Mobile Payments in the Netherlands: Adoption Bottlenecks and Opportunities, or… Throw Out Your Wallets

Farhat Shaista Waris, Fatma Maqsoom Mubarik and L-F Pau

ERIM REPORT SERIES *RESEARCH IN MANAGEMENT*	
ERIM Report Series reference number	ERS-2006-012-LIS
Publication	March 2006
Number of pages	90
Persistent paper URL	
Email address corresponding author	lpau@rsm.nl
Address	Erasmus Research Institute of Management (ERIM) RSM Erasmus University / Erasmus School of Economics Erasmus Universiteit Rotterdam P.O.Box 1738 3000 DR Rotterdam, The Netherlands Phone: + 31 10 408 1182 Fax: + 31 10 408 9640 Email: info@erim.eur.nl Internet: www.erim.eur.nl

Bibliographic data and classifications of all the ERIM reports are also available on the ERIM website:
www.erim.eur.nl

ERASMUS RESEARCH INSTITUTE OF MANAGEMENT

REPORT SERIES

RESEARCH IN MANAGEMENT

ABSTRACT AND KEYWORDS	
Abstract	The purpose of this research report is to analyse the mobile payment market size and its revenue basis, as well as adoption bottlenecks, in view of establishing the adoption and deployment of mobile banking services in The Netherlands. The research report describes various aspects with regard to mobile payments/mobile banking in The Netherlands. Issues like implementation, regulatory framework, estimated business case, deployment scenario's, recommended business model, a SWOT analysis of the technical solutions, organisational bottlenecks, an analysis of the reasons for success and failures, and open issues and challenges are addressed. The main aim is to try to answer the question whether there is a market in The Netherlands for mobile banking services, and providing an analysis of why M-banking services have not been so successful in The Netherlands. Furthermore, it needs to be mentioned that the focus of this paper was on micro-payments, which are generally considered to be payments of up to €10.
Free Keywords	Mobile payments, Mobile banking, The Netherlands , Business Models
Availability	
Classifications	

Mobile payments in The Netherlands:

Adoption bottlenecks and opportunities, or ...Throw out your wallets

Abstract (English):

The purpose of this research report is to analyse the mobile payment market size and its revenue basis, as well as adoption bottlenecks, in view of establishing the adoption and deployment of mobile banking services in The Netherlands. The research report describes various aspects with regard to mobile payments/mobile banking in The Netherlands. Issues like implementation, regulatory framework, estimated business case, deployment scenario's, recommended business model, a SWOT analysis of the technical solutions, organisational bottlenecks, an analysis of the reasons for success and failures, and open issues and challenges are addressed. The main aim is to try to answer the question whether there is a market in The Netherlands for mobile banking services, and providing an analysis of why M-banking services have not been so successful in The Netherlands. Furthermore, it needs to be mentioned that the focus of this paper was on micro-payments, which are generally considered to be payments of up to €10.

Keywords:
Mobile payments, Mobile banking, The Netherlands , Business Models

Abstract (Dutch):

Het doel van dit onderzoek is het analyseren van de marktgrootte van mobiel betalen en de bijbehorende omzetbasis, alsmede de invoering van knelpunten, om inzicht te verkrijgen in de introductie en ontwikkeling van mobiele bankservices in Nederland. Het onderzoek beschrijft verscheidene aspecten van mobiel betalen/mobiel bankieren in Nederland. Onderwerpen als implementatie, wetgeving, geschatte businesscase, aanbevolen businessmodel, ontwikkelingsscenario's, een SWOT - analyse van technische oplossingen, organisatorische knelpunten, een analyse van de redenen van succes en falen en openstaande problemen en uitdagingen komen aan de orde. Het voornaamste doel van het onderzoek is het trachten te beantwoorden van de vraag of er een markt voor mobiel betalen is in Nederland en een analyse geven van waarom mobiele bankservices niet succesvol zijn geweest in Nederland. Bovendien dient gemeld te worden dat de focus van dit verslag lag op microbetalingen, waar over het algemeen betalingen tot €10 onder verstaan worden.

***Kern woorden**:*
Mobiel betalen, Mobiel bankieren, Nederland, Business modellen

Table of contents

Executive Summary

According to Mobile Payment Forum (2002):

> *"A mobile payment is the process of two parties exchanging financial value using a mobile device in return for goods or services." A mobile device is defined as "a wireless communication device, including mobile phones, PDA, wireless tablets and mobile computers."* [1]

For the purpose of this research report, a mobile device is meant to include only a mobile phone with its basic functionality (including smart phone, but not PDA or portable computer or specialized terminal) in order to narrow down the scope; the generic term used is therefore" mobile phone" .
Moreover, the focus of the research report is on micro-payments, which are generally considered to be payments of up to €10; it is indeed stressed that the focus is on payments enabled by wireless terminals, and not on M-banking which is a much broader concept and includes many other mobile financial services apart from mobile payments.

Mobile phones have become a lifestyle product. Mobile banking is all about freedom that enables the user to pursue other interests than worrying about everyday jobs. Mobile banking transactions can be charged the same way as text messages are charged. So, is it time to throw out the wallets and start warming up those thumbs…Is it in genuinely like that? This research report tries to explore all the possible answers. How far are mobile payments in relation too different from, mobile banking developments? And what are the related factors causing failures or success in the way of M-payment progress.

Much qualitative and quantitative research has been done on electronic payment systems, though that does not hold true for mobile payments and mobile banking. Because mobile payment is an immature field, quantitative data is limited and several companies that are involved in the development process of commercial applications are reluctant to give details before going live.

In this research report the trend of mobile payments is scrutinized, in order to analyse whether there is a potential market in The Netherlands. How do potential customers perceive it as it is not a new concept anymore. Why has it not been able to become a killer application and attract the mass market? An attempt is made to analyse what needs to be done differently to attract these customers, who have been reluctant to adapt this service.

The main issues explored in this paper include, to start with the implementation. For mobile payment services, designing the architecture of the implementation model and then making it possible to work in real time is quite a difficult task to achieve.

Furthermore, another important aspect is the regulatory framework. For tracing the right direction of one's goal it is important to acquire all the required knowledge of the field. Rules and regulations are a kind of check, which warren the individuals not to get lost in something which is not possible.

Additionally, some deployment scenarios are considered. Moreover, some case studies were done to comprehend the reasons behind the 'failure' of mobile banking services in The Netherlands . Based on this, a business model that tries to address the flaws in the current business models, is recommended.

Next to that a SWOT analysis of the technical solutions that are available with respect to mobile payment services was made. The SWOT analysis gives a clear indication as to what the best and next best solution is, and which one is the worst. It also gives an indication about where the opportunities lie and what the threats are. In other words, this analysis should simplify the decision-making process regarding the choice of the technical solution. Also the organisational bottlenecks faced by various actors in the chain are touched upon in this section.

In addition, the main parties involved in mobile payment transactions have been discussed. The banking industry has little to offer mobile payments in terms of skill until the business model has been fully tested and developed in niche markets. As far banks have been entering the mobile payment world in partnership with operators to enable mobile payments to make the transition from remote payments to physical point of sale. Banking involvement in the future evolution of mobile services is dependent upon the relationship between the banks and seller. The mobile operators are not in a position to recreate the entire banking infrastructure. Banks understand that existing non-mobile payment systems such as cash and credit cards are costly and inefficient.

Last but not least, issues with respect to mobile banking services that have remained unresolved and questions that are unanswered till date are addressed. Also the challenges that will be faced by the bank or mobile operator in providing mobile payment/banking services are touched upon.

1. Introduction and Research scope

1.1 Introduction

Mobile banking is developing at different tariffs and in different directions depending on the region. The European market with its high mobile penetration is currently developing along SMS lines, while in the Far East (particularly in Japan and South Korea) and Scandinavia the technology has already gone a few steps further towards wireless enabled transactions. The industry is intended to introduce secure and easy to use technologies for mobile commerce. This will enable mobile operators to fulfil their desire to push towards 3G and multimedia services. Merchants and financial institutions are recognising the opportunity and exploring additional avenues for the technology.

The breakthrough of mobile financial services is inevitable, and could be turned into business opportunities with thorough pre-analysis and planning. If implemented proficiently mobile banking services can help financial institutions to improve customer acquisition and customer retention, reduce operational costs by migrating simple transactions away from branches, and offer superior customer service and generate new revenue streams. The main advantage as mentioned earlier will be the opportunity to cut down costs of providing service to the customers. Additionally, this new channel allows the bank to cross-sell and sell-up their other complex banking services such as vehicle loans, credit cards etc.

The service providers are provided an opportunity to achieve growth by means of mobile banking applications. In some countries, for example South Korea, mobile penetration is nearing saturation and mobile banking services are allowing the service providers to increase revenues from the now static subscriber base. The service providers are also

increasingly using the complexity of their supported mobile banking services to retain old customers and attain new ones.

As mentioned before much more research has been done on electronic payments compared to mobile payments and mobile banking. The differences between E-banking and M-banking are listed in the following table.

Table 1: Differences between E-banking and M-banking:

Technology	E-Banking	M-Banking
Device	PC	Smart phone, pager, PDA
Operating System	Windows, Unix, Linux	Symbian (EPOC), PalmOs, Pocket PC, proprietary platforms
Presentation standards	HTML	HTML, WML, HDML, i-Mode
Browser	Microsoft Explorer, Netscape	Phone.com, UP Browser, Nokia browser, MS mobile explorer & other micro-browsers
Bearer Network	TCP/IP, Fixed Wireline Internet	GSM, GSM/GPRS, TDMA, CDMA, CDPD, paging networks

Source: http://mis.ucd.ie/students/ecomm0001/misp632/justin.doc

There are various mobile banking services available, including:

- Mini-statement and account history
- Fund transfers
- Bill payment
- Commercial payments
- Real-time stock quotes
- Personalized alerts and notifications on security prices

These are some examples of mobile banking services available. A detailed list of mobile banking services including mobile payments will be provided in the section on deployment scenarios.

The abovementioned services can be provided through either of the following standards: SMS or WAP. The former is used for exchanging short text messages, while the latter is a facility offering Internet browsing possibilities on mobile devices.

1.1.1 Classification of Mobile Banking services

Mobile banking services can be classified along various dimensions. One way is to classify them on the basis of their nature, which results in two types of services: transaction based services or enquiry based services. The difference between the two is that in a transaction based service one specifically asks the bank to transfer money from one account to another, while an enquiry based service involves a request for a bank statement. Enquiry based services also diverge from transaction based services in the sense that they require less security across the channel from the mobile device to the banks data servers, as opposed to transaction based services.

Another way to classify these services is based on who the originator of the service session is, called the “Push/Pull” nature. ‘Push’ is described as the bank being the one taking the initiative to send information based upon an agreed set of rules. On the

contrary, in case of 'Pull' the customer explicitly requests a service or information from the bank.

Based upon the abovementioned classifications, the services can be divided as shown in table 2.

Table 2: Classification of mobile banking services (examples); push /pull is to end user of mobile phone

	Push Based	***Pull Based***
Transaction based	-Subject to specific physical conditions: wireless parking fees and equivalent (Bluetooth neighbourhood detection)	-Fund transfer -Bill payment -Other financial services like share trading -M ticketing at use initiative
Information based	-Credit/Debit Alerts -Minimum balance alerts -Bill payment alerts -Share index and financial information push	-Account balance enquiry -Account statement enquiry -Cheque status enquiry -Cheque book requests -Recent transaction history -Share price request

1.2 Research Scope

The research scope was limited around the following core question:
In view of establishing the adoption and deployment in The Netherlands of mobile banking, the mobile payment market size and its revenue basis were analyzed, as well as adoption bottlenecks.

This is in context of a broader issue which is: *analysis of which banking customers would like to have available on mobile terminals instead of ATM's or other payment systems in The Netherlands?* However, to trigger decisions on service selection the previous research question must be studied first.

More specifically, the focus of this research report was on micro-payments which an average customer in The Netherlands can afford. This in order to bound the focus to a limited area and not go out of the focus range. Furthermore, the centre of attention will be more accurate and clear, providing relevant information in the field.

Mobile banking is taking off due to a confluence of several factors - packet-data networks, enhanced devices, and availability of the latest content. The emerging trends in mobile banking are gradually booming. The most frequently offered mobile banking services to customers in which the customers are mostly interested are looked into. Also the market drivers, as well as obstacles to mobile banking are examined. This paper will analyse the issues impacting mobile banking such as security, billing, standards, rules and regulation and pricing models suitable for mobile banking.

Starting from the history of the traditional banking sector reveals that there are two different ways in which banks can react to the changing market conditions. Firstly, banks have tried to satisfy the customer's new needs by offering new services with higher added value. Secondly, the banks have developed new technologies to reduce their operational

costs. Indeed, the new channel that has been developed by mobile payments, is much cheaper for the banks than the already existing channels. The possible revenue streams that can come from financial services are considerable and consequently these services create opportunities for the traditional banking sector.

The use of mobile services and new technologies have changed the long-established work patterns significantly. The interaction between traditional banks and their customers have evolved from walk-ins at 'bricks-and-mortar offices' to real-time interactions supported by telecommunication and information technology (IT). Network-breakthroughs resulted in the emergence of the automated teller machine (ATM), which meant that a bank could now roll out a dense network of "mini-branches" capable of handling simple transactions automatically. Improvements in telecom technology led to the introduction of a new telephone-based channel (Mobile-banking), resulting in a more efficient interaction between the bank and its customers.

The improvements in technology have reinforced the conviction of people, more than ever before, that financial services are a matter of technological infrastructure. Moreover, people are perceiving a payment as a data transaction, rather than a transaction of money. One of the implications of developments in "mobile banking"/ "mobile payment" would be that banks are not necessarily needed for banking functions. In other words, while certain banking functions need to be performed, but the institutional arrangements that are used to carry out these functions can change over time.

The success of mobile telephony, being capable of sending voice and data independent of the location and time and by the appearance of mobile commerce, has set in motion a new revolution. As the traditional clearing and settlement route is accessible only through the traditional banking sector, the whole payment procedure is currently held by the traditional banking sector. So, inefficiencies are shown by the market. On the other hand, the mobile banking chain has its own complexities ensuing from the nature of the device and the infrastructure for mobile communications.

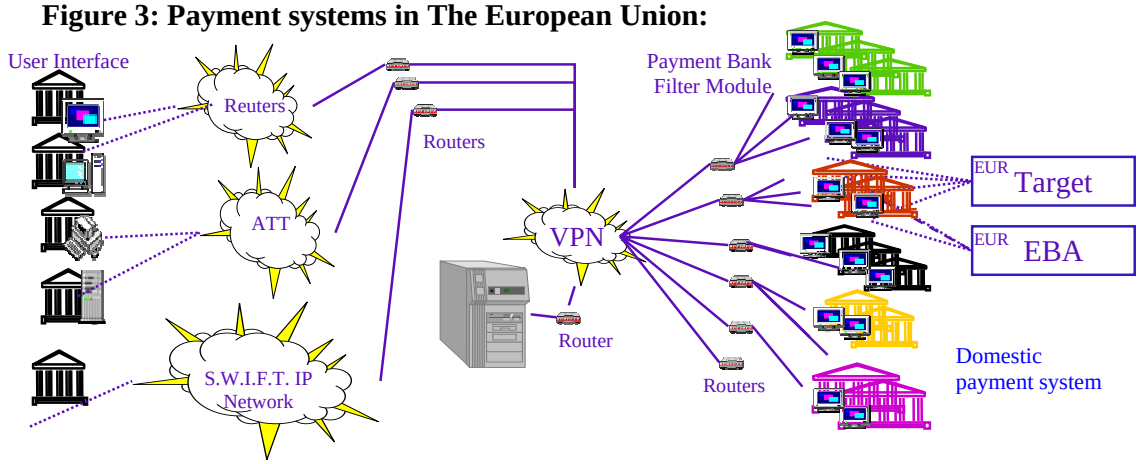
Despite the complexities involved, the new mobile technology also incites non-banking groups to enter the banking market. Suppliers of goods already use their enormous databases to offer financial services and new established companies are also trying to penetrate the financial sector. Though the main threat are the telecom companies, disposing immense networks, client databases, a billing relationship with their clients, in addition to having a lot of knowledge of mobile technology. These companies are convinced that they are well positioned to offer traditional banking functions such as cash management, risk control, short-term loans and payments. The threat of non-banking groups is relevant since the traditional banks eagerly use the "free float" between the placed order and the transaction and the deposits offered by their clients is their main resource.

2. Implementation of Mobile Payments

2.1 Implementation Architecture

There are a number of issues that need to be considered concerning the implementation, among others the various possible technical and security solutions that are available. A range of forums have been developed to promote standardization, but still banks and mobile operators are developing and recommending their own technical solution. The main forums are, Mobey Forum (mainly financial institutions), Simpay (mainly operators) that does not exist any longer and Mobile Payment Forum (mainly SIM card manufacturers). The following figure shows the payment systems used in The European Union.

Figure 3: Payment systems in The European Union:



Source: Granularity Limited, International Payment Systems Week, 2001.

EU Wide used system: TARGET

TARGET is the inter-linkage system between the Real Time Gross Settlement systems set up by all the Central Banks of the European Union. It was set-up by the predecessor of the ECB, the European Monetary Institute (EMI). It is a cross-border Gross Settlement System enabling direct payment throughout the European Union. “The system currently used by the EU central banks processes monetary policy payments, end-of-day settlements of the European clearing systems and a portion of high value/high priority payments on a real-time basis. TARGET’s business volume is however restricted by the higher price of the inter-linkage process and the high cost of maintaining the necessary levels of liquidity on the central bank’s accounts.” [2]

Euro Payments: EBA Clearing

For banks based in the European Union EBA Clearing provides euro payment clearing services. “It is a privately owned payment system operator for processing high value payments (EURO1), as well as for low value retail and mass payments (STEP 1 and STEP 2). For high value payments, Rabobank is one of the major EURO1 clearing banks. The EURO1 system allows participating banks to exchange payment instructions via S.W.I.F.T. and settle the resulting balances at the end of each clearing day in central bank money. Being a net payment system which is fully Lamfalussy compliant, EURO1 is secure and highly cost-effective.” [2]

Payment and clearing systems in The Netherlands:

- **TOP**

Within The Netherlands, payments between financial institutions are handled within the domestic payment system through Interpay and TOP. TOP is the real-time gross settlement system of De Nederlandsche Bank. TOP is used for the purpose of settling and processing, mostly large value payments in The Netherlands. Though no upper, nor lower limits for payments have been defined. Moreover, it is the entry system for TARGET. [3]

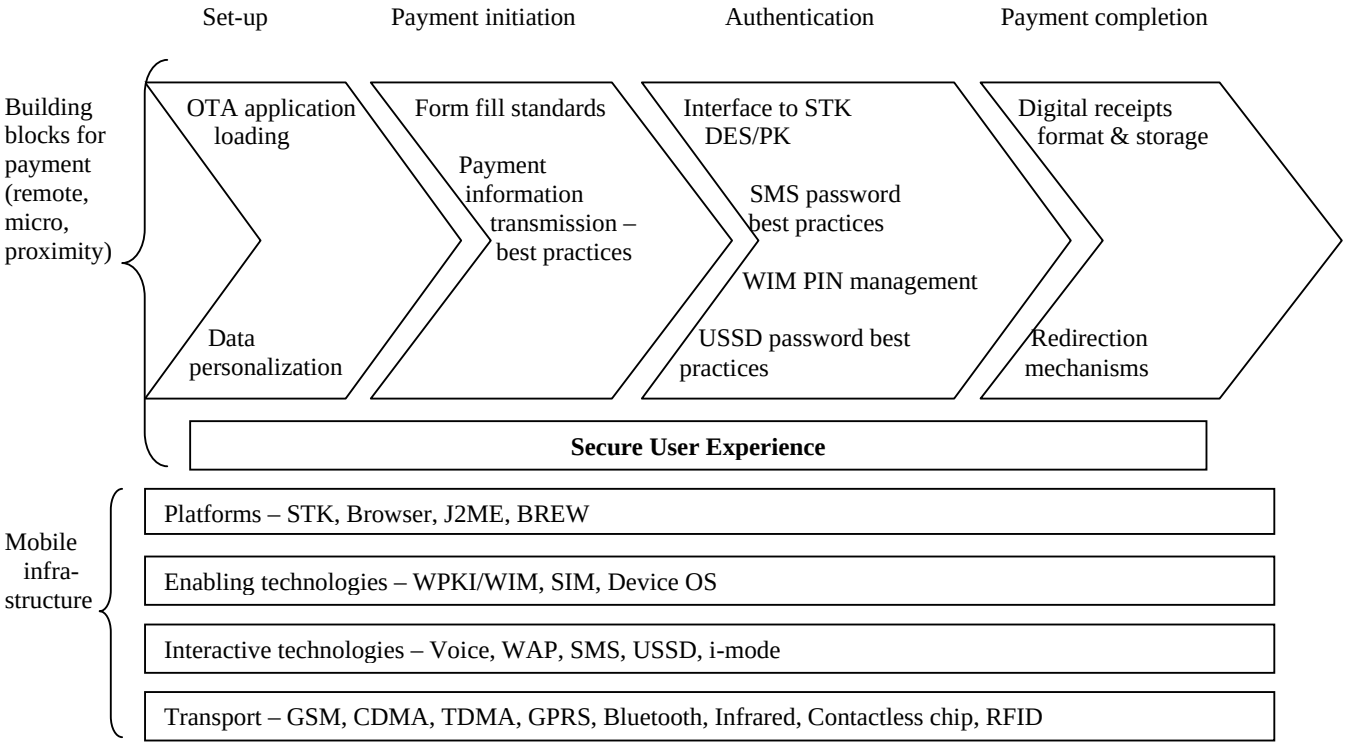
- **Interpay B.V.**

Interpay is the central automated clearing institute in The Netherlands, through which most of the retail payments are processed. Additionally, it "runs the network of POS terminals and the inter-bank authorisation network for cash dispenser transactions and issues credit cards and provides image-processing services to individual banks." [3]

2.1.1 Mobile payment infrastructure & architecture

The following figure gives an overview of the mobile infrastructure and the mobile payment process.

Figure 4: Mobile infrastructure and the mobile payment process:



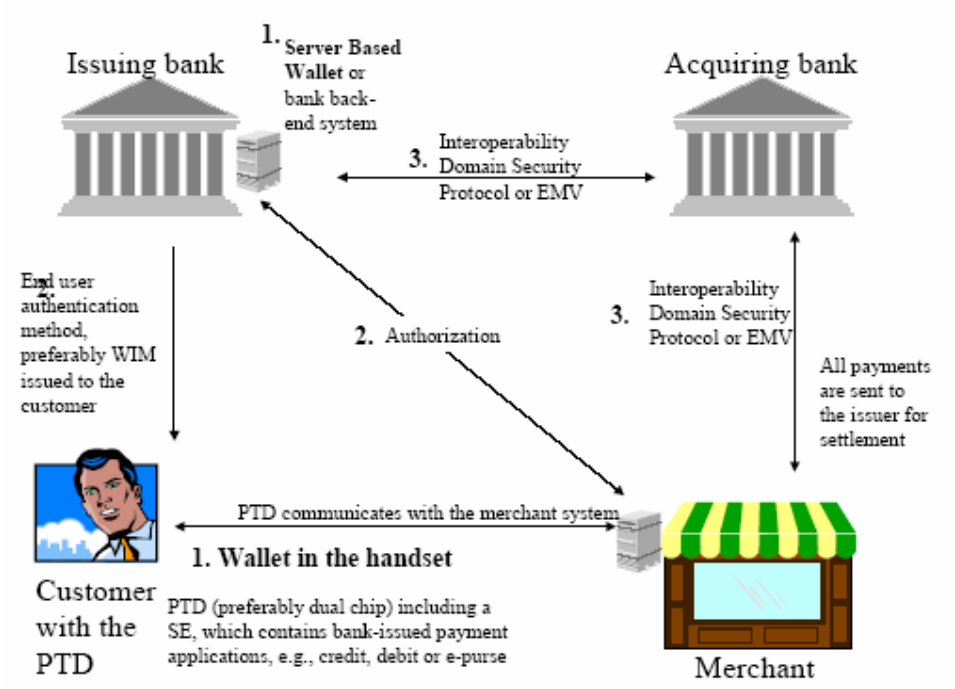
Source: Mobile payment forum

Explanation of the above figure is as following:
Set-up and configuration: concerns the way the payment mechanism takes place in the mobile environment, e.g. mobile network, physically or internet.
Payment initiation: "this involves transferring payment information over a network or wireless network."

Authentication: verification of the user is one of the most important elements in a mobile payment/transaction. There are various authentication methods e.g. passwords etc.
Payment completion: the process taking place upon completion of verification of the user and authorization for the transaction. [1]

Beyond the payment transaction there are other phases involved in the completion of a payment, including bill presentment, clearing and settlement, and risk management. The type of transport used to deliver the payment transaction information also needs consideration. The division of transport type results in two types : Over the Air (OTA) or Wide-area Network (WAN). The difference between the two is that WAN uses a "wireless network and proximity payments that transfer details over shorter distances", while OTA payments in general use "a browser-based transport infrastructure or an SMS/MMS-based system." Similar payment protocols could operate across both these transport infrastructures, despite the technical differences between them. The following figure provides an overview of the main components of the payment architecture. Though it needs to be mentioned that this is the preferred payment architecture designated by Mobey Forum.

