Elektronische Zahlungssys

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

GI-Regionalgruppe Braunschweig, 31.1.1996

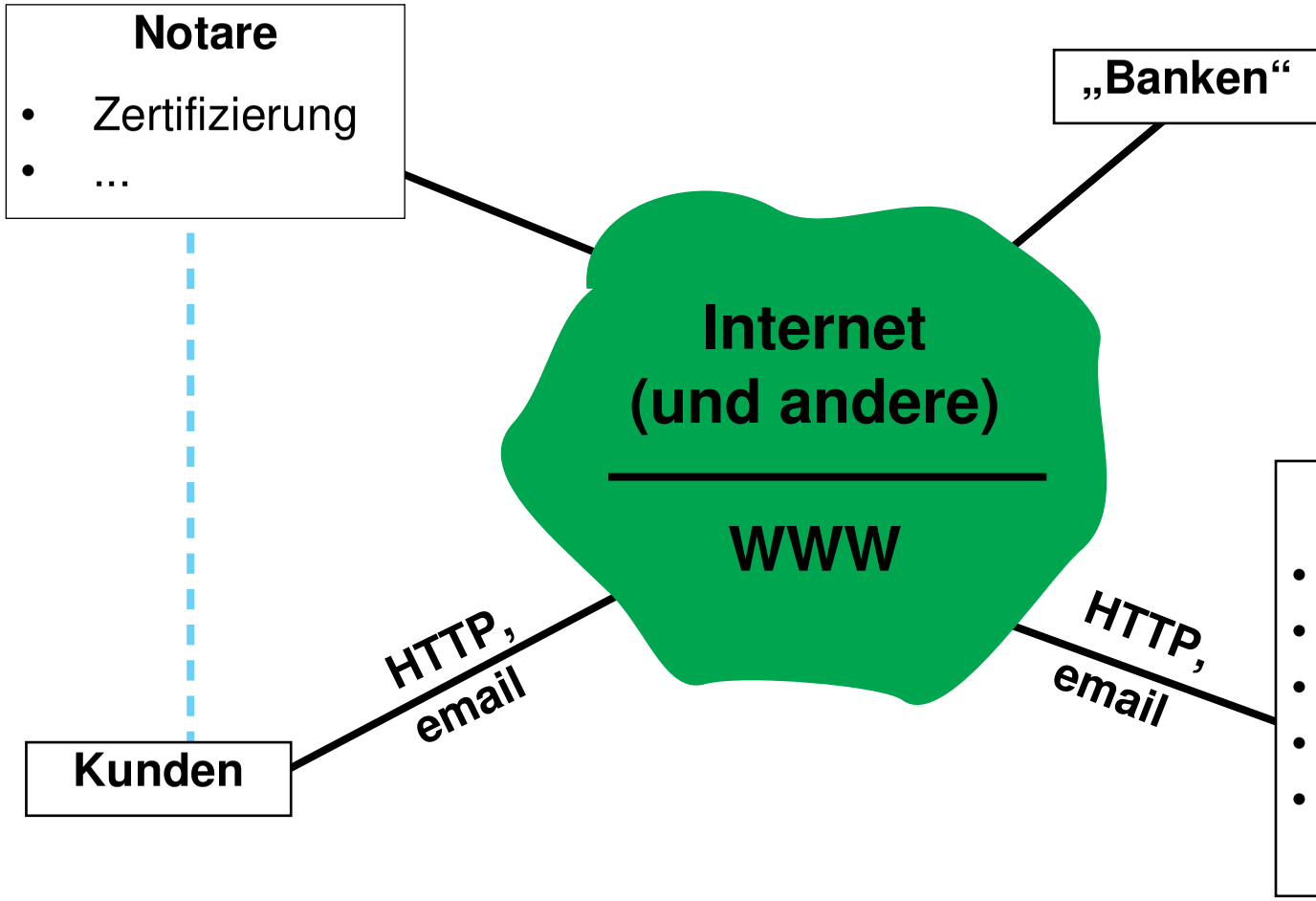
1 Einführung
2 Eigenschaften (Funktionalität, Sicherheit, Date
3 Überblick konkrete Vorschläge
4 Mechanismen
5 Elektronische Marktplätze
6 Ausblick

