4. B2C,B2E Systems: Concepts and Architectures

4.1 Business-to-Consumer Systems

Architectures and Components

Shop Functionalities, Selected Components

4.2 Electronic Fulfillment & Payment

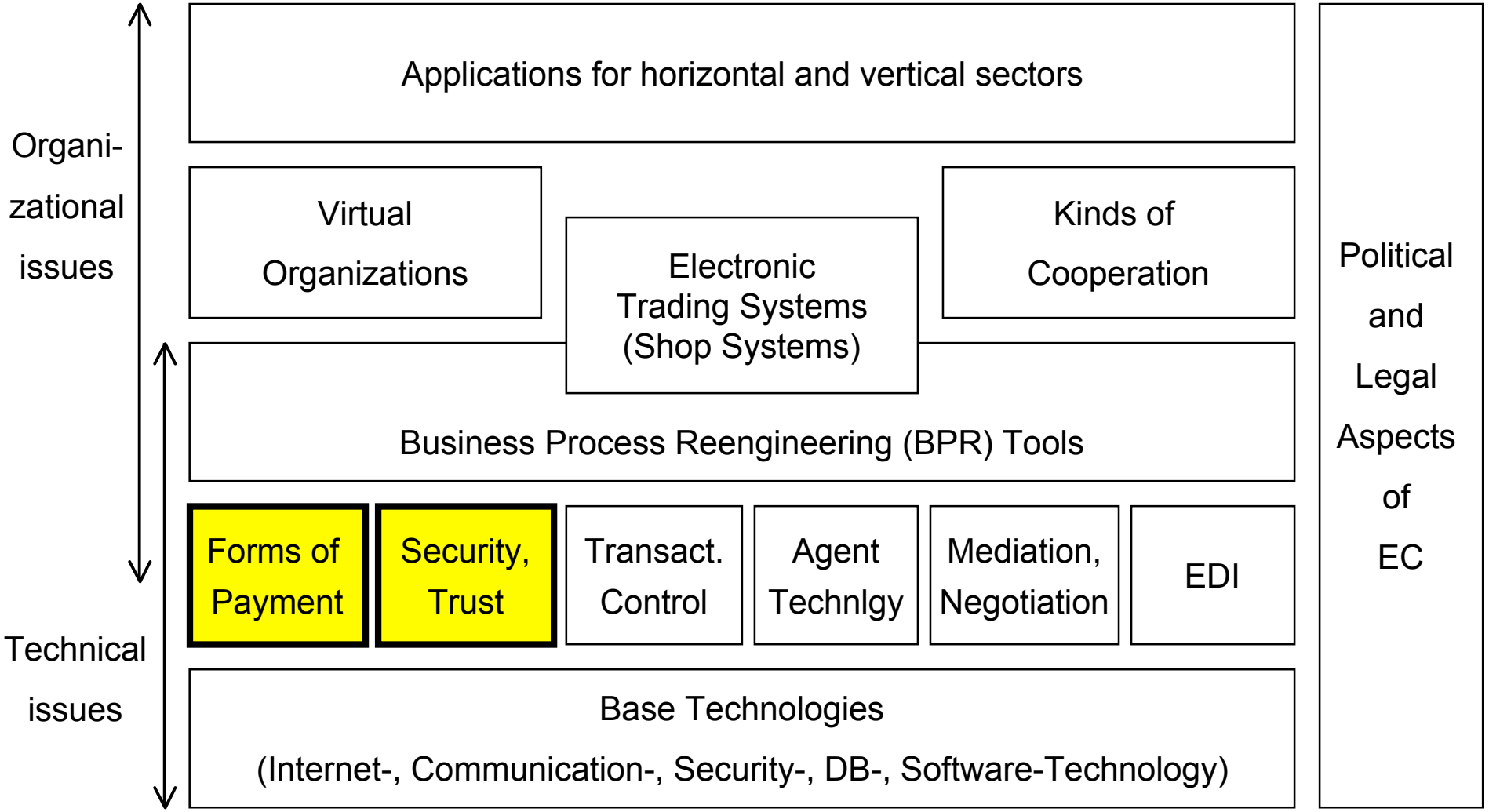
Secure Communication, Security and Trust

Encryption: Standards, Authentication: Digital Signatures, Certification Authorities

Electronic Payment Models, Standards and Systems

4.3 Mobile E-Commerce and Location-Based Services

ECommerce Reference Model

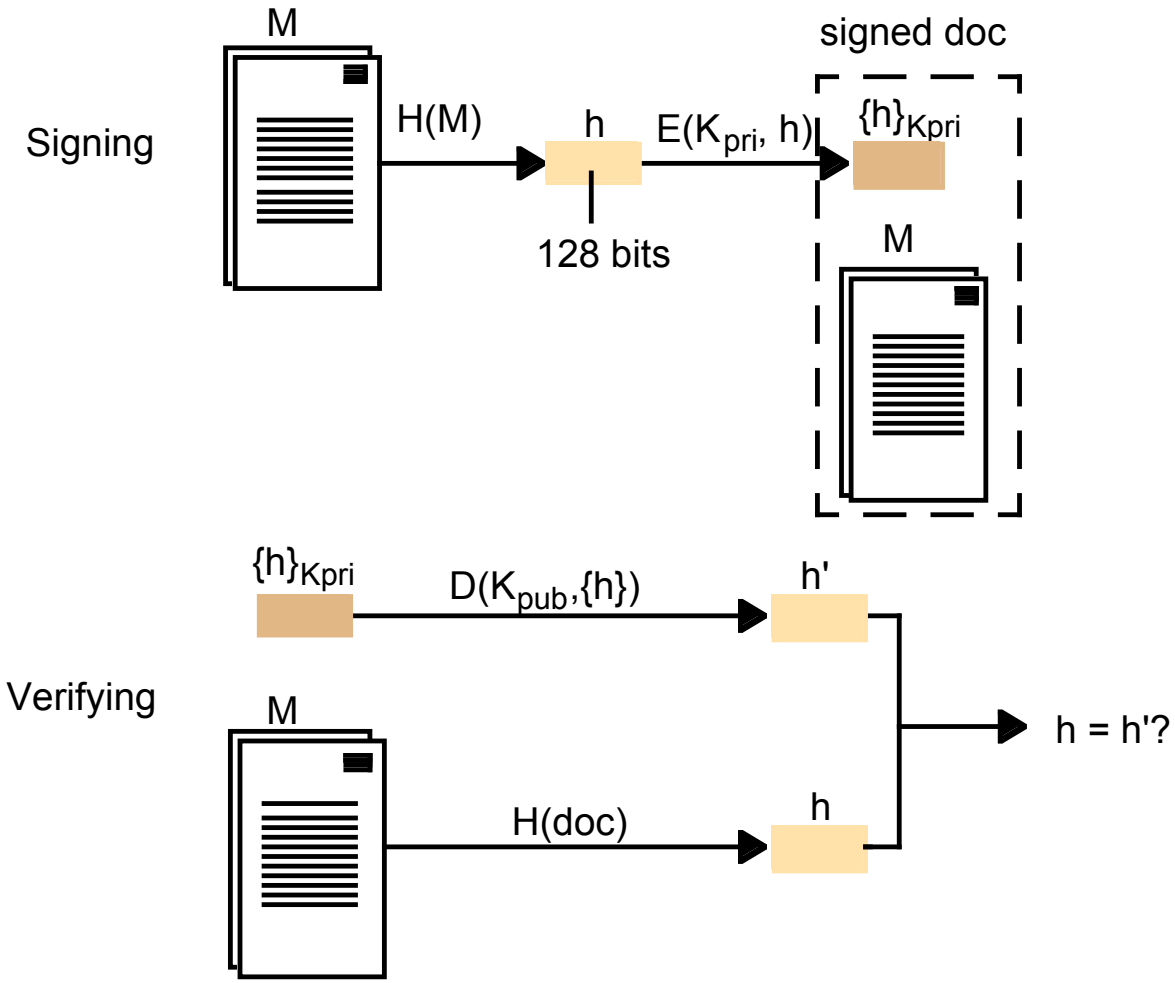


[MeTuLa99]

