Sicherheitsaspekte beim Electronic Commerce

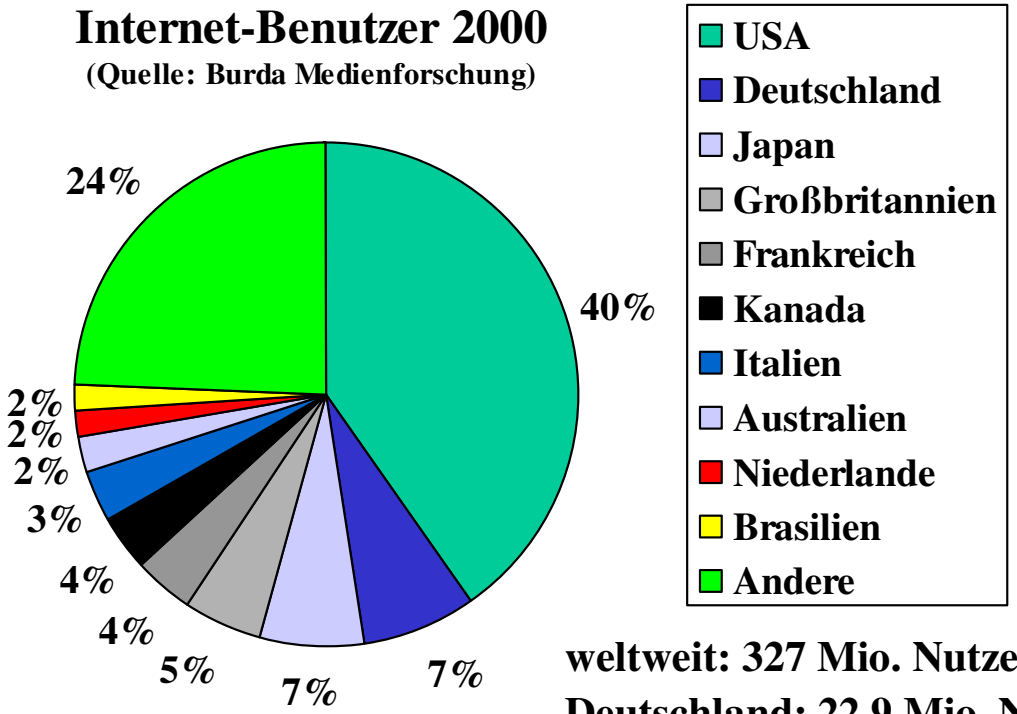
Melanie Ruhe

Seminar Anwendungsentwicklung
im WS 99/00

Gliederung

- Motivation
- Transaktionssteuerung
- Verschlüsselungsalgorithmen und Zertifikate
- Zahlungsverfahren
  - Kreditkartenbasierte Verfahren
  - Kartenbasierte Verfahren
  - Digitales Geld
  - Billing-Verfahren
- Beispiel
- Ausblick

