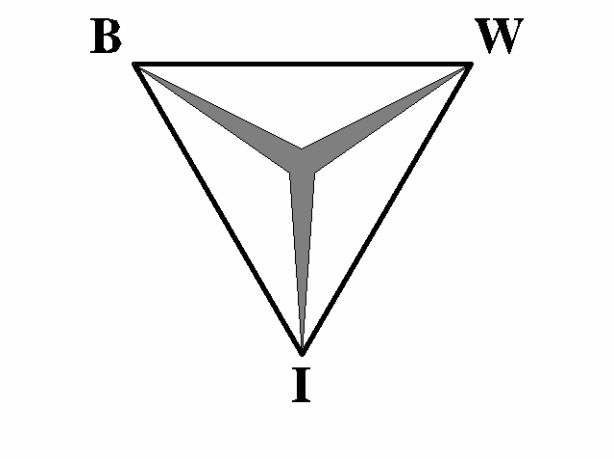
M-COMMERCE AND M-PAYMENT

'COMBINING TECHNOLOGIES'

BY J.JONKER
BEDRIJFSWISKUNDE EN INFORMATICA
– VU AMSTERDAM -



PREFACE

As one of the last parts of the BWI-study[1] at the Faculty of Exact Sciences of the Free University (VU) in Amsterdam, the so-called BWI-paper is written. In this paper, the student must clearly assess an existing problem, using existing literature.

The subject of this paper evolved from my professional interest for i-mode in December 2001 and the assignment from Eyefi interactive to research the possibilities to produce i-mode applications. Almost every bit of information was found on the Internet, I was overwhelmed by the amount and it became clear to me that I could never discuss every aspect of Mobile Payment. I choose to research the basis and I hope other students of the faculty will be able to use this paper to create more in-depth papers.

Several people provided me with information and support. I wish to thank Eyefi interactive Amsterdam, E-Commerce Platform Nederland, LogicaCMG Unwired Concepts and prof. dr. H.Kersten from the Free University Amsterdam.

I enjoyed writing this paper and I am happy to receive any suggestions or answer any questions you might have.

Jan-Willem Jonker
j.jonker@imore.nl
jwjonker@cs.vu.nl

1 *BedrijfsWiskunde & Informatica, which is best translated as Business Mathematics & Computer Science*

ABSTRACT

Mobile Payment (M-Payment) is a payment method that has attracted a growing amount of attention in the last few years. In this paper, we will discuss the possibilities for Mobile Commerce and M-Payment. I will give an overview of the available technologies, devices, protocols and their security concepts. My goal is two-fold, I wish to address the necessities for M-Payment to grow into a general accepted payment method and give advice about a possible implementation. My personal goal is to get a better understanding of the technologies currently, and in the near future, available.

First, we will go through a short general introduction about electronic commerce, payment methods, mobile devices and the current European market for mobile commerce. After this introduction, we will concentrate on a specific part of electronic commerce, that of mobile payment. Regarding mobile payment, we will discuss the transaction in-depth and compare methods, technologies and security issues. Finally, the conclusion will hold the advantages, disadvantages and a possible implementation of M-Payment.

TABLE OF CONTENTS

INTRODUCTION TO THE MOBILE WORLD

NOW AND THEN

In the last 5 years, several technologies have become available for a large public and in the next 5 years, of course more will be available. These technologies make it possible to conduct business without the use of a static connection within an office.

With the rise of the Internet, in our perception, the world has become larger and yet smaller. We are able to shop all over the world and have it delivered at our doorstep. From 1999 on, electronic business to consumer (B2C) sales in the Netherlands have doubled every year[ii]. During that same time, digital cellular phones (GSM) have become a common item and in the beginning of 2002 were used by 75% of the Dutch citizens[i]. Estimations for the end of 2002 are 86%.

Predictions for the next few years state a rise in use of mobile network technologies, the extension and upgrading of the European GSM network and a leveling of market penetration. More changes will (probably) be:

- The implementation of high speed data communication protocols and languages in telecom infrastructure and communication devices,
- Access to high speed wireless data networks becomes more and more available for the general public,
- Cellular phone- and PC-manufacturers are extending their product range towards multifunctional products, with more functionality in a smaller casing.
- Multifunctional devices will be used widespread in the near future.
- A large number of people will use wireless voice- and data communication technologies.

All these elements can contribute to an environment where electronic commerce is possible through wireless communication on devices that can hold more information and can transmit data faster and more secure. This can be a good environment for evolution of mobile commerce.

However, what is mobile commerce exactly? We will start with some definitions.

A-COMMERCE (ALL COMMERCE)

Definition of E-Commerce

Currently electronic commerce (E-Commerce) is a generally accepted term, but its use is not consistent. In this paper we will use the following definition:

> *<u>E-Commerce</u>: Any transaction over the Internet involving the transfer of goods, services, or information and any intermediary function, which helps enable those transactions. This includes B2B, B2C, C2C and information retrieval from government agencies and non-profit organizations.* [ii]

In this definition, we state that the Internet is used to transport the information and in general the device we use to perform E-Commerce transactions are PC's, directly connected to the Internet, with on the other side web servers that handle the transactions. Below we will compare E-Commerce to M-Commerce. First, we will discuss some examples and facts.

From 1999 to 2001, the number of people accessing the Internet for E-Commerce purposes has doubled within the B2B-markets and even more for B2C-markets. The high penetration of Internet in the year 2002 (between 57 and 61% of the Dutch Consumers) gives E-Commerce enough room to grow into a standard method for ordering certain products[ii,xx]).
In general, transactions require you to receive information (price, product details and products) and submit information (name, location, method of payment).

Example E-Commerce

E-Commerce is mostly conducted where there is a direct connection to the Internet, for instance at home, university or at the office.

While you are working the whole weekend on your paper, you realize you need more information and "alt-tab" to Amazon.com and order the latest book written by N.M. Sadeh, delivery method: Digital, delivery time: Now, payment: Latest American Express Blue Card (internet insurance). Because we also need to eat, we order some Thai food at thai4all.nl and pay cash on delivery.

Definition of M-Commerce

As the E-Commerce definition states, it needs a connection to the Internet to fulfill the transaction. This is one limitation that can be resolved by introducing wireless connectivity, thus introducing M-Commerce (mobile commerce).
To create a definition not limited by our current position in evolution and has no link to currently existing technologies, the following definition is used in this paper.

> *M-Commerce is the buying and selling of goods, services or information without any location restrictions, by mobile device which uses a wireless connection to establish communication between all necessary parties to complete the transaction.*

Note that in this definition, the transactions can, but not necessarily have to, use the Internet as medium. To transfer the necessary information any network can be used and in addition, the device can be any device and does not have to be a cellular phone!

For certain M-Commerce products, the definition can be extended with "with minimum of input and effort from the user", because user-friendliness and cost efficiently are key elements for high acceptation among the buyers.

E-Commerce has grown into a widespread method to buy goods or services, mainly because Internet has become an accepted communication method. M-Commerce can follow the same path if the infrastructure and support by technical parties is available.

Example M-Commerce

A possible use for M-Commerce can be theater ticket reservation where you pay through the same device as you make reservations at any location with network connectivity.

You are dining with your friends in a restaurant in a small village outside Amsterdam. The party discusses a small theater play that starts late this evening in an Amsterdam theater. It might be a nice idea to see this play. The theater telephone line is busy and you cannot get through to the operator. At this moment, it would be nice if you can ask for a list of theater plays currently playing in Amsterdam and choose the recommended play. Reservation and payment are instantly.

PAYMENT

Buying and selling goods implies payment. Payment of goods purchased using E-Commerce currently takes place using several methods. These methods are common to many people because they have been accepted outside E-Commerce for a long time now. Payment can be done:

- In advance

- By credit card online
- By debit card (rarely available in the Netherlands)
- On-delivery (cash / PIN / credit card)

These methods are well known and will not be explained further.

The location where a buyer completes a transaction is called Point Of Sales (POS). This location could geographically be anywhere, as long as data communication with that specific network is possible.

