Zahlungssysteme im INTE

Birgit Pfitzmann
Universität Hildesheim
pfitzb@informatik.uni-hildesheim.de

DFN-Betriebstagung, Berlin, 11.10.1995

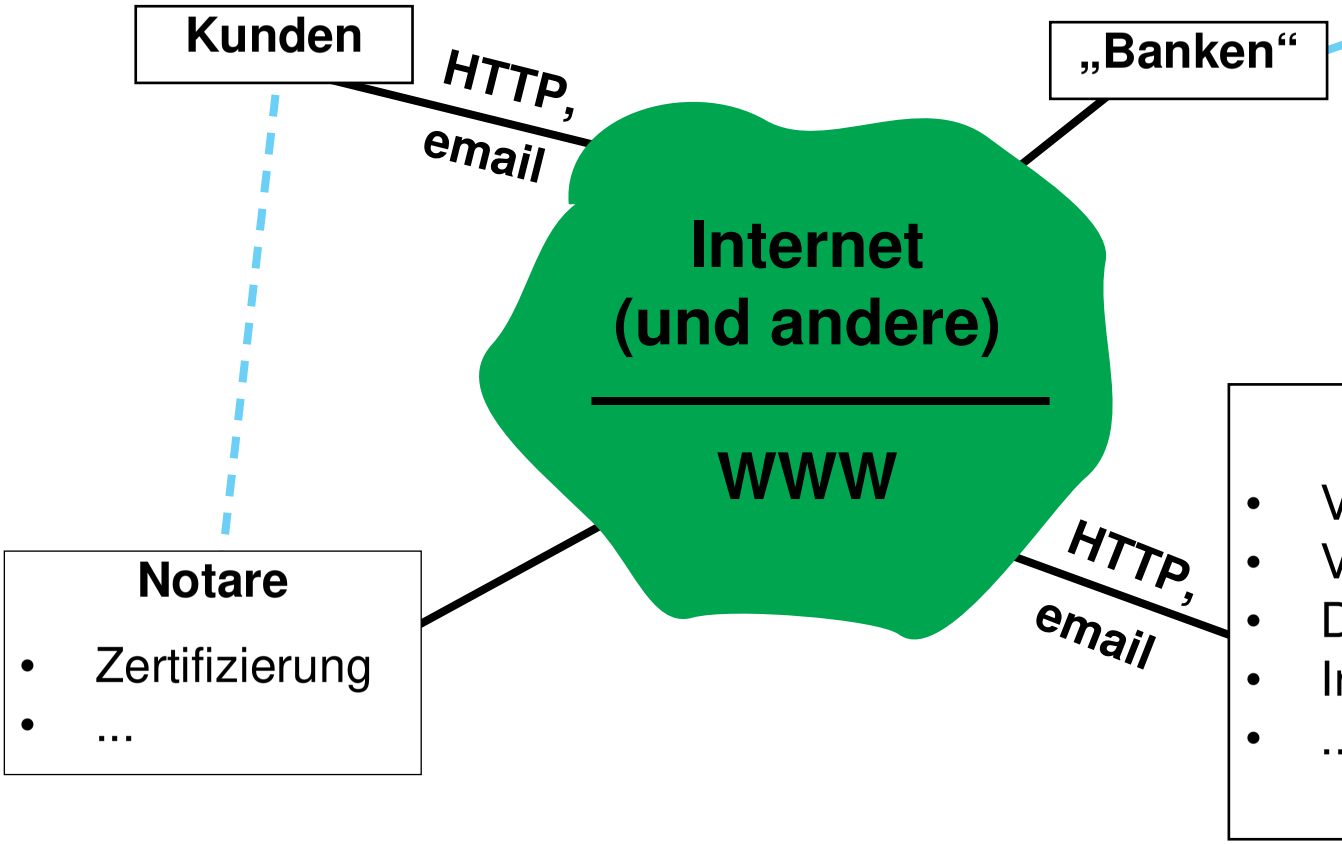
1 Einführung
2 Eigenschaften (Funktionalität, Sicherheit, Date
3 Überblick konkrete Vorschläge
4 Mechanismen
5 Ausblick

Quellen: <http://www.informatik.uni-hildesheim.de/~sirene/>
Dank: Michael Waidner, IBM Forschungslaboratorium, Zü