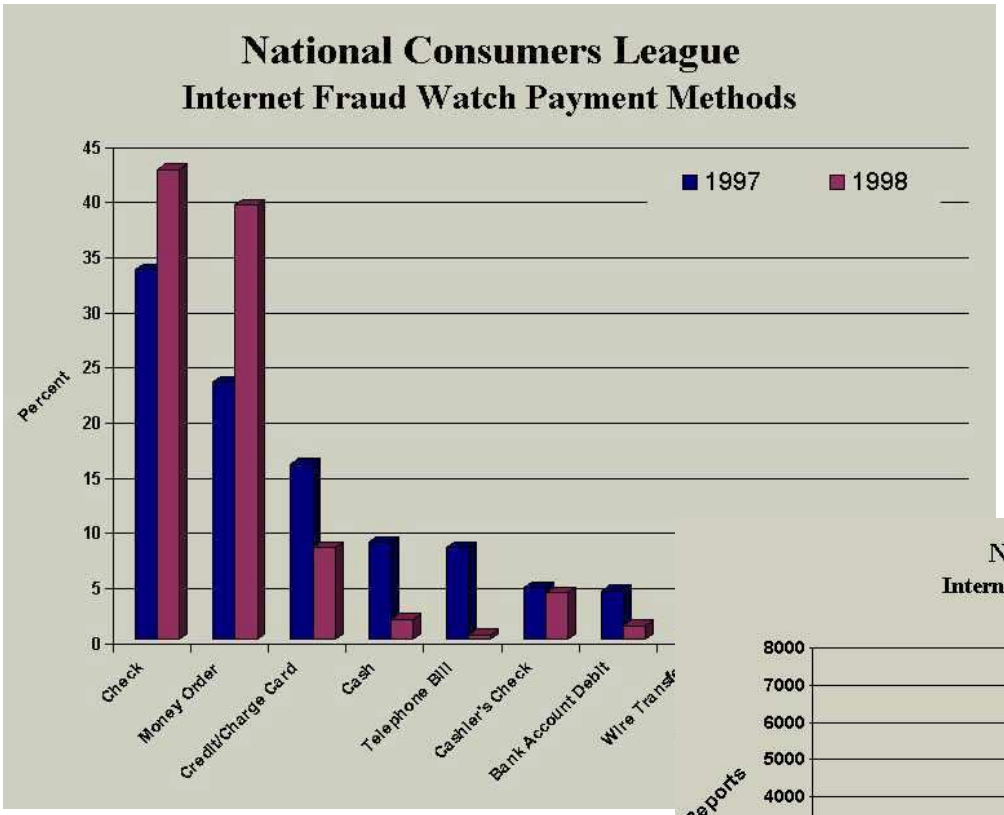
Statistik

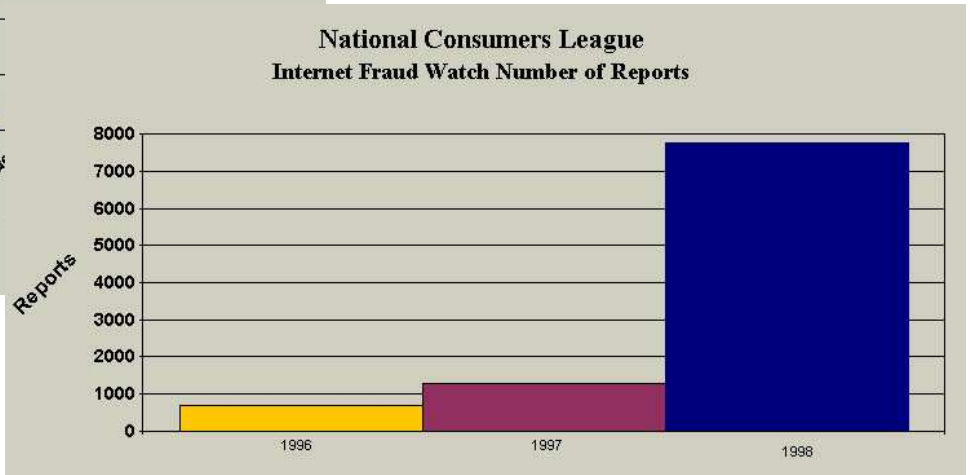


weltweit: 327 Mio. Nutzer
Deutschland: 22,9 Mio. Nutzer

Internet-Nutzung: emailen, Informationssuche, …, Online-Shopping

Statistik (II)





