung der Anforderungen, die am Samstag, am Sonntag und an Feiertagen eingehen, werden erst am darauffolgenden Werktag veranlasst. Hingegen werden bei anderen Banken, z.B. Bank 8, sogar die am Wochenende eingegangenen Aufträge noch am selben Tag erledigt.

Die Bearbeitungszeiten sind an diesen Tagen jedoch eingeschränkt. Einen rund um die Uhr Service, sieben Tage die Woche, 24 Stunden am Tag, bieten sowohl Bank 6 als auch Bank 23.

Bei acht der elf befragten Banken steht dem Onlinekunden bei Fragen und Problemen ein direkter Ansprechpartner in der Geschäftsstelle zur Verfügung. Dies entspricht einem Anteil von 73 Prozent. Der persönliche Bankberater wird dem Kunden bei der Aufnahme der Geschäftsbeziehung bzw. der Kontoeröffnung mitgeteilt. Darüber hinaus ist der Name des Mitarbeiters bei Bank 6 auf jedem Kontoauszug enthalten.

Ein unverzichtbarer Service für Homebanking ist eine Kundenhotline, an die sich der User bei Fragen und Problemen wenden kann. Die Prioritäten des Kunden liegen bei Unabhängigkeit von Zeiten und Bankfilialen. Aus diesem Grund spielt die Erreichbarkeit der Bank außerhalb der Öffnungszeiten ebenfalls eine große Rolle für ihn. Über den Service einer Hotline verfügen alle der befragten Banken. Jedoch unterscheidet sich der Service im Rahmen der Hotline von Bank zu Bank. Sieben dieser Anlaufstellen sind für den Nutzer kostenpflichtig. Es handelt sich in den meisten dieser Fälle allerdings um eine „0180- Servicenummer“. Andere bieten sie zum Ortstarif an. Eine generelle Aussage ist an dieser Stelle aufgrund der geringen Teilnahme ebenfalls nicht möglich. Neun der befragten Unternehmen haben ihre Hotline nicht rund um die Uhr besetzt. Bank 14 unterteilt ihr Call-Center nach bankspezifischen und technischen Bereichen, wobei lediglich die Abteilung, die für bankspezifische Fragen zuständig ist, im 24 Stundenbetrieb arbeitet. Nur Bank 13 ist für ihre Kunden rund um die Uhr erreichbar.

Nicht alle Banken waren bereit, Auskünfte bezüglich der Ausstattung und Auslastung ihres Call- Centers zu geben. Trotzdem sind die gegeben Werte ausreichend, um große Unterschiede zwischen den einzelnen Banken zu erkennen. Die Gesamtzahl der Bankkunden spielt hierbei natürlich eine große Rolle. Eine Bank mit sehr vielen Kunden benötigt mehr Anschlüsse als eine kleinere Bank. Für Direktbankkunden sind Internet und Telefon die einzigen Möglichkeiten mit ihrer Bank in Kontakt zu treten, da diese Unternehmen nicht mit Filialen arbeiten.

Bank	Anschlüsse (parallel)	Anrufe pro Monat	Auslastung pro Anschluss
Bank 1	10	3.000	300
Bank 4	20	Keine Angabe	Keine Angabe
Bank 6	40	11.000	275
Bank 8	340	28.000	82
Bank 12	Keine Angabe	Keine Angabe	Keine Angabe
Bank 13	Keine Angabe	Keine Angabe	Keine Angabe
Bank 14	6	400	67
Bank 17	24	1.500	62
Bank 19	7	Keine Angabe	Keine Angabe
Bank 21	10	Keine Angabe	Keine Angabe
Bank 23	20	3.000	150

Tab.6: Aufschlüsselung der Hotlineanschlüsse der einzelnen Banken, Anrufe pro Monat und Auslastung pro Leitung

5.6 Zusätzliche Anmerkungen der Banken

Einige Banken wiesen im Anschluss des Fragebogens darauf hin, dass neben dem Sicherheitsaspekt die Komplexität des Online- Banking eine zentrale Rolle für den Kunden spielt. Aus diesem Grund soll Homebanking schnell, einfach und leicht handhabbar sein. Der Kunde entscheidet sich für Homebanking, um Zeit und Geld zu sparen (vgl. Ebeling 2001, 130).

Um potentiellen Online- Kunden den Einstieg in den Homebankingbereich so einfach wie möglich zu machen, bietet Bank 19 die Möglichkeit Online- Banking unverbindlich zu testen. Sie bietet auf ihren Internetseiten ein Testkonto an. Dieses virtuelle Konto umfasst alle notwendigen Funktionalitäten. Durch Eingabe einer beliebigen fünfstelligen PIN gelangt man zum Testkonto mit Kontenübersicht, Kontostandsabfrage und Umsatzanzeige. Probeaufträge können mittels einer sechsstelligen TAN ausgeführt werden.

5. Vergleich zur „Capital- Umfrage“

5.1 Ergebnisse dieser Umfrage

Bei den Untersuchungen zu *Funktionalität, Ausstattung und Versorgung* im Bereich des Homebanking ergab sich ein überraschendes Bild. Lediglich 20- 30 Prozent der Kunden von Filialbanken nutzen die Möglichkeit, ihre Bankgeschäfte online zu erledigen. Und das, obwohl Informationen zum Thema allgemein über das Internet und über Broschüren erhältlich sind.

