



## **The Preferred Payment Architecture Business Document**

### ***Requirements for manufacturers and standardisation bodies***

**Version 1.0**

**Approved by the Mobey BoD on  
25.06.2001**

**Editor: Liisa Kanninen  
Workgroup Executive, Mobey Forum**

#### **Legal Notice**

This document is designed to provide a general overview of Mobile Payment Architecture. It is released and delivered with the understanding that the recommendations and opinions in this document shall not be regarded as legally binding opinions or recommendations. In addition no country specific regulation is included in this document. Readers are advised to review this information and check the country specific or payment system specific rules separately. No legal responsibility will be accepted by Mobey Forum Mobile Financial Services Limited (the Mobey Forum) or by the authors for the opinions appearing in this document.

The copyright of all matter and content appearing in this document is reserved by Mobey Forum Mobile Financial Services Limited. No matter contained herein may be reproduced, duplicated or copied without the prior consent of Mobey Forum Mobile Financial Services Limited.

# Table of Contents

<b><u>1</u></b>	<b><u>INTRODUCTION</u></b>	<b>3</b>
1.1	<u>SCOPE AND BACKGROUND</u>	3
<b><u>2</u></b>	<b><u>PAYMENT OPPORTUNITIES</u></b>	<b>4</b>
2.1	<u>INTRODUCTION</u>	4
2.2	<u>REMOTE PURCHASE @ WIRELESS SITES</u>	4
2.2.1	<u>The User Experience with a dual chip solution</u>	5
2.2.2	<u>The User Experience with a dual slot solution</u>	5
2.3	<u>FACE TO FACE SHOPPING</u>	5
2.3.1	<u>The User Experience with a dual chip solution</u>	6
2.3.2	<u>The User Experience with a dual slot solution</u>	6
2.4	<u>VENDING (E.G. CONFECTIONARY)</u>	6
2.4.1	<u>The User Experience with a dual chip solution</u>	7
2.4.2	<u>The User Experience with a dual slot solution</u>	7
2.5	<u>VOICE MOTO SHOPPING</u>	7
2.5.1	<u>The User Experience with a dual chip solution</u>	8
2.5.2	<u>The User Experience with a dual slot solution</u>	8
2.6	<u>ADDITIONAL PAYMENT OPPORTUNITIES</u>	8
2.6.1	<u>Vending (petrol)</u>	9
2.6.2	<u>Event Ticketing</u>	9
2.6.3	<u>Mobile Person-to-Person (P2P) Payments</u>	10
2.6.4	<u>Public Transport Ticketing</u>	10
2.6.5	<u>Continuous Payments (e.g., online news articles)</u>	11
2.6.6	<u>Cash Download</u>	11
2.6.7	<u>Transport (taxi – mobile to mobile merchant)</u>	12
<b><u>3</u></b>	<b><u>CONSOLIDATED REQUIREMENTS OF MOBEY BANKS</u></b>	<b>13</b>
3.1	<u>INTRODUCTION AND SCOPE</u>	13
3.2	<u>HEADLINE BUSINESS PRIORITIES</u>	14
3.3	<u>CUSTOMER PROPOSITION</u>	14
3.3.1	<u>Convenience</u>	14
3.3.2	<u>Security</u>	15
3.3.3	<u>Privacy</u>	16
3.4	<u>BUSINESS PRIORITIES OF BANKS AND MERCHANTS</u>	16
3.4.1	<u>Security</u>	16
3.4.2	<u>Versatility</u>	16
3.4.3	<u>Acceptance by all parties</u>	16
3.5	<u>TECHNICAL CONSIDERATIONS</u>	17
3.5.1	<u>Independence of operators and open standards as key requirements of Mobey banks</u>	18
3.5.2	<u>Use of existing standards</u>	18
3.6	<u>IMPLEMENTATION ISSUES</u>	18
3.6.1	<u>Cost factors</u>	19
3.6.2	<u>Speed to market</u>	19

# 1 Introduction

## 1.1 Scope and Background

The mobile handset is likely to become a payment device. There is a danger that this will happen in a dis-intermediated way, which would not be beneficial for customers or banks and intermediaries. A “worst case scenario” would be the issuance of multiple standards for mobile payments, therefore prohibiting the widespread take-off of the mobile commerce industry.

The objective of the Mobey Forum is to enhance the use of mobile technology in financial services, such as banking, payments and brokerage. The Mobey Forum’s method to achieve this are through creating business and technical requirements, evaluating potential business models and technical solutions, and by making recommendations to standardisation bodies, handset manufacturers, payment schemes, network operators and technology suppliers to implement the required solutions.

The Mobey preferred payment architecture is evaluated in this paper mainly from a business perspective. First, the payment opportunities are studied and the user experience described using different concepts. Then the consolidated requirements of the Mobey banks for the preferred payment architecture are explained in detail. The technical analysis of the handset implementation alternatives and the payee’s payment models can be found in Mobey Forum’s Technical documentation.

The target audience for this document are members of standardisation bodies, such as the WAP Forum, along with handset and middleware manufacturers, financial services providers and other companies interested in mobile commerce. It is suggested, that this document is read in connection with the Mobey Executive Summary document and the Technical document. All conclusions, based on both Business and Technical documents are summarised in the Executive Summary document.

