Article in T-110.501 Seminar on Network Security 2001 ISBN 951-22-5807-2
Publications in Telecommunications Software and Multimedia TML-C7 ISSN 1455-9749
Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory

http://www.tml.hut.fi/Studies/T-110.501/2001/papers/index.html

Mobile Payment and Security

XingJiang Song
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
xsong@cc.hut.fi

ABSTRACT

Mobile payment presents businesses with unrivaled new opportunities, but also with new challenges. Mobile security is one of the most urgent, and complex challenges to mobile payment. It is becoming a hot issue as web-enabled devices gain acceptance. Currently, the mobile device security is minimal, despite the number of wireless devices in use globally. As the players are only keen to get mobile payment infrastucture out to the market, this will certainly slow down the deployment of mobile payment services by consumers.

The purpose of this research is to explore mobile payment and security in order to find out cons and pons of the current mobile payment services. Due to the fact that mobile payment services involves multiple parties, including operators, banks, and network(terminal) vendors, therefore their business opportunities are also analysed.

1. INTRODUCTION:

1.1 What is Mobile-payment?

According to the research work done by Durlacher, the European mobile payment market is expected to grow from Euro 323 million last year to Euro 23 billion by the year 2003 and is currently about two years ahead of the US in development terms. At the beginning of 2002, mobile payment in Europe will start to take off on a bigger scale, as GPRS (General Packet Radio Service) start s to become more widespread. [1]

Mobile payment is any payment transaction involving the purchase of goods or services that is completed with wireless device, such as a cellular phone, personal computer (wireless), or personal digital assistant. Mobile payment is a new emerging way of paying by using a mobile terminal to initiate transcation over a mobile network. [2]

Mobile payment is exciting because it extends the reach of electronic-payment facilities beyond the limitation of the PC or TV to the hundreds of millions of mobile phone users. Many network vendors, mobile operators, and mobile services providers are enthusiastic about mobile payment, believing mobile payment is to be one of the hot topics in today' service market, creating new meaning for mobile phones.

1.2 Objectives:

The objective of this research is to study the mobile payment and security from a generic point of view in order to find out the current market situation of mobile payment services, forcasting Industry outlook and investment opportunities for equipment vendors, mobile operators.

This report is divided into the following sections: Mobile payment and security in general,mobile payment value chain and enabling technologies, mobile payment forums and standards,current mobile payment application analysis, the future trend of mobile payment service.

2. MOBILE PAYMENT AND SECURITY IN GENERAL

Mobile payment is essentially a subset of the wider electronic payment market. It essentially extends electronic payment into wireless domain. In this respect, many of those services that are common in the ordinary e-payment environment could be replicated into wireless networks.[1]

Many software and hardware vendors are betting that mobile payment will be big business. They expected many enterprises to win more customers and find profitable new sources of revenue, as both business and society becomes "always on". How ever, with a few exceptions, such as NTT DoCoMo's I-mode in Japan, mobile payment has been disappointing.

2.1 Mobile payment delivery value chain.

Different players are positioning themselves in non-traditional roles on the delivery chain.This will determine their ability to be a lead or dominant partner in an alliance offering mobile payment services. A well defined delivery chain can be categories as following parties : [3]

- Consumer, the driving force behand the mobile payment.
- Content providers, which can be a merchant or any entity that has goods or services for sale.
- Mobile voice and data communications carrier.
- Wireless device provider.
- Wireless application gateway (WAG) provider, which separates out wireless data commands from wireless voice traffic and converts the wireless payment messages into a format that can be read by a Web server or other point-of-sale (POS) terminal (e.g., cash register, vending machine) regardless of the device it is coming from or the network it is transferring .
- Authentication provider, which vouches for the identity of the consumer or payer. The common emerging forms of authentication include those provided through a phone's subscriber identity module (SIM) chip, a stand-alone user identification (ID)/password software solution, a digital certificate or biometrics identifier loaded on a mobile device or on a smart card that can be read by the mobile device itself, or by a secondary device attached to the primary device.
- Mobile device application provider, which provides the software or application services invoked by the mobile device to access the content and mobile payment service
- Payment service or software provider, which enables the payment message initiated from the mobile device to be routed to, and cleared by, the appropriate bank or payment network. This service or software generally includes an "e-wallet" application that enables payers to store their payment details, such as credit card account numbers and shipping addresses, on a provider's secure server so that they do not need to type in all the pertinent information required for each sale on small and difficult-to-use mobile keypad devices
- Consumer finance provider, which holds and issues the consumer account used to make the payment
- Merchant finance provider, which holds the merchant account where the consumer funds are deposited

The four basic components of a mobile payment application (that are managed by entities assuming some of the main roles) are: [3]

- Transmission of the data containing the payment message
- Authentication of the identify of the payer (or consumer) to protect against fraud
- Wireless gateway conversion, separating out the data message from the wireless device/network protocol and converting it to a protocol that can be read and interpreted by the destination content server or POS device
- Content conversion/application, where the content provider's content is converted to a format that can be interpreted by the payer's wireless device. The content provider's application also manages the sale and subsequent payment processing of the payment message by handing the payment message off to payment software or a service provider that connects to back-end payment networks.