M-Payment

M-Commerce payment can be conducted in several ways and at any location. All methods discussed in this paper are aimed at an "anywhere, anytime"-implementation. With that philosophy, mobile payment should be implemented as well.

Payment using an M-Commerce device is usually called M-Payment (mobile payment). When the buyer completes a transaction M-Commerce and uses M-Payment, he can receive a proof of purchase on the same device he used to complete the transaction (when the user is uniquely registered within a system, other implementations can be possible). We will call this proof of purchase a ticket or an M-Ticket (This M-Ticket is received at the POS).

An M-Ticket can be send to the buyer in many formats, which will be discussed later in this paper in chapter "M-Ticket uniqueness and redemption".

A common mistake is to make no distinction between M-Payment and µ-payment. In 1995 W3C suggested a protocol for small electronic payments through the services of any independent broker called Micro Payment Transfer Protocol (MPTP), this protocol never reached the recommendation status. Unfortunately micro(µ)-payment and M-Payment are often thought to be the same payment method or mistaken for small electronic payments in general.

In the last few years, several companies implemented their own protocols or methods, for instance PayPal, SwitchPoint and Moxmo. These systems all share the sub goal of minimizing the overhead cost of a single transaction but are not user-friendly, only for small amounts or only applicable for specific situations.

In this paper, we will explore more M-Payment methods and protocols and discuss security issues.

> *So, you've paid for the product, but how are you going to proof this, you just can't walk in and say, "Hi, I've made reservations, look it says so on my phone." Or can you?*

DELIVERY OF M-GOODS OR SERVICES

We have introduced M-Commerce and M-Payment. After payment, generally, the goods or services are delivered, a service is provided or access will be granted. At this point, there will be need for validation of purchase. It would be convenient to use the same device for validation.

Let us say that the buyer receives evidence of payment, a mobile ticket (M-Ticket), on his device. This ticket could then be used to validate the reservation and payment at the location where services or goods are transferred. The location where a buyer redeems his ticket is called Point Of Entry (POE). It is possible to create an implementation without the use of M-Tickets, like SwitchPoint discussed later in this paper.

Validation can take place in several ways. For instance, the buyer's device could display a unique value, like a unique string or a barcode. This unique value needs to be validated by viewing or copying the string (digital or optical) or reading the barcode (with a scanner) into

a validation capable system. Wireless communication of the ticket might be possible as well. Both the M-Ticket and the validation-system and -process will be discussed later in this paper.

With the use of M-Tickets, cross-promotion opportunities arise. For instance, one could receive a discount on or a promotional offer for other goods or services. This discount-ticket is usually called an M-Coupon and can be redeemed as well. M-Coupons are economically and marketing-wise very interesting and the objectives and results will probably be the same as offline coupons or promotional offers.

A very important issue with the security and uniqueness of digital tickets and coupons is the amount of effort and chance to create a fake M-Ticket. More about security will be discussed in chapter “Security” and “M-Ticket uniqueness and redemption” later in this paper.

First, we will take a look at currently available and adoption of M-Commerce / -Payment systems around the world

M-PAYMENT THROUGHOUT THE WORLD

Currently there is only one country in the world that has fully adopted mobile payment: Japan. Currently 94,4% of the number of global mobile payment users is Japanese[iii]. This country started developing mobile communication when the rest of the world focused on the Internet. Because Internet was not widespread, mobile communication became the way to communicate. While we are moving from physical commerce to m-commerce via e-commerce, Japan started using m-commerce already in 1999. Furthermore, like the Netherlands and unlike U.S.A., in Japan credit card is not a popular payment method, which makes implementation of payment services based on traditional methods, explained in chapter “Definition of E-Commerce”, more difficult.

NTT-DoCoMo offered mobile services and payments on a proprietary platform and quickly became the largest provider in Japan is NTT-DoCoMo. Their mobile environment is called i-Mode and was introduced early 2002 in Europe by KPN-Mobile, a joint venture between NTT and KPN. Six months after the introduction of i-Mode, KPN-Mobile has a little over one million customers in Belgium, the Netherlands and Germany. At the end of 2002, KPN mobile has over 100.000 users in the Netherlands only and claims a growth of 1.000 new customers a day. To put that in perspective, NTT-DoCoMo currently has over 30 million subscribers in Japan only, which was reached in 4 years. KPN-Mobile is probably not going to reach such high growth rate, but alliances between NTT-DoCoMo and France Telecom and British Telecom can have a positive impact for i-mode throughout Europe.

Of course, i-Mode is not the only way to conduct M-Commerce. WAP and Voice Response Systems (VRS) are also possible (VRS will not be discussed in this paper). In the past few years, rumors about the early death of WAP circulated among the general public. However, with the agreements made by large industries in the last two years at for instance WAP Forum, it could be possible that WAP is able to show its real potential with better protocols, higher security etc. With high-speed communication networks coming available in Northern Europe, WAP will become cheaper and faster.
These networks in combination with WAP and MMS services by Vodafone, O2 and Ben give WAP and mobile data communication new chances and growth of these services is expected.

Seems that all it needs now is a good PR-machine and content to sell.

M-COMMERCE TECHNOLOGY

COMMUNICATION PROTOCOLS

To make M-Commerce possible, infrastructure and communication protocols need to be able to transmit information between all necessary parties. To send data wireless from a buyer to a seller, the buyer needs to make contact with a data communication network. This data communication network can have many forms. We will make a distinction between a wide area network (WAN) and a local or personal area network (LAN/PAN). This distinction is necessary because the buyer should be able to make a connection at any moment, at different locations (POS and POE) where different networks are available. In the most optimal form, a buyer should be able to make a connection at home on the couch, at work, near the coffee dispenser, outside or at the store / service provider.

Wide Area Network using radio waves

In Europe GSM (Global System for Mobile Communication) is used for vocal communication and was, until the introduction of GPRS (General Packet Radio System) in 2002, also used for data communication by cellular phones or wireless modems. The main benefit of GPRS for the user is not the fact that it is faster, but you pay per received kilobyte instead of per second. This means literally that you pay for then content you receive.

Another benefit of GPRS for some service providers could be the “always-on” functionality combined with Mobile Positioning System (MPS)[iv]. This means that the service you request can be altered or special offers can be made, depending on your location. These services are called Mobile Location-based Services (MLS). In the beginning of 2002 the first services will be available in the Netherlands.

GPRS supports pull and push technologies, so a user can request information (pull) or the user can be send information without a request (push). A good example of a push technology is short message service (SMS, but also EMS / MMS). Pull technology gives the content provider or commerce server the possibility to send the M-Ticket in several formats, based on the users’ request. The pull technology can be seen in action on the Internet; you request information from a server and receive it seconds later on your computer. This is also applicable for wireless communication.

Real third generation network protocol UMTS will not be discussed in this paper as functionality is almost the same but with more bandwidth available (technology differs). Furthermore, several European telecommunication companies have cut immense on their research and development budget for UMTS for the next 12 months so “There will be some waiting involved”.

Local or Personal Area Network using Ethernet

Normally we make a connection with the content provider through a telecom infrastructure and access provider. Another possibility when you are in an area controlled or owned by one company, like a university campus, is to make contact with the company’s network first. The company’s network then directs your information to the telecom provider and so on. This extra step is possible using 802.11[v] protocols in combination with a Voice over IP protocol (VoIP). The most common version, 802.11b Wi-Fi[vi] does not have the capability to support these large data transfers but HiperLan2[vii], a technology based on the same protocol but with more bandwidth and greater reach can make this implementation possible.

A second method of communication can be a direct communication to a content provider, if a wireless network is available to the buyer. For instance, the buyer can make contact using the 802.11 protocol and gain access to content in a very easy manner. This can be used when the

buyer is at the location where he receives the goods or services. It can also be used to redeem the ticket or coupon (POE).