The scope of this document is to align the Mobey Forum consolidated view on the business aspects of mobile payments for a mass-market solution and to set forth the joint requirements of Mobey banks for a preferred solution that fulfils these requirements.

As background for this document, the Mobey Forum workgroups have evaluated various payment opportunities in terms of potential mobile payment scenarios. These are explained in Chapter 2 and it is plain to see that there are several opportunities for banks, as service providers, to offer mobile services to their customers. The four most important scenarios are explained more thoroughly, giving the reader a picture of the likely differences in user experiences with the different technical solutions (dual chip, dual slot).

The Mobey Business workgroup has created and consolidated financial institutions’ common business criteria for mobile payments. It has also addressed the requirements related to the mobile trust solution. The consolidated requirements of the Mobey banks, consisting of Customer proposition, Business priorities, Technical considerations and Implementation issues, are expressed in Chapter 3.

The payment protocols evaluated may apply to a range of devices but for simplicity we refer only to mobile phones throughout this document.

## 2 Payment Opportunities

### 2.1 Introduction

The purpose of this Chapter is to identify and define the customer experience for all possible opportunities in making a payment using a mobile device. Thus its focus is purely on identifying the user experience – important related issues such as possible business requirements per scenario, relevant security levels, technical / architectural considerations etc. will be discussed in the following sections or in the Technical documentation. Furthermore, if a specific technical solution is assumed for a scenario, it does not mean that it would be the preferred one for Mobey Forum or that other solutions would not be considered when implementing the service.

As stated elsewhere within this document, the Mobey Forum recognises that there are two major categories of consumer payment opportunities: local and remote. It is the purpose of this chapter to examine in more depth and leverage the likely different user experiences from four most important scenarios, covering each major payment type. The Mobey Forum has identified altogether eleven separate opportunities, all of which are unique and differ from other examples in some way. All of them will be listed within this chapter. The payment opportunities are handled in the order of importance for the Mobey banks.

There are several principal underlying assumptions, some of which are considered pre-requisites for mobile payments and are assumed to be necessary in every scenario:

- Brands are ever-present – i.e., bank brands, payment scheme brands, etc., will always be utilised where and when the payment process requires them. Brand elements may be presented either as traditionally on a plastic card or digitally in the phone.
- No time frames for the mass-market implementation of the scenarios has been defined or recommended. Timetables are expected to vary from country to country.
- Knowledge and possession are separated (user is required to input a PIN-code to access the security element every time a transaction is done, excluding micro payments).

The four most important scenarios will be studied from the perspective to leverage the likely differences in user experience in the dual chip and dual slot scenarios. Since operator-independency is one of the key requirements (see Chapter 4) of Mobey banks, it is assumed here, that both of these concepts are made with an operator-independent technical construction, i.e., the other card, be it smartcard chip sized or credit card sized, is totally independent of the SIM card. The current existing dual slot implementations, made with SIM Application Toolkit, would thus not be acceptable for these scenarios.

### 2.2 Remote purchase @ wireless sites

This scenario describes the situation whereby the handset can be used as a payment instrument for transactions once the user, while browsing the wireless Internet, has decided to make a purchase. It is assumed, that the user holds a wireless Internet enabled handset equipped with a bank-managed payment method. The payment method is not stored value (which is covered under another scenario). There is an underlying trust infrastructure covering merchant, acquirer, issuer and user such as a three-domain model. The Merchant is a WAP / wireless Internet-enabled merchant.

### *2.2.1 The User Experience with a dual chip solution*

1. Users surfing over the wireless Internet using their handset find an article they want to buy.
2. The user then selects the payment method available both with the merchant and the payment card inside the phone.
3. The user confirms the details of the transaction with a PIN code, (which is processed by the additional chip).
4. The user receives notification that the transaction has been successful (or otherwise) and proof of both the financial and commercial side of the transaction (i.e., a receipt or equivalent from both the issuer and the merchant is available to the user).
5. User gets access to the required article.

### *2.2.2 The User Experience with a dual slot solution*

1. Users surfing over the wireless Internet using their handset find an article they want to buy.
2. The user then selects the payment method available with the merchant.
3. The user goes to find his (physical) wallet, takes out the selected card product and inserts it into the slot in the handset.
4. The user confirms the details of the transaction with a PIN code, which is processed by the payment card in the second slot.
5. The user receives notification that the transaction has been successful (or otherwise) and proof of both the financial and commercial side of the transaction (i.e., a receipt or equivalent from both the issuer and the merchant is available to the user).
6. User gets access to the required article.
7. User takes the payment card out of the slot and stores it back in their (physical) wallet.

## 2.3 Face to Face Shopping

This description is of one model of face-to-face mobile shopping.

The user has a handset equipped with:

- Two chip readers (internal or external), one reader for SIM-card and one for a bank issued multi-application chip card.
- Bank-managed chip card with EMV-debit/credit or an equivalent payment application, merchant's loyalty application and ticketing or parking application.
- Payment capable handset software.
- Local communications link between the merchant system and the handset.
- Access to secure interoperability domain payment infrastructure supporting mobile commerce (details to be defined).