© Birgit Pfitzmann, Hildesheim, 10.10.1995

1 Einführung

1.1 Kontext: Internet als „Marktpla



1.2 Digitale Zahlungssysteme

Wie „richtiges“ Geld, nur …

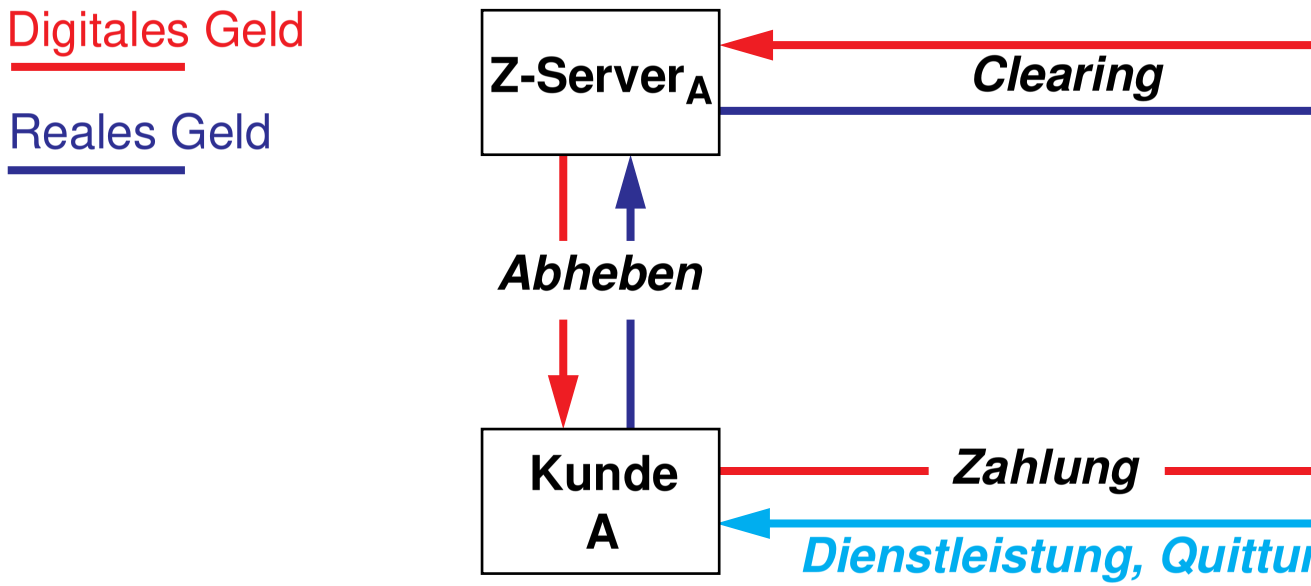
in Netzen benutzbar,
sicherer,
billiger

??

Viele Arten, keine genau wie „richtiges“
Lieber nichts voraussetzen.

2 Eigenschaften

2.1 Funktionalität

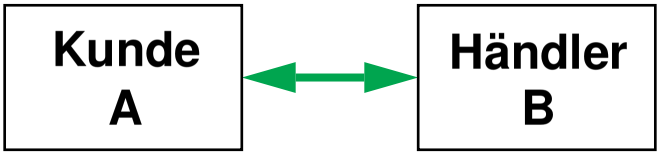


- Ablauf
  - „Prepaid“: Abheben vor Zahlung
  - „Pay-now“: " ≈ "
  - Kredit: " nach " (≠ Debit

  Bsp.: Telefonkarte / ec-Verfahren / Kreditkarten

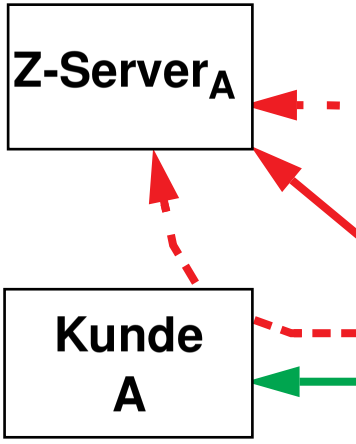
- Kommunikation bei Zahlung

Offline



+ Weniger Kommunikation
– Vermeidung von Mehrfachausgeben?
  - Sicherheitsmodule: Smartcards, PCMCIA, SmartDisks
  - Nachträgliche Prüfung

