Thema:

Sicherheitsaspekte der Bezahlung durch Agenten und deren rechtliche Stellung

Ausarbeitung im Rahmen des
Seminars zu Informationssystemen
"Ausgewählte Themen der Agentensysteme"

am Institut für Informatik der
Westfälischen Wilhelms-Universität Münster

betreut von Dr. Dietmar Lammers
vorgelegt von Daniel Beckmann, db@uni-muenster.de
im Wintersemester 2005/2006

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

„In Softwareagenten liegt ein ungeheures Potenzial“. Sie werden in der Zukunft immer häufiger als Unterstützer komplexer werdender Aufgaben agieren. Als Beispiel kann die Suche nach dem günstigsten Anbieter eines Produkts genannt werden. Hier übernimmt der Agent die Informationsbeschaffung und -filterung und kann letztendlich das Produkt erwerben und bezahlen. Ein weiteres Beispiel sind Online-Auktionen, bei denen der Agent zeitkritische Gebote zuverlässig abgeben kann.

Bei vielen denkbaren Einsatzszenarien trägt der Agent sensible Daten mit sich. Hier stellt sich die Frage, wie diese Daten vor unbefugtem Zugriff geschützt werden können und wie dieses im Agenten realisiert wird.

Ein weiterer Aspekt ist zu beachten, wenn der Agent autonom Aufgaben erledigt, also keine explizite Absegnung seiner Handlungen durch eine natürliche oder juristische Person erfolgt. Aus rechtlicher Sicht muss geklärt sein, ob seine Handlungen überhaupt rechtsgültig sind und wer für entstandene Schäden, sei es durch fehlerhaften Code oder falsche Eingaben, haftet.

Ziel dieser Arbeit ist es, die Grundlagen über Agenten zu vermitteln, d. h. die Anforderungen zu definieren und ihre Anwendungsgebiete abzugrenzen und einzuordnen.

Ist die Basis für die weiteren Kapitel geschaffen, so wird in Kapitel 3 auf den Sicherheitsaspekt eingegangen. Es werden die verschiedenen Angriffsarten auf mobile Agenten beschrieben, deren Abwehrmöglichkeiten aufgezeigt sowie die Realisierung der Sicherheit durch das „Public Key Verfahren“ vermittelt.

Weiterhin wird auf die verschiedenen Arten der elektronischen Bezahlung eingegangen, wobei die Vor- und Nachteile der Verfahren bzgl. der Ausführung durch Agenten und der Sicherheit der Daten herausgestellt werden.

Schließlich ist beispielhaft der Ablauf einer Bezahlung durch einen Agenten besonders im Hinblick auf den Sicherheitsaspekt vorgestellt.

In Kapitel 4 wird der rechtliche Aspekt beleuchtet. Hierzu werden die Handlungen des Agenten klassifiziert und die Bezahlung durch den Agenten rechtlich eingeordnet.

Letzten Endes werden die Ergebnisse zusammengefasst und ein Ausblick auf den zukünftigen Verlauf gewährt.

2 Grundlagen über Agenten

2.1 Anforderungen an Agenten

Jeder (Software-) Agent nutzt als Basis, als Grundlage für sein Handeln, ein Agentensystem. Diese Plattform stellt ihm die zum Erreichen seines Ziels nötigen Funktionen zur Verfügung.

Ist sich die Literatur über die Abgrenzung des Begriffs „Softwareagent“ grundsätzlich einig, herrscht noch keine Einigkeit über die Unterscheidung zwischen notwendigen und optionalen Anforderungen. Daher kann darüber diskutiert werden, ob diese Unterscheidung nötig ist und wenn ja, welche Anforderungen als notwendig und welche als optional angesehen werden können[1]. Generell ist ein (Software-) Agent durch folgende Anforderungen definiert:

Notwendige Anforderungen an Agenten: Ein Agent handelt …

- … **autonom** (Auswahlmöglichkeiten und selbstständige Selektion des Durchführungsweges; Handeln im Auftrag einer Person oder eines Agenten).
- … **reaktiv** (Reaktion auf eine Veränderung der Umwelt).
- … **aktiv** (selbstständige Beeinflussung der Umwelt).
- … **zielorientiert** (Orientierung seines Handelns auf das gegebene Ziel).

