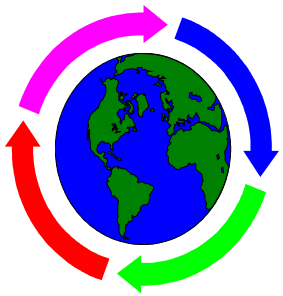


Sichere Abwicklung von Geschäftsvorgängen im Internet

Diplomarbeit von *Peter Hild*

Wirtschaftsinformatik

FHTW Reutlingen

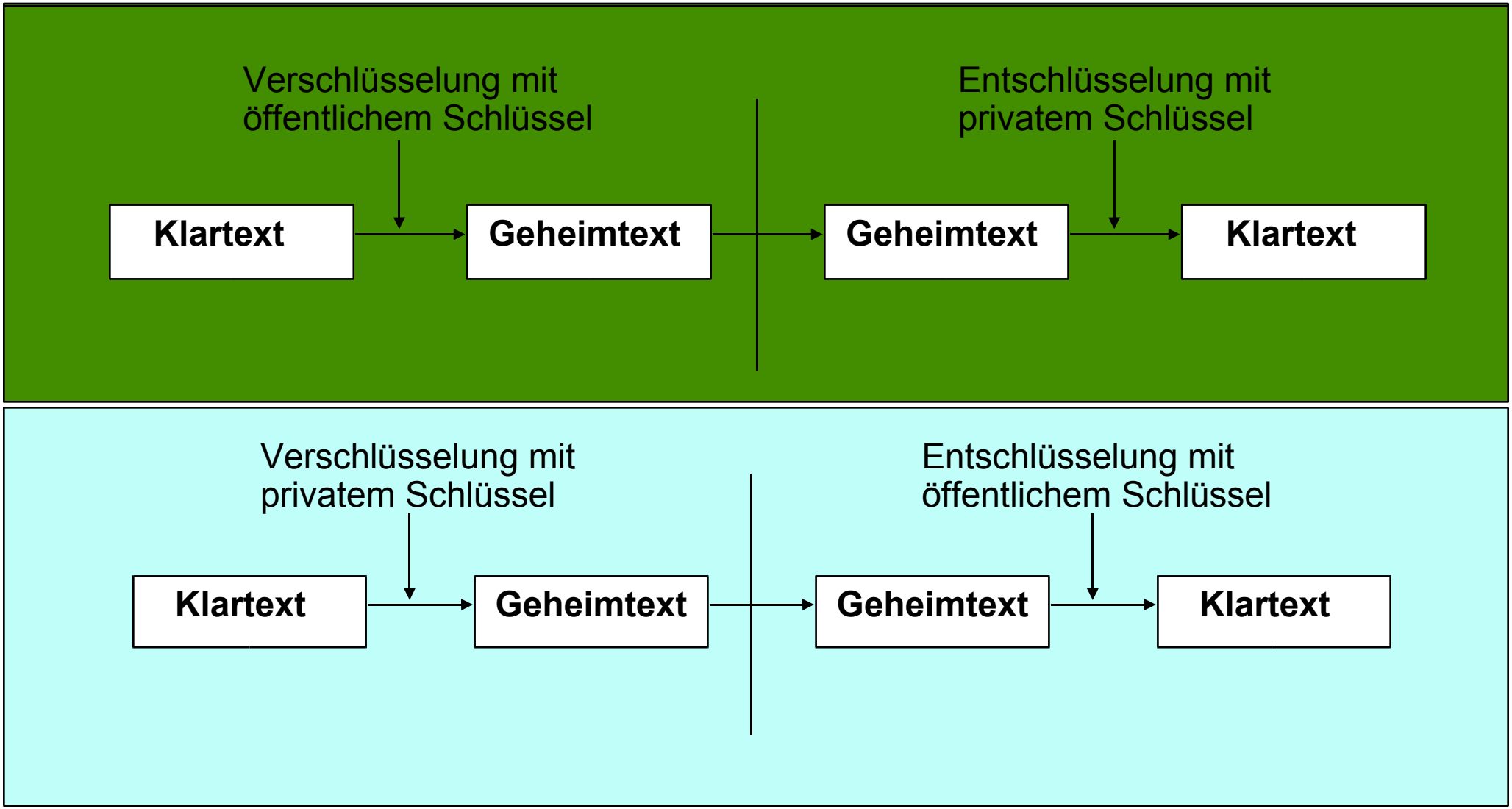
- **Theoretische Grundlagen der Kryptologie**
- **Vorhandene Sicherheitskonzepte für das WWW**
- **Bewertung dieser Konzepte**
- **Simulation eines sicheren Geschäftsvorgangs**

