EUROPEAN COMMITTEE FOR BANKING STANDARDS

BUSINESS AND FUNCTIONAL REQUIREMENTS FOR MOBILE PAYMENTS

TR603 VERSION 1-[FEBRUARY 2003]

Document History

Version 1 February 2003

TABLE OF CONTENTS

0 OVERVIEW

Due to the traditional expertise of banks in handling secure payments, it is foreseen that mobile payments (m-payments) infrastructure will be managed by banks. This could vary depending on local markets and legislation.

This report describes the understanding and requirements of a typical European bank implementing m-payment solutions. As such, it intends to serve as a guideline for the banks and their partners in m-payments (such as telecommunication companies and device manufacturers) whereby all partners can benefit. The discussions summarised in this report aim to help non-bank players in the m-payments sector to understand and consider business and functional requirements of the banks for m-payments.

The structure of the report follows established project development procedures: evaluating the internal and external environment, defining the objectives and finally specifying the requirements. Future steps may include an implementation guideline.

For each requirement, all aspects of the banking business have been taken into account, specifically: strategic, commercial and marketing, legislative and regulatory, technical and security aspects. The functional requirements consider each step of a financial transaction, including all involved actors, be they customers, acquiring banks, issuing banks or merchants.

While the primary focus throughout this effort was on defining the requirements of the banks, every attempt was made to include the needs of non-bank parties and the need for inter-industry partnerships.

The business and functional requirements of the banks provide the basis on which market actors can specify their solutions. The importance of each requirement is to a large extent implementation-dependent. Therefore, at this stage, the importance of these requirements has not yet been prioritised. This will be the objective of the implementation guideline.

This report is based on a review of some of the mobile payment solutions in the market. Today, no solution meets all the requirements identified in this report. For a viable solution, multi-sector co-operation is necessary which is the task of common working groups between the parties involved. In this way, local habits as well as strategic, commercial, marketing and technical specifics can be taken into account, for example in the establishment of common working groups.

1 INTRODUCTION

1.1 BACKGROUND

After looking at the numerous initiatives and forums on m-payments, ECBS members saw a need for a common European approach. A first report has been produced and published to increase the awareness of European bankers of business opportunities in this field.

They then decided that the European banks should define their business and functional needs independent of market competition pressures and without making unrealistic demands on their partners to implement m-payment solutions. This report addresses m-payments from a European banking perspective based on extensive consultation and review of practices across Europe and across individual banks.

To accomplish this task, ECBS established the 'Mobile Payments' working group in August 2001, under the umbrella of its Technical Committee 6, Electronic Services.

1.2 AUDIENCE

This report is to be distributed, in the validation phase, to European Bankers. In a second phase of the ECBS validation process, it will be distributed to a wider audience including other relevant parties such as equipment manufacturers, SIM card manufacturers, service providers and telecommunication companies.

1.3 OBJECTIVES

The main objective of this report is to specify the business and functional requirements of the banks for m-payments for the relevant industry partners.
This report provides a basis for future studies and business decisions and should be read when defining future work items (an implementation guideline is foreseen).

1.4 SCOPE

This report presents a unified business approach of the European banks and specifies their requirements concerning the functions that are needed to fulfil the needs of their customers.

The scope of this work is based on the following definition of m-payments:

> 'A mobile payment is not by itself a new payment instrument but an access method to activate an existing means of payment for financial transactions processed by banks between bank customers. An m-payment involves a wireless device that is used and trusted by the customer. M-payments may be card based or non-card based, in both the real and virtual world.'

An m-payment is an electronic payment across the data channels of the mobile device, electronically processed in the merchant environment, other than the conventional telephone order, and of higher security level.

M-payments enable payment at any time and in any location.

The report sees m-payments as having banking systems as a core part of the transaction where customer interaction may be through the mobile Internet and/or in the real world.

1.5 LIMITATIONS

This report does *not* constitute:

- a technical or standard specification
- (m-payments) system functionality profiles
- lower-level implementation specifications

For more information on the above issues, readers are referred to related publications.

Where items are listed, their position does not indicate a ranking or level of importance.

1.6 RELATED PUBLICATIONS

The following are related publications:

- **ECBS, EBS 105-1,** Minimum Criteria for Certification Procedures
- **ECBS, EBS 105-2,** POS Systems with On-line PIN Verification: Minimum Security and Evaluation Criteria
- **ECBS, EBS 105-3,** POS Systems with Off-line PIN Verification: Minimum Security and Evaluation Criteria
- **ECBS, SIG 106-4**, The Use of ISO 8593 for Transactions in open Networks using unattended Terminals, e.g. e-commerce, m-commerce
- **ECBS, TR 410**, Secure Card Payments on the Internet
- **ECBS TR406,** Guidelines on Algorithm Usage and Key Management
- **ECBS TR409,** The Use of Audit Trails in Security Systems
- **ISO 9564**, Banking – Personal Identification Number and Security

2 METHODOLOGY

This report covers the following four steps:

1. determine the main **characteristics** of the mobile payment market
2. define the **objectives** and intentions of the European banks to satisfy this market
3. specify the **business** requirements
4. specify the **functional** requirements

To meet the objective of this report, namely to identify the business and functional requirements of banks for m-payments, ECBS undertook an extensive review of the related documentation and results of banking internal initiatives carried out by ECBS and other players active in this area.

For example, this report takes into account the work undertaken by the Mobey Forum, the Mobile Payment Forum (following the GMCIG), and the MeT initiative.

This report, which focuses on the banking requirements, complements existing publications. It is the aim of the report to reflect the views of the banks and provide guidance to others entering the area of m-payments.

3 MARKET ANALYSES AND ACTORS

Given the limitations of existing and proposed future mobile devices[1] not all payments will migrate to the mobile platforms in the short- or even medium-term. Nevertheless, a range of scenarios is envisaged where mobile device functionality may benefit the user or enhance the payment process.

A mobile device is *not* a means of payment but a means of activating, initiating and/or confirming a payment. One could also speak of 'payment approval and/or initiation' executed by a mobile device. For example, even if a card is not used physically when paying, it may be a payment transaction using a card system. This perspective allows more flexibility and includes, for example, a mobile device initiating a pre-defined payment instruction. It is also possible that when an electronic bill or a card transaction is presented to the mobile device, the user has only to confirm the presented data. Basically, the mobile device is used to initiate and/or complete a payment transaction.

Taking the GSM as an example, the following is applicable:

- The **banks** decide the requirements needed for bank-related functions like m-payments and m-banking.

- By means of the personalisation associated with the SIM, the **users** may choose the telecommunication operator that provides the best business offer for both, traditional airtime and value-added services.

- The **telecommunication operators** decide which functions may be operational on their network and the device it can connect to.

M-payments may be used for content on the mobile (for example, prepaid airtime, actual information and ring tones) and for goods or services delivered though other channels.

If the device is personalised and contains dedicated security features (encryption as well as a trustworthy customer verification method), the mobile device therefore becomes the user's personal transaction terminal or even the user's personal trusted device.

A distinction should be made between mobile banking services (which comprise a host of value-added electronic services such as billing, payments and alerts) and m-payments per se**.**

This document focuses only on m-payments.

---

[1] In this chapter the term *mobile device* is introduced and refers to the following definition:

> 'A set of seamlessly compatible hardware and software used interactively by a customer for making transactions wirelessly to other receiving parties which can be remote (e.g., a server located on some communication network including the Internet) or face-to-face (e.g., electronic terminals like POS, vending machines, parking meters). Examples of mobile devices are mobile phones, PDAs and interactive laptops.'

Depending on the situation in which the mobile device is used, it is specified by the use of the terms *mobile trusted device* and *personalised mobile trusted device* as defined in the glossary.

3.1 MARKET CONSIDERATIONS

M-payments support different business environments, since the mobile device in the hands of the users becomes their personal payment terminal in different situations, remote or face-to-face, depending on convenience and practicality.

The market demand for m-payments may differ widely from one country to another, especially for face-to-face transactions, given various national payment habits and instruments.

3.1.1 Types of payment based on value

A range of transactions may be envisaged ranging from very low value digital content (for example, ring tones and screen logos) through to high value downloads (for example, video clips and games) and on to the purchase of physical goods (for example, CDs and books). Ultimately, we see users comparing and purchasing even higher value items such as airplane tickets or household appliances, as is now the case on the fixed-line Internet.

These payment transactions may be split into three broad categories:

Micro payments encompass the lowest values, typically under €2. Media and SMS vendors have stated that the lack of an open standardised micro payment capability is a key factor in restricting the growth of mobile commerce. At present micro payments are largely handled through reverse-charge SMS or premium rate numbers.

Medium payments are typically between €2 and €25. The ability to cost-effectively service these payments may be critical in some countries for the success of the service.

Macro payments are typically those above €25.

Banks should consider these payment categories of strategic importance to their long-term success. As a consequence, acceptance of these payment categories in the mobile space requires a consistent user experience and appropriate levels of security and authorisation in both remote and face-to-face scenarios.

3.1.2 Types of payment based on location

Remote transactions

A remote transaction can be conducted regardless of the location of the user.

For such transactions, a trusted and personalised mobile device can be used to:

- initiate a transaction
- authenticate the customer
- and/or sign a transaction

One obvious example is the use of a trusted and personalised mobile device to authenticate a user connected to a server-based wallet.

Remote payments can be:

- connected to the usage of the mobile device but not actually dependent on special applications in the device. Typical examples are enabling the use of a mobile phone (for example, top-up) and receiving information on a phone (for example, ring tones and weather forecasts).

- used for delivery of digital value stored in the device (for example, tickets, coupons and digital cash). These types of payment might require some kind of local application in the device.

- used for paying for goods and services that are not connected to the mobile device itself. In this category lie some bank payments and telephone-order shopping as well as some applications for web shopping, IDTV-shopping, IDTV pay-per-view and remote parking payments. Also included are P2P payments.

Local/proximity transactions

For such transactions, the mobile trusted device can be used to:

- pay at unattended machines (for example, vending machines and parking meters)

- pay at traditional points-of-sale (with human interaction).

Some applications for local transactions are actually implemented as remote payments (for example, "calling" a vending machine).

Local communication between a mobile device and a vending machine, or a POS terminal using infrared, RF contactless or Bluetooth technology, provides real face-to-face possibilities. Based on security concerns for existing local communications, the telecommunication industry is developing enhanced protocols like NFC (Near Field Communication).

3.2 SUCCESS FACTORS

Given the definition of m-payments and the environment in which they will be available, the following section deals with the drivers that will help to make m-payments successful.

The drivers are structural properties of an industry that shape cost behaviour, revenue models and differentiation. An industry is defined by the actors who come together (for strategic or tactical reasons) or compete against one another to create and deliver a value proposition. Typical high-level drivers in a network-type industry (such as banking or telecommunication) include:

- network promotion

- contract management

- infrastructure operations

It is also important to recognise key success factors. These comprise a set of market factors defining the competitiveness of the actors. In the mobile banking sector, the several actors are users, device manufacturers, ICC manufacturers, network providers, banks/payment providers and application/content providers.

While an industry consists of partners and competitors, a market includes the final user base, be they businesses or individuals.

The objectives of the banking sector are treated separately in chapter 5. In the next section, key drivers and incentives that affect users, merchants, network providers and device manufacturers are explored.

3.2.1 User drivers/incentives

The four main user drivers are convenience, fashion, pricing and acceptability:

- **Convenience** can be achieved by providing unique capability, new functionality and a consistent user interface in the mobile device.

- **Fashion** can be an effective driver for the adoption of new ideas and technologies, for example, customised mobile phone covers or ring tones.