Another wireless network protocol called Bluetooth is used in a Personal Area Network. The range and speed of Bluetooth are very low and the protocol is mostly used to transfer personal data to personal objects. This simple definition does not show all the possibilities of Bluetooth; it could easily be used to validate an M-Ticket at the POE. Because of the small

> *It is 21:28, the movie starts in two minutes. You push some people away and start yelling to the cashier that you are here to collect your tickets you made reservations for. Just when you want to say your name, this very large man steps in front of you. You can't see the cashier anymore and when he is finished the cashier tells you that the movie has already started, he cannot let you in .... and b.t.w. he's very sorry.*
>
> … Let's try this again.
>
> *It is 21:28 you walk straight to the entrance and while you walk through the gate your mobile device gets a request to send a specific ticket. Your mobile device checks, finds and sends it to the entrance computer. Nobody blocking your way, no worries. 2 Minutes later you and your friends enjoy the play.*

range, a wireless network scanner has less chance to pickup the signal.
In the next paragraphs more information about protocols and security will be given. Next we will discuss the current mobile devices and their suitability for M-Commerce.

MOBILE DEVICES

A mobile payment device could be any device that is capable of performing the functions mentioned earlier in the definition. It could be a PDA/XDA, laptop, cellular phone or a combination of these. The device must hold the following functionalities to be suitable for M-Commerce:

- The device has to be able to connect to a data communication network to transmit the necessary information at the POS
- The device must use an identification method to uniquely and correctly identify the buyer and the information sent by the buyer.
- The M-Ticket needs to be validated at POE.
- Payment should occur almost at the same time the transaction takes place or at least be guaranteed to the seller.

Several companies have created solutions that hold some or all of these functionalities. For instance:

- Nokia's Wireless Identity Module (WIM) used in cellular phones, which uniquely identifies the customer and completes the transaction via a secure WAP connection (WTLS 3 or SSL) with a commerce server. Read the chapter: "WIM explained" for more information.[viii]
- Siemens introduced pay@once, a payment method where identification takes place via the caller's telephone number and the M-ticket will be received through SMS. During this transaction the amount needed is reserved at the caller's bank account. After completion of the transaction the amount will be transferred to the seller.[ix]
- i-Mode, Vodafone Live! and other concepts offers the possibility to buy products or services through the their GPRS network and gateway. Users are validated through their telephone number and payment registration is done through the provider's network and the users phone bill. The user can receive it's content by messaging or via WAP or i-Mode communication. Read the chapter "example: I-Mode
- Transaction overview" for more information about i-Mode.

All these implementations use different techniques to complete the transaction, but they all share the same principle. The buyer and the seller need to identify themselves and during the transaction the buyer's credit will also be checked. At the end, the proof of purchase will be send to the buyer.

SECURITY

IN GENERAL

"The encryption method or security in general should be strong enough to make the effort to fraud more expensive than the potential profit and the cost of securing should be lower than the potential loss." is a common heard statement. In a way this statement is correct. On the other hand, if we take a closer look at the term 'cost of securing', we can think of indirect costs that can rise to an infinite amount. If system security is breached, the seller loses credibility. For a bank the indirect cost would be infinite high, this depends on the service provided. Thus, the algorithm used by a company or the chosen method depends on the business it is in and the product it secures.

In the following chapters, some security terms and protocols will be explained, like public key infrastructure, identity modules and secure protocols. We will start with PKI.

PKI EXPLAINED

PKI stands for public key infrastructure and enables users of an unsecured network such as Internet to exchange data in a secure way. This is done using a public and private cryptographic key pair that is obtained and shared through a trusted authority[x].

A public key infrastructure consists of:

- A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key.
- A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor.
- One or more directories where the certificates (with their public keys) are held
- A certificate management system on the device

Note: The numbers in the text below are related to Figure 1: PKI transaction overview found below the text.

In public key cryptography, public and private keys are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA / RA). The private key is given only to the requesting party (2) and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access (3,4). The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text (6) that has been encrypted with your public key by someone else (5).

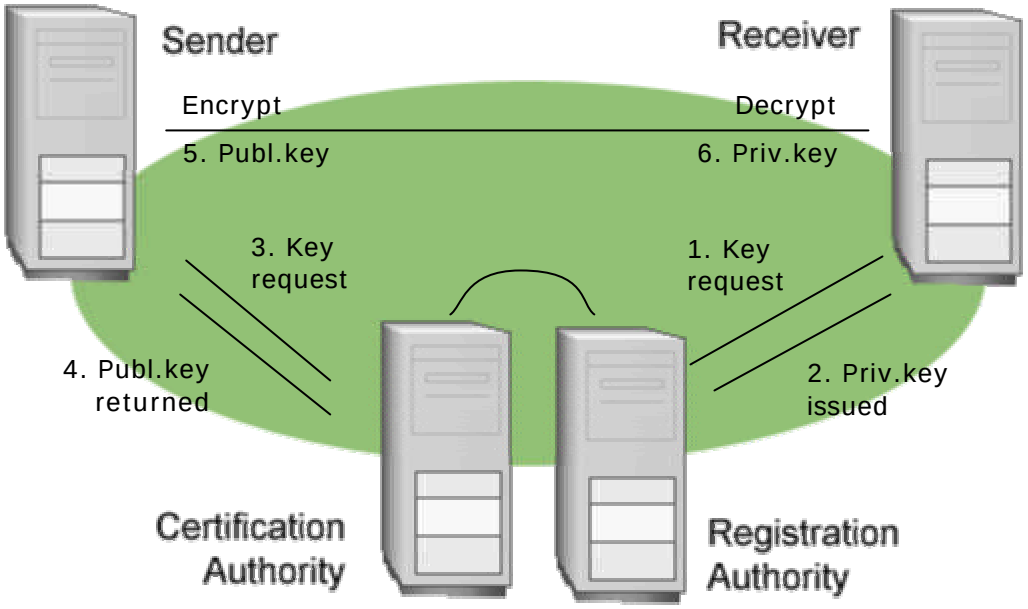


Figure 1: PKI transaction overview

The acceleration of e-commerce and business-to-business commerce over the Internet has increased the demand for PKI solutions. Related ideas are the virtual private network (VPN) and the IP Security standard.

WIM EXPLAINED

A WIM (Wireless Identity Module) stores security information in a portable device that can only be accessed through a Personal Identity Number (PIN). The module also has the ability to perform cryptographic operations.

The WIM can be implemented in different ways. By making it a part of the mobile device's hardware gives a high level of consumer convenience but makes it depended on the lifecycle of the device. By using SWIM (Subscriber Wireless Identity Module) this dependency is removed, but standardized features and interfaces are necessary to ensure interoperability between different manufacturers' technologies and SIM cards. Another approach is to use a Dual Slot implementation. A smart card can be used to store the security information and can be used in other devices. The drawbacks are the use of two different cards and implementation issues regarding the mobile device.

SWIM seems to be the best method of implementation for WIM from the end-users point of view. Network operators can, by issuing WIM cards, play an important role in the enabling of mobile services (p.e. KPN + i-Mode).
It is good to note that service providers have no interest in the method that is used for WIM implementation, because server-side execution will be identical.

An implementation of a all-in-one card is provided by Syntiq (www.syntiq.com), which has extended functionality compared to the SWIM or regular SIM cards.

