

Elektronische Zahlungsmechanismen unter Sicherheitsgesichtspunkten

Trierer Symposium Digitales Geld
20. - 21. Juni 2002 - Institut für Telematik, Trier

Dr. Rainer Baumgart



1

Agenda



- **Einleitung**
- Kreditkartengestützte Verfahren
- Kontenbasierte Verfahren
- Chipkartengestützte Verfahren
- Mobile Bezahlverfahren
- Bargeldartige (anonyme) Verfahren
- Verfahren für Micropayments
- Zusammenfassung

2

Konventioneller Handel

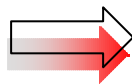


Bezahlung:

- Bargeld
- Schecks
- Kreditkarte
- EC-Karte
 - „electronic cash“ mit PIN
 - ELV (ggf. Sperrlisten des Handels)
 - POZ (ab 60,- DM Sperrlisten der Banken)
 - „electronic cash offline“
- Rechnung, Überweisung/Lastschrift
- ...

3

Elektronischer Handel



**elektronische
Zahlungsmechanismen**

4

— Agenda

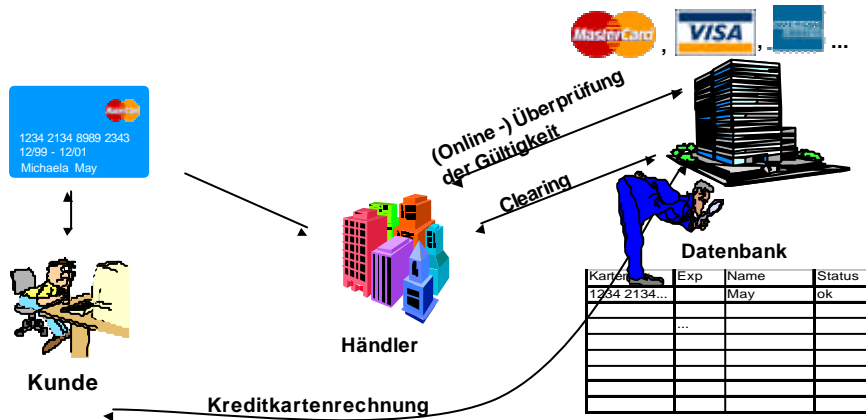


- Einleitung
- **Kreditkartengestützte Verfahren**
- Kontenbasierte Verfahren
- Chipkartengestützte Verfahren
- Mobile Bezahlverfahren
- Bargeldartige (anonyme) Verfahren
- Verfahren für Micropayments
- Zusammenfassung

— Kreditkartengestützte Verfahren

- Naive Anwendung – Mail-Order-Telephone-Order (MoTo)
- Schutz durch Kanalverschlüsselung
- SET

Das Kreditkartensystem



7

Kreditkartenbetrug (Auswahl) ...

- Gültige Kartennummern sind keinesfalls ausreichend für Autorisierung
z.B. AMEX-Cancellation Bulletin:
 - 37xx xxxxxx x101y → 37xx xxxxxx x100(y+2 mod 10)
 - Programme die gültige Kartennummern generieren
 - Trashing, ...
- Missbrauch durch „Kunden“ (bei MoTo)
 - XY missbraucht Kreditkarte von YZ und ..., Schaden: abc Tausend €
 - Kölner Betrüger „kauft“ Waren für 250.000,- € , Trashing
- Diebstahl von Kartennummern
 - (07/97, news.com) Kartennummern von NBA, ESPN Server gestohlen
 - (01/00): „Maxus“ hackt CD-Universe-Site, 300.000 Kartennummern
- Missbrauch durch Händler (05/99, LA-Times, u.v.a.)
 - Kenneth H. Taves, Malibu, „Sex-Unternehmer“
 - 49.4 Mio US\$ Umsatz in 1998, davon 3.9 Mio US\$ legitim