Theoretische Grundlagen

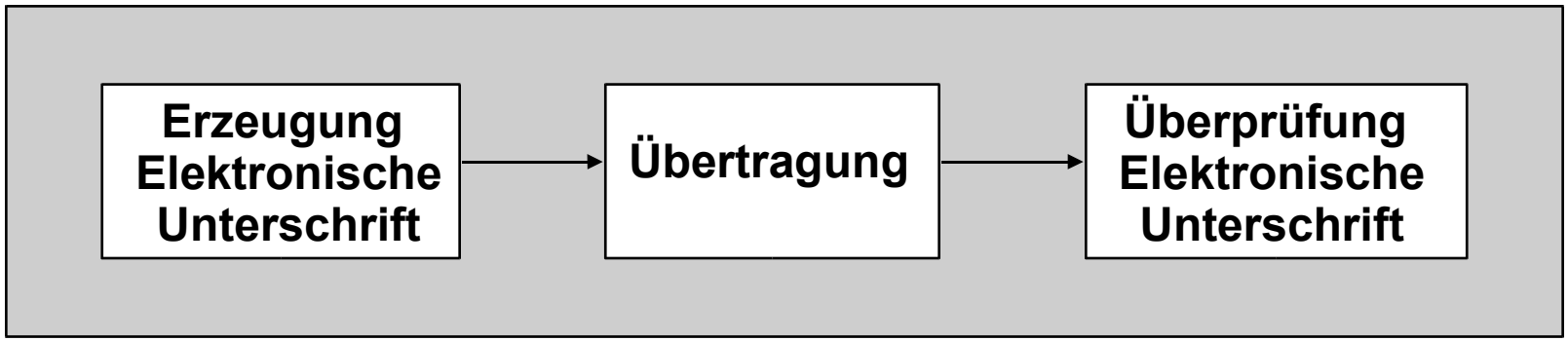
Sicherheitsmechanismen	Sicherheitsfunktionen
Verschlüsselung	Vertraulichkeit und Zugriffskontrolle
Elektronische Unterschrift	Integrität, Authentifizierung und Nichtabstreitbarkeit