2.2 Trust in Transaction Security is first proirity:

Security issues are one of the primary obstacles to the successful deployment of mobile payment services.Unlike the relatively predictable problems that emerged from colning and subscribtion frand in first- and second-generation wireless network, the wireless internet introduces endless new risks.

Today no wireless mobile payment security standards exists and, despite a push to devise one, it seems that we are still a long way off from a comprehensive security framework that is both interoperable and scalable. Internet encrption

It is impossible to extract the value of security as it applies to the wireless value chain. Security is deeply and inextricably embedded in every aspect of wireless technologies. The claim frequently made by vendors is that they offer "end-to-end" security. The wireless(mobile) security can therefore be categorised as following: [4]

- Mobile payment enabling application security
- Network Security
- Device security

Security has emerged as a key issue over the last few years. The emergence of mobile payment has not only provided customers and related parties(technique vendors, operators, banks, ISP, 3rd party software) new opportunities but has also increased risk. There is a risk of mobile payment transaction initiated by the customer mobile devices could be theft and fraud.

It's said that the oppertunities in the world of mobile payment related services are huge, but success will ultimately rely on how secure the payment transactions are. Therefore the mobile security is on the boardroom agenda. High-profile hacking events and transaction frauds have meant that security is critical for maintaining customer confidence and corporate reputation.

Ignoring wireless security is a major mistake. Currently security is not being particularly well thought out for mobile payment infrastucture implementation.Mobile device is so easy to steal, thus user authentication must be built into mobile payment applications, a process complicated by the need to support multiple wireless protocols and to facilitate device interoperability.

At present, due to the market principle, mobile security is not a priority when developing mobile payment services. Mobile security is thought to be the added services, built into the mobile payment services from the bottom up. Trust by end users in the ability of mobile operators to carry out handling and processing of transactions securely and effiently is fundamental to the successof mobile payment. In short, the end users must be confident in the financial institution handling the transaction, in the network operator transmitting the transaction, in the technology used, and in the retailer itself.[5]

2.3 Enabling Technologies

Several technologies and applications are necessary to usher in mobile payment, and they are common to many aspects of e-business and wireless environments, such as affordable high-speed wireless access, handheld communications devices and e-commerce-enhancing language standards (e.g., wireless markup language and wireless application protocol). Much of this technology is on the market. The most significant missing link is the capability of industry players to execute seamless and trustworthy wireless payment schemes.

Technologies needed to address payment industry needs include:

- Secure authentication infrastructure on mobile devices e.g., personal identification numbers, unlocking keys on smart cards and biometrics.
- Secure transmission infrastructure for wireless payment
- Trust/validation directories — i.e., buyer and seller authentication information validated along with payment transactions by validation services and directories that trust each other
- Virtual "wallets" stored on a mobile device or accessible over a network that users fill with information on their financial accounts and their payment preferences

Mobile payment is enabled by a variety of emerging technologies, many of which are still maturing. The key technologies are:

- WAP, including WAP Identity module (WIM) for additional security.

- Bluetooth
- Network, including GSM, GPRS, 3G
- Mobile payment software
- Smart card and SIMs

2.3.1 Wireless Application Protocol

The Wireless Application Protocol (WAP) is an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly. [6]

Electronic payment and electronic banking are among the most interesting services to be implemented in the WAP environment. These services have very strict requirements for the security of the system and for the confidentiality of the data.

WAP works by putting a browser into mobile phone and getting the devices to interact with WAP gateway in the network that holds the application and services. The technical limitation of WAP including the CSD and SMS bearers are not optimal for WAP, WTLS has. [7]

The security model for WAP version 1.1 is based on Wireless Transport Layer Security (WTLS). WTLS is a wireless implementation of Transport Layer Security (TLS), implemented as Secure Sockets Layer (SSL) in fixed e-commerce. [7]

The WIM constitutes the WAP version 1.2 evolution of WTLS implementations, and provides a secure environment in which to store and perform WTLS algorithms. The WIM is designed to improve end-to-end security, and to provide means for application security. The WIM security model is based on RSA's PKCS 15 standard for cryptographic tokens. The actual cryptographic operation may use either RSA or Elliptic Curve algorithms. Since the WIM uses standardized and generic interfaces and algorithms, it can be used for non-WAP applications, such as e-mail. [8]

2.3.2 Multi-purpose smartcards and SIM Toolkit. [3]

Smart card vendors are actively working with the handset vendor community to make handsets a commercial reality. Dual slot phones allow the user to use electronic cash cards, loyalty cards and debit/credit cards via phone. This technology will also allow the network operators to remotely upgrade applications supporting existing and new smartcard.

Smart cards usage for security seems practical and efficient. At least for banking applications, the usage of the card is ideal. The card is trusted hardware and provides the security services for its operation. It is probable that an external cryptographic service on the application level is still needed even with a security smart card present, because of the sophistication and cost of smart card based security solutions.

Another major technology that facilitates mobile payment is the expansion of SIM toolkit technology and applications. SIM toolkit was defined by the SMG group within ETSI between 1995 and 1997, and commercial services have since been launched by many cellular operators. Essentially SIM toolkit allows the SIM card to control the handset interface, and provides the user with greater flexibility.