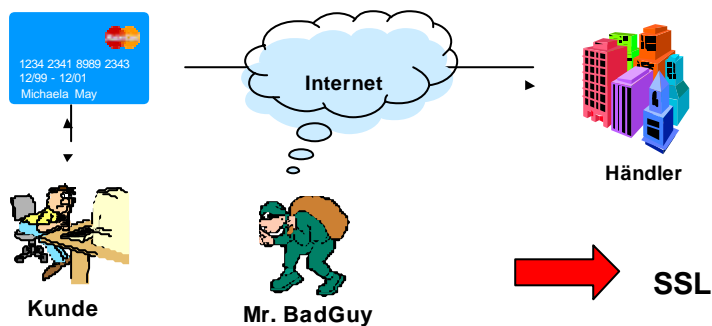
8

... Kreditkartenbetrug (Auswahl)

- 900.000 erzeugte / gesammelte Kartennummern
 - (03/00): Micro\$oft-Tochter Expedia in I/00: 4-6 Mio US\$ Verlust durch Fraud
- (05/00, dpa) Kriminalitätsstatistik Deutschland 1999:
 - Kriminalität insgesamt rückläufig, Kreditkartenbetrug +40%

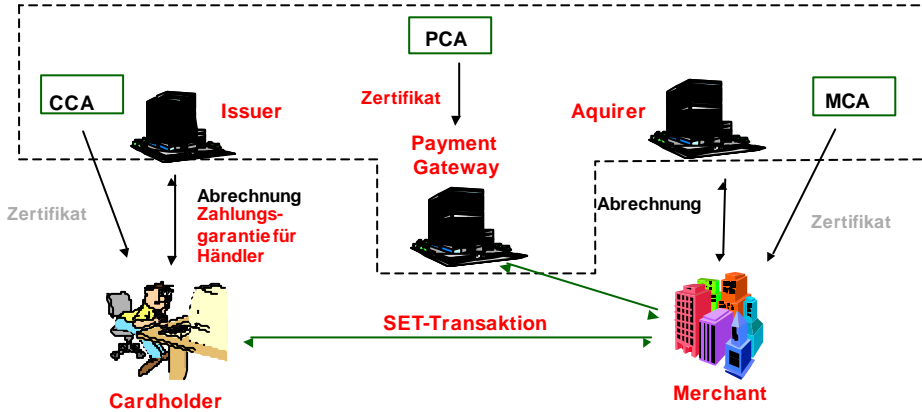
9

Kreditkarte im Internet

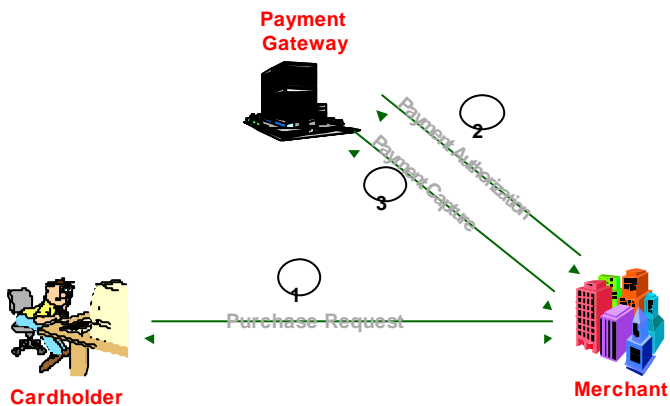


10

SET - Überblick



SET-Bezahlvorgang - Überblick



Sicherheit der Kreditkartengestützten Verfahren

- naive Anwendung der Kreditkarte im Internet ist Russisches Roulette
- SSL setzt Vertrauen in Händler voraus
 - Händler sollte weitergehende Sicherheitsmechanismen verwenden
- SET
 - sehr sicher durch PKI-Technologie
 - bislang kaum verbreitet
 - (langfristig vielleicht) die benötigte Infrastruktur für elektronische Geschäfte im B2C – Umfeld

