Mobey Forum White Paper on Mobile Financial Services (v. 1.1)

Mobey Forum Mobile Financial Services Ltd

Disclaimer:

This document is subject to change without notice.

http://www.mobeyforum.org/

Table of Contents

1. Scope

This document constitutes a white paper on the principal requirements of Mobey Forum on mobile financial services. In this document, the security requirements and technical aspects of mobile financial services are discussed. Furthermore, current and emerging mobile technologies are evaluated together with Mobey Forum requirements. Mobile financial services cover mobile banking services, mobile local payments, mobile remote payments and mobile trust services such as identification and authentication.

The main goal of the document is to give advice and information for the financial industry on how they can start offering mobile services for the customers. The document also has a purpose to communicate to other industries banks’ main requirements on mobile financial services and how financial industry sees the near future development.

2. Document Status

2.1 Version History

Version	Date	Task Force or Working Group	Description
1.0	06-06-2003	Mobey Forum Business WG	First version
1.1	15-09-2004	Mobey Forum Business WG	Version 1.1. Partly revised structure. Editorial changes through the document, Significant content updates in 6.4 Trust Services.

2.2 Errata

3. References

Mobey Forum Preferred Payment Architecture 1.0	http://www.mobeyforum.org
Mobey Forum Preferred Payment Architecture for Local Payments 1.0	http://www.mobeyforum.org
MeT Ltd White Paper on Mobile Transactions	http://www.mobiletransaction.org

4. Introduction

4.1 Background

In June 2001, Mobey Forum released an extensive documentation, the Preferred Payment Architecture 1.0 (PPA1.0), in which the financial industry's consolidated requirements on mobile financial services were stated for the first time. On the basis of these requirements, the documentation proposed an architectural model and a technical solution that would best satisfy the needs of all parties. The technical solution was based on dual chip phones, server wallets and selected secure interoperability domains (e.g. 3D Secure). This solution clearly fulfilled the Mobey Forum's requirements better than any other solution that was then evaluated.

During 2001 and 2002 various Mobey Forum members piloted easy-to-use and secure solutions according to the PPA1.0 with excellent results. The focus in pilots was on deploying banks' back-end wPKI infrastructures and using dual chip phones to access financial services. Mobey Forum members have jointly created a remote payment and banking solution implementation reference to which they have had access since September 2002. Further work in the area of the local payments has resulted in a more in-depth documentation that includes a potential migration path to a future solution. Local payment document was published in September 2002 and was supported by demonstrations of point-of-sale payments and ATM withdrawals at Mobile Commerce World Europe in 2002. Mobey Forum members Nordea and Nokia piloted local payments with real consumers and merchants in Finland in 2003-2004 in co-operation with Visa.

To summarise, Mobey Forum has successfully documented and demonstrated a technical infrastructure capable of operating both in remote and local environments. More detailed information about previous documentation, pilots and demonstrators is available at http://www.mobeyforum.org.

4.2 Vision

The vision of the Mobey Forum is that the mobile device will become a universal platform with which people will manage their financial issues (e.g. accounts, brokerage, etc.), make purchases in local[1] and remote[2] environments and secure authentication to various services.

In order to achieve the vision, Mobey Forum encourages the use of mobile technologies in financial services. Mobey Forum facilitates this through a consolidation of business and security requirements, evaluation of potential business models and technical solutions, and by making recommendations to standardisation bodies, handset manufacturers, payment schemes, network operators, regulators and technology suppliers in order to speed up the implementation of solutions.

[1] In local payments a consumer and a merchant are in the same location, and the proximity radio technologies, such as RF-ID, Bluetooth or infrared, are used for data transfer.

[2] In remote payments, transactions are conducted over telecommunication networks, such as GSM, and they can be made independently from a consumer's location

5. Consolidated Requirements of Mobey Forum

Mobey Forum requirements for mobile financial services are valid still today and they are shortly stated in this chapter. Mobey Forum has set the requirements for mobile financial services in order to:

1. Communicate both the general prerequisites for successful mobile financial service initiatives and specifically the needs of financial institutions in the m-commerce arena to different parties, such as telecom operators, standardisation organisations, handset manufacturers, other technology suppliers and regulators.
2. Evaluate how different technologies match the requirements.
3. Enhance and boost the habit formation in using mobile financial services.

The requirements are divided into four principal categories: *customer proposition, business priorities, technical issues* and *implementation issues*.

5.1 Customer Proposition

The user experience should be convenient
Financial services have to be *easy-to-use*, *fast-to-use* and they have to *offer value for money*.

The consumer should have the freedom to choose bank, operator and handset, and change them independently of each other
All three are reissued or renewed in varying cycles. Changing any one of these should not influence or be dependent on the others.

Mobile financial services should have wide acceptance and usability
The solution should support multiple payment products that can be used in a wide variety of shops. A mobile payment product that can be used only in a very limited number of shops will never reach mass market but will remain just a niche solution.

The customer habit should be built by starting early and gradually improving and expanding the services
The habit of using mobile financial services has to be formed within the user by starting service provisioning with today's technologies and exploiting new technologies as they emerge. Once consumers begin to see their mobile phone as their wallet, providing access to their trusted and accepted payment methods, the introduction of new concepts and services is much easier.

