wmi / 950317, © IBM Zurich

Sichere Verrechnung und Bezahlung auf dem Internet

Michael Waidner
IBM Forschungslaboratorium Zürich

Säumerstrasse 4, CH 8803 Rüschlikon, Schweiz
Tel. +41 1 724 8220, Fax: +41 1 710 3608
email: wmi@zurich.ibm.com

1 **Kontext: Internet als Marketplace**

2 **Übliche Einteilungen**

3 **Anforderungen**

4 **Überblick: Konkrete Vorschläge, Versuche und Produkte**

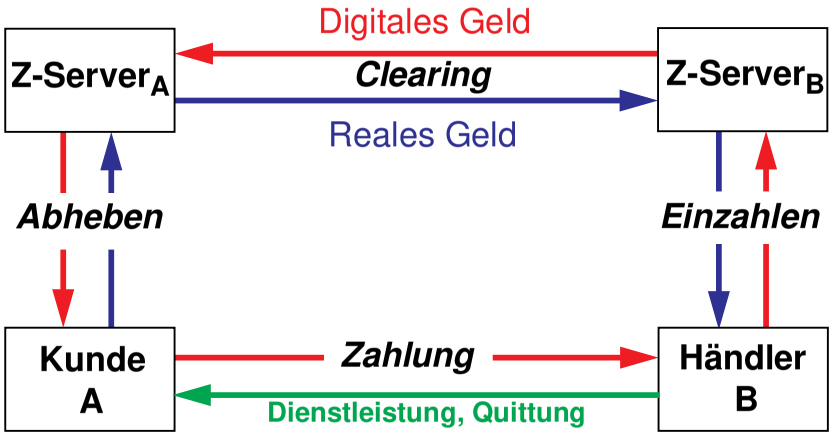
5-8 **{Anonyme/nicht anonyme} {online/offline} Zahlungssysteme**

9 **Fazit**

Literatur: <http://www.zurich.ibm.com/Technology/Security/publications/1995/rap.html>

wmi / 950317, © IBM Zurich

Was sind digitale Zahlungssysteme?

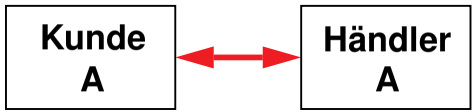


Digitales Geld ist eine spezielle Sorte von *Rechten:*

- nur Zahlungs-Server können es *erzeugen*
- *messbar* — z. B. in *ECU*
- *transferierbar* von Kunde an Händler

wmi / 950317, © IBM Zurich

2.2 Offline und online Zahlungen

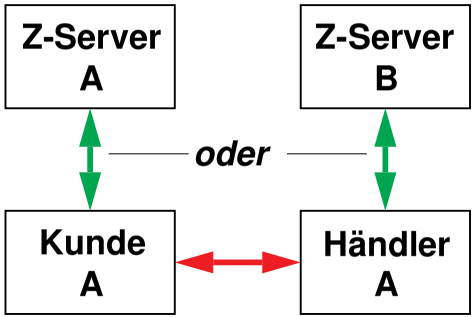


Offline Zahlungen

+ Weniger Kommunikation
– Wie verhindert/erkennt man, daß digitales Geld mehrfach ausgegeben wird?

  ... *Sicherheitsmodule*, z.B. Smartcards, PCMCIA, Smart-Disks

  ... *Explizite Tests*



Online Zahlungen

– Hohe Belastung für Z-Server, mehr Kommunikation
+ Online Autorisierung verhindert Mehrfachverwendung

wmi / 950317, © IBM Zurich

3 Anforderungen

3.1 Diensteigenschaften

- Was man hat, das kann man ausgeben ...
  - Schranken

  - Darstellbarkeit („Wechselgeldproblem“)
  - Begrenzte Gültigkeitsdauer
  - Universalität: Telefonwertkarten → Geld
- Offline Transferierbarkeit: *politisch unerwünscht ...*
- Rechtswirksame Quittungen
- Kontoauszüge, Zahlungstransparenz

3.2 Erweiterungen

- Stornierung
- offline: Verlusttoleranz
  > 1 Währungen, offline Geldwechsel

wmi / 950317, © IBM Zurich

- **Vertrauensmodell** gibt an
  - Wem *muß* vertraut werden?
    - Wer könnte betrügen, *ohne* daß das Opfer dies verhindern oder nachweisen könnte?
    - Welche Systemteile müssen "tamper-resistant" sein?

      Jeder Kunde muß seinem Gerät vertrauen

      ⇒ Für *höhere* Werte muß jeder Kunde *auch für online* Zahlungen eigenes tragbares tamper-resistant Gerät besitzen
    - Wichtigster Grundsatz: **Mehrseitige Sicherheit**

      Parteien mit *widerstrebenden* Sicherheitsinteressen sollen sich nicht blind vertrauen müssen.

