# Innovative elektronische Finanzdienstleistungen über Masseninformationssysteme

Projektbeschreibung[*]

Beitrag zu Track 2


| | |
|---|---|
| Projektleiter: | o.Univ.Prof. Dr. Hans R. Hansen |
| Berater für wissenschaftliche und praxisbezogene Fragestellungen: | o.Univ.Prof. Dr. Konrad Fuchs, Generaldirektor i. R. der Ersten österreichischen Spar-Casse |
| Wissenschaftliche Mitarbeiter: | Mag. Michael Fritscher |
| | Mag. Rainer Klimesch |
| | Mag. Oliver Kump |

Wirtschaftsuniversität Wien

Abteilung für Wirtschaftsinformatik

Augasse 2-6

A-1090 Wien

Tel. +43 (1) 31336-4443

Fax +43 (1) 31336-746



[*] Christian Bauer, Stefan Nusser und Andreas Wildberger gebührt großer Dank für die hervorragende Unterstützung.

# Inhaltsverzeichnis

# 1 Problemstellung

Zunehmende Spezialisierung und Reduzierung der Leistungserstellung auf Kernkompetenzen bei gleichzeitigem Entstehen von Allfinanzkonzernen führen zu einer Neuordnung des Finanzdienstleistungssektors. Die Entwicklungen auf dem Gebiet der Informations- und Kommunikationstechnik konfrontieren traditionelle Finanzdienstleistungsinstitute mit neuen, aggressiven Konkurrenten. Im Wettbewerb um den Kunden benutzen diese als Vertriebsmedium fast ausschließlich Masseninformationssysteme. Durch den Einsatz Internet-basierter Masseninformationssysteme eröffnen sich für traditionelle Finanzdienstleistungsinstitute große Chancen, ein umfassenderes Leistungsspektrum als Direktanbieter bereitzustellen.

Das größte Hindernis im kommerziellen Einsatz Internet-basierter Masseninformationssysteme stellt derzeit noch das geringe Vertrauen in ihre Sicherheit dar. Dies bewirkt gegenwärtig einen Wandel der Technik und der Infrastruktur. Die Teilnehmer im ehemals anonymen Netz werden durch den kommerziellen Einsatz dieser Infrastruktur zunehmend zur Identifikation und Authentifizierung gezwungen. Dies wird durch den Einsatz von digitalen Zertifikaten und Public-Key-Infrastrukturen erreicht. Das Ausstellen von Zertifikaten bedingt die Überprüfung der zu zertifizierenden Eigenschaften. Dies muß von Registrierungsstellen durchgeführt werden, die gesicherte Information besitzen. Traditionelle Finanzdienstleistungsinstitute verfügen über diese Voraussetzung und weisen darüber hinaus ein hohes Maß an Glaubwürdigkeit und Vertrauen auf. Zusätzlich dazu verfügen sie über ein gut ausgebautes Filialnetz. Informationsvorsprung und örtliche Präsenz eröffnen im Wettbewerb mit Direktbanken und anderen Direktanbietern große Chancen. Dadurch bietet sich die Gelegenheit, einen wichtigen Beitrag zur Schaffung von Rahmenbedingungen für die effiziente Nutzung von Masseninformationssystemen zu leisten.

# 2 Stand der Forschung

Grundlagen der Forschung über innovative elektronische Finanzdienstleistungen sind die Bereiche

- Masseninformationssysteme,
- Zertifizierungsdienste,
- Finanzdienstleistungen,

deren Forschungsstand und Entwicklungstendenzen im folgenden dargestellt werden.

## 2.1 Masseninformationssysteme

„Masseninformationssysteme dienen einer großen Zahl von Benutzern zur Auskunftserteilung beziehungsweise zur Durchführung von (Geschäfts-) Transaktionen in Selbstbedienung. Im Unterschied zu den üblichen Büroinformationssystemen wenden sich Masseninformationssysteme entweder überhaupt an einen anonymen Kreis von Gelegenheitsbenutzern (zum Beispiel Messe- oder Ausstellungsbesucher) oder aber an zwar registrierte Benutzer (zum Beispiel Telebanking oder Platzbuchungssysteme), die das System aber ohne persönlichen Kontakt mit dem Betreiber und oft aus großer räumlicher Entfernung, also in einer de facto anonymen Weise, benutzen.“ [vgl. HaPr94, 234]

Verwendet werden Masseninformationssysteme, um in Selbstbedienungstransaktionen Zeit und Geld zu sparen. Es kann auch die einzig wirtschaftlich sinnvolle, die effizienteste oder aber auch die bequemste Möglichkeit sein, gewisse Information oder Dienstleistungen an einen größeren Adressatenkreis zu verteilen. Von seiten der Masseninformationssystemanbieter werden Zeit- und Kostenersparnisse angestrebt. Darüber hinausgehend kann die Eröffnung eines raschen Rückkanals zu den Kunden erreicht und somit flexibler auf die individuellen Bedürfnisse der Kunden eingegangen werden.

Masseninformationssysteme können über unterschiedliche Trägertechniken wie Kioske, PC-Direktverbindungen über Telefon, kommerzielle On-line-Dienste, Internet und (Interaktives) Fernsehen realisiert werden. Hier wird der technische Rahmen auf Internet-basierte Masseninformationssysteme beschränkt.

Eine der größten Hürden für die Kommerzialisierung des Internet ist die Sicherheitsproblematik, die in zwei große Problembereiche unterteilt werden kann [vgl. Bhim96, 31; Meli95, 282; Mork96, 25 ff.]:

1. Durchführung von sicheren Transaktionen zum Abschluß von verbindlichen Rechtsgeschäften und zur Bezahlung von on-line gekauften Gütern, Dienstleistungen und Information.
2. Absicherung der betrieblichen Informationssysteme gegen unerwünschte Eindringlinge aus dem Internet (Themenbereich Firewall), worauf in Folge nicht näher eingegangen wird.

Zur Lösung dieser Probleme eignen sich besonders kryptographische Verfahren.