Optionale Anforderungen an Agenten: Ein Agent handelt …

- … **proaktiv** (Zustandsänderung ohne äußere Einwirkung).
- … **kommunikativ** (Kommunikation mit anderen Agenten).
- … **interaktiv** (Entgegennahme von Zielen und Präsentation der Ergebnisse direkt beim Benutzer).
- … **mobil** (eigenständige Verlagerung von einem auf ein anderes Agentensystem; erhöhte Sicherheitsanforderungen)[2].
- … **intelligent** (KI; Aufwand für Implementierung der Intelligenz sehr hoch).
- … **robust & anpassungsfähig** (bzgl. einer sich verändernden Umwelt).

[1] Vgl. z. B. Jennings; Wooldridge (1996).
[2] Vgl. Kotz; Gray (1999).

2.2 Anwendungsgebiete für Agenten

Zur Unterteilung der Anwendungsgebiete für Agenten kann in zwei Gruppen gegliedert werden: einerseits die **informationsgeprägt**en, andererseits die **systemgeprägt**en Anwendungsgebiete.

Ein Agent als Teil des erstgenannten Gebiets versucht, dem „information overload“[3], also der Überschwemmung des Users mit Informationen Einhalt zu gebieten, indem er für den User Informationen sammelt oder diese gefiltert als Ergebnis wiedergibt und damit eine Art Beraterposition einnimmt.

Der Agent als Teil eines systemgeprägten Anwendungsgebiets handelt auf Auktions- oder Preissuchplattformen, kann Steuerungssysteme (z. B. aus dem Bereich Robotik) simulieren und kontrollieren oder agiert in Computerspielen als Beispiel aus dem Entertainmentbereich.

[3] Vgl. Jennings; Wooldridge (1998).

3 Sicherheitsaspekte der Bezahlung durch Agenten

3.1 Angriffe und deren Abwehr

Bevor eine Bezahlung durch Agenten realisiert werden kann, muss die Sicherheit der von ihm mitgeführten Daten sichergestellt sein. Dazu ist es notwendig, die verschiedenen Arten der Angriffe auf (mobile[4]) Agenten zu kennen und durch abgestimmte Maßnahmen abwehren zu können. Die nachfolgend vorgestellten Arten decken die meisten der heute genutzten Angriffe[5] ab.

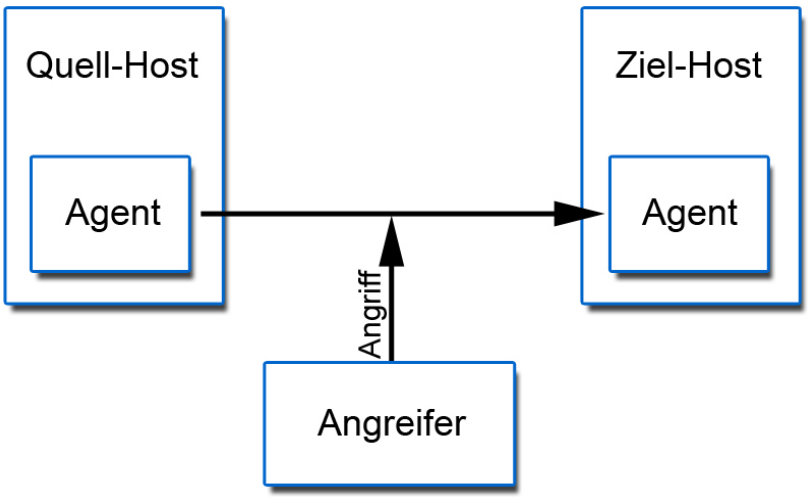

Abbildung 1: Abhören eines (mobilen) Agenten

3.1.1 Abhören eines (mobilen) Agenten

Will ein Angreifer einen Agenten abhören (siehe Abb. 1), versucht er, den Agenten auf seinem Weg vom Quell- zum Zielhost zu duplizieren. Die Kopie kann nun durch den Angreifer auf einem von ihm kontrollierten System nach sensiblen Daten untersucht werden.

3.1.2 Kopieren eines (mobilen) Agenten

Eine Erweiterung der in Kap. 3.1.1 genannten Methode ist das Kopieren des (mobilen) Agenten (siehe Abb. 2). Hierbei erstellt der Angreifer ein Duplikat des Agenten und schickt die Kopie dem Original zum Ziel-Host hinterher. Der Ziel-Host sowie der Agent selbst kann nicht erkennen, welcher Agent das Original ist und welcher die Kopie.