      Z.B.: „Abheben" sollte gerichtlich *überprüfbar* sein, d.h. Kunde sollte Z-Server nicht blind vertrauen müssen.

      Entspricht alltäglicher Rechtssicherheit: Es müssen stets ausreichende, glaubwürdige Beweismittel vorhanden sein!
  - Welche Fähigkeiten haben die „anderen" im schlimmsten Fall?

    ... insb. welche kryptographischen Systeme gelten als sicher?

wmi / 950317, © IBM Zurich

4 Überblick: Konkrete Vorschläge, Versuche und Produkte

	online Zahlungen	offline Zahlungen

Nicht anonym (bis auf feste Pseudonyme)	Kreditkarte via Internet:
	• ungesichert
	• Rückfrage: First Virtual
	• Gesicherter Austausch
	  • CyberCash
	  • OpenMarket (marketplace)
	  • NetMarket (marketplace)
	  • IBM iKP
	  • CommerceNet
	
	Zahlungsserver
	  • NetBill (accounting and billing)
	  • NetCash, Teil 1
	  • SNPP
		Sichere Zähler in Smartcard
		• Danmont, Proton ...
		• Mondex, Express ...
		• CEN IEP (Standardisierung ...)
		
		Bislang nicht für online Dienste genutzt.
		Laden erfolgt teilweise optional via Telefonnetz.

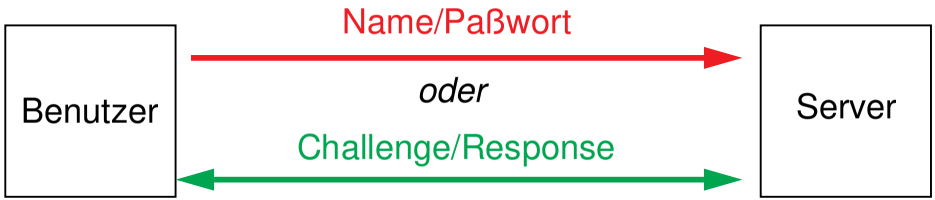
Anonym	Vertrauenswürdige „Wechsler“
	  • NetCash, Teil 2
	  • Anonymous Credit Card (ACC)
	
	Blind geleistete Signaturen
	  • DigiCash e-cash
		Blind geleistete Signaturen
		• CAFE
		
		Bislang nicht für online Dienste genutzt.
		Laden erfolgt optional via Telefonnetz.

5 Nicht anonyme online Zahlungssysteme

wmi / 950317, © IBM Zurich

5.1 *Einschub:* Hilfsmittel zur Authentisierung

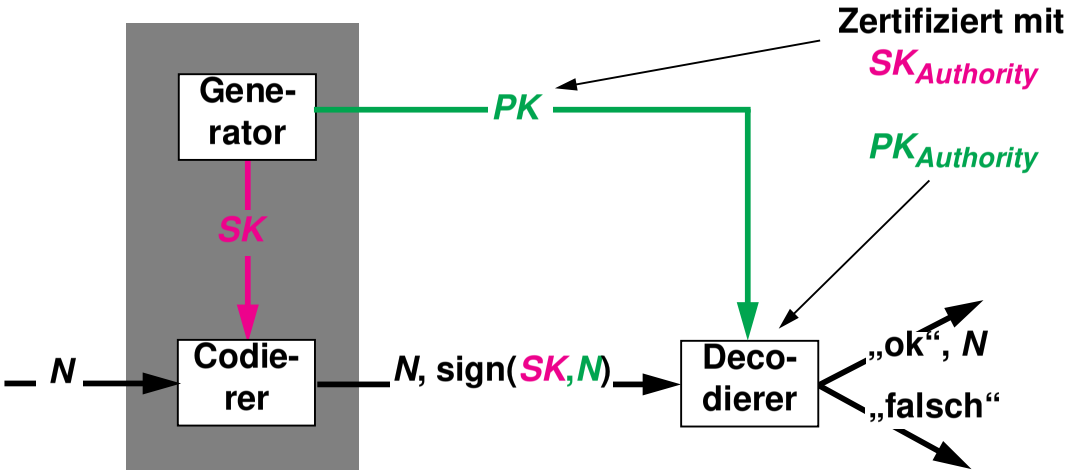
- **Benutzerauthentisierung**



- Challenge/Response deutlich sicherer, erfordert aber Berechnungen
- Oft übersehen: ***gegenseitige*** Authentisierung erforderlich
  - Server muß Benutzer authentisieren
  - Benutzer muß Server authentisieren
- Sichert noch nicht die Kommunikation zwischen Benutzer und Server.