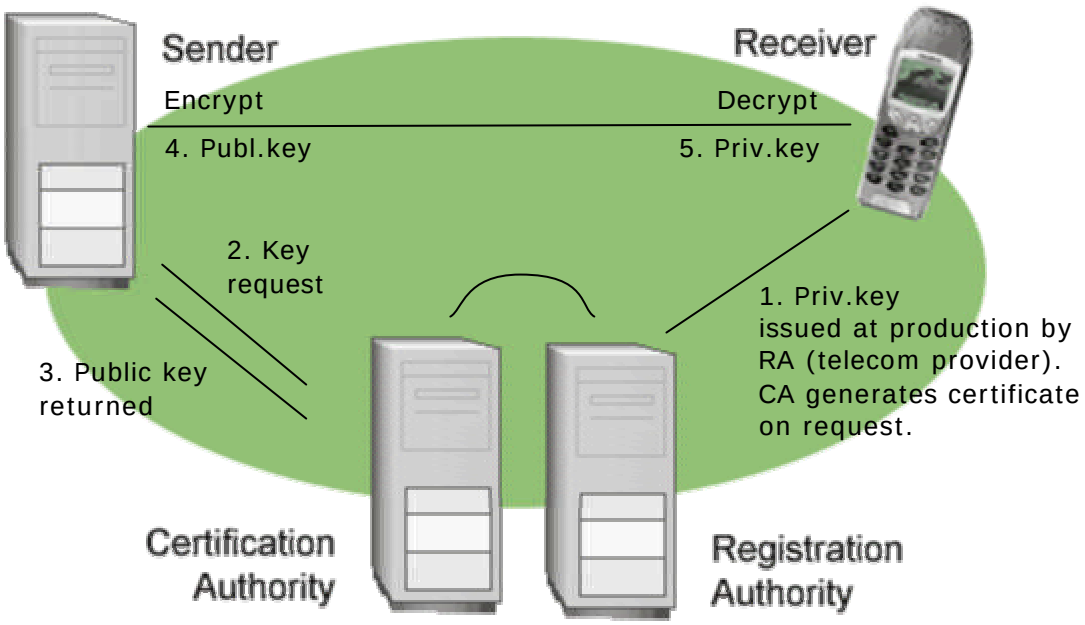
COMBINING WIM AND WPKI

Using the Wireless PKI solution (WPKI), anonymous key pairs can be pre-installed in WIM with a corresponding PIN code. In this case the manufacturer's certificate ensures the key's authenticity. In the first instance of secure service usage, the anonymous key pair will be attached to a specific user identity by the RA/CA. And from there authentication will take place through normal PKI methods.

Security mechanisms since WAP 1.2 specifications are based primarily on PKI and the extension to the mobile environment encompasses the infrastructure and the procedures required to enable the trust provisioning needed for authentication and digital signatures for servers and clients.

The key elements of the WIM/WPKI system are:

- Generally available mobile phones with WIM
- WAP Gateway-enhanced with certificate-based identity validation capability
- Registration Authority (RA) for certificate enrolment
- Certification Authority (CA) with back-end PKI infrastructure



WAP PROTOCOL EXPLAINED

WAP Basis

Within the WAP protocol, a transport level security is specified using a transport protocol known as the Wireless Transport Layer Security (WTLS) protocol. WTLS is conceptually and functionally equivalent to Secure Socket Layer (SSL), also known as Transport Layer Security (TLS). This protocol encrypts en decrypts information sent between a WAP client and a WAP gateway and ensures the integrity of the communications. In the diagram below, all layers of the WAP and Internet-protocols are shown.

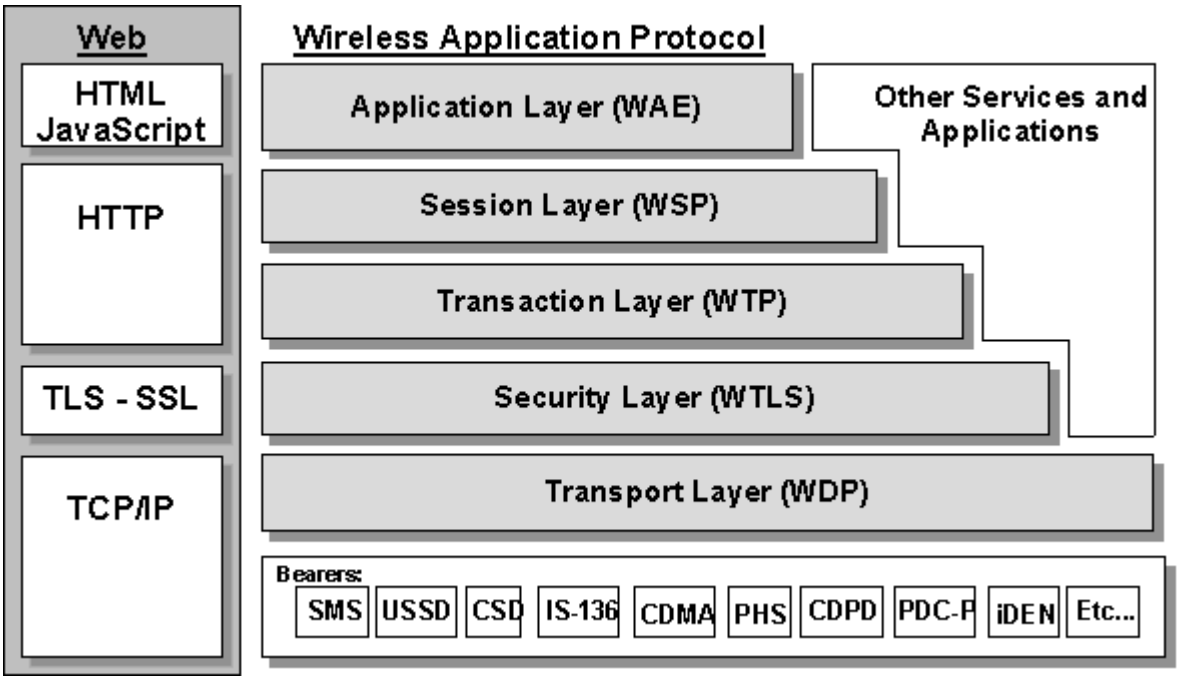


Figure 2: Comparison of Internet and WAP stack

Currently WTLS Class 3 supports client/server authentication over a secured channel and mutual authentication between the server and consumer by an exchange of certificates. The WAP/WPKI system is based on this protocol and WTLS Class 3 security is strong enough to transport M-Commerce transaction information.

Session management

When a connection is made to a server, it might still be needed to check the identity of the person sending or receiving data. To overcome this problem, sessions have been introduced. As shown in "Figure 2: Comparison of Internet and WAP stack" there is a session layer implemented in the WAP protocol stack. This layer is implemented differently from the HTTP session layer for the connection of with the mobile device can drop unexpectedly. Therefore, the WAP gateway plays a larger role by intermediating between the content providers and the mobile device. After authentication within the session, several transactions can take place. After a while the session will timeout and re-authentication will be needed. All communication then takes place using WTLS.

WAP 2.0

As of the 11th of august 2002, WAP 2.0 is a by wapform.org[1] approved recommendation for the new WAP protocol. With this protocol, security has tightened by replacing WSP, WTP, WTLS, WDP and SSL security (server side) by optimized wireless versions of HTTP, TLS and TCP/IP.
This new version of WAP makes it possible to have a direct and a more secure connection to a WAP server. Using WAP 2.0 for all communication between the commerce server and the mobile device can have a positive effect on delay times and makes it possible to use a propriety identification method.[xi]

As shown in "Figure 2: Comparison of Internet and WAP stack", the lowest level of the protocol stack is a range of protocols to transport the data over the network, depending on the network and the data that has be transported.

[1] Wapform.org is an initiative to establish a common used and accepted protocol for mobile communication, based on WAP.

WIRELESS NETWORK ENCRYPTION

When using a wireless network protocol, like Wi-Fi, HiperLan or other 802.11-based protocols, data communication is often not encrypted. This means that anyone with the software and hardware near an access point or WLAN user can intercept this communication. Several methods are developed or currently still in development. The best-known method is WEP, but this method is not good enough to secure important networks, for it sends its initialization vector un-encrypted to the server. This means the network security is compromised if the interceptor receives enough information. Other protocols are the Extensible Authentication protocol (EAP or 802.1x), Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (EAS) which probably will replace WEP in the future. Currently the implementation of a VPN connection with additional authentication and a firewall is the most secure implementation. But the equipment needed and the maintenance costs are high. A combination of WPKI and VPN is possible and even more secure.

TICKET ENCRYPTION

When a ticket is send to a mobile device, it can be delivered in encrypted form. If WIM/WPKI methods are used, the WIM module decrypts the ticket using the private key stored in the WIM. When it is send using another method, software needs to be available on the terminal to decrypt the ticket. Decryption can take place at the moment of reception or at the moment the ticket is accessed by the user. If a mobile device is considered secure and depending on the time needed to decrypt the ticket, one-time decryption at reception is an option and saves a lot of (CPU) time. If a barcode is used as a unique code, other methods can be implemented.