2.3.3 Network

Non-voice services have not achieved great prominence on cellular networks because the networks are poor at providing them. Currently, data speeds have been limited to 9.6kbit/s and/or simple messaging though SMS. Circuit-switched tariffs mean that data services are relatively expensive on cellular compared to fixed equivalents and with most applications users are paying for network resources they do not need as applications transmit data in bursts.

2.3.3.1 GPRS standard for General packet Radio Service

GPRS utilizes packet switching technology where information is transmitted in short bursts of data over an IP-based network. GPRS provides a quick session set up and fast data transmission speeds.

GPRS can use multiple time slots for data transfer as opposed to a normal single time slot. GPRS is ideal for Wireless Application Protocol (WAP) services. WAP over GPRS brings cost savings to both mobile operators and consumers, because GPRS radio resources are only needed while transferring the message. For the end user, that means customer only pays for the time it takes to download. GPRS permit burst transmission speeds of up to 115 bit/s, but in practice only reached 43.2 kbit/s downstream and 14.4 kbit/s upstream.

2.3.3.2 3G

Third generation is the generic term for the next big step in mobile technology development. The formal standard for 3G is the IMT-2000 (International Mobile Telecommunications 2000). This standard has been pushed by the different developer communities: W-CDMA as backed by Ericsson, Nokia and Japanese handset manufactures and CDMA2000 as backed by US vendors Qualcomm and Lucent. UMTS (Universal Mobile Telephone System) is the third generation mobile phone system that will be commercially available form 2003 Europe. Although many people associate UMTS with a speed of 2 Mbit/s but realistic expectations suggest a maximum capacity in metropolitan area s of 384 kbit/s at least until 2005.

It is the move to packet data infrastructure that will provide much of the impetus for mobile payment services. There are two main security concerns in mobile networks:

- Unauthorized access to the network, using stolen or modified handsets
- Eavesdropping on mobile traffic by unauthorized parties.

The security model for cellular networks is straightforward: provide a means of authenticating users to the network and encrypt transmission to prevent eavesdropping. GSM technology employs a SIM to perform much of the security requirements, but other technologies such as Bluetooth are emerging with their own security provisions.

2.3.4 SIM

The SIM provides the most basic level of security in GSM networks. The security functions provided by the SIM include: [3]

- Storing and performing the algorithm used for authentication of the SIM to the network.
- Storing the subscriber authentication key.
- Storing and performing the algorithm used to generate the cipher key.
- Storing the cipher key, which is used to encrypt information transmitted between the handset and the cellular base station.
- Control of access to data stored, and functions performed, in the SIM.

The SIM is at the heart of the security model for the entire network. But network security features are becoming re-usable by non-GSM applications on a transaction basis, as in the WAP Identity Module (WIM). The SIM itself is a tamper-resistant device, but as smart cards in general become more popular, instances of attacks have increased. In response to this, some SIM operating system suppliers are using external agencies to validate security. An example of this is MultOS, which has been assessed at ITSEC level E6. [3]

The approaches to security in mobile payment are driven by the fundamental difference between securing the network and securing applications. Securing a public network is more pertinent to circuit switched voice traffic.

However, securing applications, and more specifically transactions, is more applicable to transmission of data packets, which is what happens during mobile e-commerce. [3]

Cellular networks already provide better security than public fixed networks, because of the greater threat of eavesdropping on radio-based conversations. Data and voice communications over digital cellular networks are encrypted as standard.

However, network security is only mandated (in GSM at least) between handsets and base stations. Importantly, backbone network security is at the discretion of operators. Consequently, mobile e-commerce applications have their own security requirements, over and above basic cellular network provision.

2.3.5 Bluetooth

Bluetooth is a low power radio technology that is being developed to replace the cables and infrared links for distances up to ten meters. Devices such as PCs, printers, mobile phones and PDAs can be linked together to communicate and exchange data via a wireless tranceiver that fits on a single chip.

Bluetooth operates at 2400Mhz and transmits both voice and data at a gross rate of 1Mbit/s.Bluetooth technology enables different devices to communicate with each other without needing to be connected by wires. This will certainly reduce the traffic for network operators from mobile payment transaction over short distance, such as payment for softdrinks at vending machines. [9]

Although mobile commerce(payment) would be possible without Bluetooth, the technology is adding convenience for mobile payment and security.

2.3.6 Mobile payment software.

Due to the fact that the content providers are being faced with supplying content to multiple channels, of which mobile is the latest. Many of them have realized that the new channels are a fact of doing business. For example, the use of access gateway is expected to increase. An access gateway is a computer system that insulated a core business system from the devices and/or networks used to connect to it, handling a wide and increasing array of channels. [3]

In mobile payment, the gateway required sits between the operator network (and servers) and the content provider's system. These system types are new, but they are attracting substantial commercial and investment interest. [3]

2.4 Personal Trusted Devices.

As the nature of the moble terminal is shifting towards Personal Trusted Devices(PTD), this evolution will allow large variety of new services and applications- including mobile E-business, which is also requiring a significant improvement and new capabilities to the mobile terminal platform. Mobile E-business includes new application areas like Mobile Payment, Ticketing and Digital Rights Management. These applications are playing significant role for the future revenue generation for mobile manufactors.