The merchant could be a chain of stores or a single shopkeeper on the high street equipped with:

- A wireless connection enabled POS-terminal and an 'offering' program
- Secure payment software supporting mobile commerce (to be defined)
- EMV-upgraded or similar smart card based POS-software.

### *2.3.1 The User Experience with a dual chip solution*

1. The customer enters the shop with their handset switched on.
2. The customer fills their basket with items, which are counted at the checkout counter as usual (including any items selected from the 'offering' program that has sent special offers to the handset).
3. The customer chooses the mobile payment method once the sales clerk informs the customer of the total sum of all purchases.
4. A wireless session is activated between the phone and the POS-terminal. The customer receives the total sum and a notification of the accepted payment methods from the POS-terminal on their mobile device.
5. If the customer has more than one application on their bank card (credit/debit) they will be asked to choose the one which they prefer to use from the selection of the merchant's accepted payment methods.
6. The customer chooses the payment application and keys in their PIN for confirmation.
7. The customer receives the confirmation message after authentication by the POS-terminal and receives relevant receipts or permitted access to them. The transaction is now completed.

### *2.3.2 The User Experience with a dual slot solution*

1. The customer enters the shop.
2. The customer fills their basket as normal.
3. The customer chooses the mobile payment method once the sales clerk informs them of the total sum of all purchases.
4. A wireless session is activated between the phone and the POS-terminal. The customer receives the total sum and a notification of the accepted payment methods from the POS-terminal on their mobile device.
5. The customer will be asked to choose which payment method they prefer to use from the selection of the merchant's accepted payment methods.
6. The customer chooses the payment application.
7. The customer takes their (physical) wallet, pulls out their preferred card and inserts it into the slot in the mobile phone and keys in their PIN for confirmation.
8. The customer receives the confirmation message after authentication by the POS-terminal and receives relevant receipts or access to them. The transaction is now completed.
9. The customer can now, or whenever they like, take the card out from the slot in the mobile, store it back in their (physical) wallet and continue packing the goods.

In this scenario the user experience differs, not only by the fact that the user has to insert the card into the phone when making the payment and to take it away after the transaction (in the dual slot solution), but the service offered is different due to the fact that it can not be assumed that the user has the payment card inserted into the phone throughout. Therefore, loyalty services and the interactive shopping experience cannot be provided in the dual slot solution. Furthermore, it can be concluded that using a dual slot phone in local face-to-face shopping environment doesn't add any value either to the end user or to the merchant. Usage of dual slot phones in face-to-face situations for payments is thus by no means suggested or preferred by Mobey Forum.

## 2.4 Vending (e.g., confectionary)

This scenario describes one possible situation how the mobile phone can be used as payment instrument for transactions with vending machines where the amount to be paid is determined before the actual payment. Usually the amount is also relatively small.

Customers use a handset equipped with two chip readers (internal or external), one reader for SIM-card and one for bank issued chip card. The mobile phone is also loaded with the required software.

The merchant is the owner or the responsible party for the vending machine. The merchant is assumed to have a 'Mobile WAP shop' enabled vending machine. One alternative is to perform the payment described here with a local connection (over, for example, Bluetooth); the following example(s) do not intend to suggest any specific payment technology but rather to describe the payment opportunity and one possible user experience related to it.

#### *2.4.1 The User Experience with a dual chip solution*

1. A customer wants to buy a drink from a vending machine. On a sticker on the vending machine is a web-address and a number of the machine (or a phone number).
2. The user keys this into their handset.
3. The user is then asked to input the number of the vending machine and then the number of the drink (or select an item from a scroll list).
4. When informed of the amount due, the user selects the payment method available on his payment card in the phone and enters his PIN for confirmation of the transaction.
5. The drink is released and the user receives a confirmation on their phone.

#### *2.4.2 The User Experience with a dual slot solution*

1. A customer wants to buy a drink from a vending machine. On a sticker on the vending machine is a web-address and a number of the machine (or a phone number).
2. The user keys this into their handset.
3. The user is then asked to input the number of the vending machine and then the number of the drink (or select an item from a scroll list).
4. When informed of the amount due, the user selects the payment method offered by the merchant.
5. The customer then opens their (physical) wallet, takes out the selected payment card and inserts it into the slot in the phone and enters their PIN for confirmation of the transaction.
6. The drink is released and the user receives a confirmation on their phone.
7. The user takes out the payment card and stores it back in their (physical) wallet.

## 2.5 Voice MOTO Shopping

This scenario was selected for closer study because it was considered to differ dramatically from the other scenarios and offer a new important usage opportunity. This scenario describes one model for voice shopping with mail order/telephone order (MoTo). The customer is shopping for goods or services by using a wireless device. This scenario can be amended to include, for example, shopping via a PC; other models may exist as well, but they are not described here.

The customer is a handset and credit card holder. It is assumed, that the customer holds:

- Two chip readers (internal or external), one reader for SIM-card and one for bank issued chip card.

- Payment capable handset software.
- A bank-issued chip card application.

The merchant is a retail or mail order shopkeeper and has secure payment software supporting mobile commerce. In this case it is also assumed, that the merchant has messaging capabilities.