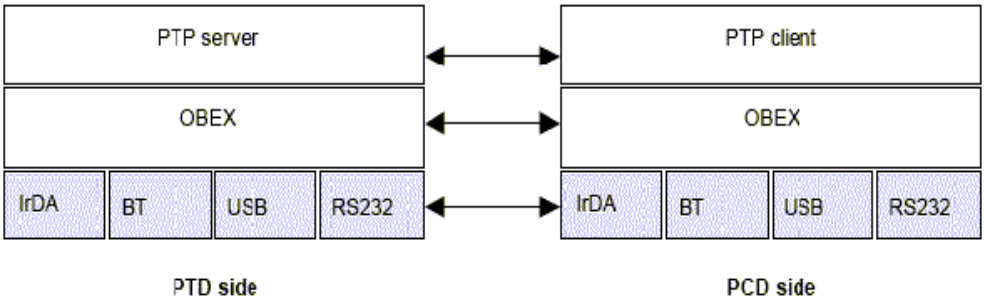
Figure 5: Main components of the preferred payment architecture:



Source: Mobey Forum

The following figures give more explanation of the PCD and PTP architecture [5].

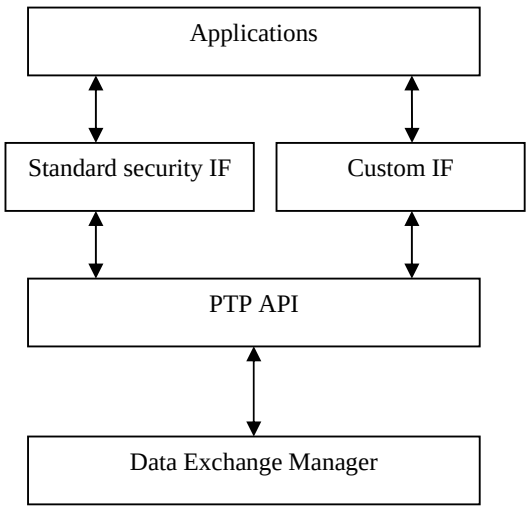
Figure 6: The PTP architecture



Source: Mobile Electronic Transactions Forum (MeT)

PTP: Person-to-Person
OBEX: IrDA Object Exchange
IrDA: Infrared Data Association
BT: Byte
USB: Universal Serial Bus
RS232: "An Electronic Industries Alliance (EIA) physical interface specification for serial data connections. Originally introduced in 1962, RS-232 (sometimes presented as "RS 232") is the most commonly employed interface between computers and modems. As the EIA and its telecom subgroup, the Telecommunications Industry Association (TIA), have released updated versions over the years, the formal name of the specification has changed — for example, to "EIA-232-D," "EIA/TIA-232-E" and, most recently, "TIA/EIA-232-F." Regardless of the version, however, the specification is still commonly referred to by the original "RS-232" appellation." [6]

Figure 7: PCD architecture



Source: Mobile Electronic Transactions Forum (MeT)

Application: a PCD application, like a browser
Standard Security IF: is a (de facto) standard interface, like Microsoft CAPI (MSCAPI) or PKSC #11.
Customer interface: contains customized functionality e.g. implemented as a browser plug-in.
PTP API: is an interface to the PTP requestor.
Data Exchange Manager: is an entity that manages connection & data exchange to the PTD.

2.1.2 Payment/Transactions Infrastructure

The IT and technology levels, as regards customer care and transaction platforms of mobile operators (Figure 44) and banks (Figure 45) , don't differ much. This 'indifference' has been the result of a number of factors, including "evolutions of both layered communication systems architecture, and of banking software systems architecture," resulting in a faster evolution of the mobile networks in comparison to fixed networks. In addition, "the security levels offered by mobile networks inside the infrastructure are on par with those in banking software, not the least because of added security hardware gives. This means that:

- For a mobile operator to operate also as a payment clearinghouse, is a relatively minor issue, provided the fulfilment systems comply with inter-banking data formats, which they do even more and more.
- For a bank to act as a virtual operator using a third party's access network, is also a relatively minor issue if subscriber data are tagged with bank customer file data, which they do even more and more." [7]

2.2 Standards

Before starting with the standards that are used for mobile banking/payment services, some interoperability requirements that need to be satisfied are mentioned first.

2.2.1 Interoperability Requirements

Interoperability is very critical in deploying services like mobile banking. Without interoperability at various levels: device-to-network, device-to-device, network-to-network etc., it is very unlikely that the content or service is going to be espoused by the mass market. Though achieving interoperability is not an easy task, as new services like mobile banking are developed with inputs from different industries, where the meaning and reliance upon standardization and interoperability differ.

As mentioned in the previous paragraph, without interoperability markets may fail. The policy objectives regarding the endorsement of service diversity and competition could be adversely affected by this, resulting in the need for regulatory intervention. The Directive 91/250/EEC addresses the interoperability issue and encloses certain provisions allowing for interoperability in particular circumstances. Moreover, in case of refusal by a dominant supplier to make information public that is needed for interoperability, as required by the Directive, "the Directive is without prejudice towards the application of competition rules". [8]

Obviously, manufacturers of mobile devices are popular partners for banks as well as for operators. So standards set in these different sectors will have to be considered, in addition to the legislation provided by the EU. Table 46 presents interoperability issues dealing with the particular aspects of GSM/WAP environment. “The intent is to identify specific algorithms, data formats and services that are not part of a PKI designed for a traditional wired network.” [9]

2.2.2 Payment protocols

Mail order/telephone order: The card number is send to the merchant over phone, followed by a request for authorisation and receipt of it by the merchant. The purchase is confirmed by the merchant and settlement takes place via the normal card payment route.

Interoperability Domain Security Protocols: The choice as to which protocol – 3D Secure, 3D SET, SPA or other - should be used is determined by the issuer and may vary depending on the situation. Moreover, the end authentication method is also selected by the issuer and may vary according to the purchase in question. “This authentication method may well involve a password-based mechanism at the beginning, the upgrade path and preferred solution being a dual chip phone with a WIM and digital signature capability.” [4]

- *3D Secure:* A checkout page using SSL is submitted by the cardholder, followed by a verification by the merchant. Subsequently, the cardholder is redirected to the issuer, who displays the payment details and requests the entry of a secret code. If successful, the issuer will sign the payment message, redirecting the cardholder to the merchant and providing a signed response message. The issuer’s signature is authenticated and stored by the merchant, processing the transaction as normal.
- *3D-SET:* A checkout page is submitted by the cardholder via the “pay with SET” button and a predefined “Wake-Up” message is send to the Wallet by the merchant. After the validation of the cardholder to the wallet, a SET purchase initiation is send to the merchant by the wallet. Moreover, a payment authorisation is requested and received, followed by a confirmation message to the cardholder. The receipt is generated and stored in the wallet.

EBPP (electronic bill presentment and payment): a distinction between two main steps can be made:

1. Bill generation: EBPP is selected as a payment tool by the customer. The merchant generates a bill and forwards it to the bank, which is the consolidator.
2. Transaction step: After the customer has logged in, the bill is presented to and accepted by the customer. Settlement takes places and the payment is confirmed.

One-time credit card number: Upon connection to the bank’s WAP site (SBW), the cardholder can download a one-time number which is to represent his credit card. This number can be submitted to the merchant, who can then request authorisation via the standard payment scheme network. Upon receipt of authorisation, a confirmation is sent to the cardholder.

EMV: EMV is a payment protocol designed by Europay, MasterCard and Visa International, mainly for local card payments. There are two implementation alternatives of EMV: static and dynamic.

1. “In the static EMV, the signature is verified by symmetric means, i.e., a DES-based Authorization Request Cryptogram (ARQC) is sent to the issuer for verification.
2. In the dynamic version a PKI system is being used, and the digital signature is sent to the issuer for verification. Technically it is possible to use EMV with the dynamic implementation option for remote payments but the feasibility of that option is yet to be evaluated.”[4]

The process of EMV is as follows: The POS is informed that EMV is the preferred payment mechanism, upon which the merchant’s POS requests customer authentication from the EMV application on SE. When the merchant has received an authorisation response, the cardholder gets a confirmation message. The off-line process differs as it does not involve the automatic transmission of an authorisation request, rather the authorisation is either based on the profile information on the chip or an on-line request is send. [4]

2.2.3 Financial Standards

2.2.3.1 Banking Standards

The banking standards are defined by The European Committee for Banking Standards, which was formed in December 1992 by Europe’s three credit sector associations: the Banking Federation of the European Union, the European Association of Co-operative Banks, and the European Savings Banks Group (collectively known as the European Credit Sector Associations (ECSAs)).

There has been a steady increase in the interest to have the possibility to influence payments through mobile devices. Banks and mobile operators in Europe are working on the development of new mobile payment/banking services in addition to new solutions. These developments have resulted in a multitude of solutions. Consequently, there is a need for the development of a standard in the field of mobile payments.

The member banks of ECBS, having developed thorough business and functional requirements, are now turning their attention to building consensus on issues like implementation architecture, interoperability (Table 47) [10]. More and more banks are realising that cooperation with mobile network operators may eventually be vital to the mobile payment strategy of the bank. TC6/WG4 will also monitor and influence relevant initiatives with the European Commission, ETSI and CEN/ISSS.

2.2.3.2 The de facto standards and interoperable payment platforms of banks and payment institutions

A number of attempts have been made in the European Union, in order to support emerging mobile payment solutions. Most of the companies dealing with the mobile market, including banks, mobile operators, hardware and software developers try to achieve standardisation by means of international forums or consortia. The purpose is to achieve an approach that is widely acceptable, having the capability of reaching global audiences. Until now the following main consortia [11] have arisen:

- Mobile network operator driven:

1. Simpay (www.simpay.com)
2. Starmap Mobile Alliance, GSM Association (www.gsmworls.com)
3. ETSI (www.etsi.org)
4. UMTS forum (www.umts-forum.org)

- Bank driven:
1. Mobey forum (www.mobeyforum.org)

- Cross-industry driven:
1. Mobile payment forum (http://mobilepaymentforum.org)
2. Mobile payment association (http://mpa.ami.cz)
3. Paycircle (www.paycircle.org)

-Device manufacturer driven:
1. Mobile electronic transactions (www.mobiletrasactions.org)

- Technology driven:
1. Open Mobile Alliance (OMA) (www.openmobilealliance.org)
2. Infra-red data association (www.irda.org)

- Identity driven:
1. Radiccio (www.radiccio.org)
2. Liberty Alliance (www.projectliberty.org)

Some consortia have merged and are working together, while others e.g. Simpay did not survive and have been abandoned. More significantly, the Mobile electronic payment transaction consortium has been merged inside OMA (and MeT is only mentioned for "historical "reasons); also UMTS work has migrated to 3GPP Application group, itself strongly linked to GSM Association. OMA on its own has added new working groups not represented by past fora. This evolution does not help users get a stable impression .

Mobile Payment platforms:
The solutions generally used by mobile operators consist of proprietary billing, from vendors like Kenan (recently acquired by Lucent), Logica or LHS. The aforementioned platforms have not been designed for charging for particular content, rather per minute of standard voice, SMS and premium rate calls are charged.

"Payment solutions targeted especially for the mobile market have been developed, for example, by start-up More Magic Software, which is financed by Siemens' Mustang Ventures. This Finnish company has developed MBroker, a micro-payment platform that lets mobile operators bill for diverse content and services rather than a per minute basis using a variety of payment methods. Brokat is offering one of the leading e-payment solutions with its Twister platform." [12]

Mobile banking platforms:
Mobile banking platforms and solution providers are emerging quickly. An overview of the main mobile banking and broking technology players is given in the following table [12]:

Table 12: Main M-banking and M-broking technology players

Category	Suppliers
Mobile financial service providers	Aether Systems, w-Trade and EmailPager (all US); Multichart, Teledata
Mobile data service providers	GIN (acquired by Saraide.com), Research in Motion, Multichart
Mobile software developers	Brokat, Yellow Computing, Netlife, Aspiro, DataDesign
Mobile system integrators	IBM, HP, Logica
Mobile communications SW/gateway companies	Apion (acquired by Phone.com), Phone.com, Nokia, Digital Mobility, 724 Solutions (Citibank with Sonera), Sonera SmartTrust, CMG

Mobile operators	Mannesmann Mobilfunk, T-Mobil with T-Online, Cellnet, Cegetel/SFR, NTT DoCoMo, Swisscom, Telia

Source: Durlacher

FINREAD:

FINREAD stands for Financial Reader, an EMV compliant chip card reader, and is the result of a Consortium of major European organisations, including six key payment systems: Banksys (Belgium), Interpay Nederland (The Netherlands), SIZ (the computer processing centre of the German Savings Banks), Europay International Visa EU and Ingenico and the leading card reader manufacturer. The consortium is coordinated by the French Groupement des Cartes Bancaires "CB", with support of the European Commission. FINREAD's functional concept is based on a Virtual Machine, in this case JAVATM, an existing standard. [13] [14]

The purpose of FINREAD is to address two main issues: security and interoperability. As a result of the interoperability stipulated by FINREAD, it provides the possibility to download various applications by different application providers into any FINREAD compliant card reader. Furthermore, the card reader authentication can be performed by cryptographic functions with the frequently used algorithms (DES, MAC, MD5, SHA-1) or with the asymmetric RSA algorithm. [14]

The de facto standards:

As the displays of most devices have certain constraints such as limited graphical capability and size, 'as well as entering complex alphanumerical text messages'; the infrastructure of the mobile payment should take into consideration these limitations. Moreover, the payment application should be restricted to a minimum number of data elements and format, complying with e.g., the ICC specifications.

- ***Protocols:***

De facto standards as UCP or SMPP should be used by the protocols between the telecommunication network and the banking environment.

"Protocols within the telecommunication network shall comply with telecommunication standards and allow for transparent transfer of messages and data from the banking environment to an application in the mobile device, regardless of the original format, for example, binary encrypted data blocks." [15]

- ***Data elements:***

An overview of data elements that may contain payment-related messages, is provided in Table 48. These data elements, facilitating conversion into standards used by banks, are derived from standards like ISO 8583, EMV and CEN ENV 1750/APACS 60. [15]

- ***JAVA Standards:***

The Java standards are driven by the Java Technology Community. The platforms and technologies critical to operators are:

J2ME Technology: JAVA 2 Micro Edition. A programming environment for mobile devices.

XML: Extensible Mark-up Language.

JAIN: JAVA APIs for Integrated Networks.

See Figure 49 for the JAVA Architecture and Figure 50 for the J2ME platform architecture.

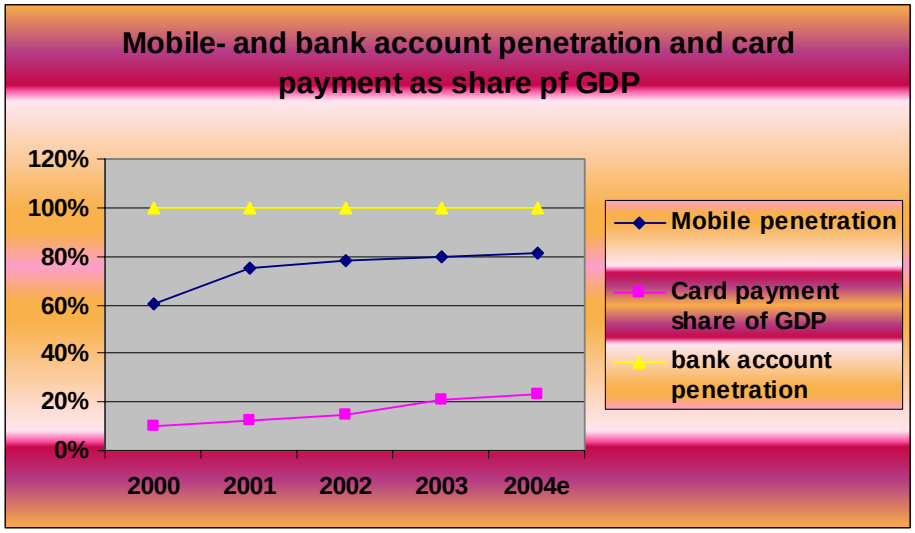
JSR 229 Payment API: It defines the APIs for initiating mobile payments from JAVA applications.

JSR 177 Security and Trust API: APIs providing security and trust are specified by integrating the Security Element. These features can be used by the J2ME services to handle value-added services like banking, payment, user identification and authentication. [16]

2.3 Business Estimation Case

The following figure shows a comparison between three types of payments' penetration in The Netherlands as a share of GDP: mobile penetration, card payment penetration and bank account penetration.

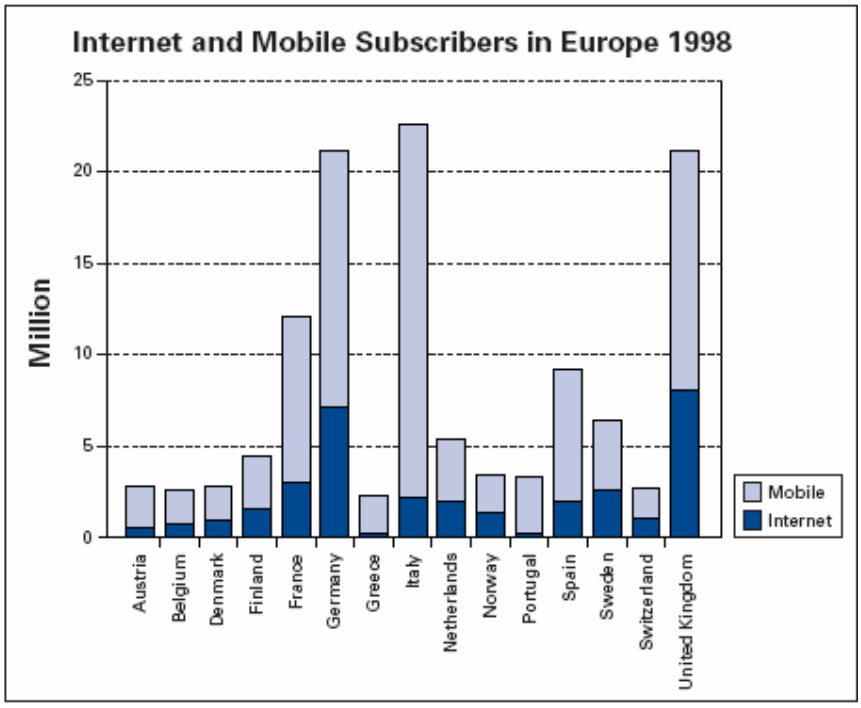
Figure 16: Mobile penetration, bank account penetration & card payment penetration as share of GDP [17]



Source: Little, A.D. Ltd

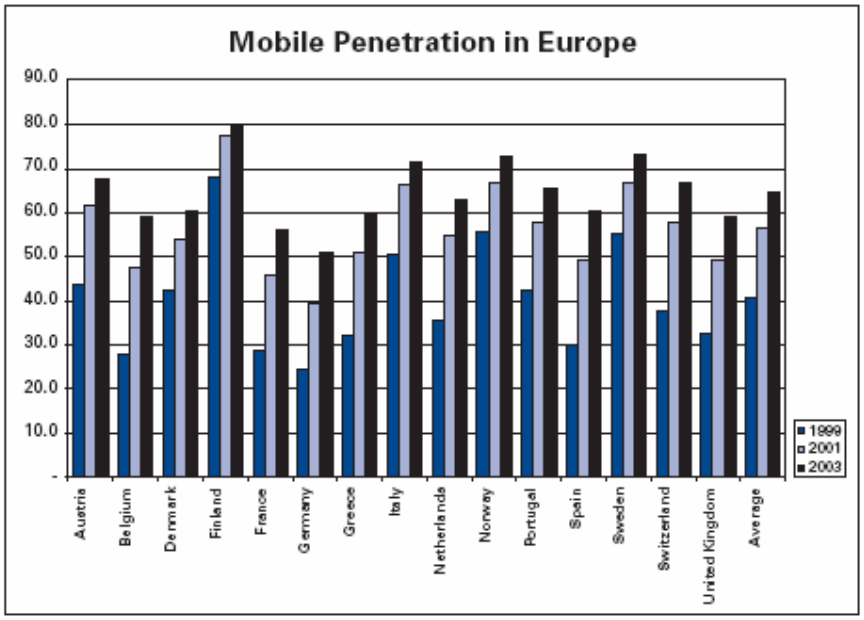
The following figures shows the mobile users and service penetration in Europe.

Figure 17: Mobile and internet subscribers in Europe



Source: Durlacher

Figure 18: Mobile penetration in Europe



Source: Durlacher

As can be seen from the above figure the penetration rate in Europe: a comparison is made between 16 countries in Europe about mobile service penetration. The Netherlands

is in the 9th place, so amongst the lowest 56.25%. While in terms of numbers of mobile users The Netherlands belongs to the top 43.75% (7th place). So, while the number of mobile users is quite high compared to many other European countries, the penetration of mobile services is quite low compared to many other European countries.

Based on some assumptions a business estimation case has been made. The assumptions made are as follows:

- All the business case estimations are based on electronic payment transactions for the year 2004. The number of mobile payment transactions was calculated by multiplying the penetration rate with the number of electronic transactions per year.
- The growth rate of electronic transactions is assumed to be 1% for the years 2005 – 2010.
- The growth rate in the number of mobile subscribers is assumed to be 5% per year for the years 2004 – 2010.
- Fee on the m-payments for the process chain actors are assumed to be €0,01; €0,10 and €0,20 (transmission costs are not included)
- The first business estimation case and revenue estimation is based on the assumption that M-payment penetration rate is 1% per year.
- The second business estimation case and revenue estimation is based on the assumption that M-payment penetration rate is 5% per year.

As can be seen from Table 51 about the revenue estimation, that the potential benefits that can be derived are considerable, even if the underlying assumptions made for this business case are not very optimistic and considerably realistic.
Figure 52 shows the development of m-payment transactions using a penetration rate amongst users of 1% and 5% respectively . As can be seen there is a considerable difference between the number of transactions based on these two alternative end user penetration rates.
Figure 53 shows the revenue estimation for M-payment services based on end user penetration rates of 1% and 5%. This graph shows clear revenue benefits from m-payments. Moreover, this graph clearly illustrates how sensitive the revenue estimation is with respect to the penetration rate. As can be seen the differences between the revenue estimations, when the penetration rate is 1% and when the penetration rate is 5%, are substantial. Moreover, the higher the fee revenue per transaction is, the higher the differences between the revenue estimations.

Taking extremes :

- An end user penetration rate of 1 % and a low fee /transaction of € 0,01; yields in 2008 a M-payment fee revenue base in the order of € 361.818 for the Netherlands.
- An end user penetration rate of 5% and a higher fee/transaction of € 0,20; yields in 2008 a M-payment fee revenue base in the order € 18.090.901 for The Netherlands.

3. Regulatory Framework for M-Banking

Regulatory efforts can obstruct the operation of flexible mobile payment applications, which have been designed to satisfy various customer needs all at once. Thus a mobile payment solution that aims at offering person-to-person transactions as well as payments may have to conform to several different regulations. There are several legal issues to be considered when it comes to mobile payments. Money laundering, market regulation, customer protection issues such as credit offering and fraud, and cross-border transactions are the most important and commonly addressed.

Though, before having a look at the regulatory framework, it needs to be mentioned that regulatory bottlenecks are out of the focus of this research report.

3.1 EU Regulatory framework

This chapter addresses various issues that might be relevant in the context of the legal framework for retail payments.

3.1.1 Legal measures to be considered regarding the allocation of legal responsibility and customer protection in case of system breakdowns/disruptions

A very important issue is the relationship between the cardholders and card-issuers, addressed by the Commission Recommendation 97/489/EC. It specifies the obligations the issuer and the holder are subject to. Issues like when the card-issuer is liable and what the amount of liability should consist of, what the responsibilities of the card-holder are etc., are addressed by this Recommendation. Moreover, it is outlined that in case of 'lost amount of value stored on the instrument' and 'defective execution of the holder's transactions' as a result of a failure of the 'instrument, of the device/terminal or any other equipment authorised for use', except if the malfunction was intentionally caused by the holder. [18]

3.1.1.1 Legal responsibility in case of a payment network breakdown

Payment systems have become more vulnerable to technical breakdowns because of the increased sophistication of the technical infrastructure, and the reliance upon them. A considerable risk might be created for payment providers and their customers, in case a disruption in the system or data transmission/funds transfer takes place. This leads to new legal responsibilities and problems. Legal uncertainty, concerning this issue should, as far as possible, be removed. [19]

Moreover, further complications about the question of legal and technical responsibility arise, if some components of the payment process are outsourced to third parties. This would mean that the payment system includes different parties, resulting in the fact that the participating institutions, also become susceptible to third-party system breakdowns, in addition to being vulnerable to such breakdowns in their own systems.

The economic loss as a consequence of such problems as disruptions in the system can be considerable. Both the customer and the payment provider can suffer a loss. For example, in case of operational disruption the customer might not be able to make a transaction or payment. Consequently, the question of consequential damage arises.

"The Commissions' services are not convinced that the legal issues are appropriately addressed." Listing all the relevant issues in this context and then discuss their relevance

as regards the legal framework might be useful. The results of these discussions might be constructive in the allocation of the legal responsibility, ensuring that the efficiency and security of payments is not impaired and guaranteeing protection of the participants. [19]

Consequential damage:
No specific rules regarding consequential damage exist in the current EU-legislation for payments. "In the (REP) concerning transactions carried out by electronic instruments. Article 8 (3) stipulates that financial consequences above the amount of the non-executed or defectively executed transaction and interest thereon as well as the sum required to restore the holder of the payment instrument to the position he/she was in before the unauthorized transaction took place, are born by the issuer in accordance with the law applicable to the contract concluded between the issuer and the holder. A similar provision can be found in Article 6.4.of (DCT)." [19]

3.1.1.2 Identification of the originator in the payment process

For transferring funds in a cost effective way it is important that data regarding the originator, beneficiary etc. are integrated throughout the intact payment process in a standardized form. For establishing STP this is a precondition.