Three fundamental issue needed to be managed before we can expect the mobile payment services to take off.

First of all the mobile phone needs to be trusted from the user perspective. This includes security technologies like algorithms but moreover softer values i.e. user experience needs to be trustedworthy and easy.

Secondly PTD is definately again one output of converging markets and technologies. It's critical that the open standard based technology like WAP and Bluetooth are accepted as a core for mobile payment. And the new_payment architecture and protocols need to be defined to combine the fixed and the mobile world.

Thirdly, terminal security is the fundament to build all this. It's not often directly visible to the end users, added value is somewhat hidden-until the harm is realized.Still,the whole idea of Mobile payment lives (dies) with the security level of the terminal meeting high standard. In the phone architecture security needs to be taken into account as a vital part of the wholeness.

One of the most important issues many mobile manufactory has to face is mobile security – the key prerequisite for successful mobile payment. A full string security must achieve confidentiality (privacy) for both parties, authentication (verifying the identity of all parties), integrity of data sent and non-repudiation of the transaction by either party(precluding denial of a valid transaction). [10]

Many players sees mobile-payment as one of the most promising areas of moible servies, and is thus activaly enhancing the take-off and development of mobile payment services, particularlly in the financial services areana. Apart from completing the payments end in an e-commerce transaction, financial institutions as banks can fulfill many others roles, such as content provision of financial services, or acting as the trusted party for transactions.

2.4.1 Public key infrastructure (PKI)

PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendors' approach and services are emerging. Meanwhile, an Internet standard for PKI is being worked on. [3]

The public key infrastructure assumes the use of *public key cryptography*, which is the most common method on hthe Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret shared private key system has the significant flaw. If the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as *symmetric cryptography* and the public key system as *asymmetric cryptography*.)

A public key infrastructure consists of: [3]

- 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

According to the research work done by Datapro, in a wireless financial transaction, there are five primary areas of security risk: at the device type itself, over the air, at the carriers' gateway, over the Internet, and at the application level. [11]

At the device lever, there needs to be protection from physical_theft of financial dataTypically device security is achieved through the use of password and PIN numbers that are unique to the user. The next protential threat exists over the air: communication can be intercepted as the device transmits to a tower and to a telecommunication carrier's gateway. Security of the communication link is often accomplished through the device's transmission. For example, a WAP device uses the wireless Transport Layer Security (WTLS) protocol for encrytion, while with a Palm device uses the Elliptical Curve Crytography (ECC)protocol. The protocols are decrypted at the gateway and exposed, and then re-encrypted for use over the Internet . Typically, SSL is used for Internet encryption security. Finally, the application itself must be hosted in a secure environment, PKI certificates can also be supported. [11]

On the other hand,wireless security is based on the same foudations as internet security. Wireless transport layer (WTLS) within the Wireless Application Protocl (WAP) provides data integrity and privacy in the same manner as SSL and TLS. Wireless authentication and nonrepudiation are available with the lauch of WAP 1.2 handsets in December 2000 and are based on PKI . [11]

As described before, a public key infrastructure is used in wired networks, like the internet. When using wireless carriers, such as in GSM, GPRS,and 3G,the basic concept is the same but with little distinction. In wireless PKI we must use network agents to overcome the lack of power, CPU performance,memory capacity, and other limitations of mobile stations. Many of the client functions are performed by the agents on behalf of the mobile device. The

GSM system uses encrption between the MS and the BTS already, but the idea of PKI is to offer end to end encryption. [29]

Many companies and organisations develop recommendations, standards and products to build a secure public key infrastructure for the use of banking, finance, information, and other services. Some of these organizations are Radicchio, Mobile Electronic Transaction. Companies like Nokia, Ericsson, Motorola are the members and founders of these organisations. They support the development of wireless PKI. Wireless PKI lacks standards. This is one of the key reasons for the lack of widespread wireless PKI solutions.

2.4.2 Mobile Giant form E-Commerce Security Standard.

On April 12 2001, three of the largest manufacturers of mobile products announced that they have joined forces to develop an open and common industry framework for secure mobile electronic transactions.

The three partners, Nokia, Ericsson, and Motorola, have been working separately to develop e-commerce applications. Nokia is working with BEA Systems to develop a standards basedsolution for building wireless e-commerce application and with IBM to develop enterprise Wireless Application Protocol (WAP). Ericsson is working with 724 Solutions, Inc. to create a moble e-commerce solution based on a common financial services paltform. Motorola announced in January that it would make all its mobile phones Internet-ready by the end of 2000. [7]

The ambition is to form an environment which allows mobile operators, financial institutions and other services providers to facilitate secure mobile transactions.The three companies have already invited representatives from telecom,_financial and IS/IT industries to participate in order to use existing and emerging standards for building a common framework and create an implementation roadmap to enhance the fast adoption of tursted mobile commerce. Their plan is to use existing WAP security functions such as Wireless Transport Layer Security (WTLS) and Wireless Identification Modules (WIM) , wireless Public Key Technologies, and already implemented mobile payment schemes as technology cornerstones for the new initiative. They may face an uphill battle in convining customers to shop in a wireless world, but the consumers may not be willing to pay_for services simply because they are wireless. [7]

However, the mobile device can be a tool for a variety of services, including banking and trading services, credit card and payment services, loyalty/bonus services and ID-card services. By creating a standard for secure mobile transaction opens up possibilities for small transactions, including paying park meters,etc..

