Wie werde ich mein Geld los?

Wie kommt der Händler an sein Geld?

In der realen Welt

bar bezahlt werden
70% der Käufe

6% mit Schecks
19% kartengestützte Systeme

Umfrage zu Zahlungsmitteln

- Institut für Wirtschaftspolitik und Wirtschaftsforschung - Universität Karlsruhe (TH) - Sektion Geld und Währung http://www.iww.uni-karlsruhe.de:8001/IZV3/
- 3.000 Teilnehmer
- 22. November 1999 bis zum 25. Januar 2000
- nicht repräsentativ

Teilnehmer-Profil

1. Geschlecht?		
Weiblich	252	9.2 %
Männlich	2479	90.8 %

2. Alter?		
bis 18 Jahre	75	2.7 %
19-25	778	28.1 %
26-35	1401	50.6 %
36-45	390	14.1 %
46-55	99	3.6 %
56 Jahre und älter	27	1.0 %

Teilnehmer-Profil

3. Höchster erreichter Bildungsabschluß?		
Volksschule/Hauptschule	40	1.4 %
Mittlere Reife bzw. weiterführende Schule ohne Abitur	147	5.3 %
abgeschlossene Berufsausbildung	245	8.8 %
Fachabitur, Fachhochschulreife	218	7.9 %
Abitur, Hochschulreife	887	32.0 %
Studium (Universität, Hochschule, Fachhochschule, Akademie, etc.)	1173	42.3 %
anderer Schulabschluß	15	0.5 %
noch kein Abschluß	47	1.7 %

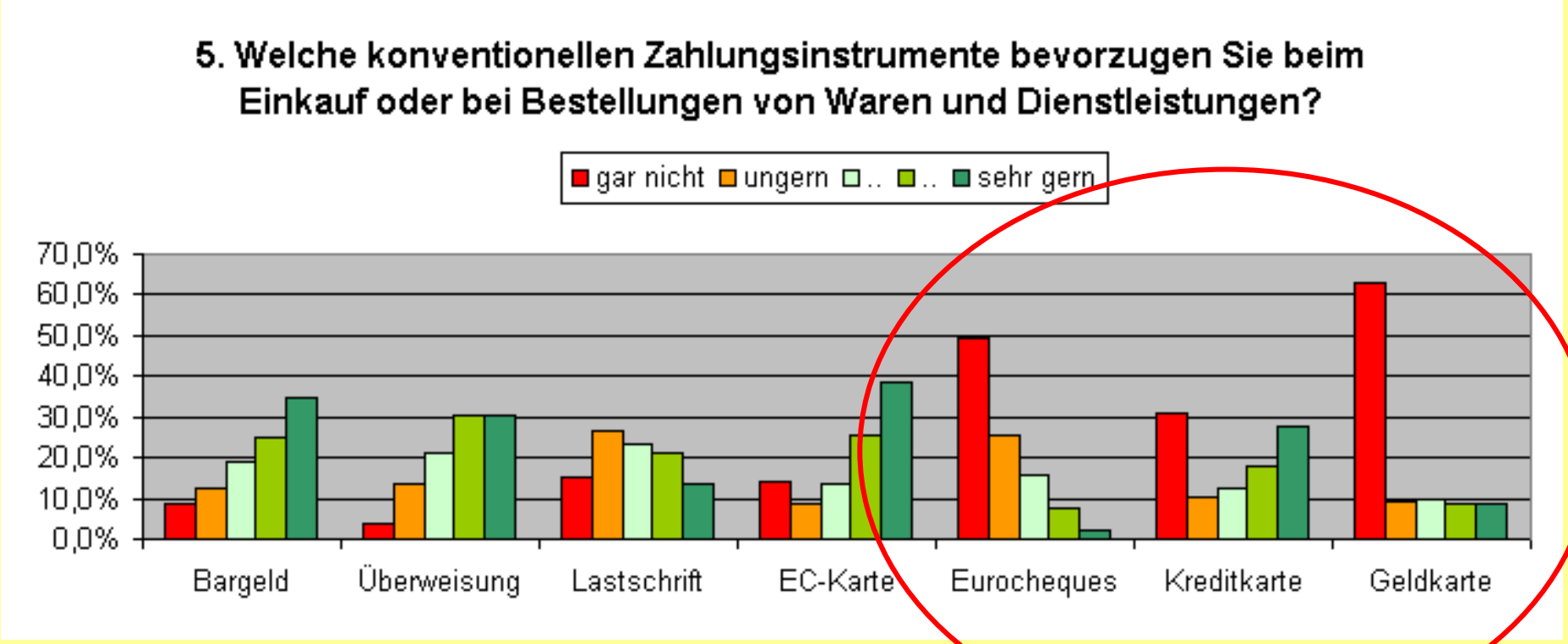
Teilnehmer-Profil

4. Derzeitige Berufstätigkeit bzw. Ausbildung?		
SchülerIn	101	3.6 %
StudentIn	741	26.8 %
Auszubildende/r	74	2.7 %
Angestellte/r	1338	48.3 %
Arbeiter/In	71	2.6 %
Beamter/In	92	3.3 %
selbständig	238	8.6 %
arbeitslos;	29	1.0 %
sonstige	84	3.0 %

Teilnehmer-Profil

13. Ist Ihnen die Bedeutung dieser Symbole bzw. dieser Begriffe klar?				
	JA		NEIN	
Sicherheitssymbole	2487	94.1 %	157	5.9 %
HTTPS	2135	81.0 %	501	19.0 %
Cookies	2541	96.4 %	94	3.6 %
Makroviren	2463	93.5 %	172	6.5 %
Elektronische Signatur	2468	93.8 %	164	6.2 %
PGP	2188	83.0 %	447	17.0 %
SSL	2138	81.0 %	501	19.0 %

Umfrage-Ergebnis



Umfrage-Ergebnis

6. Welche Eigenschaften sind Ihnen beim bargeldlosen Zahlungsverkehr am wichtigsten?

	unwichtig		..		..		sehr wichtig		INDIKATOR *(1=unwichtig;4=sehr wichtig)*
überall akzeptiert	35	1.3 %	125	4.7 %	784	29.5 %	1714	64.5 %	3.6
Nachvollziehbarkeit der Zahlungsumsätze	13	0.5 %	99	3.7 %	567	21.2 %	1996	74.6 %	3.7
einfache Handhabung (Nutzerfreundlichkeit, Zuverlässigkeit)	16	0.6 %	146	5.5 %	927	34.7 %	1583	59.2 %	3.5
Sicherheit (Risikobegrenzung, keine Übermittlung von Kontoinformationen)	9	0.3 %	86	3.2 %	361	13.5 %	2221	83.0 %	3.8
Vertraulichkeit der Transaktionen (keine Rückverfolgbarkeit)	83	3.1 %	375	14.1 %	695	26.0 %	1516	56.8 %	3.4
geringe/keine Transaktionskosten	25	0.9 %	159	6.0 %	850	31.8 %	1637	61.3 %	3.5

Umfrage-Ergebnis

15. Vier Zahlungsverfahren zur Auswahl. Bis zu welchem Geldbetrag würden Sie jeweils die einzelnen Verfahrensarten einsetzen?