Die Durchsetzung des HBCI- Standard ist bei den befragten Banken noch nicht weit fortgeschritten. Meist bieten die Banken mehr Geschäftsvorfälle mit dem PIN/TAN- Verfahren an. Der HBCI- Standard wird nicht vollständig umgesetzt und wird meist nur als Zusatz angeboten. Dies belegen die Nutzungszahlen. Werden mehrere Möglichkeiten angeboten, so liegt die Akzeptanz von HBCI bei den befragten Banken unter 10 Prozent. Banken, die den HBCI- Standard noch nicht umgesetzt haben, planen dessen Einführung gegenwärtig auch nicht. Als Gründe hierfür nennen die Banken die geringe Akzeptanz auf Seiten der Kunden. Das Verfahren wird für zu kompliziert und für den Kundenbereich als ungeeignet eingeschätzt.

Dies könnte auf eine Tendenz weg vom HBCI, hin zum PIN/TAN- Verfahren deuten. Aufgrund der geringen Nachfrage sehen sich die Banken nicht gezwungen, den HBCI- Standard umzusetzen, obwohl er mit einer höheren Sicherheit und mehr Benutzerfreundlichkeit verbunden ist (vgl. Kapitel 2).

Die mangelnde Sicherheit des PIN/TAN- Verfahrens beweist ein aktueller Vorfall. Hacker sind im Auftrag des Fernseh-Magazins "ARD- Ratgeber Technik" in den Zentralcomputer der Hypo/Vereinsbank eingebrochen. Das Sicherheitssystem des deutschen Geldinstituts war so mangelhaft geschützt, dass die Kontenknacker aus Thüringen und die Fernseh-Redakteure innerhalb von wenigen Tagen 1,5 Millionen Onlinebuchungen einschließlich Geheimnummern (PINs) und Online- Nummern in den Händen hielten (vgl. Heise 2001).

Identifizierung und Kommunikationsintegrität sind positiv zu bewerten. Es werden zusätzliche Sicherungsmaßnahmen, wie RSA/DSA- oder DES- Signaturkarten, angeboten. Diese Verfahren gelten als sicher.

Zu Beginn jeder Session und in einigen Fällen nach einer gewissen Zeit der Inaktivität wird vom Kunden eine eindeutige Identifizierung verlangt.
Eine Bestätigung der eingegangenen Aufträge bekommen alle Kunden der befragten Banken, hingegen in nur zwei Fällen in Form einer signierten, absolut beweissicheren Quittung. Dies ist insofern wichtig, da im Fall von Unstimmigkeiten der einzelne Fall bewertet werden muss.
Die notwendige *Vertraulichkeit* in der Beziehung zwischen Bank und Kunde ist ebenfalls gegeben. Die Kommunikation zwischen Client und Server wird in allen vorliegenden Fällen mittels SSL, RSA oder anderen Hybridverfahren, verschlüsselt. Die dazu benötigten Schlüssel werden von den Banken selbst oder von Trustcentern erzeugt.
Verantwortlichkeit und Haftung sind noch nicht einheitlich umgesetzt. Der Kunde erhält in allen vorliegenden Fällen eine Übersicht über seine ausgeführten Aufträge. Bei Störungen erfolgt immer eine Benachrichtigung des Kunden, jedoch werden nicht alle Bankserver über den Zwischenfall unterrichtet. Was mit dem gerade in Bearbeitung befindlichen Auftrag in einem Störungsfall geschieht, ist abhängig vom Zeitpunkt des Ereignisses. Eine Verhinderung von Doppelbuchungen ist allerdings in allen vorliegenden Fällen durch Abgleich mit dem Auftragsbuch, durch Doppelkontrolle PIN/TAN oder Information des betroffenen Kunden gegeben.
Stornierungen sind generell bei allen befragten Instituten möglich. Online- Stornierungen können allerdings nur in begrenztem Umfang und nur solange die Aufträge noch nicht ausgeführt wurden, erfolgen. Ansonsten ist die Einschaltung eines Bankberaters erforderlich.
Die *persönliche Betreuung* ist bei den einzelnen Banken sehr unterschiedlich geregelt. Die Bearbeitungsintervalle und Buchungszeiten schwanken von Institut zu Institut. Die Bandbreite reicht von Bearbeitung der Aufträge nur zu Geschäftszeiten bis hin zu einem 24 Stunden Service.
Meist steht dem Kunden ein persönlicher Ansprechpartner und in allen Fällen eine Hotline zur Verfügung. Allerdings ist die telefonische Betreuung für den Kunden nicht rund um die Uhr erreichbar. Die Zahl der Anschlüsse und die Auslastung der einzelnen Call- Center ist abhängig von der Anzahl der zu betreuenden Kunden.

6.2 Vergleich

In der ersten Umfrage wurde ein hohes Bewusstsein der Banken für *Vertraulichkeit* festgestellt. Dies ist immer noch gegeben, wie man an den sicheren Verschlüsselungsmethoden und den Signaturkarten sehen kann.

Das Bewusstsein für die *Integrität* der übermittelten Daten war 1999 nur mittelmäßig ausgeprägt. Die heutige Lage kann leider durch die geringe Teilnahme nicht abschließend beurteilt werden. Die sechs Banken, die hierzu Aussagen getroffen haben, waren sich der Gefahren allerdings bewusst und prüfen die eingegangen Aufträge syntaktisch- semantisch oder mittels einer Hash- Wertberechnung. Eventuelle Manipulationen würden somit offensichtlich werden. Die Integrität der einzelnen Daten ist, der Beteiligung der Umfrage zu Folge, nach wie vor nicht flächendeckend gesichert. Hier ist der Kunde gefragt, sich zu vergewissern, wie seine Bank damit umgeht.