wmi / 950317, © IBM Zurich

- **Digitale Signaturen**



- Häufig *RSA, DSS, Schnorr, ElGamal,* mit passender Hashfunktion
- *PK* muß ***zertifiziert*** sein,
  d.h. eine dritte Partei bestätigt Authentizität von *PK* relativ zum Benutzer
- Vorteile:
  - Meist sicherer als symmetrische Verfahren
  - Erlaubt Nachweis der Echtheit gegenüber Dritten
    (was die Voraussetzung an ein „Beweismittel“ ist!)
- Nachteil:
  - relativ rechenintensiv (in Software: im Sekundenbereich)

wmi / 950317, © IBM Zurich

- „Login“ auf Z-Server: **Open Market**

  - Prinzip:
    - Benutzer identifiziert sich gegenüber Z-Server
      - Paßwort *oder*
      - Challenge/Response mittels *SecureID* u.ä.
    - Zahlungsinformation wird in URL’s eingebettet
    - arbeitet mit existierendem HTTP, existierenden Browsern

  - Probleme
    - übliche Probleme mit Paßwörtern im Internet
    - Alle müssen Z-Server vertrauen:

      ⇒ keine mehrseitige Sicherheit

wmi / 950317, © IBM Zurich

- Digitale Signaturen mit Zertifikaten:
  - Prinzip:
    - Zu einem Signatursystem (z.B. RSA, DSS, Schnorr)
      - erzeugt Z-Server Schlüsselpaar
        (SK_Z, PK_Z) mit Zertifikat von „**Zentralbank**“
        erzeugt Kunde A Schlüsselpaar
        (SK_A, PK_A) mit Zertifikat von Z-Server
      - Alle Nachrichten werden digital signiert.

    $\Rightarrow$ Probleme mit Autorisierungsserver beseitigt.
    $\Rightarrow$ Alle Varianten möglich (1 und 3 sinnvoll)
  - Probleme
    - Zeitaufwand zum Signieren/Testen von Signaturen
  - Protokolle
    - Sicherer Austausch von Kreditkartendaten, z.B.
      iKP, CommerceNet (S-HTTP, PEM), NetMarket (PGP)
    - NetCash (als Alternative zu *Kerberos*)
  - Kryptosystem
    Jedes Signatursystem genügt.
    In den Beispielen jeweils *RSA*.

wmi / 950317, © IBM Zurich

6 Anonyme online Zahlungssysteme

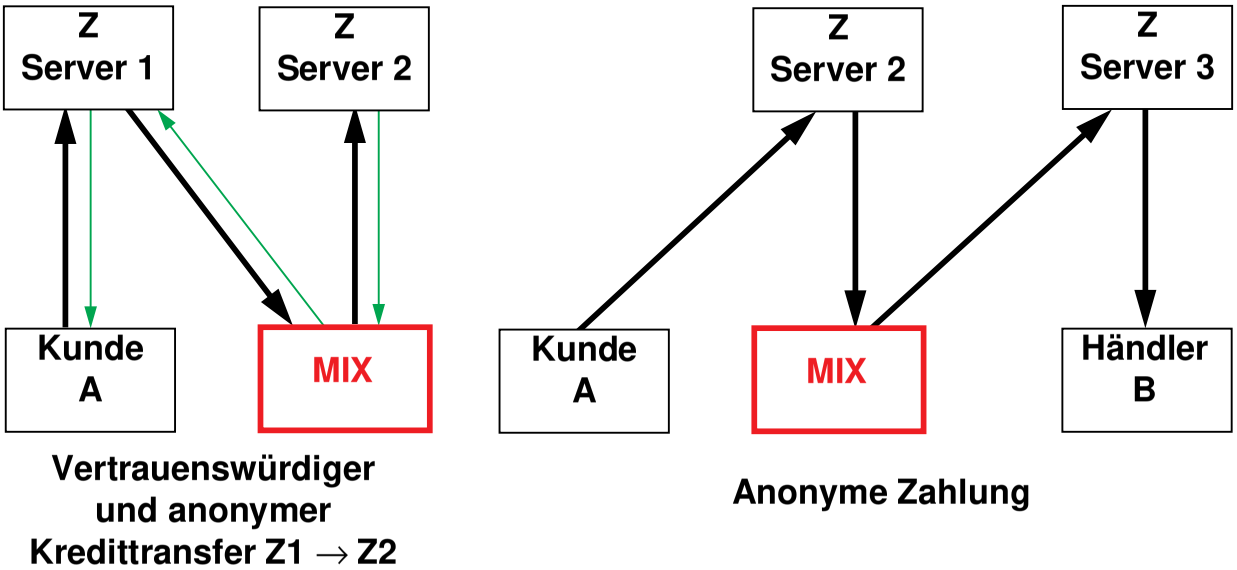
6.1 Verschlüsselung der Zahlungsdaten

6.2 Anonyme Konten

- Prinzip
  - Konto wird statt unter **Namen** unter **Pseudonym** geführt.
  - Ist praktisch bei jedem Zahlungssystem möglich.
- Probleme
  - Zahlungen sind verkettbar
    feste Pseudonyme erlauben „anonyme Persönlichkeitsprofile“, letztlich Identifikation des Benutzers
  - Keine Anonymität gegenüber dem Z-Server