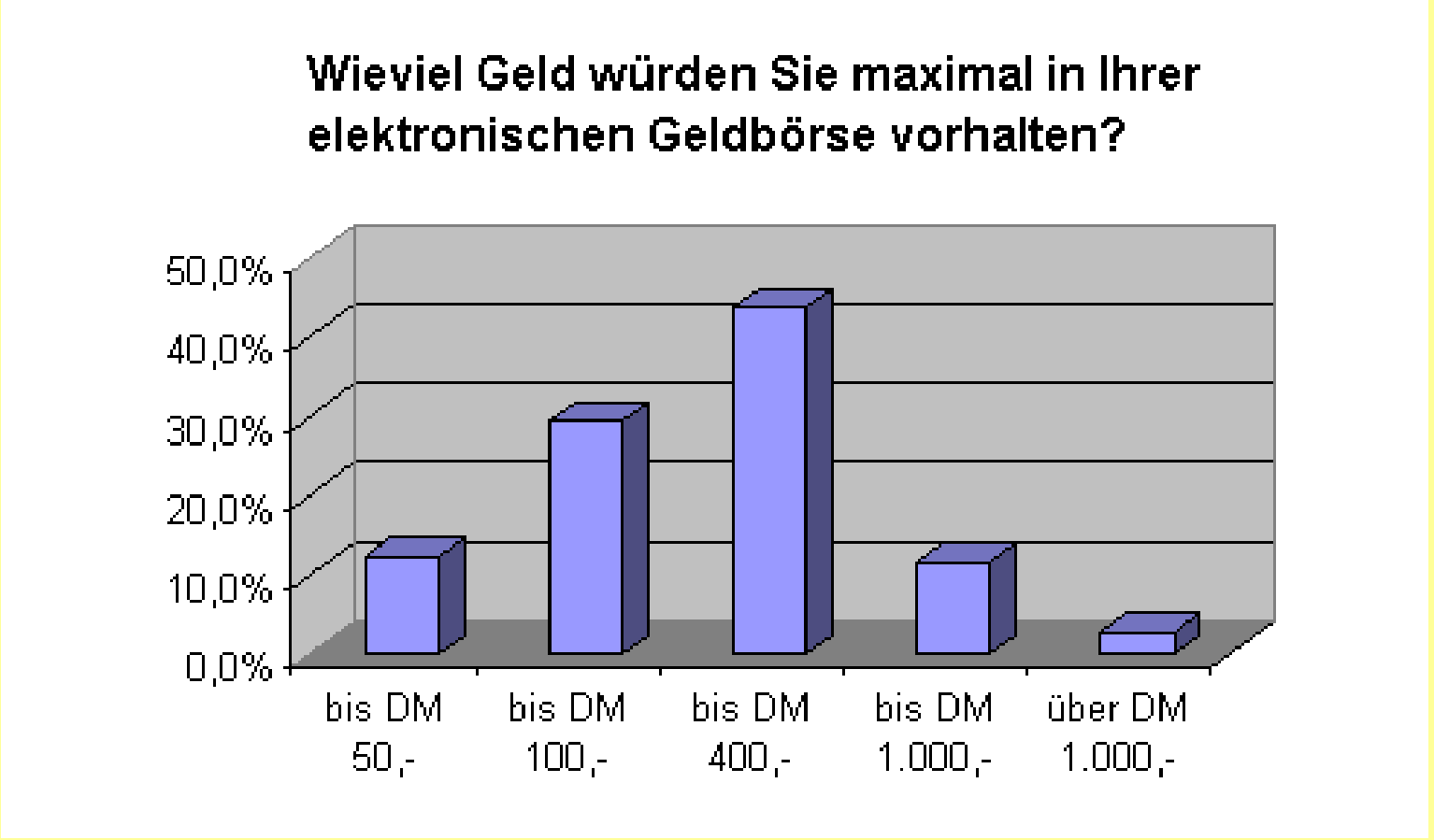
DM Zahlungssystem	gar nicht einsetzen		bis 50		bis 100		bis 400		bis 1.000		über 1.000		INDIKATOR *(1=gar nicht einsetzen;6=über 1000)*
Kreditkartenbasiert	965	37.0 %	49	1.9 %	210	8.1 %	426	16.4 %	354	13.6 %	601	23.1 %	3.4
Bankeinzug	707	27.1 %	115	4.4 %	379	14.5 %	551	21.1 %	314	12.0 %	540	20.7 %	3.5
Vorausbezahlt	1386	52.7 %	364	13.8 %	429	16.3 %	263	10.0 %	102	3.9 %	87	3.3 %	2.1
Klassisch	259	9.9 %	50	1.9 %	175	6.7 %	399	15.3 %	311	11.9 %	1412	54.2 %	4.8

Umfrage-Ergebnis

16. Welches der genannten Verfahren würden Sie bei Ihrem Online-Einkauf einsetzen?

DM Zahlungssystem	würde ich nicht einsetzen		weiß nicht		würde ich einsetzen	
GeldKarte	381	30.9 %	245	19.9 %	607	49.2 %
ecash	276	22.4 %	377	30.6 %	580	47.0 %
CyberCoin	303	24.6 %	421	34.1 %	509	41.3 %
MilliCent	583	47.3 %	376	30.5 %	274	22.2 %

Umfrage-Ergebnis



Umfrage-Ergebnis

21. Wie haben Sie Ihre Einkäufe im Internet bezahlt? (Mehrfachnennungen möglich)		
per Nachnahme (Post, Paketdienst)	1091	47.6 %
Überweisung, Vorausscheck, Rechnung	1191	52.0 %
Kreditkarte	1224	53.4 %
Internetzahlungsmittel (ecash, CyberCoin,..)	44	1.9 %
Lastschrift	772	33.7 %

Umfrage-Ergebnis

23. Wie sind Ihre Erfahrungen bezüglich...									
	gut		..		..		schlecht		INDIKATOR *(1=gut;4=schlecht)*
Benutzerführung bei Auswahl und Bestellung	717	32.0 %	1089	48.7 %	376	16.8 %	56	2.5 %	1.9
Zahlungsabwicklung	1155	51.0 %	881	38.9 %	183	8.1 %	47	2.1 %	1.6
Lieferleistung/Lieferzeit	887	38.9 %	1004	44.1 %	316	13.9 %	72	3.2 %	1.8
Reklamationen	412	22.1 %	895	48.0 %	405	21.7 %	151	8.1 %	2.2

Umfrage-Ergebnis

24. Warum haben Sie noch keine Interneteinkäufe getätigt? (Mehrfachnennungen möglich)		
Keine attraktiven Angebote	58	20.6 %
Aufwand bei der Zahlungsabwicklung	96	34.0 %
Negative Meinung und Erfahrung anderer	51	18.1 %
Fehlende Möglichkeiten (keine Kreditkarte, Alter, ...)	82	29.1 %
'Ungutes' Gefühl	179	63.5 %
Anderer Grund (Textfeld):	92	32.6 %

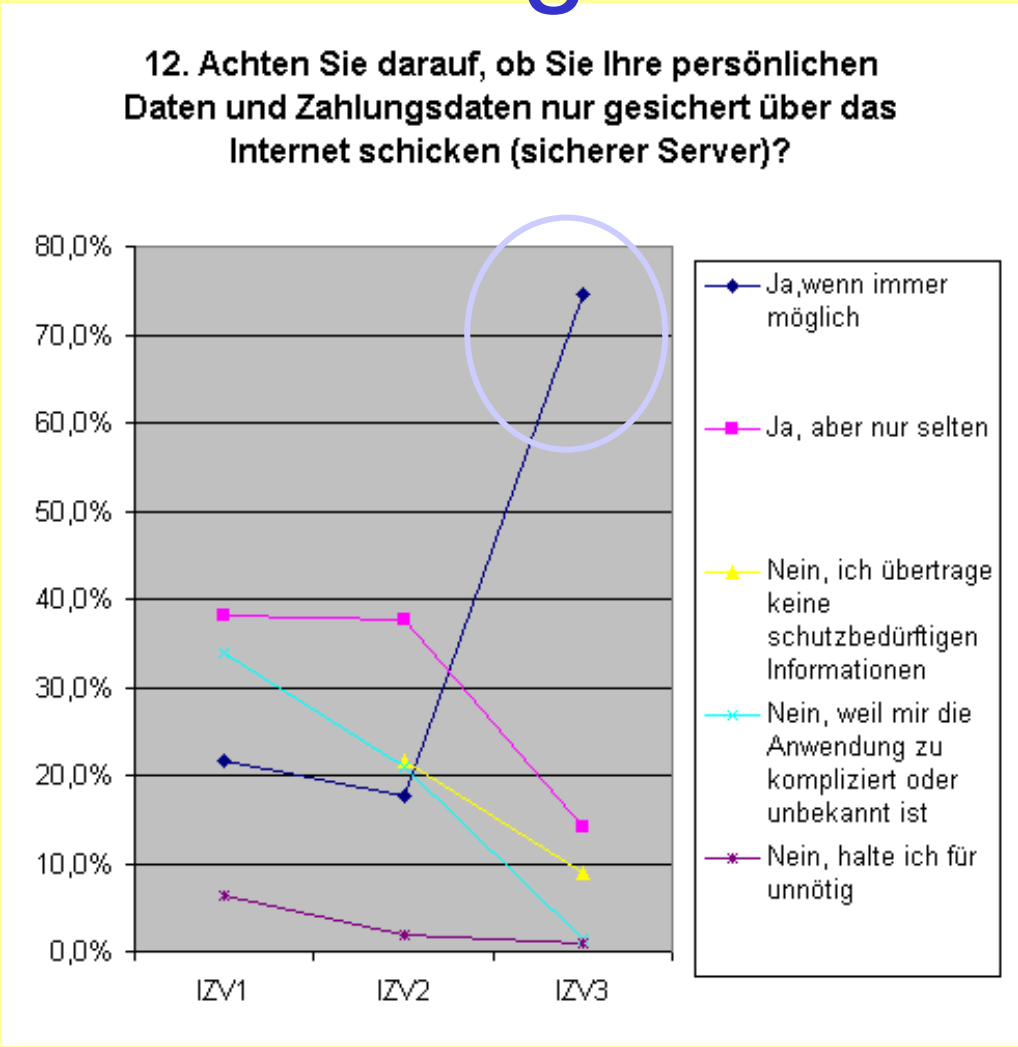
Umfrage-Ergebnis

14. Anhand welcher Kriterien entscheiden Sie, ob eine Internetseite für Sie vertrauenswürdig ist? (Mehrfachnennungen möglich)		
Design der Webseiten	500	18.9 %
Ruf oder Name des Anbieters	2207	83.6 %
Echtheitszertifikate	1564	59.3 %
Korrekte WWW-Adresse (URL)	1454	55.1 %