13

Agenda



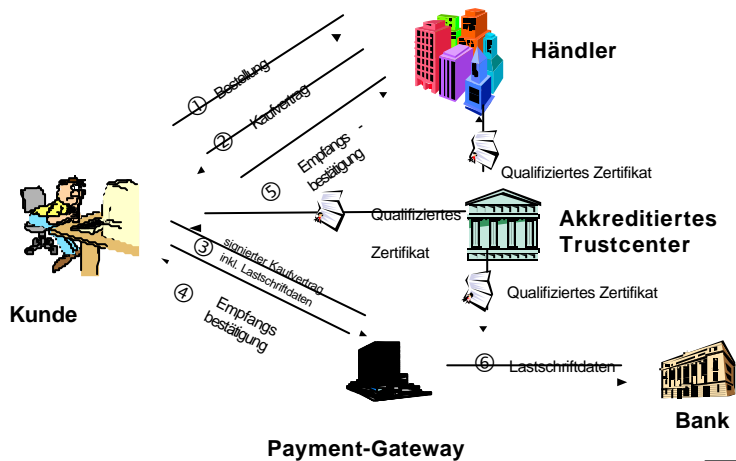
- Einleitung
- Kreditkartengestützte Verfahren
- **Kontenbasierte Verfahren**
- Chipkartengestützte Verfahren
- Mobile Bezahlvverfahren
- Bargeldartige (anonyme) Verfahren
- Verfahren für Micropayments
- Zusammenfassung

14

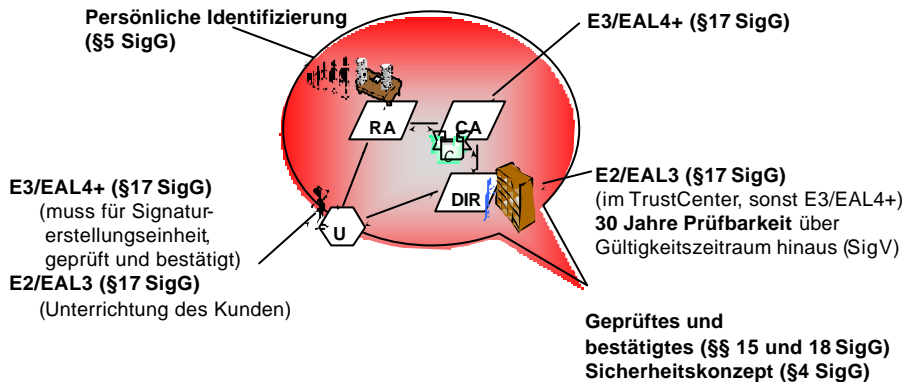
Kontenbasierte Verfahren

- Lastschrift mit elektronischer Signatur
- Eleanor (B2B)
- e-PaymentsPlus (B2B)
- internetCASH