- Differential **pricing** or other economic incentives for the user can make new channels relatively more attractive.

- **Acceptability** is important so that users find a large number of merchants that accept the access to payments through a mobile solution. When everybody can accept an m-payment, this access to a means of payment is universal.

Against these drivers for change, there is unwillingness by some users to change their behaviour, simply for the sake of some new functionality.

3.2.2 Merchant drivers/incentives

The main merchant drivers are to:

- maximise market reach (as a **new channel,** m-payment services will enable merchants to reach and be reached by customers on the move)

- **sell new types of digital services** such as music, video, games, metered payments and other digital interactive applications

- **minimise costs (fixed and operational).** A more secure means to sell existing goods or services benefits merchants and decreases the risk of repudiation. In addition, fast processing may minimise the costs.

3.2.3 Network provider drivers/incentives

The main network provider incentives are:

- generating **new income** (through increased traffic)
- **increasing** average revenue per user (**ARPU**) and decreasing churn (losing customers to another operator)
- improving the overall long-term **business case** by accepting m-payments to catalyse the value of the operators network
- **enhancing competitiveness** (vis-à-vis the banking sector) through a more 'practical' understanding of the payment schemes and processes
- becoming an **attractive partner** to content providers

3.2.4 Device manufacturer drivers/incentives

Device manufacturers are keen to:

- promote a **high turnover** of devices to maintain sales levels. Advanced content will require new functionality and compatible mobile devices (for example, bandwidth, downloading, larger and colour display, larger memory)
- segment the market and support fashion by making available mobile devices in **different designs**
- develop a **flexible business model** to firmly partner with telecommunication companies, content providers and banks

3.3 PARTNERSHIP VERSUS COMPETITION

As with the existing payment infrastructure, any successful system is built on co-operation between different industries. For example, financial institutions and fixed-line telecommunication company operators, hardware manufacturers, postal services and others are involved in traditional payments.

Successful evolution, therefore, should be based on a truly inter-industry environment, where partnerships and co-operation must be present.

Cross-industry and intra-industry co-operation is required, as long as payments are concerned, in order to define common standards and allow interoperability.

Means of payment are only successful if the payer and the payee share a common payment solution. In traditional payments, this has been achieved through co-operation between the financial institutions and has led to the definition of widely accepted domestic or international payment products. This co-operation did not prevent financial institutions from competing in other areas such as pricing or providing additional services to the customer.

Today, such co-operation can be found among all actors in the m-payment environment, in order to avoid the risk of developing incompatible schemes or systems. If banks, operators and manufacturers cannot co-operate, this would result in:

a. difficulty in reaching the critical mass and possible customer disinterest

b. lack of fluidity in the market

c. higher costs for all parties

Customers will be primarily attracted by the services they access through mobile devices. Payment solutions will be facilitators and not be basic factors of differentiation. If a widely accepted common standard is not found, this could prevent a whole new business from emerging.

Building solutions for mobile trusted devices and mobile customers require standards supporting m-payments. These standards must be cross-border, cross-bank, cross-telecommunication company, cross-device and also allow for different competing partnerships.

One of the aims of this report is to facilitate these partnerships by defining bank requirements in m-payments that will enable industry partners to supply the technology and services for financially viable and secure m-payments.

4 OBJECTIVES OF THE BANKING SECTOR

The previous chapter identified the incentives driving the bank partners in the field of m-payments. This chapter focuses on the success factors that banks need to meet to ensure a common understanding of their objectives and key drivers. The business and functional requirements expressed in chapters 7 and 8 are derived from these objectives.

The main business objectives of the banking sector to include m-payments in their service portfolio are:

- **Positive business case and competitiveness**

All businesses want to generate long-term profit. A win-win situation is necessary to achieve a sustained positive business for all parties.

If a positive business case is found in the payment application itself, complementary opportunities could emerge in home-banking applications.

- **Maintain customer confidence and bank image**

The positioning of banks in the market is mainly based on their longevity, providing customers with a range of high quality banking services and maintaining the market lead in the future m-payments environments. A number of objectives derive from this:

  - securing existing businesses
  - finding a long-term business solution (compared to the mobile communication industry the banking industry has developed slowly)
  - building up a trusted system where the security of the payment application is essential to minimise charge-backs/fraud and the related liability
  - achieving a good trade-off between security and business. Security is costly and should not be regarded in isolation. Aiming at absolute security usually prevents banks from developing their business quickly. However, at the same time, businesses must carefully evaluate market and product development risks

- **Independence of business**

In order to keep their relationship with end-users, banks have to avoid disintermediation.

This could be achieved through co-operation with other partners. A win-win co-operation supposes that each party fulfils its natural role in the payment process and that each party's core business is respected. This leads to long-term profitability for all parties.

It may even lead to strengthened customer loyalty to their banks through the establishment of an electronic communication channel.

- **Compliance with existing online transaction infrastructures**

M-payments represent a new market for banks. It offers new opportunities to use existing means of payment. Any complementary solution should be compatible with existing ones (for example, 3-Domain Model).

On the other hand, synergy can also be found since a mobile device can provide enhanced customer authentication methods within existing e-commerce / banking infrastructures. Simplicity and speed for deploying the solutions are the key issues when looking for this compliance.

5 TECHNOLOGY MODELS

Appendix B gives an overview of existing technical m-payment solutions and their corresponding strengths, weaknesses, opportunities and threats, and also a banking recommendation for each solution.

6 BUSINESS REQUIREMENTS

The business requirements described below are derived from the incentives and drivers discussed in the previous chapters and show how banks can specify and implement m-payment solutions. These business requirements are valid for the implementation of m-payments generally and are not dependent on specific solutions. Business requirements internal to banks are considered along with external ones, namely requirements vis-à-vis their potential partners such as telecommunication companies or device manufacturers.

Five categories of business requirements have been identified:

- strategic requirements
- commercial and marketing requirements
- legislative and regulatory requirements
- security requirements
- technology requirements

Each requirement is defined, specified and followed, when necessary, by a comment on how to implement it, by whom and when.

6.1 STRATEGIC REQUIREMENTS

The strategic business requirements of the banks are necessary conditions for banks to form partnerships to create and develop the market. They therefore do not conflict with those of the other players.

The following are the strategic business requirements of the banks:

St1: Independence of business – In an m-payment application, all involved parties should be organised such that each party depends as little as possible on the other and continues to develop further its respective core business. However, business independence cannot exclude functional dependence:

- **Business independence** – From a commercial point of view, the roles and responsibilities to promote the m-payment solution, enlist and manage the customer's relationship should be clearly defined between banks and other parties. Especially, data ownership and privacy shall be respected.

- **Functional synergy** – From a technical point of view, in some scenarios functional independence is not possible while the businesses are independent of each other (for example, payment applications run by the bank in a SIM). The duplication of functions shall be avoided and implementation defined to allow business independence. This is why some technical requirements result from these strategic ones and why open standards should be aimed for (see T1).

St2: Positive business case for banks – A positive business case is required for any participating bank in the short or long-term. Banks may be ready to invest in the infrastructure, but not without a positive revenue model. The payback of the necessary investments must be assured.

St3: Stability of business model – Stability of the complete business model that should be based on partnerships and reliable technology is required (long-term business).

St4: Banks shall manage or approve payment applications and products – The banking industry shall define the rules and conditions of compliance to their m-payment application.

As banks are asked to handle the guarantee of payment, they will accordingly need to control the corresponding means of payment in order to manage the associated risks

St5: Trusted and visible brand – The solution must support the bank brand and the means of payment brand thereby enabling the customer to recognise them when paying.

St6: Customer agreement to enrol (if necessary) and access payment application – Customers shall not be provided with a new means to activate payments without their previous knowledge and consent. This is necessary to position the product, as well as to establish clearly the responsibilities of each of the actors, be they holder of the device or promoters of the application.

St7: Customer relationship – Payment services are key to the banks' relationship with their customers (private/corporate and merchants).

The bank shall therefore be visible in the acquisition and enrolment of their customers to the bank's m-payment application, whether it is performed by the bank or by a partner.

It is likely that, at least in some countries, customers will be provided with payment access tools by another party (for example, a telecommunication company). In such cases the enrolment procedures should be managed or approved by a bank.

St8: Possibility of evolution – Once telecommunication companies, manufacturers and banks have defined the solution, consideration should be given to the technical possibilities of evolution. The party in charge of the migration should be defined as soon as possible.

6.2 COMMERCIAL AND MARKETING REQUIREMENTS

C1: **End-user acceptance** – Any m-payment solution should take into account fashion, pricing and convenience. Manufacturers should develop products that are easy to enrol in and use (ergonomics). Data entry and displaying information should be user friendly and comply with current standards for interoperability.

C2: Solutions should be built on common mobile communication devices – In order to achieve a faster rollout, each partner should develop solutions that are not based on special devices.

C3: Compatibility of evolving technology – In order to support the possible identified evolution of the payment application, new features should be specified in collaboration to increase the life of the device: enhancing the payment system should not result in a necessity to replace existing phones (linked to C2). However, full backward compatibility might generate additional costs and might limit new functionalities.

C4: Interconnection and standards - All partners shall explore compliance to international industry (banking and telecommunication) standards and to re-usability of parts of the system when migrating to new m-payment solutions. As far as payments are concerned, banking standards shall apply.

C5: Marketing collaboration – When offering a means of payment to customers, banks should collaborate with other partners regarding the product definition. Market experience shows that the actors must collaborate in order to achieve mass-market adoption.

C6: Consistent user experience – In order to ensure cost-effectiveness and market acceptance of the m-payment solution, the procedures for registration and transactions should be well standardised, secured and accessible through interoperable interfaces.

C7: Independence between cost of transmission and cost of payment services – The value of the payment should not determine the cost paid by the end-user for transporting the information (telecommunication company costs should not depend on the amount of the transaction).

C8: Interoperability of solution – Each bank shall do its utmost to make their m-payment solutions available to the different telecommunication networks and mobile devices. Consequently, the customer shall not be forced to change or stay with a limited set of network operators or mobile devices (and their vendors) when using m-payment solutions.

6.3 LEGISLATIVE AND REGULATORY REQUIREMENTS

L1: Compliance with banking and financial legislation – Even if pan-European regulations are to be harmonised, differences between countries will continue to exist for quite some time. Locally, banking and financial legislation can be quite complex and thereby prevent banks from marketing products on an international basis.

L2: Compliance with payment scheme regulation and banking practices – In addition to legal aspects, payment scheme regulations or agreements set up by banks impose an additional number of constraints.

M-payment solutions shall comply with these regulations in order to further exploit the common understanding between banks, reduce time to market and benefit from common working practices.

L3: Liability and rules – The responsibility of each party (telecommunication companies or banks) in providing payment application security also defines the corresponding liability.

The involved parties shall define clear rules on liability. General rules of conduct could be as follows:

- Banks are in charge of payment solutions
- If some other party takes a part of a payment solution,
    - clear rules and liabilities (scope and limits) shall be defined between the parties
    - the third party should be sound and reliable.

6.4 SECURITY REQUIREMENTS

Se1: Implemented payment application security shall be approved and/or controlled by banks – The following basic security features apply:

- authentication of parties involved in the transactions
- data integrity throughout transmission
- confidentiality of private information
- non-repudiation of the parties involved in the transaction
- acknowledgement receipt

This will result in creating a trusted communication path for all transactions between each party, be they end users, telecommunication companies, merchants or banks.

Se2: **Application and infrastructure trust** – Trust in the system and in particular the mobile device is essential for users. Therefore, the trusted mobile device shall support application integrity. Any mobile trusted device must be resistant to threats such as 'Trojan horses' (devices supporting the download of applications are more at risk).