#### *2.5.1 The User Experience with a dual chip solution*

1. The customer is browsing through a (paper) mail order catalogue, sees an advert and decides to make a purchase.
2. They complete the mail order form (including their mobile phone number) and selects "mobile" as the payment method and sends the form by mail to the merchant OR telephones the requested number and voice-fills out the form including the mobile phone number.
3. As soon as the merchant has processed the order, the customer receives a message (e.g., by SMS or WAP Push) with the goods' details, price and payment methods accepted by the merchant.
4. The client selects a payment method from what is offered and also available on their payment card in the phone, inserts a PIN-code to confirm the payment (processed off-line) and submits the payment back to the merchant.
5. The customer then receives a message confirming the payment (or information that it has been refused). Receipts will also be made available to the customer.

#### *2.5.2 The User Experience with a dual slot solution*

1. The customer is browsing through a (paper) mail order catalogue, sees an advert and decides to make a purchase.
2. They complete the mail order form (including their mobile phone number) and selects "mobile" as the payment method and sends the form by mail to the merchant OR telephones the relevant number and voice-fills out the form including the mobile phone number.
3. As soon as the merchant has processed the order, the customer receives a message (e.g., by SMS or WAP Push) with the goods' details, price and payment methods accepted by the merchant.
4. The customer then opens their (physical) wallet, pulls out the selected payment card, and inserts it into the slot in the phone.
5. The customer enters the PIN-code to confirm the payment (processed off-line) and submits the payment back to the merchant.
6. The customer receives a message confirming the payment (or information that it has been refused). Receipts will also be made available to the customer.
7. The customer can now, or whenever they like, take the payment card out from the phone and store it back in their (physical) wallet.

## 2.6 Additional Payment Opportunities

### *2.6.1 Vending (petrol)*

This scenario describes one possible situation in which the mobile phone can be used as a payment instrument for transactions with vending machines where the amount to be paid is NOT determined before the actual payment. Here, petrol vending is used as an example.

A Customer uses a handset equipped with two chip readers (internal or external), one reader for SIM-card and one for bank issued chip card. The mobile phone has the required software already loaded.

The merchant is the owner or responsible party for the vending machine. The merchant is assumed to have a 'Mobile WAP shop' enabled Vending machine. One alternative is to perform the payment described here with a local connection (for example, over Bluetooth); the following example does not intend to suggest any specific payment technology but rather to describe the payment opportunity and one possible user experience related to it.

#### The User Experience can be described as follows:

1. A customer wants to purchase fuel for their car and stops at the petrol station. Naturally, they want to pay fast and not wait in a queue. On a sticker on the petrol pump is a web-address (or a phone number) and a number of the petrol pump (the number is specific for each kind of petrol).
2. The user keys in this web address. The user is asked for the number of the petrol pump followed by the maximum amount the user wants to pay or an option to fill up.
3. The user now inserts a banking card in his/her mobile phone or uses the internal payment card, and enters their PIN to confirm the transaction.
4. The user then fills up their car to the maximum amount and is informed either on the pump itself, or through the website of the transaction's completion.
5. The user receives a confirmation of the amount on his phone. Legal receipts are stored on the servers.

### *2.6.2 Event Ticketing*

This description is one simple-to-implement model of mobile handset based event ticketing.

Customer uses a handset equipped with:

- Two chip readers (internal or external), one reader for SIM-card and one for bank issued chip card.
- Bank-managed security element is compliant with EMV debit/credit or similar smart card payment application and a ticketing application.
- Ticketing and payment capable handset software.
- Wireless connection between the merchant system and the handset, e.g., Bluetooth.

The issuer is the ticket-issuing organisation in this case. The issuer has a WAP shop selling tickets with secure payment software supporting mobile commerce (details to be defined). The venue has a wireless connection enabled ticket gate/printer/collector.

#### The User Experience can be described as follows:

1. The user follows steps 1-4 in the remote payment scenario (2.2) and purchases an event ticket.
2. The ticket is downloaded and can be stored on the handset or a multi-application security element containing the ticketing application.
3. The user arrives at the venue. There are a number of ticket gates that the user can select and go through. The customer approaches one gate and activates their handset. The handset may request a PIN code to allow access to tickets.
4. The user accepts redeeming the ticket once prompted by the gate and the gate opens.

5. After the ticket has been used, it is moved in the handset into a place for used tickets. There it cannot be used, but is available for inspection purposes.

### *2.6.3 Mobile Person-to-Person (P2P) Payments*

The P2P scenario is broadly to enable consumers to pay anyone using their mobile device to the other party's PC or mobile device in a secure manner without having to disclose any sensitive account information.

Customer uses a handset equipped with:

- Two chip readers (internal or external), one reader for SIM-card and one for bank issued chip card.
- Payment capable handset software.

The User Experience is as follows:

1. The person logs on to their virtual payment service by authenticating themselves by typing in their PIN.
2. The user enters a phone number or e-mail address of the person to whom they want to pay and enters the amount of money to be paid.
3. The user confirms the payment details.
4. The user receives a message stating whether the transaction was successful or not.

### *2.6.4 Public Transport Ticketing*

This scenario description is one simple-to-implement model of mobile handset based ticketing, where the user chooses to purchase a ticket either locally (e.g., in an agency) or while browsing the wireless Internet.