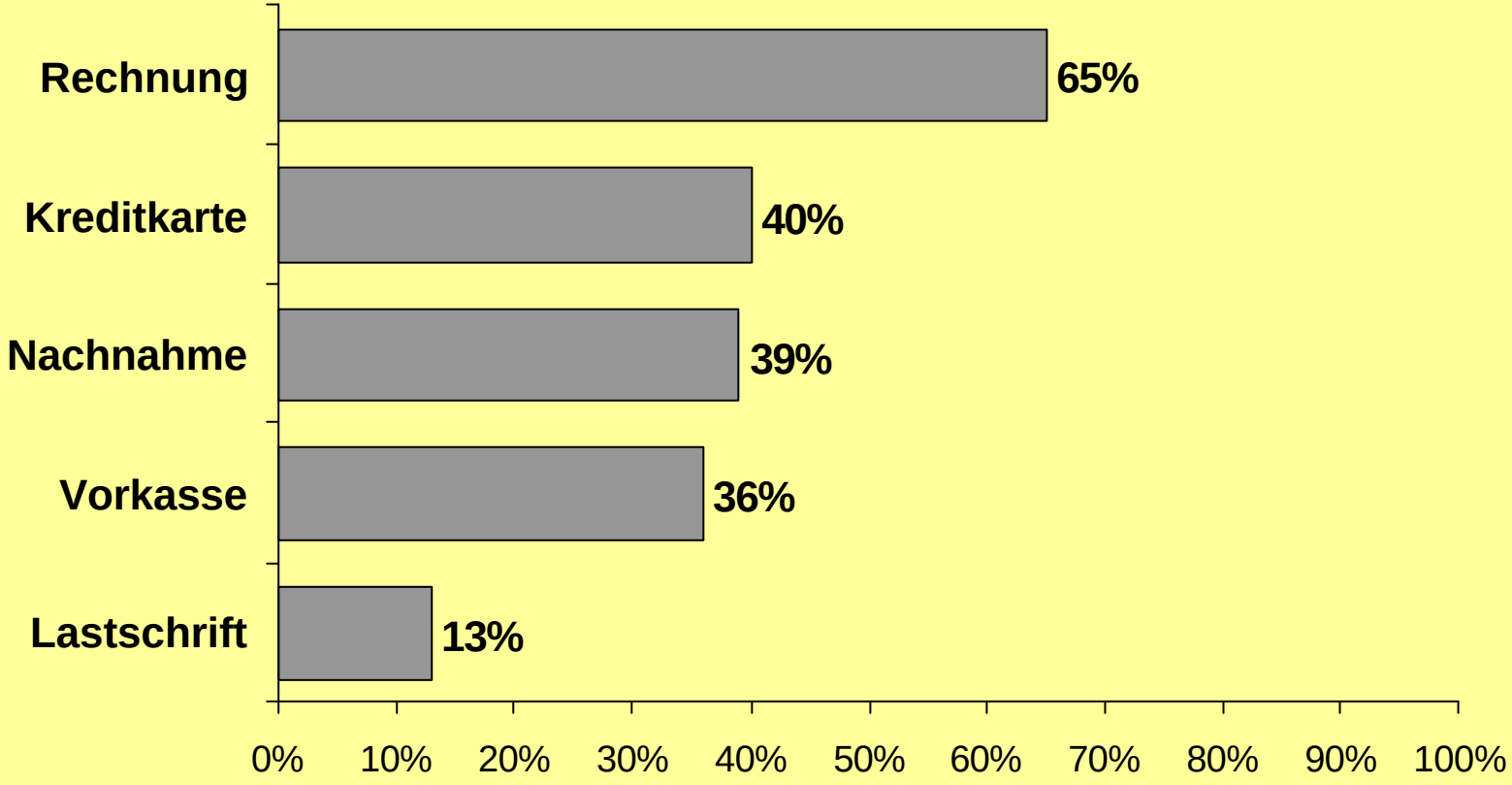
Umfrage-Ergebnis

25. In wie vielen Jahren werden für Sie persönlich Online-Einkauf und virtuelle Bezahlungsmethoden zur Selbstverständlichkeit geworden sein?		
ist bereits selbstverständlich	952	37.4 %
innerhalb von 2 Jahren	833	32.7 %
innerhalb von 5 Jahren	526	20.6 %
in mehr als 5 Jahren	142	5.6 %
niemals	95	3.7 %

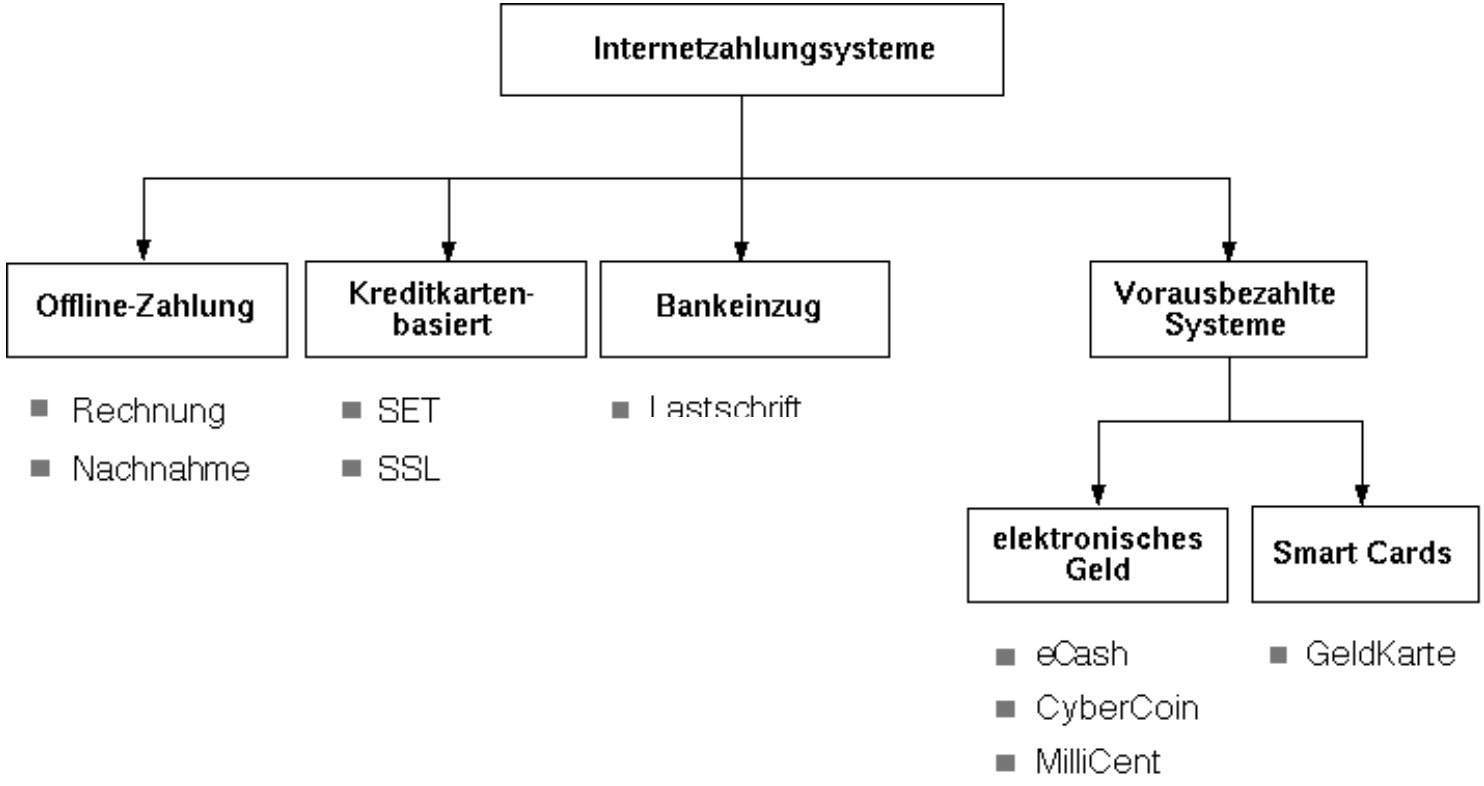
Umfrage-Trends



Angebotene Zahlungsverfahren Onlineshops



Kategorisierung der Bezahlsysteme



Kategorisierung nach Summe pro Transaktion

Picopayment

bis zehn Pfennig, Teilungen bis hundertstel Pfennig

Micropayment

bis fünf Mark, Teilungen bis ein Pfennig

Macropayment

Beträge ab fünf Mark, Teilungen bis ein Pfennig

Probleme einer Finanztransaktion über ein offenes Netz

Verlust der Vertraulichkeit

Informationsgewinn durch einen Lauschangriff

Verlust der Integrität

Stimmen die empfangenen Nachrichten mit den versendeten überein?