Online



– Kommunikation Z-Server
+ Mehrfachausgabe meidbar

- Universell?
  - Nicht: Händler = Bank
  - Nicht: Vorweg bekannter Händler
  - Beliebige Beträge
    - Schranken

    - Darstellbarkeit (Wechselgeldproblem)
    - Begrenzte Gültigkeitsdauer
- Offen?
  - Beliebige Kunden, z.B. Kinder
  - Beliebige Händler
  - Mehrere Banken
  - Mehrere Hersteller / Browser / Plattformen

- Erweiterungen
  - Quittungen
  - Kontoauszüge u.ä. (Transparenz)
  - Mehrere Währungen
  - Stornierung
  - prepaid: Verlusttoleranz
  - offline: Transferierbarkeit

Ziel: Mehrseitige Sicherheit

- Anforderungen aller Parteien betrachtet, z.B.
  - Bank: Sicherheit gegen Geldvermehrung durch Kunde
  - Kunden: Sicherheit gegen Betrug durch Händler und B
- Sicherheit von Partei *X* beruht auf
  - Geräten im Besitz von *X*
  - Software darin
  - nur minimal auf Wohlverhalten anderer Parteien

Entspricht alltäglicher Rechtssicherheit: Stets ausreichende B

Zur Zeit noch nicht in allen Vorschlägen

- Vor Außenstehenden: Verschlüsselung — una
- Anonymität
  - Meist nur für Kunden und nur bei Zahlung
  - Existierende Systeme
    - Bargeld: Zahlungen anonym und unverkettbar
    - Überweisungen, Kreditkarten: nicht anonym

    $\Rightarrow$ Bei kleinen Werten Anonymität wie bei Bargeld akzeptie
  - Rechtssicherheit und Anonymität kein Widerspruch
    - Bei Betrug (z.B. Sicherheitsmodul gebrochen) Identifizi
    - Wo nötig, Identifikation außerhalb Zahlungssystem
    - Sicherer Kauf unter Pseudonymen möglich
  - Bzgl. Händler nur zusammen mit anonymem Nachrichtena

- Abschwächungen von Anonymität:
  - Verkettbarkeit z.T. zwecks Effizienz vorgeschlagen; als
    ab gewisser Datenmenge Reidentifizierung
  - Aufdeckbarkeit für Strafverfolgung
    - Meist nur Geldempfängerzu identifizieren
    - Ggf. Spezialverfahren mit verteilter Aufdeckinforma

    Gefahr der Datensammlung, auch wirtschaftlich, mit ab
  - Wenigstens Händlerdaten vonBankdaten trennen

3 Überblick: Wichtige Vorschläge, Versuch

	online Zahlungen	offline Za

Nicht anonym (bis auf feste Pseudonyme)	Kreditkarten
	• Ungesichert
	• Rückfrage: First Virtual
	• Gesichert
	  • CyberCash
	  • CommerceNet (US-Marktplatz)
	  • iKP (IBM)
	  • SEPP (IBM, Mastercard, …)
	  • STT (VISA, Microsoft)
	Zahlungsserver
	  • NetBill (CMU, VISA)
	  • NetCheque (ISI)
		Sichere Zähler in S
		• Danmont, P
		• Express (Eu
		• CEN IEP (S
		• EMV (Europ
		... in „Wallet“
		• Mondex
		Bisher nicht für onli
		aber …

Anonym	Wechsler • NetCash (ISI) • Anonymous Creditcard (AT&T) Blinde Signaturen • e-cash (DigiCash)	Blinde Signaturen • CAFE (EU-I Bisher nicht für onli aber …

