Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen

Jan Muntermann, Heiko Roßnagel und Kai Rannenberg

Chair of Mobile Commerce & Multilateral Security
Goethe University Frankfurt
Gräfstr. 78
60054 Frankfurt/Main
[janlheikolkair]@whatismobile.de

Zusammenfassung: Mobile Push-Dienste helfen Informationen zeitnah bereitzustellen, was besonders bei Finanzinformationsdiensten interessant ist, da sie stark von zeitkritischer Informationsverarbeitung geprägt sind. Dieser Beitrag zeigt auf, welche Finanzinformationsdienste um mobile Unterstützung erweitert werden sollten, um für Anwender und Anbieter solcher Dienste einen Mehrwert zu erzielen. Eine Analyse dieser Dienste zeigt, dass mit zunehmendem Spezialisierungs- und Personalisierungsgrad der übertragenen Informationen bzw. mit abnehmendem Zeitfenster zwischen Informationszustellung und erforderlichen Finanztransaktionen das Potential mobiler Finanzinformationsdienste zunimmt, dieses jedoch mit einer Steigerung des Sicherheitsbedarfs einhergeht.

1 Einleitung

Die zeitnahe Vorsorgung mit entscheidungsrelevanten Informationen ist einer der kritischen Erfolgsfaktoren für eine erfolgreiche Wertpapieranlage. Gerade in Zeiten hoch volatiler Kapitalmärkte sind nicht-institutionelle Investoren hierbei auf eine möglichst zeit- und ortsunabhängige Versorgung angewiesen. Die Verfügbarkeit Web-basierter Informations-, Überwachungs- und Benachrichtigungssysteme hat in den vergangenen Jahren zu einer erheblichen Verbesserung der Informationsversorgung der Anleger geführt [LooCha02]. Diese klassischen Client/Server-Architekturen können jedoch weder zeitlich noch örtlich unabhängige Erreichbarkeit realisieren und eignen sich damit nur begrenzt für die automatisierte Zustellung zeitkritischer anlagerelevanter Informationen.

Die zunehmende Verfügbarkeit leistungsfähiger mobiler Endgeräte sowie drahtloser Übertragungstechnologien macht ihren Einsatz für finanzwirtschaftliche Informationsdienste interessant. Gerade im Umfeld des Wertpapierhandels, der in hohem Maße von der Verarbeitung zeitkritischer Informationen wie Kursschwankungen, Ad-hoc-Nachrichten oder der Unter- bzw. Überschreitung gesetzter Limits beeinflusst wird, verspricht der Einsatz dieser Dienste eine zeitnahe Informationsversorgung der Anleger, wodurch diese ihre Reaktionszeiten maßgeblich verkürzen können. Dabei ist allerdings darauf zu achten, dass Finanzinformationen sowohl auf dem Übertragungsweg, als auch auf dem mobilen Endgerät geschützt werden müssen. Da die Informationen direkt Wertpapiertransaktionen auslösen, verhindern oder zumindest beeinflussen können, sind an ihre Sicherheitseigenschaften

auch bei drahtloser Übertragung und Empfang hohe Anforderungen zu stellen, um möglichen und verschiedentlich reizvollen Missbrauch zu verhindern.

Ziel dieses Beitrags ist eine Darstellung, welche finanzwirtschaftlichen Informationsdienste sich aufgrund ihrer speziellen Eigenschaften für den mobilen Einsatz eignen und wie sie zu sichern sind bzw. gesichert werden. Dazu gibt Kapitel 2 einen Überblick über Finanzinformationsdienste und ihre Einsatzmöglichkeiten im mobilen Umfeld. In Kapitel 3 werden dann die an diese Informationsdienste zu stellenden Sicherheitsanforderungen betrachtet, sowie die gängigen bei Finanzinformations-Providern im Einsatz befindlichen Techniken auf die Einhaltung dieser Anforderungen untersucht. Kapitel 4 beschreibt eine technische Infrastruktur, die in der Lage ist, die in Kapitel 3 gestellten Sicherheitsanforderungen zu erfüllen. Kapitel 5 schließt den Text mit einer Zusammenfassung der Ergebnisse ab und gibt einen Ausblick auf künftig nötige Arbeiten.

2 Mobile Finanzinformationsdienste

Mobile Finanzinformationsdienste sind immer noch eine relativ neue Erscheinung innerhalb der Finanzinformationssysteme. Deswegen gibt Abschnitt 2.1 eine kurze finanzwirtschaftliche Einordnung, bevor in 2.2 und 2.3 die Bereiche Portfolioüberwachung und Portfolioanalyse im Hinblick auf mobile Unterstützung genauer untersucht werden. 2.4 und 2.5 schließen das Kapitel mit Beurteilungen aus Anleger- wie Informationsanbietersicht ab.

2.1 Finanzwirtschaftliche Einordnung

Durch die Allokation von Finanztiteln bestimmen Investoren die Zusammensetzung ihres Wertpapierportfolios. Hierbei legen die Anleger die unterschiedlichen Anteile risikoreicher und risikoarmer Finanztitel innerhalb ihres Portfolios fest, um insgesamt eine möglichst effiziente Relation aus erwartetem Ertrag und Risiko zu realisieren [ElmKi03]. Zur Umsetzung der in der Asset Allocation festgelegten Anlagestrategie sind Anleger auf leistungsfähige Informationsdienste angewiesen. Hierbei können sie einerseits auf Pull-Informationsdienste zurückgreifen, bei denen sie aktiv Informationen anfordern. Andererseits kann durch die Verwendung von Push-Informationsdiensten eine zeitnahe und ereignisgesteuerte Informationsversorgung realisiert werden. Zugestellte Marktinformationen können eine Umschichtung gegenwärtiger Portfoliopositionen nahe legen, was dann durch entsprechende Transaktionsdienste unterstützt wird. Diese Dienste übertragen die Transaktionsdaten an die Ausführungs- und Abwicklungssysteme der Broker bzw. Banken, die sich ihrerseits für die Durchführung der Transaktionen verantwortlich zeigen [Gom00]. Den entsprechenden Ablauf zeigt Abbildung 1.

Abbildung 1: Prozesse im Asset Management

Durch die Bereitstellung leistungsfähiger, Web-basierter I&K-Systeme konnten die Prozesse im Bereich der Informations- und Transaktionsdienste in den letzten Jahren entscheidend verbessert werden. Allerdings vermögen es auch diese Systeme nur begrenzt, Zeit- und Ortsunabhängigkeit zu realisieren, die insbesondere bei hochvolatilen Wertpapieren erforderlich ist. Nicht-institutionellen Anlegern ist es deshalb normalerweise nicht möglich, das Marktgeschehen fortwährend zu überwachen und zeitnah zu reagieren. Diese Lücke kann durch den Einsatz mobiler Informationsdienste geschlossen werden.