Lastschrift mit elektronischer Signatur



Anforderungen an TrustCenter mit Anbieterakkreditierung gemäß §15 SigG



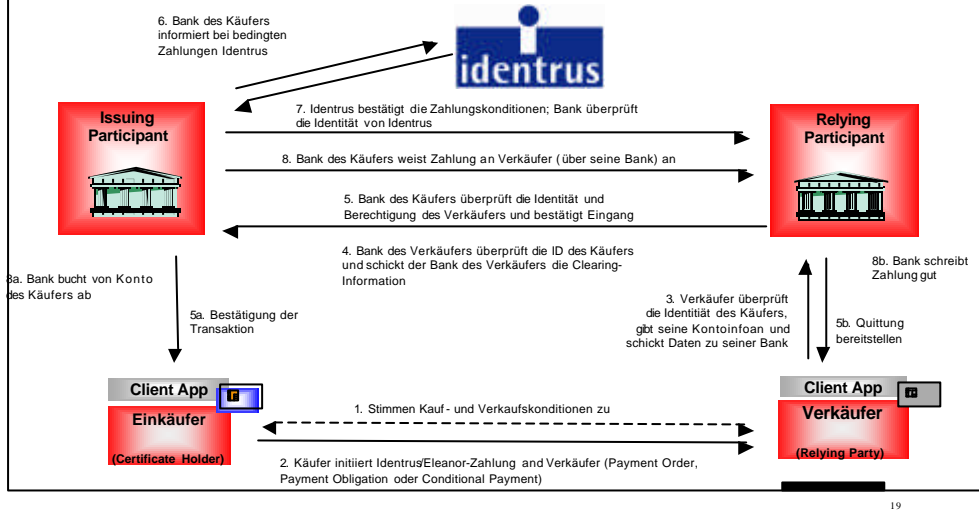
17

Eleanor Zahlungsmechanismen

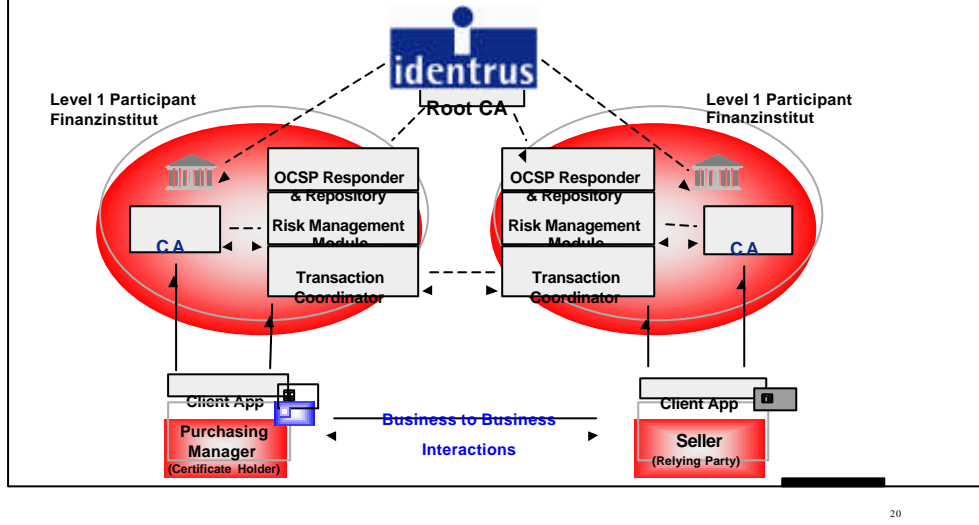
- **Verschiedene Zahlungsprodukte**
 - Payment Orders
 - durch Käufer stornierbar
 - Haftungsdeckung durch Käufer
 - Payment Obligation
 - nur durch Käufer und Verkäufer gemeinsam stornierbar
 - Haftungsdeckung durch Käufer
 - Certified Payment Obligation
 - nur durch Käufer und Verkäufer gemeinsam stornierbar
 - Haftungsdeckung durch die Bank des Käufers
- **mit optionalen Bedingungen**
 - zahlbar, sofern vereinbarte Konditionen erfüllt werden

18

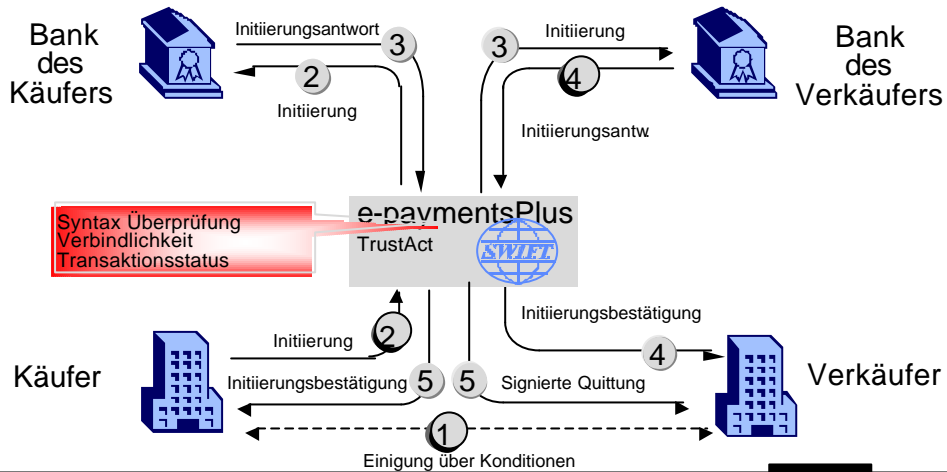
Eleanor Ablauf



Identrus - Funktionale Architektur



S.W.I.F.T.'s e-paymentsPlus



21

internetCASH

- CTO Y. Tsiounis, Verbreitung in NY, CA, MA, ...
 - vorausbezahlte Papierkarten, ähnlich wie US-Telefonkarten in Supermärkten, Tankstellen ...
- Registrierung bei www.spendcash.com über SSL
- Karten-ID von Karte, 20 Zeichen, (wegrubbeln)
- PIN 4-8 Zeichen (+ opt. Reminder falls vergessen)
- Bezahlung
 - SSL-Leitung zu Spendcash
 - PIN, Karten-ID (K-ID ggf. auf Rechner gespeichert)
 - Bestätigung zu Händler
 - einfache Möglichkeit mehrere Karten zu verbinden