Authentication: Digital Signatures (1)

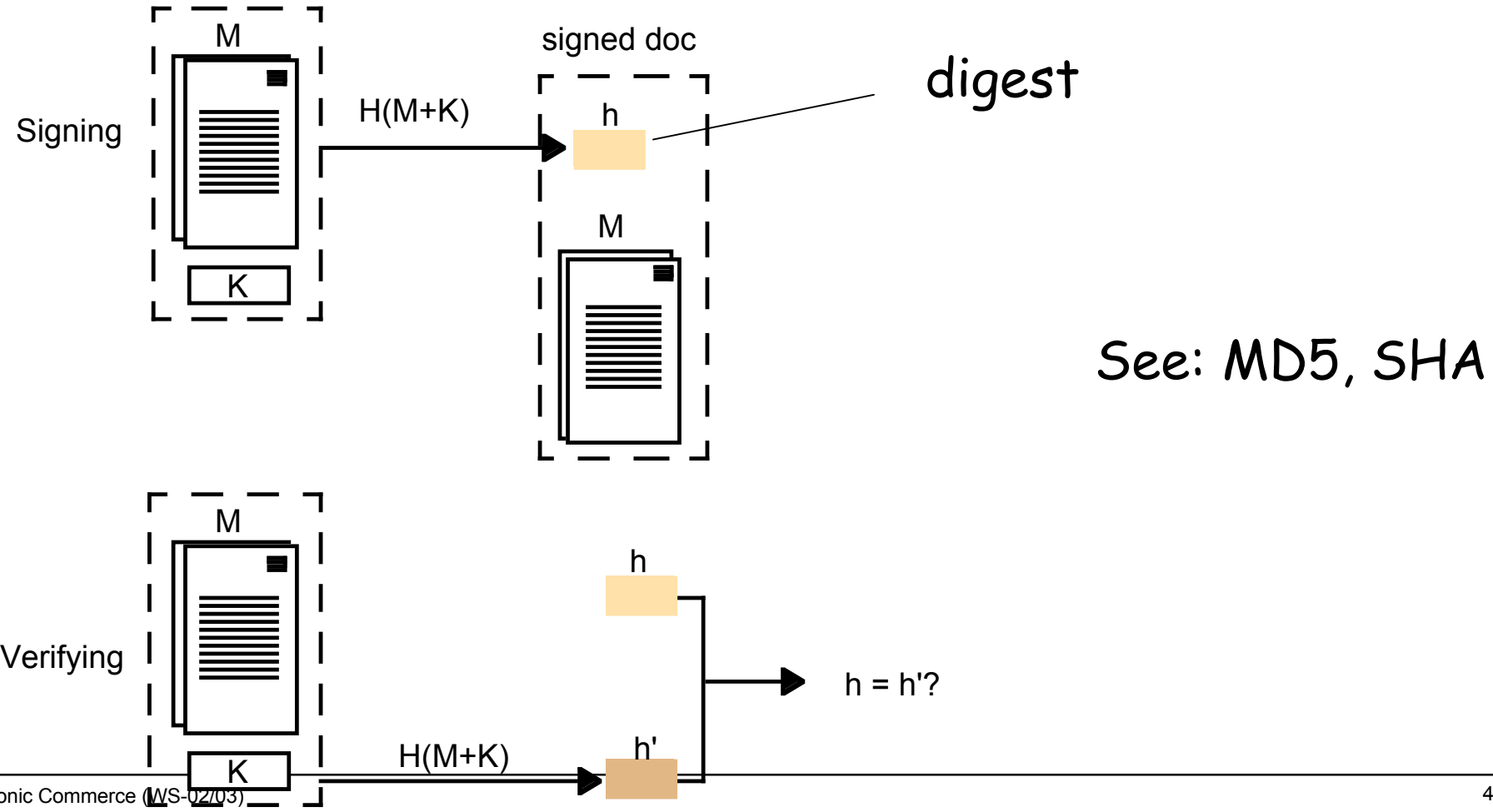
A **digital signature** is applied to a digital document. It states that the document (as an entirety) has been signed by the signer. Others can verify this.

Digital Signatures with Public Keys



Digital Signatures with Secret Keys

MACs: Message Authentication Codes



Performance of encryption and secure digest algorithms

	Key size/hash size (bits)	*Extrapolated speed (kbytes/sec.)*	*PRB optimized (kbytes/s)*
TEA	128	700	-
DES	56	350	7746
Triple-DES	112	120	2842
IDEA	128	700	4469
RSA	512	7	-
RSA	2048	1	-
MD5	128	1740	62425
SHA	160	750	25162

Problem: How to distribute keys?

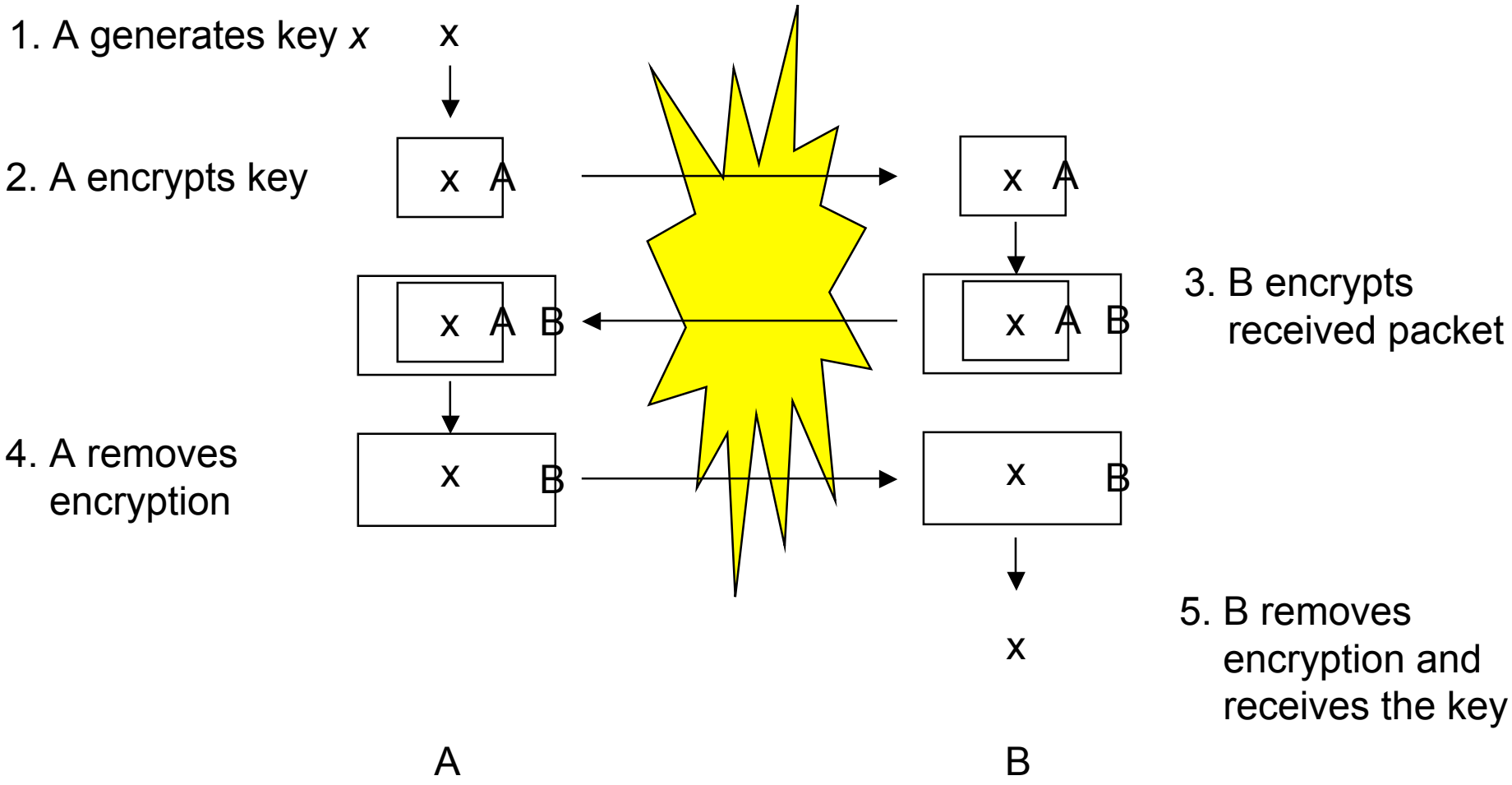
Key distribution by non-networked means is impractical for distributed object systems

Key distribution is a problem for both secret and public keys

- Secret keys: Obvious
- Public keys: How do we know the principal that gives us a public key is who we assume the principal is?

