Sicherheitsaspekte der Bezahlung durch Agenten und deren rechtliche Stellung

Vortrag im Rahmen des Seminars
„Ausgewählte Themen aus Agentensysteme“

Daniel Beckmann
15. Dezember 2005

Gliederung

- Einleitung
- Grundlagen über Agenten
- Sicherheitsaspekte der Bezahlung durch Agenten
- Rechtliche Stellung der Agenten
- Zusammenfassung und Ausblick

Einleitung (1 von 3)

- Software-Agenten und deren Potenzial werden immer häufiger genutzt.
- Beispiele der Nutzung von Agenten:
  - **Suche nach günstigstem Anbieter** eines Produkts
  - **Online-Auktionen** wie z.B. bei eBay
  - **Bezahlvorgänge**
- **Aufgeworfene Frage:**
  - Sind sicherheitsrelevante Daten vor unbefugtem Zugriff geschützt?

Einleitung (2 von 3)

- Agenten erledigen **autonom** Aufgaben.
- **Keine explizite Absegnung** einzelner Handlungen durch eine natürliche Person

- **Aufgeworfene Frage:**
  - Sind die Handlungen eines Agenten überhaupt rechtsgültig?
  - Wer haftet für Schäden, die durch den Agenten entstehen?

Einleitung (3 von 3)

- **Ziel des Vortrags**:
  - **Grundlagen:** Was ist eigentlich ein (**Software-)Agent**?
  - **Sicherheitsaspekt:** Wie ist die **Sicherheit der Daten** gewährleistet?
  - **Rechtl. Aspekt:** Wie ist ein Agent **recht**lich einzustufen?

Gliederung

- Einleitung
- Grundlagen über Agenten
  - Anforderungen an Agenten
  - Anwendungsgebiete für Agenten
- Sicherheitsaspekte der Bezahlung durch Agenten
- Rechtliche Stellung der Agenten
- Zusammenfassung und Ausblick

Anforderungen an Agenten (1 von 2)

- Genrell: **Agentensystem** als Basis für den Agenten
- notwendige Anforderungen an einen Agenten:
  - **Autonom**es Handeln (Auswahlmöglichkeiten und selbstständige Selektion des Durchführungsweges; Handeln im Auftrag einer Person oder eines Agenten)
  - **Reaktiv**es Handeln (auf eine veränderte Umwelt reagieren)
  - **Aktiv**e Beeinflussung der Umwelt
  - **Zielorientiert**es Handeln

Anforderungen an Agenten (2 von 2)

- optionale Anforderungen an einen Agenten:
  - **Proaktiv** (Zustandänderungen ohne äußere Einwirkung)
  - **Kommunikativ** (mit anderen Agenten)
  - **Interaktiv** (Entgegennahme von Zielen und Präsentation der Ergebnisse direkt beim Benutzer)
  - **Mobil** (eigenständige Verlagerung von einem auf einen anderen Computer; erhöhte Sicherheitsanforderungen)
  - **Intelligent** (KI; häufig nicht der Fall, da Ausmaß der Intelligenz proportional zum Aufwand für Implementierung wächst)
  - **Robust & Anpassungsfähig** (bzgl. einer sich verändernden Umwelt)

Anwendungsgebiete für Agenten

- **Information**sgeprägt:
  - Informationssammlung
  - Informationsfilterung
  - Agentensystem zur Beratung (z. B. Aktienkauf)
  - Groupware, CSCW (Benachrichtigung über Änderungen)