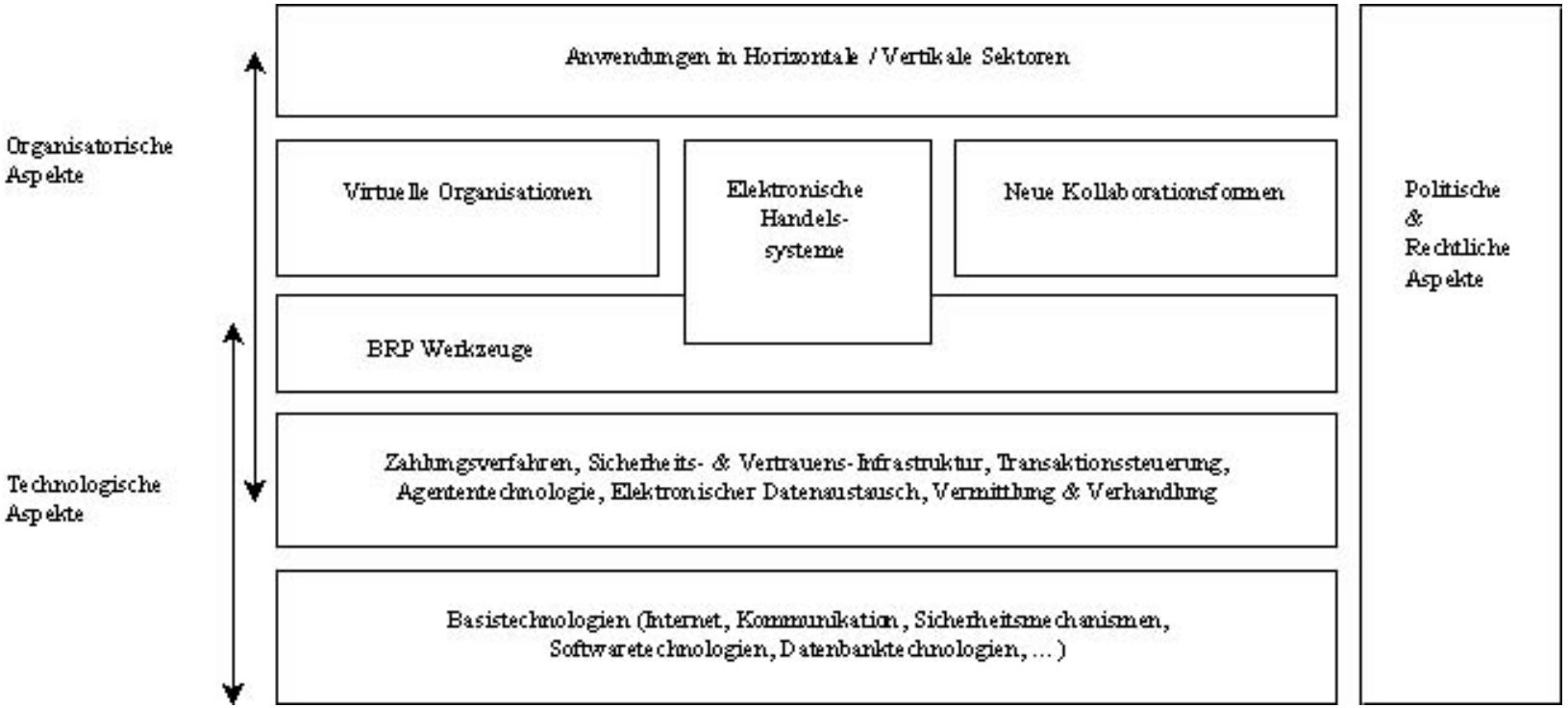
Statistik (III)

Prognosen

- 200 Milliarden Euro Weltmarktvolumen (Europäische Kommission)
- 77% davon im B2B-Bereich
- Business Week 1995: (eCommerce beinhaltet sämtliche Geldtransaktionen im Internet)