Jedoch stoßen auch diese mobilen Informationsdienste an ihre Grenzen, wenn Kurse so schnell reagieren, dass neue Informationen innerhalb von Sekunden an den Finanzmärkten verarbeitet sind. Aufgrund der Dominanz der institutionellen Anleger im Segment der Blue Chips kommt das Potential mobiler Informationsdienste eher bei Nebenwerten zum Tragen, bei denen mit einer verzögert einsetzenden Informationsverarbeitung zu rechnen ist [Oerk99].

2.2 Portfolioüberwachung

Ein System zur Portfolioüberwachung prüft fortwährend und automatisiert Portfoliozustände und relevante Marktereignisse und informiert über deren Eintreten. Der Anleger bestimmt dabei den Umfang der Überwachung, beispielsweise durch die Festlegung statischer und dynamischer (Kurs)-Limits. Zudem muss der Anleger das Medium festlegen, über das er beim Eintreten dieser Ereignisse (z.B. dem Erreichen eines überwachten Aktienkurses) informiert werden soll. Während die Konfiguration der zu überwachenden Ereignisse beispielsweise konventionell über Web-basierte Systeme erfolgen kann, muss die Informationszustellung beim Eintreten der Ereignisse über Push-Dienste wie E-Mail oder SMS realisiert werden.

Die Portfolioüberwachung dient der individuellen portfolioabhängigen Benachrichtigung bei sich ändernden Portfoliozuständen (z.B. Kursentwicklungen der Portfoliopositionen) oder kritischen Markt- (z.B. Konjunkturprognosen) und Unternehmensinformationen (z.B. Ad-hoc-Meldungen). Letztgenannte können entscheidenden Einfluss auf die kurzfristige Kursentwicklung von Wertpapieren haben, z. B. wenn publizierte Quartalsergebnisse nicht der gängigen Markterwartung entsprechen.

2.2.1 Mehrwert mobiler Unterstützung

Die Portfolioüberwachung liefert Informationen, die eine schnelle Reaktion durch den Anleger ermöglichen. Die Überwachung geschieht hierbei automatisch in den Back-end-Systemen der Online-Broker und Banken, die bei Eintreten eines überwachten Ereignisses den Anleger durch einen Push-Service informieren. Gerade durch die mobile Unterstützung bei der Informationszustellung realisiert die Portfolioüberwachung ihren Mehrwert, nämlich die automatische Informationsbereitstellung zum Zeitpunkt entscheidender Marktereignisse und nicht erst zum Zeitpunkt, zu dem sich der Anleger aktiv über seine Portfoliozustände informiert. Dieses Potential wird durch Abbildung 2 verdeutlicht, die die Aktienkursentwicklung während eines Tages nach der Publikation einer Ad-hoc-Meldung zeigt.

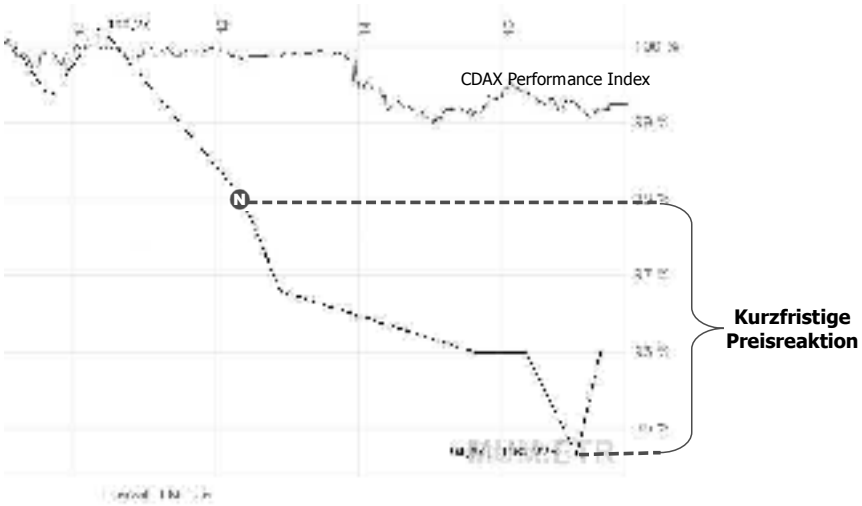

Abbildung 2: Intraday Aktienkursverlauf von Mensch & Maschine am 21.6.2004

Die Ad-hoc-Meldung wurde am 21.6.2004 um 12:23 Uhr von Mensch & Maschine publiziert. Der weitere Kursverlauf zeigt eine Kursreaktion von gut 3%. Eine generelle negative Kursentwicklung lässt sich am Markt (CDAX Performance Index) nicht beobachten, was einen allgemeinen Markttrend ausschließt. Eine rechtzeitige Benachrichtigung eines Investors, der Anteile des Unternehmens hält, hätte entsprechende Verluste verhindern können, was das Potential eines geeigneten mobilen Überwachungs- und Benachrichtigungssystems verdeutlicht.

Von entscheidender Bedeutung ist bei der Limit- und Ereignisüberwachung, dass zugestellte Informationen sich auf vergleichsweise geringe Datenvolumina beschränken. Auch diese Eigenschaft kommt dem mobilen Einsatz entgegen, da die Übertragungsraten aktueller Mobilfunksysteme noch vergleichsweise gering ausfallen bzw. sich die Größe übertragener Nachrichten auf eine bestimmte Zeichenanzahl (z.B. 160 Zeichen bei SMS) beschränkt [Schi00].

2.2.2 Technische Realisierung mobiler Unterstützung

Die in 2.2.1 aufgezeigten Arten der Portfolioüberwachung setzen eine zeitnahe, automatisierte Zustellung von Informationen voraus. Diesen Anforderungen kann durch den Einsatz mobiler Dienste mit Push-Funktionalität begegnet werden. Hierfür stehen innerhalb der Mobilfunktechnik mehrere Dienste bereit, die sich jedoch hinsichtlich ihrer spezifischen Eigenschaften (z.B. übertragbarer Datenumfang, Sicherheitseigenschaften) voneinander unterscheiden.