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

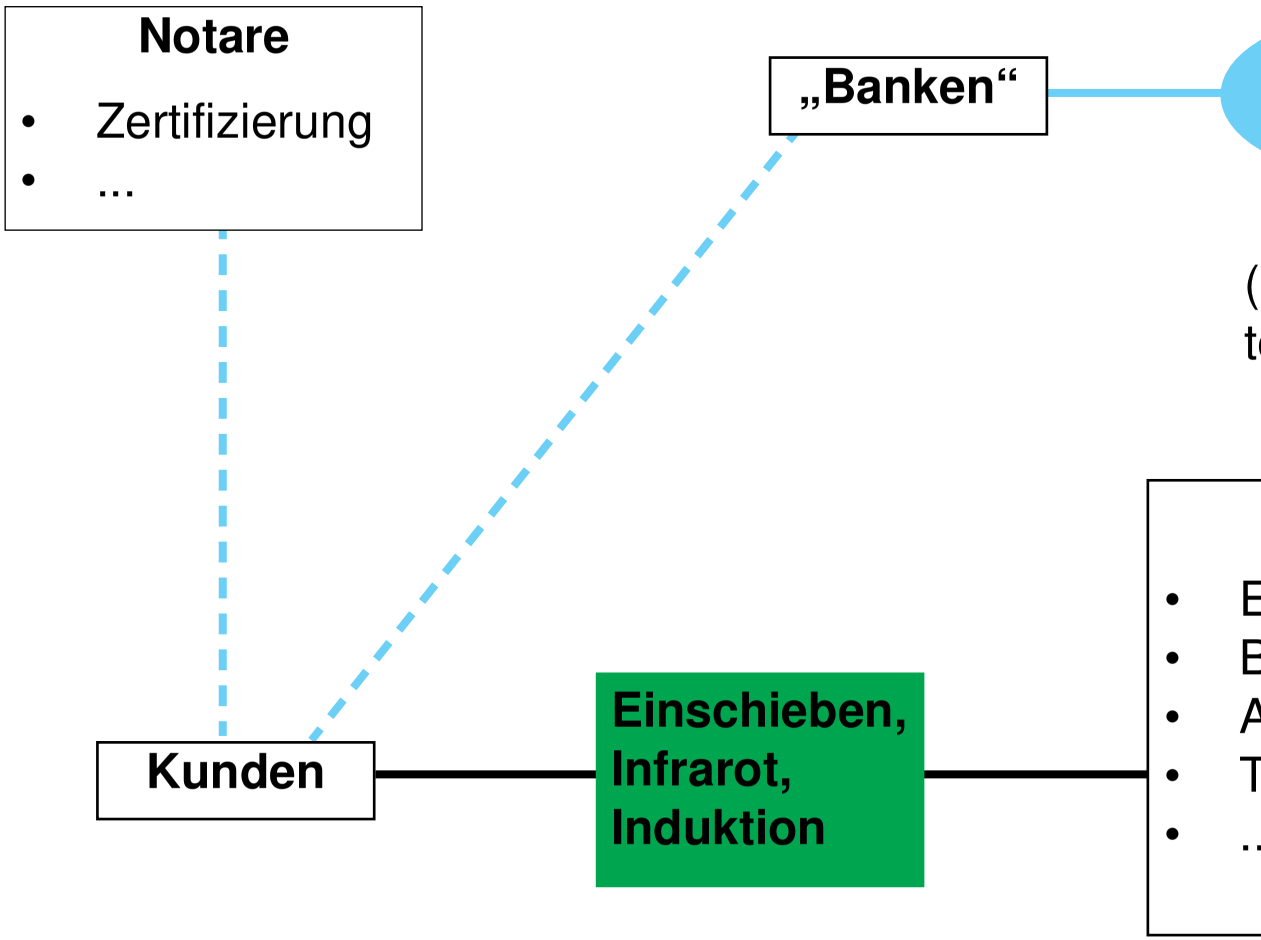
© Birgit Pfitzmann, Hildesheim, 31.1.1996

1 Einführung

1.1 Szenario A: Internet als „Marktp



1.2 Szenario B: Zahlungen in Läd



- Theoretische Kryptographie
- CAFE: ESPRIT-Projekt 92-95
  - „Conditional Access for Europe“
  - Primär Ladenszenario, mit Hardwareentwicklung
- SEMPER: ACTS-Projekt 95-98
  - „Secure Electronic Marketplace for Europe“
  - Primär Netzszenario, nicht pures Bezahlen
  - u.a. IBM, Europay, Otto-Versand

