Mobile Payments

Antti Pihlajamäki
Helsinki University of Technology, Networking Laboratory
antti.pihlajamaki@hut.fi
S-38.042 Seminar on Networking Business, Fall 2004

Abstract

This paper examines mobile payments from the technical and regulatory perspective. Mobile payment means payments that are done using a mobile device, usually a mobile phone. Often also m-payment term is used in the same meaning. There are many types of mobile payments and they are presented in this paper. Also some security issues are discussed just to give an idea of the future challenges they might bring.

From the regulatory point of view mobile payments are part of a bigger concept, electronic commerce. The directive 2000/31/EC about electronic commerce and preparatory acts describes in full detail the rules of the game in EU. Country specific legislation is made based on the directive. For example in Finland the law (458/2002) fulfilling the requirements of the directive was set in 2002.[1]

1 Introduction

1.1 Key concepts

Mobile transactions can be divided logically into four types based on the size and location of the transaction. Based on the size transactions are divided into macro- and micro payments. The limit for micro payments is seen to be approximately 10 euros. Everything above that is macro. In addition to that location categorizing is used to make a difference between local and remote payments. Local payments are typically types of payments used to pay for example when using vending machines. Remote payments include for example buying digital content from the network. Figure 1 depicts this division of payments into the four categories. Some examples are also given from each category.[2]

2 Technology

The technical solutions to make mobile payments possible, secure and easy to use basically already exist. The idea has been to use existing technology as much as possible to reduce the costs and ease the roll-out of mobile payments. The user needs a modern mobile phone to be able to use advanced technologies like Bluetooth for local payments. For remote payments the requirements are not that high. For basic remote payments charged by the operator no special features are required from the user's equipment.

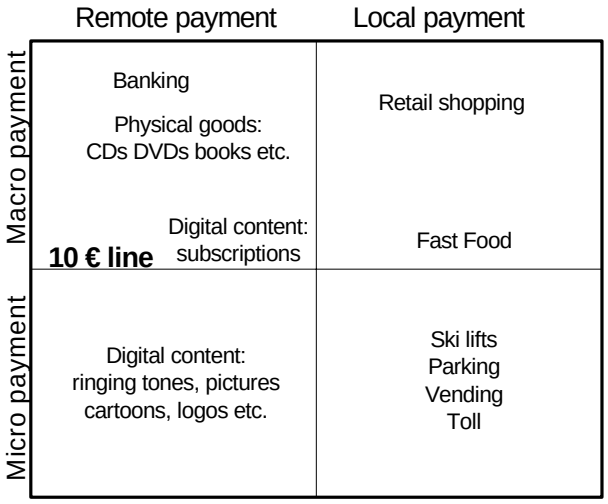

Figure 1: Transaction types

2.1 Remote transactions

Remote payments have been available for quite some time now. A prime example of a remote payment is the purchase of ringing tones. These kinds of transactions use SMS as the billing and transportation mechanism. The operator's billing machinery is well suited for these kinds of small transactions. A future scenario for remote payments is the use of mobile Internet.

2.2 Local transactions

Local transactions in mobile payment are an emerging market. The technology has to be more advanced in local transactions compared to remote transactions. The idea of local payments is to use the mobile phone preferably wirelessly to make a transaction. Several alternatives exist for making this possible. The four most often mentioned wireless technologies are:[3]

- Bluetooth
- WLAN (802.11)
- infrared
- RFID and contactless chip

Many of the latest mobile phone models are capable of communicating with at least one of the four wireless technologies. Some can use up to three of the mentioned technologies. So the user equipment shouldn't be the thing slowing down the growth of local transactions.

RFID is seen as the most promising technology for local payments because it's fast for small amounts of data and it should be easy to implement to existing infrastructures. Bluetooth is considered to be good for less time-critical transactions. The main advantage Bluetooth has is its capability to transfer relatively large amounts of data bi-directionally.

In local transactions the mobile operator is usually seen as just the party providing the required network connection. In remote transactions operators have a bigger role making them act also as a bank and a credit issuer. The number of stakeholders in remote payments is often three: user, operator and the content provider. In local payments there are more parties involved.