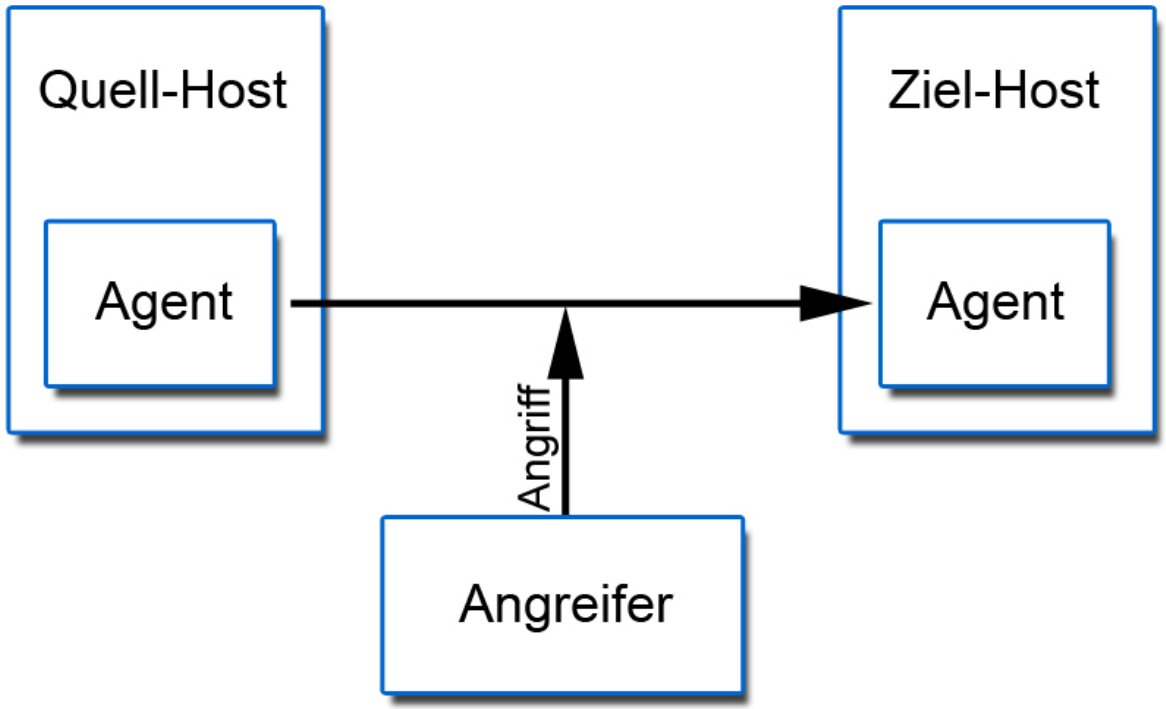
- **System**geprägt:
  - E-Commerce (Preisnachfragen, Versteigerungen)
  - Steuerungssysteme (z. B. Simulation, Kontrolle)
  - Entertainment (Computerspiele)

Gliederung

- Einleitung
- Grundlagen über Agenten
- Sicherheitsaspekte der Bezahlung durch Agenten
  - Angriffe und deren Abwehr
  - Sicherheit durch Signierung – Public Key Verfahren
  - Zertifikate und deren Verwaltung
  - Arten und Ablauf der elektronischen Bezahlung
- Rechtliche Stellung der Agenten
- Zusammenfassung und Ausblick

Angriffe auf Agenten (1 von 4)