Technical and perceived security level should be high
The customer has to be protected against fraud and hacking attempts in payments. Customers have to be sure that the payment destination is genuine in order to avoid suffering financial lose. Services have to offer confidence that personal details will not be disclosed to any unauthorised party. The security level and convenient use should match with the risk level of the service.

5.2 Business Priorities

Banks authenticate their customers while providing banking and payment services
Effective customer authentication is the most important element in facilitating mobile payments. The architectural solution must leave the level of security in authentication open for the issuer to mandate. With payment services, the institution liable for the payment, usually the issuing bank, will always be responsible for authenticating the user. The issuer of

payment products has to be in control of his customer's authentication in order to be able to manage the corresponding risk. Strong user authentication can be based, for example, on certificates and wireless PKI (Public Key Infrastructure). In macro payments and transactional banking services, strong authentication is required. In micro payments, MSISDN based authentication and PINs (Personal Identification Numbers) can be used.

The service proposition has to offer value for all the relevant parties
In the area of m-commerce there are various players who all have to approve some common rules in order for m-commerce to take off. Banks, telecom operators, handset suppliers, merchants and consumers have to all benefit from the solution that is chosen. For example, merchant acceptance is vital for any payment solution to be well received. All in all, the solution has to offer an attractive business case for all concerned parties.

Business processes of different players have to remain independent of each other
It is not feasible for a bank to limit the service to its customers having a certain mobile phone service provider. Further, it is preferable that banks do not have to enter into bilateral agreements with all the operators acting in the same markets as the bank. This problem is emphasised within banks operating in many markets around the world. Logistics may also add costs and make the process for the consumer more complicated, especially if the consumer has to visit many places or register to several companies to get services working.

The solution has to scale across all financial service opportunities
Not every mobile financial service scenario will necessarily be suited to a single generic architecture, but the solution needs to be flexible so that all types of financial services can be accommodated. Furthermore, inter-bank usage has to be guaranteed by some means.

Branding has to also be available within mobile environments
The potential to add brand is important in terms of acceptance by all parties in the value chain. For instance, payment card issuers, and credit associations view branding as vital to any proposition. The solution must allow visible branding of payment products (either on a plastic card or in some digital form within the phone) to be managed by individual institutions.

5.3 Technical Issues

Open and non-proprietary technologies have to be used
Solutions have to be based on open standards that do not require expensive license fees to be paid. The handsets and servers should work seamlessly together through standard interfaces between different manufacturers, and all service providers should be able to enter markets smoothly.

Existing standards and solutions should be used, where possible
The existing infrastructure has to be utilised as much as possible starting from what is possible today, according to stated requirements, and enlarging the scope of services with time. This applies to existing and emerging banking and payment technologies, such as the existing electronic banking services offering, and to the emerging standards for the transaction processing, such as the EMV standard, 3D Secure and SPA. In the Payer's architecture, solutions must also be based on existing standards, such as SMS, WAP and open development platforms such as Java™ and Symbian. Additionally, merchant integration into existing systems must be addressed.

Technological solutions have to enable independence between banks, operators and mobile phones
The banking relationship, operator relationship and type of handset should be independent of each other. Any walled-garden solutions must be avoided, primarily because they prohibit fast mass-market adoption. Handset independence means that the banking relationship must not be affected if the end user changes handset. The end user must be able to take the 'Security Element' from the handset with reasonable ease and move it to another handset or to easily re-enrol to authentication service provider (the bank) when the handset is changed.

End-to-end security (message integrity & confidentiality), secure authentication, and non-repudiation have to be guaranteed
Transaction level security is essential in financial services. Information transferred between mobile terminals and merchants' and banks' systems has to be encrypted. Both the consumer and the merchant have to be, in most cases, authenticated. The proposed architecture must include bank and merchant protection against customers disputing mobile transactions.

5.4 Implementation Issues

Implementation costs to banks, merchants and consumers have to be relatively low
The costs of implementing and running the services have to be relatively low. *Costs for a bank* consist of setting up a security infrastructure such as PKI (if this is the preferred security solution), maintaining it, distributing security credentials to consumers and maintaining customer support. However, these costs are rarely mobile specific as banks have to have this kind of infrastructure place also for other electronic channels. *Costs for a merchant* consist of setting up the solution and running it. In local payment environments, in many cases a merchant has to purchase or upgrade POS (point of sale) terminal to make it capable of reading the payment product information via proximity radio technology (e.g. RFID, Bluetooth). *Consumer's total cost* consists of purchasing a mobile device and other possible required equipment, and transaction and service specific costs. Different parties also have to see an attractive business case in the short-term.