Wie „richtiges“ Geld, nur …

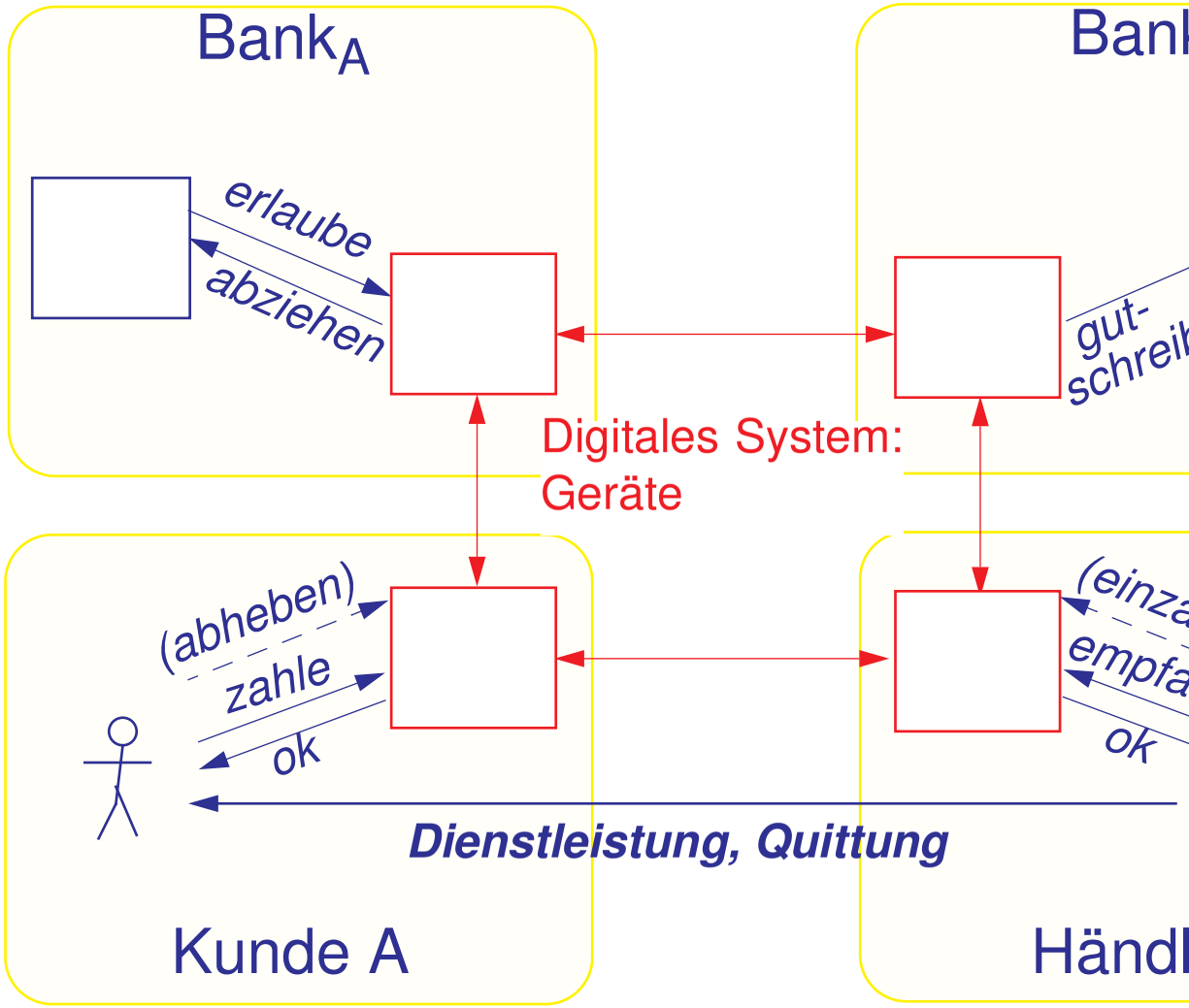
in Netzen benutzbar,
sicherer,
billiger

??

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

2 Eigenschaften

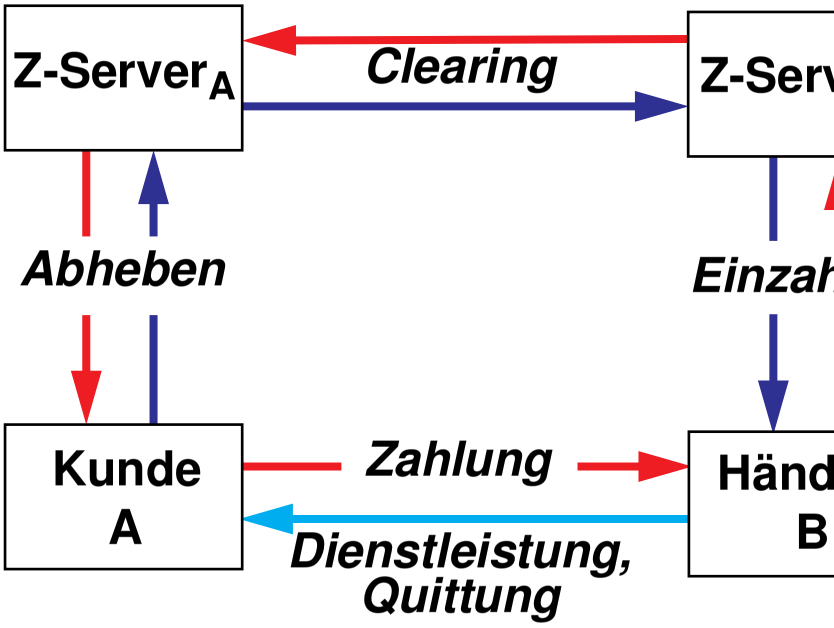
2.1 Funktionalität



- Zeitlicher Zusammenhang
  - „Prepaid“: *erlaube* vor *zahle.*
    Getrennte „Abhebung“ und „Zahlung“; üblichere Darstellun

Digitales Geld

Reales Geld

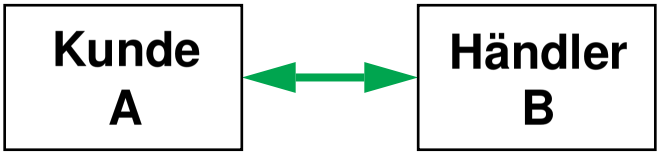


Bsp.: Telefonkarten, Bargeld relativ zu Konto

- „Pay-now“: *erlaube* während *Zahlung*
  Bsp.: ec-Verfahren, digitale Überweisung
- „Pay-later“ (vorläufige Zahlung): *erlaube* nachträglich.
  Bsp.: Kreditkarten heutzutage

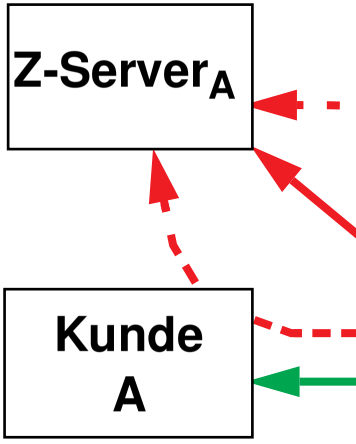
- Kommunikation bei Zahlung

Offline



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

Online



– Kommunikation Z-Server
+ Mehrfachausgemeidbar

- 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

  Könnte man meist zu Grundsystemen hinzufügen

  - 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

Beachte:

- Großrechner heutzutage nicht wirklich sicherbar.
- Mangelnde Beweismittel können beiden Seiten schade

Zur Zeit noch nicht in allen Vorschlägen

Zudem

- Keine expliziten Anforderungen $\Rightarrow$ Vorschläge oft schw
- Protokolle unvollständig, v.a. Streitfälle

- 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 im Ladenszenario oder zusammen mit a
    tenaustausch

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

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

3 Überblick: Wichtige Vorschläge, Versuch

	online Zahlungen	offline Za

Nicht anonym (bis auf feste Pseudonyme)	Kreditkarten
	• Ungesichert
	• Externe Teilsicherung: 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

- Herstellung, Auslieferung
- Im Gerät selbst erzeugte Geheimnisse
- Direkte Ein- und Ausgaben
- Gerät muß Benutzer bei Entscheidungen fragen
- Schutz vor und Verhalten bei Verlust und Diebstahl

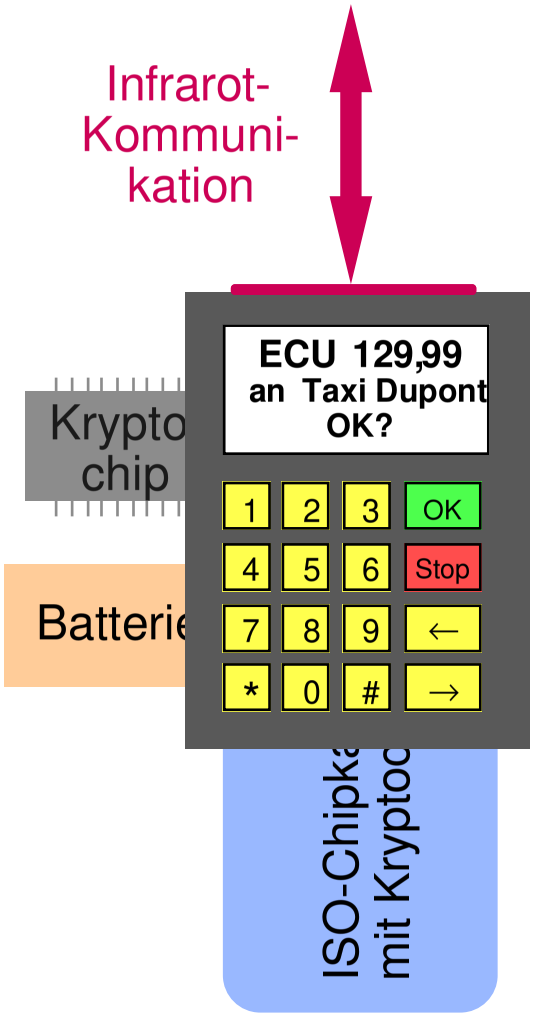
Hauptprobleme zur Zeit:

- Lädenszenario, selbst mit Smartcard:
  - PIN-Eingabe in fremdes Gerät
  - PIN-Eingabe beobachtbar
- Netzszenario: Betriebssystemsicherheit des PC oder gar M

  $\Rightarrow$ mittelfristig wohl Smartcard + eigener PC

⇒ Langfristig portable Geräte mit Ein- und Ausga

Bsp.: CAFE-Wallet



Herstellerunabhängig: Protokolle

- beliebigem Benutzergerät
- und beliebigem Sicherhei
  ISO-Chipkarte)

