eSETTLEMENT

ANDREAS MEIER & LUIS TERÁN
INFORMATION SYSTEMS RESEARCH GROUP
UNIVERSITY OF FRIBOURG
Learning Targets

- Which ePayment methods do exist?
- What are the pros and cons of offline and online distribution channels?
- How does the supply chain can be planned and managed?
- What is necessary to fulfill data protection laws?
- How does the copyright of digital goods can be protected?
- What is necessary for the security management?
eSettlement consists of the following functions:

- Confirmation of orders
- Electronic payment (ePayment) and
- Distribution of services and/or products (offline or online)

It is important that all sub-processes guarantee data protection and data security
ePayment refers to the completion of payment processes via Internet:

- Credit Card
- Paypal
- EC/Maestro/Yellowpay
- Geldkarte
- Paysafecard
- eCash
- Millicent
- Firstgate Click & Buy or
- Allopass
Classification based on the amount of money:

- **Picopayments** (amounts from a fraction of a cent up to 1 Euro)
- **Micropayments** (payments between 1 and 30 Euros)
- **Macropayments** (amounts from 30 Euros up to several thousand Euros)
Confidentiality and anonymity of the transaction concept:

- Non-anonymous transactions
- Anonymous transactions¹
Confidentiality and anonymity of the transaction concept:

- Non-anonymous transactions
- Anonymous transactions

1. The buyer gets a digitally signed note from the bank.
2. The buyer spends his note to a seller.
3. The seller deposits his note in his bank account.

Classification based on time of payment:

- **Pre-paid:** money transfer before delivery. Hardware (GeldKarte\(^1\)) and software (paysefecard\(^2\)) solutions.
- **Pay now:** money should be transfer during the order (paypal\(^3\))
- **Pay later:** money is transfer after delivery. (sum of all pico-payments/month, etc) (click&buy\(^4\))
Classification based on time of payment:

• **Pre-paid:** money transfer before delivery. Hardware (GeldKarte\(^1\)) and software (paysafecard\(^2\)) solutions.

• **Pay now:** money should be transfer during the order (paypal\(^3\))

• **Pay later:** money is transfer after delivery. (sum of all pico-payments /month, etc) (click&buy\(^4\))

---

1 www.GeldKarte.de  
2 www.paysafecard.com  
3 www.paypal.com  
4 www.clickandbuy.de
Classification based on technical solution concept:

1. Initiation
2. Authorization
3. Clearing
4. Confirmation of Transfer
5. Delivery

mPayment by Karlsson and Taga
ePayment with Credit Cards

• Credit cards have already been in use for decades in offline trading
• Credit cards are available and accepted worldwide
• The company pays the fee!
• Online payment simply needs entering the name of the card holder and the credit card number into a form
• However, credit cards should only be used by secure transaction systems
The PayPal System

• it belongs now to eBay
• it is based on credit cards
• private persons can exchange money in different currencies
• it can also be used between private persons and dealers
• most auctions demand a PayPal account
• simple and trustworthy
Payment between Two Individuals

Credit cards are not anonymous. When a product is purchased, the owner of the credit card and its number become known to both the seller and the banks involved in the transaction, which again represents a security risk.

Credit cards are not suitable for payments between private individuals. A special contract must be concluded with the credit card company and bank to enable a person to receive money through a credit card.

Credit cards are expensive for the seller. Credit card institutions and banks require the seller to pay relatively high basic charges as well as a percentage of sales to them.

7.2.2 PayPal

PayPal was created in 1998 as an independent company and was taken over in 2002 by the auction house eBay. PayPal is a credit card-oriented payment system. In contrast to the direct use of credit cards described above, it makes payments between two private individuals possible. A US-based company, for a long time PayPal only offered accounts in US dollars, but has recently backed other currencies, such as Euros or British pounds.

In order to be able to use PayPal, it is necessary to register with it. PayPal Registration process employs a simple yet effective means to protect itself against credit card abuse. A new user enters credit card information but cannot use PayPal until his account has been activated. PayPal subsequently debits a small amount (normally $1) from the credit card entered. The description of this deduction on the credit card statement contains a number. The user then sends this number to PayPal in order to activate the account. This method makes it difficult to register as to least number with PayPal, since they normally have no access to the credit card account. If the user has successfully registered himself with PayPal, he can then carry out a transaction to another PayPal member (see Fig. 7.2).
The Geldkarte can also be used for online trading
A card reader is necessary
The Geldkarte must be loaded with cash periodically
The system is used for different services (cafeteria, parking fees, cinema tickets, etc.)
7.3 Asset-Based Procedures

As well as one-off payments, incremental payments can also be carried out with the Geldkarte. Just like a phone card, a small amount is deducted from it at a certain time. Thus time-dependent online payment services can be realized.