## 2.2 Zertifizierungsdienste

Eine Schlüsselrolle unter den kryptographischen Verfahren zur Beseitigung der zuvor beschriebenen Sicherheitsprobleme nimmt die Technik der Zertifizierung ein. Die sogenannte Public-Key-Kryptographie, auch asymmetrische Kryptographie, bildet die Grundlage für digitale Zertifikate. Verschlüsselungsverfahren, die dieser Kategorie zuzuordnen sind, beruhen auf dem Einsatz von zwei einander zugeordneten Schlüsseln, von denen der eine üblicherweise geheimgehalten und der andere öffentlich bekannt gemacht wird. Eine Nachricht, die mit dem einen Schlüssel des Paares verschlüsselt wird, kann mit dem zugehörigen zweiten Schlüssel entschlüsselt werden. Das bekannteste Beispiel für derartige Verfahren ist der nach den Initialen seiner Entwickler Rivest, Shamir und Adleman benannte RSA-Algorithmus [vgl. RSA96, Schn96].

Asymmetrische Verfahren werden zur Beseitigung der mit dem kommerziellen Internet-Einsatz einhergehenden Sicherheitsproblematik auf zwei Arten eingesetzt:

- **Ver- und Entschlüsselung**

  Nachrichten, die mit dem öffentlichen Schlüssel des Adressaten verschlüsselt sind, können nur mit dem zugehörigen privaten Schlüssel entziffert werden. Solche Nachrichten kann jede Person, die im Besitz des öffentlichen Schlüssels des Adressaten ist, erstellen. Für den Entschlüsselungsvorgang wird jedoch der geheimgehaltene private Schlüssel benötigt.

- **Digitale Unterschrift und Überprüfung**

  Nachrichten, die mit dem privaten Schlüssel des Adressaten unterschrieben sind, können von jeder Person, die im Besitz des zugehörigen öffentlichen Schlüssels ist, gelesen werden. Auf diese Weise wird die Erstellung einer fälschungssicheren *digitalen Unterschrift* möglich, die ausschließlich vom Inhaber des privaten Schlüssels erzeugt werden kann.

Mit Hilfe asymmetrischer kryptographischer Verfahren lassen sich die Anforderungen an die Übertragungssicherheit in offenen Netzwerken wie folgt erfüllen:

- Die *Vertraulichkeit* kann durch die Verschlüsselung einer Nachricht mit dem öffentlichen Schlüssel des Adressaten gewährleistet werden.
- Die *Integrität* der Übertragung kann mittels einer digitalen Unterschrift des Absenders zuverlässig geprüft werden.
- Die *Authentizität* der Kommunikationspartner kann durch Verschlüsselung und digitales Signieren einer Nachricht sichergestellt werden.
- Die *Verbindlichkeit* einer Nachricht kann mit Hilfe von digitalen Unterschriften durch die beiden Kommunikationspartner nachgewiesen werden.

Im Fall von Public-Key-Verfahren muß genauso wie bei symmetrischen Verschlüsselungsverfahren das Problem der Schlüsselverwaltung gelöst werden: Eine unabdingbare Voraussetzung für asymmetrische kryptographische Operationen ist der öffentliche Schlüssel des Adressaten. Dieser muß zwar nicht auf vertraulichem Weg übertragen werden, jedoch muß gewährleistet sein, daß der Schlüssel tatsächlich vom gewünschten Empfänger stammt.

Eine Möglichkeit, dieses Ziel zu erreichen, stellen digitale Zertifikate dar. Unter einem digitalen Zertifikat versteht man ein digitales Dokument, das den Namen und den öffentlichen Schlüssel einer Person sowie die digitale Unterschrift einer ausstellenden Zertifizierungsstelle enthält. Dadurch reduziert sich das angedeutete Problem der Schlüsselverwaltung auf den öffentlichen Schlüssel der Zertifizierungsstelle: Dieser muß auf einem sicheren Übertragungsweg zum Empfänger gelangen, beispielsweise durch persönliche Übergabe. Einmal im Besitz dieses vertrauenswürdigen Schlüssels können alle von der Zertifizierungsstelle ausgestellten Zertifikate auf ihre Echtheit hin überprüft werden.

Die Aufgaben der Zertifizierungsstelle liegen folglich in der Überprüfung der Identität der Personen. Dieser Prozeß erfolgt in Übereinstimmung mit den Geschäftsbedingungen der Zertifizierungsstelle, wo festgehalten ist, welche Voraussetzungen für den Nachweis der Identität erforderlich sind [vgl. ChFo98].

Mit der Einführung von Erweiterungsfeldern in digitale Zertifikate, definiert in der ITU-T-Empfehlung X.509 der OSI-Standards der ITU-T und ISO [vgl. ITU93], ändert sich jedoch die Rolle von Zertifizierungsstellen. Während im Falle eines Identitätszertifikates die Überprüfung der Identität des Benutzers im Vordergrund steht, müssen beim Einsatz von anwendungsspezifischen Erweiterungsfeldern die entsprechenden Eigenschaften des Inhabers überprüft werden.

Der weltweite Einsatz von Zertifikaten bedingt das Entstehen einer großen Zahl von Zertifizierungsstellen. Ein Grund dafür ist, daß eine Zertifizierungsstelle, um die Überprüfung der Identität einer Person durchführen zu können, einer gewissen regionalen Präsenz bedarf. So macht es durchaus Sinn, daß ein Unternehmen, welches Zertifizierungsdienste erbringt, tatsächlich aus einer Vielzahl lokal operierender Einheiten besteht, die unabhängig voneinander Zertifikate ausstellen. Für die Benutzer ist es jedoch nicht praktikabel, eine größere Zahl von vertrauenswürdigen öffentlichen Schlüsseln zu verwalten, da diese jeweils auf einem sicheren Kommunikationsweg übertragen werden müssen.