Ein Dienst, der die Anforderungen hinsichtlich Push-Funktionalität unterstützt, ist der Short Message Service (SMS)[1]. Eine besondere Eigenschaft des SMS ist die Beschränkung der Nachrichtenlänge auf 160 Zeichen. Diese Einschränkung konnte durch die Einführung der Dienste EMS und MMS teilweise aufgehoben werden, da diese neben größerem Nachrichtenumfang auch die Übertragung multimedialer Inhalte wie beispielsweise Bilder ermöglichen. Da die Benachrichtigungen der Portfolioüberwachung größtenteils sehr kurze Informationstexte enthalten, stellt die Zeichenbegrenzung des SMS-Dienstes kaum ein Hindernis für den Einsatz als Benachrichtigungssystem dar.

Durch die in der Version 2.0 des Wireless Application Protocol definierten Push-Services wird ein Framework bereitgestellt, das in klassischen Client/Server-Umgebungen Dokumente vom Server an mobile Engeräte versenden kann [WaFo01b]. Obwohl dieses Framework 2001 vom WAP Forum veröffentlicht wurde, mangelt es derzeit noch an entsprechenden Diensten. Auch dass seit einiger Zeit geeignete Endgeräte mit WAP 2.0-Unterstützung verfügbar sind, hat diesen Tatbestand nicht ändern können. Die Open Mobile Alliance (OMA) hat als Nachfolgeorganisation des WAP Forums bereits eine Erweiterung des WAP Push Frameworks vorgestellt, welches durch die Einführung der sog. E-Mail Notification (EMN) über eingegangene E-Mails informiert [OMA02]. Hierbei kommt ein auf Clientseite, d.h. auf dem mobilen Endgerät, befindlicher EMN User Agent zum Einsatz, der über ein Push Proxy Gateway über eingegangene E-Mails informiert wird. Der EMN User Agent benachrichtigt den auf dem mobilen Endgerät befindlichen E-Mail-Client, die neue Nachricht vom E-Mail-Server abzuholen. Diese Technologie erfordert einerseits geeignete Endgeräte mit EMN-Unterstützung und einen konventionellen E-Mail-Client (z.B. mit POP3-Unterstützung), ermöglicht aber andererseits die Nutzung bestehender E-Mail-Server. Es bleibt jedoch kritisch anzumerken, dass über alle eingehenden E-Mails informiert wird, d.h. die Benachrichtigungen der Portfolioüberwachung drohen bei Eingang vieler E-Mails unterzugehen.

2.3 Portfolioanalyse

Die Portfolioanalyse hilft dem Anleger, positive und negative Zusammenhänge bei der Ertrags- und der Risikoentwicklung zu erkennen. Neben einfachen Kursinformationen sollen dem Anleger unterschiedliche Kennzahlen und Charts dabei helfen, möglichst gute Investitionsentscheidungen treffen zu können. Allen diesen Informationen ist gemein, dass sie unterschiedliche Fristigkeiten aufweisen, d.h. dass sie sich in unterschiedlicher Häufigkeit ändern, bzw. aufgrund hohen Berechnungsaufwands nur periodisch berechnet werden [DaGeM01].

Im Allgemeinen kommen für die Portfolioanalyse Pull-Dienste zum Einsatz, d.h. der Anleger wird bewusst Analyseinformationen über sein Portfolio bzw. über die darin enthaltenen Wertpapiere abfragen, da er z.B. mittels der Portfolioüberwachung über ein relevantes Marktereignis informiert wurde.

[1] Dieser GSM Phase 1 Dienst, der in den vergangenen Jahren enorme Steigerungsraten verzeichnen konnte, stellt heute eine nicht zu vernachlässigende Einnahmequelle der Mobilfunkbetreiber dar.

2.3.1 Mobile Unterstützung und ihr Mehrwert

Für Portfolioanalysen existieren seit einiger Zeit Dienste im Web, die bereits eine enorme Verbesserung der Informationsversorgung auf Anlegerseite zur Folge hatten [Patel00]. Während sich für den Einsatz im stationären Internet auch Analysen für längerfristige Anlageziele, d.h. zur Unterstützung strategischer Entscheidungen eignen, liegt die Fokussierung bei den mobilen Finanzinformationsdiensten auf der Unterstützung kurzfristiger Entscheidungen. Bereits durch die Einführung der Web-basierten Systeme konnte der Entscheidungshorizont für eine mögliche Umschichtung von Portfolios maßgeblich verkürzt werden, wobei die Prüfung einerseits von den gehaltenen Asset-Klassen und ihren Risikoeigenschaften, andererseits von der Verfügbarkeit entsprechender Systeme zur Portfolioanalyse abhängig ist [BoMe00]. Gerade bei kurzfristigem Informationsbedarf stoßen die klassischen Web-basierten Systeme an ihre Grenzen, wenn sich der Anleger spontan und schnell informieren will, ohne aber über eine Internet-Anbindung zu verfügen. Ist eine kurzfristige Umschichtung der Portfoliopositionen erforderlich, kann eine Berechnung von optimalen Kauf- bzw. Verkaufsvolumen helfen, eine effiziente Portfoliostruktur mit optimaler Rendite-Risikorelation zu erreichen. Da solche Berechnungen lange Kurshistorien als Datenbasis erfordern [Shar66], empfiehlt sich hierbei eine serverseitige Berechnung und eine anschließende Übertragung der Berechnungsergebnisse, da sonst große Datenmengen zum Client übertragen werden müssen.

Darüber hinaus kann die Veröffentlichung neuer Unternehmenskennzahlen eine spontane Informationserhebung über ein bestimmtes Unternehmen erfordern. Hierbei ist es für den Anleger wichtig, sich einen schnellen Überblick über die wichtigsten Unternehmenskennzahlen verschaffen zu können.

Die mobile Portfolioanalyse wird vor allem dann angewendet, wenn Anleger kurzfristig und unterwegs auf portfoliorelevante Marktentwicklungen reagieren müssen. Hierbei es ist besonders wichtig, dass die Informationsversorgung schnell an die aktuellen Anforderungen angepasst werden kann, beispielsweise wenn Anleger bei Kauf- und Verkaufentscheidungen unterstützt werden sollen. Die mobile Portfolioanalyse kann hierbei helfen, den Anlegern bei hektischen Entscheidungen Entscheidungsunterstützung anzubieten.

2.3.2 Technische Realisierung mobiler Unterstützung

Im mobilen Umfeld steht eine Reihe von Diensten bereit, eine mobile Portfolioanalyse zu realisieren. Da bei der Portfolioanalyse stets ein akuter Informationsbedarf vom Anleger ausgeht, sind geeignete Technologien im Bereich der mobilen Pull-Dienste zu suchen.