Se3: **Information secrecy** – Information on account data, transaction data and users'/partners' personal profiles or information must never be disclosed to any unauthorized party.

Se4: **Payment security (identification, authentication) –** Banking requirements depend on specific implementation solutions, architectures and scenarios. Payment security shall be defined by the party that offers the guarantee of payment to the user according to its own estimation of risk. In a solution involving the banks, this is the responsibility of the banks. As mentioned in L3, if a third party takes over a part of a payment solution,

- clear rules and liabilities (scope and limits) shall be defined between the parties
- the third party should be sound and reliable

Accordingly, the level of authentication (strong or not) is chosen according to the policy of the banks: on-line or off-line password, static or dynamic authentication, symmetric or asymmetric (for example, PKI) cryptography.

Se5: Transfer of devices between users – The payment services accessible through a mobile device (phone, SIM, PDA, etc) are not transferable. However, it shall be possible for users to transfer a personalised device to another person without impact on security. Suitable procedures, mechanisms and policies shall be implemented to allow a trusted change of mobile device holdership.

Since selling or giving away devices is common practice among users, re-use of a personal key by another person should not be allowed, even if a new certificate is issued.

A clear distinction must be made between transferring a mobile device from one user to another and transferring the trust a bank may have in a specific customer. The whole process of entitling (or not) a customer to use, under specific conditions, a payment application shall apply when the device is transferred.

Se6: Blocking an application – When the device is personalised, the banks must be able to close the access to their payment services independently from the use of the other functions of the device (for example, telephone services).

6.5 TECHNOLOGY REQUIREMENTS

T1: Modularity of technologies – The m-payment system should comprise a set of interoperable infrastructure modules that work seamlessly together end-to-end (from local environment [user-device] and transport network until the service side [payment systems in the banking sector]). This requirement is a consequence of St1 and key to maintaining business independence (of the parties involved in m-payments) and results in convenience for the end-users and in allowing future technical evolution.

T2: **Initialisation of service after contractual enrolment** – Some technical solutions provide for the initialisation of the payment application to a greater extent than others concerning ease of use as well as the technical availability for the customer (for example, the parts of the service that are centralised and can be activated over-the-air simplify the rollout and serve the customers' convenience). Ease of initialisation of the payment application, especially on the customer's side, is paramount to the success of the solution.

T3: Compatibility – Compatibility of different schemes will be very important not only for customer acceptance but also for merchants and shall lead to an open infrastructure. Further, the m-payment solution should be compatible with both the network infrastructure of different telecommunication companies, content providers as well as infrastructures operated by banks. It shall be possible for customers to have access to the same m-payment service should they change device, network operator or preferred content provider.

T4: Payment application independent of other applications – When several applications are present in the device, banks should provide m-payment applications independent of digital services (for example, gaming or gambling). Generally, the m-payment functionality should be compatible with different

- operating systems both at customer and server ends
- applications
- digital services
- devices

T5: Network interoperability – Existence of agreements between operators is a prerequisite to enabling a truly 'roaming' m-payment scenario. This applies to SMS, USSD, WAP, etc.

T6: Reliability and speed of infrastructure (time delivery of payment information) – Reliability and speed of the infrastructure are needed to ensure customer adoption.

T7: Compliance with standards – In a first phase, banks and telecommunication companies should work together to determine if the standards of the banks or those of the telecommunication companies should prevail. In a second phase, standards should be co-operatively developed using standards for both, payments and data transport. Payment solutions shall comply with common technical (payments and security) standards of the banks and be made available to any device complying with these standards. Similarly, on data transport through networks, banks would adopt the telecommunication standards.

T8: Flexible architecture – Banks must be able to join the m-payments network with a minimum of infrastructure changes. Specifically, the architecture of the payment system has to be flexible enough so that any interested bank can participate with minimum changes of their own infrastructure and given processes.

T9: Robustness & fault tolerance – The infrastructure must provide mechanisms, features and/or procedures that ensure its availability on a continuous basis. The solution must be stable and run continuously without regular manual intervention (for example rebooting, installing patches). It must be capable of quick recovery from disasters and other problems that cause one or more components of the systems to fail. Even a large-scale failure of the components must not result in any security breaches (for example access to applications or data by unauthorised people). The system must also be self-protecting and must be able to resist penetration and unauthorised attempts to issue, revoke or modify certificates or other system components.

7 FUNCTIONAL REQUIREMENTS

In this chapter the functional requirements of the banks for m-payments are defined. These requirements are based on the three functions of financial transactions, namely issuing, acquiring and transaction processing and the impacts on those when accessing a means of payment through a mobile device.

7.1 FUNCTIONAL ARCHITECTURE OF TRANSACTIONS

Underlying a financial transaction are the following functions[2]:

- **Issuing functions:**
  - Issuing a means of payment
  - Customer enrolment and personalisation of the application
  - Application access
  - Key and PIN management
- **Acquiring functions:**
  - Merchant enrolment and means of payment implementation
  - Clearing and settlement
- **Transaction processing functions:**
  - Initialisation of payment - selection of means of payment by customer
  - Merchant and customer authentication
  - Constitution of a transaction - for example, customer receives data and defines a transaction amount, currency
  - Processing of authorisation - transmission of a request for authorisation of the transaction to a bank, request for acceptance of the transaction, authorisation of the transaction
  - User interface and information management
  - Administrative functions - for example, tracing, certification of transaction

Each of these functions may depend on commercial agreements and implementation modalities between the banking industry and the other parties, be they telecommunication companies, service providers or manufacturers.

[2] The commercial offer phase is not part of the financial transaction.

7.2 ISSUING FUNCTIONS

7.2.1 Issuing access to a means of payment

I1: Activation of the payment application – Issuing access to a means of payment in a mobile environment is to activate a payment application. Banks shall get the consent of the customers before activating a payment application. This application might already reside within the mobile device or need to be downloaded. The application can also be split in two, part of it inside the device, part of it being located on a remote server. Banks shall be able to manage and audit the life cycle of the application (for example, knowing the version downloaded by the customer).

The functionality offered by operators to banks should allow the possibility to securely and remotely activate a payment application.

I2: Compliance of the payment application – The banking environment shall ensure compliance of the payment application with the user interface protocol, application handling, key management and general security requirements.

I3: Management of the local payment application – In order to manage the application and the customer relationship, banks shall, whenever needed, be able to identify the device and its configuration in order to update, delete and identify the application.

7.2.2 Customer enrolment and personalisation of the application

I4: Identification of customer – Prior to enrolment, a set of credentials should identify the customer. Before the payment application is activated, the banks must authenticate the customer.

I5: Personalised application – If the application is personalised and before the first payment is executed, the banks should authenticate the customer. The banks should give the customers a unique identification that enables them to access the payment application.

I6: **Customer data** – If wallet or subscriber files are used for storing customer data, these files shall be kept securely, with limited access, and preferably within the banking environment or a bank-approved one.

7.2.3 Application access

I7: **Menu selection** – If the user is to manually initiate the payment on the device, access to the payment application should be enabled through an easy entry into the operator's menu selection. If private or personal data in the application are directly accessible through this menu (for example, memorizing the PAN), the access to this menu should be protected.

I8: Two open sessions – The payment application should be able to run independently of other sessions open at the same time. For example, the user should be able to switch between the purchase session and the payment session.

7.2.4 Key management

Key management includes all processes associated with the secure generation, transport, storage and destruction of keys of all users (corporate or private) and merchants in the transaction.

Independent of the implementation, failure in key management would constitute a security compromise or breach. Such failure would spell disaster for all the partners using the m-payment service.

I9: Generation and management of keys (life and storage of keys) – The key generation system must be approved or managed by the banks. There should be dynamic key management possibilities. It is very important for the partners (bank, telecommunication company, service provider, etc.) to set a common key management policy.

7.2.5 Customer identification/authentication data management

I10: **Generation and management** – The identification/authentication data (for example, PIN or password) generation must be managed or approved by the banks.

I11:Identification/authentication data security – The identification /authentication data should be secured offline and online according to banking practices (see also ECBS EBS 105, parts 2 and 3 and ISO 9564, especially part 4).

I12: Identification/authentication data blocking/unblocking – Repeated erroneous data entries must block the access to the payment application. Unblocking should only be allowed by secure methods that are controlled by the banks.

The solution shall provide a way to block the access of a specific customer to the payment application if, for example, fraud is suspected.

7.3 ACQUIRING FUNCTIONS

7.3.1 Merchant enrolment and authentication

A1: Mobile network connection – The merchant shall not be obliged to connect to a mobile network to accept m-payments. For example, initialisation of payment could be done on the web and redirected to a bank that processes the payment with a mobile connection.

A2: Merchant enrolment – The merchant enrolment and the merchant authentication that complies with the existing acquiring and authentication standards shall be under the control of the acquiring bank.

7.3.2 Clearing and settlement

A3: Use of existing bank rules and infrastructures – Clearing and settlement of transactions should be done in accordance with the existing bank payment rules and infrastructures.

7.4 TRANSACTION PROCESSING FUNCTIONS

7.4.1 Payment initialisation and selection

TP1: Payment presentation to customer – Regardless of the link used during commercial dealing/trading, the presentation of the payment request to the customer should be uniform and, as a minimum, include:

- the merchant identification (name)
- the amount
- the currency
- a unique identification of the transaction with this merchant

TP2: Selection of several means of payment – If several means of payment may be used, the available brands should be presented to the customer before authenticating a payment. As far as possible, the implementation should allow the customer to choose between different payment products within the payment application.

TP3: Payment brand/logo visibility – During the payment process the payment brand name or logo should be presented. As a minimum, the brand used shall be visible in the confirmation or receipt message.

TP4: Means of payment from different schemes/banks in the same payment application – The application should allow the registration of several and different payment schemes and brands.

TP5: Setting a default means of payment or setting the order of preferred means of payment in the menu bar – The customer should be granted the possibility of setting parameters for each means of payment, for example a default brand.

7.4.2 Customer authentication

TP6: Customer authentication – Whenever a customer (payment user or merchant/acceptor) accesses or uses personal information relative to the transaction, they shall be authenticated by the application.

7.4.3 Constitution of a transaction

For example, customer receives data and defines a transaction amount and currency**.**

TP7: Secrecy of the transaction – No mediating party should be able to decrypt the payment data that are transmitted encrypted.

7.4.4 Processing of authorisation

This includes the transmission of an authorisation request to a bank, a request for acceptance of transaction or an authorisation of the transaction. This process is internal to banks and, therefore, no external requirements apply.

7.4.5 User interface and information management

Most of the requirements for the user interface can only be described in conjunction with a specific technical implementation setting the frames for reasonable demands. Generally, any user interface must be designed with focus on user convenience and banking security.

However, some specific key requirements, partly derived from previous chapters, should be pointed out:

TP8: Validity of payments – Best efforts should be made to check the validity of the means of payment in the specific situation. Any payment scheme that is not registered by/for the customer or not accepted by the current merchant should preferably be omitted when using the payment application.

TP9: Customer's choice of the means of payment – If a customer has access to several payment schemes he should have the possibility to connect one or more of these to the mobile application at his own choice. The user should preferably also have the possibility to choose one as default means of payment.

TP10: Enrolment should allow capture of customer personalisation data that could be used in a payment situation – It is not convenient for the customer to enter information such as address and phone number in each mobile payment situation**.**

TP11: Time management – For security reasons, it is necessary to include time management in the user interface (for example, confirmation of payment amount in a defined time frame).