Das Bewusstsein für die *Beweissicherheit* ist nach wie vor gering ausgeprägt. Dies würde sich wahrscheinlich mit der Durchsetzung des HBCI- Standards ändern, der jeden Schritt eindeutig gegenüber Dritten beweisbar macht.

Die Gefahr der Maskerade ist bei den teilnehmenden Banken im Gegensatz zu 1999 weitgehend durch die Verschlüsselung der Kommunikation mittels SSL mit Bankzertifikat behoben. Das Bankzertifikat ermöglicht es, die Banken eindeutig zu identifizieren. Die Kunden identifizieren sich beim PIN/TAN- Verfahren lediglich über ihre PIN und die Kontonummer, beim HBCI hingegen eindeutig über die UPD.

Die *Stornomöglichkeiten* sind nach wie vor recht unterschiedlich geregelt. Es ist immer noch nicht möglich, alle online durchgeführten Aufträge auch online zu stornieren. Teilweise ist eine Stornierung nur über einen Kundenberater in der Bank möglich.

Die *Verfügbarkeit* ist, im Gegensatz zur ersten Umfrage kritisch zu betrachten. Es ist bedenklich, das nicht alle Banken rund um die Uhr für Ihre Kunden erreichbar sind.

Strategische Aufgaben, die sich aus der ersten Umfrage ergeben haben, sind bis jetzt nur teilweise bewältigt worden. Hervorzuheben sind hier Beweissicherheit und Rücknahme. Dies konnte trotz der geringen Beteiligung festgestellt werden.

Wenn die großen bedeutenden Banken in Deutschland mit mehreren tausend Kunden die Beweissicherheit der Aufträge oder die Auftragsrücknahme nicht anbieten, so kann man nicht sagen, das diese Servicestandards in Deutschland als umgesetzt gelten. Auch der lokale Sicherheitsanker Smartcard ist noch umstritten. Hier gibt es noch keinen einheitlichen Standard. Momentan existieren 3 verschiedene Arten von Verschlüsselungsverfahren: symmetrisches DES- Verfahren mit Chipkarte, diskettenbasierte asymmetrische RSA- DES- Hybridverschlüsselung (RDH) und RDH- Chipkarten (vgl. Hollich 2000, 193).

6. Verbesserungsvorschläge

Sofern eine weitere Anschlussumfrage in Betracht gezogen wird, bedürfen einige Punkte einer Überarbeitung. Die Umfrage müsste insgesamt längerfristig angelegt werden als es bei dieser studentischen Projektarbeit möglich war. Durch das unterschiedliche Antwortverhalten der Banken ging viel Zeit verloren. Eine Bank sendete bereits nach 10 Tagen den ausgefüllten Bogen zurück. Die letzten Fragebögen gingen hingegen erst nach fast einem Monat ein. Die zuletzt durchgeführte Telefonaktion führte zu Absagen einiger Banken, die sich nicht in der Lage sahen, den Fragebogen noch kurzfristig zu beantworten. Leider war es nicht möglich, auf diese Fragebögen zu warten und die Auswertung noch länger zu verschieben. Eine verlängerte Antwortfrist hätte wahrscheinlich zu einer höheren Rücklaufquote geführt.

Der Fragebogen müsste ebenfalls noch einmal überarbeitet werden. Die Fragen wurden von Bank 14 teilweise als zu speziell empfunden. Nur das niederlassungsübergreifende Rechenzentrum könne einige spezifische Fragen beantworten. Dies trifft sicher auch auf einige andere Institute zu, die ebenfalls nicht alle Fragen beantworteten. Bank 18 kritisierte die Befragungstechnik. Nur wenige Banken hätten einen „selbstgestrickten Internetauftritt“, also eine komplett eigene Umsetzung des Homebanking. Die Rechenzentren der Zentralen böten den angeschlossenen Instituten fertige Lösungen an, die sich nur in den von den Niederlassungen eingesetzten Varianten unterscheiden würden. Demzufolge sei der Fragebogen zu umfangreich ausgefallen, so Bank 18.

Bank 6 war der Meinung, das die Liste der Geschäftsvorfälle nicht ausgewogen sei. Bestellungen diverser Formulare hätten ein starkes Übergewicht,

während interessantere Geschäftsvorfälle, bzw. Funktionalitäten, wie z.B. Orderbuch, Neuemissionen, Kreditkartenfunktionalitäten u.ä. fehlen würden. Hier müsste eine entsprechende Anpassung erfolgen, da auch einige andere Banken die Liste der Geschäftsvorfälle unter „Sonstiges" ergänzt hatten.
Die Formulierung einiger Fragen müsste ebenfalls überdacht werden. Zum Beispiel wurde die Frage II.3 „In welchen Abständen wird die Identifizierung erneuert?" oft missverstanden. Die Frage zielt darauf ab, zu erfahren, in welchen Abständen die Identifizierung der Kunden während einer Session erneuert wird. Die Antworten bezogen sich allerdings meistens auf die Laufzeiten der Zertifikate.