Verlust der Authentizität

Sind sich Sender und Empfänger einander sicher?

Verbindlichkeitsverlust

Ist der Vertrag verbindlich?

Möglichkeiten einer Zugangsprüfung

Überprüfung personenbezogener Merkmale

Unterschrift, Fingerabdruck

Inhaberbezogene Kriterien auf Hardwarebasis

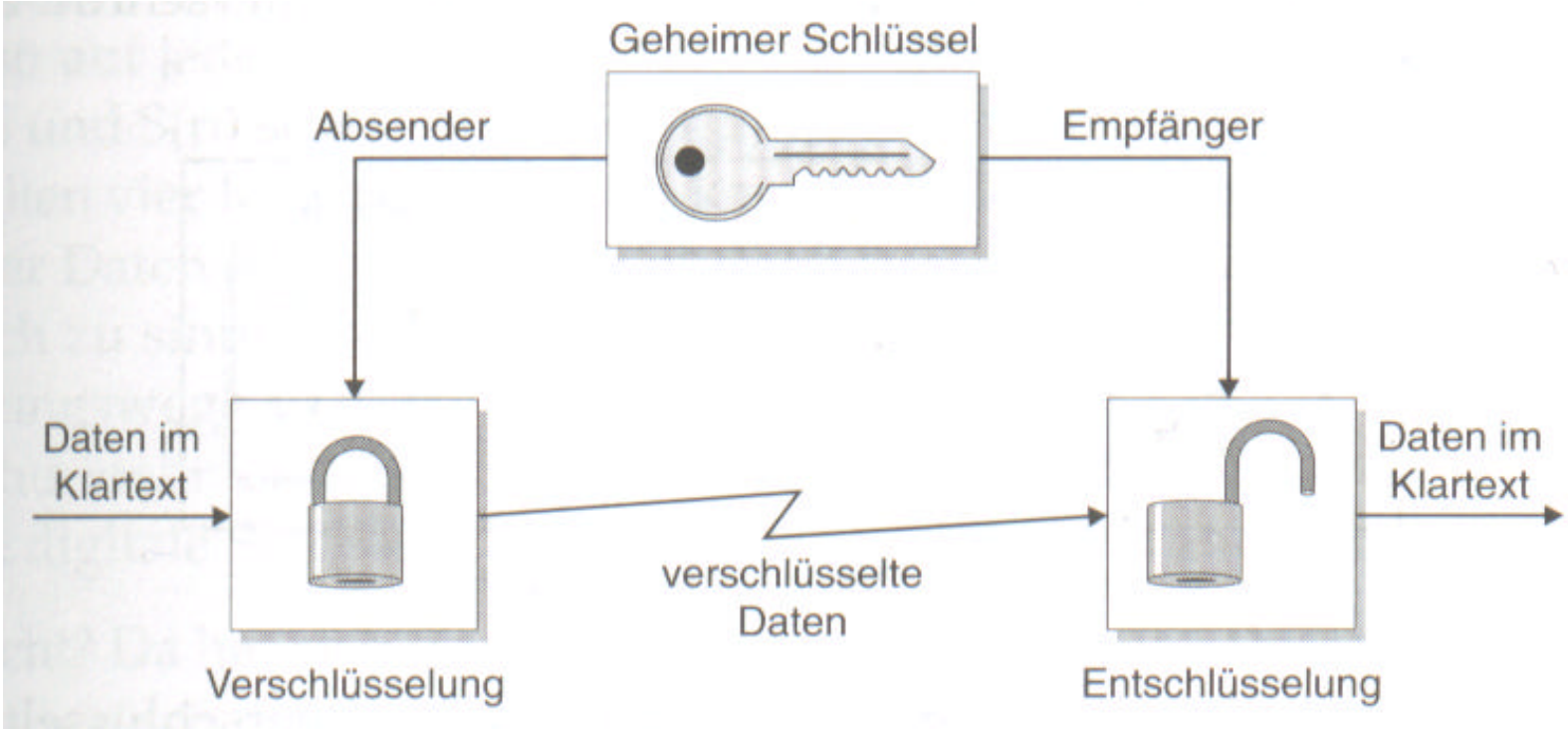
Chipkarte(nleser), bestimmte Hardware (z.B. Dongle)