For a user, a mobile phone is a highly personal device that today is expected to be easily and securely tailored according to an individual need. These expectations cover also the fast emerging mobile e-business sector. A mobile device will be the platofrm to bridge the virtual and physical world of e-business.

3. FORUMS

3.1 WAP Forum:

The WAP Forum is the industry association comprising over 500 members (including Nokia, Ericsson, and Motorola) that has developed the de-facto world standard for wireless information and telephony services on digital mobile phones and other wireless terminals. The scope for the WAP forum is to define a set of specifications to be used by service applications.[6]

The primary goal of the WAP Forum is to bring together companies from all segments of the wireless Industry value chain to ensure product interoperability and growth of wireless market.

WAP Forum members represent over 90% of the global handset market, carriers with more than 100 million subscribers, leading infrastructure providers, software developers and other organizations providing solutions to the wireless industry.

The Objectives of the WAP Forums are: [6]

- To obtain Internet content and advanced data services to digital cellular phones and other wireless terminals
- To create global wireless protocol specification that will work across differing wireless network technologies
- To enable the creation of content and applications that scale across a very wide range of bearer networks and device types.
- To embrace and extend existing standards and technologies wherever appropriate.

3.2 Mobile Electronic Transaction (MeT):

MeT is standard for Mobile Electronic Transaction which is an initiative started by Ericsson, Motorola and Nokia to establish a framework for secure mobile transactions - the ability to buy goods and services using a mobile device. [13]

The reason why MeT is formed by Nokia, Ericsson and Motorola is due to the introduction of WAP, which has made it possible to access mobile Internet services and undertake mobile e-commerce transactions. One of the key elements is the ability for any phone to operate with any service in this mobile e-commerce environment. This is why Ericsson, Motorola & Nokia have teamed together to create a common industry framework for mobile commerce - the Mobile electronic Transactions initiative.[13]

MeT defines three kinds of Interfaces:[13]
- The service registration interface
- The service execution interface
- User experience aspects of handling secure transactions with PTD

MeT defines and operates in three environments:[13]
- The remote environment, or the Mobile Internet world, by enabling access to WAP shops, WAP banks, etc.
- The physical, or local environment by facilitating payment services in a shop, ID services at work, etc.
- The personal, or home environment by working with Bluetooth technology to access and process internet.

MeT embraces and extends existing industry standards and technology. MeT draws upon WAP for WTLS (Wireless Transport Layer Security), WIM (Wireless Identity Module) and WPKI (Wireless Public Key Infrastructure), MeT also embraces Bluetooth wireless technology.[14]

3.3 Mobey Forum:

The Mobey Forum (pronounced Mo-Bay) is a financial industry-driven forum, the formation of the Mobey Forum was publicly announced by the world-leading financial institutions and mobile manufacturers (Nokia, Ericsson) on May 10th 2000. The mission of the Mobey Forum is to encourage the use of mobile technology in financial services - such as payment, remote banking and brokerage. It aims to do this by: [15]
- Raising the awareness of mobile financial service implementations
- Facilitating the open provisioning of mobile financial services
- Identifying business considerations and working to obtain the interoperability of the technical and security requirements for the mobile finance industry, in order to promote competition
- Acting as an active liaison between various standardization forums in the mobile industry and the financial industry, so as to promote competition.

3.4 Payment standards:

Currently, there are many payment related standards, like SET, 3D-SSL, EMV, and ECML.

3.4.1 Secure Electronic Transaction (SET)

SET is developed by Visa International ,MasterCard International, providing a single technical standard for safeguarding payment card purchases made over open network.

It is primarily designed to ensure the security of electronic transactions over the Internet. The process involves a series of security checks performed using digital certificates, which are issued to participating purchasers, merchants, financial institutions, and payment brands. [16]

3.4.2 3D SET

It is based on an architecture structure known as the three-domain model which uses SET (Secure Electronic Transaction) technology in Europe. It provides a standard secure method of performing transactions over the Internet, allowing for authentication of all parties involved in an online transaction.

In effect, 3D SET is a major evolution of the original distributed structure of SET as the three-domain model continues to use SET as the interoperability protocol. The innate flexibility of the system allows portability from one PC to another, WAP mobile phones and digital TV. [17]

3.4.3 Electronic Commerce modeling Language (ECML) [18]

ECML is standard for electronic commerce modeling language, is a universal format for online checkout form data fields, and was announced in June 1999. ECML provides a simple set of guidelines for web merchants that enable digital wallets from multiple vendors to automate the exchange of information between consumers and merchants. The end-result is more consumers will find shopping on the web to be easy and compelling.