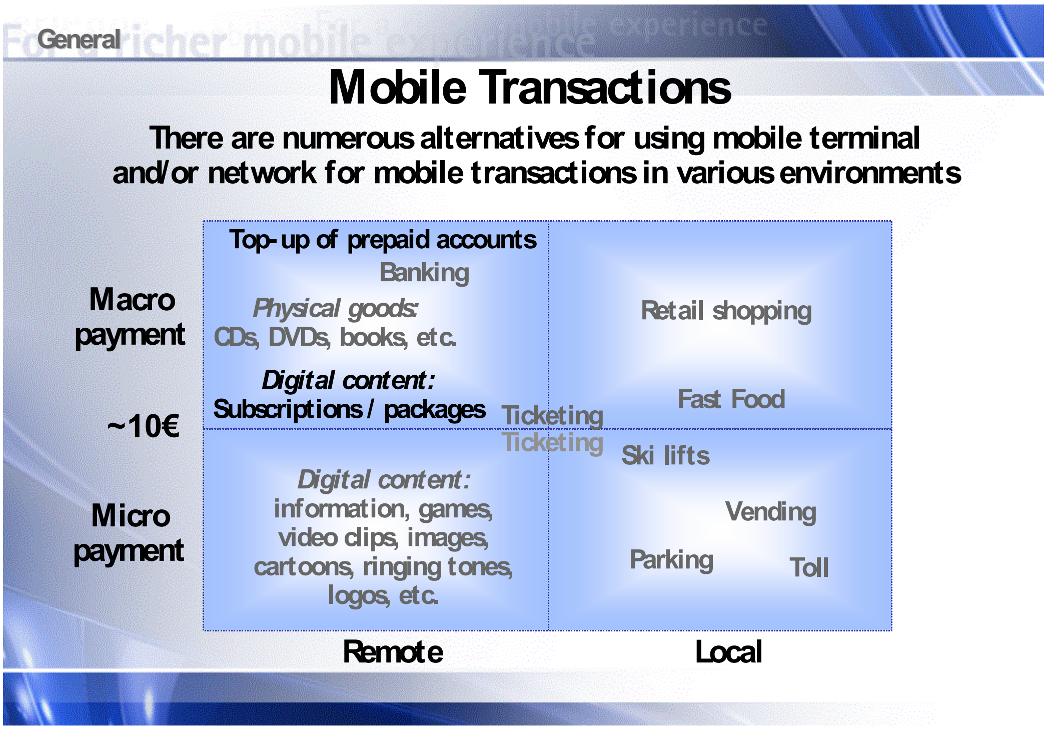
Time-to-market is of critical importance
The most important time-to-market factor is availability of existing solutions, such as suitable handsets, security applications and infrastructures, as required for a particular service.

6. Development of the Mobile Financial Service Landscape

In this chapter, mobile financial services are discussed. The focus is on introducing and evaluating existing and emerging technologies that enable the introduction of new or enhanced mobile financial services today. Analysis and conclusions provided by MeT (formed by the leading mobile phone manufacturers) about the mobile payment environment have been utilised in this chapter. [MeT White Paper, Ch.3, References]

Mobile phones can be utilised for different kinds of remote and local payment transactions, banking services and trust services.

Figure 1 depicts payment transactions divided into micro- and macro payments – an approximate value of 10 € is seen as the dividing line – and lists examples of products and services that are typically associated with each quadrant. [MeT]



General

Mobile Transactions

There are numerous alternatives for using mobile terminal and/or network for mobile transactions in various environments

	Remote	Local
Macro payment	Top-up of prepaid accounts Banking *Physical goods:* CDs, DVDs, books, etc. *Digital content:* Subscriptions / packages	Retail shopping Fast Food
~10€	Ticketing	Ticketing
Micro payment	*Digital content:* information, games, video clips, images, cartoons, ringing tones, logos, etc.	Ski lifts Vending Parking Toll

Figure 1. The mobile payment landscape [Source: MeT White Paper, 2003]

6.1 Remote Payments

Remote mobile transactions span from the purchase of ringing tones and logos sent to the mobile phone (often using SMS as the billing and transportation mechanism), to purchasing goods, services and content during a browsing session with online mobile merchant sites. SMS services constitute a majority of the remote mobile transactions today, but the availability of new browsing and Java technologies, and packet radio services ("always-on connection") have facilitated the fast development of purchasing and content downloading transactions over the mobile Internet. [MeT]

A big part of global payment transactions are card-based: a realistic and flexible entry-level solution for card-based remote mobile payment transactions is needed. Mobey Forum believes that virtual cards residing in a phone's memory (mobile wallet) or in a security element supported by the phone will be an important implementation step to make the user experience convenient and secure. In the future, there is a need to define how the mobile device of the consumer will handle multiple virtual cards issued by different parties and how these cards are managed throughout their lifecycle by the card management systems of issuers. These questions apply both to remote and local payments.

It is realistic to expect that bank-issued payment products that are and will be used in fixed Internet channel will be used also in large-scale in mobile channel. Technically speaking fixed Internet and mobile Internet channels are coming closer to each other as same protocol stacks (TCP/IP) are utilized. Banks can easily expand online payment products to cover mobile channel with similar or higher security level than in fixed Internet.

6.1.1 Payment Credential Provisioning

It is of key importance to make information input as simple and easy for the customer as possible when she is giving card number and other information needed to make the transaction. The keypad on many mobile phones is not optimal for typing lots of alphanumerical characters. Manual fill-in of information may become a barrier for a transaction if consumer has to enter even some tens of characters, and therefore automatic form fill-in is an important issue in mobile environment in order to enable fast, easy and convenient user experience.