Symmetrische Verschlüsselung

Asymmetrische Verschlüsselung

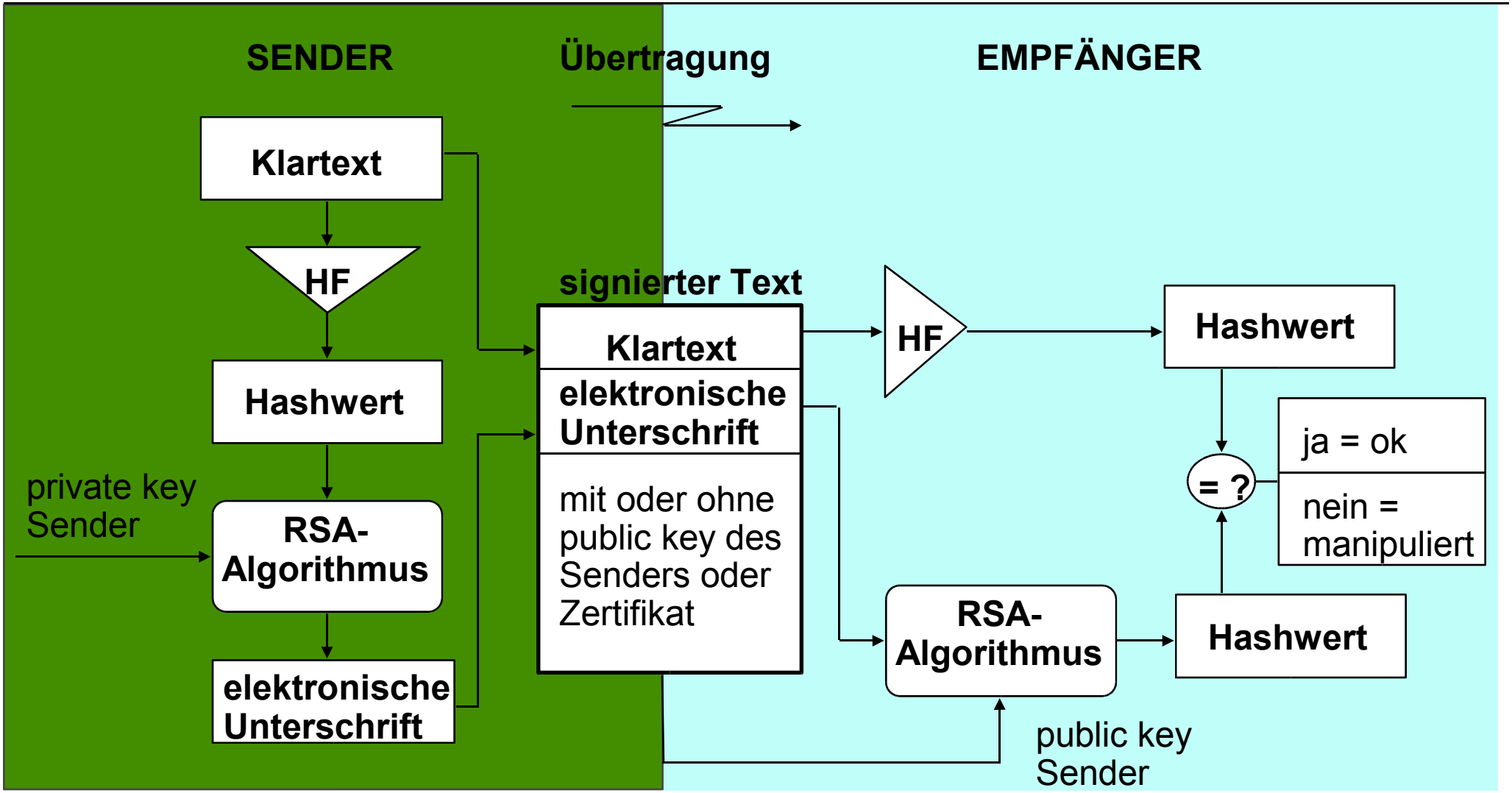


Die Elektronische Unterschrift



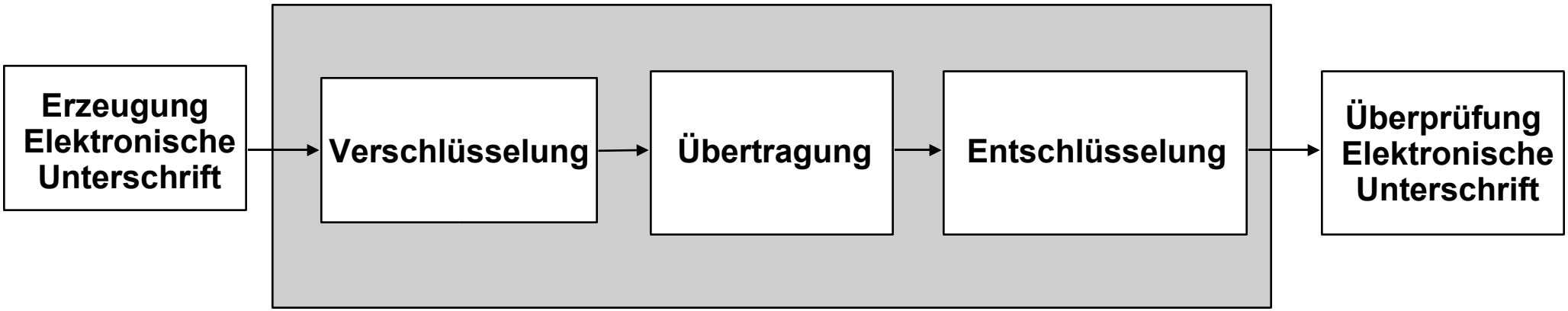
Ablauf Elektronische Unterschrift

Die Elektronische Unterschrift



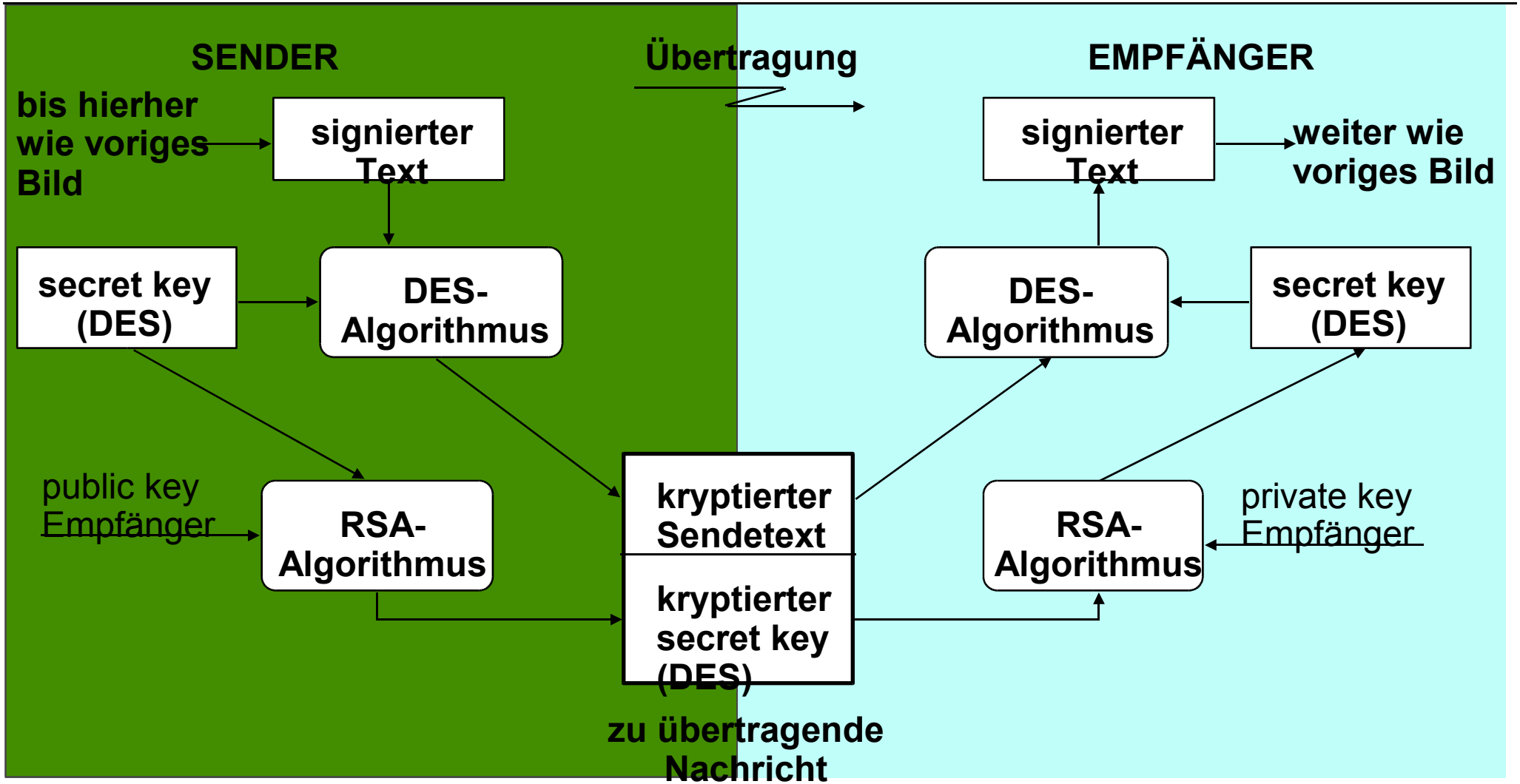