A typical payment transaction is presented in figure 2. The role of the operator is in most cases reduced to providing the necessary network connections. In the figure the consumer buys something from the merchant who gets the funds from the issuer using acquirer as the middleman. Transaction credentials authorize the transaction in the form of a PIN code or signature. Acquirer is a party who makes it possible for customers and merchants to do business by providing a link to the issuer. Issuer is the financial service provider who bills the consumer e.g. in the form of a monthly credit card bill.[4]

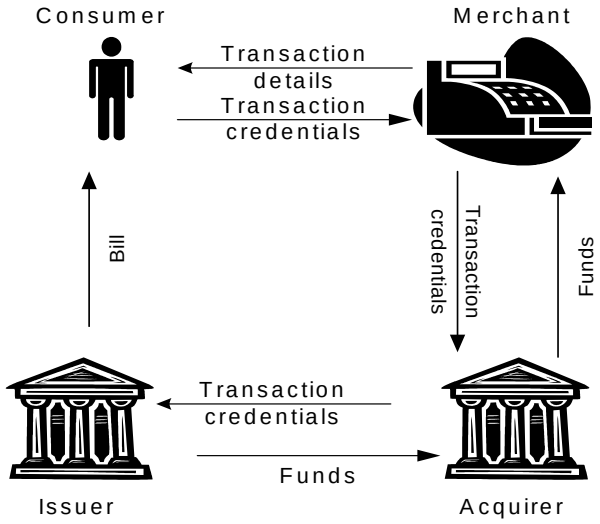

Figure 2: Payment Transaction

3 Drivers of mobile payments

3.1 Unique features of mobile commerce

Mobile payments have a combination of features that is not found anywhere else. It should be a major factor helping mobile payments to become more popular. These features include: [8]

- **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.

3.2 Critical success factors of m-payments

The critical success factors on mobile payments can be divided into three groups: contingency- and user specific factors and factors determining value for users.[5]

The contingency factors include different environmental forces likely to change. The environments likely to change are social-, legal-, commercial- and technological environment. These are uncontrollable forces but they still have to be examined. The most important of these is the commercial environment. Some major changes have to happen there to make mobile payments possible in large scale. Changes in the legal environment take their own time but luckily the laws about e-business and e-money in general should also cover mobile payments in enough detail. The technological environment is always a question mark but the recent developments in user equipment are very promising.

User specific factors are very important in mobile payments. The consumers usually make the decision about adapting new technologies when the question is about new payment methods. Of course active participation is needed also on the behalf of merchants but they tend to invest on new equipment only when the critical mass exists. Many things affect the consumers' decision to start using a new payment method and they are hard to influence. The adaptation of electronic payments in general is influenced by factors such as high income, education and even house ownership. One thing the banks and credit issuers can do to help mobile payments become more popular is the percentage they charge for every transaction. This should not be too high compared to other alternatives. This charge is usually paid by the merchant so if it's too high merchants will not invest in the equipment.

For mobile payments to succeed they have to be valuable to the users. Users include the customers and the

merchants. They both have to get some additional value from using mobile payments. The value gained needs to be greater than the investment costs for the consumer, merchant and financial institution.

4 Legislation and Regulation

4.1 Regulation in EU

In EU-area electronic commerce is regulated by the directive 2000/31/EC. In addition to that there are two directives governing e-money, 2000/46/EC and 2000/12/EC. These directives are used as a framework for country specific legislation. In the next chapter Finnish legislation based on these directives is presented as an example of country specific regulation based on the common rules in the EU.[6]

4.2 Regulation in Finland

The directives about e-commerce and e-money were published already in the year 2000. The first laws based on these directives were implemented in Finland not until 2002. The next two chapters present the legislative process based on the directive about e-commerce and e-money.

4.2.1 Regulation about e-commerce

The e-commerce directive was implemented in Finland in July 2002. The directive is implemented by the Act on the provision of information society services (458/2002). The spirit of the directive is to improve the movement of information society services in the member states by providing a legal framework. It's important that every member state has in principle the same kind of laws because the service providers are supervised according to the legislation in their home-country regardless of the place where they do business. The law requires for example that companies involved in e-commerce must have at all times certain information available about their activities that the authorities and customers can access.

4.2.2 Regulation about e-money

The directives about e-money were implemented in Finland in February 2003 by the revised Credit Institutions Act (69/2003). One major change in this law is that non-financial companies can offer customer accounts to their customers. This was before something that only banks etc. could do. Other companies have been able to collect funds from the public only in the capital markets.

The new law gives non-financial institutions the right to collect repayable-on-demand funds. They have the right to keep customer accounts that are much like bank accounts. Before this law it was possible for non-financial institutions to keep customer accounts if the customer had invested in the company. The new law requires no capital investments to be made. Some retail stores had accounts that appeared to be like customer accounts already during the old legislation but they were actually only sold under the store's brand. There had to be a deposit bank actually handling the account.

The law is very strict in limiting the non-financial institutions and prevents them from functioning as bank. The funds in the company's customer account can be used only to buy goods or services from the company itself. Cash withdrawals are possible but bills can't be paid using customer accounts. The maximum amount of money one customer can have in the account is set to 3000 euros. The party supervising companies collecting funds from their customers in the described way is the Finnish Financial Supervision Authority (FSA). Companies keeping customer accounts have to report their activities to FSA.

The funds in customer accounts are not deposits in the sense that they are not covered by the deposit guarantees. This is one reason why the amount of money in the accounts is limited. So there is a chance customers can lose their money for example in the case of a bankruptcy.