TP12: Transaction history – The user should have access to a reasonable transaction history.

TP13: Printing of transaction information – The user should be able to read and print all information regarding one or several transactions or receive explicit notification of the payment either delivered to the wireless device or to another electronic means (e.g. electronic mail).

7.4.6 Administrative functions

TP14: Certification of transaction - The messages concerning the payment transaction shall be authenticated.

TP15: Tracing and auditing payment transactions – In order to increase security, the solution must provide the capability to audit the main security functions and product functionality.

Certain processes in the transaction flow might require proof of intent from the customer, for example, entering the PIN or pressing an 'accept' key.

7.5 DATA ELEMENTS AND PROTOCOLS USED IN MOBILE PAYMENTS

The infrastructure of m-payments should take into account the capabilities and the limitations of existing networks. The displays of most devices are also limited in size and graphic capability, as well as in entering complex alphanumeric text messages. For these reasons, the payment application should restrict itself to a minimum set of data elements and a format that, for example, complies with the banking ICC specifications.

7.5.1 Protocols

Protocols within the banking environment shall conform to existing banking standards.

Protocols between the telecommunication company environment and the banking environment should use de facto standards such as UCP or SMPP.

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

7.5.2 Data elements

Appendix E describes data elements that may constitute payment-related messages, such as payment initiation, payment request, payment acceptance and payment confirmation.

The data elements derive from standards such as ISO 8583, EMV and CEN ENV1750/APACS 60. These standards will facilitate conversion into those commonly used by the banks.

Data elements are:

- action code
- alias card name
- amount transaction counter
- application transaction counter
- approval code
- date expiration
- merchant identifier
- merchant name
- message text
- MSISDN
- PIN
- POS entry mode
- primary account number
- print/display data
- protocol version number
- RND unpredictable number
- SIM-application ID
- SIM-ID number
- system trace audit number

- transaction certificate
- transaction currency code
- transaction date
- transaction sequence counter
- transaction type

7.5.3 Data element security requirements

Appendix E contains recommended security measures applying to each data element. Some are mandatory to ensure secrecy (encryption) in any communication link. Others require at least the use of a message authentication code (‘MAC’ing‘) in order to avoid tampering with the content.

Finally, encryption may be used as replacement for ’MAC’ing‘ if it already exists, and in addition ensures a similar authentication between entities.

7.6 SECURITY ANALYSIS

In a first phase, it is important to define the level of security needed. The risk analysis approach is proposed, based on a well-known method that defines step by step:

1. which data are sensitive to attacks
2. the functional security requirements for these sensitive data
3. possible attacks on these sensitive data
4. possible damage evaluation for these sensitive data if attacked
5. the level of expertise and investment that is necessary to handle each identified attack
6. how to get protection against each identified attack

Parties taking risks must conduct a risk analysis and must determine which functionalities are required (such as replay, repudiation or masquerade).

It might happen that part of the security must be provided by another party (for example, the telecommunication company). In such cases, a common and coherent approach is necessary to ensure transparency of real security offered to the market. For example, co-operation could lead to offering the market a “secure SMS”.

8 CONCLUSIONS

Based on the analysis of business and functional requirements for mobile payments by the banking sector in this report, the following conclusions are drawn:

- M-payments can be considered as a new access channel to existing payment infrastructures.

- Since m-payments are just in the early stages of deployment, no solution exists that meets all the requirements of the banking sector that are expressed in this report. In spite of the commitment on the part of the banks, this new technology will take time to reach critical mass.

- The ability to pay anytime and anywhere is an attractive proposition – for the users and for all other parties involved in the mobile payment business, such as banks, telecommunication companies and device manufacturers.

- In any m-payment scheme, the banks should provide the secure payment infrastructure, the telecommunication companies should provide the transportation network and the device manufacturers should provide the mobile device used to initiate and/or approve the payment. These are the main actors in the mobile payment environment.

- Banks prefer the four-box model as the underlying m-payment architecture. This option allows telecommunication companies to supply communication services and banks to supply payment services.

- In order to ensure secure mobile payments and take over the possible associated liability and payment guarantees, identification and authentication of the users are key services. Banks must approve and/or control these services whenever they are involved in the m-payment solution.

- Based on a truly inter-industry environment where partnership and co-operation must be present, a successful evolution of m-payments should result in a win-win situation for all involved parties. To achieve this, network independent and platform independent standards for security and interoperability are needed.

- Co-operation between the involved parties is both necessary and feasible – with benefit for all. This is reflected in the creation of common working groups and initiatives. These take into account local differences as well as strategic, commercial, marketing, and technical practices in
    - standardising efforts
    - harmonising messages to market
    - developing open solutions for both face-to-face and remote m-payments.

APPENDIX A — GLOSSARY OF TERMS

Below key definitions and concepts used in this report:

Acquirer — An entity providing transaction clearance services for the content provider. The entity and its supporting infrastructure are used synonymously. [MeT Definition]

Acquiring bank — A financial institution (or its agent, usually a card scheme), which acquires from the card acceptor the data relating to the transaction, and initiates that data into an interchange system. [ECBS Terminology]

AID — Application identifier

ARPU — Average Revenue per User

ATM — Automated teller machine

Authentication — Verification of identity [MeT Definition]

Bluetooth — A short-range radio technology designed to eliminate the need for cables between devices (for example, computer to printer connections achieved without wire and within a local area)

C2C — Customer-to-customer

C2B — Customer-to-business

CEN — (Comité Européen de Normalisation) European Committee for Standardisation

CEN/ISSS — (Comité Européen de Normalisation) European Committee for Standardisation/Information Society Standardisation System

Certificate database — Storage area in the PTD (Personal trusted device) for service certificates and root certificates [MeT Definition]

Consistent user experience (CUE) — A similar user experience among phones of different make and type. For example, the user experience of Web shopping shall be largely similar among MeT compliant phones CUE also includes consistency of user experience when using the same core function in different usage scenarios (user authorisation, for example, shall generate the same user experience in the usage scenarios Web shopping and retail shopping) [MeT Definition]

Content provider — The content provider provides goods and services to the user by hosting a content server [MeT Definition]

CRM — Customer Relationship Management

Customer — Person having subscribed to a domestic or international payment scheme of an issuing bank or institution

Dual chip – A payment solution in which the banking data (especially authentication credentials) and sometimes also the payment application is located on a bank-issued second chip, independent of the SIM. The second chip is semi-permanently installed in the mobile device by the end-user or a service provider.

Dual slot payment solution — a payment solution in which the device is equipped with a card reader in which the customer inserts his/her payment card when paying. In this model, part of the banking application resides in the SIM. In the future, the second reader may sometimes be dissociated from the mobile device, and dialogue with it using a wireless protocol (e.g. Bluetooth)

EEPROM — Electrically erasable programmable read-only memory

EMV — (Eurocard-MasterCard-Visa) Integrated Circuit Card (ICC) Specification for Payment Services

ETSI — European Telecommunication Standards Institute

Four-box model — The "four-box model" could be described as the banking version of open standards where the payer and the payee can interact although they have agreements with two different (and competing) banks. The reason for this is that the banks themselves have an agreement to participate in an enabling network (such as Visa, MasterCard, SWIFT, giro systems)

GMCIG — Global Mobile Commerce Interoperability Group (followed by the Mobile Payment Forum)

GSM — Global System of Mobile Communications (2^{nd} generation mobile network standard)

ICC — Integrated Circuit Card (chip card)

IDTV — Interactive digital television

IMSI — International mobile system identifier

Initialisation — Provisioning the PTD with one or more public-private key pairs and root certificates [MeT Definition]

ISO — International **S**tandards **O**rganisation

Issuer — An entity which has issued a service certificate for a key pair in the PTD. Typically this might be a bank or a credit card company. The entity and its supporting infrastructure are used synonymously [MeT Definition]

Issuing bank — a financial institution that issues a means of payment to its customers. A means of payment could be a real card, a virtual card, cash, virtual cash, etc.

J2ME — Java 2 Platform, Micro Edition

Local environment — An MeT-defined environment in which the PTD accesses content via local or personal area network [MeT Definition]

Macro payment — Typically those payments above €25

Medium payment — Typically those payments between €2 and €25

Merchant — a professional (or body) that is authorised to receive funds in exchange for the delivery of goods or services and that has established an agreement with a bank for accepting the said funds (means of payment). A merchant may operate a server (merchant's server), which may enable a customer to choose a means of payment and which stores the transaction for eventual compensation

MeT — Mobile electronic transactions. Technical framework and application guidelines for secure transactions with mobile trusted devices [MeT Definition]

Micro payment — Encompass the lowest payment values, typically under €2

Mobey Forum — Financial industry-driven forum, whose mission is to encourage the use of mobile technology in financial services

Mobile banking (m-banking) — A range of traditional banking services, including push payments, where a customer gives the order to the bank to execute a transfer of funds, conducted via a mobile trusted device

Mobile commerce (m-commerce) — Electronic commerce using a mobile trusted device as the customer device, e.g., a mobile phone [ECBS Terminology]

Mobile device (MD) — A set of seamlessly compatible hardware and software used interactively by a customer for making transactions wirelessly to other receiving parties which can be remote (e.g., server located on some communication network including the Internet) or face-to-face (e.g., electronic terminals like POS, vending machines, parking meters). Examples of mobile devices are mobile phones, PDAs and interactive laptops [See also mobile trusted device and personalised mobile trusted device]

Mobile payment (m-payment) **—** A mobile payment is not by itself a new payment instrument but an access method to activate an existing means of payment for financial transactions processed by banks between bank customers. An m-payment involves a wireless device that is used and trusted by the customer. M-payments may be card based or non-card based, in both the real and virtual world

Mobile Payment Forum (MPF) — Established by American Express, JCB, MasterCard and Visa end of 2001, the MPF is the follower of the GMCIG

Mobile trusted device (MTD) — A mobile device used by the customer to perform a transaction, which meets the standards for the schemes in which it will be used. This system may be owned by the customer or by a service provider or bank, e.g. PC, mobile phone, card reader provided by one's bank, etc. [see also mobile device and personalised mobile trusted device]

MSISDN — Mobile Subscriber Identification Service Digital Number

NFC — Near Field Communication

OTA — Over The Air

PAN — Primary Account Number, e.g. credit/debit card number

PDA (Personal Digital Assistant) — any small mobile handheld device that provides computing and information storage and retrieval capabilities for personal or business use

Personalised mobile trusted device (PMTD) — A mobile trusted device where personal customer information can be stored (through registration, e.g. of service certificates) that is used for his/her authentication [See also *mobile device* and *mobile trusted device*]

PIN — Personal Identification Number

PKI (Public Key Infrastructure) — a collection of hardware, software, policy and human roles that successfully bind a subscriber's identity to a key pair (public and private) through the issuance and administration of digital certificates throughout their "life-cycle" (creation, maintenance, archival records and destruction).

POS — Point of Sale

P2P — Person-to-Person

Registration — Provisioning the PTD with a service certificate is related to a public-private key pair residing on the PTD [MeT Definition]

Remote environment — An MeT-defined environment in which the PTD accesses content via a public mobile network [MeT Definition]

RF – Radio Frequency

Server — a computer program that provides services to other computer programs in the same or other computers

Service certificate — Certifies that a public-private key pair is valid for a specific service [MeT Definition]

SIM (Subscriber Identification Module) — a mobile operator's smart card that contains its subscribers' relevant data and applications (e.g. telephone application, message service, e-mail service, etc.)