HF = Hash-Funktion

Elektronische Unterschrift mit Verschlüsselung



Ablauf Elektronische Unterschrift mit Verschlüsselung

Digitaler Umschlag (RSA-Schlüsselaustausch)



signierter Text = Klartext + elektronische Unterschrift (siehe voriges Bild)

Vorhandene Konzepte für das World Wide Web

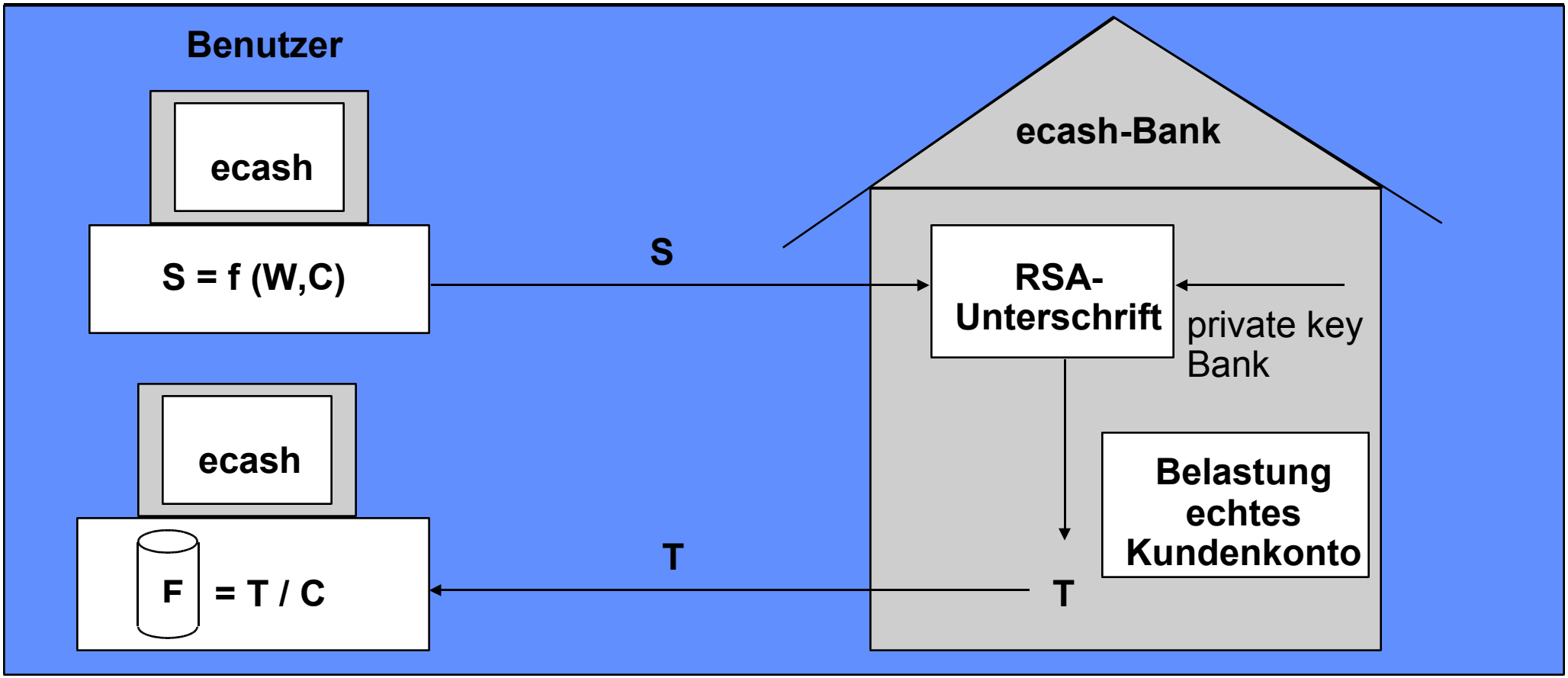
- sichere Zahlungssysteme
  - DigiCash / ecash (elektronisches Geld)
  - CyberCash (Kreditkartenzahlung)
  - First Virtual (Kreditkartenzahlung)
- sichere Protokolle
  - SSL (Secure Socket Layer)
  - SHTTP (The Secure Hypertext Transfer Protokoll)