[4] Vor- und Nachteile mobiler Agenten vgl. Gehmeyr et al. (1998).
[5] Vgl. Chess (1998).

Durch einen doppelten Agenten wird aber z. B. eine Bestellung doppelt ausgelöst, wodurch schließlich für eine oder beide Parteien ein Schaden entsteht.

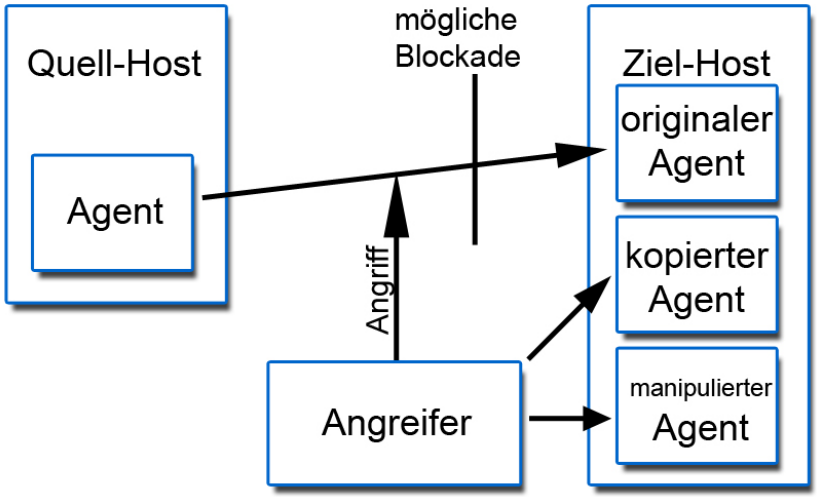

Abbildung 2: Kopieren eines (mobilen) Agenten

Ein hieraus ableitbarer erweiterter Angriff ergibt sich, wenn der Angreifer den originalen Agenten blockiert und den kopierten und manipulierten Agenten zum Ziel-Host schickt. Dieser Angriff wird in Kap. 3.1.4 detaillierter beschrieben.

3.1.3 Die „Denial of Service“-Attacke

Durch eine „Denial of Service“-Attacke (siehe Abb. 3) versucht der Angreifer, das Ausführen des Agenten auf dem Ziel-Host durch eine Vielzahl von Angriffen gegen den Ziel-Host zu beeinträchtigen oder ganz zu verhindern.

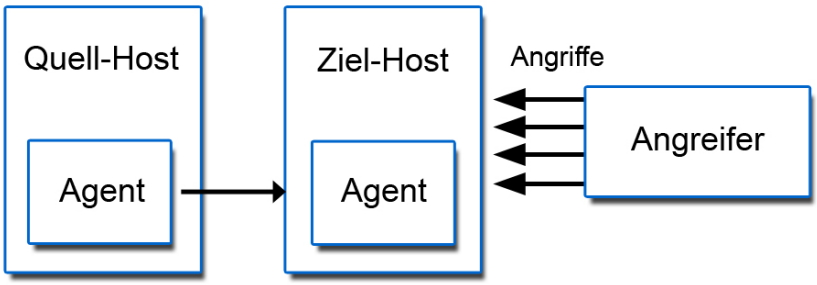

Abbildung 3: Die „Denial of Service”-Attacke

3.1.4 Der „Man in the Middle“-Angriff

Die letzte Gruppe der Angriffe beschreibt der „Man in the Middle“-Angriff (siehe Abb. 4). Hier setzt sich der Angreifer zwischen Quell- und Ziel-Host und manipuliert alle für ihn interessanten Nachrichten. Der Ziel-Host erhält somit manipulierte Daten, kann aber nicht feststellen, dass diese verändert wurden.

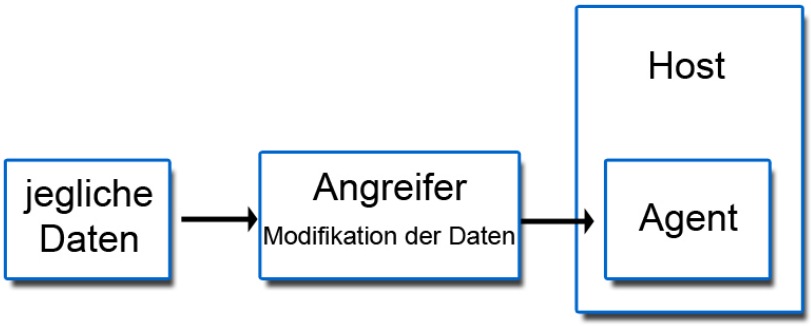

Abbildung 4: Der „Man in the Middle“-Angriff

3.1.5 Abwehr der Angriffe

Um die in Kap. 3.1.1 bis 3.1.4 erläuterten Angriffe abwehren zu können, bedient man sich mehrerer Vorkehrungen:

Hardware vor Veränderungen schützen: Die Hardware, auf dem das Agentensystem agiert, wird physisch z. B. durch ein sog. Trusted Platform Module, das einer Smartcard für den Coputer entspricht, gesichert. Dadurch kann sichergestellt werden, dass ein Angriff vom System auf das Agentensystem und auf den Agenten nicht ohne Einwirkung des Systembesitzers möglich ist.

Verschlüsselung der Datenübertragung zwischen Quell- und Ziel-Host: Die Übertragung der gesamten Daten und somit auch des Agenten vom Quell- zum Ziel-Host wird chiffriert. Aufgrund der Verschlüsselung ist es dem Angreifer nun nicht mehr möglich, den Agenten nach Beginn und vor Beendigung der Verschlüsselung abzuhören. Realisiert wird die Verschlüsselung durch das Public Key Verfahren.

Identifikation des Gegenübers durch vertrauenswürdige Zertifikate: Durch Verschlüsselung ist nicht gewährleistet, dass ein Agent nicht doch in falsche Hände gerät, da nicht ersichtlich ist, ob der vermeintliche Ziel-Host wirklich der gewünschte Partner ist. Der Einsatz vertrauenswürdiger Zertifikate, die in Kap. 3.3 vorgestellt werden, ermöglicht es, den Quell- und Ziel-Host zu identifizieren und eine Verbindung zwischen den „gewollten“ Partnern herzustellen.

Prüfsummen des Agenten-Programmcodes: Um eine Manipulation des Agenten ausschließen zu können, kann eine Prüfsumme über den ganzen Agenten-Code erstellt werden. Sobald der Agent bei einem neuen Agentensystem angekommen ist, kann das Agentensystem anhand der ihm bekannten Prüfsumme einen manipulierten Agenten entdecken und ihn „deaktivieren“. Häufig werden Prüfsummen auch von Herstellern genutzt, um nachweisen zu können, welcher Code vom Hersteller erstellt wurde und welcher nicht.

Signierung der Nachrichten: Um bei einer Übertragung von Nachrichten sicherstellen zu können, von wem diese kommen und ob der Absender auch diesen Inhalt abgeschickt hat, können die einzelnen Nachrichten signiert werden. Die Signierung wird durch das Public Key-Verfahren realisiert.

3.2 Sicherheit durch Signierung – das Public Key Verfahren

Das Public Key Verfahren[6], auch asymmetrisches Verfahren genannt, nutzt im Gegensatz zum symmetrischen Verfahren zwei unterschiedliche Schlüssel: Der öffentliche Schlüssel des Users ist allen zugänglich, der private wird unter Verschluss gehalten. Zur Ver- und Entschlüsselung einer Nachricht müssen jedoch beide Schlüssel genutzt werden. Mit dem einen Schlüssel wird die Nachricht chiffriert, mit dem anderen schließlich dechiffriert. Durch diesen Mechanismus können die beiden grundlegenden kryptografischen Verfahren, die Verschlüsselung und die Signierung einer Nachricht, erreicht werden. Die Funktionsweise ist im Folgenden beschrieben:

Verschlüsselung: Eine Person „Alice“ möchte eine Nachricht an „Bob“ schicken und dabei ausschließen können, dass irgendeine andere Person diese Nachricht lesen kann. Dazu verschlüsselt Alice ihre Nachricht mit dem ihr bekannten öffentlichen Schlüssel von Bob und schickt die chiffrierte Nachricht an Bob. Dieser kann mithilfe seines privaten Schlüssels, den nur er kennt, die Nachricht wieder dechiffrieren. Somit ist sichergestellt, dass nur Bob die Nachricht lesen kann.