Founding members that comprise the ECML Alliance Steering Committee are: America Online, American Express, Brodia, Compaq, CyberCash, Discover, FSTC, IBM, MasterCard, Microsoft, Novell, SETCo, Sun Microsystems, Trintech and Visa U.S.A.

4. CURRENT MOBILE PAYMENT APPLICATIONS ANALYSIS:

4.1.1 Current market situation of mobile payment:

The earliest mobile payment trials were based on the wide area network used for cellular phones. But the customer had to pay cell phone charges to make a payment, and also had to punch in long sequences of digits each time. Other technologies tested enable less cumbersome procedures. Palm and Verifone will use infrared data transmission for their initial trials. Among the other technologies being used are Bluetooth WiFi, and RF ID, a short-range transmission system. [14] Public key infrastructure PKI encryption - considered to be necessary for secure mobile payment in general - is currently being incorporated into digital wireless networks and into an increasing number of wireless devices, a trend that is likely to increase consumer confidence in mobile payment's security.

Mobile payment has already been used in some areas, including Europe and Asia. In North America, a series of trials are scheduled for late 2001. Commerce Systems, a company based in Kingston, New York, and Nokia jointly developed a cellular phone m-payment system that is being tested in a trial with two United States restaurant chains. One small complication hindering wide-spread acceptance of m-payment is the distinction that credit card companies make between transactions where the card is physically present at the point of sale and those where it is absent - for example, when you use your credit card for transactions over the telephone or your computer's Internet connection. For payments in what are considered "card not present" situations, credit card companies charge the merchant a higher transaction fee. Whether m-payment would qualify as a "card present" situation or not has not yet been determined; that decision may depend on the degree of confidence credit card companies have in the security of m-payment. [19]

4.2 Paybox (Pan-European Mobile Payments)

Paybox is a payment system that uses the mobile phone as an authorization and confirmation device.

The Payment Process :

A Web Paybox transaction operates as follows: [20]

- A user selects a product to purchase on a Web site and opts to pay via Paybox.
- The user enters his/her mobile phone number as a payment identifier, (for users unwilling to disclose their mobile number to merchants, Paybox provides an alternative ID).
- The merchant's system contacts Paybox with the payment request and user ID.

- The Paybox IVR system calls the user's mobile phone and asks the user to enter a PIN.
- The user enters a PIN number to confirm the payment.
- After a few seconds the user receives an SMS message as payment confirmation.

The work flow differs for person-to-person and mobile payments (e.g., to a taxi) but uses similar principles. Information such as caller ID is exploited to enhance security and minimize data entry needs.
Once authorized, Paybox payments are debited from the user's bank account. Paybox consolidates merchant payments and forwards them twice a month.

Payment Security: Banks and merchants have few ways to confirm that a credit or debit card is being used by its real owner, especially in an online environment. Additionally, credit and debit cards are inappropriate for certain forms of payment, such as person-to-person payments, as the recipient does not own the necessary infrastructure. [20]

Trust: Any successful new payment system must be trusted by all participants including consumers, merchants and banks. To enter the European payment systems market by exploiting the ubiquitous mobile phone to enhance the security, trustworthiness and convenience of Web and retailer payments. [20]

Technically, Paybox uses a centralized Envox interactive voice response (IVR) system that uses a voice over IP European backbone provided by KPNQwest. The application code is built and maintained in-house and runs in an Apache/Tomcat environment hosted on Hewlett-Packard servers using an Oracle database. This is a technically complex system that has required more than 50 man years of effort to develop to its current state. [20]

Paybox shows that ubiquitous GSM mobile phones can be used to providing a new payment system which is usable and more secure than credit cards. The Paybox experience also shows that large-scale, high-performance, pan-European mobile applications are feasible, at least when simple technology is used. The biggest challenge that Paybox and its competitors face at this time is convincing European consumers and merchants that they need new payment systems.

4.3 Consumer proposition of successful mobile payment solution:

Convenience and easy to use is the most vital component of any mobile payment solutions.Customers will not take advantage of the mobile payment if the execution of mobile transaction of any variety is not simple and straightforward to complete, and indeed as easy to use as existing alternative methods of payment.

The second important components of mobile payment solution is the speed, by complete the transaction within a reasonable timeframe. For mobile payment the transaction should not take too long.

As a significant driver, the customer also cares about the cost for each mobile payment. If the option to pay for goods or services by a mobile device is overcharged without sufficient benefit, users will not be willing to give up alternative methods of payment.

Customers will demand the financial and personal information generated by mobile payment transaction to be as secure as, if not more secure than, PC-based transactions. Security breaches could destroy the moble payment services market even before it grows.

4.4 Mobile payment challenges

Increasing number of wireless devices, such as Web-enabled mobile telephones and personal digital assistants, has led to many highly enthusiastic predictions about their being the "next big thing" in mobile payment services. Many industry analysis, and certainly vendors of devices and applications, confidently predict massive consumer demand for mobile payment services, which increases in revenue and customer retention following inevitably.

But what is the reality? The reality is at least so far, has been very different. The deployment of wireless mobile payment services for mainstream consumer use remain low, and consumer demand continues to be dramatically poorer than predict.