The encrypted string in a ticket can be created based on the buyers and sellers identification and possible a transaction id. There are several encryption methods, ranging from simple and fast to complex and slow, for instance RSA delivers a very secure 2048 bit PKI (basis of PGP and GPG).

A faster method, not based on PKI but on shared secret / symmetrical key, is for instance Blowfish. This algorithm is a 256 to 448 bits encryption algorithm and is both strong and fast[xii]. A symmetrical key involves sending your key in advance to every party you wish to communicate with. This can create certain obstacles, for we do not know which parties to trust in advance.

CONCLUSION

To create a secure payment system, it is necessary to secure both the connection and the storage, but also assure the uniqueness of the ticket. The connection can be secure using a public key infrastructure maybe in combination with an encrypted communication protocol like SSL. The storage of the key should be in a secure way. A Secure Wireless Identification Module (SWIM) can be used, this SWIM can be build onto a chip used in the communication device or can be build into the device. The ticket can also be stored in a secure area on the device, however the buyer should still be able to transfer the ticket to another person.

There are several encryption methods currently competing in the Wireless LAN area and it is possible these techniques will be used instead of the in WAP implemented security protocols. An asymmetrical key might be a better solution than a symmetrical key, because the public key is always available and CA and RA act as an intermediary.

After one hour of fine theater, it's time for some relieve and you order a few drinks and pay using your ticket ID in your phone. From the corner of your Eyefi you see a teenager being escorted to the manager's office. The security guard takes the phone and you think, "Those whiz kids are getting younger and younger". Luckily, the ticket is unique and can be validated anytime by comparing the transaction details, the ticket information and the identification of the person.

TRANSACTION OVERVIEW

In this chapter the whole transaction from making a connection to the redemption of the M-Ticket will be explained in depth. First, we need to define all the actors.

ACTORS AND ACTIONS

In a general transaction environment, several roles can be defined.

- Buyer
- Seller
- Commerce Server (p.e. WTS)
- Bank and/or clearinghouse
- Gateway and network
- Validator

An actor can have one or more role, depending on the used infrastructure and his role within the process, for instance a network provider can be the validator or the clearinghouse.

Let us look at some diagrams for a better understanding. In the diagram below a general overview of a transaction from the buyer's point of view is shown.

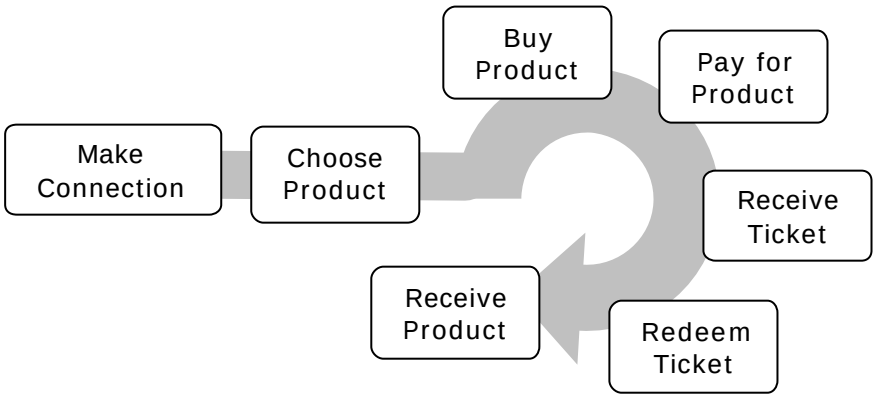


Figure 3: Transaction from buyer's point of view

This diagram looks simple and that is what it should be for the buyer. Behind this easy process a more complicated infrastructure is needed. Let's take a look at the different actors in this process and how they are connected.

Actors and the transaction

There is a large difference between a direct transaction between buyer and seller and a transaction where a commerce server, clearinghouse and a network is needed. To create an environment where buyers can buy goods or services from several sellers in an easy way, it is not advisable to use a direct communication method. In this case a commerce server can be a good option. The commerce server holds information about more than one buyer and several payment methods. It gives the buyer the possibility to choose method, brand and product.

EXAMPLE: WORLD TRADE SERVER

An example for a commerce server is a World Trade Server (WTS, Ericsson).

> *A World Trade Server is a pure Java based application platform that generates, distributes and records the clipping and redemption of electronic Coupons, Tickets at Internet sites as well as brick and mortar locations*[xiii]

Several companies have implemented their own version of a WTS with different specifications, but their core functions remain the same.

The commerce server is not the only server needed. Using the diagram below, the infrastructure and steps in the process are explained.

Let us start with a graphical view of the system. In the figure below, the buyer makes a connection with a WAP gateway (1), which guides the information flow from and to the buyer's device. The buyer contacts the world trade server (2) and his request for information is sent to a specific content provider (3). The information will follow the same path back to the buyer. For internal communication, the gateway and the servers use the Internet IP protocol.

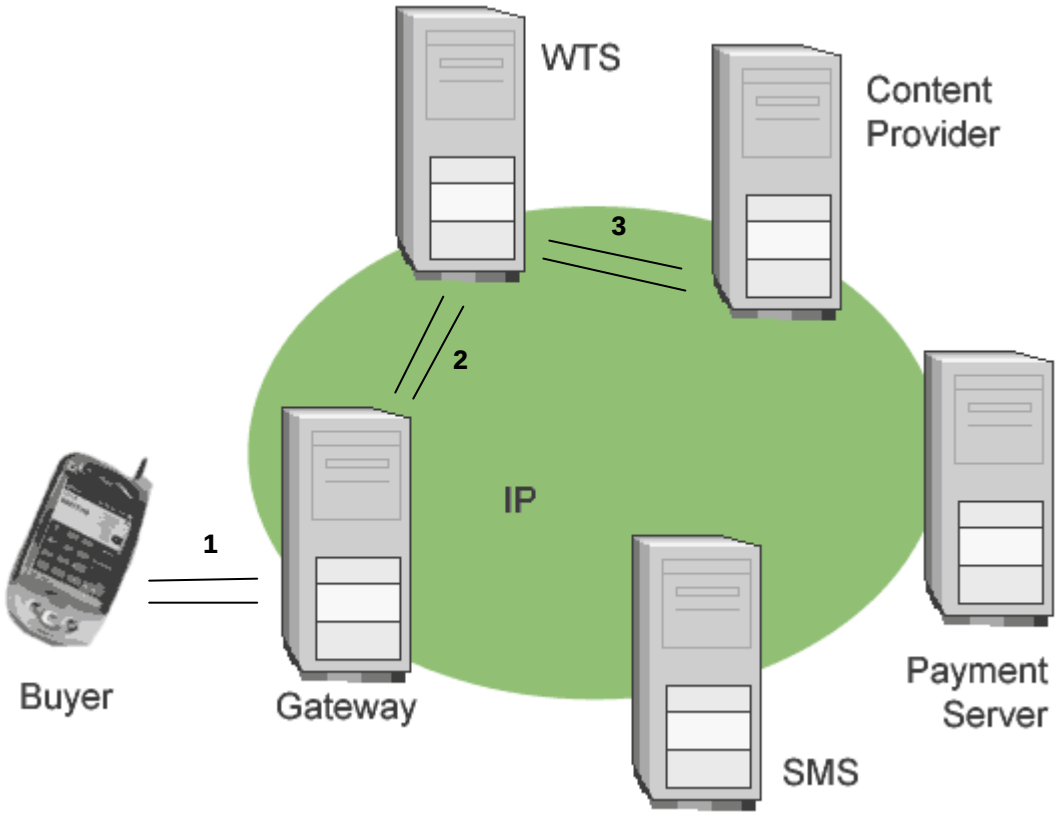


Figure 4: Transaction part I

When the buyer has made his choice, he sends the request to the WTS (4), which will handle the whole transaction from there. The WTS connects to a payment server (5), checks the buyer's account and places the order with the content provider (6).

