



Preferred Payment Architecture: Local Payment

September 2002

Document Version 1.0

**Prepared by:
Rae Saleem
(BNP Paribas)**

Filename: Local Payment Discussion Document 1.0

Document Information

Document Purpose

A prerequisite for the success of mobile commerce is the availability of services allowing mobile transactions to take place. A trust relationship over mobile payment networks is essential to build a secure, open and reliable payment framework on which all major parties can base their services on.

This document should invite discussion on the Local Payment technical framework used to support the Preferred Payment Architecture, published by the Mobey Forum in June 2001 (available at www.mobeyforum.org).

People Involved in the Preparation of This Document

Function	Name
IT Strategy – BNP Paribas Requirements & Technology Workgroup - (Local Payment Taskforce leader) – Mobey Forum	Rae Saleem
Workgroup Executive – Mobey Forum	Liisa Kanniainen
IT Strategy, ABN Amro Requirements & Technology Workgroup leader – Mobey Forum	Leonard Franken
Bank of Ireland Trust Interoperability Taskforce leader – Mobey Forum	Russell Burke
Vice President – Nordea Business Workgroup – Mobey Forum	Eero Vasenius
Development Manager, Nordea Requirements & Technology Workgroup, Mobey Forum	Jouni Jaakkonen
Project Manager – Nordea Requirements & Technology Workgroup – Mobey Forum	Ari Myllylä
Business Development Manager, Mobile E-Commerce Business Workgroup – Mobey Forum	Juha Kokkonen
Marketing Manager, E-Commerce – Nokia Business Workgroup – Mobey Forum	Veli Heikkinen
Manager, Mobile E-Commerce – HSBC Business Workgroup – Mobey Forum	Ben Arber
ABN Amro Requirements & Technology Workgroup – Mobey Forum	Jan Bartelen
Visa	Jean-Benoit Van Bunnan
Nokia	Petri Pirhonen
Mastercard (Europay)	Brian Morris
NCR	Norrie Taylor
AMEX	Tambra Nicholls
AMEX	Lee Peart
AMEX	Peter Newton
Credit Suisse	Rene Louis
Credit Suisse	Nicolas Korpela
Nokia	Risto Sipilä
Royal Bank of Scotland	Andy Hunter
Sampo bank	Hannu Kuokka
Union Bank of Norway	Bent Bentsen
Participants of Mobey Technical & Business workgroups	

Document Information, Continued

Review List

Reviewed by	Date
Mobey Local Payment Taskforce members	November 2001
Mobey Local Payment Taskforce members	June 2002
Mobey BoD	June 2002
All Mobey Members and Associate Members, Visa International, Visa EU and Mastercard.	August 2002

Change History

Version	Date	Revision Description
0.1	Nov 29 th 2001	1 st Draft
0.2	June 10 th 2002	2 nd Draft before Board submission. Inclusion of comments from the first draft. Inclusion of EMPS (Electronic Mobile Payment Project by Visa International, Nokia and Nordea) work. Inclusion of issues from various stakeholders. Preferred payment method suggested.
0.3	August 8 th 2002	3 rd Draft: Accepted by Board. Migration path agreed. For distribution and comments to Mobey Associate Members, Visa International, Visa EU and Mastercard.
0.4	September 16 th 2002	Proposal for BoD edited by Liisa Kanninen. Inclusion of comments from Mobey Members and Associate Members, Visa International, Visa EU, Visa Risk management and Mastercard.

Document Information, Continued

Glossary of Terms and Abbreviations

AID	Application Identifier.
APDU	Application Protocol Data Unit.
ARC	Authorisation Response Code.
ARPC	Authorisation Response Cryptogram.
ARQC	Authorisation Request Cryptogram.
ATM	Automated Teller Machine. A machine (e.g. bank-operated) where consumers can access a range of financial services like withdraw cash, pay their bills, make balance enquiries, order statements etc with their payment cards issued by the respective service provider.
Bluetooth	Local cellular technology capable of connecting various devices together.
CDA+	Combined Data Authentication.
CVM	Cardholder Verification Method (e.g. PIN).
DDA	Dynamic Data Authentication (in EMV).
DES	Data Encryption Standard.
EBPP	Electronic Bill Presentment and Payment.
EFI	External Functionality Interface / WAP Forum.
EMV	A payment standard defined by Europay, Mastercard and Visa International.
GSM	Global System for Mobile Communications, a (2nd generation) mobile network standard.
HTTP	Hypertext Transfer Protocol.
IrDA	Infrared Data Association, a standards body.
IrFM	Infrared standard for financial use.
IrObex	IrDA's Obex implementation
MBPS	Mega Bits Per Second.
MeT	Mobile Electronic Transactions, a Forum of handset manufacturers.
MMCA	MultiMediaCard Association.
MOTO	Mail Order Telephone Order; card not present transaction.
MSISDN	Mobile Subscriber ISDN Number.
Obex	Object Exchange, object oriented data transfer protocol.
OTA	Over the air.
PIN	Personal Identification Number.
PKI	Public Key Infrastructure.
POS	Point of sales (terminal).
PTD	Personal Trusted Device (according to MeT definition).
SAT	SIM Application Toolkit (GSM 11.14).
SBW	Server Based Wallet.
SC	Smart Card, equal to chip card (see PPA definitions).
SDA	Static Data Authentication (in EMV).
SE	Security Element (see PPA definitions).
SignText	Mechanism for creating digital signature with data generated as the result of a transaction. Enables non-repudiation. [WMLScript Crypto Library].
SIM	Subscriber Identity Module (GSM 11.11).
SIM/WIM	One or several WIM application(s) reside on the SIM card.
SRFT	Short Range Financial Transactions (subgroup of Bluetooth SIG).
SSL	Secure Socket Layer, a generic transport layer security protocol.
TC	Transaction Certificate.