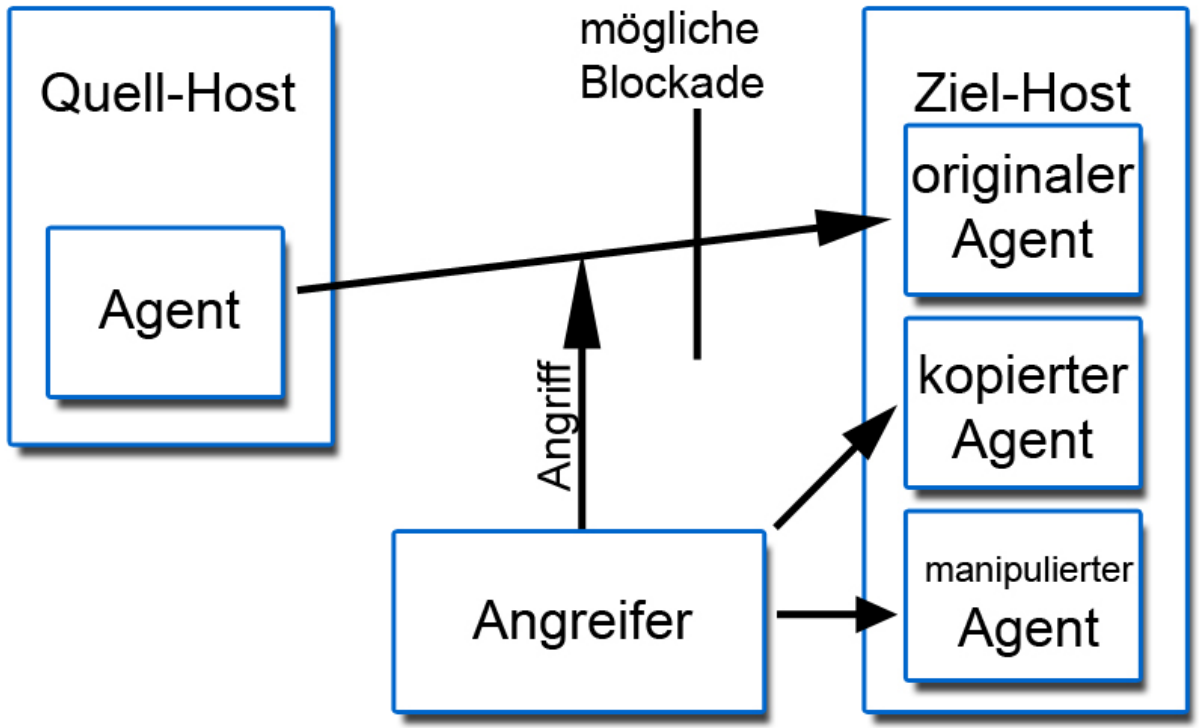
- **Abhören eines (mobilen) Agenten:**



  - Zweck: sensible Daten erlangen

Angriffe auf Agenten (2 von 4)

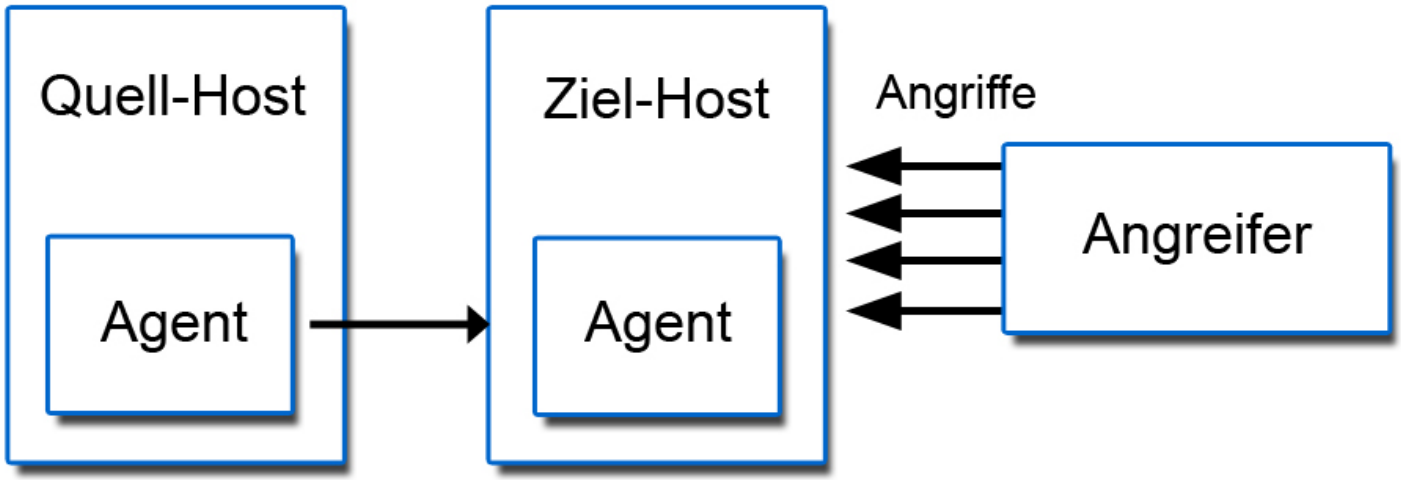
- **Kopieren eines (mobilen) Agenten:**



  - Möglichkeit der doppelten Bestellung

Angriffe auf Agenten (3 von 4)