SIM toolkit / SATK — the SIM Application Toolkit allows to develop applications on the SIM Card (ETSI: GSM 11.14) [MasterCard Europe definition]

Single SIM payment solution — a payment solution in which part or all of the banking data and sometimes of the banking application necessary to perform a payment resides on the SIM

SMS (Short Message Service) — the exchange of short messages between mobile trusted devices and possibly even computers in "store and forward" mode

SMPP — SMPP (**S**hort **M**essage **P**eer to **P**eer) is an open, industry standard messaging protocol designed to simplify integration of data applications with wireless mobile networks

SWIM — A SIM card with WIM application [MeT Definition]

Ticket — A downloaded object that shows that a fare or admission has been paid [MeT Definition]

TLS — Transport Layer Security

UCP — Universal Communication Platform

Usage scenarios — Examples of how MeT can be applied when providing services such as retail or Web shopping, Web banking, ticketing, etc. to end users [MeT Definition]

User — The person in possession of a PTD and able to verify him/herself to the PTD [MeT Definition]

User interface — The man-machine interface between the user and the PTD [MeT Definition]

USSD — Unstructured Supplementary Service Data, the exchange of short messages between mobile trusted devices and possibly even computers in "dialogue" mode

VRU — Voice Recognition Unit

VNO — Virtual Network Operator

Wallet — Something that contains a means of payment, e-commerce wallets are PC software, which contain the necessary sensitive information to handle payment transactions over the Internet [MasterCard Europe definition]

WAP (Wireless Application Protocol) — a specification for a set of communication protocols to standardise the way that wireless devices (e.g. mobile phones) can be used to access information on the Internet

WIM (WAP Identity Module) — A tamper-resistant device which is used in performing WTLS (Wireless Transport Layer Security) and application level security functions, and especially, to store and process information needed for user identification and authentication [WAP Forum Definition]

WIM card — WIM implemented on a smart card [MeT Definition]

WPKI — Wireless PKI, PKI optimised for WAP [MeT Definition]

WTLS — Wireless Transport Layer Security, the WAP equivalent of TLS [MeT Definition]

APPENDIX B – MATRIX OF M-PAYMENT SOLUTIONS (SWOT ANALYSIS)

The analysis focuses on m-payment device implementation models based on chip-based and chip-independent solutions:

- chip-based solutions:
    - single SIM
        - bank issued
        - operator issued
    - dual chip
    - dual slot
- chip-independent solutions
    - one-time or permanent passwords
    - Java based

All of the above-mentioned solutions can either be local-client-based and/or server-based.

These models may to a certain degree assume a centralised architecture. Some of the functions (for example, authentication) or applications (for example, choice of means of payment) provided to the user may be located at a wallet server instead of inside the mobile device itself. The existence of a wallet server, managed directly by banks or by a third party, may change the degree of centralisation of the system and may simplify its rollout and the evolution. Provided that communication links are safe and that the server is tamper-proof and secure, the requirements of the banks are unlikely to change.

M-Payment solution	Strengths	Weaknesses	Opportunities	Threats
CHIP-BASED				
1. a) Single SIM • Bank-issued chip with payment application (including operator's SIM functionality)	1. End-to-end security with application possible 2. Existing handsets can be used 3. Customer loyalty to payment application 4. Issuer brand visible in digital format 5. Banks are in control of the chip.	1. Close logistics required with the operator(s) 2. Higher costs for issuing banks (multi-application chip, new chip technology) 3. Duplication of bank's chip and application management, possible introduction of new processes 4. Enhanced security needed (SIM/WIM chips not yet evaluated) – current operator SIMs do not necessarily meet banks' security standards 5. This model does not exist today 6. Customer tied to ONE bank and ONE operator (if banks do not become operators' retail outlets selling every operators' contracts – and even then not free of charge for consumer to change operator or bank as a new SIM costs) 7. Difficult distinction between both partners in CRM (service confusion) and in agreement on who is the registration authority	1. Offers possibility to provide maximum level of security and functionality, since the bank controls the platform 2. Necessity to co-operate with telecommunication company operators on continuous basis or to become a VNO (banks gain the mobile phones as electronic payment terminal devices and the telecommunication companies gain sound m-payment services relying on the bank payment systems enabling m-commerce and increasing airtime and data traffic)	1. Not likely to be widely accepted by operators and thereby will not become a "global solution" 2. PIN will be entered into a device which is not tamper evident, nor complying with EMV requirements. The danger of eavesdropping and tapping is, however, limited as the device is in the personal possession of the cardholder. 3. Need to develop standards

M-Payment solution	Strengths	Weaknesses	Opportunities	Threats
CHIP-BASED				
1.b) Shared SIM ▪ Operator-issued including bank certified payment application	1. End-to-end security with application possible 2. Existing handsets can be used 3. Customer loyalty to payment application 4. Issuer brand visible in digital format controlled by application	1. Close logistics required with the operator(s) 2. Separate application development required per SIM/chip type and producer. Standard application possible in Java 3. Commercial agreement needed between bank and operator on win/win negotiation 4. Enhanced security needed (SIM/WIM chips not yet evaluated) – current operator SIMs do not necessarily meet banks' security standards 5. Customer tied to ONE wallet provider and ONE operator. Agreements may be made with several banks 6. Difficult distinction between both partners in CRM (service confusion) and in agreement on who is the registration authority. 7. Possibility of becoming global solution (even if differences may occur between operators in SIM and OTA set-up)	1. Appropriate for both micro payments where a limited level of security is needed and for macro payments requiring higher security from SIM application and system set-up 2. Necessity to have close partnerships with telecommunication companies on continuous basis (banks gain the mobile phones as electronic payment terminal devices and the telecommunication companies gain sound m-payment services relying on the bank payment systems enabling m-commerce and increasing airtime and data traffic)	1. Banks may lose control on applications that reside on the SIM. 2. Price of operators' real estate might increase over time 3. PIN will be entered into a device which is not tamper evident, nor complying with EMV requirements. The danger of eavesdropping and tapping is, however, limited as the device is in the personal possession of the cardholder. 4. Need to develop standards

M-Payment solution	Strengths	Weaknesses	Opportunities	Threats
CHIP-BASED				
1.c) Single SIM ▪ Operator-issued containing no bank payment application or data	1. End-to-end security based on SIM verification 2. Existing handsets and SIMs used 3. Clean separation of telecommunication company and banking business and infrastructures 4. Interoperability between telecommunication company and banking systems 5. Co-operative approach of banks and telecommunication companies 6. Open solution (multi-bank, multi-operator, multi-merchant)	1. Comprehensive agreements regarding business, commercial, legal, security and technical issues needed between the telecommunication companies and the banks	1. This approach could be appropriate for micro-payments	1. Risk that the co-operation cannot be established in a short time (i.e. long time-to-market)

M-Payment solution	Strengths	Weaknesses	Opportunities	Threats
CHIP-BASED				
2.) Dual chip • internal second slot (bank issued second chip and payment application)	1. End-to-end security with application possible 2. Clear distinction on the technological side 3. Distinction in each partner's responsibility of CRM (if obvious for the customer) 4. High cardholder loyalty/customer retention 5. Customers need double contract 6. Provided open access to application possible via operators' WAP or OTA platform, no continuous co-operation needed with external parties. No agreement with handset vendors needed 7. Issuer brand visible in digital format controlled by application (brands may also appear on plastic before chip placed in the mobile device) 8. Banks have more control and are not limited by the choices of a network operator	1. Not in production today 2. New mobile devices/handsets required. Increased costs must be carried by customer or by bank subsidies 3. Higher costs for issuing banks since they must invest in second ICC/WIM (multi-application chip, new chip technology) 4. Duplication of banks' chip, production and introduction of new processes	1. Offers possibility to provide maximal level of security and functionality since the bank controls the second chip platform	1. Involvement and commitment of handset vendors is critical (up front) 2. Although there are two separate chips they have to communicate in an "open handset", danger of eavesdropping and tapping 3. PIN will be entered into a device which is not tamper evident, nor complying with EMV requirements. The danger of eavesdropping and tapping is, however, limited as the device is in the personal possession of the cardholder. 4. Need to develop standards and convince manufacturers to accept and use them

M-Payment solution	Strengths	Weaknesses	Opportunities	Threats
CHIP-BASED				
3. a. Dual slot (external slot for full sized banking card. Bank chip and SIM independent of each other [like in the dual chip case]) ***Note: Not developed yet.***	1. End-to-end security with application possible 2. Customer flexible in choosing any bank, any card, any operator 3. Bank's brand visible both on plastic and digitally 4. Clear distinction on the technological side 5. Distinction in each partner's responsibility of CRM 6. High cardholder loyalty / customer retention 7. Customer needs double contract 8. No continuous co-operation needed with external parties like operators or handset vendors 9. No need to support the SIM application (less help desk calls to support) 10. Customisation and technological improvement easier	1. New mobile devices/handsets required. Increased costs must be carried out by customer or by bank subsidies 2. Not very convenient / user friendly when e.g. calling 3. As phones get smaller, extra slot for full size cards is difficult to fit into phones / may be difficult to sell "bulky banking-phones" 4. Card reader and associated applications rely on operators' willingness to accept more complex devices 5. Would not add any value to local payments	1. Offers possibility to provide maximum level of security and functionality, since the bank controls the platform	1. PIN will be entered into a device which is not tamper evident, nor complying with EMV requirements. The danger of eavesdropping and tapping is, however, limited as the device is in the personal possession of the cardholder. 2. Although there are two separate chips, they have to communicate in an "open hand-set", danger of eavesdropping and tapping 3. Involvement and commitment of device manufacturers is critical (up front) 4. Need to develop standards and convince manufacturers to use and accept them

M-Payment solution	Strengths	Weaknesses	Opportunities	Threats
CHIP-BASED				
3. b. Dual slot with SIM application toolkit (external slot for full sized banking card, i.e. the existing mobile phones, developed with SIM application toolkit [SATK])	1. End-to-end security with application possible 2. Bank's brand visible both on plastic and maybe digitally 3. "Marketing" or "perceived" distinction on each party's responsibility of CRM	1. New mobile devices/handsets required. Increased costs must be carried by customer or by bank subsidies. 2. SAT means that SIM is "the master and the other card is the slave"; the actual applications sit on the SIM chip, not on the bank-issued card 3. Separate application development required per SIM chip type 4. Commercial agreement needed between bank and operator 5. Not very convenient/user friendly when e.g. calling 6. Phones get smaller, extra slot for full size cards is difficult to fit into phones, may be difficult to sell "bulky banking-phones" 7. Enhanced security needed (SIM chip not yet evaluated) – current operator SIMs don't necessarily meet banks' security standards 8. Customer tied to ONE bank and ONE telecom operator 9. Card reader and associated applications rely on operators' willingness to accept more complex devices 10. Would not add any value to local payments	1. Appropriate for micro-payments, where no high level of security is needed 2. Necessity to have close partnerships with telecommunication companies on continuous basis (banks gain the mobile phones as electronic payment terminal devices and the telecommunication companies gain sound m-payment services relying on the bank payment systems enabling m-commerce and increasing airtime and data traffic)	1. Banks may lose control on applications that reside on the SIM 2. Price of operators' real estate might increase over time 3. PIN will be entered into a device which is not tamper evident, nor complying with EMV requirements. The danger of eavesdropping and tapping is, however, limited as the device is in the personal possession of the cardholder. 4. Although there are two separate chips, they have to communicate in an "open handset", danger of eavesdropping and tapping 5. Involvement and commitment of device manufacturers is critical (up front) 6. Need to develop standards and convince manufacturers to use and accept them