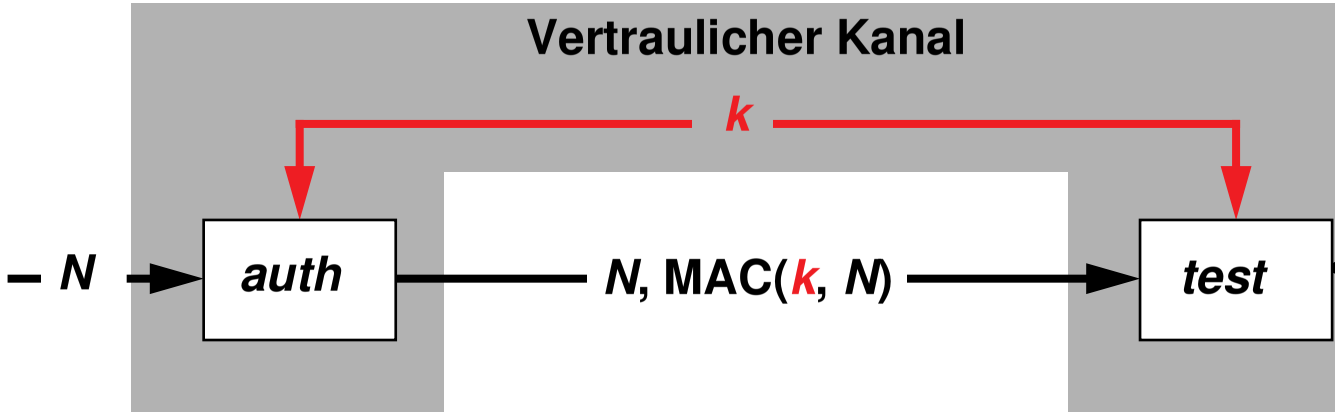
Wichtig: Multifunktionale

- Mobiltelefon
- PDA
- Uhr, Gameboy, …

Sicherheitsmodule kleine

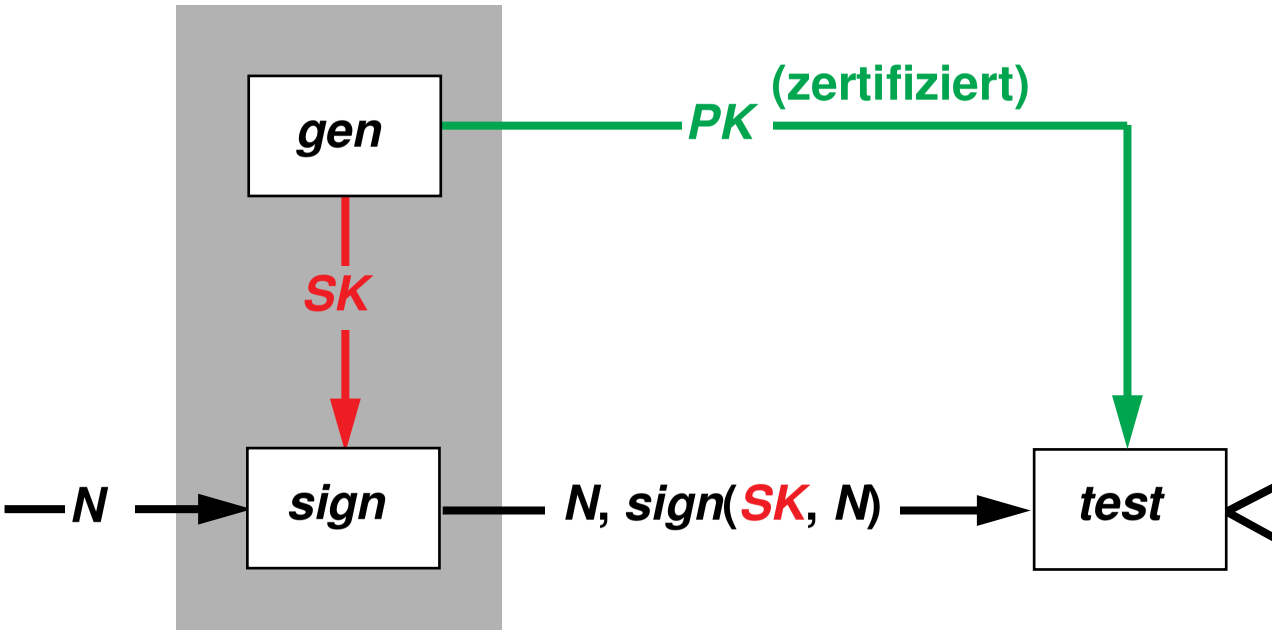
- GSM-Module
- Stahlkapseln
- In Schmuckform u.ä.