7. Zusammenfassung und Ausblick

Wie aus den Ergebnissen dieser Umfrage ersichtlich ist, hat es Fortschritte im Bereich des Homebanking gegeben. Allerdings haben sich auch neue Aufgaben ergeben. Das moderne HBCI, wie es der neueste Standard 2.2 des Bundesverband deutscher Banken vorsieht, wurde bisher von keiner der befragten Banken umgesetzt. Auch die vorhergehenden Versionen 2.01 und 2.1 sind nicht vollständig implementiert.
HBCI soll als Industriestandard etabliert werden. Für die Durchsetzung von HBCI dürfte jedoch entscheidend sein, wie schnell die Geschäftsvorfälle der Version 2.2 bei Kreditinstituten und Kundenproduktherstellern umgesetzt sein werden, welche die Investition in neue Programmupdates für den Bankkunden rentabel machen. Als Unterstützung hierfür bieten die Verbände geeignete Software Development Kits an. Weiterhin hängt der Erfolg auch am Bereich Sicherheit und damit speziell an der Akzeptanz der Chipkartentechnologie beim Kunden. Als letztes muss sich HBCI als nationaler Standard auch im internationalen, speziell im europäischen Umfeld behaupten, wobei hinzukommt, das im europäischen Ausland ähnliche nationale Eigenentwicklungen im Entstehen sind. Es ist jedoch geplant, HBCI zur Standardisierung in internationale Gremien einzubringen (vgl. Haubner, 2000).
An der Servicebereitschaft der Banken müsste ebenfalls noch gearbeitet werden. Es ist wichtig, das die Bank rund um die Uhr für ihre Kunden erreichbar ist.
Ebenfalls sind die Bearbeitungsintervalle und Buchungszeiten von zentraler Bedeutung und wichtige Servicemerkmale.

Es ist möglich, die Kundenaufträge unverzüglich nach Eingang zu bearbeiten, allerdings bieten dies noch nicht alle der befragten Banken.
Auch in Punkto Storno muss noch einiges getan werden. Eine Stornierung der Aufträge ist zwar generell möglich, aber zum Teil bisher nur offline über einen Bankberater. Eine Online-Lösung wäre weitaus kundenfreundlicher.
Die Durchsetzung von Homebanking ist, durch die vielen damit verbundnen Vorteile, nicht mehr aufzuhalten. Ob allerdings HBCI die Gunst der Kunden gewinnen wird, bleibt fraglich.

Abkürzungsverzeichnis

AOL	: America Online Incorporation
ARD	: Arbeitsgemeinschaft der Rundfunkanstalten Deutschlands
DES	: Digital Encryption Standard
DGN	: Deutsches Gesundheitsnetz
DSA	: Digital Signature Algorithm
DZN	: Deutsches Zahnarzt Netz
FTAM	: File Transfer Access Method
HBCI	: Homebanking Computer Interface
ISDN	: Integrated Services Digital Network
IT	: Information Technology
PC	: Personal Computer
PIN	: Persönliche Identifikationsnummer
RDH	: RSA- DES- Hybridverschlüsselung
RSA	: Rivest, Shamir und Adleman
SDK	: Software Development Kits
SSL	: Secure Socket Layer
TAN	: Transaktionsnummer
TCP/IP	: Transmission Control Protocol/Internet Protocol
UPD	: Userparameterdaten
URL	: Universal Resource Locator
ZVDFÜ	: Zahlungsverkehrsdatenfernübertragung

Literaturverzeichnis

Algesheimer, R. (2000). Elliptische Kurven als alternatives Public Key- Verfahren im Homebanking-Standard HBCI. Diplomarbeit, Mainz

Baschny, Ernesto (2001). HBCI- Homebanking Computer Interface. Hauptseminar: Stuttgart

Bundesministerium für Wirtschaft und Technologie (BMWI), *Bundesministerium des Inneren* (BMI), *Bundesamt für Sicherheit in der Informationstechnik* (BSI) (2001). HBCI - Schlüssel für sicheres und flexibles Homebanking. In: http://www.sicherheit-im-internet.de/themes (07.08.2001)

Bundesverband deutscher Banken e.V., Berlin; *Deutscher Sparkassen- und Giroverband* e.V. Bonn/Berlin; *Bundesverband der Deutschen Volksbanken und Raiffeisenbanken* e.V., Bonn; *Bundesverband Öffentlicher Banken Deutschlands* e.V., Berlin (2000). HBCI. Homebanking- Computer- Interface. Schnittstellenspezifikation V. 2.2 .In: http://www.hbci-zka.de/spezifikation/2.html (23.05.2001)

CC (2000): The Common Criteria for Information Technology Security Evaluation (CC). Version 2.1, Sep 2000. ISO/IEC 15408 1999 (E). Deutsche Übersetzung, Bundesanzeiger, August 1999. In: http://www.bsi.bund.de/cc/ (17.10.2001)

Cryptovision GmbH (2000). Glossar. In: http://www.cryptovision.com/deutsch/home/glossar.shtml (20.08.2001)

Ebeling, Adolf; Tege, Wolfram; Mahler, Peter (2001). Geld am Draht. Internetbanking: Günstig, aber auch sicher? In: c't 2001, Heft 13, S. 130- 139

Emagine Germany GmbH (2001). Sicherheit im E-Business. Von der PIN zum Public Key. In: http://www.sicherheit-im-internet.de/themes (08.08.2001)

Grimm, Rüdiger; Kahlen, Rudolf (1999). Sicherheit von Homebanking- Produkten in Deutschland. In: Braun, Heike; Husmann, Nele; Kahlen, Rudolf.Capital- Test: Wer ist der Beste? In: Capital 1999, Heft 1, S. 138- 152

Haubner, Kurt (1999). HBCI. Homebanking- Computer- Interface. HBCI- Kompendium V. 2.1 .Der Einstieg in die neue Welt des Homebanking. In: http://www.hbci-zka.de/allgemein/5.html (23.05.2001)