Signierung[7]: Möchte Bob nun sicherstellen können, dass die empfangene Nachricht wirklich von Alice stammt, so kann Alice diese signieren. Dazu chiffriert sie die Nachricht mit ihrem eigenen privaten Schlüssel und schickt das Chiffrat an Bob. Dieser kann anhand des öffentlichen Schlüssels die Nachricht dechiffrieren. Da nur Alice die Möglichkeit hat, einen Text zu chiffrieren, der mit dem öffentlichen Schlüssel dechiffrierbar ist, sind Absender und Inhalt nachzuweisen.

Es bleibt anzumerken, dass Verschlüsselung und Signierung gleichzeitig angewandt werden können. Der Vorteil des Public Key Verfahrens im Gegensatz zum symmetrischen Verfahren ist, dass kein Austausch von geheimen Schlüsseln stattfinden muss. Man erkauft sich diesen Sicherheitsgewinn durch eine langsamere Ver- und Entschlüsselung. Beide Verfahren haben gemein, dass sie auf nicht bewiesenen Annahmen beru-

[6] Vgl. http://www.gnupg.org.

[7] Schnittstellenspezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV. Abschnitt A2: Signatur. http://www.bsi.bund.de/esig/basics/techbas/interop/bsi/sigi-a2.pdf (31.12.2005).

hen, da noch kein Weg gefunden wurde, eine Zahl in angemessener Zeit in ihre Primfaktoren zu zerlegen.

3.3 Zertifikate und deren Verwaltung

Durch das Public Key Verfahren ist ein „Man in the Middle“-Angriff wie in Kap. 3.1.4 beschreiben immer noch möglich. Für den Sender/Empfänger ist nicht festzustellen, ob der Partner wirklich der ist, für den er sich ausgibt. Dieses Problem lässt sich durch vertrauenswürdige Zertifikate lösen. Sie bestätigen die Verbindung zwischen einer Person und ihrem öffentlichen Schlüssel.

Ein Zertifikat[8] besteht aus dem öffentlichen Schlüssel einer Person, weiteren Zertifikatsinformationen und einer oder mehreren digitalen Signaturen.

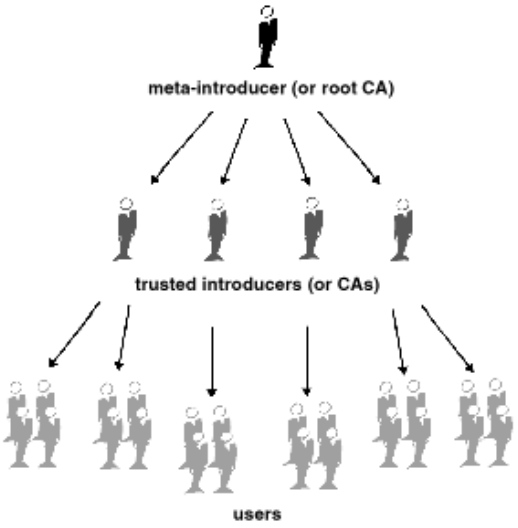

Abbildung 5: Die Verwaltungshierarchie von vertrauenswürdigen Zertifikaten

Wenn nun der Sender/Empfänger einer Nachricht einer bestimmten Organisation oder Firma vertraut, dass deren Schlüssel zu ihr gehört und mit diesem Schlüssel der öffentliche Schlüssel des Partners signiert ist, so kann der Sender/Empfänger aufgrund des aufgebauten Vertrauensnetzwerks auch sicher sein, dass der öffentliche Schlüssel des Partners wirklich zu seinem Partner gehört. Vertrauenswürdige Zertifikate sind als Vertrauenshierarchie aufgebaut (siehe Abb. 5). Hier erteilen nur von einer Root-Certificate-Authority zertifizierte Unternehmen, sog. Certificate-Authorities, Zertifikate an User.

[8] Siehe dazu Schnittstellenspezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV. Abschnitt A1: Zertifikate. http://www.bsi.bund.de/esig/basics/techbas/interop/bsi/sigi-a1.pdf (31.12.2005).

3.4 Arten und Ablauf der elektronischen Bezahlung

3.4.1 Arten der elektronischen Bezahlung

Ist die Grundlage für eine sichere Bezahlung vorhanden (siehe Kap 3.1 bis 3.3), so müssen nun die verschiedenen Arten der elektronischen Bezahlung durch Agenten selbst unter den Gesichtspunkten der Eignung für unsichere Server und des Vorhandenseins sensibler Daten untersucht werden. Im Folgenden sind die unterschiedlichen Arten der Bezahlung mit ihren Vor- und Nachteilen für eine Nutzung durch mobile Agenten aufgezählt sowie tabellarisch einander gegenübergestellt (siehe Abb. 6):

Barzahlung: Eine Barzahlung durch Agenten ist nicht möglich, da sie Geld nicht physisch mitführen können.