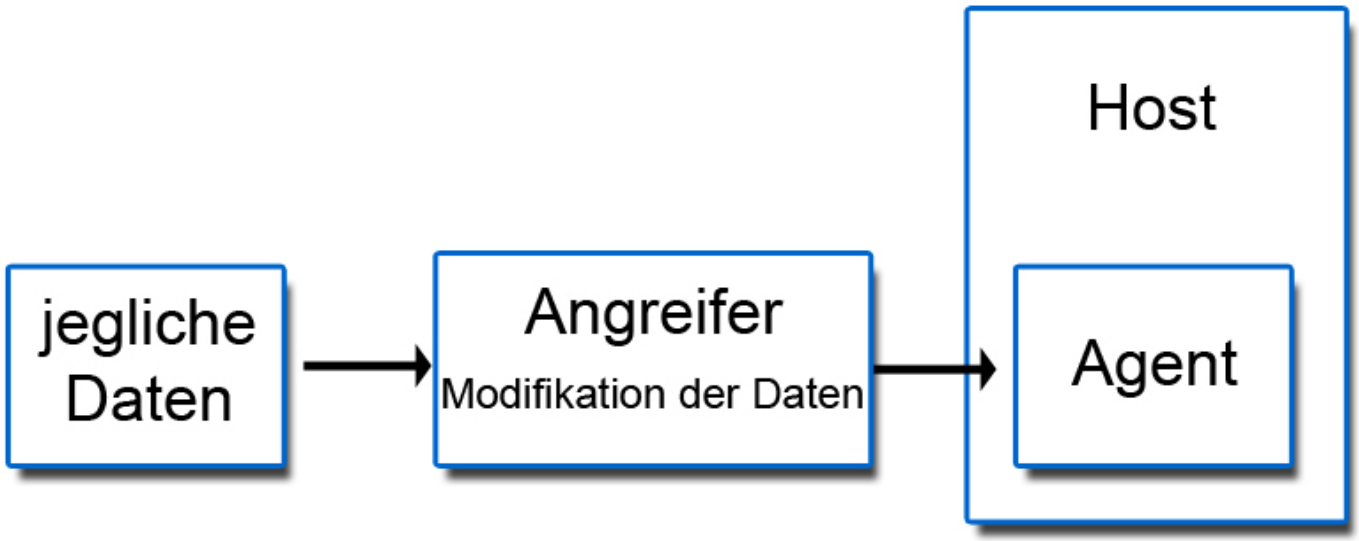
- **Denial of Service-Attacke:**



  - Störung der Ziel-Hosts, so dass der Agent...
    - ... ihn nicht erreichen kann. (Bandbreitenüberlastung, Ressourcenüberlastung, Belegung bestimmter Dienste)
    - ... in der Ausführung auf dem Ziel-Host gestört wird.

Angriffe auf Agenten (4 von 4)

- **Man-In-The-Middle-Angriff:**



  - Zweck: Manipulation von Daten
  - Bsp.: Überweisungsveränderungen

Abwehr der Angriffe (1 von 2)

- **Hardware vor Veränderungen sichern**
  - Vorteil: Agentensystem ist sicher
  - Nachteil: hohe Kosten
  - Beispiel: Trusted Platform Module (Smartcard des Computers)

- **Verschlüsselung der Datenübertragung zwischen Quell- und Ziel-Host**
  - Vorteil: keine äußeren Angriffe mehr möglich
  - Nur noch Angriffe vom eigenen Agentensystem aus möglich
  - Realisierung durch **Public Key Verfahren**

Abwehr der Angriffe (2 von 2)

- **Identifikation des Gegenübers durch Zertifikate (Signierung)**
  - keine Man-in-the-Middle-Attacke mehr möglich
- **Prüfsummen des Programm-Codes**
  - Manipulation des Agenten nicht mehr möglich
- **Signierung der Nachrichten**
  - Vorteil: Inhalt und Absender sind nachzuweisen
  - Realisierung durch Public Key Verfahren

Public Key Verfahren (1 von 3)

- **Asymmetrisches Verfahren**
- **Zwei Schlüssel**: öffentlicher und privater Schlüssel
- Daten werden **mit einem Schlüssel chiffriert**, mit dem **anderen dechiffriert**.
- **<u>Verschlüsselung:</u>**

Public Key
von Bob

Private Key
von Bob

Plaintext

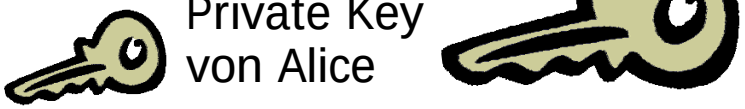
Ciphertext

Alice

Bob

Public Key Verfahren (2 von 3)

- Mittels einer **Signatur** kann **Absender und Inhalt der Nachricht nachgewiesen** werden.
- Entspricht **handschriftlicher Unterschrift, die nicht gefälscht werden kann.**
- **Signierung:**