7.3.3 Conclusion

The asset-based procedures presented above were developed for the offline payment of small amounts (micropayment). They offer the greatest advantages within this range. For the buyer, the need to get hold of hard cash is eliminated, the seller no longer has to count coins, and regular deliveries to the bank are discontinued. However, CASH and the Geldkarte are only conditionally suitable for online business since a card reader is required. Few private households have these.

An important advantage of cash payment is the anonymity of the buyer. Are CASH and Geldkarte anonymous? The providers of CASH and the Geldkarte emphasize that anonymity remains guaranteed with the solutions offered. However, it is easy to store the receiver’s details that are required when the card is issued. It is also possible to log the purchases made with the card.

With asset-based procedures, the security of the assets is of the greatest importance to the providers. If an attacker succeeds in increasing his assets on the card away from a load terminal, he can transact any purchase. Providers have resolved the issue of asset security by employing smartcards.

VISACash by VISA is an alternative and internationally available asset-based procedure which is similar to the solutions presented.

Secure Electronic Transaction (SET) was a secure protocol proposed by credit card and technical companies. It was based on the Public Key Infrastructure (PKI). SET used a dual digital signature procedure (payment information, order information).
SET Dual Signature Example

1. PurchaseInitRequest
2. PurchaseInitResponse
3. PurchaseRequest $K_{\text{public, merchant}}$ (order info.) $K_{\text{public, payment gateway}}$ (payment info.)
4. AuthRequest $K_{\text{public, payment gateway}}$ (payment info.)
5. AuthResponse
6. PurchaseResponse
eCash was based on electronic coins (cyber cash)

eCash was using digital signatures for security reasons

The electronic coins could be used for picopayments

After a test phase with international banks, eCash was rejected (lack of acceptance by the users)
Many ePayment solutions were introduced in the mid-1990s. Although they were conceptually interesting, they did not gain market acceptance. Some of these ideas are described briefly below.

### 7.4.1 eCash

eCash was a development of the DigiCash Company. It was a coin-based system which combined the advantages of cash with those of electronic payment transactions. With eCash, there was no difference between buyer and dealer; each user possessed the same electronic purse. "Electronic coins" were deposited into this purse. When the user made a payment, coins from one purse were transferred into another purse.

The transfer of electronic coins attracted the same difficulties relating to copy protection as encountered in asset-based procedures. However, a smartcard was not used with eCash; instead, eCash used a procedure based on digital signatures.

User generated his own coins. This was referred to as a blind signature in order to emphasize the anonymity of the procedure. The user of eCash generated his own coins and had them signed by his bank (see Fig. 7.5, steps 1 and 2). Provided the bank accepted the coins, it withdrew the appropriate amount from the user's account. The coins had a value (a second power of 0.01) and a serial number. The user's electronic purse randomly generated a unique serial number. This was encoded and sent along with the payment information to the bank. The bank then examined the coin transaction, and if it was legitimate, a second signature was generated by the bank and forwarded back to the user. The user then verified the second signature and completed the payment.
### Comparison of ePayment Systems

<table>
<thead>
<tr>
<th></th>
<th>PayPal</th>
<th>Geldkarte</th>
<th>Paysafecard</th>
<th>Google Checkout</th>
<th>Click &amp; Buy</th>
<th>Allopass</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of Users/Dealers</strong></td>
<td>&gt; 140 million users</td>
<td>&gt; 60 million users</td>
<td>&gt; 1000 dealers</td>
<td>&gt; 500 dealers</td>
<td>&gt; 7000 dealers</td>
<td>no indication</td>
</tr>
<tr>
<td><strong>Fee for the Seller</strong></td>
<td>1.9% - 3.9% of turnover + 0.35 Euro</td>
<td>0.3% of turnover</td>
<td>5.5% - 19% of turnover</td>
<td>1.5% of turnover</td>
<td>49 € registr. + 5 € / month + 7% - 35% of turnover</td>
<td>up to 30% of turnover</td>
</tr>
<tr>
<td><strong>Territory</strong></td>
<td>worldwide</td>
<td>Germany</td>
<td>Europe</td>
<td>primarily USA and UK</td>
<td>More than 25 Countries</td>
<td>Western Europe</td>
</tr>
<tr>
<td><strong>Classification Amount of Money</strong></td>
<td>Macropayment</td>
<td>Micropayment</td>
<td>Micropayment</td>
<td>Macropayment</td>
<td>Micropayment/Picopayment</td>
<td>Micropayment/Picopayment</td>
</tr>
<tr>
<td><strong>Classification Point of Time</strong></td>
<td>Pay-Later</td>
<td>Pre-Paid</td>
<td>Pre-Paid</td>
<td>Pay-Later</td>
<td>Pay-Later</td>
<td>Pay-Later</td>
</tr>
</tbody>
</table>
The distribution of a digital product or a digital service with the use of a communications network (e.g., Internet) is called eDistribution.