The law separates two types of money: single-use and multi-use e-money. There is a clear distinction between these in terms of the usage and the issuer. Single-use e-money can be distributed by a company to its customers and they can use it to pay for goods or services in the customer account-style. Multi-use e-money on the other hand is issued by credit institutions and it can be used more widely. In Finland an example of multi-use e-money is the Avant-system which is owned by large banks.

The usage of e-money needs a new type of a credit institution named payment organization. The job of the payment organization is to specialize in payment transactions and e-money issuance. A payment organization collects repayable funds from the public to be used for in transactions and e-money issuance. Its purpose is not to lend money to the public, only to transform it to electronic form. The law requires the payment organization to have liquid assets amounting to at least total outstanding issuance of e-money and the dept incurred from payment transactions. E-money must be repayable at all times at nominal value.[7]

5 Players in mobile commerce

Mobile commerce is likely to become a big business and therefore it interests many business entities. Mobile payments are more complex than many other payment methods even in the field of e-commerce. Typical transactions include at least the customer, merchant,

mobile operator and bank. This makes the value chain more complex than usual.

5.1 Credit card companies and banks

At the moment VISA has the biggest share of Internet payments, over 50 per cent share, and they are very interested in mobile payments. Visa has already conducted mobile payment experiments with NTT DoCoMo using IrDA ports. They expect that by 2005 375 billion USD will be spent using wireless Internet device. They expect that in four years more handsets than PC's will be connected to the Internet. VISA is trying to expand it's dominance of the wired Internet payments to the wireless Internet payments. VISA's intention doesn't seem to be in local payments. They believe remote payments using Internet is the market for them. They already have the required infrastructure which should give VISA an advantage. Although their system might not be that cost efficient which is probably one reason they are more interested on bigger Internet payments than small local payments. This gives the banks a chance in the local payments.[8][9]

5.2 Mobile operators

The mobile operators' main task is to provide the needed network connection to mobile devices and that's their key business. In addition to that their charging machinery is well suited for the smallest micro payments such as ringing tones which already is a surprisingly large business. Many of the competing charging systems are just too expensive for the smallest transactions and this gives the mobile operators an advantage for example in vending machine payments. In all the payment scenarios they always control one scarce resource, the network. So, what ever becomes the dominant solution in mobile commerce the operators' key business still survives.

5.3 Merchants

At the moment most of the e-commerce is Business-to-Business. It evaluated to be approximately 90 per cent of all e-commerce. This is not likely to be the case with mobile payments. Business-to-Consumer portion of the mobile payments is going to be a lot bigger than it is in the e-commerce in general. This should cause merchants to become interested in providing the mobile payment possibility to consumers. If the local transactions become popular than merchants not before involved in e-commerce are likely to provide the possibility to use mobile payment. There is the old chicken-egg dilemma to be faced in mobile payments. The question is, will the consumers start demanding the possibility for m-payments or will the merchants start pushing it before there is demand. Probably the consumers will first have to start using mobile payments before the majority of merchants provide it.[8]

5.4 Mobile equipment manufacturers

The mobile equipment manufacturers are in some sense one of the key players here. They have to make phones that support mobile payments. So far the mobile payments have been based on technologies that are in the phones for other reasons. IrDA ports are probably the most widely spread technology in the phones that makes wireless m-payments possible. But not all the phones have even that. The more advanced wireless technologies such as Bluetooth and WLAN are still quite uncommon. If the manufacturers won't produce phones that enable mobile payments in large scale than there is the possibility of using the SIM card combined with RFID technology for local payments. On the other hand for some remote payments all that is needed is Internet connection or the capability to send short messages.

6 Security issues

Security is going to be a major factor in the adaptation process of mobile payments. Consumers are used to secure solutions or at least the existing solutions seem be secure in the eyes of consumers. There has been credit card frauds especially in the Internet but consumers very seldom have to suffer financially form the frauds. The credit card companies have taken care of the frauds' costs. If the transaction costs merchants have to pay for mobile payments is wanted to be approximately the same as it is with credit card payments then m-commerce can't afford frauds. This is because the costs to make m-payments is at least in the beginning going to be more expensive then credit card payments. Some of the biggest risks in mobile payments are described in the following two chapters. It should be noted that the wireless local payments adds another risk factor to m-payments that doesn't exist in for example credit card payments.[10]