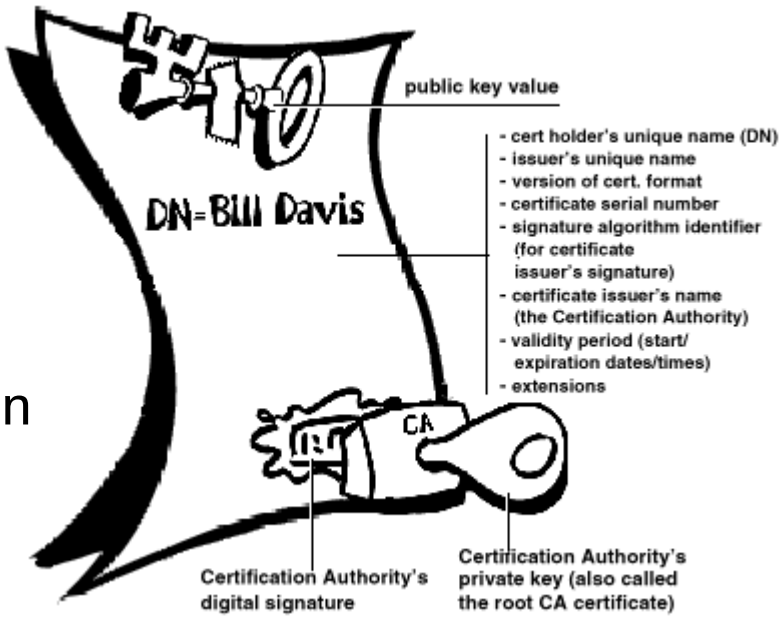
Public Key Verfahren (3 von 3)

- **Signierung und Verschlüsselung** können gleichzeitig angewandt werden.

- Vorteil: **kein Weitergeben geheimer Schlüssel** (wie bei symmetrischen Verfahren)
- Nachteil:
  - Sicherheit beruht auf **unbewiesenen Annahmen**.
  - im Gegensatz zu symmetrischen Verfahren **sehr langsam**
  - (Ausweg: Daten mit symmetrischem Schlüssel chiffrieren; nur den symmetrischen Schlüssel asymmetrisch Verschlüsseln)

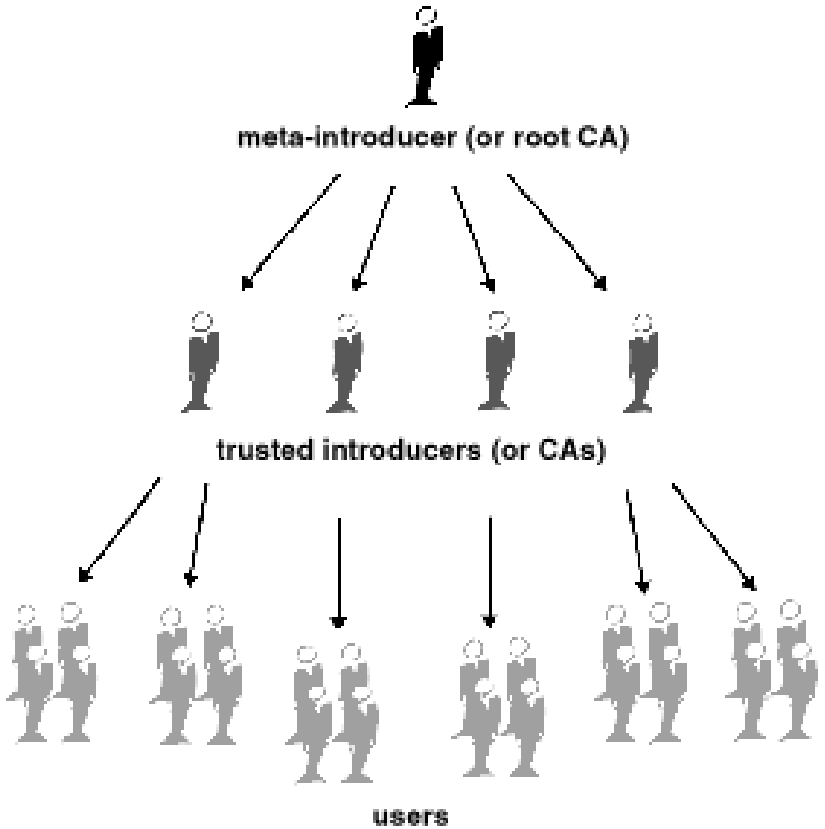
Vertrauenswürdige Zertifikate (1 von 2)