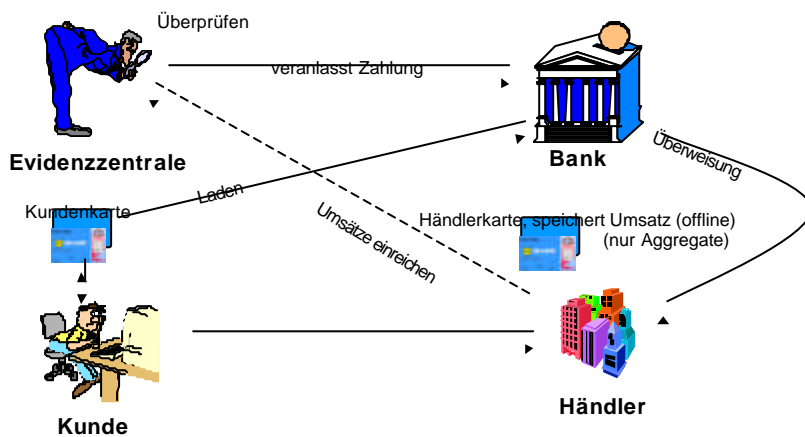
22

Agenda

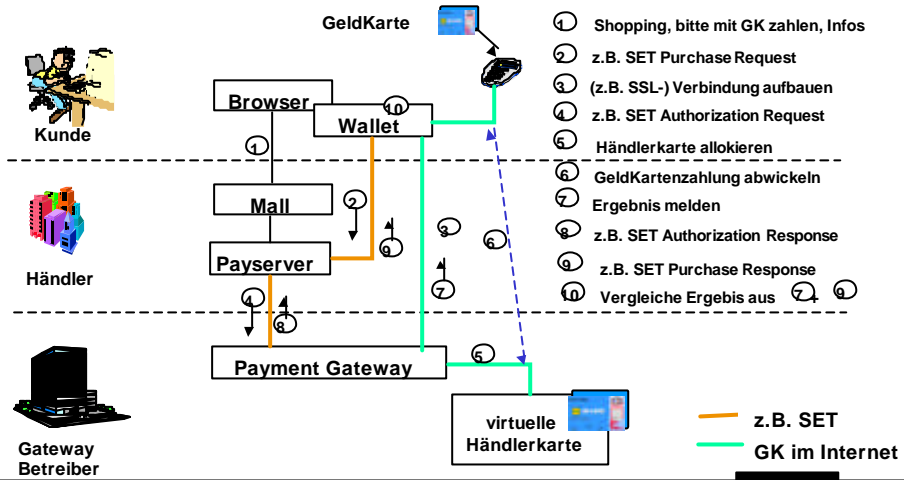


- Einleitung
- Kreditkartengestützte Verfahren
- Kontenbasierte Verfahren
- **Chipkartengestützte Verfahren**
- Mobile Bezahlfverfahren
- Bargeldartige (anonyme) Verfahren
- Verfahren für Micropayments
- Zusammenfassung