Haubner, Kurt (2000). HBCI. In: http://www.sixsigma.de/hbci/hbci-fly.htm (14.09.2001)

Hollich, Volker (2000). Geldtransporter. Konten mit MS Access 2000 und HBCI selbst verwalten. In: c't 2000, Heft 17, S. 192- 197

Jung, Michael; Schmidt, Frank (2000). HBCI- Homebanking Computer Interface. Seminar, Darmstadt

Kromrey, Helmut (1991). Empirische Sozialforschung. Opladen : Leske + Budrich

OFX - Open Financial Exchange (1997/2001). Latest Specification 2.0.1, July 2, 2001. In: http://www.ofx.net/ (17.10.2001)

o.V. (2001). Glossar. In: http://www.s-online-service.de/glossar_1.html (23.08.2001)

o.V. (2001). Grundlagen der Empirie. In: http://www.ikarus.uni-dortmund.de/dienstleistung/fragebogen/grundlagen/hinterg/empirie.htm (06.08.2001)

o.V. (2001). Hacker brechen in Zentralcomputer einer Großbank ein. In: http://www.heise.de/newsticker/data/wst-14.09.01-004/ (14.09.2001)

Porst, Rolf (1998). Im Vorfeld der Befragung: Planung, Fragebogenentwicklung, Pretesting. Arbeitsbericht, Mannheim

Schnell, Rainer; Hill, Paul B.; Esser, Elke (1999). Methoden der empirischen Sozialforschung. Wien: Oldenburg

Zierl, Marco (1999). HBCI- Der neue Homebanking- Standard. In: http://www.tecchannel.de/internet/62/index.html (08.08.2001)

Anhang

- Alter Fragebogen
- Neuer Fragebogen
- Anschreiben der Autoren an die Banken

ALTER FRAGEBOGEN 1998

Redaktion Capital, 50927 Köln. Rudolf Kahlen, Telefon (0221) 4908-271, Fax (0221) 4994148

CAPITAL-HOMEBANKINGTEST: FRAGEN ZU SICHERHEITSKRITERIEN

Geldinstitut: _____

Für Rückfragen: Frau/Herr _____ Telefon: _____

Capital bringt in kürze einen Homebanking-Test. In diesem Rahmen haben wir noch Fragen zur Sicherheit. Bitte kreuzen Sie die Antworten an oder formulieren Sie stichworthaft.

I. Hintergrund: Funktionalität, Ausstattung, Versorgung:

1. Welche Produkte (Software/Hardware) werden eingesetzt?

   Hersteller _____

   Produktname/Version _____

2. Welches Kommunikationsmedium ist möglich?

   a.) Internet ☐

   b.) T-Online ☐

   c.) Direkte Telefonverbindung ☐

   Sonstiges _____

3. Bei Internet: Welcher Internet-Provider wird empfohlen?

   T-Online Ja ☐ Nein ☐

   Sind andere Zugänge möglich? Ja ☐ Nein ☐

4. Sind Überweisungen von Konto zu Konto möglich? Ja ☐ Nein ☐

   Sind Wertpapierinfos/-transaktionen möglich? Ja ☐ Nein ☐

5. Welcher Standard wurde gewählt?

   HBCI Ja ☐ Nein ☐ Version _____

   Bankspezifische Lösung _____

6. Bei HBCI: Grad der Übereinstimmung mit dem Standard:

   Welche Geschäftsvorfälle, die der Standard vorsieht sind nicht realisiert?

   _____

   Welche Geschäftsvorfälle wurden über den Standard hinaus realisiert?

   _____

7. Gibt es eine spezielle Hardware-Unterstützung für die Sicherheit?

   Signaturkarte Ja ☐ Nein ☐

   DES-Karte Ja ☐ Nein ☐

   Me-Chip Ja ☐ Nein ☐

   Mondex- Chip Ja ☐ Nein ☐

   Sonstiges _____

8. Woraus besteht das Client-System?

   PC Ja □ Nein □

   ISDN/Modem-Anschluß Ja □ Nein □

   Kartenlesegerät Ja □ Nein □

   Die Kommunikationssoftware _____

   _____

   Sonstiges _____

II. Identifizierung und Kommunikationsintegrität:

1. Wie identifiziert sich der Kunde gegenüber dem Bank-Server? _____

   _____

2. Wie identifiziert sich der Bank-Server gegenüber dem Kunden? _____

   _____

3. Wie prüft der Bank-Server die Berechtigung des einzelnen Auftrages? _____

   _____

4. Wie prüfen Bank bzw. Kunde, daß Auftrag bzw. seine Erledigung unverletzt angekommen ist? _____

5. Wird eine digitale Signatur eingesetzt? Ja □ Nein □

   Welches Verfahren? _____

6. Wird PIN/TAN eingesetzt? Ja □ Nein □

7. Bei asymmetrischen Schlüsselverfahren (z.B. bei HBCI-RDH):

   Welches Zertifizierungsmanagement? _____

   Wer betreibt die Zertifizierungsstellen? _____

III. Vertraulichkeit

1. Wird die Kommunikation zwischen Client und Server verschlüsselt? Ja □ Nein □

2. Welche anderen Verfahren werden eingesetzt, um die Kommunikation vor unberechtigten Lauschern zu schützen? _____

3. Bei Verschlüsselung:

   Welche Verfahren? _____

   Wer generiert Bankschlüssel? _____

   Welche Schlüssel werden wiederverwendet, welche Schlüssel sind einmalig?