Customer uses a handset equipped with:

- Two chip readers (internal or external), one reader for SIM-card and one for bank issued chip card.
- A bank-managed Security Element (SE) with EMV debit/credit or similar smart card payment application and a ticketing application
- Ticketing and payment capable handset software
- Wireless connection between the merchant system and the handset

The issuer is a ticket-issuing organisation in this scenario. The issuer has a WAP or retail shop selling tickets with secure payment software supporting mobile commerce.

Transport facility could be an airline, train or bus, check-in desk. The transport facility has a connectionless card enabled ticket gate/collector.

The User Experience is as follows:

1. The user selects the appropriate ticket at the retail ticket shop or on a ticket vendor's wireless site and pays for the ticket (please refer to face to face, remote payment @ wireless sites or voice MOTO user scenarios).
2. The user receives a notification that the ticket has been downloaded onto the mobile handset and stored on the bank-issued SE with the ticketing application.
3. The user enters the train. The user approaches the ticket collection device and either brings the handset close to it or activates the ticketing function in the handset by pressing a button.
4. The ticketing transaction takes place between the handset and the ticket collection device over a wireless interface.

5. The customer receives notification on the handset display that a ticket has been validated and information such as number of remaining tickets etc.
6. The gatekeeper / conductor gets a confirmation message and let's the customer through.

### *2.6.5 Continuous Payments (e.g. online news articles)*

This scenario describes one possible situation where the mobile phone can be used as a payment instrument for small transactions of a continuous nature, e.g., online gambling, reading news articles and gaming.

Customer uses an ordinary mobile phone with an online purse application for micro payments.

The merchant is an owner or explicator of a WAP site and has a 'Mobile WAP shop' with a micro payment account.

The user Experience can be described as follows:

1. A user is looking for news with on their WAP phone. After logging in to the (first) newspaper site, and before opening the first article, the user is requested to choose the way to pay.
2. The user chooses "online micropay". The online purse of the user, which knows a maximum amount, is automatically opened based as, for example, the CLI (Caller Line Identification - the phone number of the client) is already known. This is known as lightweight authentication.
3. The user is now informed of the amount they have in their micro payment purse and is asked how much money they want to pay (to maximum) on this site.
4. Every time a user now opens an article, the user is requested to confirm the payment. If the preset amount is reached or the purse is empty, the user is notified, in the latter case with a question if they would like to reload the purse.

N.B. In order to save transaction costs, the merchant may receive the aggregated payments at the end of the day as a whole from the involved banks.

### *2.6.6 Cash Download*

This scenario describes one possible situation where cash can be downloaded with a mobile phone. One new aspect being grasped here is that the download transaction, from a user perspective, occurs during another transaction.

The customer uses a handset equipped with:

- Two chip readers (internal or external), one reader for SIM-card and one for bank issued chip card.
- E-purse application on the bank's chip card
- Payment capable handset software

The merchant is store chain or single shopkeeper.

The user experience is as follows:

1. The user initiates a face-to-face transaction and follows steps 1-4 in the face-to-face shopping scenario. (Optional; can also be other scenarios such as vending, ticketing or remote scenarios.)
2. When the choice of payment method is asked, they select "pay with cash". The amount of transaction appears on the display and the customer confirms the transaction as usual.
3. An error message appears: "You do not have enough cash in your purse. Do you want to download cash now?" By accepting, the user initiates the transaction.
4. A PIN request appears on the phone display. The customer keys in his PIN.

5. Once the chip card has validated the PIN, the customer keys in the amount to be downloaded and confirms.
6. The message "download successful" appears after a few seconds and the user automatically comes back to the page where the amount of the shopping transaction has to be confirmed. The original transaction can now be continued.
7. If the operation happened to be unsuccessful, the page with the selection of the payment methods would have been provided and the customer would be requested to choose another payment method.

### *2.6.7 Transport (taxi – mobile to mobile merchant)*

This scenario describes one possible situation in which the mobile phone can be used as payment instrument in transactions for "mobile merchants".

The customer uses a handset equipped with two chip readers (internal or external), one reader for SIM-card and one for bank issued chip card. The mobile phone has the required software.

The merchant is the owner of a venue or business, which is mobile by nature (e.g., taxi, or home delivery) and when the amount due is being paid at the moment of delivery.

Merchant has a Mobile wireless site / shop.

#### The User Experience is as follows:

1. A client is taking, for example, a taxi from London to Manchester. Shortly before arriving at the final destination, the driver asks the client how they want to pay. The user chooses mobile payment and gives the driver their mobile phone number.
2. The user receives full transaction information from the driver who has provided the information via a wireless (local or remote) connection from the meter to the user device.
3. The user connects immediately to the taxi company website.
4. The user enters their PIN for authenticating them self and for signing the payment message.
5. The user receives a confirmation on their phone.
6. The taxi driver receives confirmation as well.
7. Receipts are also made available for the user.

## 3 Consolidated Requirements of Mobey Banks

### 3.1 Introduction and scope

The Mobey Forum sees that in the current market situation banks need to take a clear position. The Mobey Forum undertook a detailed process to establish clear requirements necessary to facilitate mobile financial transactions and to prioritise those requirements. The objective is to address financial institutions' requirements in full and as such consider issues both from the customer as well as the business perspective, including technical and implementation issues.