The mobile wallet is an application in the mobile phone visualising the transaction capability in the phone – based on the metaphor of a wallet as the place to store cards, tokens, tickets, receipts and reminder notes. The mobile wallet offers trusted storage, a trusted user interface and a consistent user experience for the consumer. A wallet application in the phone supports remote and local transactions. The wallet can work autonomously or can assist other elements such as server wallets in remote transactions. Applications, virtual cards, data or links to remote functionality can be stored in the wallet. The consumer can easily retrieve data necessary for a transaction from the wallet with the help of concepts such as ECML form fill - whereby information stored in the wallet is tagged and can populate an electronic form with the click of a few buttons. The functionality in the wallet is secured by wallet security mechanisms (e.g. a PIN number). It is also possible to access security modules (such as a WIM) from wallet applications. [MeT]

6.1.2 Market Expectations on Remote Mobile Payments

Mobile remote micro payments started with the introduction of value-added SMS services such as downloadable ringtones. Global ringtone sales is expected to top 4 Billion USD in 2004 according to Strategy Analytics, and will be growing fast, due to the introduction of new personalisation elements and digital content consumed via the mobile phone.

Some of the digital content consumption involves bigger transactions (subscriptions, service packages, more complex applications). Thus, there are expectations for growth in remote macro payments. This growth will be substantially higher if topping up prepaid accounts for mobile services predominates, thereby utilising mobile phones instead of scratch cards.

6.1.3 Example Use Case: Remote Purchases at a Wireless Site

A consumer can make purchases while browsing on the wireless Internet by using a mobile device as the payment instrument. Internet-enabled handsets are assumed to have a bank-issued Security Element. There is an underlying trust infrastructure covering merchant, acquirer, issuer and user. After selecting the purchase item, the user selects the payment method, and confirms the transaction details by entering a PIN-code (which is processed by the Security Element). The user receives a receipt and a notification of a successful transaction. The product is distributed through the agreed channel.

6.2 Local Payments

Local mobile transactions represent a tremendous opportunity for the use of mobile phones as ultimate digital wallets. Local mobile transactions based on different concepts have already been piloted in different parts of the world, and the encouraging results pave a way for an exciting future. [MeT]

The key requirements for local transactions are usability and reliability. The operation should complete quickly, with very few or no keystrokes at all, and in a reliable manner. Implementations of local transaction capability in mobile phones should take into account the existing transaction handling systems and, in many cases, find the optimal way to adapt to them. Due to the wildly differing circumstances for different local transaction environments, both advanced and entry-level mobile local transaction concepts need to be implemented. The security solutions for local transactions should scale to different classes of transaction value. [MeT]

More detailed analysis about local payments can be found from the Mobey Forum document Preferred Payment Architecture for Local Payments.

6.2.1 Use of RFID and Bluetooth in Local Payments

RFID implementations in mobile phones have started with separate RFID modules being attached to mobile phones without an interface to the phone electronics. These implementations are currently being used in pilots and early commercial cases. In the next generation of implementations, however, contactless modules will also have access to phone resources, which will enable innovative combinations of remote and local services and the possibility of storing multiple virtual payment cards in the phone. It will take some time, however, for the potential of this combined concept to be fully exploited. The development of remote and local service combinations will most probably follow the usual high tech market entry patterns: pilots followed by vertical early implementations leading to full consumer adoption over time. [MeT]

The Near Field Communication (NFC) Forum is a global standards development and advocacy group dedicated to advancing near field communication technology, educating the public about its benefits, and furthering its implementation around the world. The vision of the NFC Forum is to enable users of any handheld electronic device to access content and services in an intuitive way by simply touching smart objects and connecting devices just by holding them next to each other. Evolving from a combination of contactless identification (RFID) and interconnection technologies, NFC technology bridges today’s connectivity gap.

Mobey Forum sees that NFC Forum has a great potential to make significant progress in the area of proximity communication and embraces their efforts. More information of NFC Forum can be found at http://www.nfcforum.org.

Bluetooth also has the potential to be used for local transactions in which the bi-directional transfer of large amounts of data is required. Time-critical transactions cannot yet be performed with Bluetooth as session set-up time is too slow.

6.2.2 EMV in Mobile Environment

In the area of mobile payments based on bank-issued international payment cards, mobile EMV is seen as a possible future concept, especially in local payment areas. EMV is a set of internationally agreed standards for chip payment cards, originally agreed by MasterCard

Europe and Visa. A few fundamental requirements for mobile EMV need to be met, however, for implementations to make any sense. Specifically,