- Problem: Auch mit Public Key Verfahren keine Man-in-the-Middle-Attacke ausgeschlossen
- Lösung: **vertrauenswürdige Zertifikate**
- Bestätigen Verbindung zwischen Person und deren öffentlichen Schlüssel
- Zertifikate enthalten (X.509):
  - public key
  - Certificate Informationen
  - Eine oder mehrere digitale Signaturen



Vertrauenswürdige Zertifikate (2 von 2)

- **„Verwaltung“ als Hierarchie** angeordnet:
  - Root-Certificate-Authority (zertifiziert sich selbst)
  - Certificate-Authority
  - Zertifikate der Nutzer
  - Nachrichten



Arten der elektronischen Bezahlung - Einleitung

- Elektronische Bezahlung ist mit ein zentraler Punkt von E-Commerce
- Da es sich um reales Geld handelt sind **hohe Sicherheitsanforderungen zwingend**.
- Voraussetzung: **Mitnahme der Daten muß möglich sein**. (Chipkarte nicht möglich, da Agent keine Karte mitführen kann.)
- Vorstellung der Varianten mit Vor- und Nachteilen bzgl.:
  - Eignung für unsichere Server
  - Nutzung sensibler Daten
  - Anonymität

Arten der elektronischen Bezahlung (1 von 4)

- **Nachnahme:**
  - Name und Anschrift müssen übergeben werden.
  - **Nicht sicherheitskritisch**, da Daten bekannt sein müssen

- **Überweisung:**
  - Die Sicherheit nicht gefährdender Ablauf kann wie folgt realisiert werden:
    - Agent bestellt und erhält Überweisungsdaten.
    - Kehrt zurück und führt Überweisung aus. (Vorteil: kein Transport von sensiblen Daten)

Arten der elektronischen Bezahlung (2 von 4)

- **Bankeinzug:**
  - Daten müssen vor Anbieter geheim gehalten werden.
  - Kontonummer erst preisgeben, wenn Transaktion wirklich durchgeführt werden soll.
  - **Wenig Risiko, da eine Rückbuchung möglich**

- **Elektronisches Geld:**
  - Vorteil: **absolute Anonymität**
  - Probleme:
    - Es darf keine Agentenkopie erstellt werden.
    - Wenn Agent gelöscht wird, ist das mitgeführte Geld verloren.

Arten der elektronischen Bezahlung (3 von 4)

- **Gutscheine:**
  - **Kein direktes Geld**, aber Bewertung durch Geld
  - Unterscheidung zwischen **namentlichen und anonymen Gutscheinen**
  - Geschäftsbeziehung muß schon vorher bestanden haben. (Erwerb des Gutscheins)
  - Nachteil: Zusätzlicher Schritt erforderlich (Erwerb des Gutscheins)
  - Vorteil: **Diebstahl namentlicher Gutscheine nicht möglich**

Arten der elektronischen Bezahlung (4 von 4)

- **Kreditkarte:**
  - **Sicherheitsrelevante Daten:**
    - Kartennummer
    - Ablaufdatum
    - Name
  - **keine Anonymität** beim Kauf gegeben
  - **Ungesicherte Übertragung der Daten ist eine Sorgfaltsverletzung** (siehe AGBs der Kartenanbieter) und schließt Haftung der Kartenanbieter aus.

