Mobile Payments

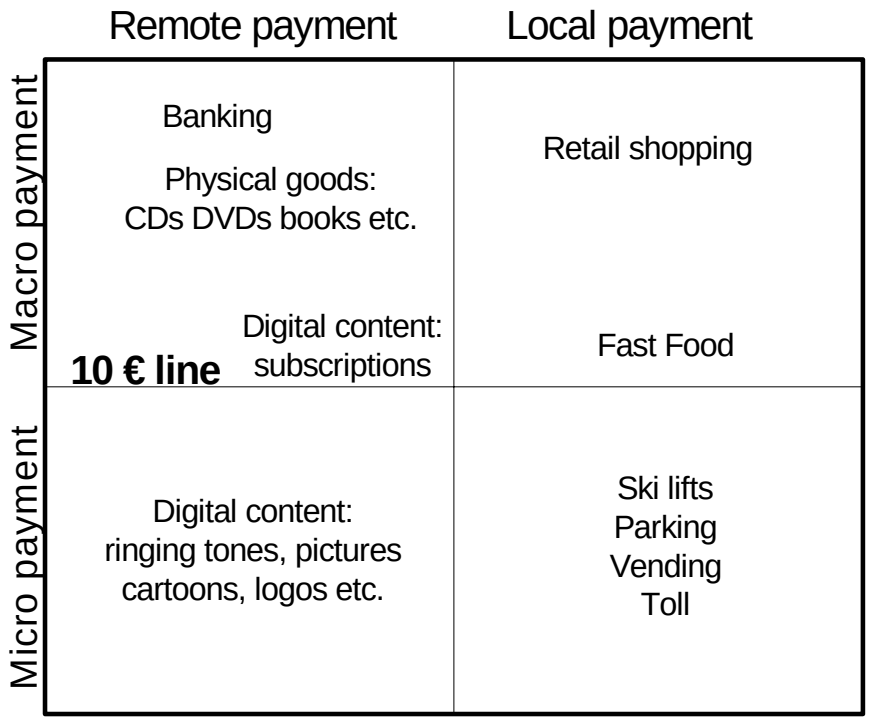
Antti Pihlajamäki 27.10.2004

Outline

- Introduction
  - Terminology
  - Basic concepts
- Technology behind mobile payments
  - Remote transactions
  - Local transactions
- Drivers of mobile payments
  - Unique features of mobile payments
  - Critical success factors
- Legislation and Regulation
  - In EU and in Finland
- Key players in mobile payments
- Some security issues

Key Concepts

- Mobile payment means payments made using a mobile device, usually a mobile phone
- M-payments can be divided into four categories based on the size and location of the transaction

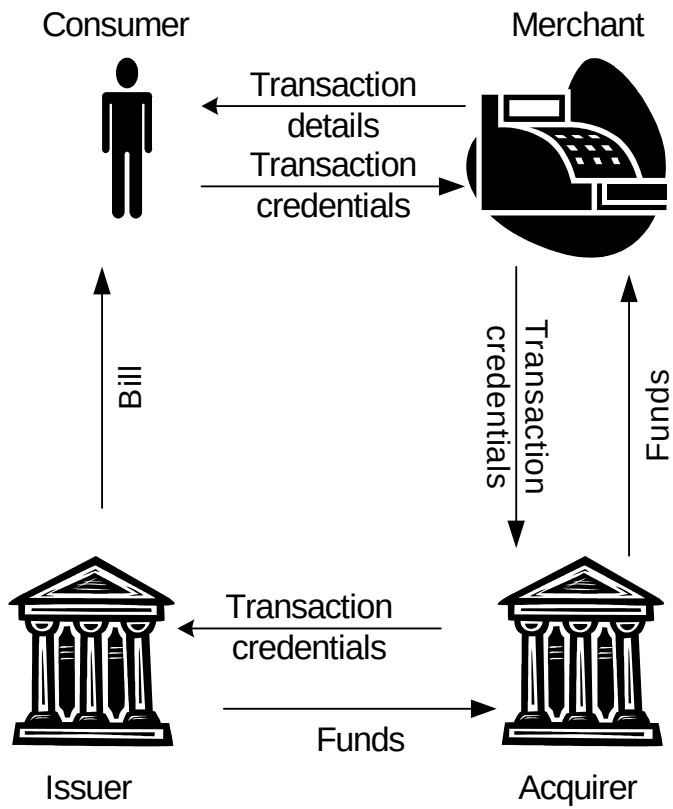


Technology in Remote Transactions

- Remote transaction means payments not made locally, like buying content from the Internet
- Technologies that enable remote transactions are
  - SMS
  - Mobile Internet
- SMS is the already existing technology while mobile Internet is emerging
  - Mobile Internet in mobile payments means handheld devices capable of browsing the Internet and not PCs connected to the Internet using mobile phones

Payment Transaction example

- In a typical transaction the consumer buys something from the merchant and the merchant gets the funds from a middleman called the acquirer. The acquirer deals with the issuer who finally bills the consumer. Transaction credentials are used to authorize the transaction.