"Public policy objectives, such as those relating to hindering money laundering, imposes also obligations for information processing in the payment process." The Council Directive 91/308/EEC on prevention of the financial system for money laundering, also requires identification of the customer. It is stated that: "credit and financial institutions require identification of their customers by means of supporting evidence unless the customer is also a credit or financial institution. Derogations are laid down for certain insurance policies." [19] [20]

3.1.1.2.1 Money Laundering

The Directive with regard to money laundering that is worth mentioning here, is the one concerning preventing the use of financial systems as mentioned in the previous paragraph. The objective of this Council Directive, Directive 91/308/EEC is: "to prevent the use of financial system for money laundering without impeding the freedom of capital movement and the freedom to supply financial services (i.e. impeding the freedom spelt out in the EC Treaty)." [20]

The purpose of this Directive is combating money laundering at community level. The relevant texts applicable at an international level are the 40 recommendations of the 'Financial Action Task Force' (FATF). This Directive though has been amended by Directive 2001/97/EC. The purpose of the latter is to update and extend the scope of the former.

Furthermore, credit and financial institutions are required to develop procedures for internal control and communication to ensure that money laundering operations are minimised. [20]

3.1.1.2.2 Privacy

**** Data protection in the electronic communication sector:***
The objective of Directive 2002/58/EC is to ensure that users rights with regard to privacy are preserved. The Directive tackles various issues that assure that the user can trust the services / technologies used for electronic communication, e.g.

sending unsolicited electronic messages and inclusion of personal data in public directories. [21]

**** Protection of personal data:***
The reference text, on protection of personal data is Directive 95/46/EC. The purpose of this framework is to create a balance between high level privacy protection and free movement of personal data within the EU. To do so, the Directive includes stipulations requiring the Member States to set up independent national bodies responsible for data protection. In addition, limits are set for data collection. [21]

3.1.2 Digital certification services in the payment sector

A general legal framework for e-signatures is established by the Directive on Electronic Signatures. The purpose of this Directive is to ensure legal recognition, as well as allowing free circulation within the Internal Market. In addition, minimum liability rules for service providers are established. Moreover "minimum requirements for qualified certificates, certification service providers, secure signature creation and verification devices" are listed. [22]

In the field of digital certification, identification and authentication of the parties involved in the payments process are, in addition to the integrity of the electronic messages, essential for the establishment of secure payments and particularly for on-line transactions.

It seems that all kinds of authentication methods are covered by the definition of e-signatures. Furthermore, "advanced electronic signatures" (AES) are also introduced by the Directive.

Technical requirements for 'AES' are not specified by The Directive, leaving that to the Electronic Signature Committee. In this respect, the European Committee for Standardisation (CEN) and European Telecommunications Standards Institute (ETSI) within the European Electronic Signature Standardisation Initiative are providing a European platform. These organisations have developed standards in accordance with the requirements of The Directive. Additionally, national accreditation schemes are allowed, resulting in diverging practices. A clarification of the technical requirements as far as 'AES' is concerned in the area of payments is enviable.

An increasing number of initiatives regarding the notion of Public Key Infrastructure (PKI) have started to emerge, in the field of e-commerce/m-commerce. A legal framework concerning e-signatures, that is clear and comprehensive, and where security and legal certainty are particularly important, is needed. For making the full deployment of e-signatures in the Internal Market it is also important that there are no legal or technical barriers. [19] [22]

Legal Requirements
The European Union has passed the Electronic Signatures Directive, which has to be implemented (2001). This law implies that a digital signature meets the juridical condition for a document to be accepted as signed. The European Electronic Signature Initiative (EESI) is the leading developer of an international standard for digital signatures in Europe. [19] [22]

3.1.3 Security of payment infrastructure

Ensuring the security of payment systems requires the security of communications networks and information technology. In order to protect the systems and transactions against unauthorized access, higher levels of security are required.

The Cyber-crime Convention has been adopted by the Council of Europe in order to address issues related to cyber-crime, at an international level. It stipulates the rules to be followed and sanctions for actions as regards "confidentiality, integrity or availability of the system, network and data." [19]

EU legislation against fraud and counterfeiting non-cash means of payments was adopted, in the payment systems field. This framework Decision is intended to list behaviours concerning payment transactions, which are considered as a criminal offence. One can think of intentionally altering/deleting a payment transaction, restraining computer data or interfering with the functioning of the computer system. The Fraud Prevention Action Plan is used to discuss preventive measures as security requirements and the like.

** Preventing fraud and counterfeiting non-cash means of payment:*
A three year Fraud Prevention Action Plan was carried out during 2001-2003. The aim was to reduce fraud and unlawful credit card payments. The objective was to tackle all issues considered as 'fraud', slowing down the development of e-commerce.

A new action plan has been developed to prevent fraud on non-cash means of payments for 2004 – 2007:
The objective of the Action Plan is as mentioned before prevention of fraud on non-cash means of payment. It "supplements the new Directive on payment services which the Commission intends to present in 2005." [23]

EU ACT: "Communication from the Commission to the Council, to the European Parliament, the European Central Bank, the Economic and Social Committee and Europol – preventing fraud and counterfeiting of non-cash means of payment." [23]

According to the Commission close cooperation between the private sector and the public authorities is indispensable in combating fraud effectively. Moreover, effective implementation of preventive measures requires an amplification of both Community and national data protection legislation in relation to fraud prevention, which will allow effective exchange of information at European level. "The integration of the ten new Member States into the Community fraud prevention framework prevention will continue to be a priority. The same applies to the strengthening of relations with public authorities in third countries." [23]

3.1.4 The EU competition law

It covers the abuse of dominant position and agreements between competitors which have a restrictive effect on trade. "The rules for European competition law are contained in Articles 81 and 82 of the Treaty of Amsterdam which have been reproduced in Articles

53 and 54 of the European Economic Area (EEA) and are therefore applicable in all 29 (25+4) States of the EEA."[1] [24]

3.2 Dutch Regulatory Framework

The general framework underlying payments and securities in The Netherlands contains numerous general laws as well as private law. An overview of the main provisions governing payments can be found below.

3.2.1 Legal aspects in respect of payments

The External Financial Relations Act includes provisions on external payments, like the "obligation to report certain transactions for the benefit of the compilation of the balance of payments." [3]

The Act on cross-border payment services, which was designed for the implementation of Directive 97/5/EC of The European Parliament and the EU Council of 27 January 1997, encloses requirements with respect to transparency and quality of cross-border payments.

In view of prevention of money laundering, the Identification Financial Services Act has been adopted. This Act compels that financial institutions ascertain the identity of the customer who wishes to effect a particular payment. "In line with this, the Disclosure of Unusual Transactions (Financial Services) Act provides that staff of, for instance, banks must report unusual transactions to a central Disclosure Office. In addition to these Acts, the Exchange Offices Act requires that exchange offices be registered and that their Directors be trustworthy." [3]

"On 1 January 1999 the Finality Act of 17 December 1998 came into force, which seeks to guarantee the final nature of the settlement of transactions in payment and securities settlement systems. To that end, the 1992 Act on the supervision of the credit system and the Bankruptcy Act were amended. This Finality Act is also designed to implement the Directive on settlement finality (Directive 98/26/EC). Under this Act, a court decision involving the invocation of the emergency regulation, an adjudication of bankruptcy or suspension of payment in respect of certain parties does not – by contrast with the zero-hour clause – affect retroactive payments made by these parties in the systems designated. It ensures the secure functioning of the payment and securities settlement systems. On the recommendation by De Nederlandsche Bank, the Minister has meanwhile designated a number of systems." [3]

3.2.2 Legal aspects with regard to internet banking

No particular regulations regarding internet banking are specified by De Nederlandsche Bank (DNB). Though, the 'Act on the Supervision of the Credit System 1992' and the 'Regulation on Organisation and Control' provide a general framework to which banks must adhere. [25]

3.3 Legal aspect with respect to Intellectual Property Rights

[1]" Within the broad framework of Articles 81 and 82, it is the Commission's task to administer competition rules of the Treaty for the States of the European Union."

3.3.1 Enforcement of Intellectual Property Rights

For the success of the internal market, the protection of intellectual property is essential. Not only is it vital for the promotion of innovation, but also for developing employment and the improvement of competitiveness. That is the reason, why establishing effective means for enforcing IPRs, is paramount. To this end, the below mentioned Directive "seeks to create equal conditions for the application of IPR in the Member States by aligning enforcement measures throughout the Union. It also aims to harmonise Member States' legislation in order to ensure an equivalent level of intellectual property protection in the internal market.

EU ACT: Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of IPR". [26]

3.3.2 Technology transfer agreements

In general licensing agreements are prohibited, as they restrict competition. The applicable rules are contained in Community competition rules, in particular in Article 81 of the EC Treaty. Though, in some cases such agreements can have a positive impact offsetting the restrictive effects on competition. So, the new stipulations include a "block exemption" regulation and guidelines, generating certainty with respect to most of the licensing agreements.

EU ACT: "Commission regulation (EC) N0 772/2004 of 24 April on the application of Article 81 (3) of the Treaty to categories of technology transfer agreements." [27]

4. Market shares and ownership conditions for payment agents in The Netherlands

4.1 Market share estimation

In addition to the various processing systems of the banks themselves, there exist two widely used payment processing and clearing systems in The Netherlands: TOP and Interpay. The competition between these different systems is on the one hand good for the customer, as the fees might eventually be subject to it. It is not the sort of thing that you think about, but payments also cost money. On average, each POS transaction costs €35 cents, even though that figure is never shown on the bill. The direct debit terminal on the counter, the cash dispenser in the wall, secure transport of bank notes and coins are just part of this. [28]

The following graph shows the market share of Interpay and TOP vs. the internal systems at banks and elsewhere. However this ownership structure is based on a number of assumptions. See Appendix 2 Tables 54.x and Appendix 3 Tables 55.x for additional information used in determining the market share.

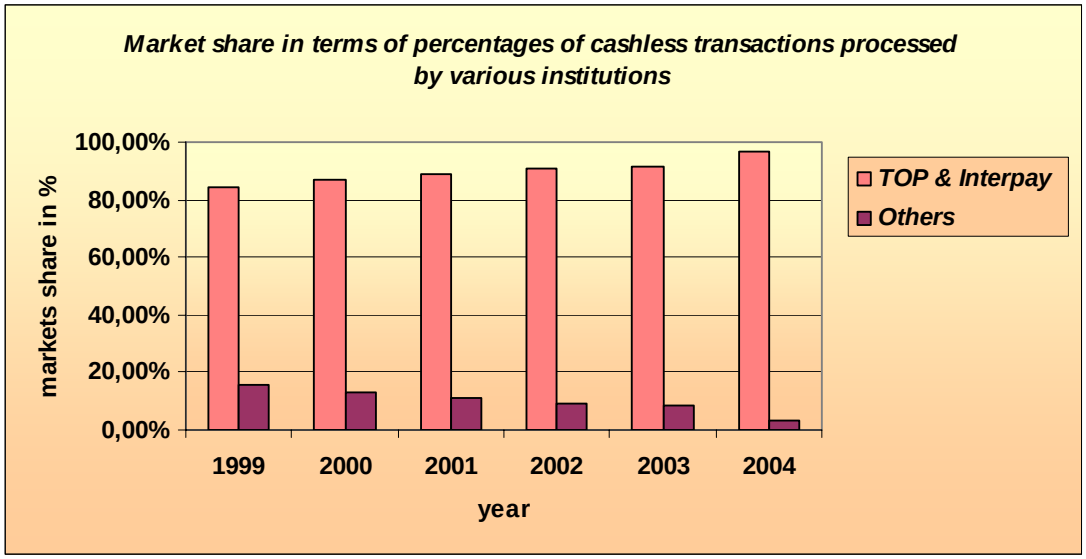
- The total number of mobile subscriber evolution is based on statistics from OECD[2].
- The total cashless payment transactions are derived from the ECB bluebook.
- The cashless payment transactions processed by TOP & Interpay, include cashless payment transactions processed by TOP, Interpay and credit card institutions as mentioned in the DNB bluebook/annual report. The cashless transactions processed by them separately could not be derived, as that information was unavailable.
- The difference between the two (total cashless transactions processed in The Netherlands as mentioned in ECB's bluebook and cashless transactions processed by

[2] Source: http://oecd-stats.ingenta.com/OECD/eng/TableViewer/wdsview/dispviewp.asp

TOP & Interpay and credit card institutions as mentioned in DNB's bluebook/annual report) is assumed to be the number of cashless transactions processed by the processing systems of various banks themselves.

- The total number of cashless transactions in The Netherlands, as indicated in the ECB bluebook, includes the number of transactions by cheques. So, payments by means of cheques were subtracted from the total number of cashless transactions, because the number of cheque transactions as mentioned in the DNB annual report of 2004 were also excluded. Transactions by cheques were excluded because these transactions are paper based. (The total electronic transactions as indicated in the annual report of DNB include: Debit card, Credit card, E-purse, Direct debit, Electronic transfer; while the total number of cashless transactions as mentioned in the ECB bluebook include, excluding the cheques: payments by Debit card, payments by Credit card, Credit transfers, Direct debits, Card-based electronic money and Network-based electronic money).
- The total cashless transactions processed by Interpay, TOP and credit card institutions for the year 2004 are an estimate derived by the DNB.
- Figures for the total cashless transactions in The Netherlands, as mentioned in the ECB bluebook, were unavailable for the year 2004. Therefore a growth rate of 1% was assumed in order to estimate by extrapolation (applying the 1% rate to the number of transactions in 2003) the total cashless transactions in The Netherlands for the year 2004.

Figure 26: Market share in terms of percentage of electronic transactions processed by various institutions:



4.2 Ownership and organisational conditions for payment agents in The Netherlands

- **Interpay:**

"Interpay Nederland B.V. is the central clearing institute set up by the banks with a view to promoting and maintaining efficient payment processing and reliable payment

systems. In order to facilitate the collection and processing of retail transfers between their customers, the banks formed a common clearinghouse in 1967, which is now called Interpay. Originally, Interpay was formed as a result of a merger between BankGiroCentrale, BeaNet and Eurocard. The banks are both its shareholders and customers. Interpay is the clearing institute for retail payments. It runs the network of POS terminals and the inter-bank authorization network for cash dispenser transactions and issue credit cards ands provides image-processing services to individual banks."
Currently, Interpay provides the possibility to recharging your prepaid phone balance. On the website of Interpay it is mentioned that Interpay will expand the mobile services range in the near future, while providing services like: 'm-ticketing', 'm-parking', and 'm-tertainment'. [3] [29]

- **Internal bank systems:**

It should be noted that apart from the clearing, which takes place through the facilities provided by Interpay, a considerable amount of retail transactions are processed at the large banks themselves, using in-house processing facilities. Since the banking sector is highly concentrated, a large number of payments are for transfers between customers of the same bank. Consequently, some of these in-house payments do not reach the clearing house, but are transmitted to the individual banks' processing centres.

- **TOP:**

" TOP is the name of the real-time gross settlement system of De Nederlandsche Bank. It has been designed for processing and settling large-value payments in euro. TOP is not an acronym. Rather, the system is named after the market sector in which it operates: the "top", i.e. the sector handling the largest-value payments in The Netherlands. The TOP system only handles credit transfers on a gross basis, which means that in the event of inadequate cover for a debit transaction on a participant's current account, either a credit balance or an unused collateralised overdraft are used. For this purpose, a queuing mechanism has been developed." [3]
In addition, access to TARGET is provided by TOP. TOP uses S.W.I.F.T., the international inter-bank communication system, for processing its transactions. TOP also provides services on behalf of Interpay, as Interpay is also a client of TOP. These services include amongst others: "settlement transactions in the context of bulk payments (debit card transactions and in-payment transfers)." On the provision of mobile services nothing was mentioned, so we assume that mobile transactions are not processed by TOP.

For a comparison of TOP and Interpay see Appendix 3 Tables 56-57.

- **TARGET:**

"The purpose of De Nederlandsche Bank's current account system is to offer current account facilities to banks and to the government, thus permitting the settlement of payment transactions." TARGET is used for cross-border payments. [3] [29]

- **Continuous Linked Settlement (CLS): the bridge between TOP and TARGET**

ABN AMRO, Rabobank and ING Bank, participate through TOP, while Fortis participates via the Belgian payment system ELLIPS in CLS bank. The CLS banks is a worldwide clearing and settlement system for transfers. [30]

Figure 27 : Payment and Securities settlement systems and overseers

Payment and securities settlement systems and overseers		
	Assessment of setup	Assessment of operation
Payment systems		
Interpay	DNB	DNB
TOP/TARGET	DNB	DNB
SSSs		
Euronext Amsterdam Stock Clearing	Au-FM/DNB	Au-FM
Euronext Amsterdam Derivatives Clearing	Au-FM/DNB	Au-FM
NIEC	Au-FM/DNB	Au-FM
Necigef	Au-FM/DNB	Au-FM
NLKKAS (Euronext Amsterdam Commodity Clearing)	Au-FM/DNB	Au-FM

Source: CPSS Redbook, Payment systems in The Netherlands

5. Deployment Scenarios

5.1 Mobile Financial Services

Taking financial services to the mobile devices provides a new service channel to banks as well as operators. There are various kinds of mobile financial services. Below are some examples [12]:

- **Mobile Banking:**

The services that are mostly considered to be offered through mobile banking are:
- "Check exchange rates
- Check interest rates
- Check account and credit card balances
- Administer credit lines
- Check interest earned on deposits
- Check last transactions
- Transfer funds
- Pay invoices
- Apply for credit line"

- **Mobile Broking:**

The following key functionalities are provided by mobile broking:
- "Receive alerts about price movements
- Receive message when order is executed
- Check quotes
- Manage portfolios
- Buy and sell stocks, options, mutual funds, other financial instruments
- Browse and delete existing orders"

- **Mobile Cash:**

"Mobile electronic cash refers to loading cash onto a stored value card via the wireless network. It is also referred to as mobile ATM or mobile phone cash machine."

- **Mobile Payments:**

"There are three ways in which a customer can purchase a product/service from a vending machine or the internet using a mobile device:

- Dial a premium rate number (0900) which has a call charge equivalent to the product price.
- Dial a prefix plus a premium rate number to indicate that the product should be charged to a different bill (important for users for corporate mobile).
- A pre-standing agreement for credit card payments is put in place. For authenticity, a PIN has to be entered at the time of purchase."

- **Mobile E-bill:**

"You can receive electronic bills to an e-mail address or mobile phone, which can be paid via semi-direct debit from the handheld terminal."

- **Mobile E-salary:**

Employees receive their monthly pay-slips via e-mail or via SMS to their mobile phones.

Besides these mobile financial services there are other services that can be provided by means of a mobile device. Following are some examples:

- **Mobile security services**
- **Mobile shopping:**
  - mobile retailing
  - mobile ticketing
  - mobile auctions
  - mobile reservations
  - mobile postcard
- **Mobile dynamic information management**
- **Mobile information provisioning**
- **Mobile entertainment**

As these mobile services are beyond the scope of this research report, a detailed description of these services has not been included.

5.2 M-Banking services provided by various banks in The Netherlands

As can be seen from the previous section there are a wide range of applications for which the mobile device can be used. In this section the banking services that are actually provided by various banks in The Netherlands are covered.

- **Rabobank:**
  - Enquiry about account balances
  - Check information with regard to money transferred from or to your account
  - Detailed information about transfers between your accounts
  - Transferring money between your accounts
  - Payment via accept-giro or via bank-giro
  - Checking transactions that are made for once or automatically
  - Changing your entry code [31]

*** Rabo Alerts:**

- Alerts regarding investment portfolio and stock exchange

- Confirmation whether your orders have been placed
- Automatic alerts: when money is transferred from any of your accounts or to any of your accounts
- Alerts and latest news regarding cycle-racing [32]

*** Mobile Investing:**
- Real-time stock exchange rates of the AEX and other information
- Placing orders via 'voice-recognition' or 'Rabo orderlijn'
- Asking practical questions about investments to the personnel from 'Rabo Service Centrum Beleggen'. [33]

*** Top up your balance:**
- Top up your balance if you have a pre-paid phone of Vodafone or KPN [34]

- **ABN AMRO:**
  - Checking account balances
  - Making payments
  - Manage your investment portfolio [35]

*** Access to the mobile link of ABN AMRO, on which:**
- Information about all ABN AMRO services, including ATM locations and service numbers
- Detailed and up-to-date news about the stock exchanges, news about home and abroad and about e-commerce
- For on the way: information about public transportation and traffic [36]

*** SMS-based services (both on request):**
- Latest stock exchange news (alerts on request)
- Checking your account balances via SMS [37]

- **Postbank:**
  - Checking your account balances
  - Transferring money
  - Top up your balance

*** SMS based:**
- Receiving confirmation of an order placed or about your account balance
- Information about stock exchanges
- Transferring money between accounts [38]

5.3 Deployment Scenarios

The boundaries of the traditional value chain are removed by mobile data, triggering the need for collaboration across industries and ensuring success.
There are various deployment scenarios possible, e.g. operator dominated scenario, mobile device manufacturers dominate, standardized software dominates, content owners dominate or banks dominate. But as the focus of this paper was on micro-payments, it is assumed that the chances that the mobile operator will dominate are the biggest. For that reason only the mobile-operator dominated scenario is considered.

A mobile operator dominated scenario implies that the largest part of the value chain is controlled by the mobile operator. The operator almost entirely spans the total value chain from publishing to billing and customer base. Operators have a large customer base as well as a strong billing relationship with those customers, allowing them to leverage this existing customer relationship. For the purpose of stimulating demand, flat fees for traffic is likely to be charged. In addition they will extort a major part of the content revenues. As the operator-proprietary portals will dominate, handsets will probably be branded and manufactured according to their specifications, at least in this scenario. Moreover, differentiation would require them to cooperate with content owners, which will give them access to some exclusive content. Some recent developments provide evidence in support of this scenario. For example, global operators like Vodafone and Orange support 'own-branded content propositions' like Vodafone Live. In addition there have been content partnerships, e.g. between Cingular and Sony for 'Spiderman'.

6. Recommended Business Model

In order for the services to be adopted by the mass market, the implementation costs have to be relatively low for banks, mobile operators, merchants and consumers. *Costs for a bank, mobile operator* consist of setting up for example a PKI (Public Key Infrastructure) infrastructure (if this is the preferred security solution), maintaining it, distributing security credentials to customers and maintaining customer support. Most banks and mobile operators already have the infrastructures to provide mobile banking services in place, so the additional cost is of providing security. The choice regarding the operating system, physical terminal, micro browser etc. will be crucial for the success of the application and the costs to the operator. *Costs for a merchant* consist of setting up the solution and running it. In local payment environments, in many cases a merchant has to purchase or upgrade POS (point of sale) terminals to make it capable of reading the payment product information via proximity radio technology (e.g. RFID, Bluetooth). *Consumer's total cost* consist of purchasing a mobile device and other possible required equipment, and transaction and service specific costs. Different parties also have to see an attractive business case in the short-term.

6.1 Business modelling

6.1.1 Target market

The focus of this paper is on The Netherlands. Moreover, the focal point will be small transactions (micro-payments i.e. payments under €10). The focus is on micro transactions where mobile operators are believed to have a competitive advantage, contrary to macro payments where financial institutions excel. Macro payments would imply for operators that they will have to implement risk management and they do not have the experience to do so. Macro payments would require high credit loans to their customers too, but would also cause two different credit positions between operators. In addition, it is very questionable if consumers are ready to trust operators with large payments. As the focus will be on small transactions only the operators are considered. Operators can avoid the main problem of micro payments by developing internal clearing so that settlement costs per transaction become almost irrelevant. Furthermore, operators already have a billing relationship with their clients, which reduces the customer's fear to entrust his financial services to non-banking groups. Operators can rely on huge client databases, so that entrance of operators in the financial market involves enormous short-term expansion possibilities.

6.1.2 Creation of revenue

According to Durlacher research, over 200 million Europeans will have access to the wireless internet with a mobile device. This represents 85% of the mobile device owners in 2003. Though as the focus of this paper is on The Netherlands where there were 10.4 million subscribers for mobile devices by the end of 2000 [12]. What the customer will pay depends on the cost charged by the mobile service provider and by the cost charged for using the network. The revenue of the supplier and the cost for the consumer can be determined by various revenue models. There are various mobile applications and the charges can be based upon the kind of application used. Mobile applications include among others:

- Account inquiry: provides the ability to request for account balance information on various current, savings, fixed deposits and credit card accounts.

- Transaction history: ability to access the account's last transaction information.

- Fund transfers: ability to transfer money between any of the consumer's accounts like checking, savings, or credit card on a real-time basis.

- Bill payment: ability to make bill payments to pre-designated payee organisations in real-time.

- Rates inquiries: ability to request for the latest bank interest rates, foreign exchange rates, loan and lending rates and other rate information.

- Electronic purse

For details on which M-banking / M-payment services are currently provided by banks in The Netherlands see Chapter 5, Section 5.2 M-banking services provided by various banks in The Netherlands.

6.1.3 Cost/Fee Structure

As can be seen from Tables 58.x M-payment services are quite expensive compared to other payment methods in The Netherlands. Though before deriving any conclusions from the business modelling of this situation, as performed in Appendix 4, it needs to be mentioned that the analysis is based on a number of assumptions, which are:

- The m-payment services are assumed to be provided through a GPRS wireless data network.
- It is assumed that the average price of a mobile transaction in The Netherlands is equal to the average cost of an e-purse transaction, because the average price for a mobile transaction was unavailable . Therefore the assumed price is € 0,931, which is taken as the total cost for making a mobile transaction. Since, the fee of mobile transactions can be divided into three categories: wireless subscription fee, transaction fee, wireless data transfer fee and this information was unavailable, the price in total including all these three categories is assumed to be € 0,931. Up to the stakeholders (wireless operator, banks, payment platforms), to divide this fee as per prevailing practice and ownership conditions .