Diese Problematik kann mit Hilfe von Kreuzzertifikaten bewältigt werden [vgl. ITU93, Male96]. Darunter versteht man ein Zertifikat, das von einer Zertifizierungsstelle für eine weitere Zertifizierungsstelle ausgestellt wird. Mit Hilfe dieser Kreuzzertifikate kann ein Benutzer auch ein Zertifikat überprüfen, das von einer Zertifizierungsstelle ausgestellt wurde, deren öffentlichen Schlüssel er nicht auf einem sicheren Kommunikationsweg erhalten hat. Die einzige Voraussetzung für diesen Vorgang der Überprüfung ist, daß mit Hilfe von Kreuzzertifikaten eine Verbindung zu einer Zertifizierungsstelle aufgebaut werden kann, von der dem Benutzer ein vertrauenswürdiger öffentlicher Schlüssel vorliegt. Man bezeichnet die auf diese Weise aufgebaute Verbindung zwischen den Zertifizierungsstellen auch als Zertifizierungspfad oder *Vertrauenskette*. Diejenigen Zertifizierungsstellen, von denen ein vertrauenswürdiger öffentlicher Schlüssel zur Verfügung steht, werden als vertrauensmaximale Zertifizierungsstellen bezeichnet [vgl. auch RüWi95].

Mit Hilfe dieser Mechanismen kann ein System aufgebaut werden, das aus mehreren Zertifizierungsstellen besteht, die sowohl Zertifikate für Personen ausstellen als auch Verbindungen untereinander mit Hilfe

von Kreuzzertifikaten herstellen. Idealerweise kann in einem solchen System jeder Benutzer mit einer *einzigen* vertrauensmaximalen Zertifizierungsstelle die Zertifikate aller anderen Personen überprüfen. Diese Kombination aus verbundenen Zertifizierungsstellen und Benutzern wird auch als Public-Key-Infrastruktur bezeichnet [vgl. auch Schn96].

## 2.3 Finanzdienstleistungen

Finanzdienstleistungen sind alle von Banken sowie banknahen und bankfremden Substitutionskonkurrenten (Versicherungen, Kreditkartenorganisationen, ...) angebotenen Leistungen [vgl. Gabl92].

Zur Einordnung der Bankgeschäfte orientieren sich die meisten deutschsprachigen Autoren der Bankbetriebslehre an ähnlichen Schemata. Die Einschränkung auf den deutschsprachigen Raum ergibt sich vor allem durch die unterschiedlichen gesetzlichen Rahmenbedingungen in anderen Ländern, die Universalbanksysteme unterbinden. In Abbildung 1 sind die Klassifikationen der Bankgeschäfte nach Funktionen aus der Sicht unterschiedlicher Autoren gegenübergestellt:

<table>
<tr><th>Becker</th><th>Priewasser</th><th>Eilenberger</th></tr>
<tr><td>Kreditgeschäft</td><td>Passivgeschäfte</td><td>Kreditleistungen</td></tr>
<tr><td>Einlagengeschäft</td><td>Aktivgeschäfte</td><td rowspan="2">Anlageleistungen</td></tr>
<tr><td>Effektengeschäft</td><td rowspan="2">Dienstleistungen<br>im engeren Sinne</td></tr>
<tr><td>Zahlungsverkehr</td><td>Zahlungsverkehr</td></tr>
<tr><td>Auslandsgeschäft</td><td>Auslandsgeschäfte</td><td>Internationale<br>Banktätigkeit</td></tr>
<tr><td>Zusätzliche<br>Bankgeschäfte</td><td></td><td>Sonstige<br>Bankmarktleistungen</td></tr>
</table>

*Abbildung 1: Gegenüberstellung der Einteilung von Bankgeschäften nach Autoren [vgl. Beck94; Prie96; Eile96]*

Dabei zeigt sich eine erfreuliche Überdeckung, sodaß die Aufstellung eines Schemas problemlos vorgenommen werden kann. In weiterer Folge dient das detaillierte Klassifikationsschema von Becker als Grundlage.

Für die Automatisierung von Leistungen ist die Komplexität der dafür nötigen Geschäftsprozesse und Funktionen ein entscheidendes Merk-

mal. Generell gilt, je einfacher die Durchführung einer Finanzdienstleistung ist, desto leichter läßt sie sich automatisieren. Zu den Faktoren, die zu einer höheren Komplexität führen können, zählen:

- Notwendigkeit der Mitwirkung des Kunden (hoher Interaktionsgrad);
- Geringe Standardisierung der Leistung;
- Erfordernis einer großen Datenmenge zur Beschreibung und Erklärung;
- Geringe Reproduzierbarkeit.

In Abbildung 2 werden die Kerngeschäfte der Banken in Aktiv- und Passivgeschäfte unterteilt. Zusätzlich werden noch unterstützende Dienstleistungsbereiche angegeben. Der Realisierungsgrad der einzelnen Finanzdienstleistungen auf der Basis von Masseninformationssystemen wird durch die Farbe dargestellt: Leistungen mit hohem Realisierungsgrad sind schwarz, während bisher noch nicht implementierte Leistungen in hellem Grau gedruckt werden.

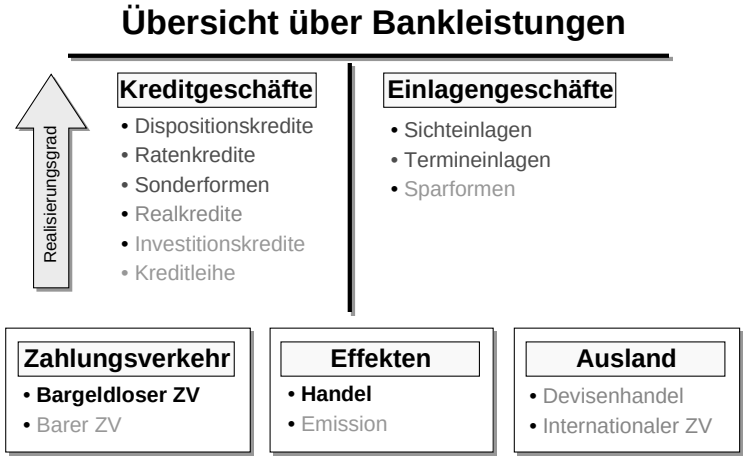


*Abbildung 2: Nach dem Realisierungsgrad mit Masseninformationssystemen geordnete Übersicht über Bankleistungen*

Aus dem oben erarbeiteten Überblick läßt sich ablesen, in welchen Bereichen Banken und andere Finanzdienstleistungsinstitute den Einsatz von Masseninformationssystemen forcieren. Vom klassischen Sortiment der Universalbanken sind vor allem die Routinetransaktionen betroffen. Diese eignen sich durch ihre geringe Komplexität besonders gut für Selbstbedienung. In diesen Bereichen besteht auch ein permanenter und exzessiver Rationalisierungsdruck, da die Abwicklung dieser Aufgaben den Banken erhebliche Kosten verursacht.