Technology in Local Transactions

- Local transactions are made for example in shops instead of using cash or credit card
- Technologies that enable wireless local transactions include
  - Bluetooth
  - WLAN (802.11)
  - Infrared
  - RFID and contactless chip
- RFID would be the fastest to use but Bluetooth is best for larger amounts of data
  - The decision about the most suitable technology is not yet made

Drivers of mobile payments

- Mobile payments have some unique features not found combined in any other payment solution
  - **Ubiquity**
    - Users can get any information they are interested any time regardless of their location.
  - **Reachability**
    - Users are reachable everywhere anytime for business entities and other people.
  - **Localization**
    - Location based services are possible. It's possible to get up-to-date information for example from nearby restaurants.
  - **Personalization**
    - Mobile commerce applications can be personalized to reflect user's needs.
  - **Dissemination**
    - Delivering information to users in a specific geographical location is possible.

Critical success factors

- Contingency factors
  - Changes in the social-, legal-, commercial- and technological environment are uncontrollable but changes in these areas are needed for m-payments to succeed. Legal- and technological environments are already going in the right direction.
- User specific factors
  - In adapting new payment methods the consumers role is the most important. If they start using m-payments others will follow.
- Factors determining value for users
  - Both the consumers and the merchants have to gain some additional value from mobile payments in order for it to become a success.

Legislation and Regulation in EU

- Directive about e-commerce (2000/31/EC) defines the rules for e-commerce in general
- The two directives (2000/14/C) and (2000/46/EC) provide the legal framework for e-money
- Member states use these directives in their own legislation
- In EU area e-commerce service providers are supervised according to the legislation in their home country regardless of the place where they do business

Legislation and Regulation in Finland (1/3)

- Regulation in Finland based on directive about e-commerce
  - The e-commerce directive was implemented in Finland by the Act on the provision of information society services (458/2002) in July 2002.
  - The law requires for example that companies involved in e-business must have at all times certain information available about their activities. This information has to bee easily accessible by the customers and authorities.

Legislation and Regulation in Finland (2/3)

- Regulation in Finland based on directive about e-money
  - The directive about e-money was implemented in February 2003 by the revised Credit Institutions Act (69/2003)
    - Non-financial institutions are now allowed to keep customer accounts that are much like bank accounts in some sense. Before this was possible only if the customer had made a capital investment to the company.
    - Non-financial institutions can't still function as a bank. Bills can't be paid using customer accounts and the funds can be used only in transactions with the company keeping the account.
    - The maximum amount of money in customer accounts is 3000 € and it's not covered be the deposit guarantee.

Legislation and Regulation in Finland (3/3)

- cont.
- The new law defines two types of e-money: single-use e-money and multi-use e-money
- Single-use money can be used in the customer account-style
- Multi-use money is issued by credit institutions and it can be used more widely. An example of this is the Avant-system.
- Strict rules govern the issuance of e-money. The law defines payment organization which is allowed to issue e-money. Payment organizations must have at all times liquid assets amounting to at least the total outstanding issuance of e-money.
- E-money must be repayable at all times at nominal value

Key players in mobile commerce

- Credit card companies and banks
  - VISA is concentrating on the mobile payments made using mobile Internet. They have forecasted that 375 billion USD will be spent in this way by 2005. Banks might have a good chance in local payments because VISA is concentrating in remote payments.
- Mobile operators
  - Key business is the network connection but small remote micro payments are likely to stay in the operators' control
- Merchants
  - Mobile payments differ from the rest of the e-commerce in the sense that it's more B-to-C concentrated and merchants provide the possibility for mobile payments when consumers start using it.

Security issues

- Security is important in the adaptation process of mobile payments. Key vulnerabilities are:
  - Mobile device can be infected by a virus
  - Too easy or guessable PINs or passwords
  - The mobile device is stolen
  - The lack of user knowledge or experience
  - GSM and SS7 security is not that good
  - It’s possible to capture and modify data during the over-the-air transmission
  - Possibility of using a false BSS (Base Station System)