Inhaberbezogenes Wissen

Geheimnummern, Passwörter

Verschlüsselungsverfahren

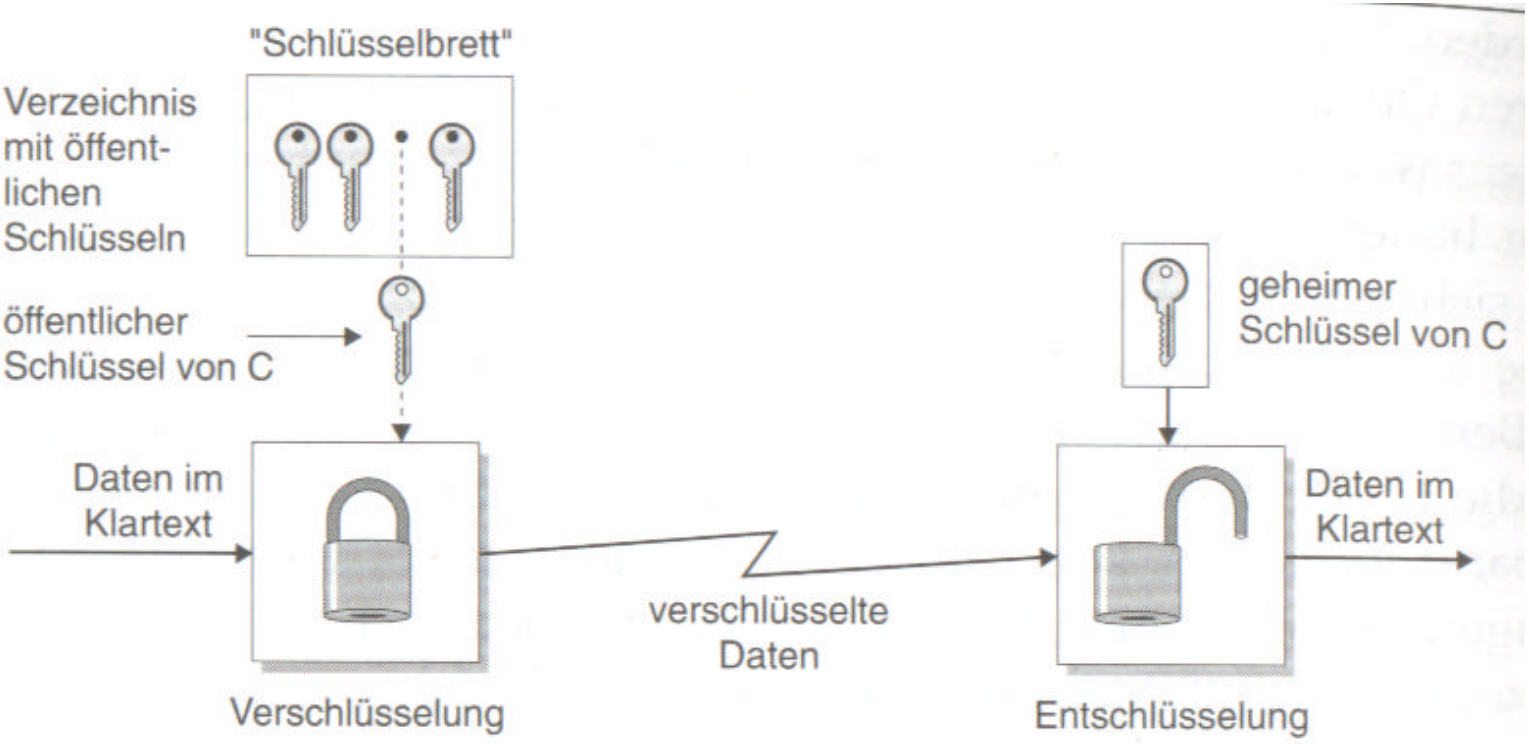
Symmetrisches Verschlüsselungsverfahren



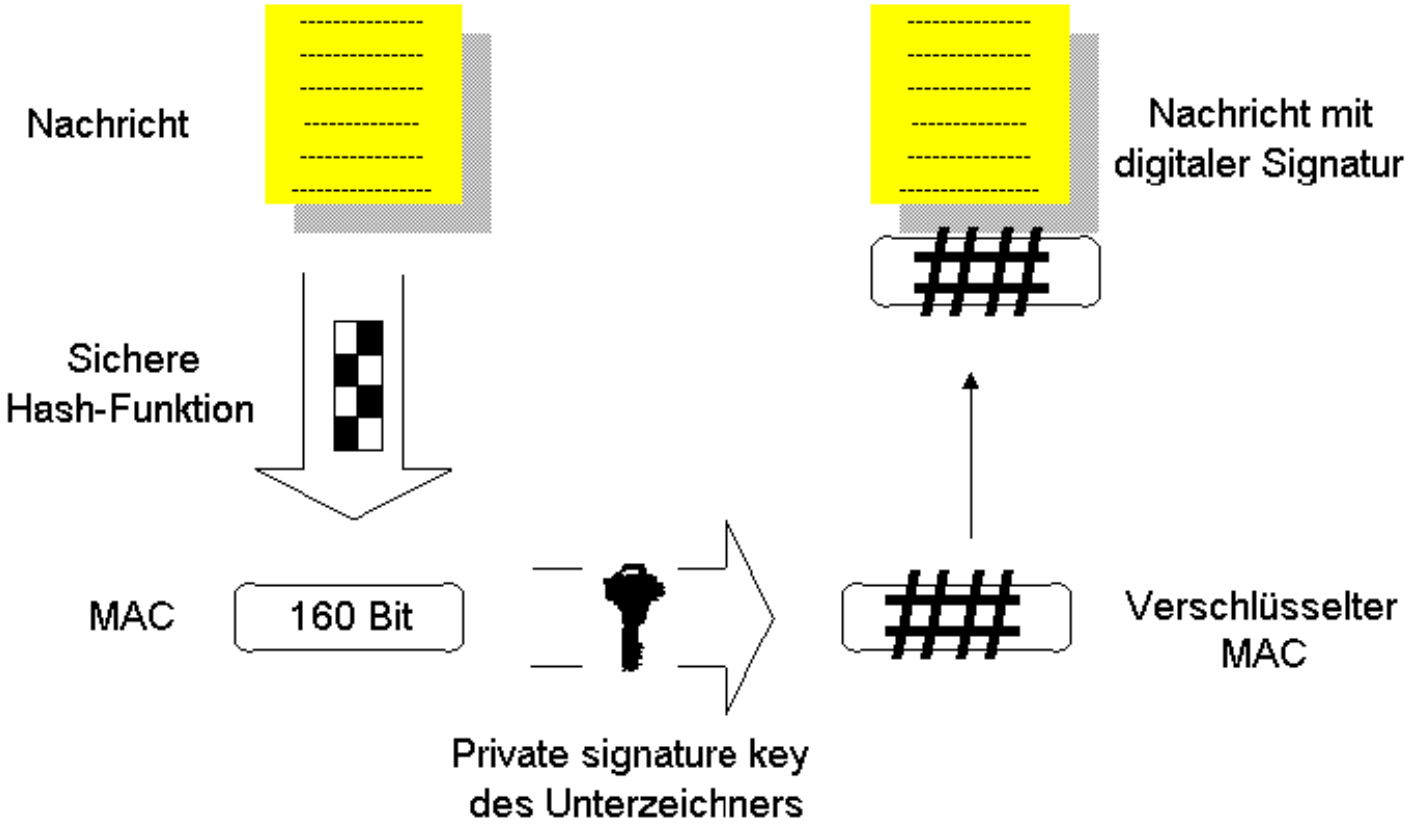
Nachteil: Schlüssel muss „geheim“ übertragen werden

Vorteil: schnell und sicher

Asymmetrisches Verschlüsselungsverfahren
Public Key Verfahren

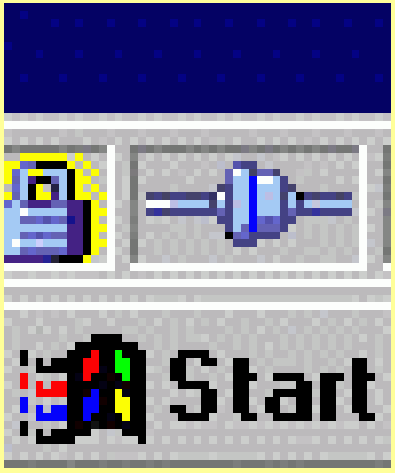


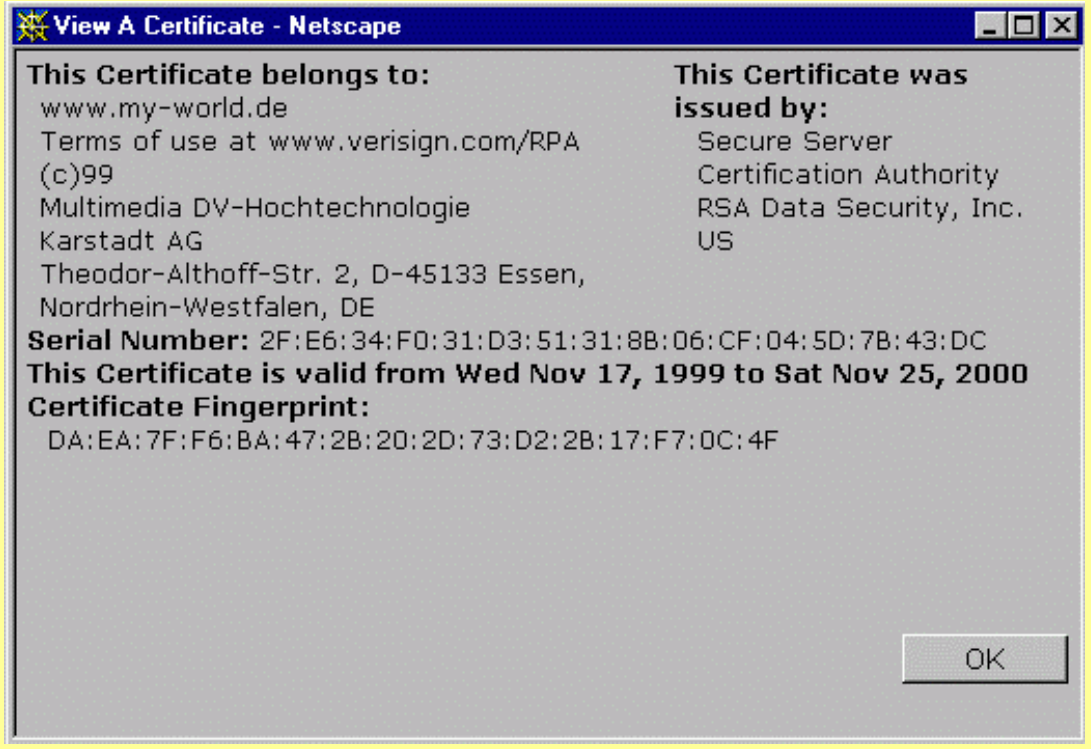
Digitale Unterschrift



SSL - Secure Socket Layer

- ursprünglich von Netscape entwickelt
- besteht aus Record-Protokoll (Definition des Formates, in dem Daten übertragen werden) und Handshake-Protokoll (Authentifizierung der Kommunikationspartner)
- Handshake-Protokoll: Browser und Server „verständigen“ sich über das zu verwendende Verschlüsselungsverfahren
- https://





Vor- und Nachteile?