Use trusted key distribution service and secure key distribution protocol!

Diffie-Hellman Key Exchange



Note: A and B do not exchange the key in plain, they do not share their encryptions.

This requires that encryption / decryptions operations may be reordered.

Needham/Schroeder Protocol

Provides a secure way for pairs of components to obtain keys to be used during communication

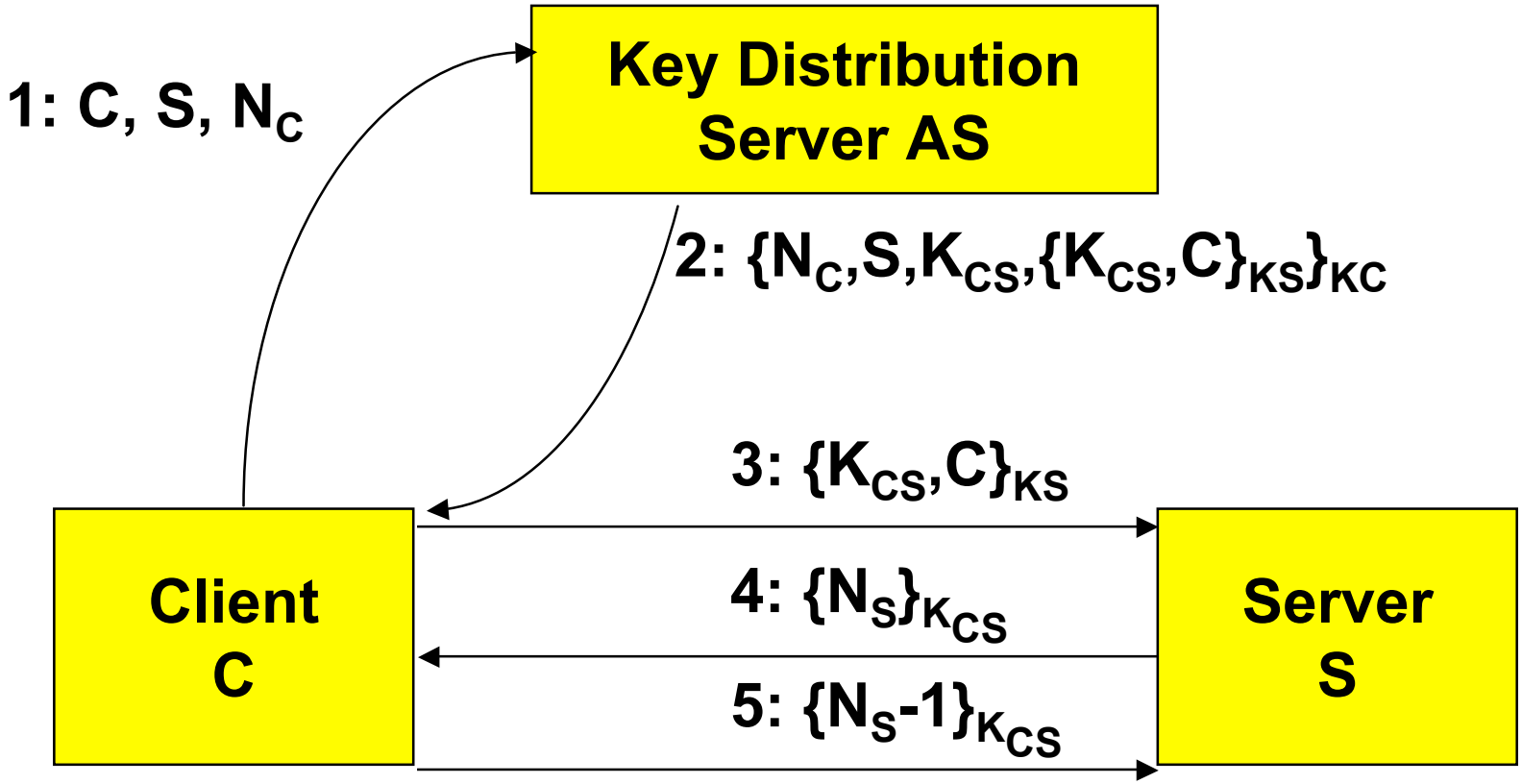
Based on an authentication server:

- maintains a name and a secret key for each component
- can generate keys for peer-to-peer communications