Das Wireless Application Protocol (WAP) wurde entwickelt, um den frühen GSM-Datendiensten mit ihren geringen Datenübertragungsraten zu genügen[2]. Ziel war die Entwicklung einer Protokollfamilie, die Zugriff auf eigens dafür entwickelte Seiten im Internet ermöglicht. Auch wenn WAP nicht die hohen Erwartungen hinsichtlich seiner Verbreitung erfüllen konnte, eignet sich die Technologie durchaus für die mobile Portfolioanalyse, da hier die mangelnde multimediale Unterstützung eine untergeordnete Rolle spielt.

[2] WAP kann jedoch unabhängig von der Netztechnik auch in anderen Netzen eingesetzt werden.

Zurzeit ist ein Trend hin zu mobilen Endgeräten (Smartphones bzw. PDAs mit eingebautem Modem) erkennbar, welche mittels fast vollwertigem HTML-Browser Zugriff auf bestehende Web-Inhalte ermöglichen. Diese Entwicklung wird auch dadurch gespeist, dass mit GPRS und künftig UMTS Datendienste zur Verfügung stehen, die auch größere Datenmengen und somit aufwendigere Inhalte in vertretbarer Zeit drahtlos übertragen können. Mit dem Einsatz der bewährten Web-Technologie steht somit ein Rahmen für die mobile Portfolioanalyse zur Verfügung, der sich mittlerweile im stationären Web bei einigen Online-Brokern etablieren konnte [HuRe01].

2.4 Beurteilung aus Anlegersicht

Der Bedarf an optimaler Informationsversorgung in zeitlicher und qualitativer Dimension ist gerade beim Eintreten kritischer Ereignisse am Kapitalmarkt von hoher Bedeutung. Die Verfügbarkeit mobiler Informationsdienste kann zu einer Verbesserung der Informationslage der Investoren beitragen, da durch die zeitnahe ortsunabhängige Informationsübermittlung entscheidungsrelevante Informationen den Anleger früher erreichen. Durch die automatisierte Selektion relevanter Informationen und deren Übermittlung können beim Einsatz mobiler Informationsdienste Transaktionskosten auf Anlegerseite reduziert werden. Einerseits können Suchkosten vermindert werden, da dem Anleger die portfoliorelevanten Informationen automatisch als Push-Dienst zugestellt werden. Andererseits ermöglicht die durch das Backend-System durchgeführte Selektion und Filterung relevanter, d.h. dem Anleger zu übermittelnder Informationen, eine Reduzierung von Kontrollkosten. Diese Selektion kann sich z.B. an den im Portfolio befindlichen Wertpapieren orientieren. Erst durch Kombination aus Selektion relevanter Informationen durch das Backend und drahtloser zeitnaher Übertragung der Benachrichtigungen an den Anleger kann der Mehrwert mobiler Finanzinformationsdienste zur Entfaltung gebracht werden. Die mobile Übertragung kann die Zeitspanne zwischen dem Zeitpunkt der Bekanntmachung und Zustellung zum Adressaten verkürzen und somit eine Steigerung der Markttransparenz bewirken [PiBoR96].

2.5 Beurteilung aus Anbietersicht

Der aktuelle Preiswettbewerb zwischen den Online-Brokern hat zu teilweise ruinöser Preispolitik geführt. Gleichzeitig haben die schlechte Entwicklung an den Kapitalmärkten und die damit verbundene Zurückhaltung bei den Anlegern enorme Einkommenseinbußen bei den Transaktionsgebühren nach sich gezogen [DAI04]. Die Online-Broker und -Banken sehen sich daher in diesem Geschäftsbereich mit großen Herausforderungen konfrontiert.

Die Entwicklung und Einführung leistungsfähiger mobiler Finanzinformationsdienste kann hierbei neben z.B. Kostenreduktion eine Antwort auf die schwierige Situation sein.

Die neuen mobilen Informationsdienste können eine Verbesserung des Leistungsangebots der Online-Broker darstellen und somit zu einer Erhöhung der Attraktivität des Gesamtangebots führen sowie einen reinen Preiswettbewerb verhindern. Zudem kann durch das Angebot individueller, hoch personenbezogener Informationsdienste, wie sie die Portfolioüberwachung und Portfolioanalyse darstellen, eine höhere Kundenbindung erreicht werden.

Darüber hinaus ist zu erwarten, dass eine schnellere und bessere Informationsversorgung und somit schnellere Reaktionsfähigkeit sich in einer Steigerung der Transaktionszahlen niederschlägt. Durch die proaktive und zeitnahe Übermittlung transaktionsrelevanter Informationen kann die Kundenzufriedenheit gesteigert werden, weil hierdurch potentiell Verluste vermieden werden können. Diese Entwicklung kann den Einbrüchen der Umsatzzahlen bei den Online-Brokern entgegen wirken, da diese direkt ihre Umsätze durch die gestiegenen Transaktionszahlen steigern können.

3 Sicherheitsanforderungen an mobile Finanzinformationsdienste

Die aufgezeigten Potentiale mobiler Finanzinformationsdienste lassen sich nur dann erfolgreich nutzen, wenn Anwender den eingesetzten Systemen zu einem gewissen Maße vertrauen. Dementsprechend muss eine sichere Infrastruktur verwendet werden, die die Schutzinteressen aller Parteien berücksichtigt. Angesichts dessen lohnt sich eine genaue Analyse, welche Parteien in welchen Situationen welche Vorteile verbuchen können sowie ob und wie „Mehrseitige Sicherheit“ [Rann00] erreichbar ist.

In diesem Kapitel wird deshalb in 3.1 zur Einführung kurz ein einfaches Schadensszenario beschrieben, dann werden in 3.2 allgemeine Sicherheitseigenschaften auf mobile Finanzinformationsdienste „heruntergebrochen“. In 3.3 werden die Anforderungen im Bereich Portfolioüberwachung und Portfolioanalyse genauer diskutiert. Diese Diskussion dient in 3.4 als Grundlage für eine Einschätzung der Sicherheitseignung der gegenwärtig bei mobilen Finanzinformationssystemen eingesetzten Technologien und möglicher Verbesserungen.

3.1 Ein einfaches Schadensszenario zur Einführung

Ein wegen der am Aktienmarkt erlebten Volatilitäten nervöser Anleger A registriert sich für einen Push-Dienst zur Portfolio-Überwachung: Wenn der Kurs der N-Aktie innerhalb einer Stunde um mehr als 10% fällt, bekommt A eine SMS, die den Kursverfall berichtet. An einem für A ohnehin hektischen Tag T kurz vor einer längeren Flugreise in die USA bekommt A die Kursverfallsnachricht und stößt eilig und mit Verlust die N-Aktien ab. Später stellt sich heraus, dass die SMS mit dem Marktverlauf nichts zu tun hatte (tatsächlich hatten N-Aktien am Tag T nach ruhigem Marktverlauf fester geschlossen und am Tag darauf zu einem Höhenflug angesetzt). Die SMS erweist sich als eine leicht modifizierte Kopie einer Tage zuvor versandten Kurswarnung, auf die Anleger A damals bereits reagiert hatte. Eine Rückfrage beim Finanzinformationsdienstleister ergibt, dass sich dort niemand für die Nachricht verantwortlich fühlt, und es kann auch nicht nachgewiesen werden, dass sie von ihm kam.