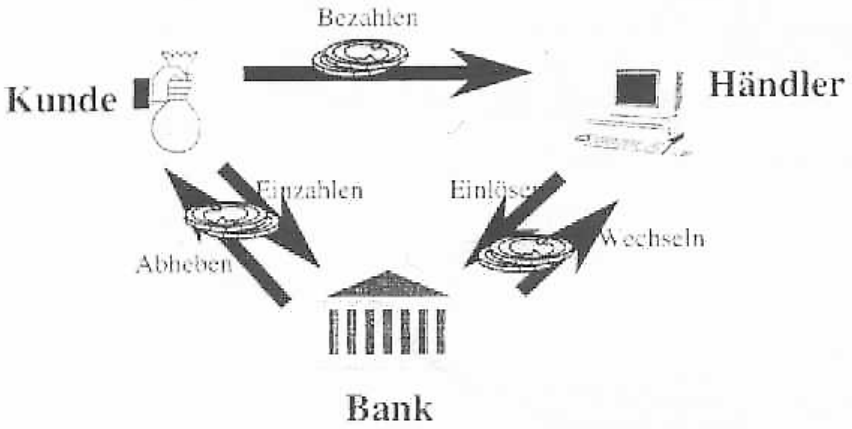
Jahr	Classic Commerce (Milliarde $)	Electronic Commerce (Milliarde $)
1994	5150	245
2000	8500	1650
2005	12000	2950

Referenzmodell Electronic Commerce [Merz]



“Sicherheit kann technisch realisiert werden - Vertrauen nicht!” [Merz]

Betrugsmöglichkeiten



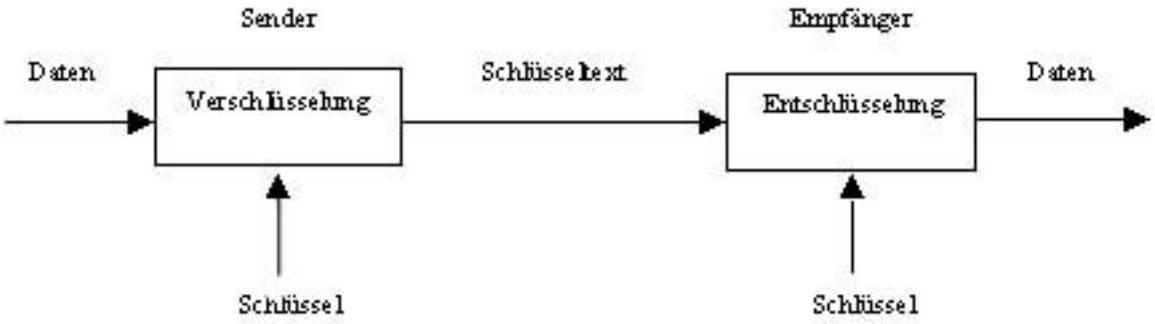
- *Double spending:* Elektronische Zahlungseinheiten werden mehrfach benutzt.
- *Stehlen von Daten:* Ein Kunde hat bspw. Kreditkarteninformationen gestohlen und gibt vor, Besitzer dieser Karte zu sein.
- *Händlerseitiger bzw. Käuferseitiger Betrug:* Händler bzw. Kunde streiten den (richtigen) Empfang von Geld bzw. Waren ab

Transaktionssteuerung

- Atomarität:
  - Geld-Atomarität
  - Güter-Atomarität
  - Zertifizierte Lieferung
- Authentifizierung (digitale Unterschrift, Passwort, Zertifikate)
- Integrität (Hashwerte)
- Autorisierung (Zertifikate, Rückfragen)
- Anonymität (gegenüber der Bank bzw. dem Händler)
- Verfügbarkeit (24 Stunden, 7 Tage)
- Mehrbenutzerbetrieb
- Transaktionsgröße (Mikro/Makrotransaktionen)

Verschlüsselungsalgorithmen

- Prinzip:



- Private-Key-Verfahren (symmetrische Schlüssel)
- Public-Key-Verfahren (asymmetrische Schlüssel)
- Dokumenten- versus Kanalverschlüsselung

- DES (Data Encryption Standard), RSA, Diffie-Hellmann

Authentifizierung mit Zertifikaten

- Ist die Herkunft des öffentlichen Schlüssels vertrauens-würdig?
- Sicherheitsmechanismus - Vertrauensinfrastruktur
- 3 Rollen: Herausgeber, Besitzer (käuflicher Erwerb), Prüfer
- Zertifizierungsautorität:
  - Registrierung
  - Online-Verifikation der Zertifikate
  - Verwaltung von schwarzen Listen
- Technische Realisierung mit Standard X.509
- Wie erfolgt die Verifikation der Zertifikate?
- Beispiel TC Trustcenter: 4 Zertifikatsklassen