A. Symmetrisch



+ Relativ schnell
– Kein Nachweis gegenüber Dritten

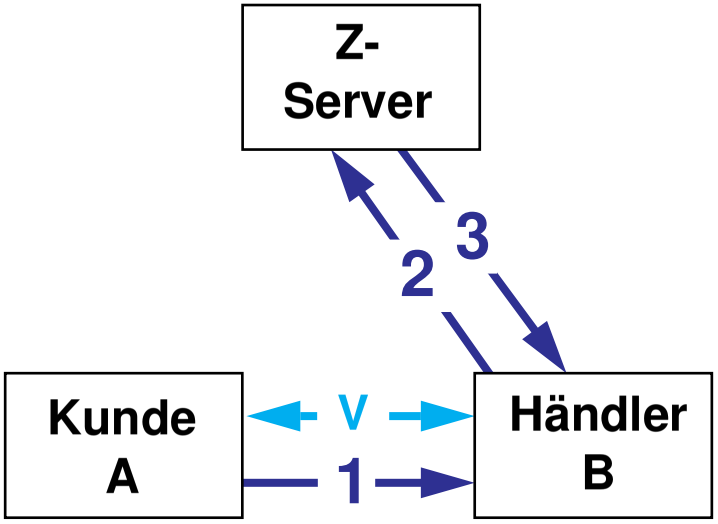
B. Asymmetrisch: Digitale Signaturen



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

4.3 Nicht anonyme online Zahlungssy

Kanonisches Beispiel: Gesicherte Kreditkartenza



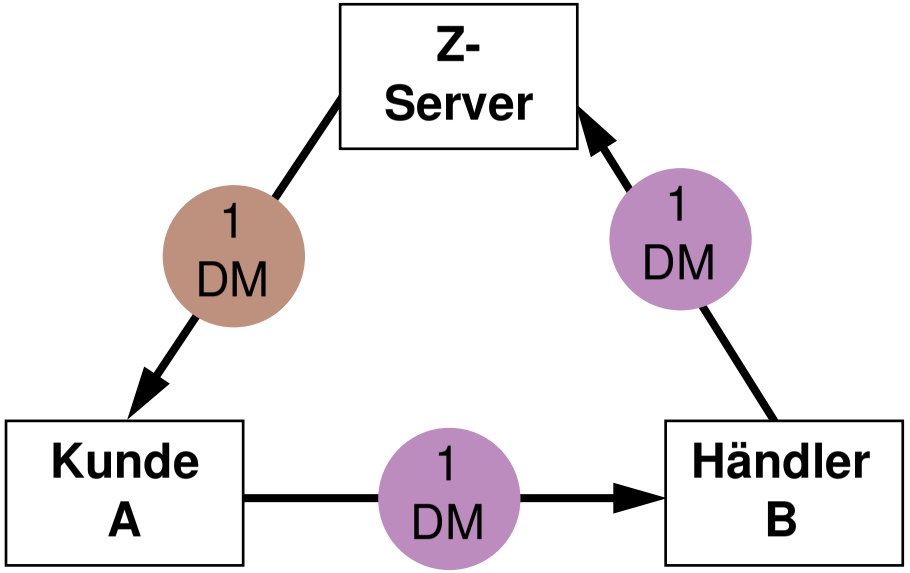
V
= Vertra

- Digitale Signaturen, v.a. 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 e-cash