Secret keys are used for communication with authentication server

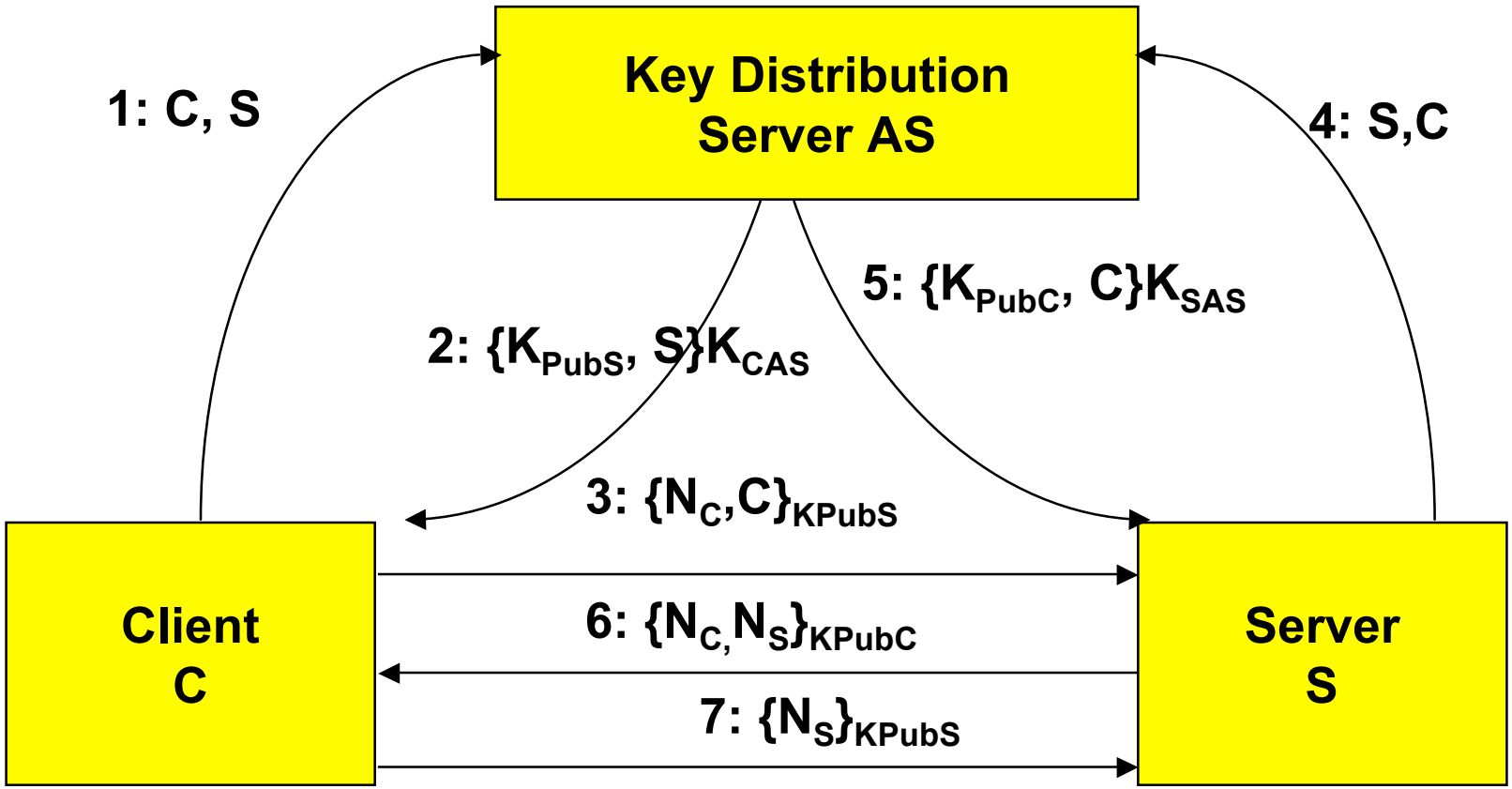
Needham/Schroeder Protocol

For Secret Keys:



Needham/Schroeder Protocol

For Public Keys:



Secure Socket Layer (SSL)

Secure Transport between Browser and Web-Server

Also used for object-oriented middleware

Based on RSA public key technology

Client generates secret session key

Client uses public key of server to encrypt session key and transmit it to the server

Session key is used to encrypt any communication between client and server

Authentication: Blind Signature (1)

Blind signatures are a way of signing electronic data that can be **authenticated without revealing** some **important aspect(s) of the information owner / information creator.**

Two Roles:

Information owner / information creator is one role.
Signer / authenticator is the other role.

Examples:

- Electronic voting: the identity of the person who voted (owner).
- Digital cash: the identity of the person who creates cash units (creator).

Blind signature properties:

- A blind signature is secure if it can be proved that the identity of the owner is never revealed. The unconditional intraceability of the owner must be guaranteed even in the case of collusion. This will ensure that the owner retains his/her anonymity. This is known as the *blindness property*.
- For a blind signature to be secure it must also be proven that the blind signature cannot be forged. [Marte03]

General Cash Properties

Properties of Cash:

- Validity:
  - valid cash units are authenticated by an authority (e.g., the ECB)
  - validity can be verified (to a variable degree, using tools) for any cash unit
- Anonymity and intraceability – except for when used in a crime, e.g. in case of ransom money, money laundry
  - process intraceability: A cash unit does not reveal the payment processes it has been used in
  - anonymity of the user: It does not reveal the spender's / receiver's identity.
- Transaction:
  - No / low transaction costs
  - Immediate transaction processing

These properties shall be provided for digital cash, too.

DigiCash Application of Blind Signatures (1)

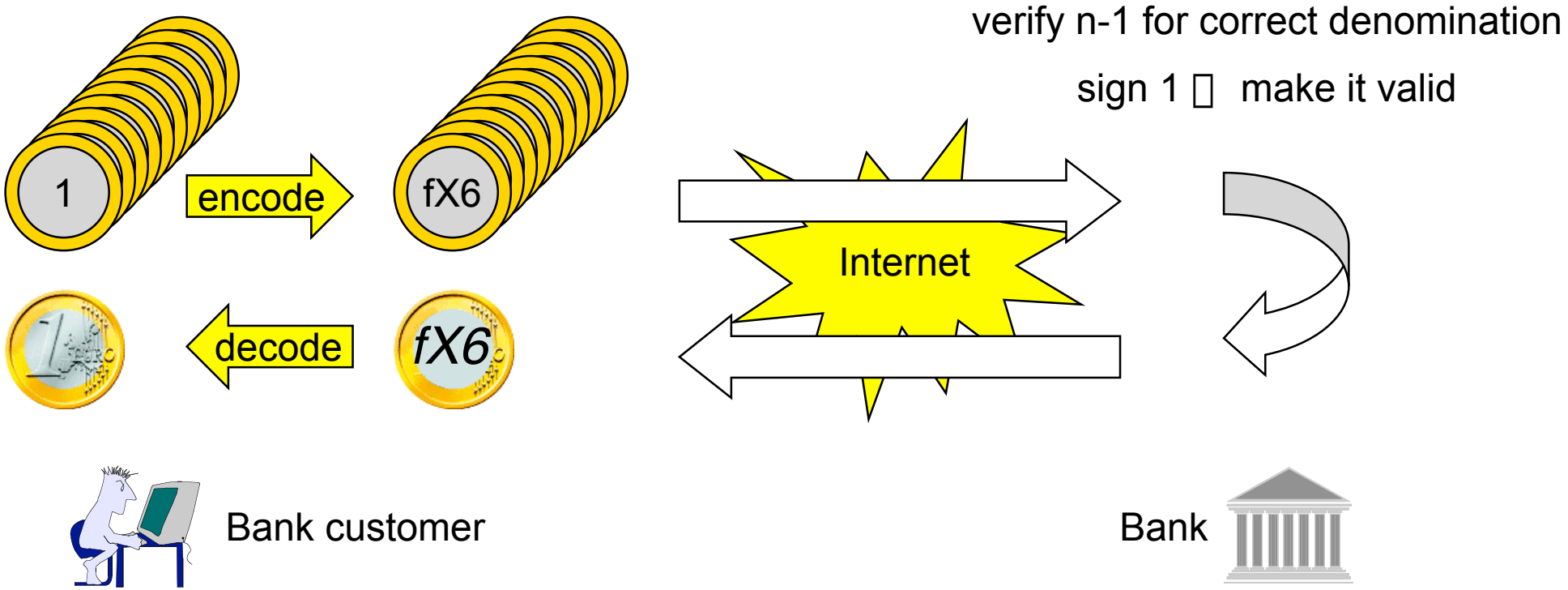
Application of blind signatures in DigiCash (ECash):

Blinding process example:

- The bank client (*information creator role*) wants to have 1 € as digital cash.
- He creates n (10.000.000) digital cash units of the value 1 € with random serial numbers. He encodes them and sends them to the bank. The bank (*authenticator role*) picks n-1 (9.999.999) at random, verifies the denomination and deletes them.
- One cash unit remains (Note: the bank does not know its serial number).
- Note: Checking the denomination reveals the serial number. It requires a decryption step by the user, thus the user knows which cash units are being verified.
- The probability is very low that the remaining cash unit is not a 1 €, but a 1.000.000.000 € cash unit (if the client tried to commit fraud).
- The bank signs this cash unit, and thus validates it to make it a *digital coin*. The coin is returned to the user who decodes it. The user has 1 € (very high probability) or 1.000.000.000 € (very low probability).

See figure on next slide.

DigiCash Application of Blind Signatures (2)



Authentication: Fair Blind Signature

Problem: The **intraceability** of anonymous electronic cash has problems: For example, criminals could obtain a ransom for a kidnapping or launder money without yielding a trace of identity.

Solution: **Unblinding the blind signature when needed**. Blind signatures that can reveal the identity of the holder of the signature are known as **fair blind signatures.**

Link-and-Recovery Fair Blind Signatures (obtain information about who spent the money)

- Involves three roles: cash user, signer (bank) and a third trusted entity (judge or certification authority).
- When needed, the cash signing protocol enables the trusted entity to reveal the sender of electronic cash (details omitted, see literature).