Kreditkartenbasierte Verfahren

- Prinzip: Übertragung von Kreditkarteninformationen an den Händler bzw. die Bank zur Bezahlung
- Vorteile: international nutzbar, einfache Umsetzung
- Problem: sichere Übertragung der Karteninformationen

- Protokoll SSL (Secure Socket Layer) - Aufbau einer sicheren Verbindung (https://)
- First Virtual - email-basiert, CyberCash - Wallet-basiert

Secure Electronic Transaction (SET)

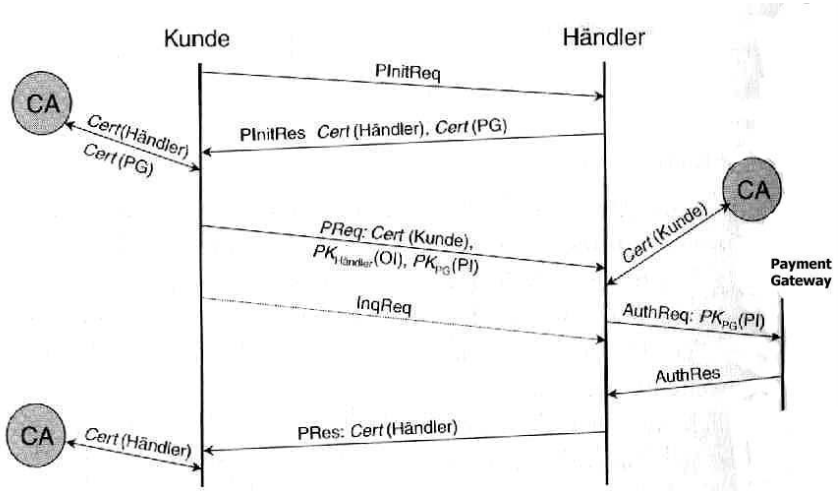
- Vorraussetzungen:
  - SET-Wallet auf Kunden-Seite
  - SET-Server auf Händlerseite
  - SET Payment Server seitens der Bank des Händlers