Four principal categories were identified when substantiating requirements for mobile payment transactions: **customer proposition**, **business priorities**, **technical issues** and **implementation issues**. These four principal categories were assessed on their relative level of importance in an overall mobile payment architectural solution in the eyes of Mobey members. The categories are now explained in the order of priority; customer proposition was considered to be the most important requirement, followed by business priorities, then technical considerations and finally implementation issues.

It should be noted that, for the purpose of this assessment, the **business priorities** section focuses purely on the relationship between *financial institutions* and their customers, both individuals and merchants.

Within each major category, the level of importance of subcategory requirements was also weighted and the detailed requirements are included below in descending order of importance. For example, in the convenience section of the customer proposition, "ease of use" was singled out as the most vital requirement, followed by "speed", followed by "price", etc.

It is recognised that there are several key issues to be addressed in relation to various groups involved in the value chain, and these issues are broadly covered under the "acceptance by all parties" section of the business priorities, which follow below. More specific comments and indeed future study is required to address the following:

**Merchants.** How to solve the problem of integrating mobile payments into existing merchant infrastructure; Merchant's requirements concerning the infrastructure and network; positioning towards other payment methods; cost incentives; process changes; confirmation/reconciliation; market opportunities.

**Network operators.** While a key requirement of Mobey banks is operator-independence so that banks do not have to rely on unique bilateral deals with every operator in every market in order to offer mobile payments to any customer grouping, acceptance of the recommended "Mobey solution" by operators will still be crucial. The network operator benefits are described in the related Technical documentation by implementation alternatives.

**Inter-Bank interoperability and usage.** Global Inter-operability of certificates and CA systems has to be guaranteed so that a customer can use services from different banks and maintain good usability.

## 3.2 Headline Business Priorities

The architectural solution must leave the level of security in the field of customer authentication open for the issuer to mandate. Strong authentication of the user is usually required for transactions above a certain value. The architecture must therefore be flexible enough to allow no authentication of either the end user or the merchant (for example, issuing banks may choose that for certain very small-value transactions related to certain kind of services no authentication is necessary at all) as well as catering for strong consumer authentication in the case of larger value transactions and services requiring them.

Operator independence is necessary in view of the importance to banks to be able to offer all their existing (and new) customers the ability to make a transfer value, whether from their existing payment instrument (e.g., credit card, current account debit) or through a new form of payment, to a beneficiary using a mobile device. While it is recognised that a financial institution may achieve this by entering into a bilateral agreement with every operator in all markets, the more realistic approach is an operator-independent service. Furthermore, this in no way precludes bank-operator agreements or implementations of mobile payment offerings.

## 3.3 Customer proposition

### 3.3.1 Convenience

“Ease of use” is defined by the Mobey Forum as the most vital component of any mobile payment architecture. If executing a mobile transaction of any variety is not simple and straightforward to complete, and indeed as easy to use as existing alternative methods of payment (for example in face-to-face local payment environments), customers will not take advantage of them. Creation of user habit is essential and a habit will not be created if the service isn't very easy to use!

Speed, in terms of completing transaction within a reasonable timeframe, has been identified as the next most important element. For remote payments in general, with some variations across scenarios, transactions should take no longer than 30 seconds excluding user input times. For example, once a user hits “buy”, a request for payment type should be received within 5 seconds. Once payment type has been selected and authentication / confirmation of details option must be served to the customer device within 10 seconds. Finally a message stating that the transaction has been successful should be received by the user 15 seconds after inputting their PIN. Local payments are subject to similar timeframes.

Price is a significantly necessary driver. 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. For all mobile payment transactions, the customer should pay for the air-time of the call (unless their network provider offers free access as part of the service agreement). Incentives should be given to merchants and consumers to use the new services through an attractive and motivating pricing structure.

Customer enrolment needs to be straightforward and fit-for-purpose.

The existing user experience in making local and remote payment transactions needs to be enhanced in the mobile environment. It is felt that to some extent it is necessary not merely to achieve parity with alternative payment methods (e.g., credit or debit cards, cash) in terms of ease-of-use, speed, etc., but actually to *improve* current methods. For example, local mobile payments such as vending for canned drinks need to be a better customer experience than

taking out loose change; local mobile mini-payments such as taxi journeys should add more value to users than having to rely on cash.

Automatic form—filling is a prerequisite, as customer convenience is of significant importance in mobile transactions. Automatic form-fill functions for Internet payments, be it through the use of a wallet, ECML or otherwise (either with merchants or financial institutions owning the wallet) has been moderately successful. This model takes on greater importance in the mobile environment, where many devices do not have efficient user interfaces or keypads and the input of information, such as shipping addresses, is considerably onerous.

In order to facilitate mobile payments the user usually needs to carry three objects. The handset, the SIM card and the bank issued card (or security application/solution). All three are reissued or renewed in varying cycles. All three are issued, reissued, sold, bought, renewed and/or distributed at different times with different processes using different methods for authenticating the user. The need of controlling these processes and authentication methods vary between the different entities that issue or sell their objects. It is crucial that the customer proposition, when it comes to issuance or re-issuance convenience, is formed with full independence between the three objects.