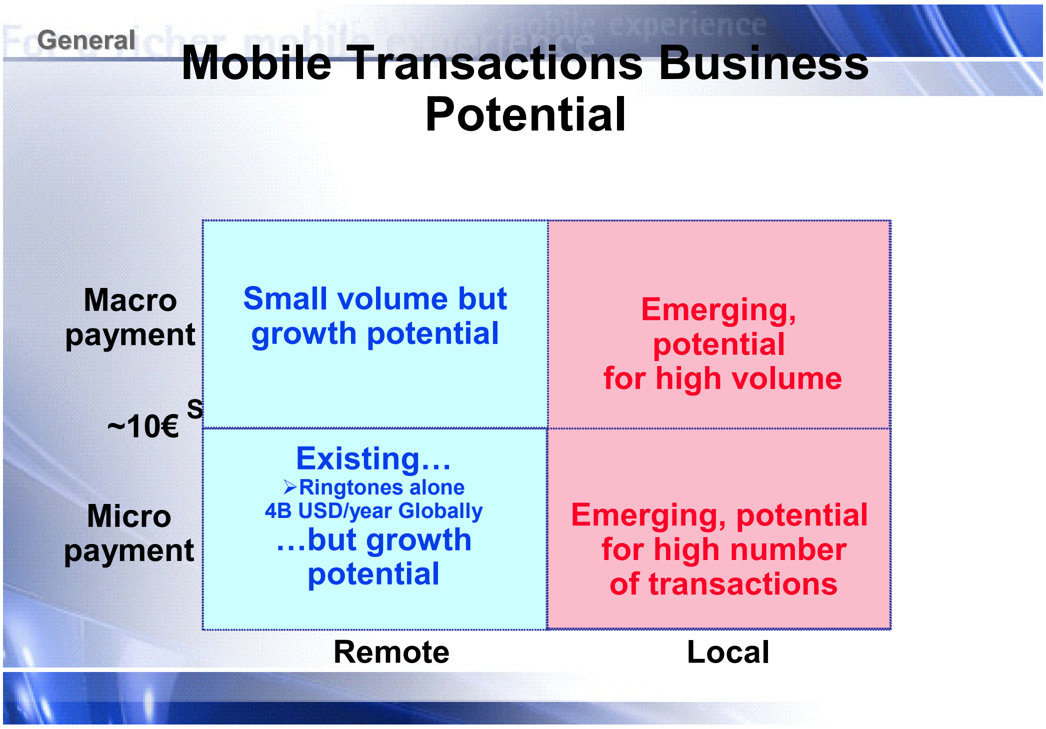
- There needs to be substantiated global demand for the concept
- The existing EMV specifications need to be further developed to take into account the special requirements of mobile devices
  - The role of the mobile device needs to be clarified
  - All protocols between EMV cards, mobile devices and POS devices need to be defined
  - Mobile device security and PIN entry requirements and rules need to be realistically assessed
- Potential device certification needs to be based on self-certification by device manufacturers

Mobey Forum is interested in solving these open issues concerning the mobile EMV concept in dialogue with all the parties managing the specifications and the roll-out of EMV technology.

6.2.3 Market Expectations on Local Payments

The local mobile payment area is in the phase of rapid development. Pilots and early implementations suggest a substantial growth potential for local micro payment transactions (e.g. ticketing) whereas the use of a mobile phone for local macro payments may require a longer lead-time.

Figure 2 depicts the growth expectations of the four quadrants of mobile remote/local micro/macro payments.



General

Mobile Transactions Business Potential

	Remote	Local
Macro payment	Small volume but growth potential	Emerging, potential for high volume
~10€ S		
Micro payment	Existing… ➢Ringtones alone 4B USD/year Globally …but growth potential	Emerging, potential for high number of transactions

Figure 2. Mobile transactions business potential [MeT]

6.2.4 Example Use Case: Vending

Mobile devices with a local payment application, such as a magnetic stripe image, an EMV application or a purse on a contactless RFID card, can be used for buying a drink from a vending machine. The vending machines are equipped with a RFID reader that is able to read the payment card information. The consumer selects the drink, and pays for it by bringing the mobile device close to the vending machine's RFID reader. The drink is delivered to the consumer together with a receipt, if it is required. A PIN may be used to authorise the order.

6.3 Mobile Banking Services

People need to manage their financial affairs independently of place and time. Mobile phones are the optimal platform for this purpose. Currently many banks are offering most of the services they offer via Internet channel also through the mobile channel. Banking services are among the most used WAP-services in many markets, as it provides clear value for the user. Also, SMS-based services, such as account balance and latest transactions request, have been deployed successfully in various markets.

The mobile channel will be a complementary channel to the Internet while enabling various services that cannot be offered with current technologies through existing channels to become available. For instance, the mobile channel will bring brokerage to a new service level. Consumers can set up triggers, and get alerts when stocks achieve a certain level or when some significant piece of news is published whenever and wherever they are. This high service level cannot be achieved through any other channel. In time critical services, the mobile channel is better than any other alternative.

Existing and emerging mobile technologies, such as enhanced browsing technologies, enhanced graphical capabilities of mobile devices, fast packet networks, Java™ MIDP, TCP/IP, etc., enable banks to improve the usability and security level of mobile banking services. These technologies, and others, are discussed later in this document.

6.3.1 Example Use Case: Balance Inquiry and the Five Latest Transactions

Within the balance and transactions inquiry service the customer can ask for the actual balance of an account, and details of the last transactions made. It is a simple service in which the customer takes the initiative and asks for the information. The natural technologies that could be utilised in this use case are SMS, and WAP. User experience is quite different between these technologies.

6.3.2 Example Use Case: Stock Trading

With this service, the customer is expected to have a trading profile with the issuing bank. By means of this profile and customer-set-triggers the customer will receive updates and alerts relating to the current market situation and to his portfolio, profile of stocks or funds etc. SMS and MMS technologies used together with WAP are suitable in this service.

6.3.3 Market Expectations on Mobile Banking Services

Developments in mobile technologies, and the increased use of delivering financial documentation, such as bills and salary information, through electronic channels, have a huge market potential for mobile banking services. The development of mobile technologies will increase the usability and security of mobile banking services, whereas the expanded range of banks' electronic services will allow bills, salaries and other financial information to be distributed directly to the consumer's handset. Already today, people in various markets manage their banking issues mainly through the Internet channel. It is fair to expect that the number of active mobile Internet service users and the number of mobile banking users will be about the same among the customer segment of economically active consumers. Thus, the success of mobile banking services is heavily influenced by the general success of mobile Internet services.