Immer mehr Direktbanken und Unternehmen aus der Informationstechnik wie Microsoft und Intuit treten als Anbieter der in Abbildung 2 dunkel dargestellten Leistungen auf. Für die Zeit nach der Umstellung auf die europäische Einheitswährung ist damit zu rechnen, daß Privatkunden verstärkt die Angebote europäischer Banken über das Internet nutzen werden. Zusätzlich dazu wächst auch im klassischen Vertrieb die Konkurrenz der heimischen Banken, da nicht nur Versicherungen, sondern auch Automobilkonzerne, Handelsunternehmen, sogar die Bahn und andere mehr in den bisherigen Banksegmenten anbieten. Besonders nachteilig wirkt sich die Konkurrenz der Allfinanzdienste und Vermögensverwalter aus, die in einem hoch spezialisierten und sehr auf den persönlichen Kontakt aufbauenden Segment den Banken die hohen Margen streitig machen. Gelänge es auch dieser Gruppe, vor den Banken ihre Dienste über Masseninformationssysteme anzubieten, so würde das den Konkurrenzdruck erheblich verstärken.

Abbildung 3 zeigt in aggregierter Form die Ergebnisse einer empirischen Studie der St. Gallen Consulting Group. Dieser Studie zufolge weisen Bankleistungen aus den Bereichen „Electronic Banking“ und „Informationsleistungen“ ein hohes Entwicklungspotential auf.

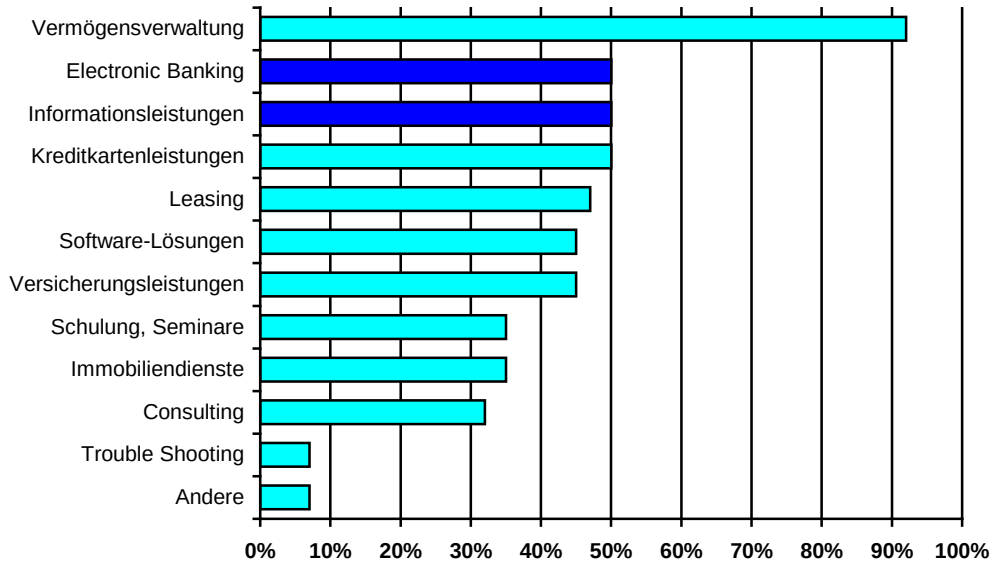


Abbildung 3: Bankleistungen der Zukunft [nach Prie94, 210]

Kurzfristig ist damit zu rechnen, daß ein Großteil der Universalbanken des deutschsprachigen Raumes mit der Zielgruppe Privatkunden einen Zugang über das Internet anbieten wird. Nach und nach wird die Sortimentsbreite der über Masseninformationssysteme angebotenen Dien-

ste erweitert werden. Eine besondere Rolle wird dabei Informationsleistungen zukommen.

## 2.4 Entwicklungstendenzen

Eine Skizzierung der Entwicklungstendenzen der beschriebenen Zertifizierungskonzepte und des geplanten Einsatzes von digitalen Zertifikaten im elektronischen Zahlungsverkehr beschließt diesen Überblick über den Stand der Forschung.

X.509-Zertifikate werden gegenwärtig in Internet-Software zur Authentifizierung der Kommunikationspartner eingesetzt und können derzeit von mehreren kommerziellen Zertifizierungsstellen bezogen werden, wobei das Netscape-RSA-Tochterunternehmen VeriSign unangefochtener Marktführer ist. Jede dieser Zertifizierungsstellen betreibt typischerweise eine unabhängige Public-Key-Infrastruktur, eine Kreuzzertifizierung mit anderen Unternehmen wird noch nicht durchgeführt [vgl. etwa Veri98].

Nationale und internationale anwendungsunabhängige Public-Key-Infrastrukturen sind gegenwärtig weltweit im Entstehen. Entsprechende Projekte sind beispielsweise ICE-TEL in Europa oder die nationale Public-Key-Infrastruktur der amerikanischen Regierung [vgl. Schn95, YoCi97]. Beide genannten Beispiele bauen auf X.509-Zertifikaten auf. Bei diesen Infrastrukturen steht in erster Linie die Identifikation der Benutzer im Vordergrund.