Mobile payment undoubtedly offers exciting new market opportunities for all associated players. Strategy Analytics predicts that, by 2004, almost 130 million people will be using mobile payment services. However, as with all new technologies and services developments, there are some major challenges lying ahead. There is clearly a long way to go before open standards and technology can be made for mobile payment development. The mobile payment movement will benefit from open standards payment transaction, security system, etc. The struggle of open standards must be continuously traded off against the vested interested of various industry payers like financial institutions, handset and infrastructure vendors, software companies) which are all competing for a slice of the mobile payment pie.

Although there are alreay a number of mobile payment service available, we have yet to see widescale introduction of mobile payment services. The process of converting successful small scale results into a national and internation services will take time and effords

Mobile security is a very important issue, and the security concerns will act as a major obstacle to mobile payment services development.

Perhaps the greatest uncertainty on the whole mobile payment proposition is connected with the cost of the services. Mobile payment services introduces a complex value chain where each player in the chain want to maximize their return. The wireless networks will look for opportunities to secure new revenue streams from mobile payments, mobile operators are looking for the airtime revenue allocation and cash transaction value, the financial institution or electronic cash providers may also seek to secure a percentage of payment fee. The most important is what do the consumer feel about the mobile payment services, if the cost of using the services is too high, they will turn into other methods of payment as mentioned previously.

5. MOBILE PAYMENT SERVICE MARKET OUTLOOK AND FORCASTING

The mobile payment services related market has developed significantly during 2001. Since 1999, the global market was characterized by many trials, conducted in disparate geographical markets, with players experimenting with alternative platform and market solutions.

Although there are still significant uncertainties, the market is being shaped by a number of successful partnerships in each region. These types of partnerships can be categorized into architecture –level partnerships, marketing-level partnerships, and geographic partnerships.[3]

Architecture-level partnerships are the issuers such as the establishment of standards and security solutions, where they are promoting certain applications in the mobile payment market to take off in a short time. For example, Radicchio (a global initiative founded by Sonera SmartTrust, EDS and Gemplus in 1999) is seeking to establish secure transactions over mobile payment services. [3]

Market-level partnerships is aimed at marketing mobile-payment applications and services, like Forums.

Geographic partnerships exist between the operators, banks, content providers, system vendors, and others to trail and launch mobile payment services within a given geographic market.

5.1 Mobile Operators

In order to support revenues and market growth, operators have to find new revenue streams, due to the fact that their core voice market is becoming a commodity. This means that content and transaction services will be much more important.

Mobile payment services can offer new revenues, new customers to the operators, but the challenger like technology is still immaturing (SIM toolkit,GPRS,3G, WAP, Bluetooth). Also mobile has been built on voice, but mobile payment services are data related services which are outside of operator's experience. In order to the success in mobile payment market, the mobile operator may have to be partner, or even merge with retail banks, to capitalize on their 3G investment. In such scenario, as relatively easy takeover targets, would be advantaged in being inside of the new payment system, instead of on the outside. Furthermore, mobile operators could assume the

role played by the credit card firms, as network software is said to detect fraud more quickly that credit card networks, while providing real-time details on spending [23].

Partnership between banks and collaboration between mobile operators and banks will be the way forward. Making mobile payment will require a great role from both sides but getting them together is a key. In fact the subscriber which mobile operator has is far beyond the banks, their combination will be a big push to Mobile payment. But the problem relays if the security of trisection went wrong, who is responsible? [24]

The major risk for mobile operator is that they could not get a key position of mobile payment services. Which means they can only get less fee on data and voice transfers. So how to position themselve with the banks and serveices providers is a key issue.

5.2 Banks and credit card firms

According to Durlacher research, Mobile payment serivces will attract 800 million users by 2004, the ability of consumers to use pre-pay or credit accounts for mobile purchases, implies a massive displacement for banks[26].

The banks who will facilitate mobile transaction will go on for the next three to five years. However if they are not rapid adopters in this field they will be losing a lot of customers to mobile operators. Some banks are now trying to solely take control of the channels for mobile payment services to make themselves mobile payment market drivers. Banks are also now very actively promoting and investigating mobile payment, mobile operator may have an early advantage, but banks are also drafting plans for mobile payment services [25]

5.3 Technology Vendors

Many mobile network provides have launched mobile portal during 1999. Mobile portal provided by a technology vendor is basically used to gather contact that can help in selling WAP gateway, WAP handsets and so forth.

Ercisson has developed Mobile payment platform which provides a secure solution for operators and services providers to launch their own, revenue-earning mobile payment services. An important feature of the Mobile Commerce Platform is that it enables charging for both site contacts as well as goods and services purchased over the Mobile Internet. Mobile Commerce platform Security functions range from simple password verification to sophisticated wireless public key infrastructure (WPKI).[27]

Nokia's payment solution enables payment service providers to mediate payment between three main parties of mobile payment:financial institutes, merchanets and consumers. Nokia payment solution is a network independent, server based solution supporting web access and WAP 1.1 and 1.2 specifications. [28]

So the technology vendors strategy is to focus where the money is made in mobile payment , and which could be the control point. Since they have a unique position in providing mobile payment enabling terminal and networks. Their aim is to also expand these advantages to the mobile payment secor.