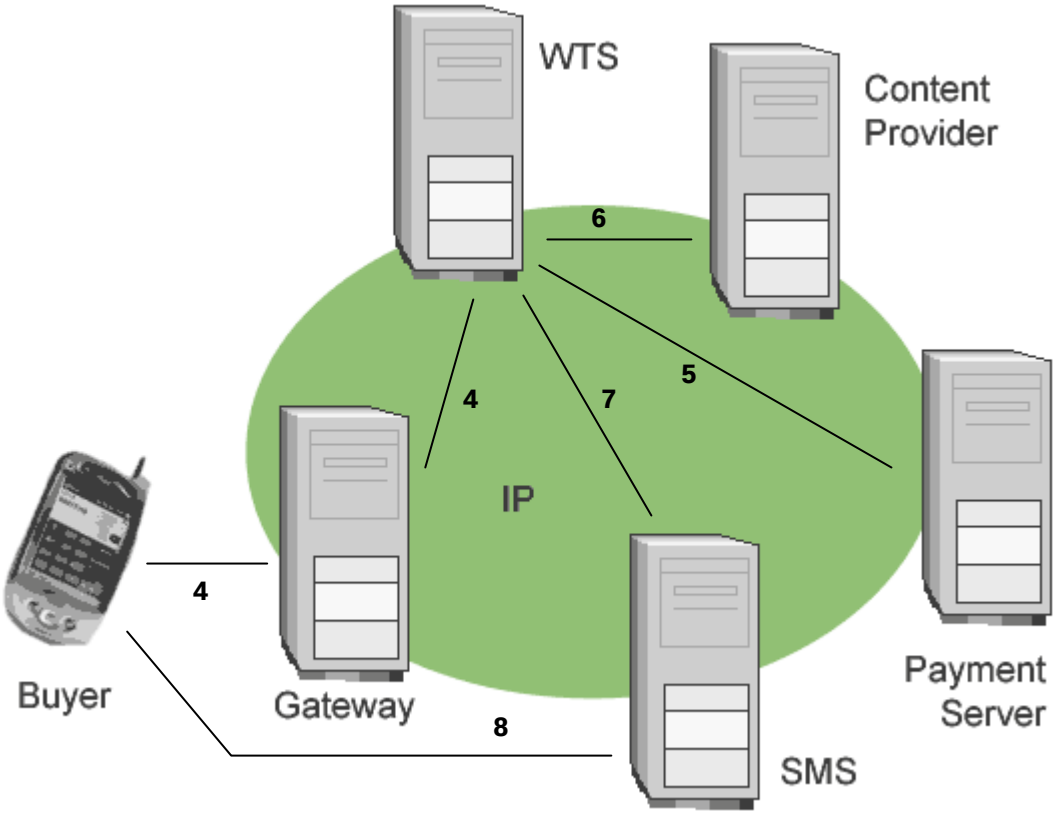


Figure 5: Transaction part II

From there two possibilities exist. To send a ticket to the buyer, the system can use the gateway or it can use an SMS-Server (7,8). When using the gateway, there still has to be a connection between the gateway and the buyer's device. To give the user as much ease of use an SMS-server would be the best option.

World trade server security

Something we did not discuss yet is the security issue. The world trade server has a security system based on the public key – private key infrastructure. We discussed this in previous chapter "PKI explained".

M-TICKET UNIQUENESS AND REDEMPTION

When a buyer receives his m-ticket this ticket hold a unique identification. When redemption of the ticket takes place, the ticket needs to be validated. This validation can take place online or locally. With online validation, the ticket is send through an access point at the POE to the commerce server. The server then returns a confirmation or an error to the POE server. So for every validation a communication with the commerce server is needed. When validation takes place locally, the m-ticket is compared with locally stored information. This will require not only a connection to the commerce server but also a database to store the validation information.

There are several forms in which a ticket can be unique; an SMS with a unique string, a barcode, encrypted by a key or another personal identification method build in the device. The security issues are discussed in the next chapter, but some advantages or disadvantages can be found very easily. When using a barcode, the display has to be readable for a scanner and it is not readable for humans. This is not the case when using a unique string within an SMS. When a public key is stored on the device, it will need a WIM to store the key and it will need a protocol to communicate this key with at the POE. This reduces the amount of potential users.

EXAMPLE: I-MODE

Transaction overview

With the introduction of KPN-Mobile's i-Mode, it also introduced electronic services (content delivery). These services are provided by KPN Partners and can be accessed using KPN's gateway. The content can be placed on a content server within the domain of the gateway.

Because the buyer has an i-Mode subscription, the telephone is identified through the caller ID and linked directly to your bank account. When the i -Mode services are not free, KPN uses the buyer's bank account registered with KPN to transfer the amount owed to the seller. KPN receives 14% of every transaction for providing the payment service and the network.

When content or a service is delivered using Internet, instead of using the KPN Partners network, on an i-Mode telephone, the buyer needs to register himself with the seller to be able to pay for the goods or services. KPN does not interfere with that kind of transaction.

KPN Mobile has two roles to play, by adding the partners to the i-Mode in-phone menu it acts as a intermediary between buyers and sellers. KPN also makes sure the payment for a service is carried out. Below an overview of the i-Mode system is displayed, note that it resembles the WTS environment. The communication between the buyer and the gateway can also be done through e-mail or SMS.

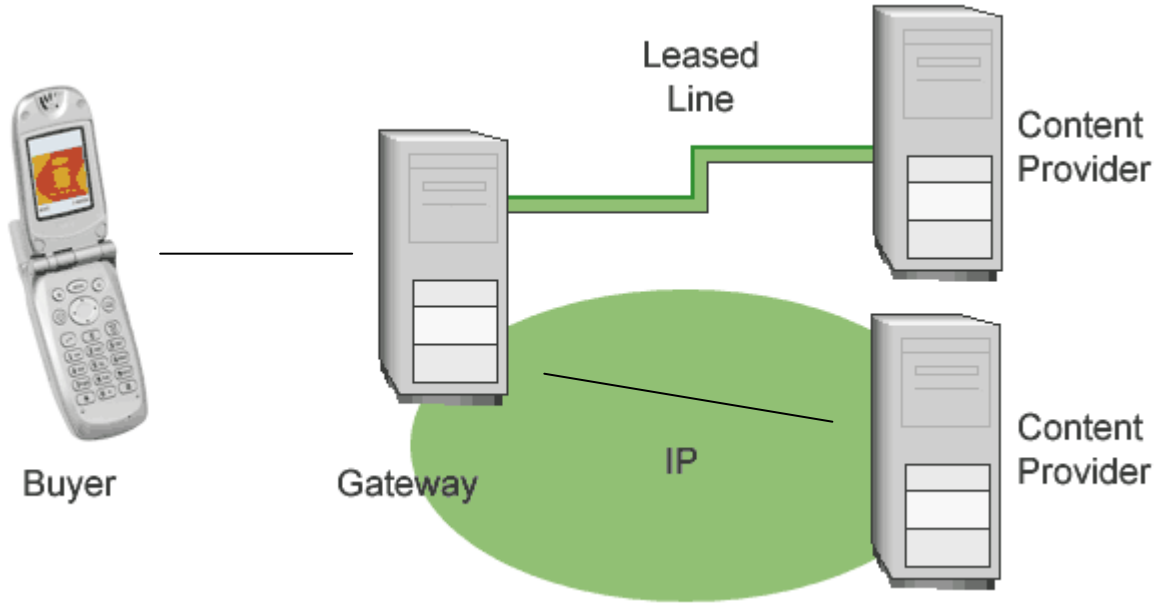


Figure 6: I-Mode overview

Future i-Mode

NTT-DoCoMo has been developing i-Mode since 1999 and is going to improve its functionality and performance in the years to come by implementing a high-speed network and adding functionality and content. It has stated in news items found on the Internet that it participates in several forums and discussion groups. When using packet switched network for i-Mode services the protocols used are that of the WAP 2.0 specification released by the WAP Forum in 2001. This might enable third parties to setup another environment like i-Mode, but for now, the i-Mode protocol en interface is owned by NTT-DoCoMo.