Der SET-Entwurf [vgl. SET97] der Kreditkartengesellschaften Mastercard und Visa hat den Aufbau von anwendungsspezifischen Public-Key-Infrastrukturen zum Ziel. SET (von engl.: Secure Electronic Transactions) bedient sich eines hierarchischen Systems von Zertifizierungsstellen, an deren Spitze eine Spitzen-Zertifizierungsstelle steht. Der für diese Arbeit bedeutsame Aspekt der SET-Entwürfe liegt in der neuen Rolle der Bank im elektronischen Zahlungsverkehr: Ihr obliegt die Zertifizierung von kreditwürdigen Personen mit Hilfe ihrer digitalen Unterschrift. Somit zertifiziert das ausgebende Finanzinstitut die rechtmäßige Eigentümerschaft einer Person an einer Karte mit Hilfe digitaler Zertifikate. Diese technische Innovation ermöglicht der Bank die Umsetzung des bestehenden Kartengeschäftes auf das Kommunikations- und Informationsmedium Internet. Diese Entwicklung führt direkt zum Themenbereich der vorliegenden Arbeit: Die neue Rolle der Finanzdienstleistungsinstitute für Masseninformationssysteme und die dadurch realisierbaren Produktinnovationen.

# 3 Projektziel und Vorgehensweise

Aus den beschriebenen Entwicklungstendenzen läßt sich ableiten, daß für Finanzdienstleistungsinstitute eine große Chance besteht, ein neues Geschäftsfeld zu erschließen: Die Erbringung von Beglaubigungsleistungen für Geschäftsparteien über Masseninformationssysteme.

Daraus ergeben sich für Finanzdienstleistungsinstitute zwei unterschiedliche, jedoch miteinander verknüpfte, Fragestellungen:

- Welche in der Realwelt bestehenden Finanzdienstleistungen können mit Hilfe innovativer Informationstechnik, insbesondere mit den Konzepten der Zertifizierung und der Erstellung digitaler Unterschriften, über Masseninformationssysteme umgesetzt werden?
- Welche Möglichkeiten zum Angebot völlig neuer Finanzdienstleistungen ergeben sich aufgrund der aktuellen Entwicklungen im Bereich der Zertifizierungs- und Registrierungsdienste?

Nur die Beantwortung dieser Fragen versetzt Finanzdienstleistungsinstitute in die Lage, auf die Herausforderungen des immer wettbewerbsintensiver werdenden elektronischen Finanzdienstleistungsmarktes aktiv einzugehen. Das vorliegende Projekt zielt darauf ab, traditionellen Finanzdienstleistern Handlungsmöglichkeiten zur Unterstützung von Geschäftstransaktionen über Masseninformationssysteme aufzuzeigen, damit sie wettbewerbsfähig bleiben und die Entwicklung elektronischer Märkte vorangetrieben wird. **Ziel dieses Forschungsvorhabens ist daher:**

> **Das Potential traditioneller und innovativer elektronischer Finanzdienstleistungen über Masseninformationssysteme zu erforschen und Handlungsempfehlungen für Finanzdienstleistungsunternehmen abzuleiten.**

Das Vorhaben läßt sich in vier Teilziele unterteilen:

**1. Evaluation vertrauensbildender Maßnahmen**

Benutzer und Betreiber von Masseninformationssystemen, insbesondere Internet-basierter, stehen vor dem Problem großer Unsicherheit bei der Beurteilung des jeweils anderen und untereinander. Vertrauen stellt eine Möglichkeit zur Reduktion von Unsicherheit bei

der Beurteilung nicht persönlich bekannter Teilnehmer von Masseninformationssystemen dar. Der Umgang mit dem Vertrauen des Kunden ist seit jeher ein wesentlicher Bestandteil bei Entscheidungen von Finanzdienstleistungsunternehmen. Dem Kunden Sicherheit, Vertrauenswürdigkeit und Glaubwürdigkeit zu kommunizieren ist ein elementares Anliegen. Beispielsweise sind diese im Bereich Vermögensverwaltung und Informationsleistungen grundlegende Voraussetzungen für das Zustandekommen von Geschäftsabschlüssen. Vertrauen stellt somit die Basis nicht nur für zahlreiche Finanzdienstleistungen in ihrer derzeitigen Form dar, sondern wird auch in Zukunft bei der Schaffung neuer Dienste in Masseninformationssystemen eine essentielle Rolle spielen.

Ziel ist es, vertrauensbildende Maßnahmen zu identifizieren und in Hinblick auf die Entwicklung neuer Finanzdienstleistungen über Masseninformationssysteme zu evaluieren.

Zur Zielerreichung wird folgende Vorgehensweise gewählt: Grundlage bildet die Aufarbeitung ökonomischer und technischer Konzepte des Vertrauensmanagements. Dabei werden zwei Ansätze verfolgt: Analyse von Konzepten, die dazu dienen können, Vertrauen in Masseninformationssysteme, deren Betreiber und Benutzer sicherzustellen. Ergänzend zu dieser Literaturaufarbeitung sollen in einer Studie vertrauensbildende Maßnahmen aus der täglichen Praxis des Finanzdienstleistungssektors erhoben werden.

## 2. Ausarbeitung organisatorischer Rahmenbedingungen

Finanzdienstleistungsinstitute, insbesondere Banken, verfügen zusätzlich zu dem Vertrauen, das ihnen vom Kunden entgegengebracht wird, über einen weiteren Vorteil: In vielen Fällen steht ein Filialnetz zur Verfügung, manchmal auch mit internationalen Repräsentanzen, das die Bank physisch in die Nähe des Kunden bringt. Im Fall der Ausstellung digitaler Zertifikate ist der einmalige Kontakt, die sogenannte Registrierung des Inhabers, von wesentlicher Bedeutung. Abbildung 4 zeigt das von der PKIX-Arbeitsgruppe (Public Key Infrastructure X.509) der IETF (Internet Engineering Task Force) erarbeitete Modell einer Public-Key-Infrastruktur.