3.2 Allgemeine Sicherheitseigenschaften und mobile Finanzinformationsdienste

Anhand vier allgemeiner Sicherheitseigenschaften [Rann00] lassen sich die Sicherheitsanforderungen geeigneter Finanzinformationsdienste für den mobilen Einsatz strukturieren.

3.2.1 Vertraulichkeit

Vertraulichkeit bezeichnet den Schutz vor der unbefugten Preisgabe von Informationen an Dritte. Dies können Mitarbeiter des Finanzinformationsproviders, des Mobilfunkanbieters oder sonstige dritte Personen sein. Im Rahmen von Finanzinformationsdienstleistungen betrifft dies beispielsweise, den Schutz des Anlegers davor, dass seine Portfoliobestände oder Handelsstrategien fremden Personen und Institutionen bekannt werden.

3.2.2 Verfügbarkeit

Verfügbarkeit ist der Schutz vor unbefugter Vorenthaltung von Informationen oder Diensten, etwa Informationsdiensten. So kann es für einen Anleger schädlich sein, zeitkritische Informationen verzögert oder eventuell überhaupt nicht zu erhalten. Da Finanzinformationsdienste unmittelbaren Einfluss auf eventuell folgende Transaktionen haben können, kann die mangelnde Verfügbarkeit eines Dienstes erheblichen Schaden für den Anleger verursachen, etwa, wenn er versäumt, bei einer Kursabwärtsbewegung rechtzeitig zu verkaufen.

3.2.3 Integrität

Integrität schützt vor unbefugter Manipulation von Daten und Systemen. Integre Daten sind weder während der Übermittlung noch auf dem Endgerät durch Unbefugte verändert worden. Integrität ist bedeutsam, denn gefälschte oder unvollständige Informationen können zu falschen Anlageentscheidungen führen und somit finanzielle Verluste der Anleger bewirken. Da unbefugte Manipulationen außerhalb vertrauenswürdiger Umgebungen nicht verhindert werden können, müssen Integritätsmaßnahmen unbefugte Änderungen an Informationen (und Systemen) erkennen und diese dokumentieren, damit die Nutzer gewarnt sind.

3.2.4 Zurechenbarkeit

Zurechenbarkeit bezeichnet die Tatsache, dass Aktionen oder Dokumente den urhebenden Personen oder Institutionen zugeordnet werden können, so dass diese im Nachhinein nicht in der Lage sind, die Durchführung der jeweiligen Transaktion zu bestreiten. Speziell wenn Kunden sich über irreführende Informationen oder unautorisierte Handelstransaktionen beschweren, die ihnen finanzielle Schäden verursacht haben, ist es wesentlich zu wissen, auf wen eine Information zurückgeht, bzw. wer eine Transaktion veranlasst hat.

3.3 Kurze Sicherheitsanalyse mobiler Finanzinformationsdienste

Entlang der durch die vier allgemeinen Sicherheitseigenschaften gegebenen Struktur werden in diesem Abschnitt die Sicherheitsanforderungen der mobilen Finanzinformationsdienste Portfolioüberwachung (3.3.1) und Portfolioanalyse (3.3.2) genauer untersucht.

3.3.1 Portfolioüberwachung

Im Bereich der Portfolioüberwachung werden meist einzelne Nachrichten zu aktuellen Ereignissen mithilfe von Push-Technologien versandt. Die Sicherheitsanforderungen hängen zunächst von der Relevanz des Portfolios bzw. der übermittelten Nachrichten ab, aber auch von dem Bezug, den die übermittelten Nachrichten zum Portfolio haben.

So muss beispielsweise für Limit-Nachrichten ein hohes Maß an Vertraulichkeit gewährleistet werden, denn jede Information, die an den Anleger gesendet wird, lässt direkte Rückschlüsse auf seine im Portfolio befindlichen Anlagepapiere zu. Die dadurch gewonnenen Informationen können direkt gegen den Portfolioinhaber eingesetzt werden, etwa indem Vermögensschwankungen daraus abgeleitet und ggf. publik gemacht werden. Sie können auch indirekt eingesetzt werden, etwa als Grundlage späterer Angriffe auf die Integrität ausgewählter Informationen, etwa indem Informationen zu ausgewählten Titeln verfälscht oder frei erfunden werden.

Bei Ad-hoc-Meldungen ist das nötige Maß an Vertraulichkeit geringer einzuschätzen als bei Limits, da der Anleger i.A. nicht nur Ad-hoc-Meldungen zu Titeln in seinem Portfolio erhält. Dennoch ist es möglich, anhand der empfangenen Ad hoc Mitteilungen Rückschlüsse auf die im Portfolio befindlichen Titel zu ziehen. Wenn allgemeine Nachrichten und Prognosen keine Rückschlüsse auf die Portfoliozusammensetzung oder die Anlagestrategie zulassen, ist es nicht unbedingt nötig, diese Daten vertraulich zu behandeln.

Ein Ausfall der Verfügbarkeit von Diensten in Push-Szenarien kann weit reichende Folgen haben und z.B. erhebliche finanzielle Schäden hervorrufen, wenn Limit-Nachrichten (versehentlich oder absichtlich) verzögert werden.

Integrität wird in vielen Fällen das primäre Schutzziel bei Informationsdiensten zur Portfolioüberwachung sein, denn Portfolioüberwachung dient ja gerade dazu, auf der Basis von Informationen über das Überwachte Entscheidungen (eventuell großen finanziellen Umfangs) zu treffen, und dies oft unter Zeitdruck.

Auch Zurechenbarkeit ist wichtig, denn gerade wenn unter Zeitdruck entschieden werden muss und keine Zweit- oder Drittquellen zur Kontrolle befragt werden können, ist die Herkunft der Informationen (etwa von einer als vertrauenswürdig einschätzten Quelle, die ggf. auch haftbar gemacht werden kann) bedeutsam.

3.3.2 Portfolioanalyse

Portfolioanalysen verraten, wenn sie eng an die Zusammensetzung eines bestimmten Portfolios geknüpft sind, sehr viel über dessen Zusammensetzung und ggfs. auch über die Handelsstrategie des Eigentümers des Portfolios. Insofern stellen sich Vertraulichkeitsanforderungen in dem Maße, in dem der Eigentümer diese Informationen vertraulich halten will.