M-Payment solution	Strengths	Weaknesses	Opportunities	Threats
CHIP INDEPENDANT				
4. One-time or permanent passwords over any connection medium	1. Cheap (if expensive tokens not in use) 2. Well-proven 3. Operator independent 4. Existing handsets can be used without changing anything on the SIM 5. Customer relationship controlled by banks	1. End-to-end security not possible as no dedicated application. Security level is poor or medium – also as seen from customer point of view 2. Current handsets do not easily facilitate text 3. User has to carry extra tokens or password lists to enable higher security 4. Customer tied to one wallet provider (neutral platform controlled by banks and operators)	1. With static passwords could be appropriate for payments where no high level of security is needed 2. If e.g. password lists or extra tokens in use, appropriate for higher value payments, but less convenient 3. Fast and low cost deployment possible given low entry barrier (no change of phone or SIM) 4. Possibility of becoming global solution given its international compatibility and co-operation requirement between both industries (de facto standard) 5. Leverages to a maximum the existing payment infrastructure of banks	1. User habit may not be created when usage is not convenient or trusted 2. Necessary to have close relationship with mobile operator on an ongoing basis (if solution implemented on the operator side or co-owned). 3. Needs to align banks and mobile operators on co-owned neutral platform (as above)

M-Payment solution	Strengths	Weaknesses	Opportunities	Threats
5. Java based application in mobile device/handset (e.g. MIDP, J2ME)	1. Cheap (if expensive tokens not in use) 2. Operator independent 3. Facilitates a wide range of services and easy update 4. Managed by the customer	1. Enhanced security needed 2. End-to-end security depends on J2ME standard 3. Existing handsets do not easily facilitate J2ME	1. Banks may provide Java applets to their customers for download 2. JAVA is an emerging technology	1. PIN will be entered into a device which is not tamper evident, nor complying with EMV requirements. The danger of eavesdropping and tapping is, however, limited as the device is in the personal possession of the cardholder. 2. Download and residence of uncertified applications 3. Need to develop standards and convince manufacturers to use and accept them

APPENDIX C – M-PAYMENT SCHEMES IN EUROPE

AUSTRIA

System, Partners:	1. Paybox (Deutsche Bank 50%), 2. Paysafecard (BAWAG, Commerzbank, Oesterreichische Post)
Launch Date:	1. Paybox: September 2002, 2. Paysafecard: YE 2000
Type of Payment:	1. Paybox: Non-bank and non-card based model, NoVRU (voice recognition unit) and SMS, customer confirms payment with PIN, PIN is transmitted by DTMF, settlement through bank transfer (direct debit, Deutsche Bank handles the transfer between banks involved) 2. Paysafecard: Micro payments and Internet payments, Paysafecard is a pre-paid card to be bought in specialised shops. There are several cards available with different amounts loaded, each card has a 16 digit PIN. For making payments, the customer needs his mobile and the PIN.
Comments:	Paybox: Merchants sign up with Paybox, using it in a role analogous to a credit card merchant/acquirer. Merchant pays between 500 € and 2500 E for software, a yearly fee of 100-300 € and 3% per transaction (depending on contract).

BELGIUM

System, Partners:	Mobile Banxafe (Banksys, Mobistar)
Launch Date:	3rd quarter 2002
Type of Payment:	Mobile Banxafe: Authentication applet on telecommunication company SIM (STK JAVA applet with a small part in native code – size: 12 KB in EEPROM). The GSM provides authentication to access a server-based wallet containing debit/credit cards. Signature requests and responses between the SIM applet and the authentication server use SMS. Applet designed to provide easy enrolment, which can be done at ATM and POS terminals using the bank card and the PIN. Mobile Banxafe is designed to support multi-requester keys, multi-applications and multi-channels (clear distinction between shopping/banking and authentication phase – shopping/banking done from GSM, TV, Internet, telephone and authentication via mobile Banxafe on GSM).

Comments:	The authentication/wallet server as well as the SIM STK applet is under the control of the Belgian banks. Mobistar will launch the SIM card with Banxafe application later in 2002. They will first target prepaid users who will use mobile Banxafe to pay for top-up of prepaid airtime. In the beginning of 2003, this will be generalised to all Mobistar customers for all mobile payments as well as mobile banking. This solution is open to all mobile operators in Belgium. As the mobile Banxafe solution requires the hosting of an STK applet on the SIM card, an agreement must be reached with the telecommunication company. As the applet is developed in JAVA, the solution is easily interoperable from one SIM manufacturer to another.

DENMARK

Systems, Partners:	PBS International A/S, card issuers (banks) and telecommunication companies
Launch Date:	Top-up of pre-paid airtime (June 2000), Open Mobile Payments- mPay (June 2001)
Type of Payment:	SIM "bank"-application (SAT2+) ensures EMV-based end-to-end cryptographic relationship with mPay server that holds the consumer wallet with relation to payment cards. Card data captured when consumer subscribes. All telecommunication company's SIM cards will hold a sleeping application or a secure socket, which is activated by subscription. Each payment is approved by means of secure offline PIN at the mobile trusted device. Pre-paid airtime is activated by menu selection at the m-terminal. Open Mobile Payments, mPay, are remote payments initiated on the Web, WAP and via traditional phone order. Authorisation requests and captures that are generated by the merchant/content provider are using existing infrastructures and hold only the mobile phone number.
Comments:	The solution offers, apart from user convenience, a reduced risk of revealing card numbers and an optimal cardholder verification. Developed by PBS in co-operation with Orange. Server is being installed at PBS in January 2002, which will allow all telecommunication companies to join. Potential mobile phones only need a new SIM. Figures on activated subscribers, mPay enabled merchants and transaction volumes are not available.

FINLAND

Name, Main Partners: 1. Nordea, Nokia, Visa, 2. Nokia, IBM, Luottokunta, Radiolinja

Launch Date: 24 September 2001

Type of Payment: 1. Mobile phones to be used for payments with inserted 'Open Platform' chip card issued by Nordea. Mobile phones will help to make purchases and pay using a Nordea issued plug-in size chip card, which resides on a special chip card reader inside the phone. The phone has an additional reader for a chip card. Visa Electron transactions can be done by using this additional chip with WIM. The m-commerce concept tested in this project is called dual chip, which consists of a chip card that can be issued by a bank and a GSM SIM card. In the pilot, the chip card, which accommodates a WIM application, is inserted into the WAP enabled mobile phone, providing the customer with integrated payment functionality. Wireless authentication and signature method is based on WAP and WIM specifications. WAP is used as a transport layer.

2. The players developed secure mobile transactions using the wallet for transferring payments/loyalty program information and WIM for making non-repudiated transactions to demonstrate an m-wallet solution supported by digital POS and WPKI. Nokia will provide the pilot phones with wallet applications & WIM functionality support including a GSM SIM/WIM (SWIM) card. Further:

Radiolinja (Finnish telecom) issues a chip card, adhering to WAP Forum and WIM specifications, supports standard mobile public key functionality, offers digital signature capability and certificate database. It will also serve as network operator and TTP.

Luottokunta (issuing/acquiring Visa and Eurocard/MasterCard cards, jointly owned by Finnish banks) to provide digital POS (for merchants), which can validate WPKI signatures. Digital POS was developed with IBM Finland.

Radiolinja's WPKI signatures and certificates simultaneously with credit card payment authorizations received from the WAP stores via Internet.

IBM to act as system integrator and provide payments infrastructure, comprising WebSphere commerce suite and WebSphere payment manager.

FRANCE

Name, Main Partners:	GIE Cartes Bancaires, banks and telecommunication companies (Orange, Cegetel & Bouygues) Main Others retailers: France Telecom, Electricité de France, Alapage, 3 Suisses, Interflora
Launch Date:	September 2000
Type of Payment:	Dual slot model, 3 SMSs, Bank application in SIM, PIN presentation and certification of transaction by bankcard, usage of 45 million bank smart cards. Mail order and virtual POS. For dual-slot phones where users insert smart CB credit card, security lies in the credit card chip. SMS used for order confirmation only. Also uses SIM toolkit card.
Comments:	700 000 dual slot mobile phones, up to 3000 transactions/day, growth : 20%/month, mobile telecommunication companies: reloading prepaid accounts, other retailers: payment of invoices when buying through Internet, telephone, paper catalogue, coupons, Minitel, etc.

GERMANY

Name, Main Partners:	1. Paybox (Deutsche Bank 50%), 2. Pay-it-mobile (Gesellschaft fuer Zahlungssysteme, E-Plus, Accenture, Materna), 3. Paysafecard (BAWAG, Commerzbank, Oesterreichische Post), 4. Street Cash (Inatec), 5. Tanpay (Antros), 6. Genion m-payment (VIAG Interkom, Hypo-Vereinsbank, Telecash)
Launch Date:	1. Paybox: May 2001, 2. Pay-it-mobile: February 2000, 3. Paysafecard: May 2001, 4. Street Cash: October 2000, 5. Tanpay: 2001, 6. Genion m-payment: March 2001
Type of Payment:	1. Paybox: Non-bank and non-card based model, NoVRU (voice recognition unit) and SMS, customer confirms payment with PIN, PIN is transmitted by DTMF, settlement through bank transfer (direct debit, Deutsche Bank handles the transfer between banks involved) 2. Pay-it-mobile: Internet based, PIN presentation, SMS, wallet server at GZS. 3. Paysafecard: Micro payments and Internet payments, Paysafecard is a pre-paid card to be bought in specialised shops. There are several cards available with different amounts loaded, each card has a 16 digit PIN. For making payments, the customer needs his mobile and the PIN. 4. Street Cash: SMS and PIN based. 5. Tanpay: SMS based, mobile and TANs (Transaction Numbers). 6. Genion m-payment: System is open for VIAG Interkom customers - mobile WAP and additional PIN, SMS. Customer receives a TAN for every transaction to be put on a payment page, the payment itself is done by direct debit, debit or credit card.

Comments:	Paybox: Merchants sign up with Paybox, using it in a role analogous to a credit card merchant/acquirer. Merchant pays between 500 € and 2500 E for software, a yearly fee of 100-300 € and 3% per transaction (depending on contract). Pay-it-mobile: Positioned as neutral link between banks, card companies, telecommunication companies and merchants, only available for Internet/WAP merchants, no figures available (it is assumed that merchants are charged a fee of 2% per transaction). Street Cash: merchant pays 275 € once 2% or min. 0,30 € per transaction, no other figures available. Tanpay: No costs for the customer, merchant pays 2,5% per transaction. Genion m-payment: pilot was running with 1000 customers and 7 online shops.

ITALY

Name, Main Partners:	Bankpass Mobile (ABI)
Launch Date:	1st Quarter 2003
Type of Payment:	SIM-/handset-/bank-/operator-independent model. Customer inserts in a wallet his debit (PagoBancomat) and credit (Visa and MasterCard) cards, accesses them by entering a PIN and uses them in a SMS based transaction.
Comments:	Bankpass Mobile has been developed by the Italian banking system as the standard model for m-payments. This system can be used both in C2C and C2B transactions.

NORWAY

Name, Main Partners:	Smartpay, DnB – Telenor
Launch Date:	27 October 2001
Type of Payment:	Mobile phone payment, account, credit card and purse.
Comments:	Telenor's SmartPay platform provides full online access to bank accounts and credit cards with the use of digital certificates. The user interface is simplified with the use of PIN codes.