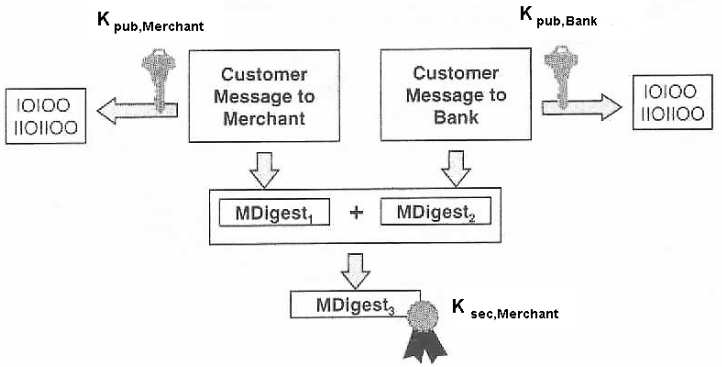
– teuer, nur geld-atomar

– komplexe Autorisierung

+ Anonymität ggü. Händler

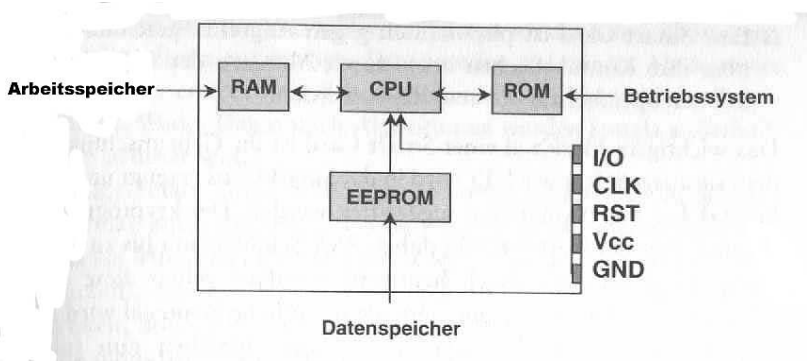
+ Vermeidung von Betrug





Kartenbasierte Verfahren

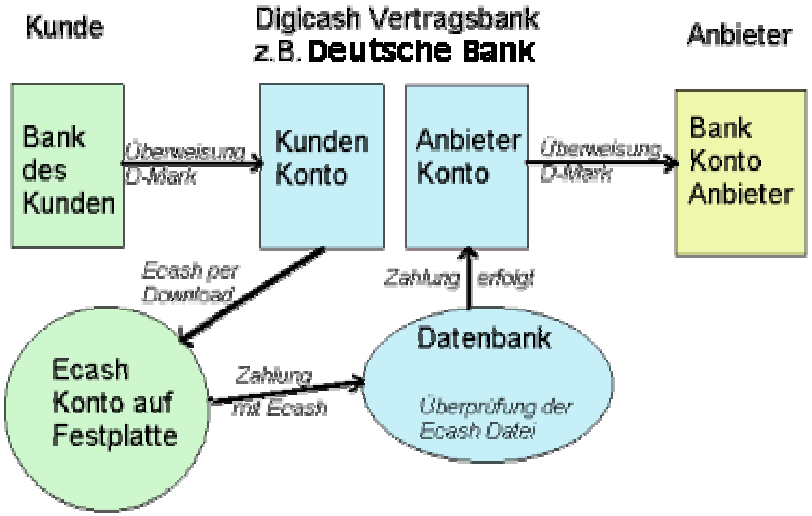
- Prinzip: Bezahlung wird über Karten abgewickelt
- Vorteil: Eignung für Mikrotransaktionen
- Probleme: technische Realisierung, Sicherheit
- SmartCard: Geldkarte



- Mondex: Karte + Lesegerät

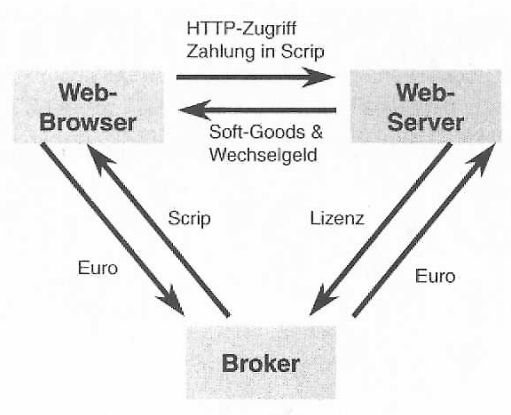
Digitales Geld

- Prinzip: Zahlungsmittel, die Bargeldcharakter haben
- Vorteil: vollkommene Anonymität
- Probleme: keine Atomarität, gesetzliche Schranken
- eCash