   _____

IV. Verfügbarkeit:

1. Wie oft/wie lange hat es Systemausfälle und Systemunterbrechungen gegeben?

   _____

2. Wie reagiert das Homebanking-System bei Unterbrechung gegenüber dem Kunden?

   _____

3. Welche Mechanismen bietet das Verfahren, daß bei Unterbrechung der Kunde verbindlich erfährt, was ausgeführt worden ist und was noch nicht?

   _____

V. Information und Beweise:

1. Bekommt der Kunde Orientierung seiner Aufträge? Ja ☐ Nein ☐
2. Sind Quittungen beweissicher, z.B. mit Hilfe einer digitalen Signatur? Ja ☐ Nein ☐
3. Sind die Aufträge des Kunden beweissicher, z.B. mit digit. Signatur? Ja ☐ Nein ☐

VI. Verantwortlichkeit und Haftung:

1. Hat der Kunde einen Ansprechpartner in der Bank? Ja ☐ Nein ☐

   Gibt es eine „Hotline“? Ja ☐ Nein ☐

2. Wie ist die „Hotline“ ausgestattet?

   24 Stunden in Betrieb? Ja ☐ Nein ☐

   Mit mehreren parallelen Zugängen? Ja ☐ Nein ☐

3. Hat der Kunde Stornomöglichkeiten (etwa so wie bei Lastschriftverfahren)?

   _____

Zusätzliche Anmerkungen:

_____

_____

_____

_____

BESTEN DANK FÜR IHRE MITHILFE!

BITTE FAXEN SIE DIE ANTWORTEN BIS ZUM 25. SEPTEMBER AN DIE NUMMER (0221) 4994148

NEUER FRAGEBOGEN 2001

Technische Universität Ilmenau. Prof. Dr. Rüdiger Grimm, Telefon (03677) 69-4732, Fax (03677) 69-4724

FRAGEN ZU HOMEBANKING UND SICHERHEITSSTANDARDS

Geldinstitut: _____

Name: Frau/Herr _____ Telefon: _____

E-Mail: _____

Abteilung:_____

Tätigkeitsbereich: _____

Bitte kreuzen Sie die Antworten an. Sie können auch mehrere Kreuze zu einer Fragestellung setzen. Bei Fragen ohne Möglichkeit zum Ankreuzen formulieren Sie bitte stichpunktartig.

VII. Funktionalität, Ausstattung, Versorgung:

Die Fragen des ersten Punktes sollen klären, welche Grundvoraussetzungen sowohl der Bankkunde als auch die Bank selbst für das Homebanking erfüllen müssen.

9. Welche Produkte (Software/Hardware) werden von Ihnen eingesetzt?

   Hersteller _____

   Produktname/Version _____

10. Was benötigt der Kunde?

    PC ☐ Ja ☐ Nein

    ISDN/Analog- Anschluss ☐ Ja ☐ Nein

    Kartenlesegerät ☐ Ja ☐ Nein

    Die Kommunikationssoftware _____

    _____

    Sonstiges _____

11. Welche Zugangsmöglichkeiten bieten Sie an?

    Internet ☐

    T-Online ☐

    AOL ☐

    Sonstiges _____

12. Wieviel Prozent aller Ihrer Kunden nutzen die Möglichkeit des Homebanking ? _____

13. Wie informieren Sie Ihre Kunden über die Sicherheitsstandards des Homebanking? Über:

    ☐ Mitarbeiter

    ☐ Infopost

    ☐ Broschüren

    ☐ Kontoauszüge

    ☐ Internet/Homepage

□ Newsletter

□ Plakate

Sonstiges _____

14. Welche Standards bieten Sie an?

HBCI □ Ja Version _____ Seit wann? _____

□ Nein Warum nicht? _____

Vorgesehen ab?_____

PIN/TAN □ Ja □ Nein

Bankspezifische Lösung _____

15. Wie viele Ihrer Kunden nutzen...?

HBCI (in %) _____

PIN/TAN (in %) _____

Bankspezifische Lösung (in %) _____

16. Welche Geschäftsvorfälle kann der Kunde bei Ihnen online abwickeln?

	HBCI	PIN/TAN	Bankspezifisch
Kontenabfrage	□	□	□
Kontoauszüge	□	□	□
Einzelüberweisungen	□	□	□
Sammelüberweisungen	□	□	□
Terminierte Überweisungen	□	□	□
Auslandsüberweisungen	□	□	□
Euroüberweisungen	□	□	□
Sonderform der Überweisung	□	□	□
Daueraufträge	□	□	□
Lastschriften	□	□	□
Scheckbestellung	□	□	□
Vordruckbestellung	□	□	□
Reisescheckbestellung	□	□	□
Kartenbestellung	□	□	□
Kartensperre	□	□	□
Unterkontenerstellung	□	□	□
Sorten-/Devisenkurse	□	□	□
Wertpapierinformationen	□	□	□
Wertpapiertransaktionen	□	□	□
Depotauszüge	□	□	□
Festgeld/Termineinlagen	□	□	□
Elektronisches Geld	□	□	□

Kreditrechnungen □ □ □

Sonstiges _____

_____

17. Bieten Sie Ihren Kunden eine spezielle Hardware-Unterstützung für die Sicherheit bei Homebanking?

Signaturkarte (RSA, DSA) □ Ja □ Nein

DES-Karte □ Ja □ Nein

Bankkundenkarte □ Ja □ Nein

Spezieller Chip □ Ja □ Nein

Welcher? _____

Sonstiges _____

VIII. Identifizierung und Kommunikationsintegrität:

Der Bankserver muß den Homebanking-Kunden eindeutig identifizieren können und umgekehrt. Die nächsten Fragen nehmen darauf Bezug.