6. CONCLUSION

The core of mobile payment is the use of a terminal (mobile phone, PDA) and public mobile network to conduct a transactions which result in the transfer of value in exchange for information, services or goods. Mobile payment is essentially a subset of the wider electronic payment market, but refers specially to those transactions that are carried out from a mobile terminal.

Mobile payment is enabled by a variety of emerging technologies, many of which are still immature. The key technologies including WAP, bluetooth, Network (GSM, GPRS, 3G), mobile payment software, smart card and SIM. A variety of Forums have been founded to promote the development of mobile payment services

Many software and hardware vendors, mobile operators and banks are betting that mobile payment services will be big business. But the market development for mobile payment services is currently at a very early stage, it looks like that it is more promise than an achievement with mobile payment.

Also the uncertainty levels of mobile payment services are high, particularly as the development depends on the actions of a wide group of players. The level of consumer adoption is uncertain, user's willingness to adopt and pay for new wireless services is unproven.

As an essential corner stone of mobile payment services, the security must be the first priority for developing mobile payment related solutions. But until now, the security issue is still not high lighted due to the rush to the market.

Since they are numerous technology (like GSM, SMS,GPRS,Bluetooth), standards, forums available for mobile payment, the stardardization of technologies is a key issue for mobile payment market taken off. Therefore companies must form partner-ship or co-operate with each other in order to be part with the busines.

It 's really hard to predict what will happen with mobile payment in a long term since so many uncerterties exists. But one thing is for ture, the market opportunity for mobile payment related solutions is tremendous.

7. REFERENCES:

1) E-commerce from wired to wireless, 2000 Ovum Ltd.

2) Wireless Financial Services: Perspective. Datapro research Gartner.

3)Mobile E-commerce: Market structure, 2000 Ovum Ltd.

4) Secure Mobile Commerce, Mobile Commerce Strategies Report Vol.1 No7 YANKEE Group.

5)Trust In Transaction Security Is First Priority
http://www.epaynews.com/index.cgi?survey=&keywords=mobile%20payment&optional=&subject=&location=&ref=keyword&f=view&id=10002116152121201505O&block=3

6) WAP Forum homepage
URL: www.wapforum.org

7)"WAP 2.0 Technical White Paper", WAP forum,
URL: http://www.wapforum.com/what/WAPWhite_Paper1.pdf

8)"Wireless Application Protocol Architecture Specification" WAP-210-WAPArch-20010712-a,
URL: http://www.wapforum.com/what/technical.htm

9) Bluetooth homepage
URL www.bluetooth.org

10) "Met PTD Security Requirements", Met
URL: http://mobiletransaction.org"

11) Wireless Financial Services :perspective. Datapro research, Gartner Ltd.

12) "Ericsson, Motorola and Nokia team to develop a common framework for mobile e-business",
Nokia Press release 11.4.2001.
URL:http://www.northgate.nokia.com/nokia/common/nokiamet.nsf/document/OU04T4P9R46?OpenDocument

13) "Met Core Specification", Met URL: http://www.mobiletransaction.org"

14) "Met Account-Based Payment version 2, 21 February 2001,
Met URL: http://mobiletransaction.org"

15) "The Preferred Payment Architecture Technical Document" version 1.0.

Lissa Kanniainen,Mobey Forum/LK

16) SET homepage
RUL: http://www.setco.org/faq_usr.html

17) VISA Intonation homepage.
URL: http://visaeu.com/virtual_visa/merchants/faqs.html#3

18) ECML homepage
URL: http://www.ecml.org.

19) Building an E-Commerce Trust Infrastructure." Verisign communication Ltd.
URL: http://www.verisign.com/rsc/gd/pmt/ecomm-tech/

20) Gartner research Paybox: Pan-European Mobile Payments 18 September 2001 Nick Jones

21) Sonera Homepage
RUL: http://www.sonera.fi/english/solutions/mobilepay/services/

22) "Mobile Commerce Report" Falk Muller-Veerse, Durlacher Research Ltd.
URL: http://www.durlacher.com

23) Bank 'Now investigating mobile payments' epaynews.com Aug 09 2001

24) Carriers may even merge with bank epaynews.com Apr 27 2001

25) " Europe 'Biggest Market For 3G mCommerce" epaynews.com Sep 11 2001

RUL:http://www.epaynews.com/index.cgi?survey=&keywords=mobile%20payment&optional=&subject=&location=&ref=keyword&f=view&id=1000211615212120150 50&block=3

26)Mobile Commerce Report Durlacher Reseach Ltd.
RUL: http://www.durlacher.com

27)Ericsson Press Releases Ericsson launches Mobile Commerce Platform - enables charging for Mobile Internet services

28) "Nokia Payment Solution enables mobile e-commerce services with multiple payment methods and enhanced security", Nokia press release

29)Radicchio. Wireless PKI:Fundamentals, 2000
RUL: http://www.radicchio.org/download/SMD-002.PDF