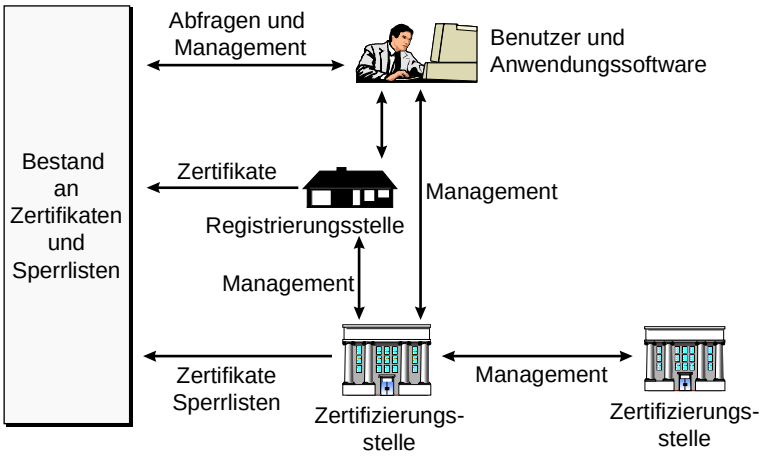


*Abbildung 4: Zertifizierungsstellen und Registrierungsstellen*

Der wesentliche Aspekt dieses Entwurfes liegt in der Trennung zwischen Zertifizierungsstelle (führt die Erstellung der Zertifikate durch) und Registrierungsstelle (überprüft die zertifizierten Eigenschaften der Realwelt). Es ist daher abzuklären, welche Dienstleistungen in den Bereichen Zertifizierung und Registrierung Banken übernehmen sollen.

Ziel ist es, organisatorische Rahmenbedingungen für Zertifizierung und Registrierung durch Finanzdienstleistungsinstitute auszuarbeiten.

Zur Zielerreichung wird folgende Vorgehensweise gewählt: Grundlage bildet die Analyse des Aufbaues und der Entwicklung existierender Public-Key-Infrastrukturen und des Zusammenspiels unabhängiger Unternehmen bei der Bildung von Vertrauensketten sowie die Beschreibung gängiger Praktiken der Kreuzzertifizierung. Dazu ist es notwendig, eine eingehende Literaturanalyse anhand von Standardentwürfen, Berichten und Empfehlungen einschlägiger Gremien und Organisationen vorzunehmen. Zu diesen Gremien und Organisationen zählen unter anderem das World Wide Web Consortium (W3C), die International Organization for Standardization (ISO), die International Telecommunication Union (ITU), die Internet Engineering Task Force (IETF), das European Committee for Banking Standards (ECBS). Deren Ergebnisse sind auf Vollständigkeit, Widerspruchsfreiheit sowie Anwendbarkeit auf den Finanzdienstleistungssektor zu prüfen und sollen entsprechend adaptiert in die Erstellung eines Schemas organisatorischer Rahmenbedingungen für Finanzdienstleistungsinstitute einfließen.

### 3. Untersuchung bestehender Finanzdienstleistungen

Finanzdienstleistungsinstitute setzen seit geraumer Zeit Masseninformationssysteme für den Vertrieb von Routinetransaktionen ein, da sich diese durch ihre geringe Komplexität besonders gut für Selbstbedienung eignen. Der Umfang von elektronischen Finanzdienstleistungen, die über Internet-basierte Masseninformationssysteme angeboten werden, steigt ständig und beschränkt sich nicht mehr nur auf stark standardisierte Produkte. Von großer Bedeutung für dieses Forschungsvorhaben sind diejenigen Geschäftsbereiche, in denen die Leistung der Finanzdienstleistungsinstitute bereits jetzt auf dem Vertrauen aufbaut, das ihnen aufgrund ihrer besonderen Rolle im Wirtschaftsgeschehen entgegengebracht wird. Durch die neuen Techniken eröffnen sich Möglichkeiten, komplexere und beratungsintensivere Finanzdienstleistungen über Masseninformationssysteme anzubieten.

Ziel ist es, bestehende Finanzdienstleistungen auf ihre Eignung zum Vertrieb über Masseninformationssysteme zu untersuchen.

Zur Zielerreichung wird folgende Vorgehensweise gewählt: Grundlage bildet die Identifikation geeigneter Geschäftsbereiche. Dabei werden zwei Ansätze verfolgt: Der Aufbau eines detaillierten Kriterienkataloges, der die speziellen Anforderungen an elektronische Finanzdienstleistungen spezifiziert und die Erfassung und Bewertung identifizierter Bereiche ermöglicht. Ein qualitativer Überblick der über Internet-basierte Masseninformationssysteme angebotenen Finanzdienstleistungen ergänzt die theoretische Analyse.

### 4. Erforschung innovativer elektronischer Finanzdienstleistungen

In vielen Transaktionen üben Finanzdienstleistungsinstitute seit jeher die Rolle von Trusted-Third-Parties aus. Akzeptkredit, Avalkredit oder Dokumentenakkreditiv sind Beispiele für Geschäftsbereiche, in denen die Finanzdienstleistungsinstitute von dem Vertrauen, das ihnen aufgrund ihrer Reputation entgegengebracht wird, profitieren. Glaubwürdigkeit und Vertrauen prädestiniert die Finanzdienstleistungsinstitute für die Leistungserbringung von Beglaubigungsdiensten durch den Einsatz von Zertifikaten und digitalen Unterschriften. Die aktuellen Entwicklungen in diesem Bereich eröffnen Perspektiven für das Angebot völlig neuer Finanzdienstleistungen über Masseninformationssysteme. Zertifikate können nicht nur zur Authentifizierung der an einer Transaktion beteiligten Parteien eingesetzt werden, sondern darüber hinaus auch zur Integration zusätzlicher rele-

vanter Information über die zu zertifizierende Person. So kann ein Finanzdienstleistungsinstitut beispielsweise mittels digitaler Unterschrift die Bonität von Personen zertifizieren. Diese technische Innovation eröffnet Möglichkeiten für neue Transaktionsformen, innovative elektronische Finanzdienstleistungen und neue Geschäftsbereiche.

Ziel ist es, innovative elektronische Finanzdienstleistungen, neue Transaktionsformen und neue Geschäftsbereiche zu erforschen, und auf ihre praktische Umsetzung hin zu analysieren.