Sichere Zahlungssysteme:

DigiCash (ecash)

- Verfahren, das Münzgeld elektronisch simuliert
- Kunde "kauft" virtuelles Geld (ecash) bei einer Bank, die das ecash-System unterstützt
- Anonymität des Käufers durch "Blinding"-Verfahren
- ecash basiert auf dem *public key digital signatur*-Verfahren von RSA
- Speicherung der elektronischen Münzen (*coins*) beim Benutzer (Festplatte, Diskette oder Chipkarte)
- spezielle Benutzersoftware nötig

ecash: Erzeugung von elektronischen Münzen



W = Zufallszahl (Rohmaterial für die elektronische Münze)
C = Zufallszahl (Tarnzahl)
S = Zahl für die Bank
T = von der Bank signierte Zahl
F = elektronische Münze (coin)

ecash: Zahlungsablauf und Verrechnung

Kunde

ecash-coin

Ware

Händler

ecash-coin

Bestätigung

ecash-Bank

überprüft Authentizität
der digitalen Unterschrift

1) prüft Signatur und
Doppelausgabe

2) schreibt Betrag dem
echten Händlerkonto
gut

Vorhandene Konzepte für das World Wide Web

- sichere Zahlungssysteme
  - DigiCash / ecash (elektronisches Geld)
  - CyberCash (Kreditkartenzahlung)
  - First Virtual (Kreditkartenzahlung)
- sichere Protokolle
  - SSL (Secure Socket Layer)
  - SHTTP (The Secure Hypertext Transfer Protokoll)

Sichere Zahlungssysteme:

(Secure Internet Payment Service TM)

- **Schutz von Kreditkartennummern bei WWW-Einkäufen durch Verschlüsselung**
- **Spezielle Helper-Application-Software**
- **Zusammenarbeit mit Bank des Händlers (online-Autorisierung)**
- **Verwendete Algorithmen:**
  - **768-Bit-RSA-Verschlüsselung**
  - **56-Bit-DES-Verschlüsselung**
  - **MD5-Hash-Funktion**
- **Elektronische Unterschrift für jede Transaktion**

Vorhandene Konzepte für das World Wide Web

- sichere Zahlungssysteme
  - DigiCash / ecash (elektronisches Geld)
  - CyberCash (Kreditkartenzahlung)
  - First Virtual (Kreditkartenzahlung)
- sichere Protokolle
  - SSL (Secure Socket Layer)
  - SHTTP (The Secure Hypertext Transfer Protokoll)