- Furthermore, the price for a mobile transaction in Norway is mentioned by Norges Bank as €0,29[3]. This is the transaction cost. This is the average price for paying giros with a mobile device. As the price was mentioned in NOK, it was converted in € using the actual exchange rate early 2006 (for lack of precise timing of norwegian data) . The share of the mobile subscription cost was approximately €0,20, while the transfer costs were unknown. So € 0,49 has been taken as the average price of making a mobile transaction in Norway, excluding the transfer costs. Because on the site of Norges Bank this was mentioned as the average price ,and as the exchange rates usually fluctuate, a mark-up of € 0,21[4] is used to estimate business in the Netherlands (with similar cost structures) in addition to the price of € 0,49 . It needs to be mentioned that the price of € 0,21 was mentioned as a internet transaction price in Norway [39] ,but is used here as the mark-up to reflect transfer costs and enutral exchange rate fluctuations .

These are the most important assumptions being made. Other assumptions made are mentioned in the Appendix.

Continuing with the analysis of the cost/fee structure, the following conclusions can be drawn:

- A comparison of electronic payments with other payment methods in The Netherlands (Tables 58.x) shows that electronic transactions are relatively more expensive than other payment methods, except the debit card that is the only method using which you end up paying more than electronic transactions. If the charges for a mobile transaction are assumed to be approximately equal to the price of an electronic transaction, resulting in a price of almost € 1 per transaction, that would be quite high for micro-transactions, generally considered to be transactions under € 10.
- It can also be seen that mobile transactions would be quite expensive (see Tables 59 and 60) as compared to Norway, where these services are used more frequently.

So, that means that for M-banking/M-payments to become a mass market application the prices would need to be reduced. If the mobile transaction does not offer the customer any added value; e.g. the customer pays less compared to other payment methods, it probably will not be adopted by the mass market. In Norway, for example, these services are used more often than in The Netherlands, but then as can be seen the prices there are quite low compared to the tariff charged in The Netherlands.

Also two scenario's are added in Appendix 4 (Tables 61-71) : one scenario is based on WAP m-banking services, while the other scenario is based on SMS based m-banking services. The assumptions made in these scenarios are also included in Appendix 4 .

A survey on consumer criteria for selecting M-payments [Figure 42], shows the following results:

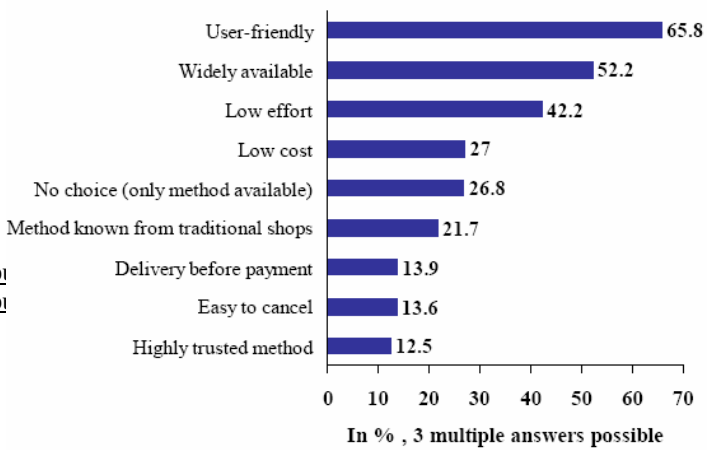


Figure 42: Consumer criteria for selecting M-payments:

[3] So
[4] So

(This survey was based on a total of 10,604 replies. The question above was only addressed to experienced online shoppers; Source: Tariff Structures and infrastructure in the Dutch retail payment systems, Quarterly Bulletin 2002; De Nederlandsche bank).

As we can see from this figure low cost is the fourth most important criterion, but one needs to bear in mind that this survey was addressed to experienced online users only. For other customers it might be more important then some other criteria.

As the focus is on small micro-payments, the price charged should not be so high that it exceeds the payment itself or does not add value for the customer. The conclusion that can de derived from the analysis is that the cost is not justified by the benefits, at least for the micro-payments as micro-payments are usually less than 10 euro.

6.1.4 Customer requirements

There might be various reasons for a customer to use M-payment services, for example, ease of use, accessibility from any place and any time etc. As can be seen from figure 7 in the previous section, there a number of criteria M-payments have to satisfy in order to become a success.

These are the conditions that a potential user demands of a mobile payment system before using the offered applications:

- ***Universality:*** the ability to receive information and perform transactions with any business partner and independent of the location or network.
- ***Instant connectivity:*** the time critical element has to be much better on the mobile than on the fixed internet.
- ***Personalisation:*** the continuous adapting of the content and the services offered to individuals in order to match it with the user's profile.
- ***Convenience:*** the client will prefer those organisations that offer the most convenience. Users require interfaces (what the client gets to see) that are easy to use, visually interesting, interactive and where a major part of the users information is pre-programmed in the device, with the providers.
- ***Expenses:*** what the client is willing to pay will depend on the added value the payment system offers.
- ***Protection of privacy:*** in order to perform mobile trade and more specifically mobile payments, the customer has to hand over personal information. These kind of data will have to protected to prevent abuse.
- ***Security:*** each business transaction requires elements of trust.

Other criteria, as can be seen from Figure 7 in the previous section, include among others:

- *User-friendliness*
- *Wide availability*
- *Delivery before payment*
- *Easy to cancel a payment*

6.1.5 Drivers for operators to provide M-payments:

This section looks at the drivers for operators and not banks as the emphasis is on micro-payments.

1. One of the reasons for operators to provide mobile payment/mobile banking services might include the penetration of mobile phones. As mobile phones have increased in popularity in the recent years, the number of mobile subscribers has increased. In The Netherlands the number of mobile subscribers per 100 inhabitants is approximately and continuously evolving about 75 % . [40]
2. Furthermore, mobile operators are carried along most of the time and are personalised.
3. Operators have been quite successful with their solution of charging your telephone bill account.
4. Moreover, they have the experience in the realm of international standardisation and have roaming agreements.
5. In case of micro-payments operators can avoid the main problems of settlement, by developing internal clearing so that settlement costs per transaction become almost irrelevant.
6. Additionally, operators have already a billing relationship with their clients, reducing the customers' fear of entrusting his/her financial services to non-bank groups.
7. Operators can also rely on the huge client databases, so that entrance of operators in the financial market includes enormous short-term expansion possibilities.

7. SWOT analysis of technical solutions [4] [15]

7.1 Chip based solutions

7.1.1 SIM based

7.1.1.1 Bank issued, single SIM

Bank issued chip with payment application (including operators SIM functionality):

Strengths	Weaknesses	Opportunities	Threats
Brand visibility: issues/payment brands can be visible in the digital format	Specific agreements between banks and operators are required	Since the platform is controlled by the bank, the maximum level of security and functionality can be achieved	It is unlikely that it will be widely accepted by operators, so the chances that it becomes a 'global' solution are very low
Existing devices can be used	"Service confusion": distinguishing between both partners in CRM is hard	For banks it is necessary to establish a close relationship with the operators on a continuing basis or to become a VNO	There is a need to develop standards
"End-to-end security": integrity & confidentiality with the application is possible	No choice for the customer to switch between banks or operators, thus he is bound to one operator/bank; switching brings additional costs		Since the device is neither 'tamper evident', nor complying with EMV requirements there is a danger of 'eavesdropping' and

			'tapping' when entering the PIN. Though the menace is restricted because of the device being in personal possession of the cardholder.
'Customer loyalty' as regards the payment application	As banks control the chip, agreements between the bank and the third party are required, for the third party to provide authentication services. As a result operators might need security enhancement, if their SIM's do not meet the banks security standards.		

7.1.1.2 Operator issued, Single SIM

Operator issued containing no bank application or data:

Strengths	Weaknesses	Opportunities	Threats
Clear distinction between the systems of the banks and the operators	Extensive agreements, concerning various issues e.g. legal, technical, commercial and security issues, between banks and operators are required	Appropriate for micro-payments as high levels of security are not required	The time to market may be long, as a result of disagreements between banks and operators in the short run
Existing devices can be used			
"End-to-end security": integrity & confidentiality with the application is possible			
"Open-solution (multi-bank, multi-operator, multi-merchant."			

7.1.1.3 Operator issued, shared SIM

Operator issued containing bank certified payment application

Strengths	Weaknesses	Opportunities	Threats
Brand visibility: issues/payment brands can be visible in the digital format	Specific agreements between banks and operators are required	It is suitable for both micro-payments and macro-payments; the former requiring low levels of security and the latter necessitating in high security standards	Since the device is neither 'tamper evident', nor complying with EMV requirements there is a danger of 'eavesdropping' and 'tapping' when entering the PIN. Though the menace is restricted because of the device being in personal possession of the cardholder.
Existing devices can be used	"Service confusion": distinguishing between both partners in CRM is hard	For banks it is necessary to establish a close relationship with the operators on a continuing basis or to become a VNO	There is a need to develop standards
"End-to-end security": integrity & confidentiality with the application is possible	No choice for the customer to switch between banks or operators, thus he is bound to one operator/bank; switching brings additional costs		As operators control the platform, banks may loose applications residing on the SIM
'Customer loyalty' as regards the payment application	Operators might need security enhancement, if their SIM's do not meet the banks security standards.		
	"Separate application development required per SIM/chip type and producer. Standard application is possible in JAVA."		

7.1.2 Dual Chip

Internal second slot (bank issued second chip and payment application):

Strengths	Weaknesses	Opportunities	Threats
Brand visibility: issues/payment brands can be visible in the digital format	Increased costs for customers as new devices will be required, as well as for banks as they will have to invest in second ICC/WIM (multi-application chip, new chip technology)	Providing high levels of security possible as the bank also controls the second platform	Since the device is neither 'tamper evident', nor complying with EMV requirements there is a danger of 'eavesdropping' and 'tapping' when entering the PIN. Though the menace is restricted because of the device being in personal possession of the cardholder.
"End-to-end security": integrity & confidentiality with the application is possible	"Duplication of the bank's chip, production and introduction of new processes."		Close co-operation between the bank and handset manufacturers is needed, also when standards are developed manufacturers should be convinced to use these standards
No agreements between various external parties are required (from the bank's perspective)	Currently not produced		Despite the fact that it concerns two separate chips, there is a danger of 'eavesdropping' and 'tapping', as the chips have to communicate in an 'open handset'
'Customer loyalty'			
The distinction on the technological side is clear			
Responsibility regarding CRM distinguished			

7.1.3 Dual Slot

- "External slot for full sized banking card. Bank chip and SIM independent of each other [like the dual chip case]." As this has not been developed yet a SWOT analysis for this solution is not included.
- "External slot for full sized banking card, i.e. the existing mobile phones, developed with SIM application toolkit."

Dual slot with SIM application toolkit:

Strengths	Weaknesses	Opportunities	Threats
Brand visibility: issues/payment brands can be visible in the digital format	As there is a tendency that the mobile phones are getting small, fitting an extra slot for a full sized card into the phone might be difficult and selling 'bulky-banking phones' hard	Appropriate for micro-payments as high levels of security are not required	Since the device is neither 'tamper evident', nor complying with EMV requirements there is a danger of 'eavesdropping' and 'tapping' when entering the PIN. Though the menace is restricted because of the device being in personal possession of the cardholder.
"End-to-end security": integrity & confidentiality with the application is possible	"Card-reader and associated applications rely on operators willingness to accept more complex devices"		Despite the fact that it concerns two separate chips, there is a danger of 'eavesdropping' and 'tapping', as the chips have to communicate in an 'open handset'
'Marketing' or 'perceived' distinction on each party's responsibility of CRM	No choice for the customer to switch between banks or operators, binding the customer to one operator/bank		Loss of applications (by banks) that reside on SIM
	Operators might need security enhancement, if their SIM's do not meet the banks security standards.		
	Increased costs for customers as new devices will be required		
	Not very convenient to use		
	"Separate application development required per SIM chip type"		
	No added value to local payments		

7.2 Organisational bottlenecks

7.2.1 General remarks and networking effect methodology

The success of m-payment will be driven by strong network effects, allowing to reach a critical mass of customers and merchants (including banks and credit card companies). To attract a significant number of merchants it is important to have an attractive revenue and cost model, and platform standardisation in place. Large investments will be required to achieve this as it also involves marketing and customer education. The marketing may best succeed if m-payments are positioned as best to handle payment steps in specific services or business processes, instead as being positioned as a replacement / substitute to e-payments (broadband, ATM terminals etc).

As a consequence of the network effect in the adoption of m-payment services, merchants are not willing to adopt a m-payment system unless the number of customers is high enough and the same is true for consumers, i.e. they are not willing to adopt a particular m-payment service, but only if widely accepted among merchants for specific services or business processes. Consequently, this will require a self-supported penetration process in the service from both sides, the customers and the merchants. An imperative point, both from the perspective of consumers and regulators, and in the wide acceptance of a payment system is the payment security characteristics. In order for a payment system to be widely adopted it is important that the underlying payment security characteristics are independent from the underlying payment channel. Currently, solutions exist whereby mobile payments are equally if not more secure than Internet based solutions.

7.2.2 Bottlenecks for mobile operators

If mobile operators are considered or choose to become m-payment merchants , the main obstacles faced by them in the successful deployment of mobile-payment and mobile-banking services include amongst others: lack of standardization, high investments for roll out, and their own traditional culture of overemphasizing traditional payment systems. Another major challenge mentioned by various operators and content providers are regulatory and legal issues. Furthermore, if operators desire to become m-payment merchants they also face the challenge of not only ensuring the security of their own platform, but also promoting this in their offering. Though there is also another issue linked to security enhancement, namely user convenience which often conflicts with security enhancement. Thus the operator has to seek a balance between these two conflicting issues.

Additionally, the success of m-payments is also determined by the cooperation between various mobile operators. Next to co-operation among network operators, various players in the value chain of the m-payment service need to co-operate as well. Mobile operators in particular should consider close cooperation with traditional payment service providers or merchant acquirers, or take on these roles under regulatory frameworks allowing it, or should take participations in payment clearinghouses with wireless communication assets/agreements. For the growth of the m-payment sector, it is essential that the different players in the value chain, define and agree upon roles and incentives.

7.2.3 Bottlenecks for other actors

It can be said that the large number of players involved in m-payments is a major obstacle in the success of m-payments, as the large number of players have to make m-payment financially viable and the margins might not be enough to be shared by everyone. Also authentication, liability, insurance and risk management along too long payment chains is

a very complicated and risky proposition. There are a plenty of indications, including the potential of the pooled customer base, that the total paper payments have declined considerably in recent years and the total electronic payments have increased on the other hand (see Tables 22.x and 23.x in Appendix 3 & Table 58.x in Appendix 4). From this it can be concluded that probably there is also a potential market for mobile payments, as a couple of years back electronic payments were also considered to be a failure. This clearly illustrates that the rewards are present, only if the players can get the balance right.

As mentioned in the previous paragraph the main stumbling blocks with regards to cooperation comprise of sharing the revenues amongst all the members of the chain, and it might be the case that margins are not enough to be shared by everyone. So, determining the right balance of sharing the revenues is one the main reasons hindering cooperation. Still, there are some easier areas of cooperation. A close cooperation between the various players might stimulate the introduction of a standard solution, which will be desirable from the viewpoint of aggregate increase in revenues. Because a universal, standard solution would simplify the use for the customer, it would stimulate the demand for mobile payments. In addition, as large investments may be needed, the costs of these investments could be shared by the various players.

In a press release in June 2005, it was stated that Simpay (set up by Orange, Vodafone, T-Mobile and Telefonica Moviles), had a new payment system that billed directly to the mobile phone. So micro-payments can be done with the mobile (while a small portion is taken by Simpay for each transaction), and the cost will be debited from the mobile phone bill[41]. In a more recent article [42], it was declared that Simpay had been disbanded. Though no specific reasons were given publicly by Simpay with respect to the disbandment, analysts from Gartner have attributed four reasons to the failure of Simpay:

1. Implementation delays, which strengthened potential competitors hands
2. Underestimation of the challenges of a Europe-wide payment system
3. Cost of launching a consumer payment brand may have been unattractive, particularly to T-Mobile
4. Local operators' resistance to the scheme

7.2.4 Interoperability bottlenecks

Progress in the process of standardisation, it seems will take place gradually over the coming couple of years. As mentioned before in the section on interoperability, interoperability is a must for consumer and merchant acceptance, and as a result for growth. The likelihood that merchants join, will increase, in case customers of all operators can use the solution. And the probability that customers make use of m-payments will increase, the more widely he can use a specific m-payment solution. An open and interoperable m-payment standard has two essential advantages for the consumers, regulators and merchants . The first is that achieving critical mass will be easier and faster as all merchants will be available to all end-users and the other way around, all users will be available to all merchants. The second is that it provides the m-payment agents (whether mobile operators , payment clearing-house, or retail chains, to cite a few) with the possibility for flexible billing so that subscriptions are not necessary. As a standardised foundation implies higher deployment, the chances for success will be greater, as m-payment penetration will accelerate and the costs reduced, due to the network effect.

As an illustrative conceptual example would be the use of m-payments for purchases in retail chain stores, where the coupling between RFID tags on packages, RFID readers at exit points in the store with Bluetooth links and mobile terminals essentially dismiss present-day cash machines (and staff). So, only the use of the same platform across all stores will enable customer adoption. The flexibility and competition between store chains mandates no subscription based service.

As mentioned in the section customer requirements; flexibility, simplicity, security and convenience are issues that have to dealt with from the customers' point of view. In addition to that the payment solution needs to be universal and suitable for mobile commerce. Dependability and profitability are the main issues from the merchants' point of view, in addition to concerns like security, flexibility etc.

Yet another challenge faced in the successful development of m-payment services is that any payment method has to be possible for a majority of the mobile users. The development of a successful sophisticated technology is slowed down by the continuous advancement of mobile handsets as well as various types of platforms and operating systems.

7.2.5 Bottlenecks for banks and credit card companies

For the generation of perceived confidence and integrity from m-payment services, support from banks' and credit card companies' trusted brand can play a major part.

An important point that needs attention is the payment culture which is forming a barrier to the wide deployment of mobile payments, as customers are satisfied with the traditional payment methods. This pattern will have to be broken if success in the m-payment services is to be attained and the only way to do this is that the m-commerce service provides added value to the customer, and banks /credit card companies face an issue of internal competition between their alternative payment channels. It is known that cheque was already a competition to cash settlements in the old days, then electronic payments competed with cheques, as can be seen from Table 56, the cheques have decreased in use and the use of electronic payments has increased, and credit card competed all along hindered only by regulatory frameworks: the lesson learnt is that all payment methods survive, but each must find a competitive position with their advantages /disadvantages.

In addition the consumer will have to be educated to start using the m-payment services. As also mentioned in the section reasons for failure, the bank density is quite high indicating satisfaction with the current payment methods. Though customers do not drive bank branches but banks do , but apparently proximity services are important in The Netherlands. And one could argue that customers are less inclined to use e.g. mobile payment services, not only because they are satisfied with the current system, but also because they know that they can go to a bank branch. If the banking density would be low, and a customer would need to travel 'a large distance' to go to a bank branch, the customer might be more inclined to use e.g. mobile / electronic payment services. Research has shown that users in Scandinavia and Asia are more comfortable with using m-commerce services and that m-commerce services are more advanced in that part of the world. In Europe there is a division in social acceptance of m-payment services. In the Nordic countries the social acceptance of m-payment services is considerably higher than in the remaining parts of Europe. Though the mobile phone penetration is high in

Europe, providing a base for exploring m-payments, it will require m-commerce applications that add real value for the customer.

8. Analysis of cases – reasons for success and failures

The case study is used in many situations to contribute to the knowledge of the individual, group, organization, social, political, and related phenomena. A number of case studies about mobile banking were looked into in order to be able to understand the reasons behind their success and failures. Additionally, the reasons of success and failure were thoroughly studied in order to determine what needs to be done differently to overcome the obstacles in field mobile banking services.

The cases of Rabobank[5], Postbank[6] and Vodafone[7] and some other cases were genuinely studied, in an attempt to find out the reasons behind their success and failures considering all the essentials in the field of mobile banking.
Until now, the results of mobile financial services appear to be mixed. Some operators like Vodafone used mobile banking services with some success to increase their customer retention rate. However, banks have been less successful with the launch of mobile banking services. This has been ascribed to technical restrictions of the mobile technology available currently, which has not been geared towards high performance data transmission.

The emerging convergence among Internet and the mobile technology will most probably lift these limitations and consequently lead to the emergence of a wireless broadband Internet platform that will allow ubiquitous access and a wide range of new value-added services, many of which would be settled via payment systems based on the platform.

From the perspective of mobile operators, it is questionable whether they will succeed in mobile payments on their own, despite their technical expertise and their familiarity with micro-billing and massive customer base. On the other hand, if banks want to develop a dedicated mobile payment infrastructure they need to rely on general purpose wireless network operators. So a close co-operation between the mobile operators and banks is a sine qua non condition for the success of mobile payments.

8.1 Reasons for failure – limited deployment

Until present the technical solutions as well as the service/product mix are far from clear. Uncertainties are rooted in technology, but also have to do with the unknown attitudes and preferences of customers and merchants. Experience of both internet and mobile payment schemes to date suggest:

- “Limited customer interest in new payment systems
- Strong price/cost sensitivity among customers and merchants
- Strong linkage between payment schemes and underlying e-commerce.”

Interesting enough, these same arguments were identified for limited development of Mobile payments in Switzerland (see Additioanl bibliography) . The technical interconnection of payment systems needs to go along with agreements on common operational rules and procedures. In payment services, the recurrent challenge has been

[5] http://www.fenestrae.com/customers/case_Studies/Rabobank.asp
[6] http://www.fenestrae.com/customers/case_Studies/Postbank.asp
[7] http://www.vodafone.co.nz/business/10.6.1_mobilise_casestudy.jsp?ss=casestudy

the reconciliation between the technical and the business interoperability. All parties engaged agree that standards are essential and yet they have strong preferences and keep recommending their own preferred solution. In the absence of clear directions, customers are reluctant to implement them.
Moreover, there is a certain risk involved in mobile payments, while security is a major concern for the customers. It is obvious that mobile payments involve more risk compared to traditional (physical) payment systems. As a result, both the customer and merchant need to be authenticated and the virtuality of the payment instruments as well as the transaction amplify the potential for uncertainty and fraud. The payment cycle is also more complicated, including parties that would not have been present in the physical world (e.g. portals and service aggregators).

The generally accepted view is that transaction security has to be ensured by deploying encryption technology. In other words, PKI is seen as the evident solution that allows secure transactions between unrelated parties across heterogeneous networks. Banks and non-banks have been working on the development of PKI. Despite the fact, some critical issues have remained unresolved as yet:

- "Co-operation between key actors: financial actors, merchants, technology suppliers and mobile operators etc.,
- Standardisation and interoperability between various PKI approaches,
- Customisation, generic or service-specific PKI,
- Governance of certification authorities, their oversight and regulation,
- Cost recovery and pricing of PKI services."

Whether the customers accept the services will depend on a number of factors, involving the recovery of cost and pricing the security infrastructure. The current pricing approach makes e-commerce and m-commerce not only more complex but also more expensive compared to the traditional systems.

Other reasons that have led to limited deployment of M-banking/M-payment services, specifically in The Netherlands, include the social acceptance and the bank density in The Netherlands. The Dutch customers have been reluctant to make use of services like mobile payments. As the focus was on micro-payments, maybe price played a role. The prices charged for a mobile transaction exceed the value of the transaction.
Also the bank density for The Netherlands has been calculated; the calculation has been as follows:
The total area of The Netherlands is: 33,946 km²
The total number of branches[8] in The Netherlands: 348.
33,946/348 = 97,5 km²
Though there is no bank density calculated for any other country with which this could be compared, it is known that the bank density in some other countries e.g. Norway is quite low. And m-banking services are used more often there. So, bank density probably also plays a role in the reluctance of Dutch customers to adopt m-banking services. Though as mentioned before, customers do not drive bank branches but banks do, but apparently proximity services are important in The Netherlands. And one could argue that customers are less inclined to use e.g. mobile payment services, not only because they are satisfied with the current system, but also because they know that they can go to a bank branch. If the banking density would be low, and a customer would need to travel 'a large distance'

[8] Only branches of the following banks were included: ABN AMRO, ING, Postbank and Rabobank.

to go to a bank branch, the customer might be more inclined to use e.g. mobile / electronic payment services.

8.1.1 Case of Postbank

Name of partners: Postbank m-banking (ING/Postbank, Telfort, Genie)
Launched in July 2001
Details on the mobile banking services provided by Postbank can be found in Chapter 5, section 5.2 about Mobile banking services provided in The Netherlands by various banks.

- In this case digital signing is provided by WIM within the WAP application.
- Digital signing via SMS (also through WIM), enables the use of the digital signing function on the internet.

Access to these functions is protected by means of an off-line PIN, which is called the m-code.

No figures about the services provided by the system (including direct prepaid airtime balance top-up, secure SMS-based communication between bank and customer, "WIM provides digital signing within WAP applications, and digital signing via SMS") are available, except that the number of users is 500,000. [15] The total number of mobile users was 10.4 million in 2000. That implies that in percentages the number of users of this particular mobile banking service for Postbank was 4.8%. That is relatively low in absolute terms ,although data for the relative usage amongst sole Postbank customers is unknown; but it confirms that m-banking services are not very popular in The Netherlands in general anyway.