SET
Secure Electronic Transaction

aus STT (Secure Transaction Technology) von Visa und Microsoft

und SEPP (Secure Electronic Payment Protocol) von MasterCard, IBM, Netscape und Cybercash

entstand SET (Februar 1996)

Ziele von SET

1. Garantie der Vertraulichkeit von Informationen (durch Nachrichtenverschlüsselung)
2. Garantie der Integrität von Zahlungen (durch digitale Unterschrift)
3. Garantie der Identität des Karteninhabers (durch digitale Unterschrift mit Zertifikat)
4. Garantie der Identität des Händlers (durch digitale Unterschrift mit Zertifikat)
5. Verwendung bestmöglicher Sicherheitssysteme während eine Transaktion
6. Gewährleistung größtmöglicher Kompatibilität aller SET-Systeme auf allen Plattformen

Beteiligte

- Kartenbesitzer (Cardholder)

  Jede Person, die eine Kreditkarte besitzt, und an SET teilnehmen möchte (oder schon teilnimmt)

- Kartenausgebende Bank (Issuer)

  Das ist das Unternehmen, das den Kartenbesitzer mit der Kreditkarte versorgt. Der Kartenaussteller ist letztendlich für die Begleichung der Schulden des Kartenbesitzers verantwortlich und trägt das Risiko

Beteiligte

- Händler (Merchant)

  Jede Institution, die Waren oder Dienstleistungen (Service) im Internet anbietet und sie an Kartenbesitzer verkaufen möchte

- Bank des Händlers (Acquirer)

  Der Acquirer besorgt die Kartenautorisierung und die Erfassung und Transferierung der Bezahlung für die Händler. Über Acquirer Akzeptanz mehrere Kreditkartengesellschaften möglich. Der Acquirer vergibt an Händler SET-Zertifikate

Beteiligte

- Payment Gateway

  Das Payment Gateway stellt eine Schnittstelle zwischen SET und den existierenden Netzwerken der Kreditkartengesellschaften dar, die zur Autorisierung und zur Erfassung der Wertausgleiche dient.

- Kreditkartengesellschaft (Brand)

  Stellen Regeln auf für Gebrauch und Akzeptanz von Kreditkarten. Sie unterhalten ein Netzwerk zur Autorisation der Bezahlungen und der Transferierung der Gelder

Beteiligte

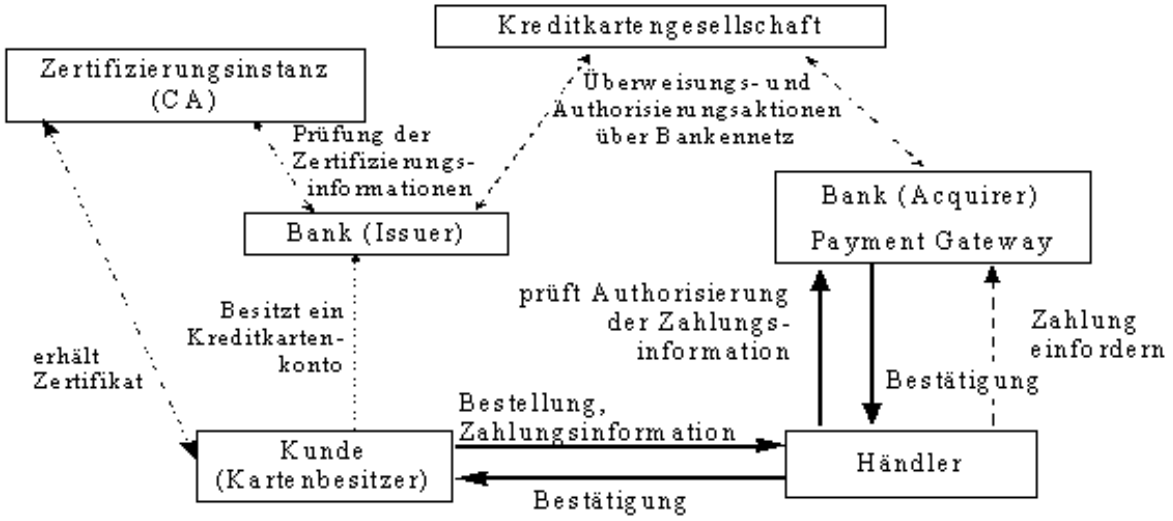
- Drittanbieter (Third Parties)

  Issuer und Acquirer können sich der Dienst von Drittanbietern zur Geschäftsabwicklung bedienen

- Zertifizierungsinstanzen (Certification Authorities)

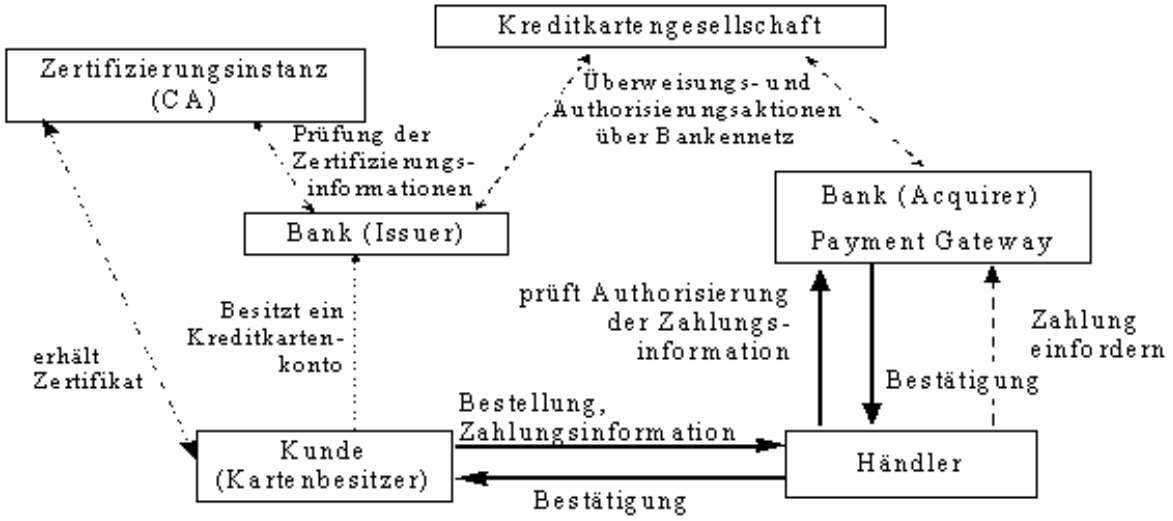
  Zur Autorisierung der Kartenbesitzer, Händler und des Payment Gateway werden Zertifizierungen der öffentlichen Schlüssel vorgenommen.

Zahlungsabwicklung nach dem SET-Protokoll



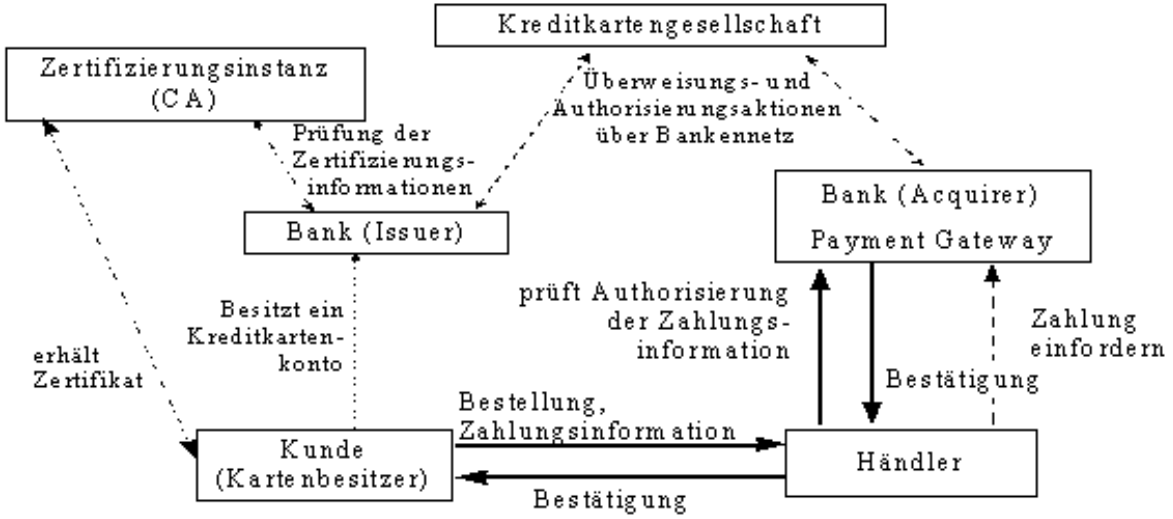
1. Initialisierungsnachricht Kunde an Händler
2. Händler sendet digital signierte Nachricht, die zusätzlich das Verschlüsselungszertifikat mit dem öffentlichen RSA-Schlüssel der Zertifizierungsstelle/Kreditkarteunternehmen/Clearing Stelle enthält.
3. Kunde fertigt signierte Bestellung und signierte Zahlungsanweisung an. Keditkartendaten werden mit dem öff. RSA-Schlüssel verschlüsselt, sind also durch den Händler nicht lesbar.