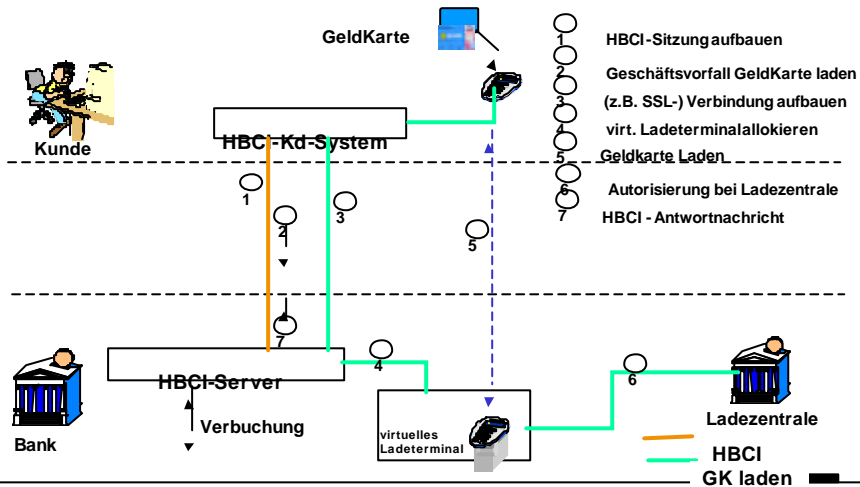
GeldKarte - Systemarchitektur



Bezahlen mit GeldKarte im Internet



Aufladen der GeldKarte über HBCI



Sicherheit der GeldKarte

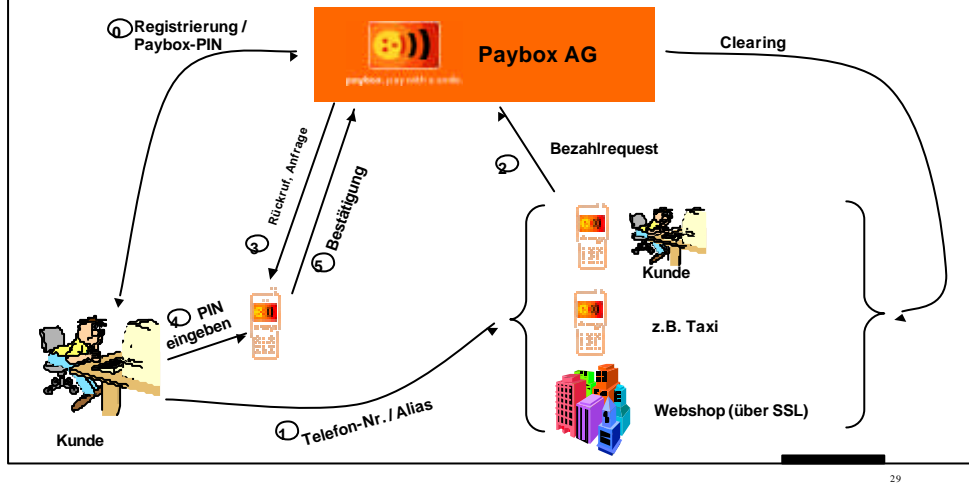
- Hohe Sicherheit durch Chipkarteneinsatz
- Grundsätzliche Problematik des symmetrischen Schlüsselmanagements erfordert hohe (technische und organisatorische) Sicherheitsmaßnahmen im Backend
- Adaption für Internet-Anwendung erfordert weitere Sicherheitsmaßnahmen (Klasse 3 Leser)

Agenda



- Einleitung
- Kreditkartengestützte Verfahren
- Kontenbasierte Verfahren
- Chipkartengestützte Verfahren
- **Mobile Bezahlverfahren**
- Bargeldartige (anonyme) Verfahren
- Verfahren für Micropayments
- Zusammenfassung

Paybox



29

Sicherheit des Paybox-Verfahrens

- Basiert auf GSM-Sicherheitsmechanismen
- Bekannte Schwachstellen in GSM
 - IMSI-Catcher erlauben
 - eine Basis-Station zu maskieren und
 - Verschlüsselung zwischen Handy und „Basis-Station“ auszuschalten
 - Benutzer kann maskiert werden durch
 - Clonen der SIM-Karte
 - Ausnutzen von Schwachstellen in COMP128 (A3/A8)
 - Angriff setzt Zugang zu Handy und PIN für 8-12h voraus
 - <http://www.isaac.cs.berkeley.edu/isaac/gsm.html>
 - Abhören der Authentifikationsinformationen
 - Zur Authentifikation wird das Tripel (RAND, SRES, Kc) vom AuC im Heimatnetz erzeugt
 - Übertragung des Tripels zum besuchten Netz meist über unverschlüsselte Richtfunkstrecken