Trustee-Based Fair Blind Signatures (obtain information about user spending habits)

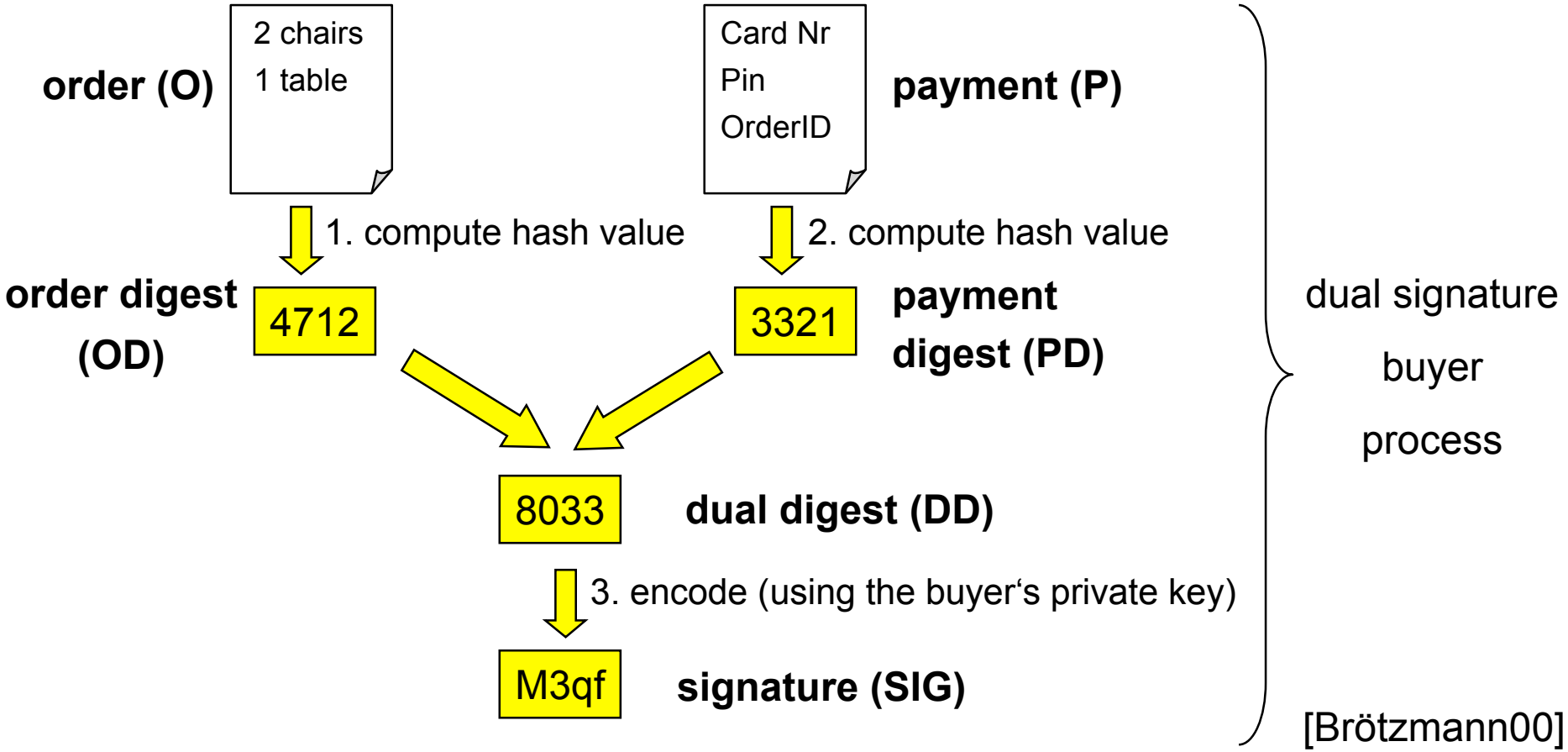
- The user provides *trustees* with information that allow the trustees to recognise the electronic notes of the user. Each of the trustees receives a part of this information that makes the electronic spending of the user traceable.
- When needed, the spending pattern of the user can be revealed by putting together the trustees' individual information. Problem: If trustees collude (get together), they can build up a user's spending profile.

[Marte03]

Authentication: Dual Signature (1)

Definition

A **dual signature** is used to verify whether data constitute different parts of a single logical unit. Example: Using a dual signature, one can verify whether ordering information (items, quantity) and payment information (card and pin number) belong to the same order.

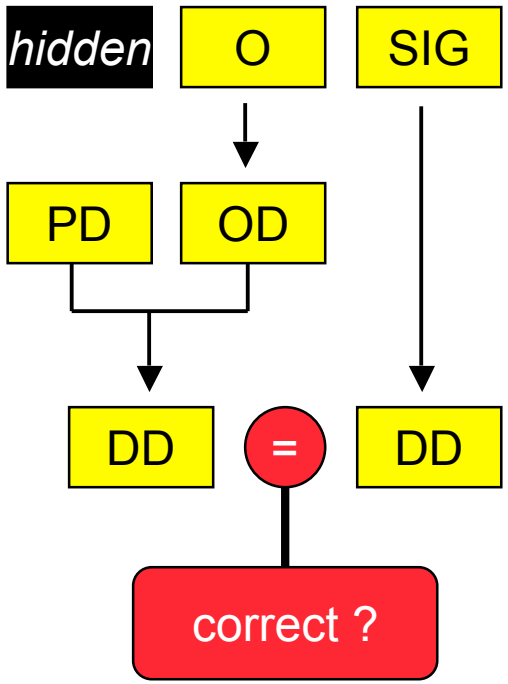


[Brötzmann00]

Authentication: Dual Signature (2)

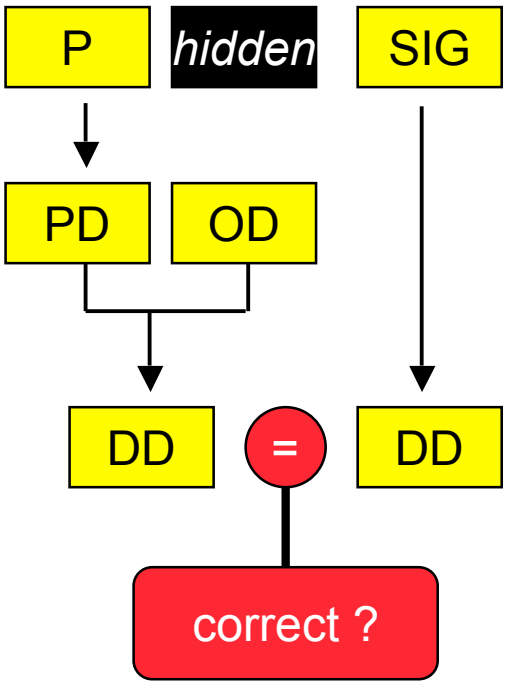
Seller Validation:

does not know payment information (P)



Bank Validation:

does not know order information (O)



[Brötzmann00]

Authentication: Certificates

Definition

A **certificate** is a verifiable statement made by a legal person / institution about circumstances (ex: driving license, master degree).

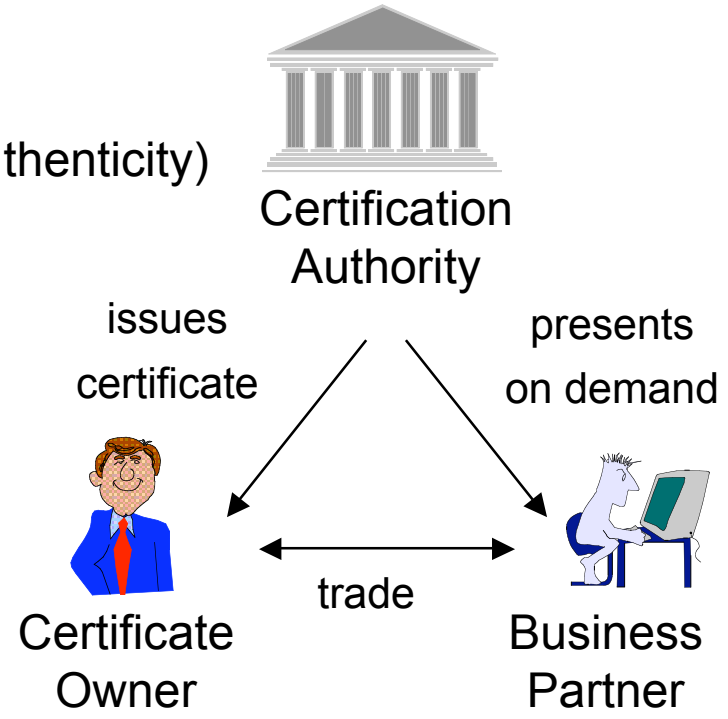
Digital Certificates are used in ECommerce for proving the affiliation of a *public key* to a *legal person*. They comply with the x.509 standard.