4 Mechanismen

4.1 Benutzergeräte

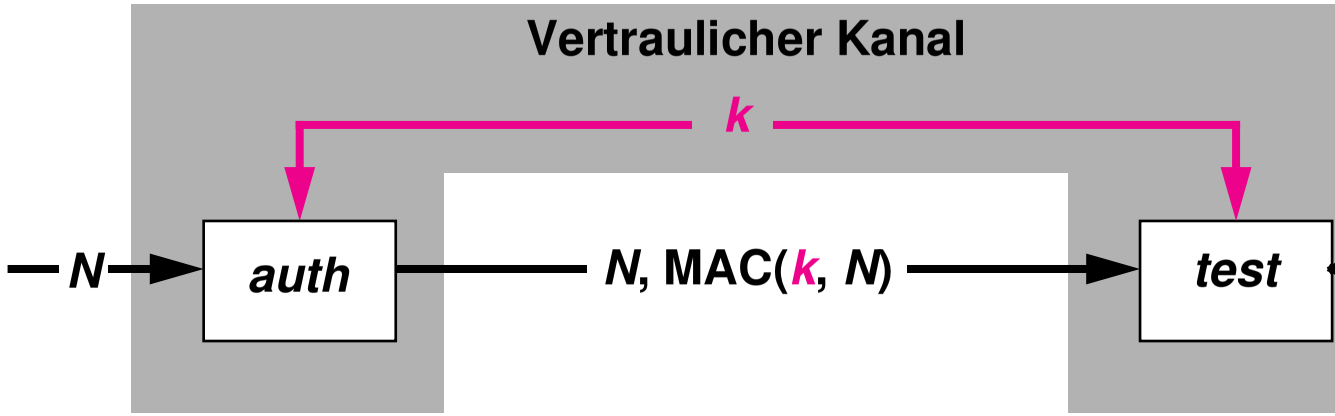
Benutzer muß Gerät vertrauen

- Zumindest während einer Sitzung („Fake-Terminal-Angriff“
- Bei sichereren Protokollen auch Schlüsselspeicherung

⇒ Mehrbenutzersysteme eigentlich unakzeptabe
blematisch

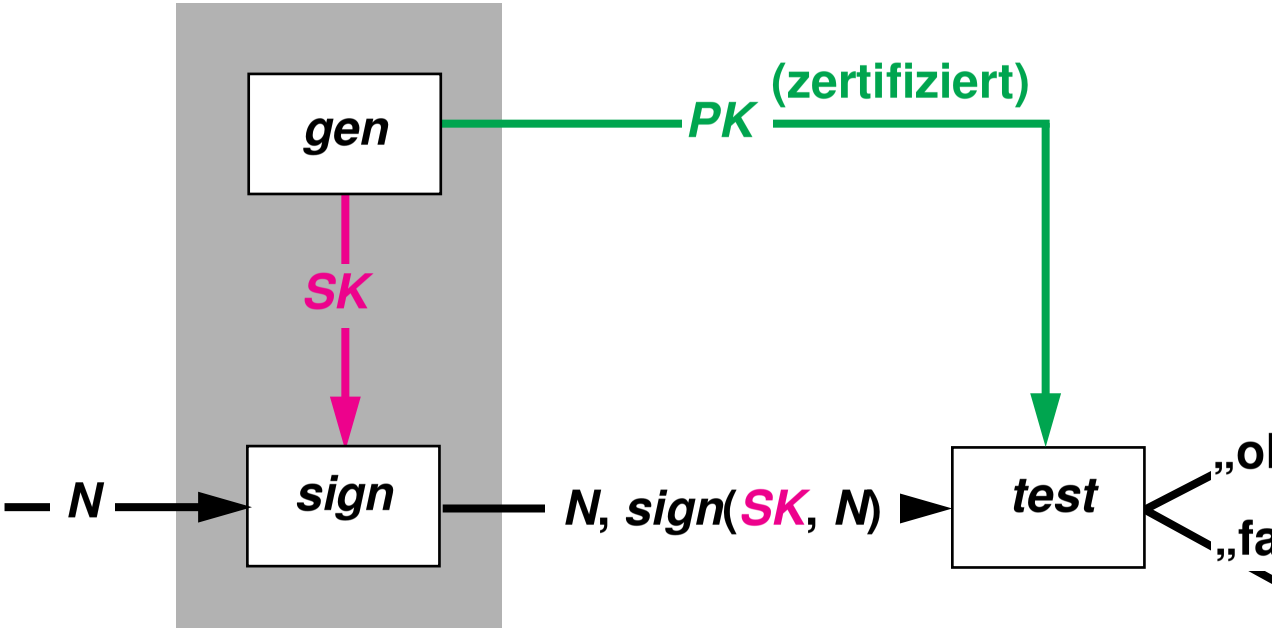
⇒ Mittelfristig wohl Smartcards o.ä. (Infrarotansc
langfristig portable Geräte mit Ein- und Ausgab