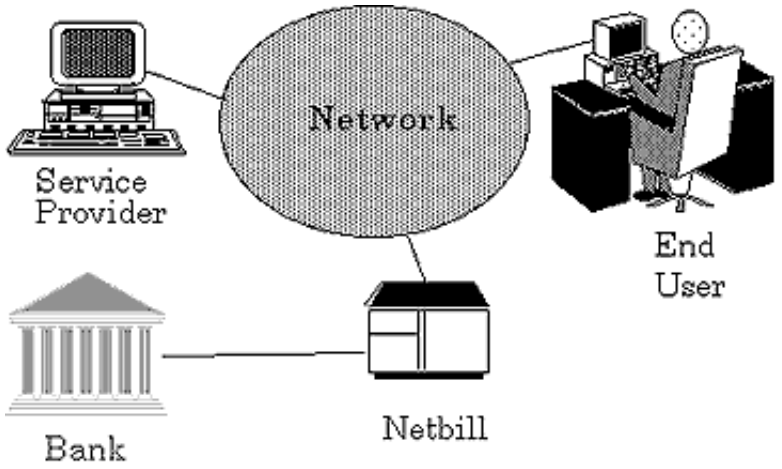
Billing-Verfahren

- Prinzip: Bezahlung wird in 2 Ebenen unterteilt
  - Buchung wird auf einem Konto beim Händler verbucht
  - Bezahlung erfolgt durch Abbuchung oder Rechnungsstellung durch den Händler an alle Konteninhaber (Kontenausgleich)
  - Vergleich mit Telefonrechnung (eCharge)
- Vorteil: geeignet für Mikrotransaktionen
- Problem: keine Anonymität
- MilliCent



NetBill

- Mikrotransaktionssystem für Informationsgüter (Geld und Güter werden im Internet transferiert)
- Vorraussetzungen:
  - Konto beim NetBill-Server auf Kunden- & Händlerseite
  - NetBill-Server über den alle Transaktionen abgewickelt werden
- Protokoll:



Zusammenfassung

System	Atomarität	Anony-mität	Authenti-fizierung	Transak-tionsgröße	Voraussetzungen auf der Kundenseite
FirstVirtual	Geld-atomar	Nein	Konto-Nr.	medium-macro	Kunde benötigt Konto in den USA; Email
CyberCash	Geld-atomar	Nein	Cyber Cash Wallet	medium-macro	CyberCash-Wallet
SET	Geld-atomar	Nein	Zertifikate	medium-macro	Zertifikat; SET-Wallet
Geldkarte	Geld-atomar	Nein	Karte, PIN	micro-medium	Karte
Mondex	k. A.	Nein	Karte	micro-medium	Karte & Lesegerät
eCash	keine	Ja	Seriennr. der Münzen	micro-medium	eCash-Software zur Verwaltung der Münzen
MilliCent	Geld-atomar	Nein	Seriennr. der Münzen	micro-medium	Wallet-Software
eCharge	Geld-atomar	Nein	Telefon-Nr.	micro-medium	Telefonanschluß
NetBill	Zertifizierte Lieferung	Nein	Konto-Nr.	micro-medium	NetBill-Konto

Beispiel FCK-Shop

- Verwendung von Cookies
- Zahlungsverfahren: per Nachnahme, Verrechnungsscheck oder Kreditkarte
- Bestellung über gesicherte Verbindung (https://) möglich
- Zertifikat hat folgende Inhalte (Signaturgesetz):
  - Aussteller, Antragsteller: FCK
  - Verschlüsselung US-Export-geeignet (40 Bit)
  - Verfahren: md5RSA (Signatur)
  - Gültigkeitsdauer: 1 Jahr (bis 22.10.99)
  - Fingerabdruck des Zertifikates
- Browser warnt: Zertifikat abgelaufen und nicht vertrauenswürdig!

Sicherheitsaspekte beim Electronic Commerce

- Probleme und Anforderungen
- Verschlüsselungsalgorithmen und Zertifikate
- Zahlungsverfahren
- Unterschiede zwischen Theorie und Praxis

- Rechtliche Aspekte und Konsequenzen
- Vision: eWallet, das Kundeninformationen speichert
- ECML: Standard zur Benennung von HTML-Formularfeldern ⇒ Wallet kann Formular ausfüllen

Diffie-Hellman (Public-Key-Verfahren)

- A und B einigen sich auf zwei Zahlen n und g
  mit: n ist Primzahl und g mod n prim zu n
- Partner A wählt eine beliebig große Zahl x
  und sendet an Partner B die Zahl $X=g^x \bmod n$
- Partner B wählt eine beliebig große Zahl y
  und sendet an Partner A die Zahl $Y=g^y \bmod n$
- A berechnet seinen Schlüssel $k=Y^x \bmod n$
- B berechnet seinen Schlüssel $k'= X^y \bmod n$
- Es gilt nun für beide Schlüssel
  $k=k'= g^{xy} \bmod n$