A certificate is used by legal persons in three roles:

- Certificate issuer (certification authority, CA)
- Certificate owner (legal person to be described)
- Certificate users (others verifying the owner‘s authenticity)

Certificates comprise the following information:

- Owner‘s name and public key
- Public hash function (algorithm) name
- Certificate serial number
- Start date and expiration date of certificate
- Certificate authority‘s name



Authentication: Certification Authority

Definition

Certification Authorities (CAs) ensure that a public key is affiliated to a legal person. CAs have different certification classes. Every class comprises costs, required documents for certification and liability of the CA.

Example: VeriSign (www.verisign.com) certification classes.

Class	Client (buyer) or server (seller)	Required information	Costs p.a.	CA Liabilty
1	Client	name, email	-	100 USD
2	Client	name, email, postal address, date of birth, SSN, employer	19,95 USD	5.000 USD
3	Client	...	290 USD first year, 75 USD following yrs	100.000 USD
4	Server	...	290 USD first year, 75 USD following yrs	100.000 USD

[Merz99]

Authentication: Public Key Infrastructure

A **Public Key Infrastructure** (PKI) is a system of Certificate Authorities (and other registration authorities) that verify and authenticate the validity of each party involved in an Internet transaction based on digital certificates. A PKI is also called a *trust hierarchy.* [WOp00].

PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI. Reliable PKIs are a necessary requirement for some forms of "pure" electronic commerce.

Two steps are necessary to build a successful PKI:

- ❏ The majority of legal persons (single persons, companies) register at a CA.
- ❏ The CAs must be certified.

Question

- ❏ Which organization certifies the CAs?

Answer

- ❏ CAs certify each other via cross-certification.

Electronic Payment (1)

Classification of payments by transaction volume [Merz99]:

- Zeropayments (0 €)
- Nanopayments (0.001 – 0.1 €)
- Micropayments (0.1 - 5 €)
- Medium Payments (5 – 1.000 €)
- Macropayments (> 1.000 €)

Different transaction volumes require different forms of payment. Example: Credit cards are not suitable for nano– and micropayments as transactions costs are higher than transaction volume.

Electronic Payment (2)

Mind the buyer‘s payment habits. Dominant forms of payment:

USA:

- Credit-cards
- Cheques

Germany:

- Credit-cards
- Direct debit (Lastschriftverfahren)
- Cash-on-delivery (Nachnahmesendung)

Asia

- Credit-cards

Implication: Global businesses must localize their forms of payment.

Payment Systems: Requirements

General Issues

- Security
- Scalability
- Reliability
- Usability

Electronic-Commerce related

- Must allow micropayments (low transaction costs)
- Payment channels (B2C, C2C, ...)
- Anonymity
- Immediate transactions (especially for soft goods, e.g. software licenses)

Note: Different delivery and payment models apply for hard good stores and soft good stores.

[Brötzmann00]