In terms of the flexibility of a customer's mobile payment service, it is felt that the most important element is to allow users options and the freedom to renew contracts with the chosen network operator (or change operator) without having to make alterations to payment-related services. This includes hardware, applications, authentication mechanism or otherwise.

Similarly, it is felt that the renewal of bank payment services should be simple and should not involve unnecessary change – of network operator or handset Renewal of payment services must be able to be performed over the air (OTA). Finally, the renewal of mobile payment options, when a customer changes card or certificate must be simple and straightforward. Also this updating must be possible OTA.

### 3.3.2 Security

Customers' protection against fraudsters, hackers and other criminals looking to hijack payment details for their own illegal use, is of primary importance. Both the user's perceived security (i.e., comfort level) and the actual (technical) level of security must be sufficient and the transaction-level encryption must be effective and of a high standard enough for the service offered. In other words, users need to feel confident and secure enough that their payment will not be jeopardised and also need to see the results – and avoid becoming the victim of fraud loss.

The customer's assurance that the payment destination is genuine is also an important requirement. This is possibly more important in the mobile market than in the traditional Internet environment, where false web merchants can be spotted more quickly than on a small mobile display. For example, a fraud perpetrated by setting up a "Marks and Spenser" web site and accepting credit card transactions (incorrectly spelled – the genuine site is "Marks and Spence~~r~~") would be well hidden over wireless due to the lack of branding on many wireless (WAP) pages.

Both corporate and private customers must be able to use the certificate solutions globally (need for cross-certification) and through multiple channels.

### 3.3.3 *Privacy*

Confidence that personal details will not be forwarded on to ANY organisation, individual, authority, etc., for any reason whatsoever is essential. Any concerns that customers may have around submitting personal details and the risk that these may be transferred to third parties for malevolent or other purposes (for example, unsolicited spam-type marketing) need to be addressed and concerns nullified. However, if additional marketing is wanted and approved by the customer then naturally this information can be passed on.

## 3.4 Business priorities of banks and merchants

### 3.4.1 *Security*

Effective customer authentication is deemed the most vital element in facilitating mobile payment. Authentication must be fit for purpose and the level of authentication will doubtless vary depending on both the amount involved and the type of transaction. The institution liable for the payment, usually the issuing bank, will always be responsible for and have the flexibility to define the level of user authentication. The Mobey solution will cater for all required levels of customer authentication. Micro payments will usually only require a low level of authentication, and will be based on solutions such as, PIN-codes and no digital certificates. Mini payments in excess of EUR 10, however, may require a better authentication mechanism. Macro payments, here above EUR 100, will in most cases require strong authentication, which can be based on digital certificates and wireless PKI solutions. The issuer of the service will always define the security level required.

Transaction-level security is essential. In other words, the passage of sensitive payment-related data between the user's mobile device and other parties to the transaction needs to be encrypted to a sufficient level to protect it from access by unauthorised or fraudulent third parties.

Merchant authentication required depends on the risk assessment and varies from one acquiring bank to other. To some extent this may rely on which interoperability domain security is the dominant one; there are variations in the ways with which these protocols handle merchant authentication.

### 3.4.2 *Versatility*

Scalability across all payment opportunities is a key requirement. Not necessarily every mobile payment scenario will be suited to a single generic architecture, but the solution needs to be flexible so that all payment varieties can be accommodated. For example, an institution should not have the need to develop a new infrastructure to cater for local payments if it is already in a position to offer remote payments.

The payment opportunities were ranked in order of importance, and they are explained in Chapter 3.

Support of multiple payment products is vital in terms of banks being able to offer customers the choice of using credit, debit, virtual e-cash transactions and others to execute a wireless payment.

Support of other banks/payment schemes will be an integral part of a financial institution's mobile payment service offering in future. However, several issues are critical: holding credit cards issued by other banks on proprietary wallets is an example. Additionally, inter-bank interoperability over certificate authentication needs to be discussed— i.e., will an agreement

between two chosen banks lead to one of the banks authenticating the other bank's customer and vice versa, and are there opportunities to form a wider agreement? Such issues will be addressed at a later stage within the Mobey Forum and are thus not in the scope of this document. However, it is agreed that the Inter-Bank usage has to be guaranteed by some means.

### *3.4.3 Acceptance by all parties*

One crucial area in regard to the appropriateness of a Mobey-recommended architecture for mobile payments is the acceptance by relevant involved parties. It is felt that merchant acceptance is vital for the ability of any solution to be well received. However, this can entail changes to existing merchant systems, POS terminals, etc., but obviously the goal is to introduce the minimum of alteration and expenditure along with a clear explanation of the benefits. As mentioned at the head of this section, further examination of the merchant proposition is necessary and will be undertaken by Mobey Forum in the near future.

The business requirements in relation to network operators are clear from a financial institution perspective, in that the need to offer customers a non-operator-specific service is key. Providing payment ability to only a segment of a bank's customer base (i.e., the segment which has relationship with one or more specific operators) is an unacceptable long-term strategic solution. Similarly, avoiding bilateral agreements with every operator in every market is advantageous, particularly for large international banks with operations in many markets.