8.2 Reasons for success

Regulatory attention is certainly not an issue in the emerging payment systems. In Europe, promotion of innovation and competition within the payment industry and the influence of new payment systems on financial stability, have been major areas of policy concern. While a legislative and regulatory framework is absolutely necessary, it does not facilitate large scale deployment. "Financial technology projects, particularly in the domain of financial smart card infrastructure, have been supported by EC R&D funding. However, this was done on a case-by-case basis. Commission at present is considering whether to set up a formal e-finance support line in the context of the 6th Framework Programme, scheduled to start in January 2003.
Though there are no reliable converged standards, there is insufficient bandwidth, incomplete coverage and an affluence of devices and software available in the market, there is an opportunity to design and implement highly effective applications that provide a good return on investment. These applications would have to overcome the aforementioned problems/shortcomings, e.g. by handling the incomplete coverage for example by providing the possibility for storing the data and synchronising the later as the network can be accessed and supporting several devices/networks etc.

The following are the most important issues that lead to offering successful mobile banking services:

1. *Introduce an open business model*, as the end-user is free to choose the desired payment product issuer, mobile operator and handset manufacturer and change any of these without influencing the others. Business processes of different players should be independent. Open business models and freedom of choice will lead to open

competition in each part of the value chain resulting in increased quality of the services and lower end-user prices. An open business model is the only alternative for wide scale m-payment solutions, and to the kick-off of the m-commerce market.

2. *Interoperability between different m-payment systems* is a precondition for wide scale acceptance of m-payments. M-payment systems should be compatible with different banks, telecom operators, merchants and mobile devices. Standardisation is the key for interoperable systems. Both inter-industry cooperation is required to achieve widely accepted domestic or international m-payment products. Existing standards and technologies should be utilised and supported to the maximum. Mobile payment infrastructure should also support multiple payment products. Use of existing payment instruments in the mobile channel should certainly accelerate the take-up because of the familiarity of the payment product. Additionally, the end user trust, payment infrastructures, standards and processes would be in place.

3. It is of great importance to enable *easy, fast and convenient mobile transactions*. In addition, they have to be *attractively priced*. Latest developments of mobile technologies, such as larger high-resolution colour displays, JAVA MIDP, networks enabling high data transmission rates and enhanced mobile browser technologies have increased the usability of the mobile devices to a totally new level and enabled convenient use of even complicated services. Service discovery and activation should be easy but safe for the end user. The use of service registration and activation processes used in existing payment products will offer the fastest way to wide take-up, as end-users are familiar with and trust these processes. Wide acceptance of m-payment products that can be used in a large variety of shops will reach the mass market. Both technical and end-user's perceived security has to be guaranteed. PKI-based (Public Key Infrastructure) security solutions guaranteeing secure authentication and transaction non-repudiation are suitable for transactions with higher risk whereas lighter security mechanisms can be used for low-value transactions. Payment security should be controlled by the party carrying the risk. When using bank-issued payment products, it is the responsibility of banks to manage end-user authentication and other security aspects.

4. *End-user, merchant, payment product issuer and mobile operator have to see value in the m-payment solutions* in order for it to be successful. End-users' preferences are as already discussed ease, speed of use, convenience, security and attractive pricing. Merchants require that m-payment products reach a big customer base and that the customer base finds the merchant. Merchants are waiting for m-payment products to bring additional revenues (e.g. through expanded service offering) or cost savings (e.g. through increased security lowering the transaction repudiation). The cost of enabling customers to use a new payment method should be low and the system should be set up easily. Furthermore, fund cycle from the end-user to the merchant should be fast. In current systems, based on SMS and monthly mobile phone billing, the delay is approximately 1.5 months. In effective m-payment systems crediting should work on a daily basis. Payment product issuers, usually banks, have to see a positive business case in m-payments to be able to cover the development costs of the system. Customer loyalty can also be increased with new innovative products. Payment product branding is extremely important also in the mobile channel. Strong brands make the use of product easier for the end-users. The potential to add brand is important in terms of revenue streams from value added services. Widely adopted m-payment products will have a business opportunity in providing value added services

for merchants and other parties in the value chain. Terminal manufacturers benefit from end-users use of new value added services, utilising new capabilities of mobile phones through increased terminal sales.

5. *M-payment products will not be adopted by the mass market overnight.* The development will be gradual and consumers will have to be educated to use their mobile devices in new ways.

9. Open issues and challenges

The proceedings so far in mobile banking / payments have been slow, not in the last place because of the difficulty of the development of feasible business models. The undertaking of designing business models is a complicated one as the user, organizational, financial and technical requirements need to be balanced and accommodated. In addition to this, mobile payment systems need to take into account not only the business logic of the financial service sector but also the business logic of the telecommunications sector and the retail sector.

There are many questions that have remained unanswered with respect to the design of business models for mobile payment services. For example, what should be the value proposition towards merchants and towards customers? How indispensable are banks in introducing mobile payment services? Should user interface designs be text or voice based? Should the authentication functionality be included in the existing SIM cards or in a separate SIM card?

The success of mobile banking/payment services will be dependent on a number of factors, including satisfying the needs and wishes of at least two kind of end-customers:

- the customer who has to adopt the mobile payment as a way of paying, besides the existing payment methods like debit and credit card systems
- the merchants who have to accept the mobile payment as a valid means of electronic payment.

This focus of mobile payment services that has a dual nature further complicates the progress in mobile banking/mobile payment services.

Recently, banks, mobile operators and mobile device manufacturers have begun to build the authentication functionality in the mobile device. Though this gives rise to another technological issue, namely whether the security functionality including the authentication, should be incorporated in a removable or in a non-removable fashion. The non-removable solutions result in forcing the customer to buy a new mobile device whenever they switch from bank. On the other hand, the removable solutions offer more flexibility and acts in accordance with the idea of having a transparent, open and flexible payment infrastructure.

Other open / unknown issues include:

- Competition between banks and non-banks providing services relating to payment settlements.
- Effective pricing strategies to attract and retain customers.
- Role of “payment intermediaries” that specialize in back-office payment systems.
- Internet payments such as credit cards combined with transaction codes etc.

- Electronic banking services, currently used by some to send and receive account information.
- Other mobile terminals than mobile phones.
- Development of electronic money and electronic payment systems.
- As mentioned before the mobile payment transaction fee can be divided in three categories: wireless access provider subscription fee, mobile transaction fee and wireless payment data transfer fee. It is not known how in the Netherlands the split of the fee will be made between stakeholders (banks, payment platforms, wireless operator , billing agent) as this depends on political and ownership factors (not covered in this report). For a bundled mobile payment fee, and from practice outside the Netherlands, one can give a benchmark split of 25 % to bank , 25 % to payment platform , 25 % to wireless operator, and 25 % to billing agent (part or not of operator).

10. Conclusion

Prospects for various actors

- **Mobile Operators:**

A mobile system run totally by a mobile operator requires a banking license or an EMI, though the distinction may be blurred. This needs to be done in order to manage the pre-paid accounts that are not just usable for goods/services of the firm itself, but also accepted by other companies. Knowing that there is a large market of mobile phone contracts, there might also be created an opportunity by offering pre-paid accounts for m-payment. Furthermore, a banking license is also required to grant shops a payment guarantee. The attainment of a banking license can take place through either a direct application by the operator or through co-operation with a bank.

The prospects for various operators differ; as there are threats and opportunities involved. As far as the difficulties are concerned, first of there is an increase in the mobile operators exposure to financial risk. Except when payments are limited to micro-payments, the payables will be much higher as compared to airtime charges. In addition, there is an increased risk of fraud occurrence as 'cash equivalent credit' is available on the pre-paid account. Also, the fraud will be extra costly for the operator: as an m-payment claim will have a full affect on the costs of the operator, as opposed to theft of 'airtime' that brings little additional costs.

There are certain aspects that need consideration. For example, settlement between networks that will become more complex as a consequence of roaming, if the payment takes place via a phone bill. In addition to roaming of traditional services, there will also be a need for 'payment roaming', if customers of one operator are to make m-payments in another operators' network. One implication of this is increased financial risk not only for customers, but also for operators. Last but not least, the mobile operators would not only be required to establish more reliable billing processes, but also build a reputation for this reliability. Considering issues as risk management, clearing and settlement one feels operators would have to build certain core competencies of financial service institutions. So, in the short to medium term alliances between operators and banks are considered to be more promising.

- **Banks:**

Banks have experience in both risk management as well as in payment services. Furthermore, they are perceived to be very reliable and they have long standing relationships with customers. In 2000 the Mobey Forum was founded, by ten international banks, VISA and three mobile phone manufacturers, "to encourage the use of mobile technology in financial services such as payment, remote banking and brokerage." [Mobey forum]

The consortium 'MoSign' is also driven by financial institutions. It recommends the storage of the signature on a separate smartcard. This would provide the possibility of using it in various card readers (PC, POS). Though this would require an additional reader for use with the mobile phone. However, there are chances that this endeavour will not be successful as additional infrastructure (card reader) is required both for use with a PC and a mobile phone, and users may be reluctant to purchase it. In most of the m-payment projects until now some banks or credit card companies have been involved. So the complete replacement of banks in payment process seems unlikely. The front end users, however, could become a domain of mobile operators.

- **Mobile phone manufacturers:**

Mobile phone manufacturers do not have the experience in payment processes. As a result they are not very ambitious to play the central role in mobile payments. However, they have a strong influence on which technical realization wins through, as they are the ones who build the device in the hand of users. They mainly decide whether SIM and WIM chips are separate, or whether there is a dedicated 'key' sign on the mobile phone. Thus working together with the mobile phone manufacturers is vital for other players.

The manufacturers have a strong interest in m-payments becoming a success, regardless of the type of m-payment that will prevail: the 'purse in mobile phone' would stimulate the demand for mobile phones and their further technical development. The consortium MeT (merged with OMA) was developed in order to pursue this goal. The framework defined by MeT includes description on how mobile – electronic transactions are performed securely by the mobile device, using the standards leveraged by MeT (which has merged with OMA). These standards are wider than the ones of mSign and MoSign and are aimed at a broader application of mobile as 'PTD.'

- **Customers:**

Mobile banking services are the most cost effective and convenient access for bank customers, which they can access from anywhere and any time using their mobile devices. Mobile banking solutions are based on the most up-to-date mobile application technologies i.e. Wireless Application Protocol, SIM Application Toolkit, Short Messaging Services and Interactive Voice Response (IVR). The advantages of these solutions includes transaction status inquiries, ability to view and pay bills, ability for customers to report lost cheques, ease in sending alerts and notifications to bank customers and order new services with ease and distantly etc.

For M-banking/m-payment services in The Netherlands to become a success, there are a number of issues that need to be addressed. Among one of the most important is the cost of making a mobile transaction. As can be seen from the analysis in section cost / fee structure, it could be argued that price has certainly been an obstacle for micro-payments to become a mass market application in The Netherlands. Because it is quite expensive compared to other payment methods, currently it is not adding any value for the customer

to use a mobile device for micro-payments. Since micro-payments are usually defined as payments below 10 euro, paying e.g. 1 euro would not provide an incentive for a customer to make use of this service. Comparing this with Norway confirms this. The prices charged on a mobile transaction are considerable lower than in The Netherlands and the usage is also higher. A low price, is thus a must for wide adoption of mobile transactions. Maybe a price decrease leads to higher social acceptance. Another cost to the customer might be the cost of purchasing a mobile device that provides the possibility of making mobile transactions[9]. Table 43 provides an overview of the mobile devices that allow you to make use of Rabobank M-banking services, all of which are quite expensive. Other issues that need to be addressed include: satisfying the customer that making a mobile transaction is safe and secure. Other requirements that the customers demand from an M-banking/m-payment service before they make use of this particular service are addressed in section 6.1.4 Customer requirements.

Table 43: Mobile device you need in order to make use of Rabobank m-banking services:

	KPN	*Orange*	*T-Mobile*	*Vodafone*
Device	LG 34li	Nokia 6230	Nokia 6230	Nokia 6230
	NEC n34li	Nokia 6600	Nokia 6600	Nokia 6600
	NEC n400i	Siemens SX1	Sharp TM100	Motorola V980
	NEC n40li	Sony Ericsson T630i	Sony Ericsson T630i	Sony Ericsson T630i
	NEC n410i			
	Mitsubishi m34li			
	Mitsubishi m342i			
	Mitsubishi m430i			
	Panasonic p34li			
	Sagem SG34li			
	Samsung s34li			
	Samsung s342i			

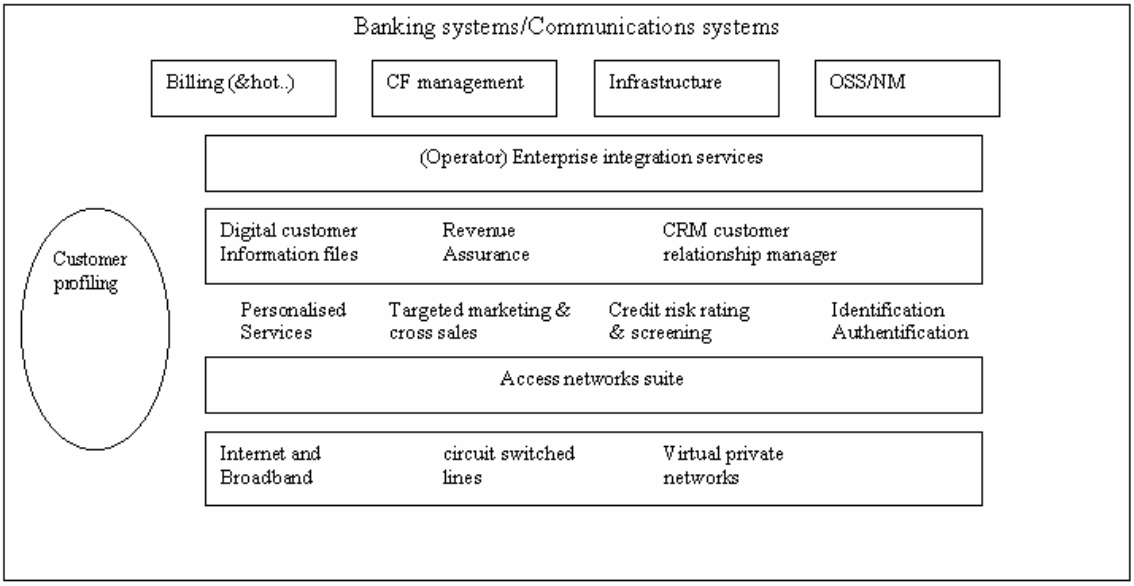
Source: www.rabobank.nl

[9] The table is based on mobile phones that provide the possibility of making use of Rabobank mobile banking/payment services.

11. Appendices

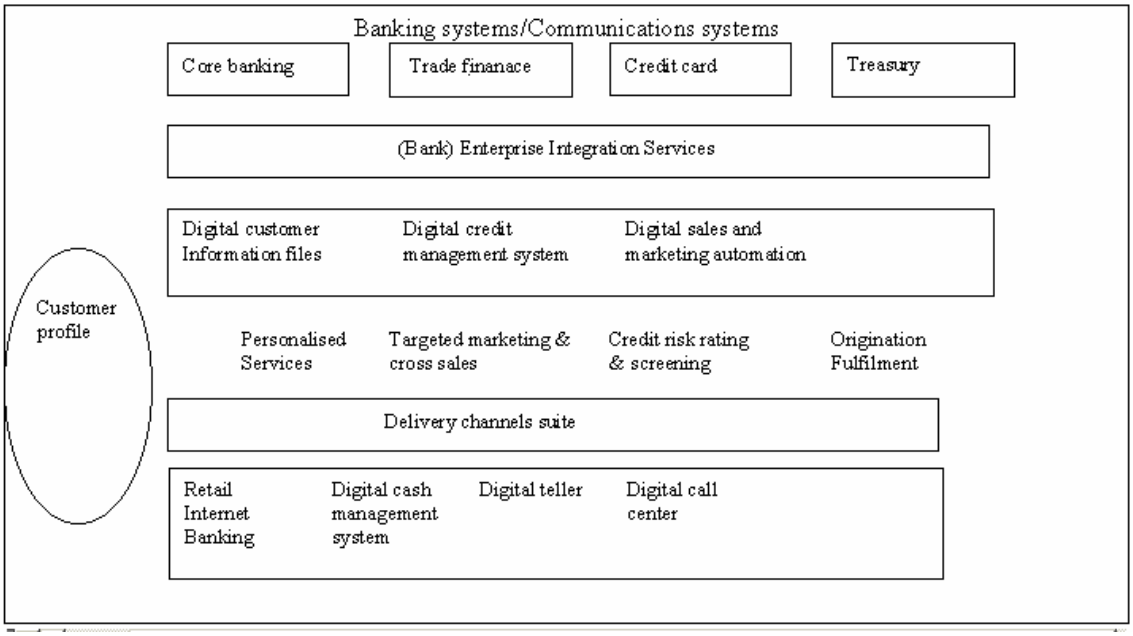
Appendix 1:

Figure 44 : Mobile communications systems, customer management and the billing architecture:



Source: Pau, L.F.(2004) [7] , Mobile operators as banks or vice-versa

Figure 45 : Payment/Banking systems, customer management and settlement architecture:



Source: Pau, L.F (2004) [7]., Mobile operators as banks or vice-versa

Table 46 : Interoperability issues dealing with particular aspects of GSM/WAP environment:

Requirement	Description	Minimum/Desirable
WAP certificate and CRL profiles	Special profiles for client and CA certificates may be used to accommodate a X.509v3 certificate to the WAP unique requirements	Compatibility with specific profiles
Alternative certificates	WTLS and X9.68 certificates should work seamlessly with any WAP gateway/server	Compatibility with different certificate formats
Certificate URL	Client certificates can be stored in a special network repository; the client only sends a certificate pointer to the server	Compatibility with URL pointer instead of complete certificate
Short-lived certificate	WTLS server certificate with validity limited to typically one day	Issuance of new server certificates daily
PKI portal	Integration with the portal, that is the interface between the CA and WAP clients/servers/gateways. The portal is an entity performing RA and/or CA functions	Provision of an entity that offers a set of basic PKI services to all WAP actors
Digital signature format	The signature is represented in a WTLS special version of PKCS #7 (compressed header)	Conversions from and to the WTLS encoding format

Source: Smart-IS A.M. and eESC TB 12 AES; Public Electronic Identity, Electronic signature and PKI

Table 47 : Interoperability issues that need to be considered:

Term	*Definition*	*Reference*
Commercial interoperability	The economic benefits are divided among the parties engaged in a "certificate validation process" to assure both service and performance levels	ECBS TC 6 WG 3
Legal interoperability	The relationships and dependencies between the parties involved in the "certification validation process" are subject to an acceptable legal framework	ECBS TC 6 WG 3
Message format interoperability	The following areas are covered: - message format of the application - electronic signature format - certificate format - validation protocol	ECBS TC 6 WG 3
Operational interoperability	Rules defining the presentation, processing and storage of a certificate, including rules describing the interaction between the parties involved in the "certification validation process"	ECBS TC 6 WG 3
Participant interoperability	"The Certificate Service Provider that issued the certificate is of an acceptable quality and can meet its obligations on an ongoing basis."	ECBS TC 6 WG 3
Policy interoperability	"The certificate is for the purpose to which it will be put and that this is within the contemplation of parties involved in a certification validation process"	ECBS TC 6 WG 3
Technical interoperability	"The format of the certificate is to an acceptable precise standard, with prescribed cryptographic algorithms including padding rules, formal data representation and processing rules and other technologies affecting the data to be signed."	ECBS TC 6 WG 3
Trust scheme interoperability	The following aspects are covered: - Legal interoperability - Policy interoperability - Commercial interoperability - Technical interoperability - Participant interoperability	ECBS TC 6 WG 3

Source: ECBS, Interoperability of bank trust services; www.ecbs.org

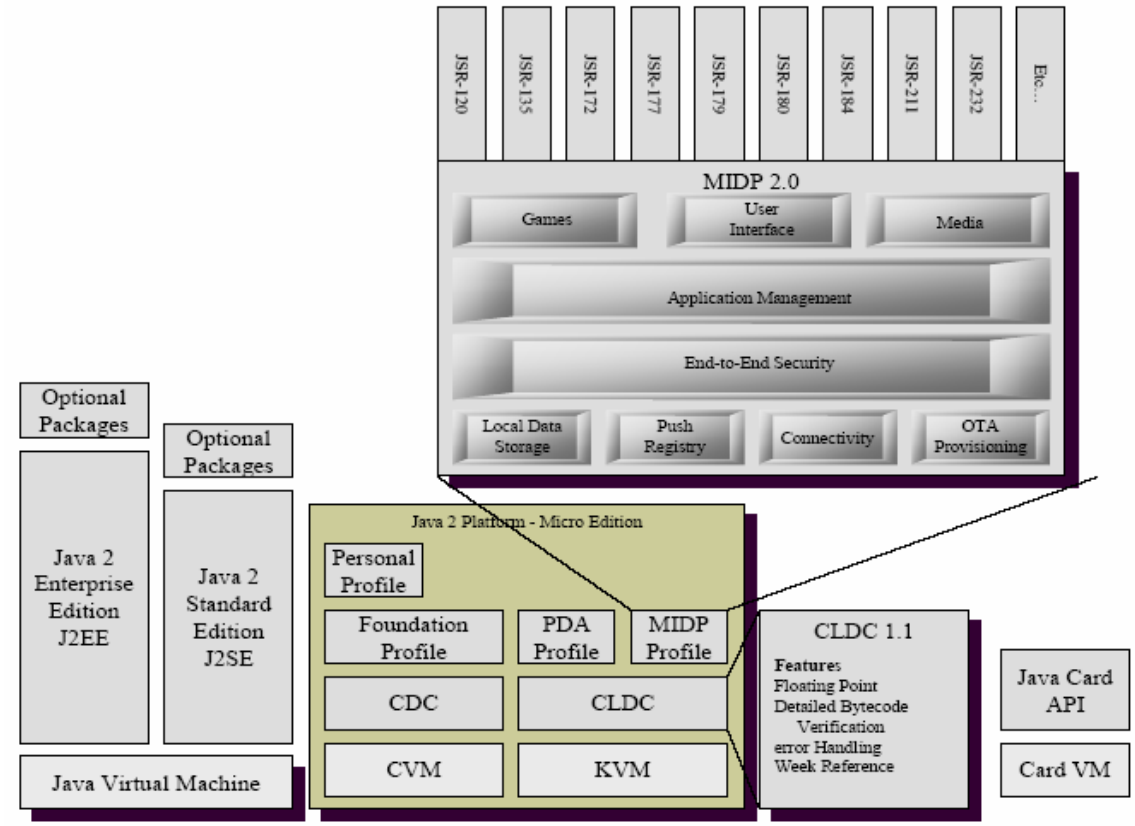
Table 48 : Data elements used in mobile payments:

Data element	Format	Description	TAG (EMV)	Bit no. in ISO 8583	Encrypt-ion	MAC'ing
Action code	n 4	See response Code		39	C	C
Amount Transaction Counter	n 12	Amount	9F02	4	C	M
Application Transaction Counter	b 2	SIM payment application transaction sequence counter, binary count	9F36	38	C	M
Approval code	anp 6	Issuer generated code of approval	(89)	14		C
Date, expiration	n 4			42	C	M
Merchant identifier	ans 15	Card acceptor ID code	9F16	43		C
Merchant name	ans 18	Short description of merchant's name	TBD!			C
Message text	ans 20	Message text for MT. Determined from Action Code or sever	TBD!			
MSISDN	ns .. 28	Assigned the SIM by the telecommunication company		52		
PIN	b 8	Personal Identification number (ISO 9564-1)				
POS entry mode	n 6	Conditional to entry and authentication method used		2		
Primary account number	n 11..19	Original payment card number		31	C	M
Print/display data	anscb.. 255	Notification of info and receipt	TBD!			
Protocol version number	b 1	Version of SIM protocol used	9F37	55		
RND, unpredictable number	b 4	SIM application generated true random number	9F06		C	M
SIM-application ID	b 5 – 16	SIM application identifier (AID) issued by ISO				
SIM-ID number	n 11..19	ITU issued Issuer-ID and individual SIM-ID number		11		
System trace audit number	N 6	Generated for each transaction attempt	9F29	55	C	M
Transaction certificate	b 8	MAC for Payment Accept Message	9F2A	49	C	M
Transaction currency code	n 3	Currency according to ISO 4217	9A	12	C	M
Transaction date	n 6	Local date of authorisation, YYMMDD	9F41	31	C	C
Transaction sequence counter	n 6	Acquirer reference data/ Order number	9C		C	M
Transaction type	b 1	Type of transaction and message	TBD!		C	C
Alias card number	an 12	Alias card name of payment card used			C	C

C = conditional security measures; M = mandatory security measures (encryption by 3 DES or PKI)

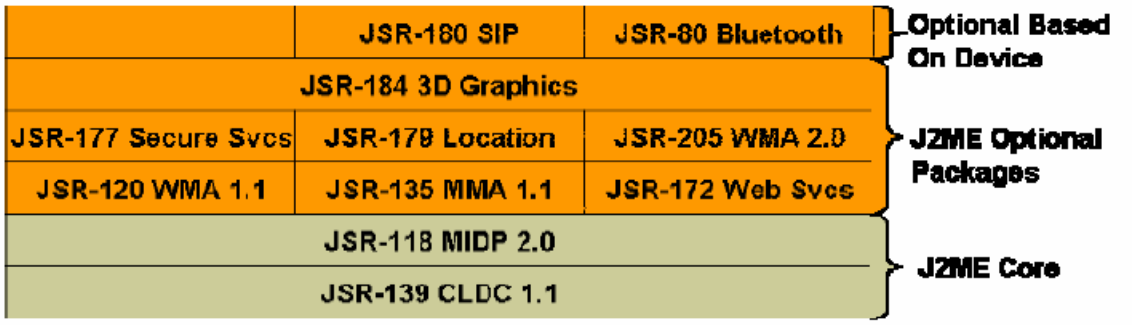
Source: ECBS, business and functional requirements for mobile payments