Die Anforderungen an Integrität und Zurechenbarkeit von Portfolioanalysen wachsen mit der Bedeutung, etwa der Kostenträchtigkeit, der Entscheidungen, die diese Portfolioanalysen beeinflussen. Die Anforderungen an die Integrität werden auch umso größer, je be-

grenzter die (zeitlichen) Möglichkeiten der Empfänger sind, weitere Analysen zum Vergleich einzuholen.

Die Anforderungen an die Verfügbarkeit von Portfolioanalysen hängen davon ab, wie nötig der Anleger sie für seine Entscheidungen braucht und wie zeitkritisch sie sind.

3.4 Sicherheitseignung eingesetzter und verfügbarer Technologien

Im Folgenden wird untersucht, inwieweit die heutigen von Finanzinformationsdienstleistern eingesetzten bzw. einfach verfügbaren Technologien die geforderten Schutzziele erfüllen und für welche Finanzinformationsdienste sie sich (ggf. mit Ergänzungen) eignen.

3.4.1 Short Message Service (SMS)

Als attraktive Variante für Finanzinformationsdienstleistungen bietet sich die Nutzung des Kurzmitteilungsdienstes (Short Message Service – SMS) an. Hierbei werden die Daten vom Informationsdienstanbieter an den Betreiber eines SMS-Servicecenters (meist ein Mobilkommunikationsanbieter) gesendet; dort werden sie über Datenleitungen weitergeleitet und schließlich per Funk an das mobile Endgerät übermittelt. Dabei liegen die Daten, abgesehen von der Funkübertragung im Klartext vor. Dementsprechend kann von einer Erfüllung des Schutzziels der Vertraulichkeit nicht ausgegangen werden, solange nicht Schutzmaßnahmen auf Anwendungsebene getroffen werden [FuFri01].

Auch eine Veränderung der Daten auf dem Kommunikationsweg ist für den Anleger nicht erkennbar oder nachvollziehbar. Ebenso wenig ist eine effektive Kontrolle der Zurechenbarkeit der Nachricht möglich, denn das Absenderfeld der SMS, das i.A. die Mobilfunknummer des Absenders enthält, kann im SMS-Servicecenter beliebig manipuliert werden, und Angebote, SMS unter beliebigen Absenderkennungen zu verschicken, finden sich im Internet[3].

Ein Lösungsansatz ist die Verwendung gängiger Signaturverfahren [RaFRo03], die auf Applikationsebene die Integrität und Zurechenbarkeit schützen. Dann muss aber das mobile Endgerät über Software zur Verifikation der Signaturen verfügen. Dies stellt aufgrund der großen Heterogenität mobiler Endgeräte eine enorme Hürde dar. Ähnliche Probleme ergeben sich auch, wenn die Vertraulichkeit von Nachrichten von der Quelle bis zur Senke durch ein Verschlüsselungsverfahren auf Anwendungsebene geschützt werden soll.

Die Verfügbarkeit von SMS-Nachrichten ist prinzipiell nicht gegeben: Es gibt keine Garantie, dass Nachrichten ankommen, und auch eine zeitnahe Übermittlung ist nicht zwingend gegeben, da SMS-Nachrichten in Abhängigkeit von der Auslastung des Mobilfunknetzes verschickt werden [Schi00] [GSM01].

Aufgrund ihrer mangelnden Sicherheitseigenschaften eignet sich SMS bestenfalls für den Einsatz bei Portfolioüberwachungsdiensten, die nur geringe Vertraulichkeitsanforderungen stellen (z.B. allgemeine Konjunkturprognosen). Darüber hinaus sollte die Anwendung

[3] Etwa bei Sportlogos.de [Sport03] unter dem in diesem Zusammenhang leicht irreführenden Titel „anonyme SMS“

auch nicht zu hohe weitere Sicherheitsanforderungen, speziell im Bereich Verfügbarkeit, nach sich ziehen, oder aber SMS sollte nur als einer von mehreren parallelen (nicht alternativen) Kommunikationskanälen eingesetzt werden.

3.4.2 WAP

WAP 1.X verwendet WTLS, eine an SSL angelehnte Sicherheitsschicht, um die Sicherheit beim Datentransport zu gewährleisten [Schi00]. Das WTLS Protokoll unterstützt primär die Schutzziele der Zurechenbarkeit, Vertraulichkeit und Integrität.

Doch auch hier entsteht ein Problem, wenn der WAP-Server nicht im sicheren Rechenzentrum des Finanzinformationsdienstleisters steht und über einen direkten Anschluss an die Infrastruktur des Mobilfunkproviders verfügt. In diesem Fall geht nämlich die Ende-zu-Ende-Sicherheit genau dort verloren, wo der WAP-Server die Daten entschlüsselt [FuFri01]. WAP 2.0 verwendet TLS um die Kommunikation zu schützen und ermöglicht so eine echte Ende-zu-Ende-Sicherheit [OMA04].

3.4.3 Webbasierte Lösungen

Gerade das Zusammenwachsen von PDAs und Mobilfunkgeräten ermöglicht völlig neue Perspektiven für mobile Finanzinformationsdienstleistungen. Neuere Mobilfunkgeräte, wie beispielsweise der T-Mobile MDA (ein PocketPC-PDA mit zusätzlicher GSM-Funktionalität) verfügen über Webbrowser, die in der Lage sind, die übertragenen Daten mittels Secure Socket Layer (SSL) zu verschlüsseln. Sie ermöglichen so eine echte Ende-zu-Ende-Sicherheit auf dem Übertragungsweg.

Prinzipiell sind bei Web-basierten Lösungen alle Sicherheitsanforderungen so gut wie im „klassischen“ Internet erfüllbar, allerdings müssen sowohl der Dienstanbieter als auch das mobile Endgerät die entsprechenden Sicherheitstechnologien unterstützen.

4 Eine sichere Infrastruktur für mobile Finanzinformationsdienste

Während für Pull-Dienste ausreichende Sicherheitstechnologien vorhanden sind, besteht für die Push-basierten Dienste noch ein Bedarf an geeigneten Sicherheitsvorkehrungen, um insbesondere die Authentizität und Integrität der übertragenen Finanzinformationen zu gewährleisten. Weiterhin kann durch die Push-basierten Informationsdienste ein Bedarf für anschließende Transaktionsdienste erzeugt werden. Daher ist es wichtig, dass die Infrastruktur eine geeignete Integration von Informationsdiensten und Transaktionsdiensten ermöglicht. Da die Investitionsentscheidungen meistens recht zeitnah gefällt werden müssen, sollte der Prozess – beginnend mit der Notifikation bis hin zum Abschluss der resultierenden Transaktion – so zeitsparend wie möglich sein [MuGü04]. Weiterhin sollte gewährleistet werden, dass die Notifikations- und Transaktionsdienste mit möglichst vielen mobilen Endgeräten benutzt werden können.