8. Wie kann die Authentizität des Kunden bewiesen werden?

□ HBCI mit Signatur

□ HBCI mit DES- Karte

□ PIN/TAN

□ Sonstiges _____

9. Wie identifiziert sich der Bank-Server gegenüber dem Kunden? "Welche kryptographischen Verfahren und zugehörige Schlüssellängen werden eingesetzt?"

RSA _____ Bits DES/Triple-DES _____ Bits

DSA _____ Bits Sonstiges _____ Bits

10. In welchen Abständen wird die Identifizierung erneuert?

_____

11. Wie prüft der Bank-Server die Berechtigung des einzelnen Auftrages?

Bei HBCI_____

Bei PIN/TAN_____

Bei Bankspezifischer Lösung_____

12. Wie prüft die Bank , daß der Auftrag unverletzt angekommen ist?

_____

_____

13. Wie prüft der Kunde , daß der Auftrag angenommen wurde?

_____

_____

14. Erhält der Kunde eine digitale Quittung seines Auftrages?

□ Ja □ Nein **(weiter mit Frage II.9)**

15. Ist sie signiert? □ Ja □ Nein

16. Bei wem liegt die Beweislast im Fall von Unstimmigkeiten?

    □ Bank □ Kunde □ Sonstige _____

17. Was gilt als Beweis? _____

    _____

18. Wie schützen Sie sich und Ihre Kunden vor Maskeraden?

    Maskerade: Scheinhomepage bzw. Scheinidentität. Man gibt sich als etwas aus, was man nicht ist. Durch Irreführung des Clients können Dritte PINs und TANs abfangen und anschließend gegenüber der Bank mit einer falschen Identität auftreten.

    □ SSL mit Bankzertifikat

    □ SSL ohne Bankzertifikat

    □ Aufkaufen ähnlicher URLs

    □ Sonstiges _____

IX. Vertraulichkeit

1. Wird die Kommunikation zwischen Client und Server verschlüsselt?

   □ Ja □ Nein **(weiter mit Frage III.4)**

2. Welche Verfahren?

   □ RSA-Schlüssel □ SSL □ Sonstiges _____

3. Welche Kommunikationsteile werden verschlüsselt?

   □ Gesamte Kommunikation

   □ Der Übertragungskanal (SSL)

   □ Jede einzelne Transaktion

4. Wer generiert Ihre Bankschlüssel?

   □ Bank □ Trustcenter □ Sonstige _____

5. Wer generiert die Kundenschlüssel?

   □ Bank □ Trustcenter □ Kunde □ Sonstige _____

X. Verantwortlichkeit und Haftung:

Serviceleistungen der Banken bei Störfällen und Problemen sind in diesem Abschnitt das zentrale Thema. Welche Möglichkeiten hat der Kunde und wie helfen Sie ihm dabei?

4. Bekommt der Kunde eine Übersicht über die ausgeführten Aufträge?

   □ Ja

   □ Nein Warum nicht? _____

5. Wie reagiert das Homebanking-System bei Unterbrechungen, wie z.B. bei Systemausfall oder Verbindungsabbruch?

   □ Fehlermeldung bei Bank

   □ Fehlermeldung beim Kunden

   □ Erneute Identifizierung des Kunden

   □ Sicherung der durchgeführten Aufträge

- □ Löschen des gerade auszuführenden Vorgangs
- □ Speichern des gerade auszuführenden Vorgangs
- □ Sonstiges _____

6. Erfährt der Kunde verbindlich, was bei einer solchen Unterbrechung ausgeführt worden ist und was noch nicht? □ Nein □ Ja **(weiter mit Frage IV.5)**
7. Wie stellen Sie sicher, daß in solchen Fällen Aufträge nicht doppelt durchgeführt werden?

   _____

   _____
8. Wie gehen Sie mit Vertippen oder Verklicken seitens des Kunden um?
   - □ Zurück- Button
   - □ Abbruch - Button
   - □ Eingabe löschen - Button
   - □ Neu Laden
   - □ Sonstiges _____
9. Hat der Kunde die Möglichkeit einen Auftrag online zu stornieren (wie z.B. bei Lastschriftverfahren)? □ Ja □ Nein**(weiter mit Frage IV.10)**
10. Welche Möglichkeiten der Stornierung räumt die Bank dem Kunden hierbei ein?

    _____

    _____
11. Gibt es Vorgänge, die online vom Kunden selbst nicht storniert werden können?

    □ Ja □ Nein**(weiter mit Frage IV.10)**
12. Welche Vorgänge können vom Kunden selbst nicht storniert werden? (Begründung!)

    _____

    _____
13. Welche Fristen sind bei der Stornierung zu beachten?

    _____

    _____

XI. Persönliche Betreuung:

4. In welchen Zeitabständen werden die Kundenaufträge bearbeitet?
   (Zutreffendes bitte unterstreichen!)

   Montag bis Freitag von _____ bis _____ Uhr: Aller _____ Sek/Min/Std.
   Montag bis Freitag von _____ bis _____ Uhr: Aller _____ Sek/Min/Std.
   Samstag, Sonn- und Feiertag von _____ bis _____ Uhr: Aller _____ Sek/Min/Std.
   Samstag, Sonn- und Feiertag von _____ bis _____ Uhr: Aller _____ Sek/Min/Std.
5. Hat der Kunde einen persönlichen Ansprechpartner in der Bank? □ Ja □ Nein
6. Wann wird der Bankberater dem Kunden mitgeteilt?