Figure 49 : JAVA Platform Architecture



Source: Original source : www.gemplus.com , and also Java platform evolution (Sun Microsystems and Java consortium)

Figure 50 : J2ME Platform



Source: Original source : www.gemplus.com , and also Java platform evolution (Sun Microsystems and Java consortium)

Table 51 : Forecasts for mobile transactions and revenue fee estimation for the Netherlands for the years 2005-2010, with a user penetration rate of 1% and 5% respectively, and an assumed growth rate for transactions of 1%/year , and a growth rate for mobile subscribers of 5% /year (assuming both subscriber growth and multiple phones per user from where transactions are made)

	Actual	**Actual**	**Forecast 1% growth in transactions/year**					
	2003	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**
Online number of subscribers in NL	7.149.000	7.235.932	7.323.921	7.412.980	7.503.121	7.594.359	7.686.707	7.780.177
mobile subscribers	13.100.000	13.755.000	14.442.750	15.164.888	15.923.132	16.719.288	17.555.253	18.433.016
e-payments (number of transactions /y)	3.267.000.000	3.477.000.000	3.511.770.000	3.546.887.700	3.582.356.577	3.618.180.143	3.654.361.944	3.690.905.564
m-payments (=e-payment*penetration rate; where penetration is 1%; unit/y)	32.670.000	34.770.000	35.117.700	35.468.877	35.823.566	36.181.801	36.543.619	36.909.056
m-payments (=e-payment*penetration rate; where penetration is 5%; unit/y)	163.350.000	173.850.000	175.588.500	177.344.385	179.117.829	180.909.007	182.718.097	184.545.278
ratio m-payments/subscribers (penetration rate is 1%); unit: transactions/y/subscriber	2,49	2,53	2,43	2,34	2,25	2,16	2,08	2,00
ratio m-payments/subscribers (penetration rate is 5%); unit: transactions/y/subscriber	12,47	12,64	12,16	11,69	11,25	10,82	10,41	10,01
Revenue estimation	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**
Number of transactions (penetration rate is 1%)	32.670.000	34.770.000	35.117.700	35.468.877	35.823.566	36.181.801	36.543.619	36.909.056
Fee revenue of 0,01 Euro	€ 326.700	€ 347.700	€ 351.177	€ 354.689	€ 358.236	€ 361.818	€ 365.436	€ 369.091
Fee revenue of 0,10	€ 3.267.000	€ 3.477.000	€ 3.511.770	€ 3.546.888	€ 3.582.357	€ 3.618.180	€ 3.654.362	€ 3.690.906
Fee revenue of 0,20	€ 6.534.000	€ 6.954.000	€ 7.023.540	€ 7.093.775	€ 7.164.713	€ 7.236.360	€ 7.308.724	€ 7.381.811
Number of transactions (penetration rate is 5%)	163.350.000	173.850.000	175.588.500	177.344.385	179.117.829	180.909.007	182.718.097	184.545.278
Fee revenue of 0,01 Euro	€ 1.633.500	€ 1.738.500	€ 1.755.885	€ 1.773.444	€ 1.791.178	€ 1.809.090	€ 1.827.181	€ 1.845.453
Fee revenue of 0,10	€ 16.335.000	€ 17.385.000	€ 17.558.850	€ 17.734.439	€ 17.911.783	€ 18.090.901	€ 18.271.810	€ 18.454.528
Fee revenue of 0,20	€ 32.670.000	€ 34.770.000	€ 35.117.700	€ 35.468.877	€ 35.823.566	€ 36.181.801	€ 36.543.619	€ 36.909.056

Figure 52 : Development of M-payment transactions in Netherlands using a user penetration rate of 1% or 5%

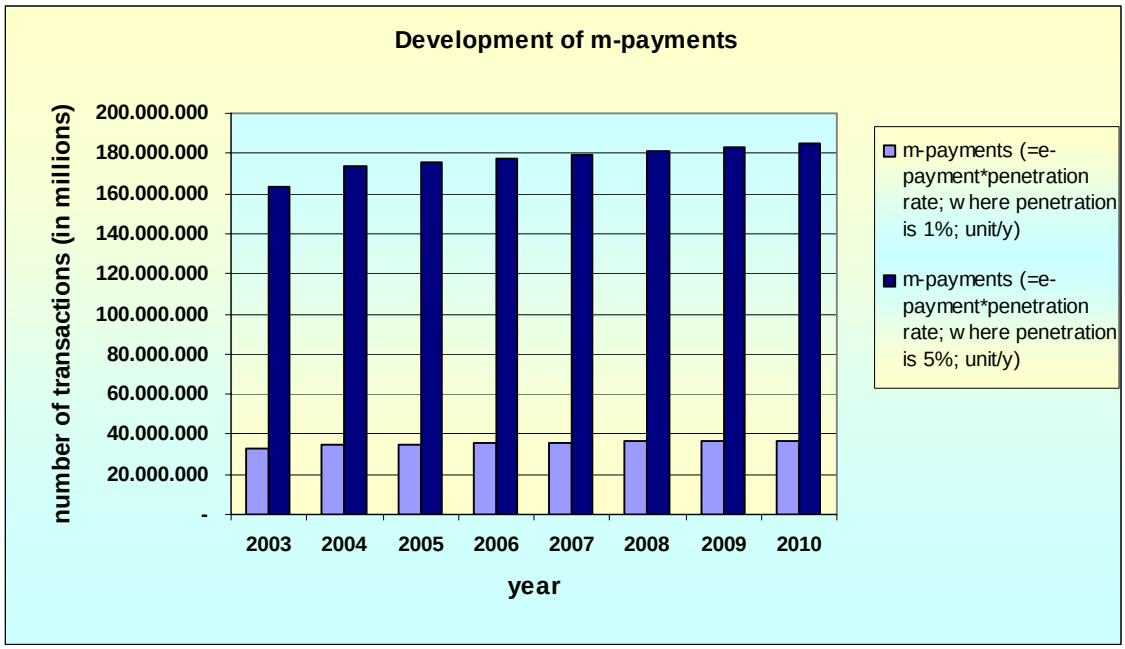
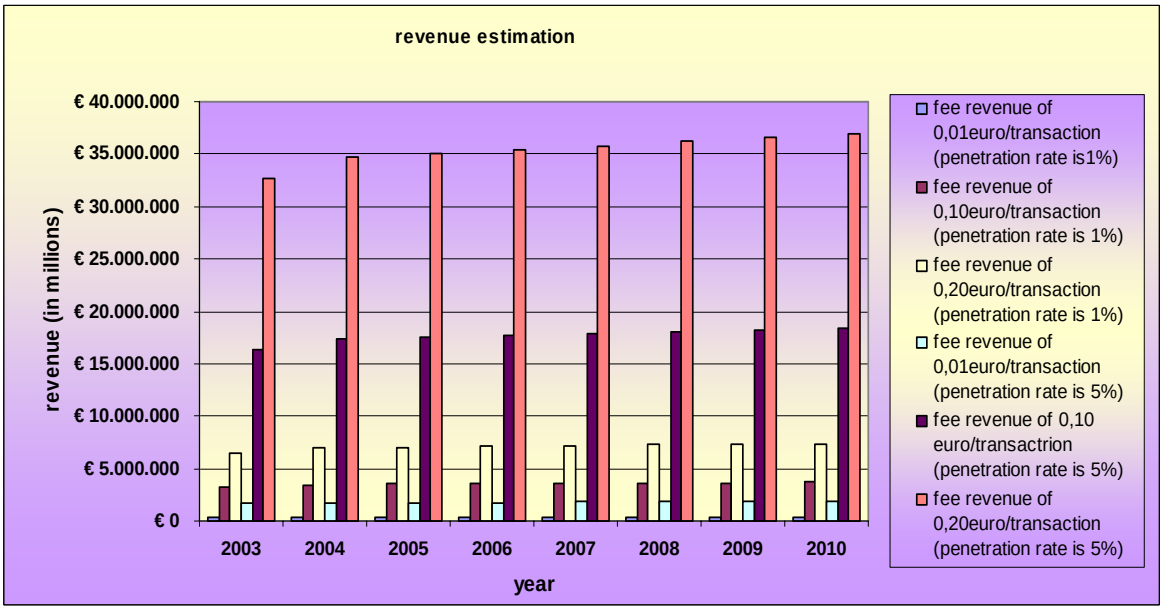


Figure 53 : Revenue estimation for the Netherlands based on M-payment end user penetration rates of 1% or 5%



Appendix 2

Table 54 : Indicators of the use of various cashless payment instruments in The Netherlands

Table 54.1: Volume of transactions

Indicators of the use of various cashless payment instruments in NL:
Volume of transactions *(in millions)*

	1999	2000	2001	2002	2003
Instruments					
Cheques	26,7	14,2	5,3	0,1	-
of which:					
face-to-face	26,7	14,2	5,3	0,1	-
via PC or other terminal	nap	nap	nap	nap	nap
Tele-banking	nap	nap	nap	nap	nap
via mobile phone	nap	nap	nap	nap	nap
Payment by debit card	700,3	801,5	954,4	1.068,60	1.157,10
of which:					
face-to-face	700,3	801,5	954,4	1.068,60	1.157,10
via PC or other terminal	nav	nav	nav	nav	nav
Tele-banking	nav	nav	nav	nav	nav
via mobile phone	nav	nav	nav	nav	nav
Payment by credit card	44,1	46,8	47,5	45,6	44,1
of which:					
face-to-face	44,1	46,8	47,5	45,6	44,1
via PC or other terminal	nav	nav	nav	nav	nav
Tele-banking	nap	nap	nap	nap	nap
via mobile phone	nav	nav	nav	nav	nav
Credit transfers	1.105,50	1.170,40	1.226,90	1.260,50	1.261,40
of which:					
face-to-face	1.105,50	1.170,40	1.226,90	1.260,50	1.261,40
via PC or other terminal	nav	nav	nav	nav	nav
Tele-banking	nav	nav	nav	nav	nav
via mobile phone	nav	nav	nav	nav	nav
Direct debits	785	836,2	876,1	947	990,1
of which:					
face-to-face	785	836,2	876,1	947	990,1
via PC or other terminal	nav	nav	nav	nav	nav
Tele-banking	nav	nav	nav	nav	nav
via mobile phone	nap	nap	nap	nap	nap
Card-based e-money	21,8	25,3	30,9	87	109,2
Network-based e-money	nap	nap	nap	nap	nap
Total	2.683,40	2.894,30	3.141,10	3.408,80	3.561,90

nap = not applicable; nav = not available;

Source: ECB Bluebook, payment and securities settlement systems in the European Union; august 2005

Table 54.2: Value of transactions

Indicators of the use of various cashless payment instruments in NL: Value of transactions *(EUR billions)*					
	1999	2000	2001	2002	2003
Instruments					
Cheques	2,1	1,8	0,5	-	-
of which:					
face-to-face	2,1	1,8	0,5	-	-
via PC or other terminal	nap	nap	nap	nap	nap
Tele-banking	nap	nap	nap	nap	nap
via mobile phone	nap	nap	nap	nap	nap
Payment by debit card	32	37,3	44,2	50,6	53,9
of which:					
face-to-face	32	37,3	44,2	50,6	53,9
via PC or other terminal	nav	nav	nav	nav	nav
Tele-banking	nav	nav	nav	nav	nav
via mobile phone	nav	nav	nav	nav	nav
Payment by credit card	4,4	5,2	5,3	5,3	4,9
of which:					
face-to-face	4,4	5,2	5,3	5,3	4,9
via PC or other terminal	nav	nav	nav	nav	nav
Tele-banking	nap	nap	nap	nap	nap
via mobile phone	nav	nav	nav	nav	nav
Credit transfers	2.368,90	2.863,60	3.279,90	3.363,70	3.587,80
of which:					
face-to-face	2.368,90	2.863,60	3.279,90	3.363,70	3.587,80
via PC or other terminal	nav	nav	nav	nav	nav
Tele-banking	nav	nav	nav	nav	nav
via mobile phone	nav	nav	nav	nav	nav
Direct debits	141	162	175,3	187,6	203,9
of which:					
face-to-face	141	162	175,3	187,6	203,9
via PC or other terminal	nav	nav	nav	nav	nav
Tele-banking	nav	nav	nav	nav	nav
via mobile phone	nav	nav	nav	nav	nav
Card-based e-money	0,1	0,1	0,1	0,2	0,3
Network-based e-money	nap	nap	nap	nap	nap
Total	2.548,40	3.069,90	3.505,20	3.607,40	3.850,80
nap = not applicable; nav = not available					

Source: ECB Bluebook, payment and securities settlement systems in the European Union; august 2005

Appendix 3

Table 55 : Payment instructions handled by selected inter-bank fund transfers in The Netherlands

Table 55.1: Volume of transactions handled by selected inter-bank fund transfers (in millions) in the Netherlands

Payment instructions handled by selected inter-bank fund transfer systems in NL: Volume of transactions
(millions)

	1999	2000	2001	2002	2003
Interpay	2,152.5	2,328.4	2,558.3	2,812.3	2,964.9
of which:					
cheques	*16.7*	*8.8*	*3.4*	*0.1*	-
other	*2,135.8*	*2,319.6*	*2,554.9*	*2,812.2*	*2,964.9*
Top	3.2	3.7	4.0	4.5	4.7
Concentration ratio[10]					
Interpay	96%	93%	93%	94%	nya
Top	62%	73%	67%	56%	55%

Source: ECB Bluebook, payment and securities settlement systems in the European Union; august 2005

Table 55.2: Value of transactions handled by selected inter-bank fund transfers (in EUR billions) in the Netherlands

Payment instructions handled by selected inter-bank fund transfer systems in NL: Value of transaction
(EUR billions)

	1999	2000	2001	2002	2003
Interpay	1,344.5	1,457.8	1,574.1	1,673.3	1,778.4
of which:					
cheques	*1.4*	*0.8*	*0.3*	*0.0*	-
other	*1,343.1*	*1,457.1*	*1,573.8*	*1,673.3*	*1,778.4*
Top	14,987	17,974	20,689	20,803	21,365
Concentration ratio					
Interpay	92%	92%	92%	93%	nya
Top	72%	74%	72%	78%	75%
nya = not yet available					

Source: ECB Bluebook, payment and securities settlement systems in the European Union; august 2005

[10] Concentration ratio: a way of measuring the concentration of market share held by particular suppliers in a market. "It is the percentage of total market sales accounted for by a given number of leading firms." Thus a four-firm concentration ratio is the total market share of the four firms with the largest market shares. (Sometimes this particular statistic is called the CR4).

Table 56 : Key figures on non-cash payments in The Netherlands (TOP, Interpay and credit card institutions)

Key figures on non-cash payment in The Netherlands *(millions of transactions)*	1999	2000	2001	2002	2003	2004
Electronic:						
Debit card	700	801	954	1.069	1.157	1.247
E-purse	22	25	31	87	109	127
Credit card	44	47	48	46	44	49
Direct debit	785	836	876	947	1.001	*1.055*
Electronic transfers	683	776	854	921	956	*1.000*
Total electronic	2.234	2.486	2.763	3.069	3.267	*3.477*
Paper:						
Euro-cheques, giro-cheques	27	13	5	0	0	*0*
Transfers	146	136	130	99	84	*73*
In-payment transfers	276	258	243	241	231	*215*
Total paper	450	407	378	339	316	*288*
Total retail payments	2.684	2.893	3.141	3.409	3.582	*3.765*

Source: De Nederlandsche bank, annual report 2004

Table 57 : Transactions processed by Interpay in the Netherlands (in millions)

Number of transactions processed (in millions)	1997	1998	1999	2000	2001	2002	2003	2004
POS terminal transactions	485,50	595,00	655,40	755,40	894,20	1.038,90	1.121,10	1.212,70
Collections and reversals	465,80	533,90	581,40	626,60	681,30	771,60	845,40	895,00
Business payments	284,30	293,90	303,30	313,70	327,90	337,60	340,20	346,30
Converted transfers	164,10	179,80	194,40	210,30	225,50	238,80	236,70	251,00
Accept-giros (giro transfers)	221,10	217,40	207,20	197,80	191,50	182,10	176,70	167,00
ATM 'guest' transactions'	78,30	109,40	142,70	134,00	145,80	152,00	149,60	151,90
ATM domestic transactions	-	9,20	11,40	13,60	14,60	13,60	13,70	13,90
ATM foreign transactions	-	11,90	11,90	12,70	14,30	14,10	15,20	16,30
Regular transfers	39,00	41,90	44,90	48,70	52,80	56,60	59,60	63,20
Tele-giro (urgent traffic)	4,70	5,20	5,90	6,10	5,60	5,80	6,10	6,40
Guaranteed cheques (formerly euro-cheques)	23,80	17,80	10,30	5,20	1,90	0,00	0,00	0,00
Euro traveller's cheques	1,90	1,60	1,30	1,00	0,50	0,00	0,00	0,00
Girocheques	14,20	9,80	5,80	2,70	0,90	0,00	0,00	0,00
Mass payments	0,10	0,30	0,40	0,60	0,70	0,80	0,80	0,60
Total number of transactions processed	1.782,80	2.006,00	2.153,00	2.328,40	2.558,30	2.812,30	2.965,00	3.123,50

Source: Annual reports Interpay 1998 - 2004

Appendix 4:

Table 58 : Comparison of costs of various payment methods used in The Netherlands

Table 58.1: 'Frequent' Usage scenario

Scenario of 'frequent' use, using an end user penetration rate of 5%									
total costs based on number of transactions									
	price/transaction	*2003*	*2004*	*2005*	*2006*	*2007*	*2008*	*2009*	*2010*
Credit card	€ 3,587	€ 585.936.450	€ 623.599.950	€ 629.835.950	€ 636.134.309	€ 642.495.652	€ 648.920.609	€ 655.409.815	€ 661.963.913
Debit card	€ 0,486	€ 79.388.100	€ 84.491.100	€ 85.336.011	€ 86.189.371	€ 87.051.265	€ 87.921.777	€ 88.800.995	€ 89.689.005
Cash	€ 0,300	€ 49.005.000	€ 52.155.000	€ 52.676.550	€ 53.203.316	€ 53.735.349	€ 54.272.702	€ 54.815.429	€ 55.363.583
E-purse	€ 0,931	€ 152.078.850	€ 161.854.350	€ 163.472.894	€ 165.107.622	€ 166.758.699	€ 168.426.286	€ 170.110.549	€ 171.811.654
*Note: the same number of transactions are used to determine the total costs, as that will allow us to make a comparison between the various methods. We used the number of mobile transaction in 2003 and used a penetration rate of 5% in this scenario to estimate the number of mobile transactions made per year. Moreover, the number of mobile transactions were determined as follows: e-payment*penetration rate. The prices per transaction were obtained from DNB, payments are no free lunch.*									

Table 58.2: 'Low' usage scenario

Scenario of 'low' usage, using an end user penetration rate of 1%									
total costs based on number of transactions									
	price/transaction	*2003*	*2004*	*2005*	*2006*	*2007*	*2008*	*2009*	*2010*
Credit card	€ 3,587	€ 117.187.290	€ 124.719.990	€ 125.967.190	€ 127.226.862	€ 128.499.130	€ 129.784.122	€ 131.081.963	€ 132.392.783
Debit card	€ 0,486	€ 15.877.620	€ 16.898.220	€ 17.067.202	€ 17.237.874	€ 17.410.253	€ 17.584.355	€ 17.760.199	€ 17.937.801
Cash	€ 0,300	€ 9.801.000	€ 10.431.000	€ 10.535.310	€ 10.640.663	€ 10.747.070	€ 10.854.540	€ 10.963.086	€ 11.072.717
E-purse	€ 0,931	€ 30.415.770	€ 32.370.870	€ 32.694.579	€ 33.021.524	€ 33.351.740	€ 33.685.257	€ 34.022.110	€ 34.362.331
*Note: the same number of transactions are used to determine the total costs, as that will allow us to make a comparison between the various methods. We used the number of mobile transaction in 2003 and used a penetration rate of 1% in this scenario to estimate the number of mobile transactions made per year. Moreover, the number of mobile transactions were determined as follows: e-payment*penetration rate. The prices per transaction were obtained from DNB, payments are no free lunch.*									

Table 59 : Average price for making a transaction (Norway's' price is based on giro payment with mobile phone)

E-purse transaction cost/transaction in NL	€ 0,931
Average price for paying giro with mobile device/ transaction in Norway[11]	€ 0,49
Cost per internet transaction in Norway[12]	€ 0,21

Table 60 : Comparison of total costs for mobile transactions in The Netherlands, applying a price / transaction of € 0,931; € 0,49, € 0,21 respectively to the mobile transactions assuming an end user penetration rate of 1% and 5%

	2003	2004	2005	2006	2007	2008	2009	2010
Mobile transactions (penetration rate 1%)	32.670.000	34.770.000	35.117.700	35.468.877	35.823.566	36.181.801	36.543.619	36.909.056
If m-transaction cost is assumed to be 0,931eurocent/transaction	€ 30.415.770	€ 32.370.870	€ 32.694.579	€ 33.021.524	€ 33.351.740	€ 33.685.257	€ 34.022.110	€ 34.362.331
If m-transaction cost is assumed to be 0,49eurocent/transaction	€ 16.008.300	€ 17.037.300	€ 17.207.673	€ 17.379.750	€ 17.553.547	€ 17.729.083	€ 17.906.374	€ 18.085.437
If m-transaction cost is assumed to be 0,21 eurocent/transaction	€ 6.860.700	€ 7.301.700	€ 7.374.717	€ 7.448.464	€ 7.522.949	€ 7.598.178	€ 7.674.160	€ 7.750.902
Mobile transactions (penetration rate 5%)	163.350.000	173.850.000	175.588.500	177.344.385	179.117.829	180.909.007	182.718.097	184.545.278
If m-transaction cost is assumed to be 0,931eurocent/transaction	€ 152.078.850,00	€ 161.854.350,00	€ 163.472.893,50	€ 165.107.622,44	€ 166.758.698,66	€ 168.426.285,65	€ 170.110.548,50	€ 171.811.653,99
If m-transaction cost is assumed to be 0,49eurocent/transaction	€ 80.041.500,00	€ 85.186.500,00	€ 86.038.365,00	€ 86.898.748,65	€ 87.767.736,14	€ 88.645.413,50	€ 89.531.867,63	€ 90.427.186,31
If m-transaction cost is assumed to be 0,21 eurocent/transaction	€ 34.303.500,00	€ 36.508.500,00	€ 36.873.585,00	€ 37.242.320,85	€ 37.614.744,06	€ 37.990.891,50	€ 38.370.800,41	€ 38.754.508,42

[11] Source: annual report Norges Bank 2004
[12] Source: [39] National forum on the payment system, report 2004

Scenario 1: WAP based M-banking services

The following assumptions were made in this scenario:

- An enquiry based service takes, on average, 1 minute
- A transaction based services takes on average 2 minutes
- The number of mobile transactions was equally divided among enquiry-based mobile banking services and transaction-based mobile banking services in the following scenarios.

Table 61 : Price charged per minute

WAP based	
	Price per minute
Normal price per minute	€ 0,24
100 minutes	€ 0,18
250 minutes	€ 0,13
500 minutes	€ 0,08
1000 minutes	€ 0,05

Table 62: Average cost to the customer, based on the price/minute mentioned in the table 61 above

	Enquiry-based service	*Transaction-based service*
Average costs for the customer[13]	€ 0,24	€ 0,48
Average costs for the customer[14]	€ 0,18	€ 0,36
Average costs for the customer[15]	€ 0,13	€ 0,26
Average costs for the customer[16]	€ 0,08	€ 0,16
Average costs for the customer[17]	€ 0,05	€ 0,10

[13] Assuming that the customer is charged the normal price per minute
[14] Assuming the customer buys a 100 minute bundle
[15] Assuming the customer buys a 250 minute bundle
[16] Assuming the customer buys a 500 minute bundle
[17] Assuming the customer buys a 1000 minute bundle

Table 63: Additional costs to the customer

Additional costs for the customer:	
1. Charges by the bank for making use of m-banking services[18]	€ 1,00[19]
2. The customer needs a mobile phone that provides the possibility to make use of m-banking/m-payment services,	€ 400 - € 800[20]
In case the customer doesn't have one, he needs to buy one.	

[18] Rabobank does not provide transaction services, except between own accounts or via bank-giro/accept-giro, but transfer is only possible to bank accounts to which you have transferred money before. For more details about which mobile banking services Rabobank provides see: http://www.rabobank.nl/info/execute/node?node_id=269585&tab=1

[19] This tariff is based on Rabobank, see:
http://www.rabobank.nl/info/execute/node?node_id=269585&tab=2

[20] Most of the mobile phones (we have looked at the possibilities of Rabobank with KPN, Orange, T-Mobile and Vodafone) are 'handset free', but you have to sign a contract for a certain number of months ranging from 12-18 months often and prices per month vary from 30 euro - 40 euro.