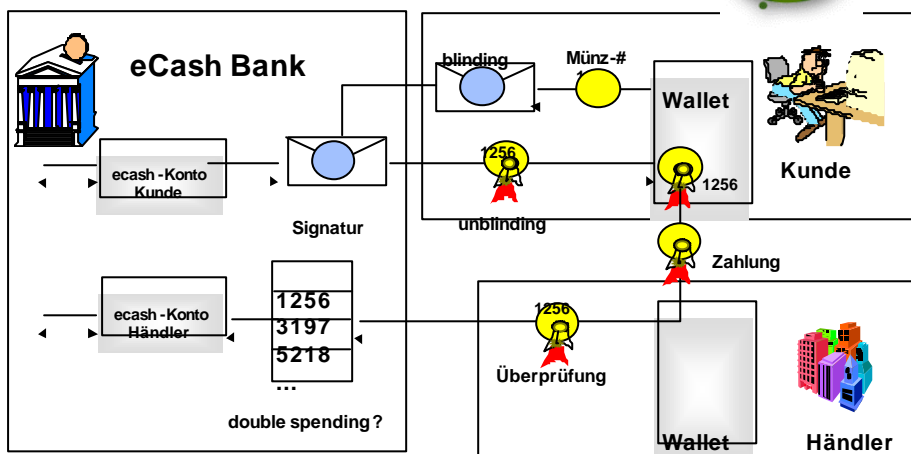
30

Agenda



- Einleitung
- Kreditkartengestützte Verfahren
- Kontenbasierte Verfahren
- Chipkartengestützte Verfahren
- Mobile Bezahlfverfahren
- Bargeldartige (anonyme) Verfahren
- Verfahren für Micropayments
- Zusammenfassung

eCash-Ablauf




eCash-Bemerkungen

- Blind signatures von Chaum eingeführt (Crypto '82)
- RSA-Blinding: rohe Münze x , Blinded $r^{eh(x)}$, signed/unblinded $(x, h(x)^{1/e})$
- DigiCash - Konkurs 1998 \Rightarrow eCash Technologies Inc.
- Übernahme durch InfoSpace Inc. (Feb. 2002)
- Münzen haben bestimmten Wert
- Wechseln der Münzen durch Einreichen und Neuausgabe bei Bank
- Zahlung zwischen Personen möglich, z.B. in email / als Anhang


```
-----BEGIN ECASH PAYMENT-----
oLmQgwAExKGgiqCukiEbkIECKIIF3JCBMZCBCZGEMvhctpCEMwrRtpCBG5KFYmx1
....
LbNqsFvuff9lx9r0i3tJ1x2VNy7DqhCKXD+za9XOP6CimUY8obTXIVDvoaC*kIEB
-----END ECASH PAYMENT-----
```
- Erhaltene Münzen müssen erst bei der Bank gegen neue „getauscht“ werden

SuperCash

- NTT, japanische Telekom 
- ähnlicher Aufbau wie eCash, münzbasiert, anonym + einige Features
- basiert auf Arbeit „An efficient divisible electronic cash scheme“ von T. Okamoto, CRYPTO '95
- bei doublespending wird Identität des Betrügers festgestellt
- bei Initialisierung wird BitCommitment der ID durchgeführt
- Münzen können **ohne** Bank geteilt werden
- aus einer gespeicherten Münze wird Binärbaum abgeleitet und nur mit einem bestimmten Blatt des Baumes bezahlt
- **zusätzlicher** SmartCard-Einsatz
 - auch in realen Geschäften einsetzbar
 - für die Speicherung elektronischer Tickets
 - Aufladen über Telefon

Agenda



- Einleitung
- Kreditkartengestützte Verfahren
- Kontenbasierte Verfahren
- Chipkartengestützte Verfahren
- Mobile Bezahlverfahren
- Bargeldartige (anonyme) Verfahren
- **Verfahren für Micropayments**
- Zusammenfassung