Nachnahme: Eine Zahlung per Nachnahme ist für den mobilen Agenten durchführbar. Sicherheitskritische Daten werden nicht mitgeführt. Name und Anschrift müssen bei Bestellung bekannt sein.

Überweisung: Generell sind für die Durchführung einer Überweisung sicherheitskritische Daten notwendig (PIN/TAN). Jedoch ist dies durch folgenden Ablauf abschwächbar: Der Agent bestellt und erhält Überweisungsdaten, begibt sich zurück zum eigenen Agentensystem und führt erst dort die Überweisung aus. Der Vorteil liegt darin, dass die sensiblen Daten nicht mitgeführt werden müssen.

Bankeinzug: Bei der Zahlungsart „Bankeinzug“ müssen bei der Wanderung des Agenten z. B. bei der Suche nach dem günstigsten Anbieter Kontonummer und Bank vor den Anbietern, mit denen man kein Geschäft abschließt, geheim gehalten werden. Die Kontonummer darf erst preisgegeben werden, wenn wirklich eine Transaktion stattfinden soll. Falls diese Daten doch in falsche Hände geraten ist, zumindest in Deutschland eine Rückbuchung innerhalb von sechs Wochen durchführbar.

Elektronisches Geld: Der Vorteil bei elektronischem Geld ist die absolute Anonymität bei Transaktionen. Nachteilig ist es, wenn ein Agent gelöscht oder dupliziert wird, da so das Geld mit gelöscht wird oder durch das Duplikat vorzeitig ausgegeben werden könnte.

(Namentliche) Gutscheine: Namentliche Gutscheine sind zwar kein Geld im eigentlichen Sinne mehr, jedoch werden sie anhand dessen bewertet. Vor allem bei namentlichen Gutscheinen muss schon vorher eine Geschäftsbeziehung bestanden, um den Gutschein zu erwerben. Daher ist eine gewisse Bindung an einen Anbieter für namentliche

Gutscheine Voraussetzung. Der Vorteil ist, dass namentliche Gutscheine nicht gestohlen werden können.

Kreditkarte: Bei der Bezahlung mit Kreditkartendaten muss der Agent diese mit sich führen. Als sicherheitsrelevant und daher schützenswert werden der Name des Inhabers der Karte, die Kartennummer sowie die Prüfnummer angesehen, da mit Ihnen Kreditkartenzahlungen durchgeführt werden können. Es sei darauf hingewiesen, dass eine ungesicherte Übertragung der Daten eine Sorgfaltsverletzung (siehe AGBs der Kartenanbieter[9]) darstellt und die Haftung der Kartenanbieter ausschließt.

	Vom Agenten verwendbar	Für unsichere Server geeignet*	Sensible Daten erforderlich**
Bargeld, Chipkarte	Nein	---	---
Nachnahme	Ja	Ja	Nein
Überweisung (Bezahlung)	Ja	Ja	Nein
Überweisung (Durchführung)	Ja	Nein	Ja
Bankeinzug	Ja	Ja	Nein
Elektronisches Geld	Ja	Nein	Nein
(namentliche) Gutscheine	Ja	Ja	Nein
Kreditkarte	Ja	Nein	Nein

* auf unsicheren Servern ohne Gefahr durchführbar
** vor dem Zahlungsempfänger zu verbergende Daten (z.B. PIN/TAN)

Abbildung 6: Übersicht der Arten der elektronischen Bezahlung durch Agenten mit ihren Vor- und Nachteilen

3.4.2 Ablauf einer elektronischen Bezahlung

Ein sinnvoller Algorithmus für eine elektronische Bezahlung[10] erfüllt folgende Ziele:

1. Ziel-Host kann das **Angebot nicht abstreiten**.
2. Wenn der Agent (bzw. sein Quellhost) angenommen hat, kann er nicht mehr verweigern.
3. **Nur Ziel-Host kann die Zahlungsdaten** verwenden.
4. Ziel-Host kann die **Lieferung nicht verweigern**. (Ziel-Server kann natürlich nur theoretisch gezwungen werden, Daten zu liefern. Aber: Nachweis, dass Verpflichtung besteht, durch vertrauenswürdige dritte Partei möglich.)
5. **Überprüfung**, ob Angebot der Lieferung entspricht, ist jederzeit möglich.