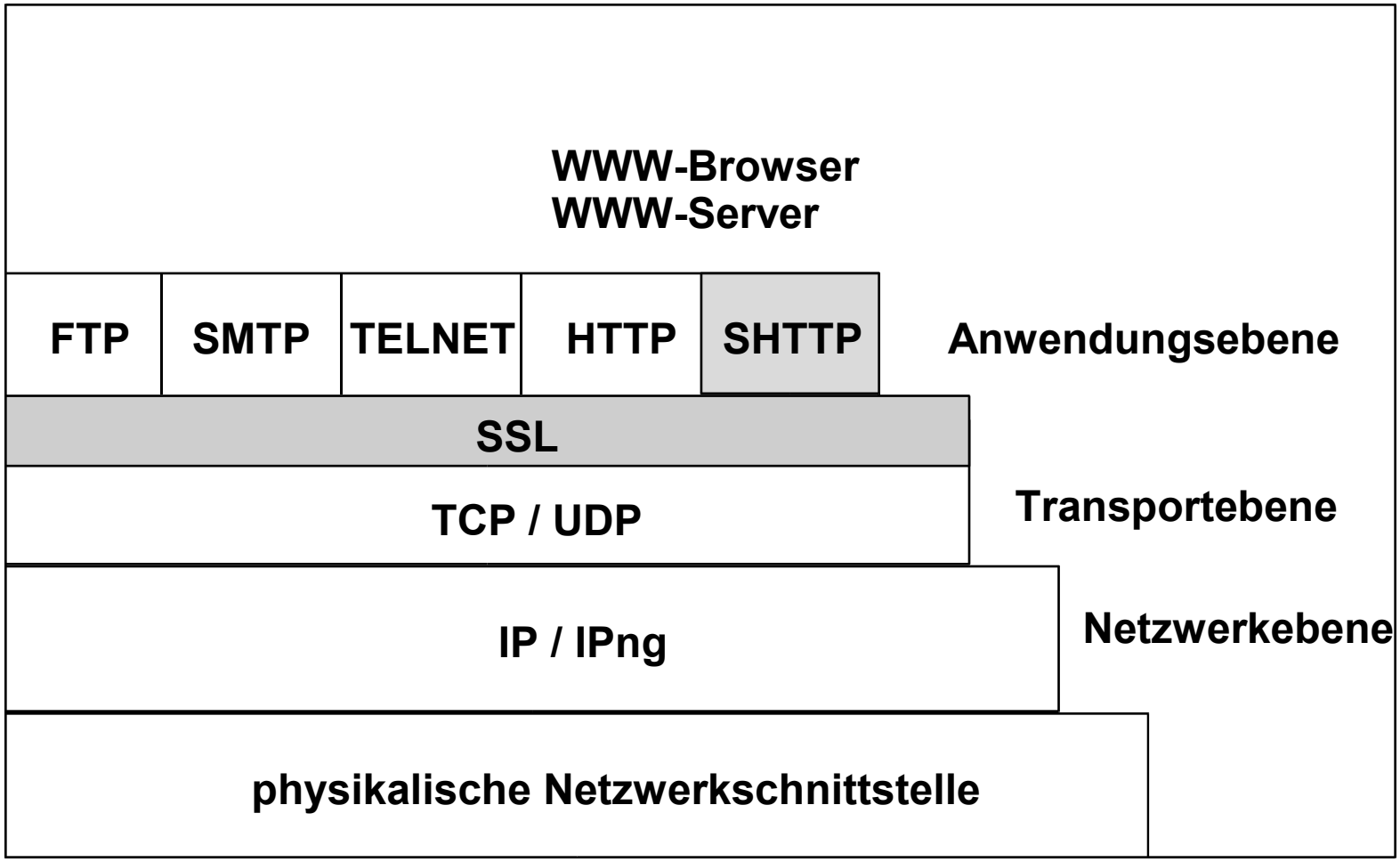
Sichere Zahlungssysteme:

- Ersatz der realen Kreditkartennummer durch die FIRST VIRTUAL account ID
- keine Verschlüsselungsverfahren nötig
- Voraussetzungen:
  - Master- oder Visacard
  - Konto bei Bank in den USA
  - Email-Adresse
- Kaufbestätigung oder Kaufablehnung mittels E-mail
- Abwicklung der realen Finanztransaktionen über einen "sicheren" Server

Vorhandene Konzepte für das World Wide Web

- sichere Zahlungssysteme
  - DigiCash / ecash (elektronisches Geld)
  - CyberCash (Kreditkartenzahlung)
  - First Virtual (Kreditkartenzahlung)
- sichere Protokolle
  - SSL (Secure Socket Layer)
  - SHTTP (The Secure Hypertext Transfer Protokoll)