Table 64: WAP-based Scenario: frequent use of m-payment services, assuming a penetration rate of 5% and the average costs per transaction as mentioned in table 62

Scenario 1.1: Frequent use, using WAP: assuming an end user penetration rate of 5%,								
	2003	2004	2005	2006	2007	2008	2009	2010
Mobile transactions	163.350.000	173.850.000	175.588.500	177.344.385	179.117.829	180.909.007	182.718.097	184.545.278
Enquiry-based services	81.675.000	86.925.000	87.794.250	88.672.193	89.558.914	90.454.504	91.359.049	92.272.639
Transaction-based services	81.675.000	86.925.000	87.794.250	88.672.193	89.558.914	90.454.504	91.359.049	92.272.639
Costs assuming:								
Normal price:								
1. Enquiry based services	€ 19.602.000	€ 20.862.000	€ 21.070.620	€ 21.281.326	€ 21.494.139	€ 21.709.081	€ 21.926.172	€ 22.145.433
2. Transaction based services	€ 39.204.000	€ 41.724.000	€ 42.141.240	€ 42.562.652	€ 42.988.279	€ 43.418.162	€ 43.852.343	€ 44.290.867
Total costs	*€ 58.806.000*	*€ 62.586.000*	*€ 63.211.860*	*€ 63.843.979*	*€ 64.482.418*	*€ 65.127.243*	*€ 65.778.515*	*€ 66.436.300*
100 minutes bundle:								
1. Enquiry based services	€ 14.701.500	€ 15.646.500	€ 15.802.965	€ 15.960.995	€ 16.120.605	€ 16.281.811	€ 16.444.629	€ 16.609.075
2. Transaction based services	€ 29.403.000	€ 31.293.000	€ 31.605.930	€ 31.921.989	€ 32.241.209	€ 32.563.621	€ 32.889.257	€ 33.218.150
Total costs	*€ 44.104.500*	*€ 46.939.500*	*€ 47.408.895*	*€ 47.882.984*	*€ 48.361.814*	*€ 48.845.432*	*€ 49.333.886*	*€ 49.827.225*
250 minutes bundle:								
1. Enquiry based services	€ 10.617.750	€ 11.300.250	€ 11.413.253	€ 11.527.385	€ 11.642.659	€ 11.759.085	€ 11.876.676	€ 11.995.443
2. Transaction based services	€ 21.235.500	€ 22.600.500	€ 22.826.505	€ 23.054.770	€ 23.285.318	€ 23.518.171	€ 23.753.353	€ 23.990.886
Total costs	*€ 31.853.250*	*€ 33.900.750*	*€ 34.239.758*	*€ 34.582.155*	*€ 34.927.977*	*€ 35.277.256*	*€ 35.630.029*	*€ 35.986.329*
500 minutes bundle:								
1. Enquiry based services	€ 6.534.000	€ 6.954.000	€ 7.023.540	€ 7.093.775	€ 7.164.713	€ 7.236.360	€ 7.308.724	€ 7.381.811
2. Transaction based services	€ 13.068.000	€ 13.908.000	€ 14.047.080	€ 14.187.551	€ 14.329.426	€ 14.472.721	€ 14.617.448	€ 14.763.622
Total costs	*€ 19.602.000*	*€ 20.862.000*	*€ 21.070.620*	*€ 21.281.326*	*€ 21.494.139*	*€ 21.709.081*	*€ 21.926.172*	*€ 22.145.433*
1000 minutes bundle:								
1. Enquiry based services	€ 4.083.750	€ 4.346.250	€ 4.389.713	€ 4.433.610	€ 4.477.946	€ 4.522.725	€ 4.567.952	€ 4.613.632
2. Transaction based services	€ 8.167.500	€ 8.692.500	€ 8.779.425	€ 8.867.219	€ 8.955.891	€ 9.045.450	€ 9.135.905	€ 9.227.264
Total costs	*€ 12.251.250*	*€ 13.038.750*	*€ 13.169.138*	*€ 13.300.829*	*€ 13.433.837*	*€ 13.568.176*	*€ 13.703.857*	*€ 13.840.896*

Table 65: WAP-based scenario: Low use of m-payment services, assuming a penetration rate of 1% and the average costs per transaction as mentioned in table 62

Scenario 1.2: Low use, using WAP, assuming an end user penetration rate of 1%								
	2003	2004	2005	2006	2007	2008	2009	2010
Mobile transactions	32.670.000	34.770.000	35.117.700	35.468.877	35.823.566	36.181.801	36.543.619	36.909.056
Enquiry-based services	16.335.000	17.385.000	17.558.850	17.734.439	17.911.783	18.090.901	18.271.810	18.454.528
Transaction-based services	16.335.000	17.385.000	17.558.850	17.734.439	17.911.783	18.090.901	18.271.810	18.454.528
Costs assuming:								
Normal price:								
1. Enquiry based services	€ 3.920.400	€ 4.172.400	€ 4.214.124	€ 4.256.265	€ 4.298.828	€ 4.341.816	€ 4.385.234	€ 4.429.087
2. Transaction based services	€ 7.840.800	€ 8.344.800	€ 8.428.248	€ 8.512.530	€ 8.597.656	€ 8.683.632	€ 8.770.469	€ 8.858.173
Total costs	*€ 11.761.200*	*€ 12.517.200*	*€ 12.642.372*	*€ 12.768.796*	*€ 12.896.484*	*€ 13.025.449*	*€ 13.155.703*	*€ 13.287.260*
100 minutes bundle:								
1. Enquiry based services	€ 2.940.300	€ 3.129.300	€ 3.160.593	€ 3.192.199	€ 3.224.121	€ 3.256.362	€ 3.288.926	€ 3.321.815
2. Transaction based services	€ 5.880.600	€ 6.258.600	€ 6.321.186	€ 6.384.398	€ 6.448.242	€ 6.512.724	€ 6.577.851	€ 6.643.630
Total costs	*€ 8.820.900*	*€ 9.387.900*	*€ 9.481.779*	*€ 9.576.597*	*€ 9.672.363*	*€ 9.769.086*	*€ 9.866.777*	*€ 9.965.445*
250 minutes bundle:								
1. Enquiry based services	€ 2.123.550	€ 2.260.050	€ 2.282.651	€ 2.305.477	€ 2.328.532	€ 2.351.817	€ 2.375.335	€ 2.399.089
2. Transaction based services	€ 4.247.100	€ 4.520.100	€ 4.565.301	€ 4.610.954	€ 4.657.064	€ 4.703.634	€ 4.750.671	€ 4.798.177
Total costs	*€ 6.370.650*	*€ 6.780.150*	*€ 6.847.952*	*€ 6.916.431*	*€ 6.985.595*	*€ 7.055.451*	*€ 7.126.006*	*€ 7.197.266*
500 minutes bundle:								
1. Enquiry based services	€ 1.306.800	€ 1.390.800	€ 1.404.708	€ 1.418.755	€ 1.432.943	€ 1.447.272	€ 1.461.745	€ 1.476.362
2. Transaction based services	€ 2.613.600	€ 2.781.600	€ 2.809.416	€ 2.837.510	€ 2.865.885	€ 2.894.544	€ 2.923.490	€ 2.952.724
Total costs	*€ 3.920.400*	*€ 4.172.400*	*€ 4.214.124*	*€ 4.256.265*	*€ 4.298.828*	*€ 4.341.816*	*€ 4.385.234*	*€ 4.429.087*
1000 minutes bundle:								
1. Enquiry based services	€ 816.750	€ 869.250	€ 877.943	€ 886.722	€ 895.589	€ 904.545	€ 913.590	€ 922.726
2. Transaction based services	€ 1.633.500	€ 1.738.500	€ 1.755.885	€ 1.773.444	€ 1.791.178	€ 1.809.090	€ 1.827.181	€ 1.845.453
Total costs	*€ 2.450.250*	*€ 2.607.750*	*€ 2.633.828*	*€ 2.660.166*	*€ 2.686.767*	*€ 2.713.635*	*€ 2.740.771*	*€ 2.768.179*

Scenario 2: SMS based M-banking services

The following assumptions were made:

- An enquiry based service takes 0,2 MB
- A transaction based service takes 0,5 MB
- The number of mobile transactions was equally divided among enquiry-based mobile banking services and transaction based mobile banking services in the following scenarios.

Table 66: Price per MB

SMS based	
	Price per MB
Normal price per MB	€ 2,83
10 MB	€ 1,79
25 MB	€ 1,31
50 MB	€ 0,83
100 MB	€ 0,51

Table 67: Average number of MB required per m-payment transaction

Average MB required per enquiry-based service	0,2
Average MB required per transaction-based service	0,5

Table 68: Average cost to the customer for an m-payment transaction

	Enquiry-based service	*Transaction-based service*
Average costs for the customer per service[21]	€ 0,57	€ 1,42
Average costs for the customer per service[22]	€ 0,36	€ 0,90
Average costs for the customer per service[23]	€ 0,26	€ 0,66
Average costs for the customer per service[24]	€ 0,17	€ 0,42
Average costs for the customer per service[25]	€ 0,10	€ 0,26

Table 69: Additional costs to the customer

Additional costs for the customer:	
1. Charges by the bank for making use of m-banking services	€ 1,00[26]
2. The customer needs a mobile phone that provides the possibility to make use of m-banking/m-payment services,	€ 400 - € 800[27]
In case the customer doesn't have one, he needs to buy one.	

[21] Assuming that the customer pays the normal price per MB.
[22] Assuming that the customer buys a 10 MB bundle.
[23] Assuming that the customer will buy a 25 MB bundle.
[24] Assuming that the customer will buy a 50 MB bundle.
[25] Assuming that the customer will buy a 100 MB bundle.
[26] This tariff is based on Rabobank. See:
http://www.rabobank.nl/info/execute/node?node_id=269585&tab=2
[27] Most of the mobile phones (we have looked at the possibilities of Rabobank with KPN, Orange, T-Mobile and Vodafone) are 'handset free', but you have to sign a contract for a certain number of months ranging from 12-18 months often and prices per month vary from 30 euro - 40 euro.

Table 70: SMS-based Scenario: Frequent use of m-payment transactions, assuming a penetration rate of 5% and average costs per transaction as mentioned in table 68

Scenario 2.1: Frequent use, SMS based, assuming a penetration rate of 5%,								
	2003	2004	2005	2006	2007	2008	2009	2010
Mobile transactions	163.350.000	173.850.000	175.588.500	177.344.385	179.117.829	180.909.007	182.718.097	184.545.278
Enquiry-based services	81.675.000	86.925.000	87.794.250	88.672.193	89.558.914	90.454.504	91.359.049	92.272.639
Transaction-based services	81.675.000	86.925.000	87.794.250	88.672.193	89.558.914	90.454.504	91.359.049	92.272.639
Costs assuming:								
Normal price per MB:								
1. Enquiry based services	€ 46.228.050	€ 49.199.550	€ 49.691.546	€ 50.188.461	€ 50.690.346	€ 51.197.249	€ 51.709.222	€ 52.226.314
2. Transaction based services	€ 115.570.125	€ 122.998.875	€ 124.228.864	€ 125.471.152	€ 126.725.864	€ 127.993.123	€ 129.273.054	€ 130.565.784
Total costs	*€ 161.798.175*	*€ 172.198.425*	*€ 173.920.409*	*€ 175.659.613*	*€ 177.416.209*	*€ 179.190.372*	*€ 180.982.275*	*€ 182.792.098*
10 MB bundle:								
1. Enquiry based services	€ 29.239.650	€ 31.119.150	€ 31.430.342	€ 31.744.645	€ 32.062.091	€ 32.382.712	€ 32.706.539	€ 33.033.605
2. Transaction based services	€ 73.099.125	€ 77.797.875	€ 78.575.854	€ 79.361.612	€ 80.155.228	€ 80.956.781	€ 81.766.349	€ 82.584.012
Total costs	*€ 102.338.775*	*€ 108.917.025*	*€ 110.006.195*	*€ 111.106.257*	*€ 112.217.320*	*€ 113.339.493*	*€ 114.472.888*	*€ 115.617.617*
25 MB bundle:								
1. Enquiry based services	€ 21.398.850	€ 22.774.350	€ 23.002.094	€ 23.232.114	€ 23.464.436	€ 23.699.080	€ 23.936.071	€ 24.175.431
2. Transaction based services	€ 53.497.125	€ 56.935.875	€ 57.505.234	€ 58.080.286	€ 58.661.089	€ 59.247.700	€ 59.840.177	€ 60.438.579
Total costs	*€ 74.895.975*	*€ 79.710.225*	*€ 80.507.327*	*€ 81.312.401*	*€ 82.125.525*	*€ 82.946.780*	*€ 83.776.248*	*€ 84.614.010*
50 MB bundle:								
1. Enquiry based services	€ 13.558.050	€ 14.429.550	€ 14.573.846	€ 14.719.584	€ 14.866.780	€ 15.015.448	€ 15.165.602	€ 15.317.258
2. Transaction based services	€ 33.895.125	€ 36.073.875	€ 36.434.614	€ 36.798.960	€ 37.166.949	€ 37.538.619	€ 37.914.005	€ 38.293.145
Total costs	*€ 47.453.175*	*€ 50.503.425*	*€ 51.008.459*	*€ 51.518.544*	*€ 52.033.729*	*€ 52.554.067*	*€ 53.079.607*	*€ 53.610.403*
100 MB minutes bundle:								
1. Enquiry based services	€ 8.330.850	€ 8.866.350	€ 8.955.014	€ 9.044.564	€ 9.135.009	€ 9.226.359	€ 9.318.623	€ 9.411.809
2. Transaction based services	€ 20.827.125	€ 22.165.875	€ 22.387.534	€ 22.611.409	€ 22.837.523	€ 23.065.898	€ 23.296.557	€ 23.529.523
Total costs	*€ 29.157.975*	*€ 31.032.225*	*€ 31.342.547*	*€ 31.655.973*	*€ 31.972.532*	*€ 32.292.258*	*€ 32.615.180*	*€ 32.941.332*

Table 71: SMS-based Scenario: Low use of m-payment transactions, assuming a penetration rate of 1% and an average cost for making an m-payment transaction as mentioned in table 68

Scenario: Low use, SMS based, assuming a penetration rate of 1%,								
	2003	2004	2005	2006	2007	2008	2009	2010
Mobile transactions	32.670.000	34.770.000	35.117.700	35.468.877	35.823.566	36.181.801	36.543.619	36.909.056
Enquiry-based services	16.335.000	17.385.000	17.558.850	17.734.439	17.911.783	18.090.901	18.271.810	18.454.528
Transaction-based services	16.335.000	17.385.000	17.558.850	17.734.439	17.911.783	18.090.901	18.271.810	18.454.528
Costs assuming:								
Normal price per MB:								
1. Enquiry based services	€ 9.245.610	€ 9.839.910	€ 9.938.309	€ 10.037.692	€ 10.138.069	€ 10.239.450	€ 10.341.844	€ 10.445.263
2. Transaction based services	€ 23.114.025	€ 24.599.775	€ 24.845.773	€ 25.094.230	€ 25.345.173	€ 25.598.625	€ 25.854.611	€ 26.113.157
Total costs	*€ 32.359.635*	*€ 34.439.685*	*€ 34.784.082*	*€ 35.131.923*	*€ 35.483.242*	*€ 35.838.074*	*€ 36.196.455*	*€ 36.558.420*
10 MB bundle:								
1. Enquiry based services	€ 5.847.930	€ 6.223.830	€ 6.286.068	€ 6.348.929	€ 6.412.418	€ 6.476.542	€ 6.541.308	€ 6.606.721
2. Transaction based services	€ 14.619.825	€ 15.559.575	€ 15.715.171	€ 15.872.322	€ 16.031.046	€ 16.191.356	€ 16.353.270	€ 16.516.802
Total costs	*€ 20.467.755*	*€ 21.783.405*	*€ 22.001.239*	*€ 22.221.251*	*€ 22.443.464*	*€ 22.667.899*	*€ 22.894.578*	*€ 23.123.523*
25 MB bundle:								
1. Enquiry based services	€ 4.279.770	€ 4.554.870	€ 4.600.419	€ 4.646.423	€ 4.692.887	€ 4.739.816	€ 4.787.214	€ 4.835.086
2. Transaction based services	€ 10.699.425	€ 11.387.175	€ 11.501.047	€ 11.616.057	€ 11.732.218	€ 11.849.540	€ 11.968.035	€ 12.087.716
Total costs	*€ 14.979.195*	*€ 15.942.045*	*€ 16.101.465*	*€ 16.262.480*	*€ 16.425.105*	*€ 16.589.356*	*€ 16.755.250*	*€ 16.922.802*
50 MB bundle:								
1. Enquiry based services	€ 2.711.610	€ 2.885.910	€ 2.914.769	€ 2.943.917	€ 2.973.356	€ 3.003.090	€ 3.033.120	€ 3.063.452
2. Transaction based services	€ 6.779.025	€ 7.214.775	€ 7.286.923	€ 7.359.792	€ 7.433.390	€ 7.507.724	€ 7.582.801	€ 7.658.629
Total costs	*€ 9.490.635*	*€ 10.100.685*	*€ 10.201.692*	*€ 10.303.709*	*€ 10.406.746*	*€ 10.510.813*	*€ 10.615.921*	*€ 10.722.081*
100 MB minutes bundle:								
1. Enquiry based services	€ 1.666.170	€ 1.773.270	€ 1.791.003	€ 1.808.913	€ 1.827.002	€ 1.845.272	€ 1.863.725	€ 1.882.362
2. Transaction based services	€ 4.165.425	€ 4.433.175	€ 4.477.507	€ 4.522.282	€ 4.567.505	€ 4.613.180	€ 4.659.311	€ 4.705.905
Total costs	*€ 5.831.595*	*€ 6.206.445*	*€ 6.268.509*	*€ 6.331.195*	*€ 6.394.506*	*€ 6.458.452*	*€ 6.523.036*	*€ 6.588.266*

12. Bibliography and Additional Bibliography

[1] Mobile payment forum (2002) , White paper: “Enabling Secure, Interoperable and User-friendly mobile payments”, December 2002;

Mobile payment definition: page 10

Figure 2 - Mobile infrastructure and payment process: page 12

[2] Rabobank no.1, “Institutional solutions”:
http://www.rabobank.com/content/services/institutes/payment_services/correspondent_banking/payment_systems.jsp
“Information retrieved from this site in May 2005.”

[3] ECB Bluebook (2001), “Payment systems in The Netherlands”, June 2001, Frankfurt a/Main

Section - Interpay B.V.: page 345

Section - TOP: page 351

Section - Legal aspects in respect of payments: pages 340 - 341

Section - TARGET: page 351 ,

[4] Mobey forum (2001) , Preferred payment architecture – technical documentation ;

Figure 3 - Components of the preferred payment architecture: page 36

Section - Payment protocols: pages 28 - 29

Section - SWOT analysis of Technical solutions: pages 14 - 22

[5] Mobile Electronic Transactions Forum(MeT) (2002), Personal Transaction Protocol Version 1.0;

Figure 3.1 – The PTP Architecture: page 12

Figure 3.2 – The PCD Architecture: page 75

[6] Gartner Inc (continuously updated), glossary:
http://www.gartner.com/6_help/glossary/GlossaryR.jsp

[7] Pau, L-F (2004), Mobile operators as banks or vice-versa? and: the challenges of mobile channels for banks, ERIM Research report ERS-2004-015-LIS , January 2004 http://hdl.handle.net/1765/1663 ; and : Proc. 3 rd Austin Mobility Roundtable , Austin , TX, 10-12 March 2004

Section - Payment/Transactions Infrastructure: page 4

[8] Commission of The European Communities, Communication from The Commission to The Council, The European Parliament, The European Economic and Social Committee and The Committee of The Regions, Mobile Broadband Services; Brussels
http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2004/com2004_0447en01.pdf

Section – Interoperability Requirements: page 5

[9] Smart-IS A.M. and eESC TB12 AES, Open Smart Card Infrastructure for Europe *v2*; Volume 4: Public Electronic Identity, Electronic Signature and PKI, Part 7: Telecom Operator Requirements;

Appendix 1, Table 1 – Interoperability Issues dealing with particular aspects of GSM/WAP environment: page 79

[10] European Committee for Banking Standards (2003), Interoperability of Bank Trust Services; TR 604 – Version 1 – July 2003, Brussels;

Section - Banking Standards: Table 2 Appendix 1

[11] Karnouskos,S. and Vilmos,A (2004) ., The European Perspective on Mobile Payments ; http://www.semops.com/uploadfiles/SEMOPS_Sympotic2004.pdf

Section - the de facto standards and interoperable payment platforms of banks and payment institutions - Consortia: page 1

[12] Durlacher research Ltd (Date unknown)) , Mobile Commerce Report;

Section - Mobile payment platforms: page 26

Section - Mobile banking platforms: page 27

Table 3 – Main m-banking & m-broking technology players : page 27

Section - Business estimation case :

Figure 5.1 - Mobile and internet subscribers Europe: page 12

Figure 5.2 - Mobile penetration in Europe : page 11

Section - Mobile financial services:

Mobile banking services: page 42

Mobile broking services: page 43

Mobile cash: page 43

Mobile payments: page 44

Mobile e-bill: page 46

Mobile e-salary: page 46

Mobile Security Services, Mobile Shopping, Mobile Dynamic Information Management, Mobile Information Provisioning, Mobile Entertainment: pages 46 - 55

Section about Creation of revenue, number of users: page 60

[13] FINREAD project; www.finread.com

[14] FINEAD (2003) , CWA 14174-4 “Financial transactional IC card reader (FINREAD) – Part 4: Architectural overview” Review, CEN ISSS, 2003; France: http://www.finread.com/pages/about/specifications/01_specifications.html
“Information retrieved from this site in August 2005”

Section – FINREAD

[15] European Committee for Banking Standards, Business and Functional Requirements for Mobile Payments (2003); TR 603 – Version 1 – February 2003;

Section - The de facto standards used:

Protocols: page 29

Data elements: page 29

Appendix 1, Table 3 - Data elements used in m-payments: page 60

Section - SWOT analysis of technical solutions: page 38 - 46

Section - Case of Postbank: page 52

[16] JAVA Standards: Java Consortium www.java.org ,and Sun Microsystems, and www.gemplus.com

[17] Little, A.D. Ltd , (2004), Global M-payment report 2004,

Figure 4 – Mobile penetration, bank account penetration and card payment penetration as share of GDP: page 144

[18] Official Journal of European Communities (1997) , Official Journal 208 of 02.08.1997, 'Act' Recommendation 97/489/EC concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, Brussels
http://www.europa.eu.int/scadplus/leg/en/lvb/l24182.htm

[19] European Communities (2001) , A possible legal framework for the single payment area in the internal market, European Commission - Internal market DG – Financial institutions – Retail issues and payment systems (Payment Systems Market Group & Payment Systems Government Group), Working document ; MARKT/208/2001 – Rev.1 ; Brussels

Section – Legal responsibility in case of a payment network breakdown : page 21

Consequential damage : page 30

Section – Identification originator in payment process: page 22

Section – Digital certification services in the payment sector : page 23

Section – Security of payment infrastructure : page 20

[20] Official Journal of European Communities (1991), L 166 of 28.06.1991, Council Directive of 20 June 1991 on prevention of the use of financial system for the purpose of money laundering (91/308/EEC), Brussels
http://www.europa.eu.int/scadplus/leg/en/lvb/l24016.htm
http://www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1991&nu_doc=308;

Section – Identification of the originator in the payment process

Section – Money laundering

[21] Official Journal of European Communities (2002) , Official Journal L 201 of 31.07.2002, Directive 2002/58/EC of The European Parliament and of The Council of July 2002 concerning the processing of personal data and the protection of privacy in the

electronic communication sector (Directive on privacy and electronic communications); 31-07-2002, Brussels;
http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf;

Section - Data protection in the electronic communications sector: http://www.europa.eu.int/scadplus/leg/en/lvb/l24120.htm

Section - Protection of personal data: http://europe.eu.int/scadplus/leg/en/lvb/l14012.htm

[22] Official Journal L of European Communities (2000) of 13, 19.01.2000, Directive 1993/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Brussels

Section - Digital certification services in the payment sector: http://europe.eu.int/scadplus/leg/en/lvb/l24118.htm

[23] Official Journal L 149 of European Communities (2001) of 02.06.2001, Framework Decision 2001/413/JAI of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment; Brussels

Section – Payment of security infrastructure; Act: "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol - A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment [COM(2004) 679 final - Not published in the Official Journal]": http://europe.eu.int/scadplus/leg/en/lvb/l33306.htm

Related Acts: Report from the Commission based on Article 14 of the Council Framework "Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment [COM(2004) 346 final - Not published in the Official Journal]": http://europe.eu.int/scadplus/leg/en/lvb/l24212.htm

[24] Official Journal L 108 of European Communities (2002) of 24.04.2002, Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications network and services, Brussels

Section: The EU competition law: http://europe.eu.int/scadplus/leg/en/lvb/l24216a.htm

[25] DNB (Date unknown) , no.1

Section – Legal aspects with regard to internet banking: http://www.dnb.nl/dnb/pagina.jsp?pid=tcm:13-40207-64

[26] Official Journal 195 of European Communities (2004) 02.06.2004, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, Brussels

Section – Enforcement of intellectual property rights:
http://europe.eu.int/scadplus/leg/en/lvb/l26057a.htm

[27] Official Journal L 123 of European Communities (2004) 27.04.2004, Commission Regulation (EC) No 772/2004 of 27 April 2004 on the application if Article 81(3) of the Treaty to categories of technology transfer agreements, Brussels
Section – Technology Transfer Agreements:
http://europe.eu.int/scadplus/leg/en/lvb/l26108.htm

[28] Brits, H. & Winder C., (2005) Payments are no free lunch, occasional studies , Vol.3 , Nr.2 (2005), De Nederlandsche Bank, Den Haag
Section about Payment Clearinghouse ownership structure in NL,
- POS payment costs: page 3