[9] Vgl. Allgemeine Geschäftsbedingungen für die Mastercard.
[10] Vgl. Asokan et al. (1996).

Um diese Ziele zu erfüllen, läuft der Algorithmus wie folgt ab:

Schritt 1: Agent sendet mit Transaktionsschlüssel verschlüsselte Leistungen an Server und einen Hashwert (Anwendung einer sicheren Hashfunktion auf die Konkatenation von Nachricht und Schlüssel). Server handelt genauso.

Schritt 2: Aus eigenem und fremden Hashwert kann gemeinsamer Hashwert errechnet werden. Hieraus werden Ursprungs- und Empfangsbeweis erstellt und dem Partner gesendet.

Schritt 3: Agent schickt Name des Partners, die verschlüsselten Leistungen, den Hashwert und den zur Entschlüsselung nötigen Transaktionsschlüssel an dritte Partei. Server handelt genauso.

Schritt 4: Dritte Partei überprüft die Daten und veröffentlicht ein P, das dem Agenten und dem Server ermöglicht, den Transaktionsschlüssel des Partners zu extrahieren.

Schritt 5: Agent und Server können mithilfe des Transaktionskeys die Leistungen des Partners entschlüsseln.

4 Rechtliche Stellung der Agenten

Aus den obigen Kapiteln der elektronischen Bezahlung durch mobile Agenten ergeben sich rechtliche Fragen. Zum Beispiel ist zu klären, ob und in wie weit ein Agent rechtlich befugt ist, Willenserklärungen abzugeben. Dieses Kapitel behandelt ausgewählte Fragen der rechtlichen Stellung der Agenten.

4.1 Klassifikation von Handlungen durch Agenten

Um Handlungen von Agenten rechtlich einordnen zu können, müssen diese analysiert werden. Es kann festgestellt werden, dass ein Agent eine elektronische Willenserklärung abgibt. Er ist rechtlich gesehen aber nicht handlungsfähig, daher muss die Willenserklärung einer Person zugeordnet werden. Der BGH hat dazu folgendes entschieden: „Auch elektronische und andere automatisierte Erklärungen sind echte Willenserklärungen [...]. Sie sind dem Betreiber der EDV-Anlage [hier der Betreiber/Besitzer des Agenten] zuzurechnen, auch wenn sie wegen einer von ihr zu vertretenden Fehlleistung der Soft- oder Hardware abgegeben wurden.“

Gibt ein Agent eine Willenserklärung ab, so ist anhand des elektronischen Zertifikats des Agenten der Besitzer feststellbar. Hinsichtlich der Haftung wird zwischen Hersteller und Besitzer des Agenten sowie Betreiber der Agentenplattform differenziert:

- **Der Hersteller** des Agenten signiert sein Programm und haftet für die in der Dokumentation definierten Funktionen.
- **Der Betreiber** des Agenten (-systems) ist für ordnungsgemäßes Funktionieren verantwortlich. Es stellt sich hier das Problem: Wie kann ein Agent ein fehlerhaftes Agentensystem beweisen?
- **Der Besitzer** des Agenten ist generell verantwortlich für alle Handlungen des Agenten einschließlich der vom Hersteller definierten konkreten Eingabemöglichkeiten (Werte, Bedeutung).

4.2 Handlungsort

Handelt der Agent über Ländergrenzen hinweg, so muss geklärt sein, welches Recht Anwendung findet. Gemäß des **Europäischen Vertragsstatutübereinkommens bei Verbraucherverträgen** steht dem Verbraucher die freie Rechtswahl zu, jedoch nur eingeschränkt, denn: **„Wenn dem Vertragsabschluß ein ausdrückliches Angebot oder eine Werbung in diesem Staat vorausgegangen ist und der Verbraucher dort**

die zum Abschluss des Vertrags notwendigen Rechtshandlungen vorgenommen hat“, so gilt das Recht des Landes des Anbieters.