Zahlungsabwicklung nach dem SET-Protokoll



4. Händler schickt eine digital signierte Anfrage (erst DES [symmetrisches Verfahren] verschlüsselt und dann RSA verschlüsselt), dazu kommt das Verschlüsselungszertifikat des Händlers, die Zahlungsanweisung und der verschlüsselte DES-Schlüssel.
5. Die Kreditkartenfirma entschlüsselt die Nachricht und authorisiert die Zahlung.
6. Der Händler erhält eine Bestätigungsnachricht.

Zahlungsabwicklung nach dem SET-Protokoll



Drei Phasen der SET-Transaktion

1. Bestellung (*Purchase Request*)
Bestellung des Kunden und Quittung des Händlers
2. Authorisierung (*Payment Authorisation*)
Anfrage des Händlers an seine sog. Zertifizierungsstelle (*Payment Gateway*), ob die Zahlungsanweisung des Kunden akzeptiert wird
3. Abrechnung (*Payment Capture*)
Abrechnung des Händlers mit der Bank des Kunden

SET-Sicherheitsmechanismen

- Symmetrische Verschlüsselung (DES)
  - für Verschlüsselung der Session Keys
  - Schnelligkeit
- Public-Key-Verfahren mit Einsatz von zwei Public-Key-Schlüssel-Paaren
  - ein Paar für Übergabe der symmetrischen Session Keys (jeweils für Händler und Payment Gateway)
  - ein Paar für Signatur(jeweils für Kunde, Händler und Payment Gateway)

SET-Sicherheitsmechanismen

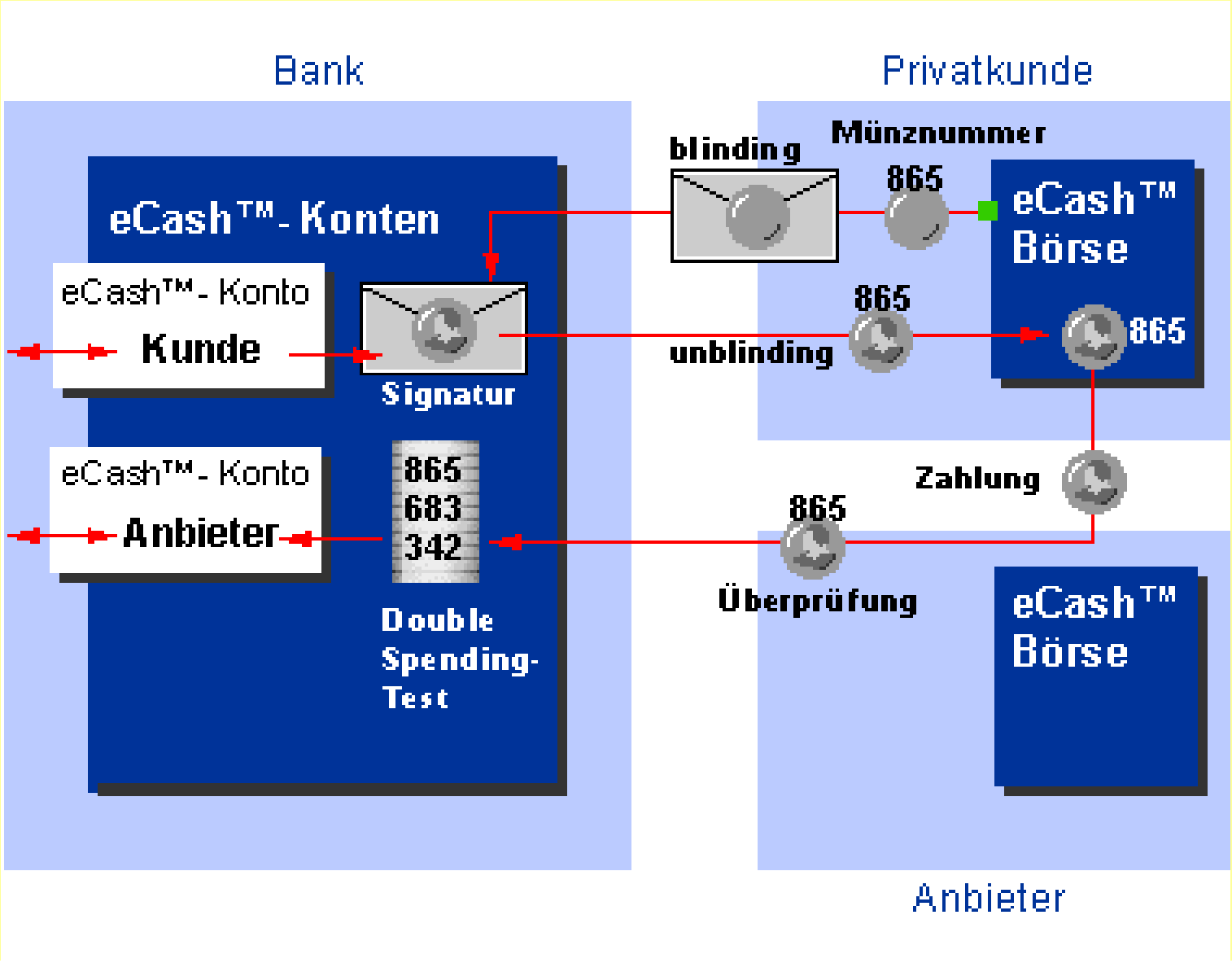
- Hash-Verfahren (Digest)
- Zertifikate (Problem der gesicherten Schlüsselübergabe)
- Für Kartenzahlung maximale Anonymität
  - Händler: nur Orderinfo
  - Bank: nur Zahlungsinfo

Vor- und Nachteile?

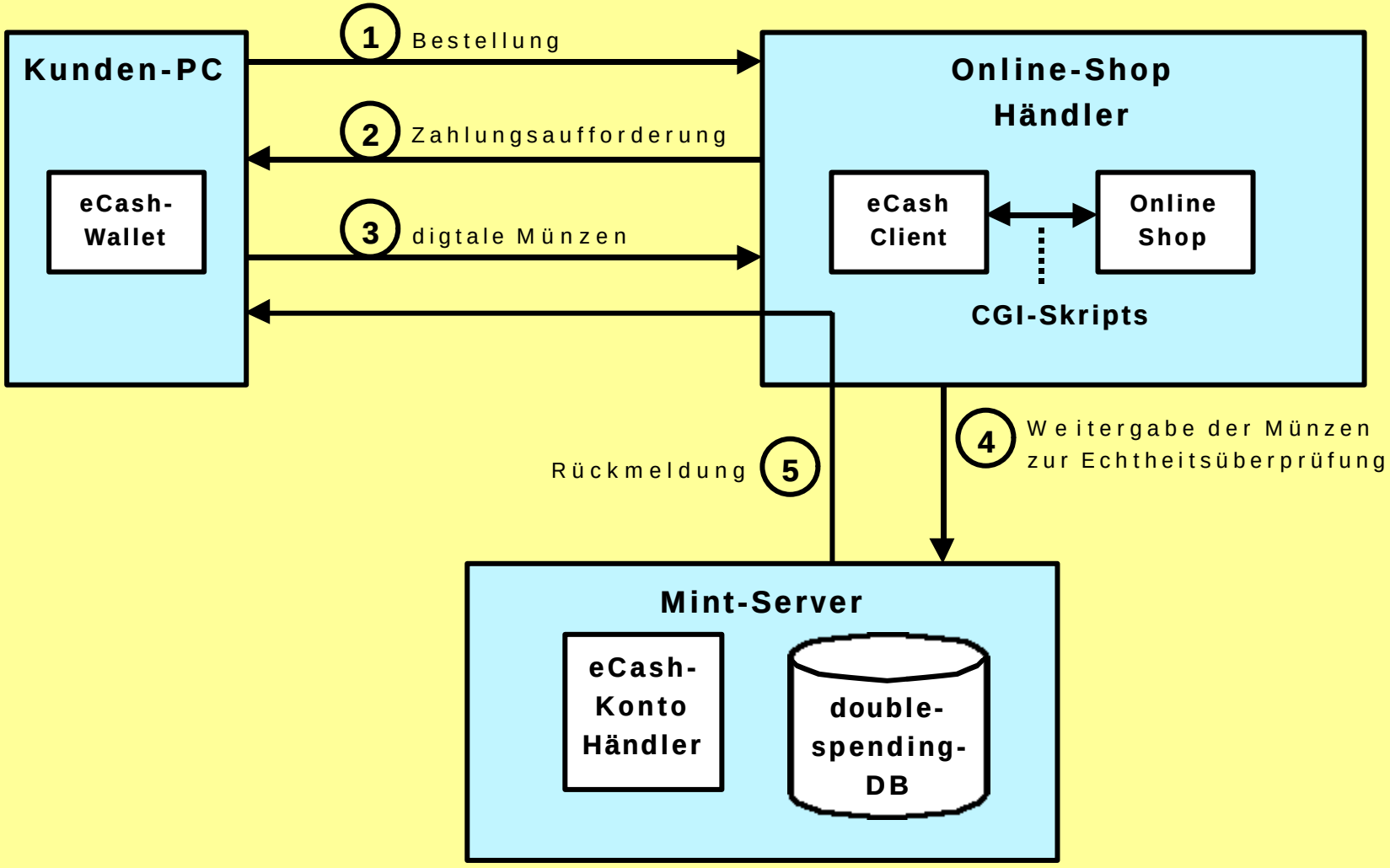
eCash-System
Bsp. Yahoo-Card (Deutsche Bank)