- eDistribution supports the ubiquity of services in the digital economy
- The distribution is independent from time and place if the citizen possesses a mobile device (cell phones with Internet access, iPad, palmtop, notebook, ...)
Components of a Distribution System

- Distribution System
  - Distribution Channel
    - Direct Outlet
      - broker
      - subsidiary
      - electronic automation
      - eShop
    - Indirect Outlet
      - wholesale trade
      - retail trade
      - franchising
      - infomediaries
  - Distribution Logistics
    - Warehousing/Storage System
      - warehouses
    - Transport Network
      - roads
      - waterways
    - Service
      - delivery service

Key: digital channels and digital components in bold
Characterization of the Online Distribution

Case a)
Direct Sales Channel

Authority

Citizen

---

Case b)
Indirect Sales Channel

Authority

Intermediary

Citizen

Legend:
Digital Transmission Medium
Online distribution

• Advantages:
  - Purchasing at anytime
  - Direct contact between government and citizen
  - Reduces costs of production, storage and distribution

• Disadvantages:
  - Distribution costs are added to citizen
  - Social impacts
  - Quality loss of digital goods due to compression
  - Duplication and spread of digital products (watermark needed)
  - Digital divide
Characterization of the Offline Distribution

**Legend:**
- Physical Transport

- Temperature requirement
- Location and number
- Spatial demands
- Time stress
- Optimization of the ways
- Delivery or collection
- Time of transfer
Offline distribution

• Advantages:
  - Download time reduced (big data)
  - Quality of digital good can be maintained
  - Better protection for authors rights (copyright)
  - High storage options in future (plasma and nano technology)

• Disadvantages:
  - Defective data parts cannot be fixed by citizens
  - Complicated data storage (self organization)
  - Problems with new formats and updates
  - Time and place dependent
Hybrid Distribution

Key:
- digital channel
- physical transport route

eGov Authority

Intermediary

storage and transport

point of delivery

Citizen

Citizen
The Supply Chain Operations Reference (SCOR) model has two parts:

- the phase PLAN and
- the phases SOURCE (procurement), MAKE (production) and DELIVER (delivery).

Starting from the need of a citizen, different activities must be done to deliver the expected services.

In addition, the whole supply chain has to be planned in advance.
Steps of a Supply Chain

Sub-steps within a supply chain according to the SCOR model (ePassport example)
• **Data protection**: protection of personalized data from unauthorized access and utilization.

• **Data security**: technical or software-based methods to protect data falsification, destruction or loss

• **Protection of privacy of citizens**:
  - Ideological, political or religious views/activities
  - Belonging to ethnical groups or minorities
  - Data about deseases (health record)
  - Criminal records, penalties, etc.
  - Information on a person’s private sphere

Personal data may only be obtained in legal ways and used in good faith.
Protection of personal data

Rights of Citizens

Rights to Information
• Insight into their own data
• Declaration of purpose
• Legal foundation for processing
• Data receipt

Amending Law
• Incorrect information to be corrected
• Operators are responsible for securing and storing

Information and correction according to privacy legislation
• Digital documents or contracts can be copied easily (copy and paste)
• Citizens want to protect their artwork (music, fotos, videos, literature, poems etc.)
• Software developers need to protect their applications
• Producers of digital goods or services try to protect their rights etc.
• A Digital Watermark is used to identify the ownership of a digital product or service
• A watermarking systems supports watermark embedding and watermark extraction
• There exists text watermarking, image watermarking, video or audio watermarking methods
• Robustness is the ability to resist signal processing attacks
Watermark Embedding

a) Original Image

b) Original Watermark

c) Watermarked Image

Security Strategy Needed

• Which citizens have access to which information system?
• How can a web user be identified? (name or user identification)
• How can a web user be authenticated? (password or biomedical methods such as fingerprint, speech, pupil or face measurement etc.)
• Which functions are offered and which data can be accessed? (authorization of web users)
• What should be done if hackers are discovered? etc.
Securing Applications and Data Through Firewalls

Internet → Firewall 1 → Web-server → Application server → Firewall 2 → Back Office System → Data Base

Securing Applications and Data Through Firewalls