Sichere Protokolle - Einordnung



Vorhandene Konzepte für das World Wide Web

- sichere Zahlungssysteme
  - DigiCash / ecash (elektronisches Geld)
  - CyberCash (Kreditkartenzahlung)
  - First Virtual (Kreditkartenzahlung)
- sichere Protokolle
  - SSL (Secure Socket Layer)
  - SHTTP (The Secure Hypertext Transfer Protokoll)

Sichere Protokolle:

SSL (Secure Socket Layer)

- **Arbeitsweise:**
  - **neuer Layer zwischen TCP/IP Transportebene und TCP/IP Anwendungsebene (aufgesetzt auf Socket-Schnittstelle)**
  - **etabliert einen sicheren Kanal (Vertraulichkeit, Authentifizierung, Integrität)**
  - **erlaubt Verschlüsselung anderer Anwendungsprotokolle (telnet, ftp usw.)**
  - **Handshake-Protokoll, in dem die entsprechenden Verschlüsselungsverfahren ausgehandelt werden**
- **neuer URL: https://**
- **abgedeckte Sicherheitsfunktionen:**
  - **Vertraulichkeit durch Datenverschlüsselung (DES, RC4, RC2)**
  - **Server-Authentifizierung (public key-Verfahren; X.509)**
  - **Datenintegrität durch MAC (Hash: MD2, MD5)**
- **Server-Zertifikat (X.509 oder PKCS#6)**
- **Schlüsselaustauschverfahren (RSA)**
- **Nachteil: keine digitale Unterschrift**

Vorhandene Konzepte für das World Wide Web

- sichere Zahlungssysteme
  - DigiCash / ecash (elektronisches Geld)
  - CyberCash (Kreditkartenzahlung)
  - First Virtual (Kreditkartenzahlung)
- sichere Protokolle
  - SSL (Secure Socket Layer)
  - SHTTP (The Secure Hypertext Transfer Protokoll)

Sichere Protokolle:

SHTTP (The Secure Hypertext Transfer Protokoll)

- Ersatz/Erweiterung für HTTP (nur WWW-Sitzungen sicherbar)
- Rahmen für verschiedene kryptographische Standardmethoden
- neuer URL: shttp://
- Kapselung von Nachrichten mittels PGP oder PEM
- Aushandlung zwischen Client und Server
  - symmetrische Verschlüsselungsverfahren (RC2, RC4, DES, IDEA)
  - asymmetrische Verschlüsselungsverfahren (RSA)
  - Elektronische Unterschrift (RSA-Verfahren)
  - Hash-Algorithmus (MD2, MD5, NIST-SHS)
  - Zertifikate (X.509, PKCS#6)
- Schlüsselaustausch (in-band, out-of-band, ...)
- Sicherheitsfunktionen
  - Elektronische Unterschrift
  - Vertraulichkeit durch Datenverschlüsselung
  - Authentifizierung von Client und Server

Bewertung der sicheren Protokolle

	SSL	S-HTTP
Realisierte Sicherheitsfunktionen		
Vertraulichkeit	Verschlüsselung	Verschlüsselung
Zugriffskontrolle	ACL (Server)	ACL (Server)
Integrität	MAC	MAC
Nichtabstreitbarkeit	nein	Elektronische Unterschrift
Client-Authentifizierung	optional	ja
Server-Authentifizierung	ja	ja
Verbreitung (Client)	stark	gering
globale Version	ja	nein (mittlerweile ja)
Unterstützung anderer Anwendungsprotokolle	ja	nein (nur HTTP)

Bewertung der sicheren Zahlungssysteme

Kreditkartensysteme	Elektronische Kunstwährung
+ einfach zu realisieren + eingeführtes System	+ Anonymität + transportabel + geringe Transaktionskosten
- hohe Transaktionskosten - bei Kleinstbeträgen unwirtschaftlich - zentrale Datenerfassung	- Zweifel an der Sicherheit der neuen Zahlungsform (Mißbrauchsgefahr)

Vielen Dank

für Ihre

Aufmerksamkeit!