Arten der elektronischen Bezahlung - Zusammenfassung

	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

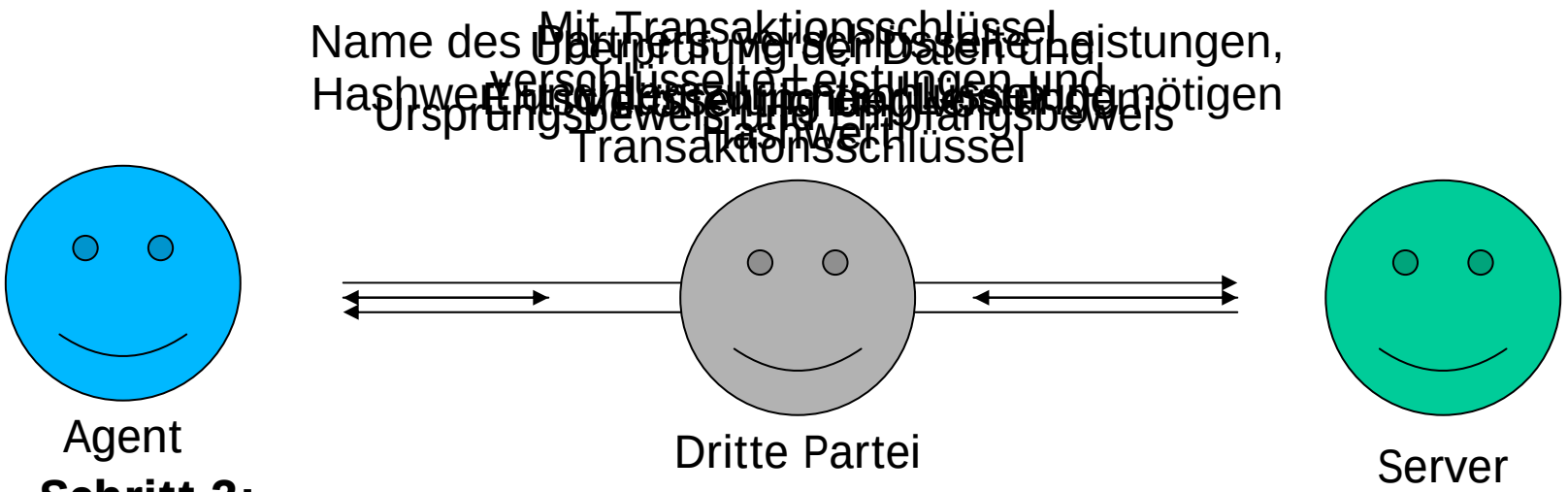
** vor dem Zahlungsempfänger zu verbergende Daten (z.B. PIN/TAN)

Ablauf einer Bezahlung (1 von 2)

- Vorstellung eines Algorithmus, der folgende Eigenschaften besitzt:
  - Ziel-Host kann das **Angebot nicht abstreiten**.
  - Wenn der Agent (bzw. sein Quellhost) angenommen hat, kann er nicht mehr verweigern.
  - **Nur Ziel-Host kann die Zahlungsdaten** verwenden.
  - 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.
  - **Überprüfung**, ob Angebot der Lieferung entspricht, ist jederzeit möglich.

[siehe Asokan et al. 1996, Optimistic Protocols for Fair Exchange. IBM Research Report]

Ablauf einer Bezahlung (2 von 2)



Schritt 3:
Schritt 2:
Schritt 4:
Schritt 5:

Schickt Name des Partners, die verschlüsselten Leistungen, den Aus eigenem und fremden Hashwert kann gemeinsamer Hashwert Anwendung einer sicheren Hashfunktion auf Transaktionsschlüssel, verschlüsselte Leistungen und Ursprungsbeweis erstellt und dem Partner gesendet.

Server und Agent können mit Hilfe des Transaktionskeys die Leistungen des Partners entschlüsseln.

Server handelt genauso.

Erfüllte Anforderungen:

- ☑ Nur Ziel-Host kann die Zahlungsdaten verwenden.
- ☑ Ziel-Host kann das Angebot nicht abstreiten.
- ☑ Wenn der Agent (bzw. sein Quellhost) angenommen hat, kann er nicht mehr verweigern.

Gliederung

- Einleitung
- Grundlagen über Agenten
- Sicherheitsaspekte der Bezahlung durch Agenten
- Rechtliche Stellung der Agenten
  - Klassifikation von Handlungen durch Agenten
  - Handlungsort
  - Signierung durch Agenten
- Zusammenfassung und Ausblick

Klassifikation von Handlungen durch Agenten (1 von 2)

- **Ist die Handlung eines Agenten rechtsverbindlich?**
  - Agent gibt **elektronische Willenserklärung** ab.
  - Agent ist **im Rechtssinne nicht handlungsfähig**.
  - daher **Zurechnung an eine Person**
- „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.“
  [BGH NJW 02, 363; Borges, Vertreter im elektronischen Geschäftsverkehr]