Abbildung 3 zeigt eine mögliche technische Infrastruktur, die die genannten Anforderungen erfüllt. Diese Infrastruktur basiert auf der Annahme, dass der Investor über eine SIM-

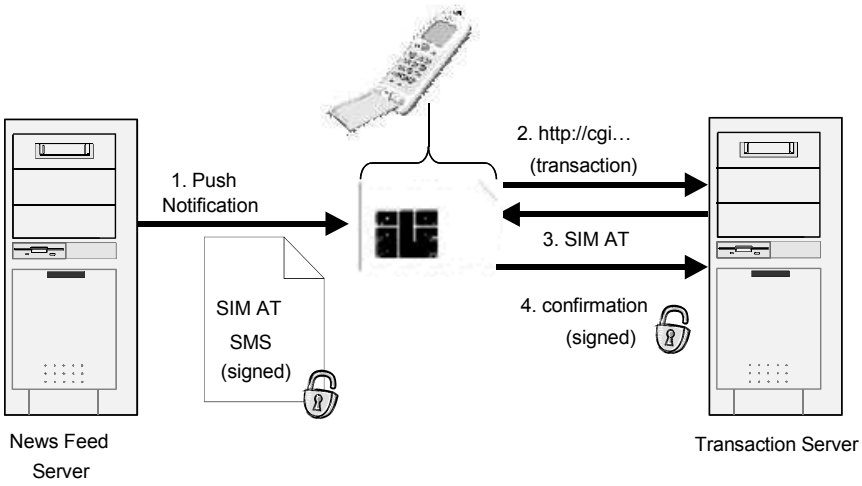

Abbildung 3: Systeminfrastruktur für sichere mobile Finanzinformationsdienste

Karte verfügt, die in der Lage ist elektronische Signaturen zu erzeugen und zu verifizieren. Solche signaturfähigen SIM-Karten existieren, sind aber nicht weit verbreitet. Im Rahmen des von der EU geförderten Projekts Wireless Trust for Mobile Business (WiTness) [Witn04] wurde eine solche SIM-Karte entwickelt. Sie ist in der Lage RSA Signaturen [RSA78] zu erzeugen und ermöglicht darüber hinaus eine 3DES Verschlüsselung. Um eine möglichst breite Basis an mobilen Endgeräten verwenden zu können, empfiehlt sich eine Lösung auf Basis des SIM-Application Toolkit [GuCr02].

Bei Eintritt eines für den Investor relevanten Ereignisses sendet der Service Provider eine signierte SMS an den Investor. Durch die digitale Signatur bestätigt der Finanzinformationsprovider, dass er der Urheber der Nachricht ist und schützt die enthaltenen Finanzinformationen auf dem Übertragungsweg zum Endgerät vor ungewollten Veränderungen. Nach erfolgreicher Prüfung der Signatur kann der Investor dann den Brokerage Client starten und eine Verbindung zum Transaktions-Server herstellen. Die Authentifizierung erfolgt durch die Eingabe einer PIN. Der Investor kann nun nötige Transaktionen anweisen und diese Anweisungen signieren. Der Transaktionsserver überprüft die Signaturen und vollendet die Transaktion. Durch die Signatur ist sowohl die Zurechenbarkeit als auch die Integrität der Transaktion gewährleistet.

Zwei Varianten sind zu untersuchen, was die Prüfung der Signatur bei Empfänger angeht. Diese Aufgabe könnte im mobilen Endgerät erledigt werden oder aber auf der SIM. Für die Prüfung auf der SIM spricht, dass sie vermutlich schwerer zu manipulieren ist. Außerdem ist die Prüfung dann endgeräteneutral und muss nicht für jedes Endgerät neu implementiert werden. Ein Nachteil ist jedoch, dass Kunden, die am Service teilnehmen wollen, vorher eine neue SIM bekommen müssen. Für die Prüfung auf dem Endgerät spricht, dass für High-End-Geräte vermutlich in absehbarer Zeit zwei standardisierte Plattformen (PocketPC Phone Edition und Symbian) existieren werden und nur für diese zwei Platt-

formen die Software benötigt wird. Im übrigens machen bei Vielnutzern die Kosten eines neuen Gerätes nur einen kleinen Teil der Gesamtkosten aus, wenn man dort die laufenden Kosten einbezieht.

Es ist auch im Sinne der Verfügbarkeit dafür Sorge zu tragen, dass die „gepushten" Nachrichten die Empfänger erreichen. Da der SMS-Dienst normalerweise keine Garantien bezüglich Auslieferung an Empfänger vorsieht, ist eine vollständige Realisierung schwierig. Allerdings ist eine Ergänzung denkbar, bei der die Zweistufigkeit der Auslieferung von MMS-Nachrichten genutzt werden kann. MMS-Nachrichten werden im Allgemeinen nicht direkt an den Empfänger geschickt, sondern auf dem MMS-Server zwischengespeichert. Das Empfängergerät wird informiert, dass eine neue Nachricht vorliegt und kann sie dann beim Server abholen. Wird die Information, ob die Nachricht abgeholt wurde, dem Sender zugänglich gemacht, kann dieser bei kritischen Verzögerungen Redundanzmaßnahmen ergreifen, also je nach Sicherheitspolitik etwa die Nachricht erneut senden oder auf einen alternativen Nachrichtenweg ausweichen. Es gibt auch Länder wie Südafrika, in denen Absender einer SMS eine Bestätigung der Auslieferung an das Empfängergerät bekommen. Dies löst das Problem der Verfügbarkeit zwar auch nicht vollständig, kommt aber einer Lösung schon näher.

5 Zusammenfassung und Ausblick

Die mobile Versorgung mit Finanzinformationen bietet Anreize und Vorteile, sowohl für Anleger als auch für Anbieter solcher Dienstleistungen. Die zeitnahe und ortsunabhängige Übermittlung von kritischen Anlageinformationen, lässt Anleger über eine verbesserte Informationsversorgung verfügen, was zu besseren Investitionsentscheidungen führen kann. Für Anbieter können mobile Finanzinformationsdienste zu einer Steigerung der Attraktivität des Angebotes führen, und es kann durch personalisierte Dienste die Kundenbindung erhöht werden.

Für den mobilen Einsatz eignen sich im Bereich der Portfolioüberwachung push-basierte Dienste, die eine zeit- und ortsunabhängige Informationszustellung verwirklichen.