- Voraussetzung: eCash-Software (Geldbörse)
- eCash-Münzen werden in Form einer Datei übertragen
- erhaltene eCash-Münzen können nicht weitergegeben werden, sondern müssen auf dem eCash-Konto eingelöst werden
- Zahlungen sind anonym (sog. „Blendungsverfahren“), eindeutige Seriennummer wird vom Kunden „verblendet“, Bank bestätigt dann Echtheit über digitale Signatur
- eCash-Münzen werden vom eCash-Konto in Geldbörse übertragen
- Geldbörse wird auf der Festplatte gespeichert (max. 400 DM)
- Der Kunde ist dazu verpflichtet, die „Geldbörse“ zu schützen.
- Sobald der Bank der Missbrauch mitgeteilt wurde, haftet sie für alle Schäden.

Erzeugen von eCash-Münzen



Zahlen mit eCash-Münzen



Sicherheitsmerkmale eCash

Sicherheitsmerkmale:

- 768 bit RSA, Triple-DES 64 bit
- Anonymität des Kunden gegenüber der Bank durch blinde Signaturen
- Fälschungssicherheit durch double-spending-Test
- Secret-Splitting zur Aufhebung der Anonymität bei Doppelnutzung einer Münze
- Recovery-Mechanismus, um Münzen nach Systemcrash zu regenerieren
- Schutz der Wallet über Paßwort

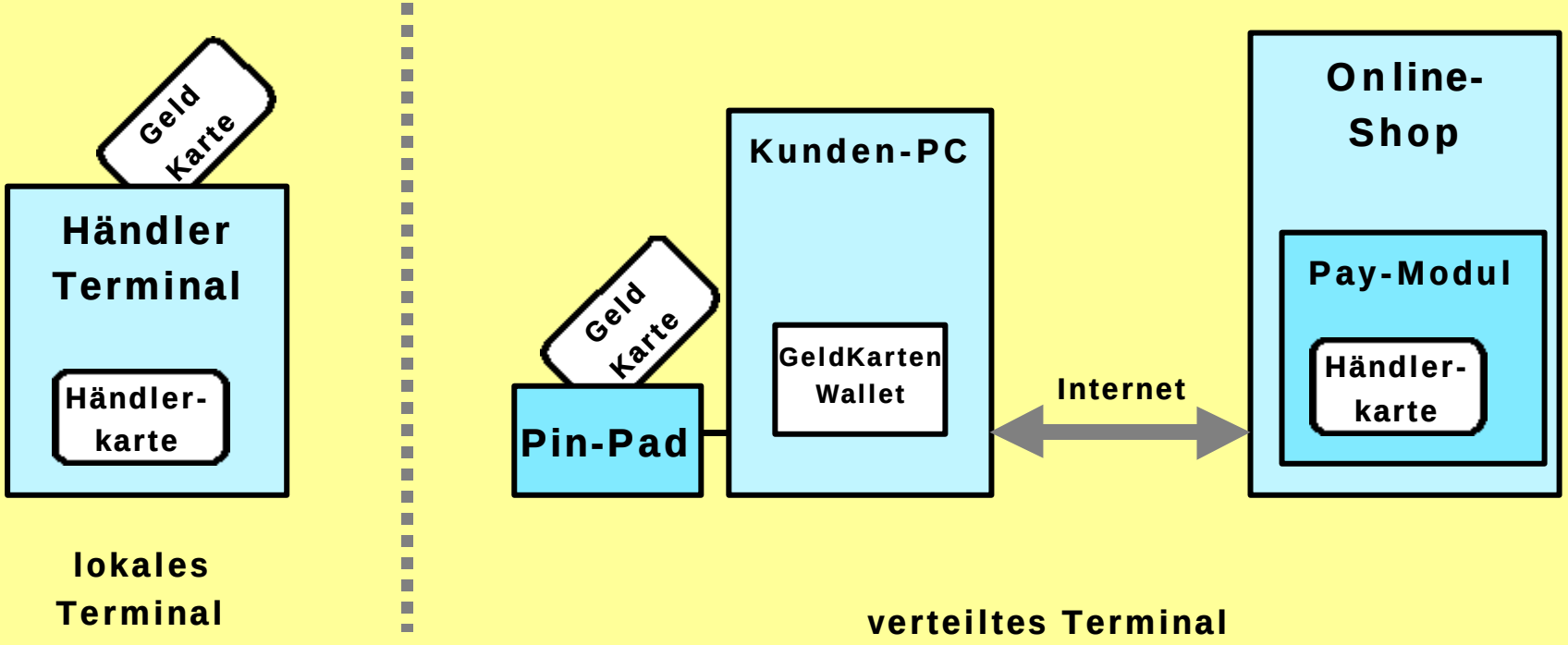
Mögliche Schwachstellen:

- Betrüger könnte abgehörte Münzen vor dem Händler bei der Bank einlösen
- Durch trojanisches Pferd könnte Betrüger Münzen aus der Wallet stehlen und bei einem Händler einlösen.

Bezahlen per Geldkarte im Internet
Beispiel Sparkasse

- Voraussetzung: Kartenlesegerät (seriell oder USB), Geldkarte, Software
- Kunde sucht Waren aus und wählt Zahlungsart „Geldkarte“
- Browser startet Java-Applet, das Rechnungsdaten anzeigt
- Geldkarte wird eingelegt
- Daten werden vor der Übertragung mit einem Kryptogramm versehen (Authentizität)
- Geldkarten-Akzeptanzstelle bucht das Geld ab und schreibt es dem Händler gut
- Geldkarten-Akzeptanzstelle meldet erfolgreiche Gutschrift an Händler, der die Ware auf den Weg bringt

Die GeldKarte im Internet



Net900
von der Telekom-Tochter TeleCash

- Abrechnung über die Telefonrechnung
- „Nachfolger“ des Inkassosystems von T-Online
- spezielle Software notwendig (400 kB)
- aktuelle Datenverbindung wird unterbrochen und kostenpflichtige Verbindung wird aufgebaut
- anschließend wird ursprüngliche Datenverbindung wieder aufgebaut
- Summen bis 4,99 DM pro Zeiteinheit/Transaktion möglich

Bezahlen über Handy paybox

- Vertragspartner wird Handy-Nummer angegeben
- Händler ruft bei Paybox an und gibt Betrag und Mobiltelefonnummer ein
- Paybox ruft Kunden an und läßt sich Bestellung durch Eingabe der paybox-PIN bestätigen
- Betrag wird per Lastschrift eingezogen
- jährliche Grundgebühr für Kunden

Click & buy Firstgate

- Kunde muss sich bei firstgate mit Konto- oder Kreditkartennummer registrieren
- Kunde klickt kostenpflichtigen Link an, wird zum firstgate-Server geleitet, muss sich per Paßwort identifizieren und bekommt kostenpflichtige Inhalte angezeigt
- Abrechnung pro Besuch der Site und für Nutzungsdauer möglich
- monatliche Abrechnung von firstgate mit dem Kunden und dem Anbieter
- Provision zwischen 30% und 50%
- monatliche Gebühr für Anbieter: 9,90 DM

Anforderungen an elektronische Zahlungssysteme

Sicherheit

- Vertraulichkeit
- Transaktions-integrität
- Authentizität

Systemtechnik

- Verfügbarkeit
- einfache Benutzung
- Haltbarkeit
- Skalierbarkeit

Zahlungssystem (im engeren Sinn)

- Anonymität
- Akzeptanzfähigkeit
- Universalität
- Kompatibilität
- Internationalität
- Risikoverteilung
- Spontanität

Wirtschaftlichkeit

- Transaktionskosten
- Einstandskosten

Recht

- Verbindlichkeit
- bankrechtliche Anf.