wmi / 950317, © IBM Zurich

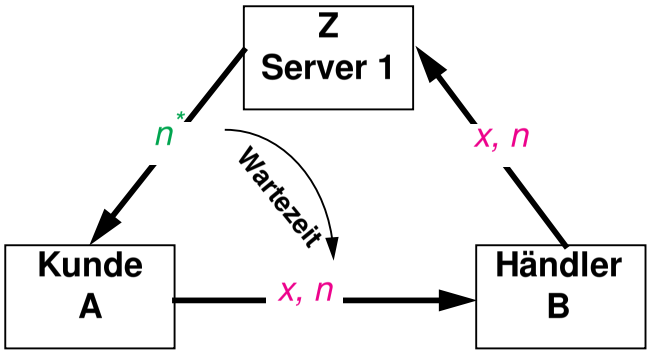
- **Anonymous Credit Card (ACC)**



- Legt Verwendung digitaler Signaturen nahe
- Annahme: MIX hält Zusammenhänge zwischen Konten geheim
  ⇒ "schwache" Anonymität, MIX + Z-Server können beobachten
- Hoher Kommunikationsaufwand je Transfer

wmi / 950317, © IBM Zurich

- **Grundzahlungssystem**



- Kunde perfekt anonym
- Z-Server muß eingehende „Münzen“ (*x, n*) auf „noch nicht eingereicht“ prüfen.

- Ansatz Grundlage für **DigiCash ecash**

- Zahlreiche **Erweiterungen**
  z. B.
  - Sicherheit gegen Z-Server beim Einreichen
  - Erzwingen von Quittung von B

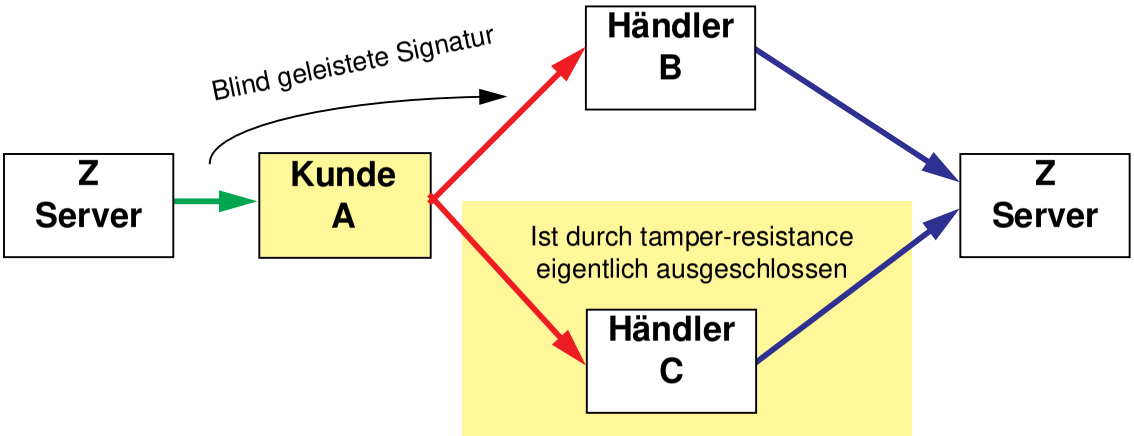
  und hier nicht dargestellte **Details**
  z. B.
  - Codierung des Zahlungsbetrages

- Alternative Signatursysteme, insbesondere *Schnorr Signaturen*

wmi / 950317, © IBM Zurich

8 Anonyme offline Zahlungssysteme

- **Prinzip: Sicherheitsmodule+ Erkennen von Betrug als Rückfallposition**



- Kunde ist **perfekt anonym** (spezielle Form blind geleisteter Signaturen)
- Gelingt es durch Manipulation des Kundengerätes Geld mehrfach auszugeben, so wird Kunde deanonymisiert
  ⇒ Z-Server muß alle eingehenden „Münzen“ auf Dubletten vergleichen
- Nutzung: wie oben
- **CAFE** (auf *Schnorr-Signaturen*), mit Kombination aus „Münzen“ und „Schecks“ (mit Erweiterungen, z.B. Verlusttoleranz)