6.4 Mobile Trust Services

Different aspects of security are often divided to confidentiality, integrity, nonrepudiation and authentication. By confidentiality it is meant that encrypted secrets are not available to unauthorized users. Integrity is often referred as message authentication. Non-repudiation techniques ensure that nobody can repudiate or deny sending or receiving the message. Authentication techniques are used to make sure that messages are from the genuine origin.

Mobile trust services enable secure user identification, authentication and making a digital signature. Authentication is needed when customers access mobile banking services, make payments or access 3rd party services, which are utilizing bank's authentication services. Digital signature is used to guarantee non-repudiation of a transaction or a message.

6.4.1 Authentication

Username-password mechanisms, one-time passwords as well as other entry-level authentication mechanisms are being used for present mobile financial services. For services requiring a higher level of security and non-repudiation, in particular, security elements supporting digital signatures (WIM[3]) have been introduced. Key dimensions for security solutions are ease-of-use, the security level attained and the cost of the solution. Ease-of use directly affects the consumer adoption of the security solution whereas costs associated with the solution forms a critical component in the business case for its implementation. For some services (e.g. mobile banking) the security level requirements are largely set by the nature of the services themselves and cannot be downgraded. It is challenging to be able to develop easy-to-use authentication mechanisms that offer a good balance between cost and security level attained. [MeT]

There are various options that banks can use for authenticating the end user. These vary by security level and usability in every channel through which banks serve their customers. For instance, MSISDN (with/without bank controlled PIN), and digital signatures using a shared secret or mobile PKI, can be used as authentication mechanisms. Also, methods used with Internet banking, e.g. tokens and one-time passwords, can be used, but the usability of them is often poorer as they are not integrated in the mobile device.

The keys and PINs involved in signing functions must be stored in a trusted environment. These environments should be tamper proof and not accessible by non-authorised users or applications so that they can be used in financial services requiring the highest level of security. The actual algorithms used for these functions are not the subjects of Mobey Forum's preferred architecture.

6.4.2 Security Element

The storage of security credentials has the continued attention of Mobey Forum. Mobey Forum keeps evaluating new technologies suitable for Secure Elements that may include the use of both software and hardware based solutions and combinations of these.

[3] The earlier WAP Forum (currently OMA – Open Mobile Alliance) has standardised digital signature capability for security modules such as smart cards. This is called the WIM concept. [MeT]

Many banks require that the storage and processing of private keys and other credentials is based on tamper-proof hardware based Security Element. Furthermore, the environment of the Security Element has to be proven secure. Security Elements can be, for example, integrated components in the mobile device, such as Secure Memory Cards[4], SIM-card based solutions or some other dedicated hardware components. It is important to remember that in every case the interface towards the Security Element has to be non-proprietary and based on open standards.

Open software model refers to security elements installed on top of the open phone operating environment such as Java™ MIDP or Symbian. Having tamper-proof hardware based component with crypto processing software accessible from the open software environment of the phone is one of the most promising solutions to meet the financial industry's requirements and to reach wide market reach. **It is crucial that business independence and customers' freedom to choose and change bank, MNO or handset will be guaranteed, no matter what is the chosen technology to implement it.**

[4] Secure Memory Card (SMC) is a memory card including a smart card (a chip), and smart card controller features.

7. Review to Interesting Existing and Emerging Mobile Technologies

Significant changes are happening in the mobile telephony landscape. More and more mobile phones are equipped with large colour displays enabling an intuitive graphical user interface. "Always on" data communications technology such as GPRS, a new generation of mobile browsers and an open application environment (Symbian, Java™ MIDP) for mobile phone applications are being developed by the vast global developer community. These fundamental technologies form the basis for the implementation of mobile transactions and banking capabilities. Their effect is being dramatically enhanced by concepts described in this chapter. [MeT]

Guaranteeing sufficient customer privacy is important for banks. One of the key aspects to these technologies is how much control a bank needs over a certain technology to be able to consider it as secure enough for transactions. Here, legal and regulatory requirements play an important role.

7.1 SMS

SMS can ideally be used for information services such as balance inquiries and different types of alerts. SMS is a compelling service due to the fact that there is an extensive user habit created already. Also, almost all phones today support sending and receiving SMS messages. However, the aspect of user experience and convenience must be carefully watched.

For banks, starting with the SMS-based alert and information services easily creates within the user the habit of using mobile financial services. The next natural steps are personalised and time-critical alerts with important content to which the user can react.

Security of SMS has not been a major concern although SMS alerts are stored in a mobile and if the mobile is stolen, a third person will have access to that information and to information sent afterwards, as long as the mobile is on. Also, the unreliability of SMS services can mean that a mission critical short message may never arrive and the sender may not be aware of this. This "send and forget" is not acceptable to banking services – so, for example, confirmation of delivery should be considered as a minimum requirement or only low value transactions should be allowed with SMS.