   _____
7. Gibt es eine Hotline? □ Ja □ Nein

8. Ist die Hotline für den Kunden kostenpflichtig? □ Ja □ Nein
9. 24 Stunden in Betrieb? □ Ja □ Nein
10. Wie viele Anschlüsse stehen gleichzeitig zur Verfügung? _____
11. Wie viele Anrufe erhält die Hotline durchschnittlich im Monat? _____

Zusätzliche Anmerkungen Ihrerseits:

_____
_____
_____
_____
_____
_____
_____
_____

BESTEN DANK FÜR IHRE MITHILFE!

BITTE FAXEN SIE DIE ANTWORTEN BIS ZUM 10. JULI 2001 AN DIE NUMMER (03677) 69-4724

Anschreiben C. Hänseroth, A. Zobel an die Banken 14.6.2001

Sehr geehrte Damen und Herren,

wir sind zwei Studentinnen der Technischen Universität Ilmenau und studieren im 8. Semester Angewandte Medienwissenschaft. Derzeit arbeiten wir an einer Projektarbeit zum Thema „Die Entwicklung von Homebanking und den dazugehörigen Sicherheitsstandards". Im Rahmen dieses Diplomprüfungsprojektes führen wir eine Evaluation dieser Aspekte aus organisatorisch-technischer Sicht durch. Schwerpunkt dieser Umfrage stellt der Sicherheitsaspekt dar, der eingebettet in die Nutzerfreundlichkeit betrachtet werden soll. Ziel dieses Projektes ist es, Erkenntnisse über die sich weiterentwickelnde Situation von Sicherheitsstandards der Banken zu gewinnen. Darüber hinaus soll dieser wissenschaftliche Erkenntnisprozess die Veränderungen und Neuerungen der Nutzerfreundlichkeit der Homebankingangebote verdeutlichen.

Nach Abschluss unserer bisherigen Recherche folgt nun die Befragung. Wir wenden uns deshalb an Sie, als Vertreter Ihrer Einrichtung, mit der Bitte, unseren beigefügten Fragebogen auszufüllen. Ihr Institut, als eines der wichtigsten und bekanntesten in der deutschen Bankenlandschaft, nahm bereits an der 1998 durchgeführten „Capital"- Umfrage teil. Unsere Ausführungen sollen an die damalige Befragung anschließen und die Entwicklung der letzten zweieinhalb Jahre in Ihrem Hause aufzeigen. Wir erhoffen uns von Ihnen allgemeine Auskünfte zu den Sicherheitsstandards Ihrer Bank im Bereich des Homebankings aus heutiger Sicht.

Wir möchten Sie bitten den ausgefüllten Bogen bis spätestens den **10. Juli** an **0377-69-4724** zu faxen.

Bei Rückfragen wenden Sie sich bitte telefonisch an uns.

Wir würden uns sehr freuen, wenn Sie sich die Zeit für den Fragebogen nehmen würden und bedanken uns schon jetzt sehr herzlich.

Mit freundlichen Grüßen

Angelika Zobel und **Christiane Hänseroth**
Max-Planck-Ring 2 / H512
98693 Ilmenau
Telefon: 03677 / 896208
e-Mail: Angelika.Zobel@amw.stud.tu-ilmenau.de
Christiane.Haenseroth@amw.stud.tu-ilmenau.de

Anlage: Schreiben unseres betreuenden Professors

Anschreiben Prof. Grimm an die Banken 13.6.2001

Sehr geehrte Damen und Herren,

vor zweieinhalb Jahren, zur Jahreswende 1998/1999, hatte die Zeitschrift „Capital“ Sie über das Homebanking Ihres Hauses befragt und in der Titelgeschichte der Ausgabe 1/1999 Ihre Antwort zusammen mit den Antworten von etwa 30 weiteren Banken ausgewertet. Ich hatte damals als Mitarbeiter der GMD Darmstadt den Anteil der IT- Sicherheit wissenschaftlich begleitet.

Inzwischen habe ich einen Lehrstuhl für Multimediale Anwendungen mit besonderer Berücksichtigung von Finanzdienstleistungen in der TU Ilmenau und interessiere mich für die technische und organisatorische Entwicklung der Netzdienste der Finanzdienstleister.

Seit 1999 hat sich die technische Landschaft erheblich weiterentwickelt.

Im Rahmen einer studentischen Projektarbeit würde ich gerne Sie als prominenten Player befragen, wie Sie mit der technischen Entwicklung für sicheres Homebanking umgehen. Im Fokus unseres Interesses stehen dabei Fragen nach der Akzeptanz von HBCI, der Beweissicherheit von Homebanking und der persönlichen Online-Ansprache bei Problemen.

Bitte unterstützen Sie die Befragung der Studentinnen, indem Sie den beiliegenden Fragebogen nach bestem Wissen sorgfältig ausfüllen. Unser Ziel ist weder eine repräsentative Umfrage unter Banken, noch eine Wiederauflage des vergleichenden Rankings der „Capital“- Umfrage von 1998, sondern ein Erkenntnisgewinn der technischen Weiterentwicklung der prominenten Finanzdienstleister.

Das Ergebnis der Projektarbeit werden wir Ihnen selbstverständlich zukommen lassen.

Mit freundlichen Grüßen

Prof. Dr. Rüdiger Grimm