A. Symmetrisch



+ Relativ schnell
– Kein Nachweis gegenüber Dritten

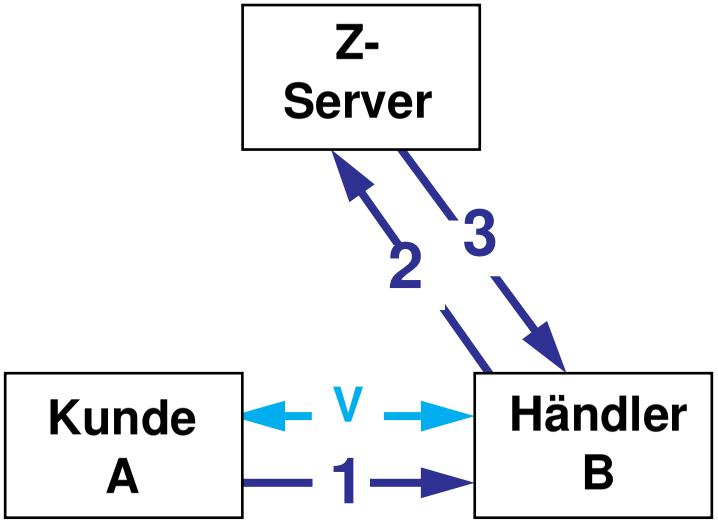
B. Asymmetrisch: Digitale Signaturen



+ Nachweis gegenüber Dritten („Beweismittel"
– Rechenintensiver (Software: Sekundenbere

4.3 Nicht anonyme online Zahlungssy

Kanonisches Beispiel: Gesicherte Kreditkartenza



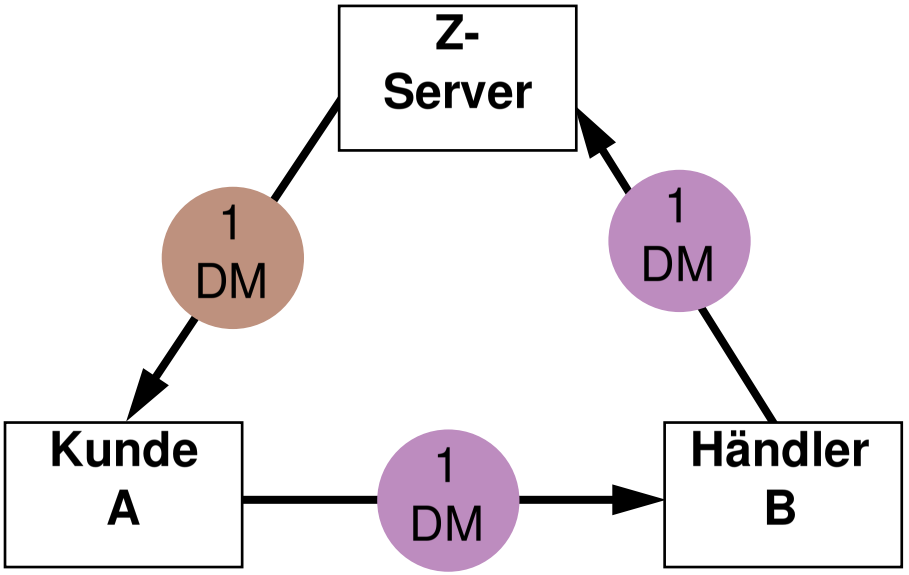
V
= Vertra

- Digitale Signaturen, insbes. in 1, 3 (Bsp. 3KP)
- 1 in 2 enthalten
- 1 verschlüsselt gegen Händler, zumindest wenn nur PIN-b

Sicherstes Beispiel: Blind signierte „Münzen“

z.B. Grundlage für DigiCash ecash

- Information bestimmter Form
- von Bank digital signiert



abwarten;
umformen

- Kunde p
- Online-F
  noch nic

5 Ausblick

- Parallele Systeme zu erwarten
  - Bargeldartig für kleine Beträge
  - Kreditkartenartig für große Beträge
  - Evtl. „Micropayments“ noch extra
- Wandlungen zu erwarten, insbes. bei Geräten
- Marktplatz: Mehr als nur Zahlungssystem

  Sicherer Austausch, Kennenlernen, Copyright-Schutz

  …

  → SEMPER (EU-Projekt)
- Exportkontrolle aus USA ⇒ europäische Lösu

Nochmal Quellen: http://www.informatik.uni-hildeshei