Klassifikation von Handlungen durch Agenten (2 von 2)

- **Wer haftet für den Agenten?**
  - Agent trägt elektronische Identität mit sich (Zertifikat). **Zuordnung zu einer Person** möglich.
  - **Hersteller** des Agenten signiert sein Programm und haftet für die in der Dokumentation definierten Funktionen.
  - **Betreiber** des Agenten (-systems) ist für ordnungsgemäßes Funktionieren verantwortlich.
    - Problem: Wie kann ein Agent ein fehlerhaftes Agentensystem beweisen?
  - **Besitzer** des Agenten generell verantwortlich für alle Handlungen des Agenten
    - Hersteller definiert Eingabemöglichkeiten (Werte, Bedeutung), für deren konkreten Inhalte der Benutzer verantwortlich ist.

Handlungsort des Agenten (1 von 2)

- **Welches Recht ist anwendbar?**
- **Europäisches Vertragsstatutübereinkommen bei Verbraucherverträgen:**
  - Freie Rechtswahl
  - Verbraucherschutz jedoch unwirksam, 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“, gilt das **Recht des Landes des Anbieters**.
  - Voraussetzung: **Informationspflichten müssen eingehalten werden** (FernabsatzG).
- Frage: Wie sieht die Rechtslage aus, wenn der Anbieter nicht aus der EU kommt oder die Voraussetzungen nicht erfüllt?

Handlungsort des Agenten (2 von 2)

- **Wo agiert der Agent, welches Recht ist speziell bei Agenten anwendbar?**
  - Agent ist **im rechtlichen Sinne Transportmittel**.
  - Folglich: Anwendbares Recht, wie wenn Besitzer direkt über Webbrowser handelt (d.h. Verbraucherschutz ist zu beachten).
  - Jedoch: Agent wandert zum Anbieter hin. **Tätigkeit ausschließlich im Anbieterstaat.**
  - Daher: **Agenten handeln beim Anbieter** und machen so Verbraucherschutz des Heimatlandes unwirksam.
  - Schlussfolgerung: **Bei Einsatz von Agenten gilt jeweils das Landesrecht des Anbieters!**

Elektronische Signaturen (1 von 2)

- **Ist die elektronische Signatur / Unterschrift des Agenten rechtsgültig?**
  - Gem. EU Signaturrichtlinie können **nur Personen unterschreiben.**
  - **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]
  - Agent kann jedoch **normale digitale Signatur** erstellen, die ähnliche Stärke aufweist.
  - **Willenserklärung durch Agenten bedingt rechtsgültig**; kann aber als Beweismittel gelten.

Elektronische Signaturen (2 von 2)

- **elektronische Signatur / Unterschrift** trotzdem möglich:
  - **Vorgehen 1:**
    - Agent befindet sich auf vom Signator **kontrollierten PC.**
    - Signator löst elektronische Signatur aus.
  - **Vorgehen 2:**
    - Agent befindet sich auf **Fremdrechner.**
    - Dokument wird zu Heimatrechner geschickt, vom Signator „unterschrieben“ und zurückgeschickt.

- **Zukunft:** Im Electronic Signatures in Global and National Commerce Act ist eine **Gleichstellung zu handschriftl. Signaturen** für Signaturen durch Agenten vorgesehen.

Gliederung

- Einleitung
- Grundlagen über Agenten
- Sicherheitsaspekte der Bezahlung durch Agenten
- Rechtliche Stellung der Agenten
- Zusammenfassung und Ausblick

Zusammenfassung und Ausblick

- **Sicherheitsaspekt:**
  - Hoher Grad an **Automatisierung und Nutzenvorteil durch Agenten möglich**
  - Dabei darf die **Sicherheit nicht vernachlässigt** werden.
  - **Abwägung** zwischen **erhöhtem Nutzen** und dem dadurch einhergehenden **Sicherheitsverlust**

- **Rechtl. Aspekt:**
  - **Agenten „verändern“ die Rechtslage!**
    (z.B. Verbraucherschutz nicht anwendbar)
  - Rechtliche Lage der Agenten wird noch erarbeitet
    („Electronic Signatures in Global and National Commerce Act“).

Fragen und Antworten

Noch Fragen

?

Danke für die
Aufmerksamkeit