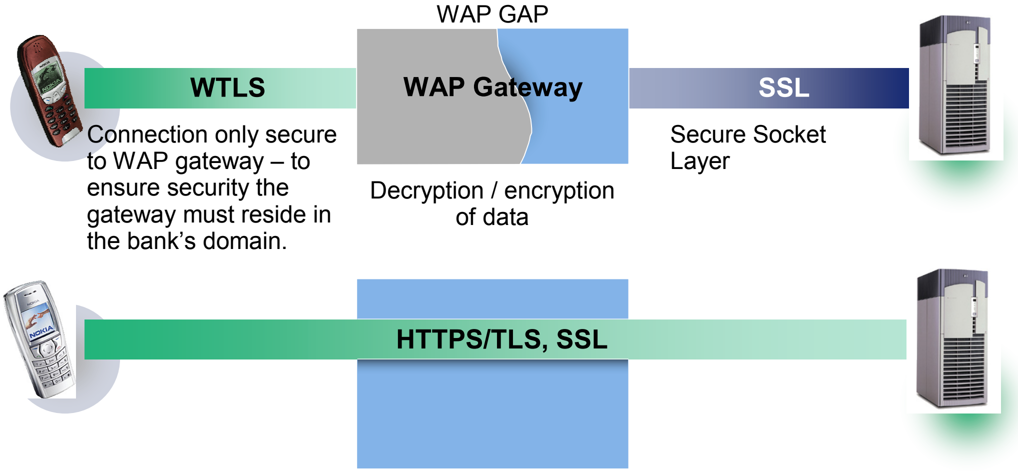
7.2 Evolution in Browsing Experience

WAP is the interface technology that allows users with mobile phones or other wireless devices to access and interact with Internet- and Intranet-based services and information. Browsing in WAP 1.0 was optimised for the limited capabilities of mobile phones such as small black and white displays, lack of processing power and slow transmission speeds. The services were only occasionally designed to be intuitive or easy to use. As a result, the expectations and promises of a "mobile Internet" were not fulfilled in the first round of mobile data services.

However, due to the introduction of new types of (2.5G) phones and of more capable networks, this picture is changing. The new developments offer completely new kinds of approaches to the role of the mobile phone as a part of the banks' presence and visibility and thus can affect the mind share and emerging user habits of consumers. The browsing experience will be enhanced by the speed of GPRS networks, and xHTML browsers offering optimised views to the content. The overall browsing experience is already enriched by large colour displays with frames, text styles, fonts, and graphics.

7.3 Security in WAP 1.0 and WAP 2.0 over TCP/IP

The security problem in WAP 1.0 occurred in the gateway. The end-to-end confidentiality was compromised in the session change from 1) mobile phone to gateway and then 2) onwards to the origin server unless the gateway was in the bank's domain. With TCP/IP and WAP 2.0 a secure connection between applications providing end-to-end security can be implemented. With WAP 2.0 and TCP/IP connections the need for banks to have their own gateway will disappear, as this is no longer an issue with TLS tunnelling able to be used to ensure end-to-end confidentiality. However, to support legacy phones in WAP banking, it is a necessity still to have a gateway for these services at the bank's premises i.e. within the secure domain. TCP/IP phones were launched to the markets in 2003 and most new phone models have the TCP/IP support available.



Connection only secure to WAP gateway – to ensure security the gateway must reside in the bank's domain.

Security is comparable to the Internet model – confidentiality to the origin server can be secured.

Figure 3, Security benefits from TCP/IP

7.4 Banking Services and Applications Distribution through Java™ MIDP

Java™ – with its MIDP (Mobile Information Device Profile) - forms an important open application platform relevant to all mobile devices across a wide range of mobile phone models. As the specifications for the Java™ environment in mobile phones evolve in the future, it is important that there is a direct access to all relevant security module implementations from the Java™ environment in mobile phones. [MeT]

For banks, Java™ MIDlets enable an opportunity to reach mobile consumers in a visually pleasing and easy way. Also, branding can be done in a much more attractive way. The MIDlets can be downloaded OTA (over-the-air) in a WAP session. One of the aspects of Java™ services is that from a Java™ MIDlet it is possible to use an http connection. So, two-way services are becoming possible just as in a browsing situation. However, lack of TLS support in MIDP 1.0 limits the use of it in financial applications. Although some limitations still exist in file sizes and security aspects of the MIDP 1.0 environment, this landscape is changing for the better. The second version, Java™ MIDP2.0, will improve the usability and security of MIDlets. For example, https is supported in Java MIDP2.0. Improved security together with increased variety of functionalities will enable many new opportunities for banks to develop new mobile financial services. For the banks, the MIDlets will play an important role in the range from thick to thin clients.