Motivation / Einsatzgebiete

- **Kleinstbezahlungen**
(bis zu < 0,10 €) für
 - Zeitungsartikel
 - Aktienkurse
 - Datenbankrecherchen
 - ...
 - **Earn-per-click**
 - man erhält Geld für's surfen, z.B. bei Umfragen etc.
 - Kundenbindung, Bonusprogramme
 - **Problem**
 - herkömmliche Zahlungsmechanismen zu aufwendig
⇒ Transaktionskosten oft größer als Wert
 - Studien: (noch?) Marktlücke
- } „Content“-Billing, d.h. Infos, Dienstleistungen, die zum Verschenken zu teuer sind

— Micropayments - konventionelle Alternativen

- Kundenkonto bei Anbieter
 - pre/post-paid, Clearing über Macropayments
 - Datenbankeintrag bei Verkäufer ist Konto
 - Authentisierung durch Klartext-Passwort unzureichend
 - nur für statische Geschäftsbeziehungen, kein Surfen möglich
- Bezahlung über Provider
 - T-Online / BTX
 - abhängig von Zeit für kostenpflichtige Angebote
 - bei wirklichen Micropayments nicht rentabel
- Finanzierung durch Werbung
 - nur für große Anbieter machbar
 - oft störend (/ unwirksam, da Filter)
- Nicht Anbieten / Verschenken von Informationen

— Micropayment-Verfahren

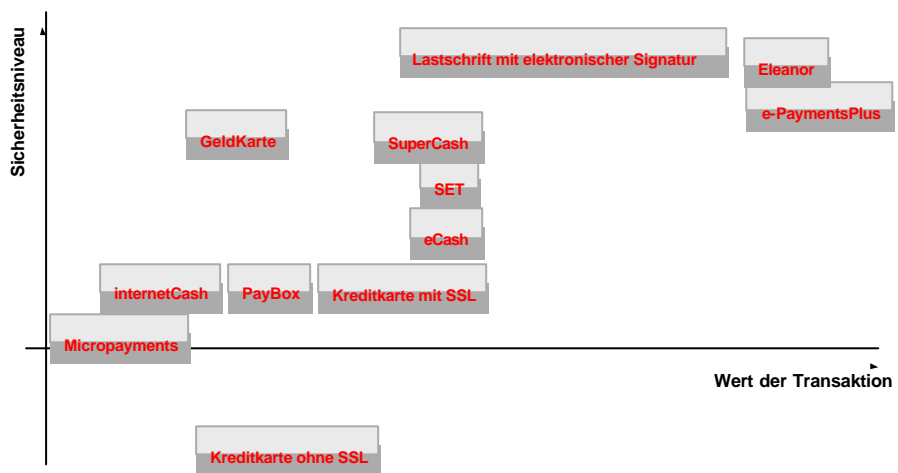
- Millicent
 - vernünftige Performance
 - Bezahlung führt zu keinem Performance-Verlust
 - Schlüsselverwaltung jedoch problematisch
 - Vertrauen für Broker und Händler nötig
- MiniPay
 - relativ großer Overhead durch PK-Technologie
 - Vertrauen für Händler und Clearingstellen nötig
- PayWord
 - elegantes Verfahren
 - jedoch noch keine (sichtliche) praktische Umsetzung
- W3C: „Common Markup for micropayment per-fee-links“

Agenda



- Einleitung
- Kreditkartengestützte Verfahren
- Kontenbasierte Verfahren
- Chipkartengestützte Verfahren
- Mobile Bezahlverfahren
- Bargeldartige (anonyme) Verfahren
- Verfahren für Micropayments
- Zusammenfassung

Die vorgestellten Maßnahmen im Überblick



Zusammenfassung

- Wert der Transaktionen bestimmt adäquates Schutzbedürfnis
- Angemessene Sicherheit elektronischer Zahlungsmechanismen ist wichtige Grundvoraussetzung für langfristigen Erfolg
- Einsatz zeitgemäßer Mechanismen, wie
 - Public-Key-Infrastrukturen
 - Smart Cardskann die sichere Umsetzung erleichtern

Vielen Dank für Ihre Aufmerksamkeit.

secunet Security Networks AG
rainer.baumgart@secunet.com
www.secunet.com