NETHERLANDS

Name, Main Partners:	Postbank m-banking (ING/Postbank, Telfort and Genie)
Launch Date:	July 2001 (mobile banking including top-up of pre-paid airtime)
Type of Payment:	A strong combination of a SIM based application toolkit ("bank" application) and a WIM application, both controlled by the bank, delivers the following functions: • Direct prepaid airtime balance top-up, initiated via a convenient menu interface on the mobile phone. • Secure SMS that enable the bank to communicate in a secure way with the customer, send a message to the customer, asking the customer to input date and require the customer to confirm the transaction. • WIM provides digital signing within WAP applications. • Digital signing via SMS, using the WIM signing function via SMS, enables for instance the use of the digital signing function on the internet. An offline PIN, called m-code, protects access to these functions. Currently, the functions are used for direct prepaid top-up and as a support to a WAP m-banking application for account access and direct payments. Usage for payment is envisaged in a server-based wallet set-up. It has been implemented in a demonstration set-up.
Comments:	The current number of users of the system is 500.000. Figures on top-ups are not available. The main aims of ING/Postbank are to open the mobile channel as a bank channel and more specifically to use the mobile phone to strengthen the customer/bank relationship.

SPAIN

Name, Main Partners:	1. Paybox, 2. Mobipay
Launch Date:	1. Paybox: November 2000, 2. Mobipay: May 2002
Type of Payment:	1. Paybox: Non-bank and non-card based model, VRU (voice recognition unit), PIN presentation, settlement through bank transfer. (Deutsche Bank handles the transfer between banks involved). 2. Mobipay: Collaborative model incorporating banks (80% of Spanish banks), all mobile operators, payment processors and VISA Spain. Card based model that does not require any change of the phone or on the SIM. Current SIM is associated to a wallet with various payment cards incorporated. Based on USSD (Unstructured Supplementary Service Data), messaging technology allowing on-line interactive payment session with speed and integrity. The client confirms payments with his PIN. Solution covers macro and micro payments for both face-to-face and remote, like Internet, pre-paid top-up or order taking. Mobipay acts as a payment activator of existing payment products and brands (e.g. VISA, MasterCard, etc). It is being commercialised directly by the participating banks.

Comments:	1. Paybox: 500 POS and 250 Internet shops. 2. Mobipay: Deployed initially in Valladolid where it counted with over 1,800 merchants (85% acceptance rate) and close to 5,000 clients prior to the national roll-out. Includes BBVA, SCH, Vodafone, Telefónica and Amena as shareholders. The system is being launched internationally.

SWEDEN

Name, Main Partners:	1. Paybox, 2. Mint
Launch Date:	1. Paybox: 2001, 2. Mint: 2001
Type of Payment:	1. Paybox: Card-, bank-, handset- and operator-independent model. Transaction authorised with a voice call from Paybox where the customer enters a 4-digit PIN. Bank account based settlement, in Sweden currently handled by Den Danske Bank. 2. Mint: Account based model, pre-paid or post-paid. Mint account and payment to Mint via the giro system. Mint as front-end to non-bank card account soon to be launched. Transaction authorised with a phone call to Mint using number recognition (PIN usage see below).
Comments:	1. Paybox: About 250 Internet shops in Sweden. The customer can do cross-border purchases (over 10000 acceptance points in 5 European countries). Other applications are pre-paid top-up, mobile voice shop and P2P payments. 2. Mint: Most successful application is parking payments in Stockholm (city and surroundings), plate number pre-registered, no PIN. Accepted at a number of POS in central Stockholm (merchant plastic card and customer PIN used in POS terminal). Mint also provides P2P payments (password needed). Internet payments announced but not launched yet.

SWITZERLAND

Name, Main Partners:	Payserv AG, CS, UBS, Viseca, Europay (Switzerland), Swisscom, Sunrise, Orange
Launch Date:	Mid 2003
Type of Payment:	The architecture follows the server-based model. The consumer accesses the wallet server from his mobile handset via the mobile network operator's m-payment gateway. As bearer protocol the main focus is on USSD which facilitates an interactive electronic communication between the consumer, the merchant and the wallet server and is available in the whole mobile equipment base deployed. Authentication is achieved by a 4-12 character mnemonic m-PIN and the IMSI or a unique alias thereof. In the enrolment process the cardholder is authenticated by his ec/Maestro card and ec-card PIN. He then chooses an m-PIN (different from ec-card PIN). The SIM card of his handset is then linked to the respective ec/Maestro card. Change of m-PIN, renewal or replacement of the ec/Maestro card and change of operator and SIM card are handled by the solution.

Comments: The initial implementation of the m-payment focuses on the 3.5 mio. ec/Maestro cards widely used in Switzerland. The marketing plan foresees a rapid enablement of a significant part of the card base. No special mobile equipment or SIM cards are required. No card or bank data or applications are stored in the handset or on the SIM card.

UNITED KINGDOM

Name, Main Partners: 1. Vodafone M-Wallet, 2. Paybox (Deutsche Bank hold a 50% share in Paybox, Debitel AG hold a 4.8% share in Paybox)

Launch Date: 1. Vodafone M-Wallet: Trials commenced in Q1 2002, 2. Paybox: Launched in UK in September 2001

Type of Payment: 1.Vodafone M-Wallet: Vodafone is developing a mobile payment system to allow users to pay for small value items using their phone and their operators are likely to follow. Trial users will be identified by their mobile trusted devices and will enter a PIN code to confirm and authorize each transaction using established credit and debit cards. The customer's payment and address details are kept in an electronic wallet so that card details do not need to be entered for each transaction.

2. Paybox: Users pre-register with Paybox, giving personal information, a mobile phone number and filling in a direct debit mandate to enable the payment process. Merchants sign up with Paybox, using it in a role analogous to a credit card merchant acquirer.

To make an Internet payment (e.g. via a PC), a user selects "Paybox" as the payment method and enters their mobile number on the merchant web site. The data is passed to Paybox, which performs an ID and credit check before ringing the mobile number given. The system relies on the phone. SIM's network identity code to establish that it is connected to the correct user's phone. The user is prompted by an automated voice to confirm the transaction by entering their Paybox PIN directly on the keypad. Note that due to the call-back process the Paybox system does not integrate very well with WAP-based m-commerce models.

An acknowledgement is sent to the user through SMS – this is the only time it is used. Transactions are estimated to take around 30 seconds to complete.

Comments: 1.Vodafone M-Wallet: Mobile payment system that allows customers in the UK, Germany and Italy to pay for goods using a cell phone. If trials are successful, the company hopes to launch a larger public trial later in 2002. Eventually Vodafone aims to make the service available to 50m customers across the UK and Europe.

Vodafone aims to eventually broaden the scope of the system to enable point of sale transactions.

2. Paybox: Paybox charges merchants a fee of between 2-5% for processing each transaction. User bank accounts are then debited by Paybox. In the UK Paybox has signed up around 50 merchants, although no separate figures for customers are available.

Its ambition is to become the "VISA of wireless transactions". They are looking to partner with an institution, which provides "real time accounting"

Paybox is actively inviting telecommunication companies, banks and other interested parties worldwide to become part of its network as a strategic partner and potential shareholder.

APPENDIX D - PAYMENT MODELS (ARCHITECTURES)

Payment models can be described using the 'box model' concept, which is a conceptual description of the necessary architecture to enable a transaction between the payer and the payee. Each 'box' represents an actor in the payment process. The following functions are to be addressed in the entire payment system:

- Identification – authentication of parties
- Processing of payment orders
- Transfer of value

Traditional payment models can be described as four-box-models (since they comprise a merchant, a merchant's bank, a customer and a customer's bank). This framework is often considered as the preferred payment model, since universal means of payment function this way, whether or not card payments are used.

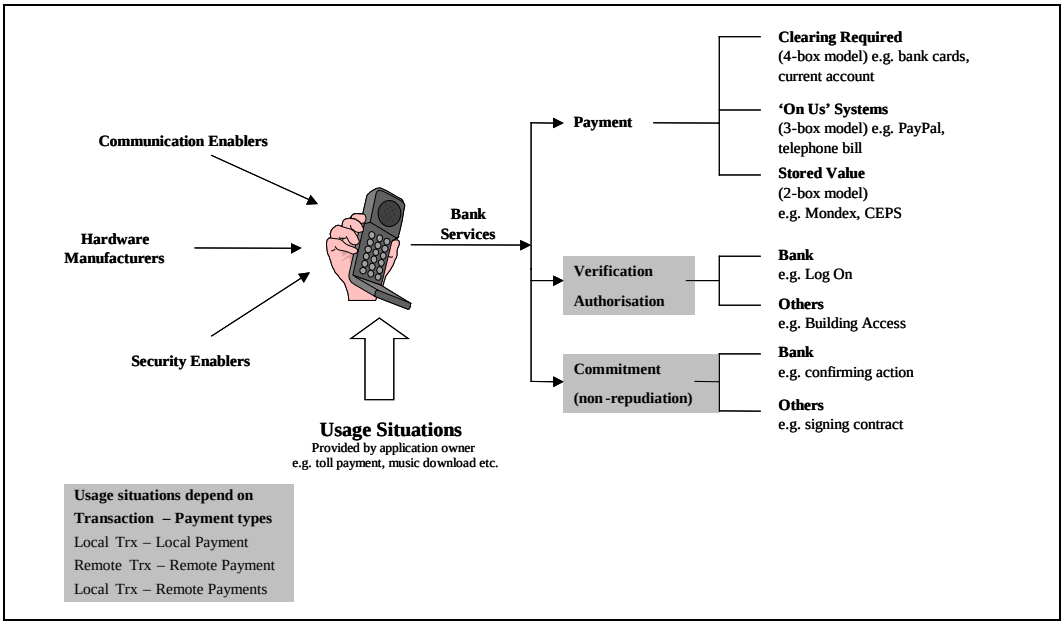
Some electronic and m-payments can be based on three-box models (that means that merchant and customer have accounts at the same bank or institution). Such solutions either have to be domestic (with relation to a specific country or region) or 'walled-gardens'.

'Technical boxes' may appear between the banks (as well as between the bank and its customer/merchant). Such boxes are not recognised if they can be seen as service providers and if they do not play any role in terms of risk and liability for individual transactions.

The diagram below shows examples of box models and identifies the three enablers of m-payments for which banks are logical providers, which are:

- payment
- verification/authorisation
- commitment.

To complete the model, communication, hardware and security enablers are also included:



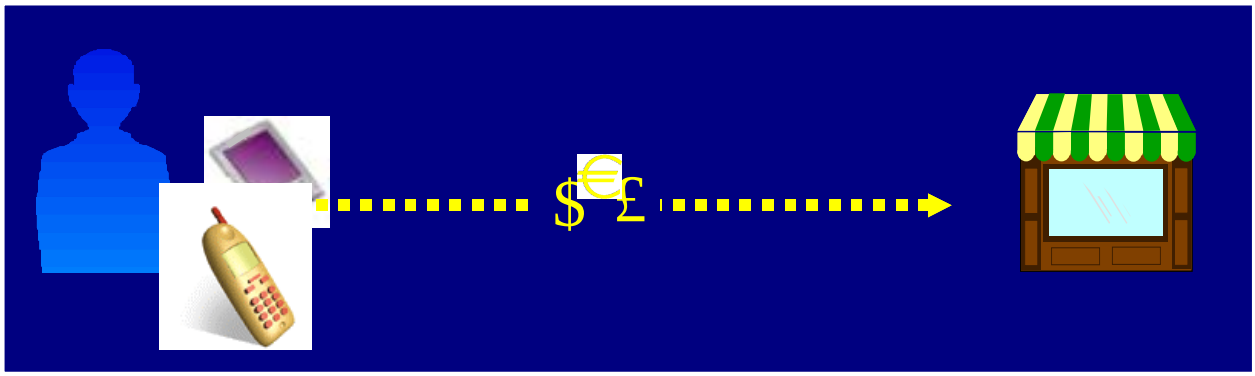
The box models

This section describes in more detail the box models introduced above. In this context, the following abbreviations are used:

SID: Sender Identification / Authentication
RID: Receiver Identification / Authentication
PO: Payment order
FT: Financial transfer.