The potential to add brand is also important in terms of acceptance by all parties in the value chain. Card payment issuers, credit associations, etc., view branding as vital to any proposition, and the Mobey architecture must allow visible branding of payment products (either on a plastic card or in the phone) to be managed by individual institutions.

The ability for banks to assimilate the proposed solution within existing proprietary e-payment strategy models is important, both conceptually and from a systems integration standpoint. This implies that the Mobey solution must retain a certain amount of flexibility in its implementation options.

Protection for merchants against consumer non-repudiation is a significant motive for merchants to adopt bank- and payment scheme-proposed secure payments protocols. This has been addressed by, for example, the Visa EU mandate. The proposed architecture must include merchant protection against charge backs from customers disputing mobile transactions.

Similarly to the requirement that the proposed solution fit well within proprietary existing bank e-payments infrastructures, merchant integration into existing systems must also be addressed.

## 3.5 Technical Considerations

The most important technical requirements are that the banking relationship is independent of the operator relationship and that the solution is based on open interoperable standards.

### *3.5.1 Independence of operators and open standards as key requirements of Mobey banks*

The banking relationship and the operator relationship with the end user must be independent of each other's. If the customer decides to change one part of the solution (e.g. the SIM card), it must not have implications to the other relationship (e.g. with the bank) and vice versa. We strongly believe that intermingling the businesses would lead to an unclear end user experience, for example, leading to the end user not knowing whom to contact when he has lost his PIN code for banking services.

It is also very important, that the solution is based upon open interoperable standards. This means that it cannot contain proprietary technologies, the handsets and servers should work seamlessly together, between different manufacturers, and all service providers should be able to enter the market smoothly. It also poses requirements for the creation of any new technology not yet in existence: any new protocols needed must be specified and standardised with a cross-industry effort to guarantee interoperability.

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' out from the handset and move it to another handset without difficulties or to make an easy and safe backup and restore, if a software solution is concerned. This applies also to different manufacturer's handsets.

### *3.5.2 Use of existing standards*

Existing infrastructure must be utilised as much as possible. This is recognised as a very important requirement. This applies to for instance existing banking technologies, such as the EMV standard, and to the emerging standards for the transaction processing, such as 3D SET and 3D Secure. In the Payer's architecture, solutions must also be based on existing standards, such as, WAP, as much as possible. We realise that not all the technological pieces are yet standardised and not all required technologies exist, but we plan to work towards getting the required technology standardised and in place as soon as possible.

Reusability means that banks should be able to utilise the same authentication mechanisms to offer services to customers coming in from multiple channels. This applies to both back-office systems and technologies used in the payer's solution: basically, additional infrastructure investments should be minimised.

Additional technical requirements are that the solution should be gateway independent and include all security components. Gateway independence means that the gateway should be transparent to the mobile commerce applications such as banking and mobile payments and if the gateway is changed, e-banking applications shouldn't be affected. Security solutions should include all four components: Confidentiality, Integrity, Authentication and Non-repudiation (whenever required by the issuer, depending upon the service offered and value of the transaction).

## **3.6 Implementation issues**

It is also essential to understand the factors affecting the ability to implement a proposed solution. The focus of this chapter is to study these issues. Implementation issues are divided into cost and speed-to-market factors. The cost factors are studied first.

### *3.6.1 Cost factors*

The most important cost driver is the set-up cost per consumer. Set-up costs per consumer consist of additional costs to the issuing bank related to the security tokens required by the solution, setting up the distribution of them and finally distributing them to the consumers, setting up the required security infrastructure such as PKI, customer services supporting the solution and all other tasks required in making the service operational divided by the amount of users expected for the service.

Almost as important is the cost for a merchant to implement the solution. Merchant's total costs consist of once-only implementation costs and run-time costs. The main cost factors for the merchant are implementation costs of the Payee's security solution such as, 3D SET, potential required changes to the POS terminals, data communication costs and the provisions required for transactions. As the merchant acceptance is perhaps the most crucial factor for the success of the new services, individual banks should investigate how much they are able to subsidise merchants with any additional costs caused by the new service.

Consumer's total cost to implement the banking solution is also very important. This includes once-only costs, such as purchasing the handset and also operating costs, such as actually using the services. These costs should also be reasonable compared to the value of the service, and form a lucrative service package for the consumer.

A minor cost factor is issuer's cost to run the service. Issuer's total cost to run the service consists of operational costs related to running the security solution, such as issuing, validating and updating of certificates, validation of digital signatures, updating of revocation lists and other required databases, and of managing, accounting and clearing of the monetary transactions. Issuer of the service may also want to buy (outsource) this service from another trusted party.

### *3.6.2 Speed to market*

The most important speed-to-market factor is availability of existing solutions, such as suitable handsets, required chip cards and security infrastructures that may be required for a particular service. Availability and penetration of technologies such as Bluetooth is also an essential factor.

The main factors affecting the speed of rollout are the availability of suitable handsets and required middleware solutions, in-house or external. Speed of rollout is expected to vary also due to local market conditions, such as the size of market, national culture and consumer experience related to use of mobile technology in financial services.

The solution should also be international, meaning that the user has to be able to use the (local and remote) services when travelling to other countries and to use the remote services offered in other countries when at home.