Zur Zielerreichung wird folgende Vorgehensweise gewählt: Grundlage bildet die Ermittlung der Anforderungen an Beglaubigungsleistungen. Dabei werden zwei Ansätze gewählt: Identifikation notwendiger Schlüsseltechniken für die Erstellung von Beglaubigungsleistungen. Darunter fallen Standards und Formate zur Verkodierung von Zertifikaten, Sperrlisten sowie Protokolle für den Austausch von Zertifikaten und die Abwicklung der den Beglaubigungsleistungen zugrundeliegenden Transaktionen. Ergänzend zur Literaturaufarbeitung soll eine Untersuchung bestehende und in Entwicklung befindliche Leistungen kommerzieller Zertifizierungsstellen in Hinblick auf innovative, mit finanziellen Transaktionen in Verbindung stehenden Beglaubigungsleistungen erheben. Die solcherart ermittelten Anforderungen an Beglaubigungsleistungen müssen einer Durchführbarkeitsanalyse unterzogen werden. Die Überprüfung der Umsetzbarkeit der auf konzeptueller Ebene beschriebenen Beglaubigungsleistungen soll durch die Entwicklung prototypischer Realisierungen mit frei verfügbaren Komponenten erfolgen.

Die erarbeiteten Ergebnisse der einzelnen Teilziele bilden die Grundlage für die Erstellung eines Vorgehensmodells, mit dem das Potential innovativer elektronischer Finanzdienstleistungen über Masseninformationssysteme erschlossen wird. Dazu ist es notwendig, die strukturierten und klassifizierten Untersuchungsergebnisse der einzelnen Teilziele zur Ausarbeitung von Kriterien heranzuziehen, die eine Vorgehensweise für die Aussprache von Handlungsempfehlungen aus den Ergebnissen ableiten läßt. Eine Akzeptanzanalyse der für Masseninformationssysteme identifizierten Geschäftsbereiche und Beglaubigungsleistungen soll bei Finanzdienstleistungsinstituten und Kunden in Form von Umfragen, Fallstudien und Interviews durchgeführt werden. Gemeinsam mit den Ergebnissen der zuvor angeführten Teilziele soll die empirisch abgesicherte Studie der Akzeptanz traditioneller und innovativer elektronischer Finanzdienstleistungen über Masseninformationssyste-

me Finanzdienstleistungsunternehmen Handlungsempfehlungen in die Hand geben.

Abbildung 5 gibt Projektziel und Teilziele sowie Vorgehensweise und gewählte Methodik wieder.


*Abbildung 5: Projektziel, Teilziele und Vorgehensweise*

# 4 Zeit- und Arbeitsplan

Die Aktivitäten zur Zielerreichung des Forschungsvorhabens werden in vier Phasen unterteilt. Das Projekt beginnt mit Juli 1998. In Phase I werden vertrauensbildende Maßnahmen durch die Aufarbeitung ökonomischer und technischer Konzepte und die Erhebung angewandter Konzepte des Finanzdienstleistungssektors evaluiert.

Daran anschließend folgt ab Dezember 1998 Phase II. Die organisatorischen Rahmenbedingungen werden durch die Analyse von Public-Key-Infrastrukturen, der Bildung von Vertrauensketten sowie der Leistungen kommerzieller Zertifizierungsstellen ausgearbeitet. Gleichzeitig wird die Untersuchung bestehender Finanzdienstleistungen durch Identifikation von geeigneten Geschäftsbereichen und die Ermittlung von Anforderungen an Beglaubigungsleistungen durchgeführt.

Phase III, die im Juni 1999 beginnt, hat die Erforschung innovativer elektronischer Finanzdienstleistungen zum Gegenstand. Über einen Zeitraum von acht Monaten werden die Anforderungen an Beglaubigungsleistungen erhoben, spezifiziert und einer Durchführbarkeitsanalyse unterzogen. Phase III endet mit der Entwicklung prototypischer Realisierungen ausgewählter innovativer elektronischer Finanzdienstleistungen.

In Phase IV werden ab Februar 2000 die Ergebnisse der Teilziele wie auch die Akzeptanzanalyse der innovativen elektronischen Finanzdienstleistungen in ein Vorgehensmodell eingebracht und daraus abzuleitende Handlungsempfehlungen erarbeitet. Ende Juni 2000 wird das Projekt abgeschlossen.

Die einzelnen Phasen des Forschungsvorhabens werden in Abbildung 6 auf der nächsten Seite zusammenfassend dargestellt.

| **Aktivität** | **Phase** | | | |
|---|---|---|---|---|
| | **I** | **II** | **III** | **IV** |
| **Evaluation vertrauensbildender Maßnahmen** | | | | |
| Aufarbeitung ökonomischer und technischer Konzepte | | | | |
| Erhebung angewandter Konzepte | | | | |
| **Ausarbeitung organisatorischer Rahmenbedingungen** | | | | |
| Analyse existierender Public-Key-Infrastrukturen | | | | |
| Analyse der Bildung von Vertrauensketten | | | | |
| Praktiken der Kreuzzertifizierung | | | | |
| **Untersuchung bestehender Finanzdienstleistungen** | | | | |
| Identifikation von Geschäftsbereichen | | | | |
| Untersuchung der Eignung zum Vertrieb | | | | |
| **Erforschung innovativer elektronischer Finanzdienstleistungen** | | | | |
| Anforderungen an Beglaubigungsleistungen | | | | |
| Analyse der praktischen Umsetzung | | | | |
| **Potential innovativer elektronischer Finanzdienstleistungen** | | | | |
| Ausarbeitung von Kriterien | | | | |
| Ableitung von Vorgehensweisen | | | | |
| Aussprache von Handlungsempfehlungen | | | | |

*Abbildung 6: Zeit- und Arbeitsplan*

# 5 Literaturverzeichnis

[Beck94] Becker, H. P.: Bankbetriebslehre. 2. Auflage, Kiehl, Ludwigshafen 1994.

[Bets95] Betsch, O.: Wettbewerbsveränderungen auf den Finanzdienstleistungsmärkten und der Umbruch der Vertriebssysteme. In: Betsch, O.; Wiechers, R.: Handbuch Finanzvertrieb. Fritz Knapp Verlag, Frankfurt am Main 1995, S. 3 - 21.

[Bhim96] Bhimani, A.: Securing the Commercial Internet. In: Communications of the ACM, June 1996/Vol. 39, No. 6, S. 29 - 35.

[Bitz97] Bitz, M.: Finanzdienstleistungen. 3. Auflage, Oldenbourg, München, Wien 1997.