[29] CPSS Red book (2003), Payment systems in The Netherlands
Section - Interpay: page 297
Section - TARGET: page 302
Figure 6 - Payment & securities settlement systems and their overseers: page 296

[30] De Nederlandsche Bank (2003), Jaarverslag 2003
Section – CLS

[31] Rabobank no.2,
Section – Mobile Banking services provided by various banks in The Netherlands; Rabobank: http://www.rabobank.nl/info/execute/node?node_id=269585
"Information retrieved form this site in May 2005"

[32] Rabobank no.3,
Section - Mobile Banking services provided by various banks in The Netherlands; Rabo Alerts: http://www.rabobank.nl/info/execute/node?node_id=261818
"Information retrieved from this site in May 2005"

[33] Rabobank no.4,
Section - Mobile Banking services provided by various banks in The Netherlands; Rabobank, Mobile investing:
http://www.rabobank.nl/info/execute/node?node_id=300098
"Information retrieved from this site in May 2005"

[34] Rabobank no.5,
Section - Mobile Banking services provided by various banks in The Netherlands; Rabobank, Top up your balance:
http://www.rabobank.nl/info/execute/node?node_id=101423
"Information retrieved from this site in May 2005"

[35] ABN AMRO no.1,
Section - Mobile Banking services provided by various banks in The Netherlands; ABN AMRO:
http://www.abnamro.nl/nl/particulier/bankieren/mobiel_bankieren/voordelen.html

[36] ABN AMRO no.2,
Section - Mobile Banking services provided by various banks in The Netherlands; Access to the mobile link of ABN AMRO:
http://www.abnamro.nl/nl/particulier/bankieren/mobiele_diensten/mobiele_site/voordelen.html
"Information retrieved from this site in May 2005"

[37] ABN AMRO no.3,
Section - Mobile Banking services provided by various banks in The Netherlands; SMS-based services:
http://www.abnamro.nl/nl/particulier/bankieren/mobiele_diensten/sms_diensten/voordelen.html
"Information retrieved from this site in May 2005"

[38] Postbank no.1,
Section - Mobile Banking services provided by various banks in The Netherlands; Postbank:
http://www.postbank.nl/ing/pp/page/banking/modern/0,2838,1859_103828,00.html?linktype=int

[39] National Forum on the payment system (2004), Report 2004 (n/a);
Cost of electronic transaction in Norway: page 17

[40] ECB (2002) , E-payments without frontiers (n/a);

[41] http://www.theregister.co.uk/2005/06/27/simpay_halts_project/

[42] Stream Magazine (2005), Simpay pulls the plug on pan-European payments, October 2005,
Simpay abandoned: page 5

Additional bibliography (not referenced inside report)

[1] B. Adrian. Overview of the mobile payments market 2002 through 2007. *Gartner*, November 2002.
[2] J. Bower and C. Christensen. Disruptive technologies: catching the wave. *Harvard Business Review*, 73(1):43–53, January 1995.
[3] Y. Chou, C.-W. Lee, and J. Chung. Understanding mcommerce payment systems through the analytic hierarchy process. *Journal of Business Research*, 57:1423– 1430, 2004.
[4] T. Dahlberg, N. Mallat, and A. Oorni. Trust enhanced technology acceptance model - consumer acceptance of mobile payment solutions. *The Stockholm Mobility Roundtable 2003*, may 2003.
[5] M. De Lussanet. Mobile payment's slow start. *ForresterResearch*, 2001.
[6] C. Hort, S. Gross, and E. Fleisch. Critical success factors of mobile payment. Technical report, M-Lab, 2002.
[7] T. Iacobuzio. The cashless, cardless society: Coming soon to a paypoint near you. *TowerGroup ViewPoint Report*, 2006.
[8] S. Kassicieh, S. Walsh, S. Cummings, J. McWhorter, P. Romig, and D.Williams. Commercialization of disruptive technologies: moving discontinuous innovations into products. *IEEE Transaction on Engineering Management*, (49 (4)):375–387, 2002.
[9] R. Kostoff, R. Boylan, and G. Simons. Disruptive technology roadmaps. *Technological Forecasting and Social Change*, 71:141–159, 2004.
[10] N. Mallat. Theoretical constructs of mobile payment adoption.*IRIS27*, 2004.
[11] J. Ondrus and Y. Pigneur. A disruption analysis in the mobile payment market. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05),IEEE Computer Society*, 2005.
[12] J. Ondrus and Y. Pigneur. A multi-stakeholder multi-criteria assessment framework of mobile payments: An illustration with the swiss public transportation industry. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), IEEE Computer Society*, 2006.
[13] K. Pousttchi. Conditions for acceptance and usage of mobile payment procedures. *The Second International Conference on Mobile Business*, pages 201–210, 2003.
[14] K. Taga and J. Karlsson. Arthur D. Little GlobalM-Payment Update 2005. Technical report, Arthur D. Little's Telecommunications, IT, Media & Electronics (TIME) Practice, Vienna, Austria, 2005.
[15] S. Walsh. Roadmapping a disruptive technology: a case study. the emerging microsystems and top-down nanosystems industry. *Technological Forecasting and Social Change*, 71:161–185, 2004.
[16] A. Zmijewska, E. Lawrence, and R. Steele. Towards understanding of factors influencing user acceptance of mobile payment systems. *IADIS WWW/Internet, Madrid*, 2004.

13. Glossary [23]

3G: Third Generation Mobile Network.

"Generic name for third generation networks; for example, UMTS." [mobile payment forum]

AES: Advanced Electronic Signature.

"Under section 2 (2) of the Digital Signature Act (SigG), this is defined as the electronic signatures which permit the 'reliable' identification of the 'signatory' and effectively protect the integrity of the signed data." [source: www.bsi.bundes.de]

API: Application Programming Interfaces.

"A set of calling conventions that defines how a service is invoked through software. An API enables programs written by users or third parties to communicate with certain vendor-supplied software."

ARQC: Authorisation Request Cryptogram.

ARQC means that the transaction is approved and that it has to go on-line (an authorisation request has to be sent to the issuer).

ATM: Automated Teller Machine.

"A public banking machine that customers can access by inserting or swiping a magnetic card and entering a password. ATMs are usually connected to central computers through leased local lines and multiplexed data networks."

BREW: Binary Runtime Environment for Wireless. *(Qualcomm TM, It is not an acronym though)*

BT: Byte.

CA: Certification Authority.
"Also known as a "certificate authority," this is an internal or third-party entity that creates, signs and revokes digital certificates that bind public keys to user identities. A repository or directory stores digital certificates and certificate revocation lists (CRLs) to allow users to obtain the public keys of other users and determine revocation status. Typically, the repository is a traditional X.500 directory or a database that supports Lightweight Directory Access Protocol (LDAP)."

CDMA: Code Division Multiple Access.
"A digital wireless technology used in radio communication for transmission between a mobile phone and a radio base station. CDMA was developed by Qualcomm, and commercially introduced in 1995. It enables the simultaneous transmission and reception of several messages, each of which has a coded identity to distinguish it from the other messages."

CEN: Comité Européen de Normalisation.
"It is the European Committee for Standardisation." [ECBS]

CEN/ISSS: Comité Européen de Normalisation.
"European Committee for Standardisation/Information Society Standardisation System" [ECBS].

CLS: Continuous Linked Settlement.
It is the bridge between TOP and TARGET and provides worldwide clearing an settlement for transfers.

COTS: Commercial Off-the-Shelf.
"Descriptive term for software that can be purchased from an external supplier, as opposed to that which is developed within the enterprise."

CRM: Customer Relationship Management.

DECT: Digital European Cordless Telecommunications.
"An interface specification for European digital mobile telephony. DECT employs 10 carrier frequencies between 1.88 gigahertz (GHz) and 1.9 GHz, and has a transmission speed of 144

kilobits per second. It is typically used for short-range communications and wireless-local-loop applications."

DNB: De Nederlandcshe Bank.

DES: Data Encryption Standard.
"A security specification developed by IBM in 1977. Still in use today, it is available at no charge from many online bulletin boards and is based on a single-key encryption algorithm. If user A wants to send an encrypted file to user B, user A would first encrypt it with a secret key. User B would then decrypt the file using the same key. Recipients must prearrange for possession of the appropriate key for decryption to take place."

EBA: Euro Banking Association.

EBPP: Electronic Bill Presentment and Payment.
"The ability for consumers to view and pay their bills online (for example, via the Web or e-mail)."

EC: European Commission.
"The EC is charged with upholding the general interests of the EU."

ECB: European Central Bank.

ECBS: European Committee for Banking Standards.

ECSA: European Credit Sector Association.

EEA: European Economic Area.

EEC: European Economic Community. (See also EU).

EESI: European Electronic Signature Initiative.

EESSI: European Electronic Signature Standardisation Initiative.

EFTA: European Free Trade Association.

EMI: European Monetary Institute.

EMU: Economic and Monetary Union.
"The European process of standardizing on a single currency (i.e., the euro)."

EMV: a payment standard defined by Europay, MasterCard and Visa International.

ETSI: European Telecommunications Standards Institute.

"A not-for-profit enterprise whose mission is to produce the telecommunications standards that will be used throughout Europe. Some of the standards developed by the ETSI may be adopted by the European Commission as the technical base for directives or regulations. The ETSI's main task is to remove any possible variation from a global standard and to focus on a defined European-specific set of requirements. The ETSI also ensures that there is interoperability between standards such as Integrated Services Digital Network (ISDN), Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS)."

EU: European Union.

"A European body, created by a 1993 treaty, with the goal of working toward the economic and political unification of Europe. (Previous incarnations were known as the European Community and the European Economic Community.) Many EU activities have a major impact on information technology — for example, many of its directives govern telecommunications and computing standards, and the EU process of economic and monetary union (EMU) — featuring a single European currency called the euro — has a major impact on financial IT system compliance."

FATF: Financial Action Task Force.

FINREAD: Financial Reader.

It is an EMV compliant card reader.

FPAP: Fraud Prevention Action Plan.

GDP: Gross Domestic Product.

GPRS: General Packet Radio System.

"GPRS is a packet-oriented overlay to Global System for Mobile Communications (GSM) networks supporting connection- and connectionless-oriented services and diverse quality-of-service mechanisms. The theoretical maximum speed is 171.2 kilobits per second (Kbps), but real-life user throughput is expected to be 56 Kbps or less."

GSM: Global System for Mobile Communications.

"The dominant digital cellular technology for mobile telephone networks in Europe. GSM (formerly called "Groupe Speciale Mobile") utilizes the 905-915 MHz and 950-960 MHz reserved spectrum to provide roaming capability across 18 countries in Europe. GSM 1900, the North American version of GSM, allows the standard to be used in the 1,900 MHz frequency band, which the U.S. Federal Communications Commission and Industry Canada have allocated for personal communication services (PCS). GSM is also the name of the European Telecommunications Standards Institute technical committee responsible for the developing the standard."

ICC: Integrated Circuit Card *(chip card).* [ECBS]

IF: Interface.
"1. A point or means of interaction with a system, whether by a human user or another system;
2. In communications, the boundary between two pieces of equipment across which all the signals that pass are carefully defined. The definition includes the connector signal levels, impedance, timing, sequence of operation and the meaning of signals."

i-Mode: Interactive Information over Mobile Communication Network
"NTT DoCoMo's mobile system that allows users to view specially formatted Web sites, receive e-mail, and access financial, travel and news information via their mobile phones. A key feature of i-mode is that it offers constant connection to the Internet."

IP: Internet Protocol.
"The basic underlying protocol of the internet, originally developed during a 15-year period under the auspices of the U.S. Department of Defence. Used in conjunction with Transmission Control Protocol (TCP), it provides a common address system and communication protocol to track the addresses of network nodes, route outgoing messages and recognise incoming ones. Today, its use has spread beyond the Internet to become a de facto standard in enterprise networking."

IPR: Intellectual Property Right.

IrDA: Infrared Data Association.
"An international organisation that produces standards for infrared data transmission at speeds up to four megabits per second; also the name for the standard itself."

ISO: International Organisation for Standardisation.
"A voluntary, non-treaty organization established in 1949, as a technical agency of the United Nations, to promote international standardization in a broad range of industries. ISO's Open Systems Interconnection (OSI) Reference Model establishes guidelines for network architectures."

IST: Information Society Technologies.

IT: Information Technology.
"The common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use."

IVR: Interactive Voice Response.

J2ME: Java 2 Platform, Micro Edition.

"An edition of Sun's Java Platform that focuses on small-form-factor devices, such as PDAs, pagers and cell phones."

JAVA:
"The term 'Java' can be applied to Sun Microsystems' Java platform or to its Java programming language. The java platform include the Java Virtual Machine (JVM), which provides a uniform Java byte code emulator for Java's cross-platform runtime environment; the Java programming language, which provides a robust object-oriented language for constructing Java components and applications; and the standard Java class library packages, which provide sets of reusable services that promote consistency among components and applications. The Java programming language is based on C and extend and compliments the basic capabilities of XML. Java permits the creation of applications and application modules (called "applets") that run in the JVM on the browser."

M-Banking: Mobile Banking.
"A range of traditional banking services, including push payments, where a customer gives the order to the bank to execute a transfer of funds, conducted via a mobile trusted device." [ECBS]

M-Commerce: Mobile Commerce.
"Electronic commerce using a mobile trusted device as the customer device e.g. a mobile phone." [ECBS]

MeT: Mobile Electronic Transactions.

MHz: Megahertz.
"A unit equal to 1 million hertz (1 million cycles per second)."

MMS: Multimedia Messaging System.
"A mobile-messaging standard jointly defined by the 3G Partnership Project and the Wireless Application Protocol Forum. MMS provides a broad set of features that cannot be delivered through traditional wireless-messaging standards, such as the ability to send and receive messages containing rich multimedia content, and to send messages to both mobile phone numbers and e-mail addresses. Unlike Enhanced Messaging Service, MMS does not draw on established messaging technology such as Short Message Service. Instead, it requires new infrastructure to be deployed by the network operators, and new functionality in mobile terminals."

MoUs: Memoranda of understandings.

M-payment: Mobile payment.
"A payment initiated or completed through a wireless device. As a point of entry into retail payments, many carriers are targeting the underdeveloped market for micro-payments (payments of less than $10) for digital content and physical goods."

OBEX: IrDA Object Exchange.

OMA: Open Mobile Alliance.

OS: Operating System.
"The main control programme that runs a computer and sets the standard for running application programmes. It is the first programme loaded when the computer is turned on, and it resides in memory at all times. An operating system is responsible for functions such as memory allocation, managing programmes and errors, and directing input and output."

OTA: Over the Air.

PC: Personal Computer.

PDA: Personal Digital Assistant.
"A handheld computer that serves as an organizer and electronic notepad. It typically uses a stylus or pen-shaped device for data entry and navigation. Types of PDA include clamshell (a computer system that weighs less than 3 pounds and opens lengthwise to expose a keyboard and screen) and tablet (a computer system that weighs less than 4 pounds and that is operated by direct screen contact via a pen or touch interface)."

PIN: Personal Identification Number.
"A numeric code — typed on an automated teller machine or telephone keypad, or a computer keyboard — used to gain access to personal funds or information."

PKI: Public Key Infrastructure.
"The techniques necessary to manage public-key cryptography (see separate entry), as well as the various systems for authentication, non-repudiation and integrity that can be built on top of a public-key system."

POS: Point of sale terminal.
"A category of systems that use personal computers or specialized terminals in combination with cash registers, optical scanners or magnetic-stripe readers to capture and record data at the time of transaction. POS systems are usually online to a central computer for credit checking and inventory updating. Alternatively, they may be independent systems that store daily transactions until they can be transmitted to the central system for processing."

PTD: Personal Trusted Device.

PTP: Person-to-Person.

RA: Registration Authority.

“An optional component in a public-key infrastructure (PKI) security implementation. The RA proves an entity's identity before passing its credentials to the certification authority for certificate creation. See **PKI** and **certification authority**.”

R&D: Research and Development.

RFID: Radio frequency Identification.

“An analogue-to-digital conversion technology that uses radio frequency (RF) waves to transfer data between a movable item and a reader for identification, tracking or location purposes. It does not require physical contact or a line of sight between the reader or scanner and the tagged item. This is one advantage over a bar code system, while another is that RFID tags can be read over a longer range — 100 feet or more. A typical RFID system has three components:

- An antenna
- RFID tags (sometimes called transponders or e-tags), which are electronically programmed with unique information
- An RF module with a decoder (transceiver).”

RS 232:

“An Electronic Industries Alliance (EIA) physical interface specification for serial data connections. Originally introduced in 1962, RS-232 (sometimes presented as "RS232") is the most commonly employed interface between computers and modems. As the EIA and its telecom subgroup, the Telecommunications Industry Association (TIA), have released updated versions over the years, the formal name of the specification has changed — for example, to "EIA-232-D," "EIA/TIA-232-E" and, most recently, "TIA/EIA-232-F." Regardless of the version, however, the specification is still commonly referred to by the original "RS-232" appellation.”

SDO: Standards Development Organisation.

SE: Security Element.

SET: Secure Electronic Transaction.

“A standard in conceived in 1995 by Visa and MasterCard to ensure that all Internet-based payment transaction details are encrypted, the parties authenticated, acknowledgements fully recorded and the customer payment details made available only to the bank. Due to its complexity and security flaws, SET failed to gain widespread acceptance. Meanwhile, Visa and MasterCard have pushed ahead with their own, separate standards: Verified by Visa and MasterCard Secure Payment Application.”

SIM: Subscriber Identity Module.

“A small, programmable smart card containing a cellular service subscriber's identity key. The SIM contains codes to identify a subscriber to a digital mobile service and the details of the special services the subscriber has elected to use. The SIM may be fixed within the

phone, or removable (enabling users to swap phones without changing their subscriptions). The SIM is the key to security on Global System for Mobile Communications (GSM) networks. In addition to GSM SIMs, two other types have been developed: the removable user identity module (R-UIM), which can be used in code division multiple access (CDMA) networks along with GSM ones, and the universal SIM (USIM), designed for use in third-generation (3G) networks."

SMPP: Short Message Peer-to-Peer.

SMS: Short Message Service.

"A bidirectional paging function that is built into Global System for Telecommunications (GSM) systems. Each message can be up to 160 characters long. The network stores messages for several days (typically a maximum of 72 hours) and attempts to deliver the messages whenever the portable phone is switched on. Confirmation of receipt is available as an option in some networks."

SPA: Service Process Optimisation.

"Software designed to track and allocate the major resources of service companies or departments — people, intellectual capital and time. Most SPO applications address of six core areas of functionality:

1. Project initiation (opportunity management)
2. Engagement structuring
3. Engagement execution (project management)
4. Resource management
5. Knowledge management
6. A business-to-business exchange for procuring resources and collaborating with clients and colleagues

Professional services administration (PSA) is a related term, but one that applies only to external service providers (ESPs). SPO applies to internal service departments as well as ESPs."

SSL: Secure Sockets Layer.

"An Internet security standard developed by Netscape Communications. SSL offers session-level security — that is, after a secure session has been initiated, all information transmitted over the Internet during that session is encrypted. SSL also offers features such as server and client authentication as well as message integrity."

STEP: Standard for the Exchange of Product Model Data.

"An international standards effort for defining the exchange of complete, unambiguous product model data. The goal of STEP is not only neutral file exchange, but also to serve as the basis for implementing, sharing and archiving entire product databases."

STK: Satellite Tool Kit.

STP: Straight-through-processing.
"A system configuration in which a transaction (such as a payment, a trade or a change to a residential phone service) is entered only once. Thereafter, it proceeds in an automated fashion through the rest of its life cycle, which may include dozens of steps in different application systems in various locations. The goal is to avoid re-keying information, thereby reducing input errors and shortening the time to completion."

SBW: Server Based Wallet. [ECBS]

SWOT: Strengths, Weaknesses, Opportunities and Threats analysis.

TARGET: Trans European Automated Real Time Gross Settlement Express Transfer System.

TDMA: Time Division Multiple Access.
"A technology for digital transmission of radio signals between, for example, a mobile phone and a radio base station. TDMA enables communicating devices at different locations to share a multipoint or broadcast channel by means of a technique that breaks signals into sequential pieces of defined length, and reconstructs the pieces at the end of the transmission."

TLS: Transport Layer Security.
"A general term describing the practice of billing for services based on the cumulative time worked and materials purchased, rather than based on a fixed price."

TOP:
TOP is not an acronym. "It is the name of the real-time gross settlement system of De Nederlandsche Bank. The system is named after the market sector in which it operates: the "top", i.e. the sector handling the largest-value payments in the Netherlands." [ECB]

UCP: Universal Computer Protocol.

UML: Unified Modelling Language.
"A language for specifying, visualizing, constructing and documenting the artefacts of software systems."

UMTS: Universal Mobile Telecommunication System.
"The first of the third-generation (3G) cellular networks, UMTS is being designed to offer speeds of at least 144 Kbps to fast-moving (e.g., vehicle-based) mobile devices, and offer an initial 2 Mbps to campus sites — designers expect to increase this to 10 Mbps by 2005."

URL: Uniform Resource Locator.
"The character string that identifies an Internet document's exact name and location."

USB: Universal Serial Bus.

"A standard desktop input/output bus that provides a single peripheral connection and vastly increases bus speed. It simplifies peripheral connections via a "daisy chaining" scheme whereby the desktop system has only one input/output port to which all peripherals are connected in a series. Up to 120 peripherals can be connected to a single system."

USSD: Unstructured Supplementary Services Data.

"USSD is a means of transmitting information via a GSM network. It is to some extent similar to SMS, but in contrast to SMS, which is basically a store and forward service, USSD offers real-time connection during a session. The direct radio connection stays open until the user or the application disconnects it. A USSD message can have up to 182 characters. It is relevant for real-time applications such as mobile stock-trading, where a confirmed information transmission is needed. USSD is a WAP bearer service." [Durlacher]

VNO: Virtual Network Operator.

WAN: Wide-Area-Network.

"A communications network that connects computing devices over geographically dispersed locations. While a local-area-network (LAN) typically spans a single building or location, a WAN covers a much larger area such as a city, state or country. WANs can use either phone lines or dedicated communication lines."

WAP: Wireless Application Protocol.

"WAP is a set of specifications developed by the WAP Forum for efficient communication of data over wireless networks to small devices, such as personal digital assistants and cell phones. WAP specifications are based on Internet standards, with extensions to reflect the wireless device environment. Specifications in the WAP architecture are arranged in a protocol stack consisting of application, session, transaction, security and transport layers."

WIM: WAP Identification Module (Wireless Internet Module).

WML: Wireless Mark-up Language.

"A programming language similar to XML, used to create pages that can be displayed in a Wireless Application Protocol (WAP) browser (for example, a WAP phone)."

WPKI: Wireless Public Key Infrastructure.

WTLS: Wireless Transport Layer Security.

"Within the Wireless Application Protocol (WAP) framework for cellular-phone interface services, WTLS provides security functions similar to those of the Secure Sockets Layer (SSL) protocol used on the Web. See **WAP** and **SSL**."

XML: Extensible Mark-up Language.

“A metalanguage approved as a World Wide Web Consortium (W3C) recommendation in February 1998. A simplified version of Standard Generalized Mark-up Language (SGML), XML captures SGML's key advantages (such as extensibility) without its more obscure features. Because it is a metalanguage (a language to define languages), it intrinsically offers Hypertext Mark-up Language (HTML) capabilities and can be used to create HTML documents. A family of XML-related standards (formally called "recommendations") has been under development by the W3C since 1997. These include XML Linking Language (XLink), XML Path Language (XPath), XML Pointer Language (XPointer), Extensible Stylesheet Language (XSL) and XSL Transformations (XSLT). Together, they form a critical foundation for today's Web-based computing and e-commerce infrastructures.”

Publications in the Report Series Research* in Management

ERIM Research Program: "Business Processes, Logistics and Information Systems"

2006

Smart Business Networks Design and Business Genetics
L-F Pau
ERS-2006-002-LIS
http://hdl.handle.net/1765/7319

Designing and Evaluating Sustainable Logistics Networks
J. Quariguasi Frota Neto, J.M. Bloemhof-Ruwaard, J.A.E.E. van Nunen and H.W.G.M. van Heck
ERS-2006-003-LIS
http://hdl.handle.net/1765/7320

Design and Control of Warehouse Order Picking: a literature review
René de Koster, Tho Le-Duc and Kees Jan Roodbergen
ERS-2006-005-LIS
http://hdl.handle.net/1765/7322

A Theoretical Analysis of Cooperative Behavior in Multi-Agent Q-learning
Ludo Waltman and Uzay Kaymak
ERS-2006-006-LIS
http://hdl.handle.net/1765/7323

Supply-Chain Culture Clashes in Europe. Pitfalls in Japanese Service Operations
M.B.M. de Koster and M. Shinohara
ERS-2006-007-LIS
http://hdl.handle.net/1765/7330

From Discrete-Time Models to Continuous-Time, Asynchronous Models of Financial Markets
Katalin Boer, Uzay Kaymak and Jaap Spiering
ERS-2006-009-LIS
http://hdl.handle.net/1765/7546

Mobile Payments in the Netherlands: Adoption Bottlenecks and Opportunities, or… Throw Out Your Wallets
Farhat Shaista Waris, Fatma Maqsoom Mubarik and L-F Pau
ERS-2006-012-LIS

---

* A complete overview of the ERIM Report Series Research in Management:
https://ep.eur.nl/handle/1765/1

ERIM Research Programs:
LIS Business Processes, Logistics and Information Systems
ORG Organizing for Performance
MKT Marketing
F&A Finance and Accounting
STR Strategy and Entrepreneurship