Für die Sicherheitsanforderungen an mobile Finanzinformationsdienste gilt, dass mit steigender Spezialisierung und Personalisierung der abgefragten Informationen bzw. mit sinkender Zeitspanne zwischen Informationseingang und Entscheidungsbedarf auch der Bedarf an Sicherheit wächst.

Die existierenden Pull-Dienste stellen hierbei im Wesentlichen angepasste Abbildungen bestehender Web-Lösungen dar, die sich nicht die spezifischen Potentiale der mobilen Infrastrukturen zu Nutze machen. Während für diese Dienste zwar komplexe, aber etablierte Technologien zur Erfüllung der Sicherheitsanforderungen existieren, erfüllen die bei Push-Diensten in der Praxis eingesetzten Verfahren die wünschenswerten Sicherheitseigenschaften prinzipiell nicht oder noch nicht in ausreichendem Maße. Die besonderen Potentiale der Push-Dienste und der damit verbundene Mehrwert für Anleger lassen sich so nicht in vollem Umfang realisieren. Sie müssen um Sicherheitsmaßnahmen wie Verschlüsselungs- und Signaturverfahren sowie anwendungsbezogene Redundanzkonzepte ergänzt werden.

Literatur

[BoMe00] Bodie, Zvi; Merton. Robert C.: Finance. Prentice Hall, Upper Saddle River, New Jersey, 2000.

[DaGeM01] Dacorogna, Michel; Gençay, Ramazan; Müller, Ulrich A.; Olsen, Richard B.; Pictet, Olivier V.: An Introduction to High-Frequency Ad hoc Nachricht Finance. Academic Press, San Diego, Califonia, 2001.

[DAI04] Deutsches Aktieninstitut: Vertrauensschaffung bedarf eines langen Atems. DAI-Kurzstudie 2/2004 zu Aktionärszahlen, Frankfurt am Main, 2003.

[DeuBu01] Deutscher Bundestag: Gesetz zur digitalen Signatur v. 16.5.2001. http://www.bmwi.de/bmwa/generator/Navigation/Service/Gesetze/rechtsgrundlagen-informationsgesellschaft,did=22112.html, (2004-08-05).

[ElmKi03] Elmiger, Gregory; Kim, Steve S.: RiskGrade Your Investments. John Wiley, New Jersey, 2003.

[FuFri01] Fuchß, T.; Fritsch, L.: Endgeräte für den M-Commerce: Defizite und Aussichten. In KES 1, S. 6-8. SecuMedia, Ingelheim, 2001.

[Gom00] Gomber, Peter: Elektronische Handelssysteme – Innovative Konzepte und Technologien im Wertpapierhandel. Physica, Heidelberg, 2000.

[GSM01] GSM Association: Identification of Quality of Service aspects of popular services (GSM and 3G), Version 3.0.0. http://www.gsmworld.com/documents/ireg/ir41.pdf, 2001, (2004-08-05).

[GuCr02] Guthery, S. B. and M. J. Cronin, Mobile Application Development with SMS and the SIM Toolkit, McGraw-Hill, New York, 2002.

[HuRe01] Huther, Andreas; Reitwiesner, Bernd: Portfolioanalyse im E-Brokerage. In: Buhl, Hans U.; Kreyer, Nina; Steck, Werner (Hrsg): e-Finance. Springer, Berlin et al, 2001.

[LooCha02] Looney, Clayton A.; Chatterjee, Debabroto: Web-Enabled Transformation of the Brokerage Industrie. In: Communications of the ACM, Vol. 45, No. 3, August 2002.

[MuGü04] Muntermann, J.; Güttler, A.: Mobile financial information services: Capabilities of suitable push services, Proceedings of the Eighth Pacific-Asia Conference on Information Systems (PACIS 2004); Shanghai, China, July 2004

[Oerk99] Oerke, Marc: Ad-Hoc-Mitteilungen und deutscher Aktienmarkt: Marktreaktion auf Informationen. Deutscher Universitäts-Verlag, Wiesbaden, 1999.

[OMA02] Open Mobile Alliance: E-Mail Notification Version 1.0, http://www.openmobilealliance.org/release_program/docs/CopyrightClick.asp?pck=EmailNot&file=OMA-EMN-V1_0-20021031-C.zip 2002, (2004-08-05).

[OMA04] OMA: Wireless Application Environment Specification Version 2.1, http://www.openmobilealliance.org/release_program/docs/Browsing/OMA-WAP-WAESpec-V2_1-20020909-C.pdf, (2004-08-05).

[Patel00] Patel, Alpesh B.: Net-Trading – Die besten Strategien für den Aktienhandel im Internet. Financial Times Prentice Hall, München, 2000.

[PiBoR96] Picot, Arnold; Bortenlänger, Christine; Röhrl, Heiner: Börsen im Wandel – Der Einfluß von Informationstechnologie und Wettbewerb auf die Organisation von Wertpapiermärkten. Knapp, Frankfurt, 1996.

[RaFRo03] Ranke, Johannes; Fritsch, Lothar; Rossnagel, Heiko: M-Signaturen aus rechtlicher Sicht. In Datenschutz und Datensicherheit 27, S.95-100, Vieweg & Sohn, Wiesbaden, 2003.

[Rann00] Rannenberg, Kai: Mehrseitige Sicherheit – Schutz für Unternehmen und ihre Partner im Internet. In: Wirtschaftsinformatik 42 (2000), S.489-497.

[RSA78] Rivest, R., L. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Communications of the ACM 21 (2), 1978, pp.120-126.

[Schi00] Schiller, Jochen: Mobilkommunikation. Addison Wesley, München, 2000.

[Shar66] Sharpe, William F.: Mutual Fund Performance. In: Journal of Business, 1966, Vol. 39, No. 1, S. 119-138.

[Sport03] Sportlogos.de: „anonyme SMS“, http://www.sportlogos.de, (2003-02-14).

[WaFo01a] WAP Forum: WAP Push Architectural Overview, Version 25-April-2001. http://www1.wapforum.org/tech/documents/WAP-205-MMSArchOverview-20010425-a.pdf, 2001, (2003-08-28).

[WaFo01b] WAP Forum: WAP Push Architectural Overview, Version 03-Jul-2001. http://www1.wapforum.org/tech/documents/WAP-250-PushArchOverview-20010703-a.pdf, 2001, (2003-08-28).

[Witn04] European IST Project,Wireless Trust for Mobile Business‘ (WiTness), SIM Application Hosting – Detailed description of the concept, http://www.wireless-trust.org/publicdocs/Witness_32275_D4_ExecSum.pdf, 2004.