- Information bestimmter Form
- von Bank digital signiert

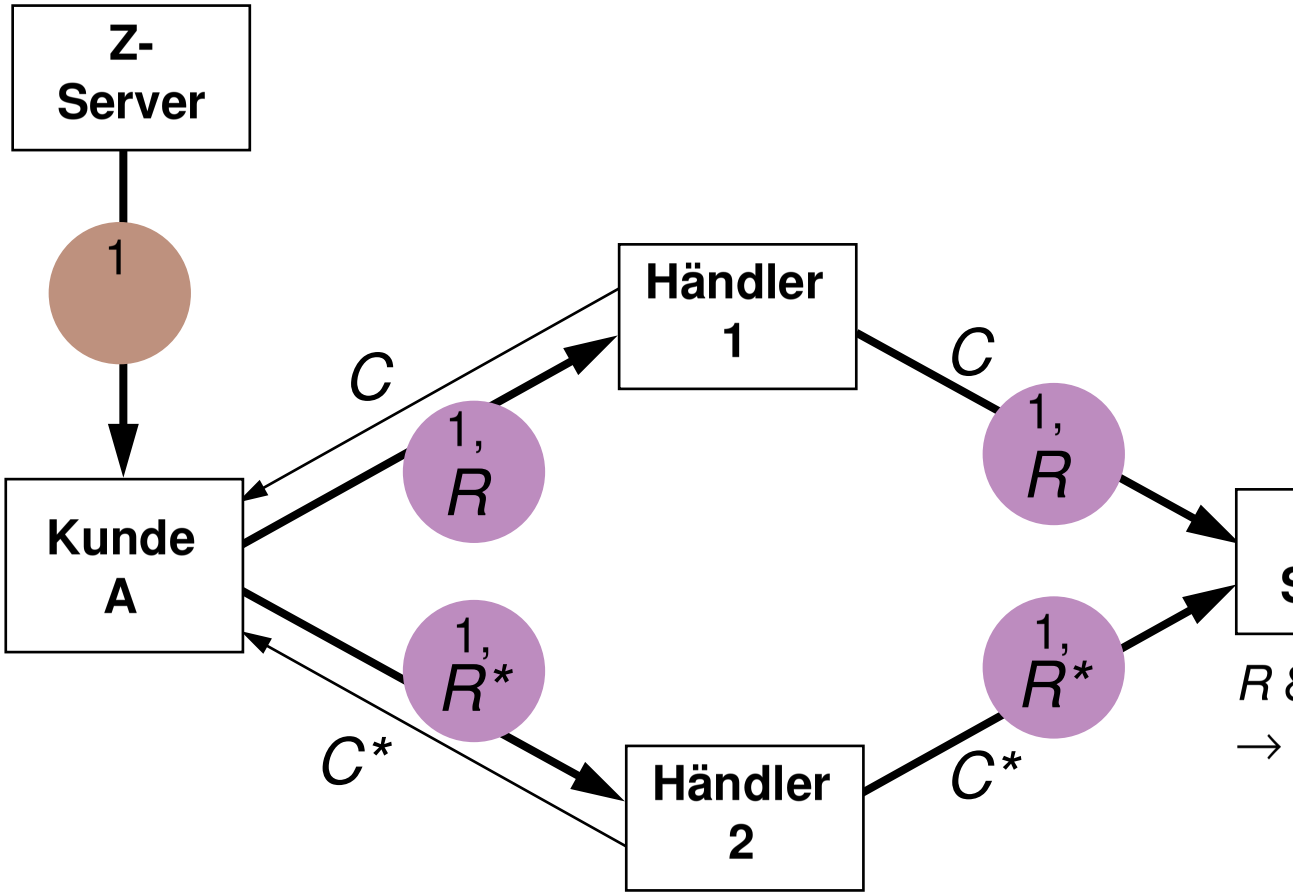


- Kunde p
- Betrag i
  diert
- Online-F
  noch nic

4.5 Anonyme offline Zahlungssyst

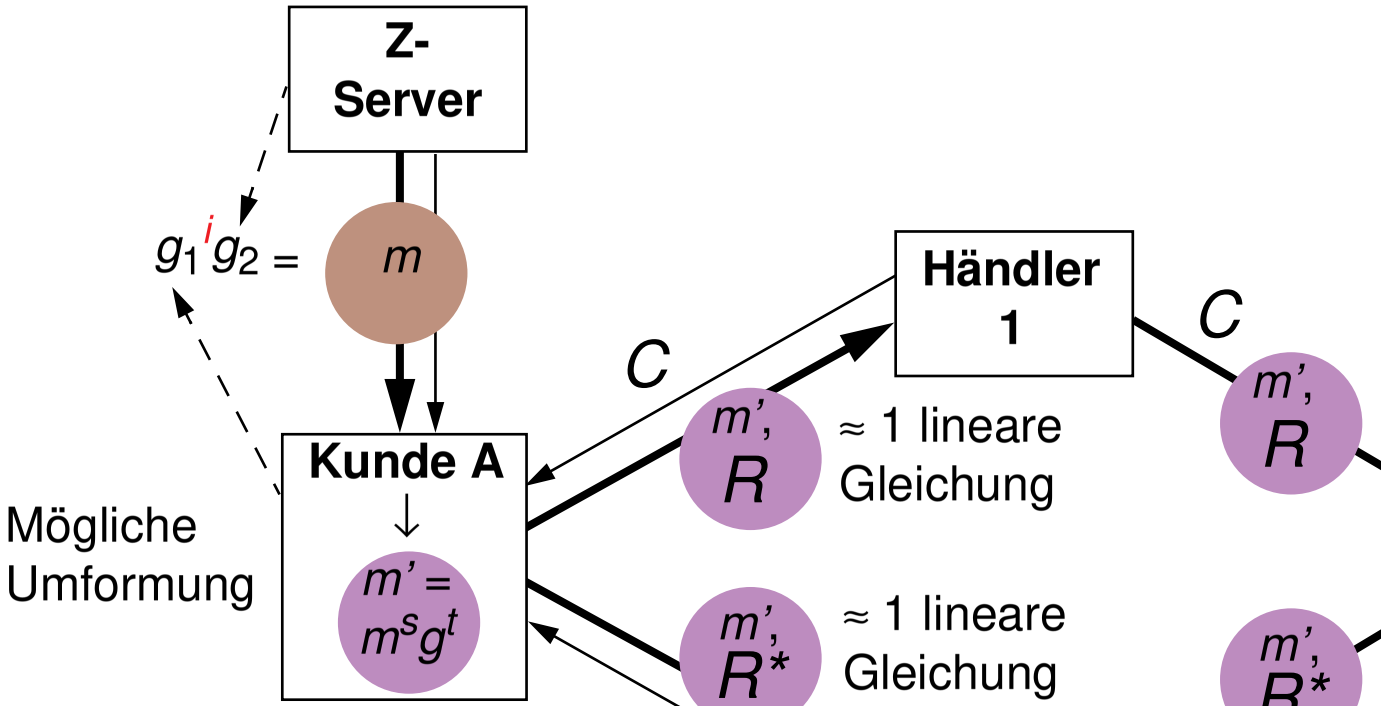
- Fast immer mit manipulationssicherer Hardwar
  fallmaßnahmen
- Kryptographie immer nötig: Mindestens gegens
  kation der Geräte
- Sicherstes Beispiel wieder: Blind signierte „Mü
  - Grundlage für CAFE
  - Trick: Identifikation bei Mehrfachausgeben (nach Brechen
    - Ehrliche bleiben anonym
    - Betrüger werden identifiziert

Identifikation bei Mehrfachausgeben



- *C* enthält Händleridentität
- Keine falschen Verurteilungen ehrlicher Benutzer

Ein paar Einzelheiten



Nötig zum Ausgeben:

$m' = g_1{}^{x_1} g_2{}^{x_2}$

$\Rightarrow t = 0,\ m' = g_1{}^{is} g_2{}^s$

Invariant: $x_1/x_2 = i$

5 Elektronische Marktplätze

5.1 Allgemeines

Mehr als nur Zahlungssystem, z.B.

- Kennenlernen
- sicherer Austausch
- Offenheit für mehrere Zahlungssysteme
- andere Geschäftsabläufe

5.2 SEMPER

Secure Electronic Marketplace for Europe

- ACTS-Projekt, 9/95-8/98
- einziges europäisches Projekt dieser Art
- umfassendster Marktplatz-Ansatz