[ChFo98] Chokhani, S.; Ford, W.: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework. Internet-Draft, 1998.
In: http://www.ietf.org/html.charters/pkix-charter.html

[Eile96] Eilenberger, G.: Bankbetriebswirtschaftslehre: Grundlagen - internationale Bankleistungen - Bank-Management. 6. Auflage, Oldenbourg, München, Wien 1996.

[ElFr97] Ellison, C.; Frantz, B.; Lampson, B.; Rivest, R.; Thomas, B.; Ylonen, T.: Simple Public Key Certificate. Internet-Draft, 1997.
In: http://www.clark.net/pub/cme/html/spki.html

[Gabl92] Gabler-Wirtschafts-Lexikon. Gabler, Wiesbaden 1992.

[Garf95] Garfinkel, S.: PGP: Pretty Good Privacy. O'Reilly, Sebastopol 1995.

[HaBa95] Hansen, H.R.; Bauer Ch.: Masseninformationssysteme bei Banken. Eigenverlag der Abteilung für Wirtschaftsinformatik, WU Wien 1995.

[Hans95a] Hansen, H.R.: A Case Study of a Mass Information System, In: Information & Management, 28th Vol. 1995, No. 2.

[Hans95b] Hansen, H.R.: Conceptual Framework and Guidelines for the Implementation of Mass Information Systems, In: Information & Management, 28th Vol. 1995, No. 3.

[Hans96a] Hansen, H.R.: Wirtschaftsinformatik I. Grundlagen betrieblicher Informationsverarbeitung. 7. Auflage, Lucius & Lucius Verlag, Stuttgart 1996.

[Hans96b] Hansen, H.R. und Mitarbeiter: Klare Sicht am Info-Highway: Geschäfte via Internet & Co. Orac-Verlag, Wien 1996.

[Hans96c] Hansen, H.R.: Geschäftspotentialanalyse für neue interaktive Dienste in Österreich - Ergebnisse einer Haushalts- und Unternehmensbefragung, In: Der Wiener IT-Kongreß 96, Globale Informationsverarbeitung - Auswirkungen der Internationalisierung, Bd. 1, ADV-Verlag, Wien 1996.

[HaPr94] Hansen, H.R.; Prosser, A.: Entwicklung und Betrieb von Masseninformationssystemen. Schlußfolgerungen aus dem Studenteninformationssystem der Wirtschaftsuniversität Wien. In: Wirtschaftsinformatik 35 (1994) 3, S. 233-242.

[HoFo96] Hously, R.; Ford, W.; Polk, W.; Solo, D.: Internet Public Key Infrastructure - Part 1: Certificate and CRL Profile. Internet-Draft, 1996.
In: http://www.ietf.org/html.charters/pkix-charter.html

[ITU93] ITU-T Recommendation X.509: Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. ITU, 1993 and ISO/IEC 9594-8, 1993.

[ITU95] ITU-T Draft Amendments to ITU-T X.509 and ISO/IEC 9594-8 on Certificate Extensions, 1995.

[MaAr96] MacGregor, R.; Aresi, A.; Siegert, A.: www.security - How To Build a Secure World Wide Web Connection. Prentice Hall, New Jersey 1996.

[Male96] Maley, J.: Enterprise Security Infrastructure. In: Proceedings of the Fifth Workshops on Enabling Technologies: Infrastructure for Collaborating Enterprises, Stanford, California 1996.

[Meli95] Meli, H.: Sicherheitsarchitektur für eine Electronic Mall. In: Schmid, B. et al.: Electronic Mall: Banking und Shopping in globalen Netzen. Stuttgart 1995, S. 279 - 314.

[Mork96] Mork, S.: Protecting Information Assets. In: The Bankers Magazine, January/February 1996, S. 23 - 30.

[Nuss98] Nusser, S.: Sicherheitskonzepte für WWW-Informationssysteme. Springer Verlag, Heidelberg 1998.

[Pelz82] Pelzmann, L.: Empirische Wirtschaftspsychologie. Habilitationsschrift, Wien 1982.

[Prie94] Priewasser, E.: Die Priewasser-Prognose - Bankstrategien und Bankmanagement 2009. Fritz Knapp Verlag, Frankfurt am Main 1994.

[Prie96] Priewasser, E.: Bankbetriebslehre. 5. Auflage, Oldenbourg, München, Wien 1996.

[RiLa96] Rivest, R.; Lampson, B.: SDSI - A Simple Distributed Security Infrastructure. In: Proceedings of DIMACS Workshop on Trust Management in Networks, South Plainfield, NJ, 1996.

[RSA96] RSA Laboratories: Frequently Asked Questions 3.0 on Cryptography. 1998.
In: http://www.rsa.com/ rsalabs/newfaq/

[RüWi95] Rüppel, R. A.; Wildhaber, B.: Public Key Infrastructure – Survey and Issues. In: Horster, P. (Hrsg.): Trust Center – Grundlagen, rechtliche Aspekte, Standardisierung und Realisierung. Vieweg Verlag, Wiesbaden 1995.

[Schn95] Schneider, W.: Internetworking Certification Infrastructure for Europe. In: Horster, P. (Hrsg.): Trust Center – Grundlagen, rechtliche Aspekte, Standardisierung und Realisierung. Vieweg Verlag, Wiesbaden 1995.

[Schn96] Schneier, B.: Applied Cryptography - Protocols, Algorithms, and Source Code in C. 2nd Edition, John Wiley & Sons, Inc., New York 1996.

[SET97] Secure Electronic Transactions: Book 2: Programmer's Guide. Version 1.0, 31. Mai 1997.
In: http://www.mastercard.com/set/specs2.html
In: http://www.setco.org/set_specifications.html

[Veri98] O.V.: VeriSign Certification Practice Statement. 1998.
In: http://www.verisign.com/repository

[Vögt97] Vögtle, M.: Intelligente Informationssysteme für das Bankgeschäft: eine theoretische und empirische Analyse ihrer strategischen Bedeutung. Rudolf Haufe Verlag, Freiburg i. Br. 1997.

[YoCi97] Young, A.; Cicovic, N.K.; Chadwick, D.: Trust Models in ICE-TEL. In: Proceedings of Internet Society Symposium on Network and Distributed System Security. 1997.