6.1 Security threats of the payment model

The mobile device that is used in m-payments and the users them self cause major risks for the security of mobile payments. The mobile device can be infected with a virus that could perform unauthorized payments or send user info such as PIN codes to a third party. The first mobile phone viruses spreading using Bluetooth already exist, so this is a major threat. The second threat is caused by the fact that many people have guessable or default PINs or passwords. It's very likely that PIN code would be used as an identification method in m-payments, so having for example default PIN causes a threat. The third risk is that the mobile device is stolen and then used to make unauthorized payments. Another alternative is to borrow the device for a while and obtain the necessary information needed to make transactions and then returning the device without the user noticing anything. The fourth risk comes with lack of user knowledge or experience. It's important that the user

always checks properly that the other party is who he claims to be. The user might accept a payment that he didn't intend to do. Roaming causes another threat. It's not always possible to send all the necessary authentication information to a roaming mobile phone. This is obliviously a threat that could slow down the adaptation of m-payments. Many vulnerabilities are involved in the SMS usage in m-payments. They can be spoofed, replayed, lost or misrouted by the operator. The wireless local payments are also threaded by security attacks similar to attacks used with wireless networking in general.

6.2 Security threats of the carrier network

One thing common to m-payments is the fact that all mobile phones operate in mobile networks. The network itself causes security threats. The situation might get better with 3G networks but with GSM the security is not that good. The encryption in GSM is not that strong and it makes it possible to capture or modify data during the over-the-air transmission. It's also possible to capture data using a false BSS (Base Station System) because in GSM the mobile phone is authenticated to the network but the network itself is not authenticated to the user. Some security concerns are also related to the security of the BSS and the SS7 signaling network.

7 Conclusion

Mobile payments are likely to become more popular despite the many difficulties still waiting to be solved. The single fact that there should be two billion mobile phone users by 2008 makes m-payments an attractive market. Many of the biggest players like VISA believe in mobile payments which is a good sign considering that VISA has the biggest share in Internet-payments. One thing that is not yet clear is what technology will be used in mobile payments. VISA believes that mobile Internet is the tool to make mobile payments. This might be thru in remote payments but local payments is another story. In local payments one possible alternative is the use of Bluetooth or RFID combined with the mobile network. The smallest remote micro payments are likely to stay in the control of mobile operators. There are a lot of problems to be solved before mobile payments become reality in large scale. The regulation already exists which should help in trust issues. Also the fact that e-money is so well regulated helps a lot in developing mobile payments. The whole mobile world is known for rapid development and fast adaptation of new technologies. Maybe that will be the case with mobile payments too.

8 References

[1] E-Finland forum, E-kauppa Suomessa ja EU:ssa, http://www.e-finland.org/cgi-bin/center/xhtml?/pageID=58//list=perus/from=81//sort=up+25/find=+/show=, (Referenced 7.10.2004)

[2] MeT White Paper on Mobile Transactions, 2003, http://www.mobiletransaction.org/pdf/R200/white_papers/MeT_White_paper_on_mobile_transactions_v1.pdf, (Referenced 7.10.2004)

[3] Mobile Payment Forum White Paper: Enabling Secure, Interoperable and User-friendly Mobile Payments, 2002, http://www.mobilepaymentforum.org/pdfs/mpf_whitepaper.pdf, (Referenced 7.10.2004)

[4] PayCircle White Paper: Standards that get m-commerce flying, 2003, http://www.paycircle.org/downloads/file.php?id=21&kat_id=2 (Referenced 8.10.2004)

[5] Hort, Christian: Critical Success Factors of Mobile Payment, 2002, http://www.m-lab.ch/pubs/13_CriticalSuccess_MobilePayment.pdf (Referenced 8.10.2004)

[6] Jyrkönen, Hanna, Paunonen Heli, Bank of Finland, Card, Internet and mobile payments in Finland, 2003,http://www.bof.fi/eng/6_julkaisut/6.1_SPn_julkaisut/6.1.5_Keskustelualoitteita/0308.pdf, (Referenced 9.10.2004)

[7] Bank of Finland Bulletin, 2002, http://www.bof.fi/eng/6_julkaisut/6.1_SPn_julkaisut/6.1.2_BOf_bulletin/02b4.pdf, (Referenced 9.10.2004)

[8] S-38.041 Networking Business Lecture Slides: Charging and Billing, 2004, http://www.netlab.hut.fi/opetus/s38041/k04/Lectures/L6_Charging_billing.pdf, (Referenced 8.10.2004)

[9] Visa mobile: Facts and Figures, http://www.visa-asia.com/visamobile/facts.shtml, (Referenced 8.10.2004)

[10] Mobile Payment Forum: Risks and Threats Analysis and Security Best Practises, 2003, www.mobilepaymentforum.org/pdfs/MPF_Security_Best_Practices.pdf, (Referenced 9.10.2004)

[11] Lim, Ee-Peng, Advances in Mobile Commerce Technologies, Idea Group Inc., 2003

[12] Lubbe, Sam: The Economic and Social Impacts of e-commerce, Idea Group Inc., 2003

[13] Shi, Nansi: Mobile Commerce Applications Idea Group Inc., 2004