Kommt der Anbieter nicht aus der EU, kann durch folgende Begründung wiederum das Recht des Anbieterlandes gelten:

Der Agent ist im rechtlichen Sinne ein Transportmittel. Folglich wäre das Recht anzuwenden, wie wenn der Besitzer direkt über den Webbrowser handelt. Jedoch wandert der Agent zum Anbieter hin und ist beim Abschluss der Willenserklärung ausschließlich im Anbieterstaat tätig. Dadurch wird der Verbraucherschutz des Heimatlandes unwirksam; bei dem Einsatz von Agenten gilt jeweils das Landesrecht des Anbieters!

4.3 Signierung durch Agenten

Es muss noch geklärt werden, ob die elektronische Signatur des Agenten im Sinne einer handschriftlichen Unterschrift rechtsgültig ist.

Gemäß EU Signaturrichtlinie können nur Personen unterschreiben. Daher ist eine elektronische Signatur des Agenten keine rechtsgültige Unterschrift, denn: „**Eine sichere elektronische Signatur muss mit Mitteln erstellt werden, welche der Signator unter seiner alleinigen Kontrolle halten kann**“. [§ 2, Z. 3, lit. c SigG]

Ein Agent kann jedoch eine normale digitale Signatur erstellen, die eine ähnliche Stärke aufweist. Diese durch Agenten unterschrieben Willenserklärung ist bedingt rechtsgültig und kann rechtlich als Beweismittel gelten.

Über Umwege ist elektronische Signatur/Unterschrift trotzdem möglich, und zwar wie folgt:

Vorgehen 1: Der Agent befindet sich auf einem vom Signator kontrollierten PC: Der Signator löst elektronische Signatur aus.

Vorgehen 2: Der Agent befindet sich auf einem Fremdrechner: Das Dokument wird zum Heimatrechner geschickt, vom Signator „unterschrieben“ und zurückgeschickt.

Die rechtliche Ausarbeitung ist noch nicht abgeschlossen. Im „Electronic Signatures in Global and National Commerce Act“ ist zukünftig eine Gleichstellung zu handschriftl. Signaturen für Signaturen durch Agenten vorgesehen.

5 Zusammenfassung und Ausblick

Zusammenfassend kann festgestellt werden, dass die Bezahlung durch einen Agenten einen hohen Grad an Automatisierung und Nutzenvorteil ermöglicht. Dabei darf die Sicherheit aber nicht vernachlässigt werden; dem Sicherheitsverlust muss entgegengewirkt werden.

Eine Abwägung zwischen erhöhtem Nutzen und dem dadurch einhergehenden Sicherheitsverlust ist zwingend.

Aus rechtlicher Sicht wurde herausgestellt, dass Agenten die Rechtslage im Gegensatz zur Abgabe der „konventionellen“ Willenserklärung verändern. Der durch den Gesetzgeber zugesicherte Verbraucherschutz wird ausgehebelt und ist beim Einsatz eines Agenten nicht anwendbar.

Bleibt anzumerken, dass die rechtliche Entwicklung noch in vollem Gang ist. Eine erste Standardisierung, eine rechtliche Gleichsetzung von der handschriftlichen Unterschrift und der elektronischen Signatur durch Agenten, wird in Zukunft voraussichtlich im („Electronic Signatures in Global and National Commerce Act“) verabschiedet.

Literaturverzeichnis

Asokan et al. (1996): N. Asokan, Matthias Schunter, Michael Waidner: Optimistic Protocols for Fair Exchange. IBM Research Report.

Chess (1998): David M. Chess: Security Issues in Mobile Code Systems. 1-14 In: Giovanni Vigna (Ed.): Mobile Agents and Security. Berlin: Springer 1998.

Gehmeyr et al. (1998): A. Gehmeyr, J. Müller, A. Schappert: Mobile Information Agents on the Web. In: Matthias Klusch, Gerhard Weiß (Ed.): Cooperative Information Agents II. Learning, Mobility and Electronic Commerce for Information Discovery on the Internet. Berlin: Springer 1998.

Jennings; Wooldridge (1996): Nicholas R. Jennings and Michael J. Wooldridge: Software Agents. IEE Review, Januar 1996, S. 17-20.

Jennings; Wooldridge (1998): Nicholas R. Jennings, Michael J. Wooldridge: Applications of Intelligent Agents. In: Nicholas R. Jennings, Michael J. Wooldridge: Agent Technology. Foundations, Applications and Markets. Berlin: Springer 1998.

Kotz; Gray (1999): David Kotz, Robert S. Gray: Mobile Agents and the Future of the Internet. Operating Systems Review, Juli 1999. S. 7-13 (Volume 33, Number 3).