EXAMPLE: SWITCHPOINT[xiv]

In 2002, KPN introduced SwitchPoint for payment of digital services. When a buyer has found a product or service he wants to receive, the buyer can make a call and type in a unique id displayed with the product or service on an Internet webpage. The payment is instantly and

the digital content is made available directly. The payment transaction is done through identification of the telephone and the connected bank account. These payments are mostly small. Using SwitchPoint has two disadvantages, the first is the fact that you do not exactly know what you buy. A description is given, but this can sometimes be not enough to know exactly what you are buying. The seconds disadvantage is not really a disadvantage but more an inconvenience. You always need two media to communication, the Internet for viewing and the mobile phone to pay for the content. In January 2003 a KPN MultiMedia Services developed an SwitchPoint interface for KPN's i-mode phones.

EXAMPLE: MOXMO[xv]

Moxmo introduced a mobile payment system based on a 'mobile wallet'; this wallet is stored on a server inside the Moxmo system. You create an account and transfer money from your bank account to the Moxmo account. When the account is active, you can use your mobile phone's SMS functionality to transfer money to other Moxmo mobile wallets. Besides payments to mobile phones (with mobile wallets), you can also use your phone to pay for products or services when the service provider is registered as a Moxmo acceptant.
Advantages:

- The system itself is well structured
- Validation is secure using a PIN-code and a verification call from Moxmo.
- According to Moxmo, easy to use.

The disadvantages are:

- Debit account without interest
- Support must be widespread before customers can benefit from the advantages, especially for transferring money to other mobile wallets.
- The callback function can become an annoying feature .

Moxmo is also porting its functionality to i-mode phones in the near future (using Java Applets). Maybe it would be an interesting idea to use KPN's identification methods to remove the callback function from the process and put Moxmo in the phone's Partner Menu.

You can compare this with the Chipper™ or ChipKnip™ but also with SwitchPoint when using it for online transactions.

On December 26 2002, Moxmo, CMG and Partyscene.nl started a trial for a mobile party ticket system. Buying the ticket in advance gives the buyer 50% reduction on the entrance fee. In the first trial the M-Ticket was received through SMS containing a barcode. Moxmo will step in later to add mobile payment for the M-Ticket[xvi].

EXAMPLE: NOORDNED[xvii]

NoordNed public transport has introduced a mobile ticketing service in a joint effort with Free University Amsterdam (VU Amsterdam), LogicaCMG Unwired Concepts and Rabobank. The service is in a testing stage at the moment and will be finished by the end of the year 2003.

Through an Interactive Voice Response / Voice Response System (IVR/VRS) or through Internet a ticket for a specific route at a specific time with a bus or train is requested. This ticket is send by SMS to the user's mobile phone and the user has to show the SMS (M-Ticket) to the conductor. The conductor checks the information in the M-Ticket and validates the information through a PDA with GPRS connection (when available) with the ticket server. When the ticket is found valid, it will be marked as used on the server and cannot be used again. By enlisting to the NoordNed service, you give NoordNed direct access to your bank account and your phone number or login account are used to identify you.

This is a very good example of combining available technologies to an easy to use product. The only disadvantage I see, can be the registration. However, this disadvantage is not enormous.

TRANSACTION SETTLEMENT

The transaction examples above can be separated into two groups based on the payment service. One group uses a special bank account created by the user with money transferred to

it from their normal bank accounts. The other group uses the permission the telecom provider has to transfer the amount due from the buyer to the seller. The main issue is that you need to be registered with any company to give them access to your bank account. What other company than your telephone company is suitable for function? You already trust them with your bank account, don't you?

The access provider's functionality can be separated in to distinct functions, infrastructure and identification. For instance, it is possible to call via KPN to an access provider (like O_2 or Genie) for mobile connections. From there you can access several services on the Internet. There is one problem, you need to be identified by one of the parties and the content provider should have a financial understanding with that party. It might be possible to register yourself with the content provider, but this is not very handy when you use a lot of content providers. Then one party that handles the financial part of the transaction and is able to identify you might be the best option.

The content provider then faces a dilemma. If there is more than one access-provider it might be necessary for the content providers to choose several access providers to distribute their service to enough and as much potential customers as possible. This can be very expensive this service does mean investing money and if you don't have enough users you cannot make this investment profitable.

SYNTHESIS

In this essay, I tried to give the user an overview of all available communication technologies, an overview of the transaction itself. Unfortunately, there is not enough time to discuss the transaction server-side, which could be a valuable addition to document. Furthermore, Voice Response Systems and Interactive Voice Recognition can be a user interface extension to certain payment systems and should not be forgotten when looking for implementation solutions.

The communication technologies described here, have been available for several years and at this moment, an opportunity to use these technologies for mobile commerce is here. It seems that technology is not a blocking factor for growth. The economic growth in the first two years of this century was relatively low compared to the last years of the 20th century. This has had its impact on research and development, but not on consumer expenditure until the end of 2002. At that time, GPRS came available in Europe and gave new possibilities for WAP. Mobile commerce and mobile payment have finally become available for the public. The main obstacles are the content and trust, which can only be overcome with more research on security, more trials and more participants.

CONCLUSION

When we compare all technologies and think of a solution without thinking of economical feasibility, this solution could give us a possible solution in the near future. At this moment, only proven and fully tested combinations of methods and technology will be used to create a mobile commerce and payment solution. While researching these technologies and writing this paper the mobile world changes and keeps on changing.

Currently the implementation of payment through the network provider is the easiest and cheapest method to give the buyer the possibility to conduct mobile commerce. KPN, Vodafone, Ben and O2 use this implementation. The content currently offered is only enough to attract customers but not enough to keep them. If more content becomes available, rapid growth in this sector is expected. At this moment, some restrictions are applied to the providers' networks, for instance SMTP access.

In my opinion promotion, content and ease of use are the drivers for mobile commerce growth. The growth of content is a continuous process but ease of use is something that should be thought of from the start. Like Nokia's cellular phone menu, which used to be the most intuitive and mature when all others were just starting to think about usability?

While WAP and i-Mode take off in the telecom sector, Wireless LAN or Wi-Fi products have become affordable and accessible to the public. High speed wireless LAN, like HiperLan are not yet fully available but it seems that more and more companies implemented a wireless LAN. Also publicly available wireless networks have become popular and are rapidly growing (for instance the city Leiden). When a high-speed wireless network becomes available in the future, VoIP might be able to carry all internal communications in a campus-like environment. Of course, there are some security issues involved.

In my opinion that a communication protocol like Bluetooth can be used to communicate at the POE (a static POE). Another possibility could be a SwitchPoint type of payment, where you receive a special code at the POE and make a connection to the SwitchPoint server. Currently in the NoordNed case the validation of the ticket is done by a conductor who has a device with a GPRS connection to the ticket server. The ticket has a code and information about the route and this information is used to validate the ticket. In the same way a ticket for a theatre play can be validated at the POE when the POE server has a direct connection to the validation server. The problem with these last two methods is the necessity to have a connection.

There were two types of mobile wallets / payment methods described in this paper, one method where a new account must be created and the users need to enlist for the service. And another method where all payment is done through the network provider. Implementation of the last will hold the largest ease of use for the consumer but then the diversity of access providers will be the next subject of investigation. For instance, sellers might choose the three largest network providers and forget about the others making the products not available to all Dutch users.

Security is not a problem but a matter of choice. While researching I noticed several tailor-made implementations ranging from callback to a separate code generator but I did not see implementations of WPKI. Because of the quality of the encryption and the easy to use key infrastructure, I am surprised not to have found more examples. Of course when sending information that is not interesting for hackers, security measures can be kept to a minimal.