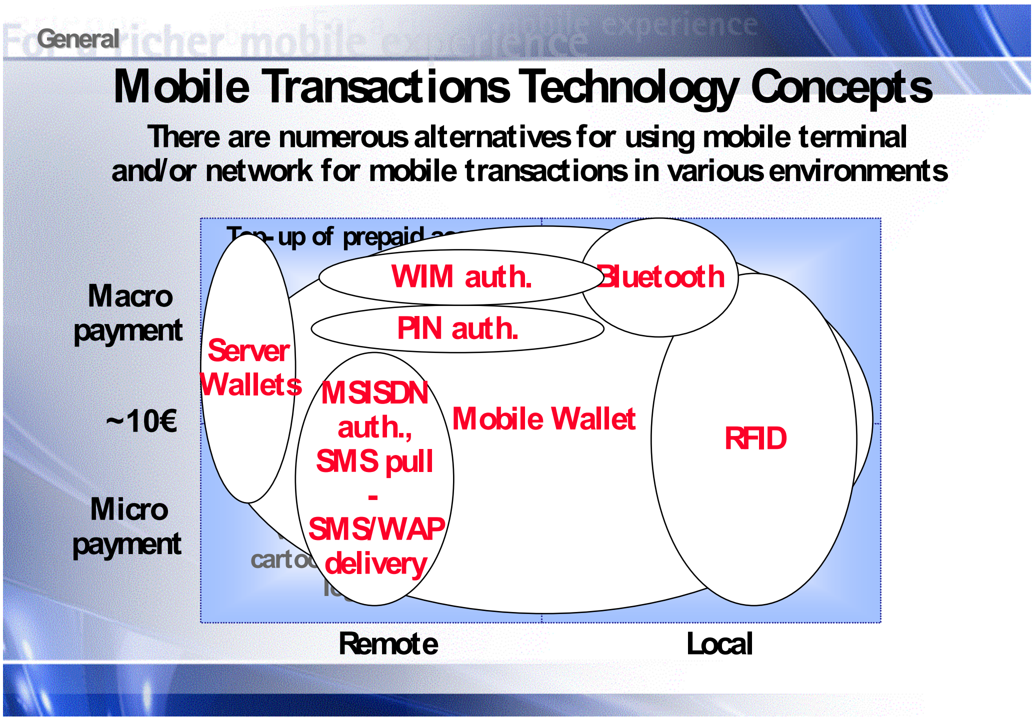
A Java™ MIDlets, especially in combination with secure elements can be used for storage of the keys, algorithms and applications. Thus, the security aspects of the Java™ environment will be important for banks. The mobile Java™ environment must offer a certain level of protection against Trojan horses and viruses to secure the mobile financial environment on the mobile device.

There are operator and handset vendor owned proprietary versions of Java™ MIDP in the market, which have to be taken into account when implementing solutions based on this technology. Furthermore, some functions of the Java™ MIDP standard are not mandatory and may differ manufacturer by manufacturer.

7.5 Enrolment OTA

The term **over-the-air provisioning (OTA)** describes the ability to download and install content over a wireless network, typically on demand. For mobile client applications to succeed, the entire lifecycle of the applications must be properly managed, and the phases must be painless from both the customers' and the financial institutions' view points. From the mobile customer's perspective, OTA is simply a matter of finding an interesting application (i.e. financial services) on the Web (i.e. eBanking Web service) and initiating its download over the wireless network. However, in financial applications the consumer has to be totally confident about the source of the download. MIDP 2.0 will support the signing of the applications (MIDlets), which will increase the security of downloading a piece of software.

7.6 Combination of Technology Concepts



General

Mobile Transactions Technology Concepts

There are numerous alternatives for using mobile terminal and/or network for mobile transactions in various environments

Figure 4. Mobile transactions technology concepts [MeT]

Figure 4 shows the typical areas of use for some of the key mobile transaction technologies. Currently, mobile digital content is predominantly being paid for by operator billing, i.e. ordered by SMS and delivered via SMS or WAP downloads. Server wallets are being introduced especially for remote macro payments. PIN-based or equivalent authentication is being utilised in mobile banking transactions. The use of WIM is being piloted for high security environments. In the emerging local transactions space, RFID-based solutions concentrate on high-speed, high- throughput environments (public transport, fast food), whereas Bluetooth pilots are being introduced in the local macro payment area for implementations involving the transformation of the transactions process. [MeT]

8. Conclusions

Mobey Forum stated its requirements for mobile financial services in its Preferred Payment Architecture 1.0 document, published in 2001. Despite the significant changes in the technical and business environments since that time, the requirements are still valid. Service provisioning by banks, operators and terminal manufacturers have to be independent from each other. Banks manage the authentication in their banking and payment services. Open and non-proprietary standards are to be supported. Easy-to-use and fast-to-use services that offer value for money are the key success factors to wide-scale customer acceptance in mobile financial service area.

The financial institutions are interested in catering for all values of mobile payments, ranging from micro to macro, whenever there is a business case on a specific market. The authentication solution selected by the issuer bank naturally depends on other risk management options in use in addition to the value of the payment. The Mobey Forum sees that average sizes of mobile transactions are rapidly increasing. This means, so to say, that a micro today is macro tomorrow.

The Mobey Forum thinks that the basis of co-operation between the financial industry and the mobile operators should be open business models and the business requirements that the Mobey Forum has set out in the Preferred Payment Architecture documentation (PPA).

By utilising current mobile technologies, significant improvements can be made to banks' service offerings. For instance, Internet banking services can be complemented with SMS/MMS alerts, and new convenient-to-use mobile financial services can be introduced with enhanced browser technologies and Java™ MIDP applications. Matching high security and high usability with low costs remains a challenge. Open software based solutions combined with hardware secure elements are expected to meet this challenge in the near future. Pure software based security solutions are available today and they offer various benefits, such as low cost and large numbers of compatible handsets already in the market.

Market demand for remote payments is increasing rapidly and technologies are mature for introduction of banks' online payment schemes into mobile channel. Content providers have excellent tools for marketing and selling different kinds of content through mobile Internet or dedicated applications and banks' online payment products should be supported in these solutions. Mobey Forum encourages banks and merchants to start cooperation to realize the full potential of m-commerce in near future.

9. Terminology

For explanations on some of the terminology used in this white paper, please refer to the Mobey Forum PPA1.0 document. Also the MeT document MeT Terminology Version 2.2 is recommended.