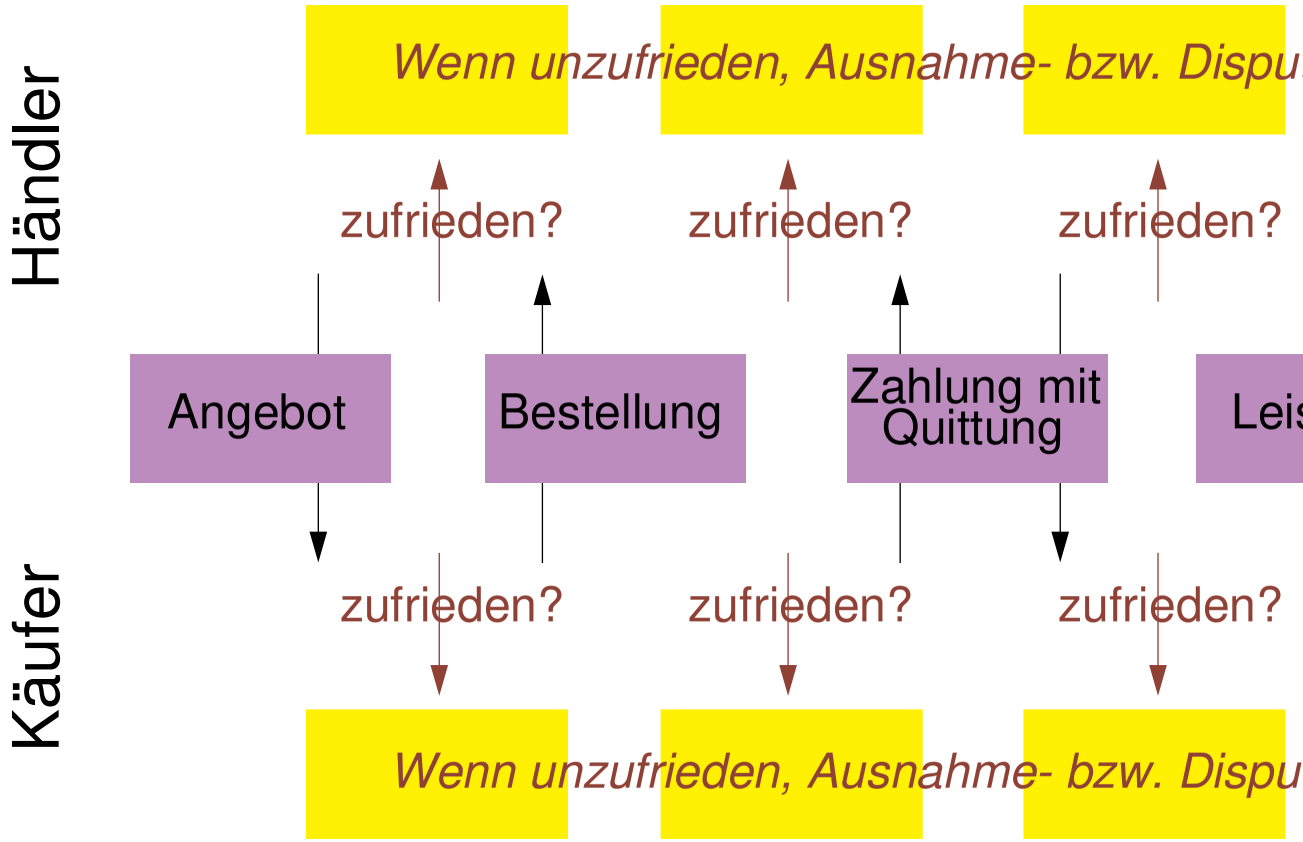
- SEMPER-Konsortium
  - Koordination IBM France
  - Finanzsektor: Europay International, Telekurs (CH), Banks
  - Händler: Otto-Versand, Eurocom (GR), Fogra (D)
  - Kommunikation, Multimedia: Postforschung (F, NL), Intrac CWI (NL)
  - Sicherheit: Cryptomathic (DK), DigiCash (NL), GMD (D), IB IBM Forschung Zürich, r3 security engineering (CH), Univ.
  - Sozialwissenschaft, Marktforschung, rechtliche Fragen: Un engineering (CH), Europay.

- Ablauf
  - 3 Ausbauphasen à 1 Jahr, jede endet mit „Trial“.
  - + „Special Interest Group on Secure Electronic Commerce“ gebnisse von Trial 1 möglichst schon in Jahr 2.
  - Jahr 1:
    - Basisdienste: Angebot, Bestellung, Zahlung, Lieferung
    - Mit existierender Technologie, z.B. iKP, e-cash
  - Jahr 2:
    - Notardienste:
      Einschreibbriefe, anonyme Kommunikation, Archivi
      Beglaubigungen
      Fairer Austausch
      Vertragsunterzeichnung
    - Copyright-Schutz
  - Jahr 3:
    - Mehrparteiendienste, z.B. Auktionen
    - Auch breitbandig

- Bausteine: Transfer und Austausch

Austausch was wogegen?	Geld	Unterschrift	Inf
—	Zahlung	Willenserklä-rung	„Beh
Geld	Fairer Geld-tausch	Zahlung mit Quittung	Kauf
Unterschrift		Vertragsunter-zeichnung, Einschreibe-brief	Bedi gang
Information	= rechts oben		Faire tions

- SEMPER-Beispielablauf



- TINGUIN: Trusted Interactive Graphical User I
  - Eigenes Fenster für gesicherte SEMPER-Meldungen
  - Konsistenter Entwurf zur Sicherung gegen Bedienfehler

6 Ausblick

- Parallele Systeme zu erwarten
  - Bargeldartig für kleine Beträge
  - Kreditkartenartig für große Beträge
  - Evtl. „Micropayments“ noch extra
- Wandlungen zu erwarten, insbes. bei Geräten

  $\Rightarrow$ Zusammenwachsen Netzszenario $\leftrightarrow$ Lädenszenario
- Für Netze: Marktplatz nötig, nicht nur Zahlungs
- Exportkontrolle aus USA $\Rightarrow$ europäische Lösu

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