Two-box model

The minimum payment scheme, the two-box model, involves two parties: A merchant and a customer:



This model is characterized by the following:

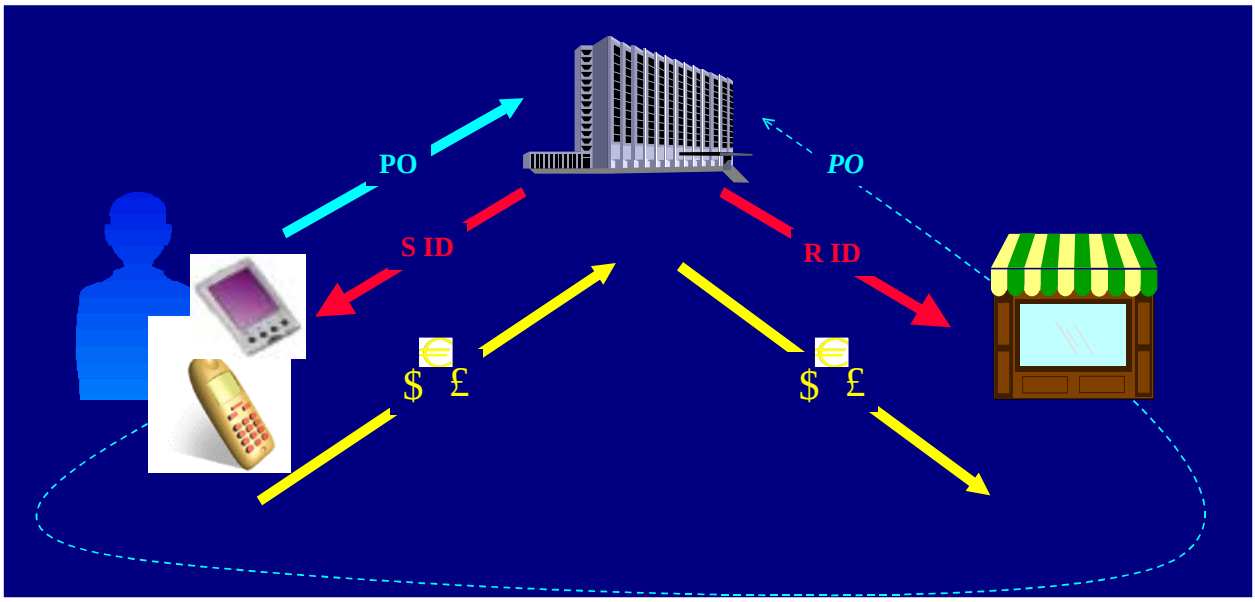
- Two parties involved: a merchant and a customer (no third party)
- No authentication of parties (replaced by local authentication of money transferred)
- Direct payment (no payment order)
- Immediate payment (no payment delay).

An example of this payment model is an e-purse like Mondex where the receiver, without any book keeping by the purse issuer, can immediately spend the electronic money.

Three-box model

In this model, a third party is necessary either for one or more of the following activities:

- Authentication
- Account keeping



Several examples can be assimilated to this model like:

- Non-bank payment schemes (American Express, Diners)
- Third party money transfer schemes (PayPal, Kiosque)
- Private bank schemes in which merchant's and customer's bank are the same
- E-purse (Most electronic purses are best described using this model, although purses issued by a joint venture of banks are rather like four-box solutions).

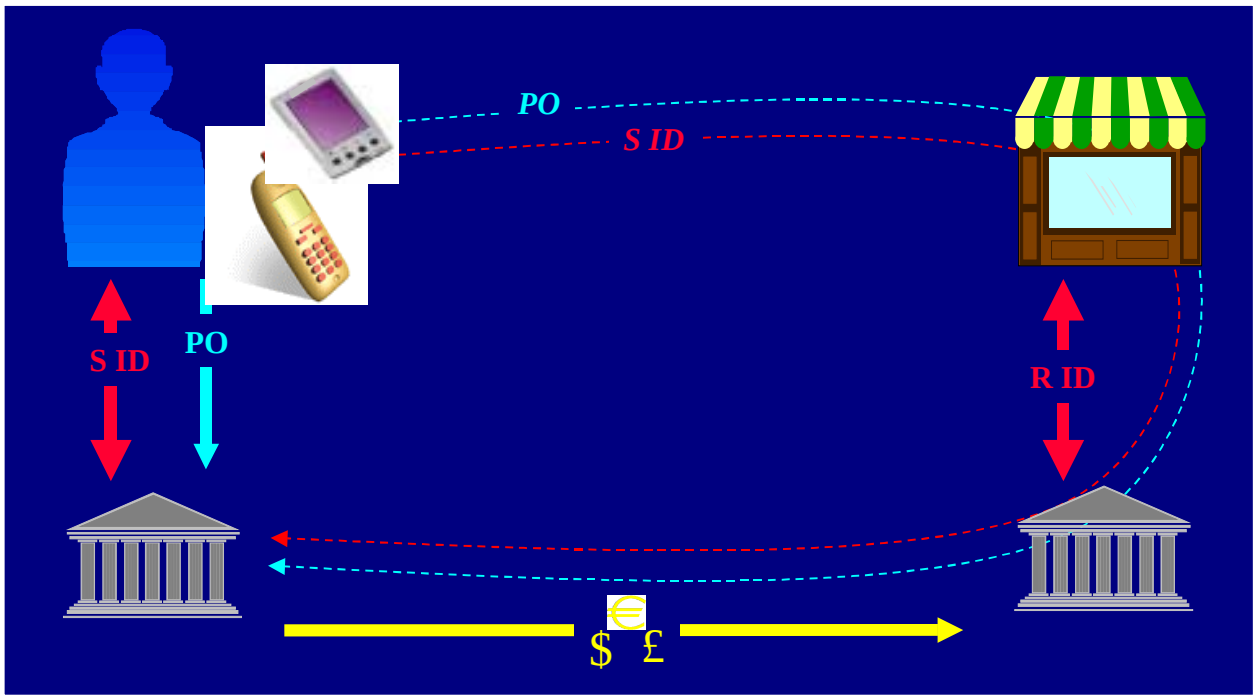
The bank's role is peripheral, that is to manage bank accounts and to transfer money between each party's accounts.

Four-box model

In this case, the preferred payment model, the customer and the merchant each have their own bank.

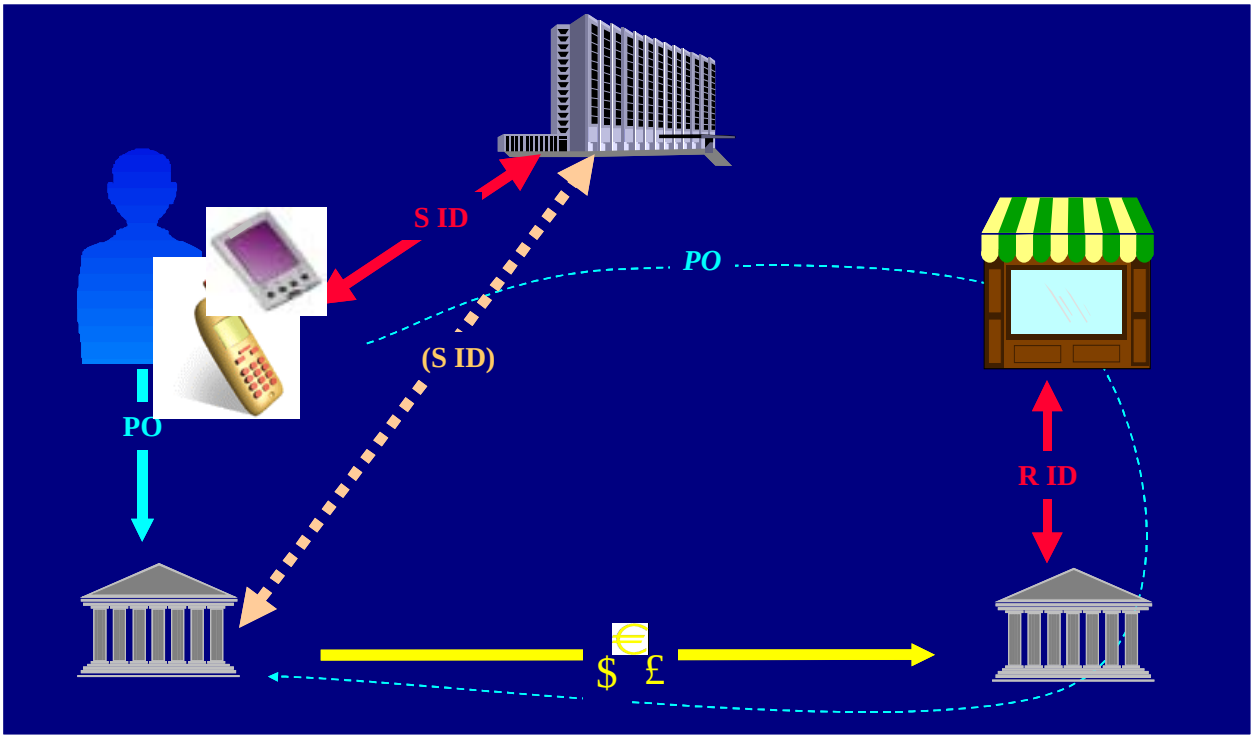
This model is the common one both for card payments (for example Visa and MasterCard) and for national giro systems.

Authentication of the customer is either done by the customer's bank (push payment and PIN transaction) or by the merchant (non-PIN transaction).



Five-box model

A typical five-box scenario is applicable when the customer's ID is verified and guaranteed (and not just authenticated) by a fifth party:



Box Model Analysis

Understanding the dynamics of the different box models is necessary, but not sufficient for the success of a mobile payment solution, which remains a key objective. Two key issues on box model facing partners who are implementing a mobile payment solution are:

- How sustainable is the chosen model?
- Which factors enhance (or diminish) its stability in long-term and daily operations?

The answers to these fundamental questions depend on a case-to-case basis of the mobile payment business case.

Box models can be sustained if

- the fundamental roles of the different partners do not conflict with each other
- new requirements do not arise that cannot be met in a given timeframe

Sustaining the partnerships (illustrated through various box models) is not enough. They must be profitable as well. Hence, the m-payments (for example, micro or macro, local or remote) that banks prioritise for development should be synchronised with the demands of service providers.

Assuming, for example, a four-box payment model with each of the four parties having their own choice of telecommunication company combined with customer and merchant telecommunication company roaming, one can draw a picture with six telecommunication companies and two banks. The resulting solution where all these parties are involved in the liability chain, and as such share the revenue of the financial transaction would tend to be very complicated and extensive.

Each communication link between the boxes, except perhaps that between the banks, might be done wirelessly, although merchants capable of accepting and processing wireless transactions are currently not yet common. Each link in the box models might involve two telecommunication companies building a four-box structure in terms of telecommunication. If the customer is roaming in to his telecommunication company a five-box communication is formed. The same situation applies to a mobile merchant.

From a bank's point of view a four-box model is the preferred solution where telecommunication companies gain profit by supplying communication services and banks by supplying payment services. Other models are probably more expensive for customer and merchant, especially in non-domestic situations.

APPENDIX E - DATA ELEMENTS USED IN M-PAYMENTS

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

C = Conditional security measures M = Mandatory security measures (encryption by 3 DES or PKI)