APPENDIX A: SUPPORTING DATA

SIZE AND USAGE OF ELECTRONIC NETWORKS (THE NETHERLANDS)

Consumer	% of the total nr. of persons						
- Persons with a PC at home			55	60	66	70	74[1]
- Persons with a internet connection at home				16	26	45	57[1]
- Electronic shopping				2	4	7	11[1]
Business	% of the total nr. of businesses						
- Number of companies with a computer	78	74	75	84	85	93	93[1]
- Number of companies with external data communication	45	45	51	60	67	76	84[1]
- Number of companies with access to the Internet	11	13	26	42	55	71	82[1]
- Electronic ordering of goods and services					20	34	38[1]
- Electronically receiving orders		1	3	6	18	28	34[1]

Table 1 De digitale economie 2002 – CBS.nl[ii]

NEWS ITEMS

"mmO2 growth of SMS messages has risen 6% in the second quarter of 2002. Entertainment is the main driver for WAP and SMS. mmO2 has been able to grow the amount of 'active' GPRS connections by 10,000 per month, driven largely by business users." [xviii]

"KPN Mobile has passed the milestone of 100,000 i-Mode customers in the Netherlands and Germany. So far there are already more than 23,000 subscribers in the Netherlands and 77,000 with E-Plus in Germany. The expectation is that one million customers will be using i-Mode in 2003. The use of the official i-Mode services is as expected and averages slightly more than two content subscriptions per user. At this moment the most interest is for the categories 'melody and images' and 'news and weather'. Content partners already offer more than 80 official sites on i-Mode in the Netherlands and 100 in Germany. The number of independent sites continues to grow strongly. Estimates indicate that there are already more than 7,000 independent or open i-Mode sites in both countries." [xix]

"Het internetgebruik in Nederland is dit jaar harder gestegen dan in 2001. Met het online winkelen wil het ondertussen nog niet echt vlotten. Dit blijkt uit het derde Global e-Commerce Report van NIPO Interactive. Inmiddels maakt 61 procent van de bevolking van zestien jaar en ouder minimaal een keer per maand gebruik van het internet. Een jaar geleden was dat percentage nog 52 procent. Volgens het NIPO is het aantal gebruikers sneller gegroeid dan een jaar geleden." [xx]
Relevant information translates to: Internet use in the Netherlands rose this year more than 2001. Currently 61% of the population older than 16 years old uses the Internet at least once a month. Last year this number was 52%

[1] End 2002. values from survey "Automatiseringsenquête 2000–2002".

APPENDIX B: SOME NUMBERS

Below are two small paragraphs with additional information about M-ticket size and an overview of the different networks.

M-TICKET SIZE AND COST

Using WAP: Product description can be done on average with 300 words, possibly with a picture. This means around 3 kilobytes to download. Navigating the shop can take a long time and can be around 16 kilobytes (i.e. 7 pages + logo). Currently for price to download 19 kilobytes the costs are around 0,10 euro.
Using SMS: Size of uncompressed ticket is between 40 and 100 Bytes, sending this ticket by SMS is possible and will cost around 0,09 euro per ticket. Subscribing to an SMS service can cost 450 euro per month for a medium volume subscription (5000-35000). The costs for sending a ticket by SMS is very low compared to the infrastructure and consultancy needed to link the SMS server to the transaction server. Estimations for an interface between the two servers are not accurate because of the vast amount of possible environments and implementations. 30,000 and 100,000 Euro can give a simple solution.

INFRASTRUCTURE

For M-Commerce and M-Payment several method exist to communicate with the transaction server. Below is a list of protocols on different layers and their capabilities.

USED TECHNOLOGY	DATA SPEED (KBPS)	VOICE CAPABLE	INTERNAL SECURITY	HARD- / SOFTWARE
Voice + Data Comm.				
GSM	9 – 19	Yes	Normal	Hardware
GPRS	13 - 104	Yes	Normal	Hardware
UMTS	128 - 2048	Yes	Normal	Hardware
Data communication				
Bluetooth	Max 1024	No	No	Hardware
Wi-Fi	1024 – 11264	Possible	No	Hardware
HiperLan2	25600 – 55296	Possible	No	Hardware
Communication protocol				
WAP 1.x	-	-	Normal	software
WAP 2.0	-	-	High	software
i-Mode	-	-	Normal	software
Encryption implementation				
Storing information in WIM	-	-	high	Hardware
Encryption via PIN	-	-	high	Software
Using protocol WTLS	-	-	high	Software
Encryption via WPKI	-	-	high	Software

Explanation

The diagram above gives an overview of different technologies. The technologies are grouped per technology-type. For communication technologies on a hardware level, the theoretical speeds are displayed. The column Hard- / Software shows the reader on which level the implementation of this technology takes place. For instance the protocols WAP / i-Mode could function on several hardware platforms
When using TCP/IP over a data communication technology, the data speed drops logarithmic with the number of users on the network. All communication protocols have their own compression techniques, which make it possible to enhance the practical data speed.

ABBREVIATIONS

B2B, B2C	Business to Business, Business to Consumer, other variations are possible
CA	Certification Authority
EMS	Extended Message Service
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
HTTP, HTTPS	(Secure) Hyper Text Transfer Protocol, protocol used for packaging information to be send over the Internet.
IMEI	International Mobile Equipment Identification Number
IMSI	International Mobile Subscriber Identity
IVR	Interactive Voice Recognition
MLS	Mobile Location-based Services
MMS	Multimedia Messaging Service
MPS	Mobile Positioning System
MPTP	Micro Payment Transfer Protocol
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POE	Point of Entry, moment when or location where a mobile ticket is redeemed
POS	Point of Sale, moment when or location where a mobile ticket is received by the buyer
RA	Registration Authority
SIM, SWIM	Subscriber (Wireless) Identity Module
SMS	Short Message Service
SSL	Secure Socket Layer
SWIM	Secure Wireless Identity Module
TCP/IP	Transmission Control Protocol / Internet Protocol, standard protocol used for sending and receiving packets of information over computer networks.
TLS	Transaction Layer Security
UMTS	Universal Mobile Telecommunications Systems
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRS	Voice Response System (other possibilities: Voice Recognition System)
W3C	World Wide Web Consortium, a organization that creates uniform recommendations of protocols or languages, mostly on the Internet.

WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
Wi-Fi	Wireless Fidelity
WIM	Wireless Identity Module
WPKI	Wireless Public Key Infrastructure
WSP	Wireless Session Protocol
WTLS	Wireless Transaction Layer Security
WTP	Wireless Transaction Protocol
WTS™	World Trade Server, a Regisoft Product
XDA	Extended Digital Assistant

BIBLIOGRAPHY

Unavoidable not all items are in English.

---

[i] "Overview of the GSM- market", by Verdonk Klooster & Associates, June 2002, www.vka.nl
[ii] Statistics found in 'de digitale economie 2002' by http://www.cbs.nl.
[iii] Mobile Payments published by Wireless World Forum 2002, http://www.w2forum.org
[iv] Ericsson Mobile, Mobile Positioning System Whitepaper, http://www.ericsson.com/mobilityworld/sub/open/technologies/mobile_positioning/SubPages/mps_system_overview?PU=mobile_positioning.
[v] http://www.rfc.org ….
[vi] Wi-Fi worldwide forum
[vii] More information about HiperLan2 can be found at http://www.hiperlan2.com/
[viii] Nokia, WAP Wttp://hitepaper, http://press.nokia.com/PR/200002/775090_5.html, *http://www.nokia.com/corporate/wap/NMIT31_DS.pdf*
[ix] Siemens Mobile Division, Mobile Payment Whitepaper, *http://www.siemens-mobile.de/pages/payment/en/s_nav15.html*
[x] Definition by techtarget.com, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214299,00.html
[xi] More information about the new WAP2.0 standard can be found at w3c.org and http://www.wapforum.org.
[xii] Blowfish information and speed comparison, http://www.counterpane.com/blowfish.html
[xiii] Ericsson, 'TelematikTage Bern', 2001
[xiv] SwitchPoint information found at http://www.switchpoint.nl, which is a KPN product.
[xv] Moxmo information was received from Moxmo information can be found at www.moxmo.nl.
[xvi] Moxmo, CMG, Partscene example, http://www.persberichten.com/Detail.asp?id=11559
[xvii] Information received from CMG Unwired Concepts participant in NoordNed project http://www.logicacmg.com.
[xviii] 'mmO2 continues strong growth in mobile data', 18th of July 2002 on http://mmO2.com
[xix] 'newsitem', 14th of August 2002 on http://www.ntt-docomo.com/ .
[xx] Newsitem, 28 juni 2002 on http://www.webwereld.nl