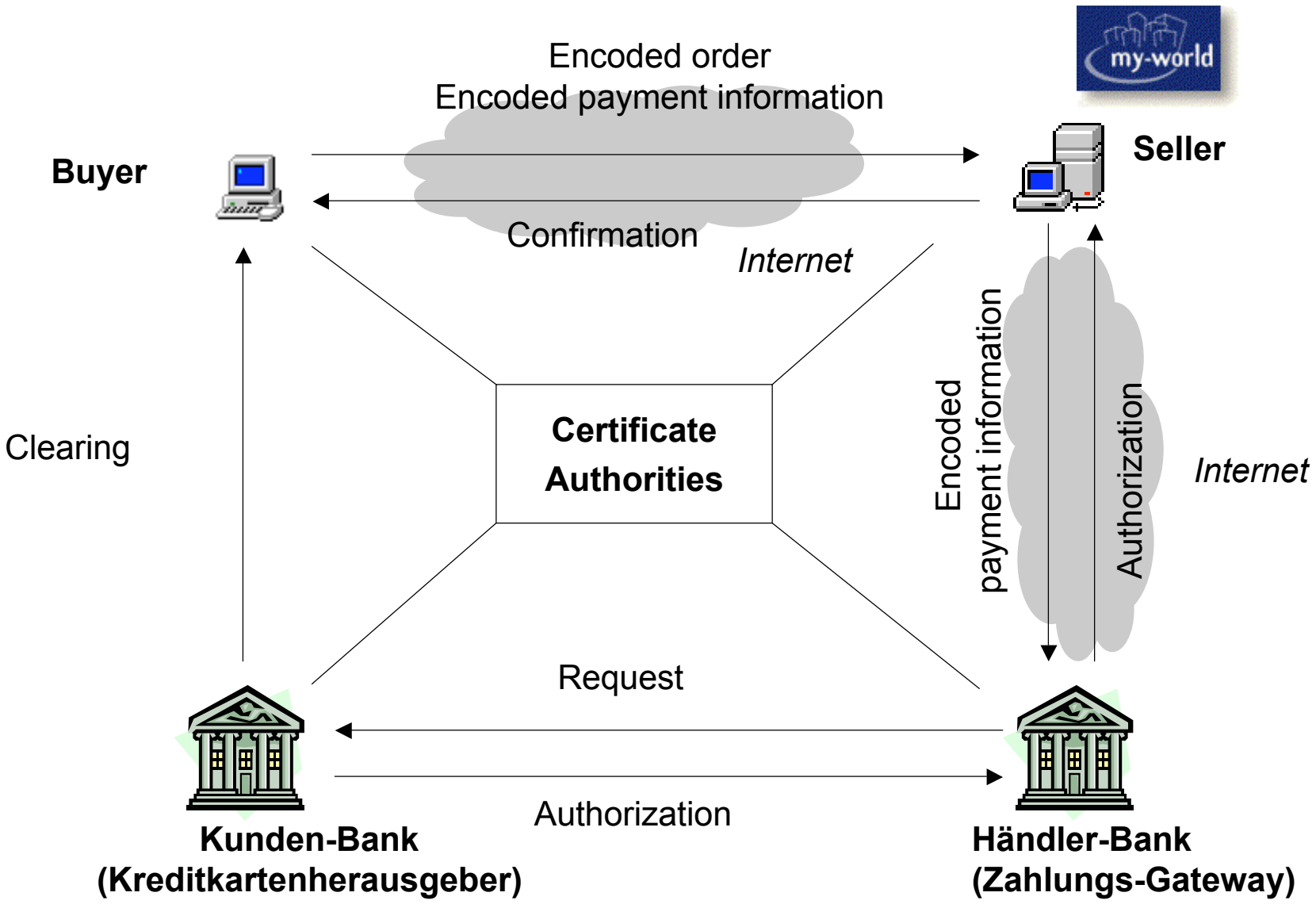
Payments: Macropayments

Transactions volume: > 1.000 €

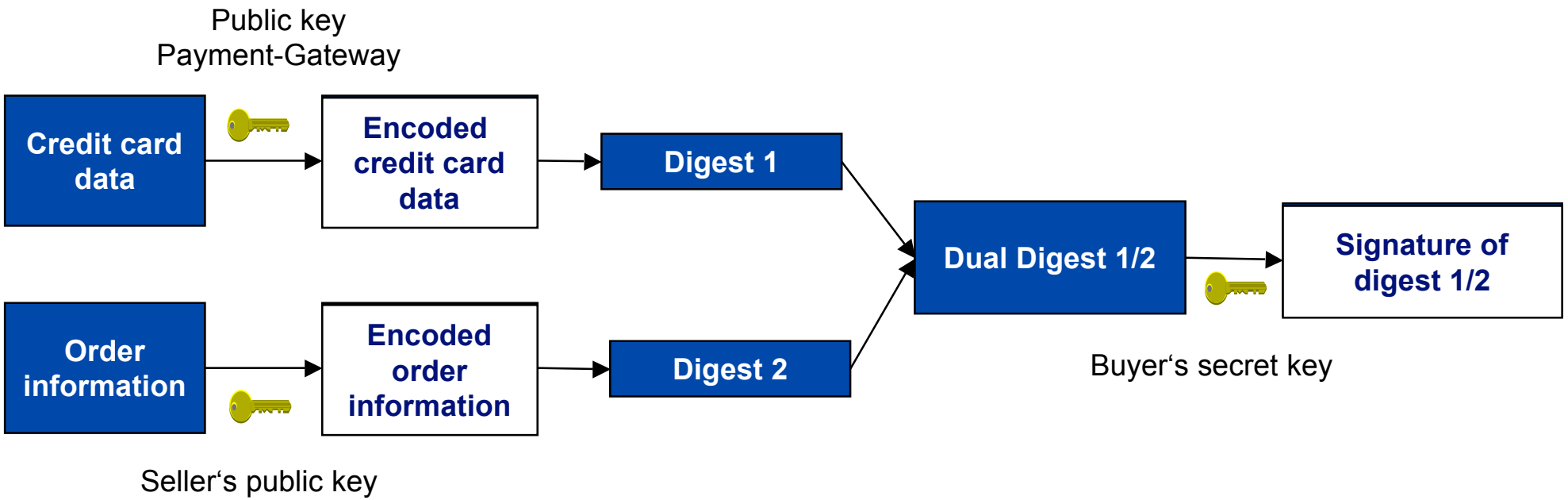
Established business relationship between sellers and buyers. Business relationship is fixed by contracts. Therefore, payments are not as important as continuous business relationship.

Payments are not internet-based No internet based payment infrastructure.

Medium Payments: Secure Electronic Transactions: SET



Dual Signature and Encoding



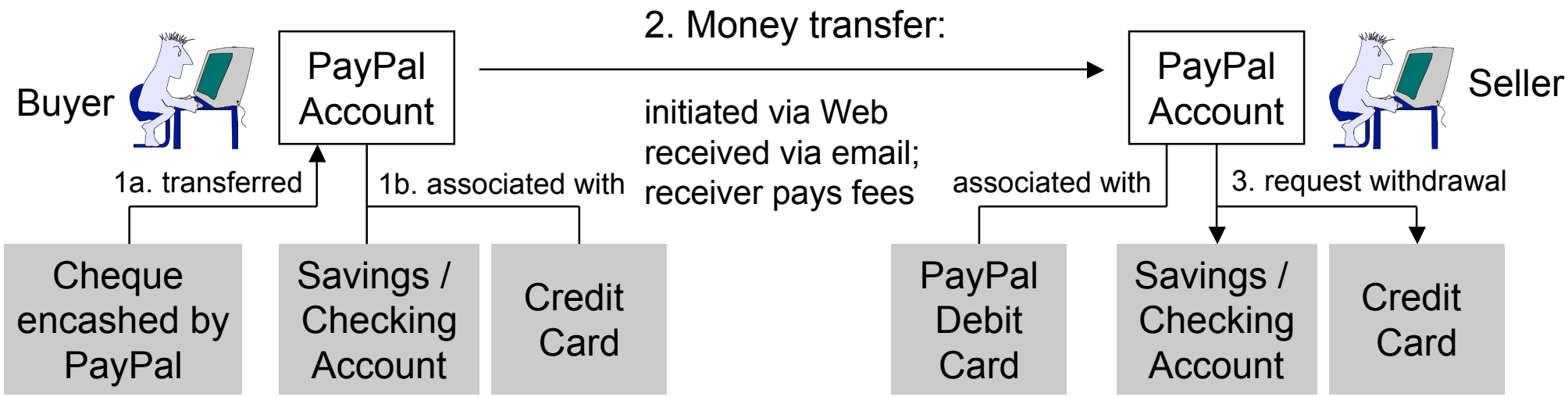
Medium Payments: PayPal

PayPal was introduced as a C2C email-based money transfer system, then extended to handle B2C financial transactions. Mainly used in US for online auction-related payments.

Buyer initiates a money transfer on PayPal's WebSite. PayPal debits his associated bank account / credit card, sends receiver an email notification and deposits on receiver's PayPal account.

Receiver always pays fees: 0,30 U$ + 2.2 % of payment amount.

Receiver can withdraw money directly via PayPal debit card (only B2C merchant, not in C2C model) or request money transfer to bank account / credit card.



Payments: Micropayments (1)

Transactions volume: 0.1 – 5 €

- Form of payment in traditional commerce: cash.
- Idea: Map **cash** to electronic commerce digital cash.
- Currently, there is no successful and widely adapted digital cash model.

Success factors for digital cash are:

- Offline usability (No bank needed / wanted for verification at every transaction)
- Anonymity (money spender stays anonymous, unless trying to double-spend digital cash)

Payments: Micropayments (2)

Current digital cash models:

Billing: Reduce costs by consolidating transaction volumes

- Phone + Code: Call a number. After a period of time a code is disclosed. Important: What percentage of the fee is taken by the telecommunication service provider (Germany: 50% by Deutsche Telekom!)
- Token-based and account-based billing systems (see following slides)

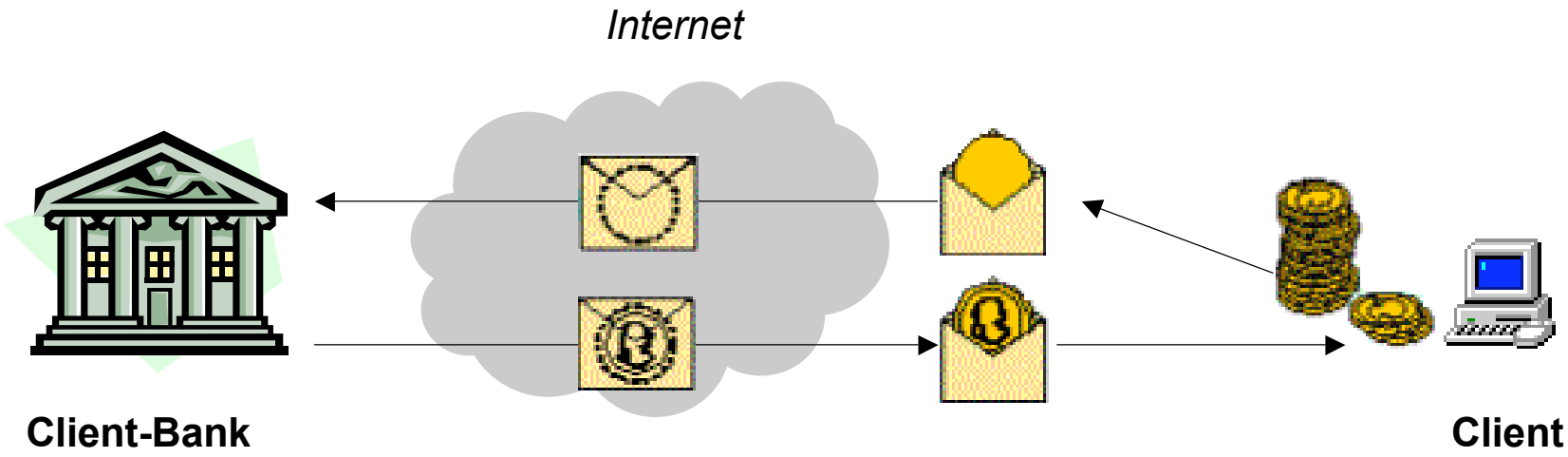
Money cards:

- White Cards (anonymous users), e.g., Mondex

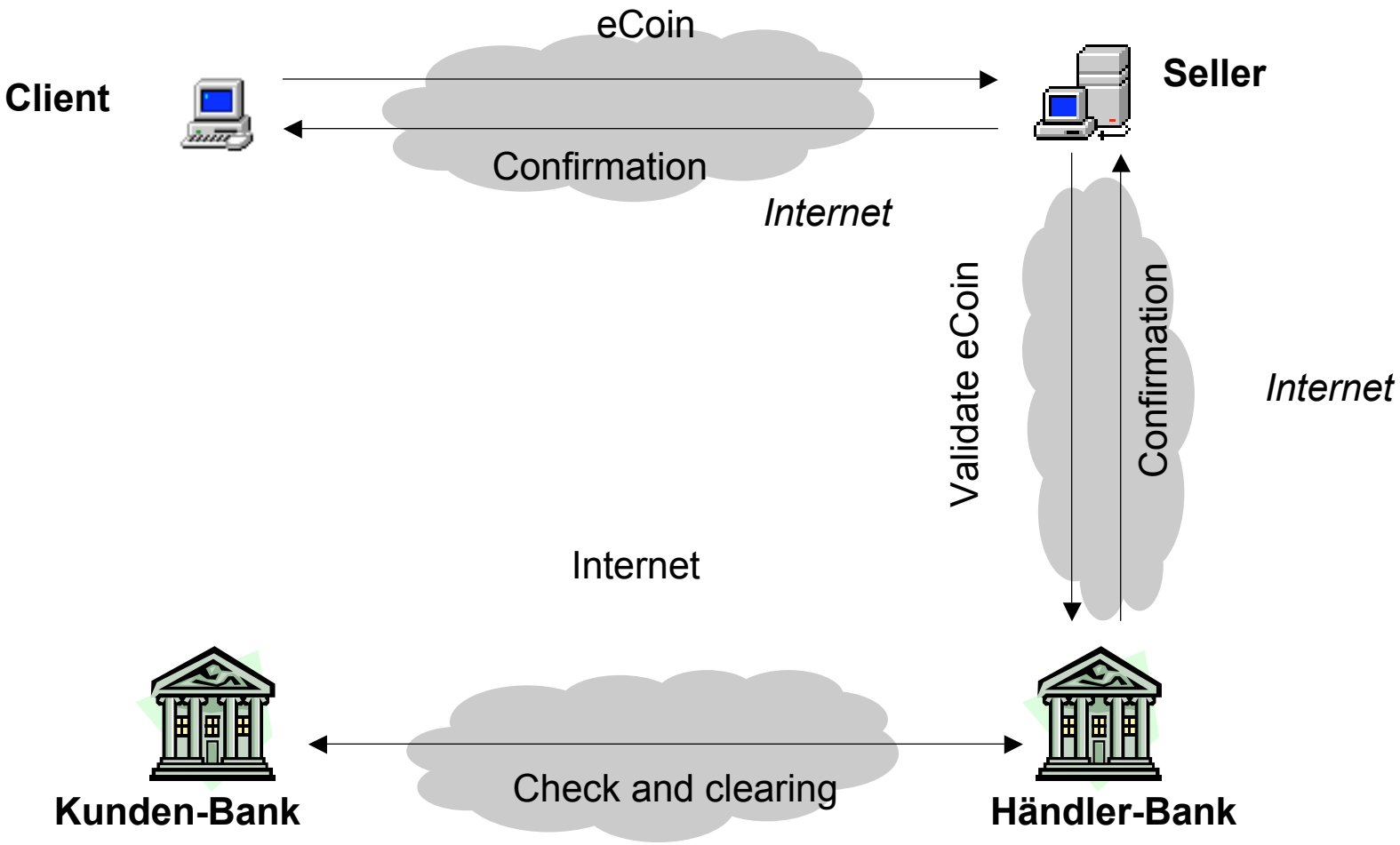
Digital cash (buyer is anonymous, double spending problem)

- eCash

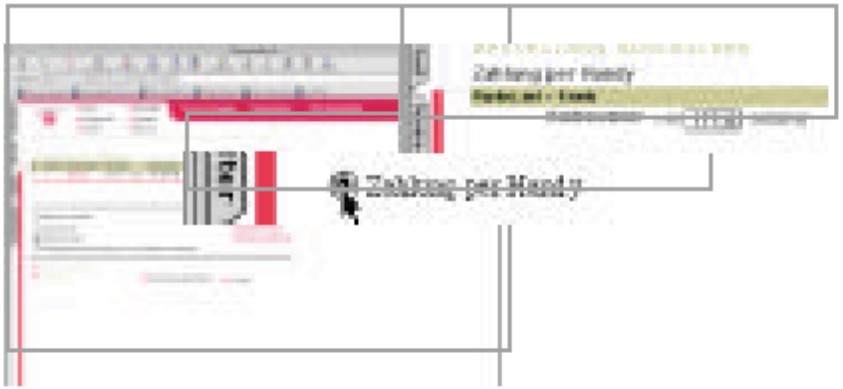
Ecash with *blind signature*



ecash


eCoin
Client
Seller
Confirmation
Internet
Validate eCoin
Confirmation
Internet
Internet
Kunden-Bank
Check and clearing
Händler-Bank

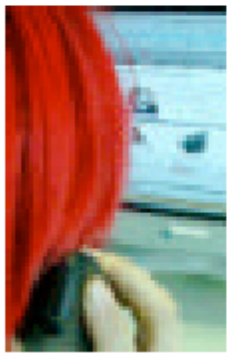
PayBox.net, liberECO.de and others



1 Der Kunde füllt den Warenkorb im Internet, wählt „Paybox - Zahlen per Handy“ und gibt seine Mobiltelefonnummer oder einen Alias an

2 Paybox verbindet die Transaktions-partner und stellt die Verbindung zum Han-dy des Kunden her

3 Der Kunde autorisiert den Betrag und die Zahlung an den Internet-Shop...



4 ...durch Eingabe der Paybox-PIN auf seinem Handy

5 Der Ausgleich der Rechnung erfolgt per Lastschrift-einzugs-verfahren

Quelle: paybox.net

Example Application: Pay the Taxi Driver

1 Der Fahrgast wählt ein als Paybox-Akzeptanzstelle gekennzeichnetes Taxi

2 Der Taxifahrer initiiert den Zahlungsvorgang mit einem gebührenfreien Anruf bei Paybox

3 Paybox verbindet die Transaktions-partner und stellt die Verbindung zum Handy des Fahrgastes her

4 Der Kunde autorisiert die Zahlung durch Eingabe der Paybox-PIN auf seinem Handy

5 Der Ausgleich der Rechnung erfolgt per Lastschrifteinzugs-verfahren

Quelle: paybox.net

New Developments: e.g. Web-Coupons

Web-Coupons are not linked to convertible currencies (U$, €) issued by countries but are an **artificial currency** created by company consortia to increase customer loyalty.

Earn coupons:

- Buy specific goods or services
- Provide information about yourself
- Provide information / services to others

Spend coupons:

- Discounts on sales and services of affiliates
- Privileged access to goods and services

Non-Internet Examples:

- Lufthansa Miles & More (many global partners)
- American Express Bonus "Miles" (many global partners)
- Payback Points (Germany only)

Internet-Only Examples:

- Former Web-Miles (dead)

Summary: Web-Coupons did not succeed (yet).

Payments: Summary

Summary

- Currently, no models for nanopayments exist.
- No successful model for micropayments, except for money cards.
- No standard for micropayments, standard models starting at medium payments only.
- Medium payments: Best supported model (online credit-card payments, email-based money transfer)
- Most payment systems vendors are gone bankrupt.
- Micropayment models can also be used for medium payments.