Document Information, Continued

WAP	Wireless Application Protocol.
WIM	Wireless Identification Module / WAP Forum.
WTLS	Wireless Transport Layer Security (protocol) / WAP Forum.

Table of Contents

<i>Executive Summary</i>	8
1 Introduction	10
1.1 Requirements	10
1.2 Local Payment Model	11
2 Mobile Local Payments- Overview	12
2.1 The Local Payment Environment – Mobey Focus	12
2.2 Overview of Local Payment Transactions	13
2.3 Mobile Payment Opportunities	14
3 Application–Layer Alternatives	17
3.1 EMV in the mobile environment	17
3.2 Magnetic-stripe image	22
3.3 WIM Signature added to a magnetic-stripe image	23
4 Transport Layer Alternatives	25
4.1 Object Exchange Protocol (OBEX)	25
4.2 WAP as transport protocol	26
4.3. Contactless Protocol with ISO 7816 APDUs	26
4.4 Specific	26
5 Media Layer Alternatives	27
5.1 Bluetooth	27
5.2 Radio Frequency – Contactless	27
5.3 Infrared	29
6 Analysis	30
6.1 EMV in the mobile environment	30
6.2 Magnetic-stripe image	32
6.3 WIM Signature	36
6.4 Connectivity/Transport Protocol Comparison	38
7 Industry Bodies Developing Local Transaction Specifications	40
7.1 The MeT Forum	40
7.2 The IrFM SIG	40
7.3 The Bluetooth SIG SRFT Study Group	41
7.4 The National Retail Federation - ARTS	41
7.5 Conclusions	42
8 The Preferred Payment Solution for Local Payments	43
8.1 The First Step: Contactless Chip and Existing Infrastructure	43

Table of Contents, Continued

8.2 The Second Step: A More Integrated Solution – PIN Entry at Mobile	44
8.3 Towards the Target Solution – Mobile EMV Payments	46
8.4 Conclusions – the Migration Path	46

Executive Summary

There are a lot of expectations towards local mobile payments from various parties. Merchants expect it to shorten the queues through fast, small payments. They also look forward to offering more convenient means for payments. Security will also be increased and maintenance costs cut, for example, in vending machines, which may accept only cash today. Banks expect it to facilitate the transfer to electronic payments in terms of offering added convenience and leading thus to savings in cash and cheque handling.

Local payment is a crucial element in creation of a customer habit of using the mobile device as the means of payment. Once the habit starts from a familiar application area like the proximity payment, it is expected to transfer also to other application areas like remote payments and mobile banking. This will benefit banks, but perhaps even more the mobile operators; kick-starting mobile commerce is most crucial for their business.

The challenge of performing payments with mobile devices in the proximity environment is tied to the fact that existing traditional payment standards, processes and protocols widely used in the physical environment are another world when compared to the mobile technologies. The technology lifecycles, business processes and, for example, certification requirements of POS terminals and mobile phones differ a lot, and for obvious reasons.

We have witnessed the convergence of various industries taking place during the past years. The convergence of the mobile and payment technologies is also happening, for the benefit of more economical and efficient processes and increased customer convenience. The prerequisite for this convergence is a new open-minded way of thinking in both industries and speedy development of new pieces of technology and processes whenever necessary.

This document is complementary to the original *Preferred Payment Architecture* (PPA, version 1.0 published in June 2001). The main technical alternatives to perform payments in the local environment are presented and evaluated within this document. Finally a migration path is proposed towards the target solution, that is, mobile EMV payments.

The protocols between the mobile phone and the POS terminal are divided in three layers: the *media* layer – Bluetooth, RF or Infrared, – the *transport* layer – Obex, WAP or a specific protocol – and the *application* layer, the actual payment protocol. The application layer alternatives are the usage of an EMV-based payment, usage of the existing magnetic stripe technology as a digital image, and adding a WIM signature to the magnetic stripe image payment.

Mobey requirements towards media and transport layers are expressed in the document – the main ones being security, speed and fit for purpose. Although some suggestions are being made in this area, it is assumed that the final decisions here will be done by practical reasons along the line.

The application-layer choices are the ones that really matter from Mobey's perspective. The EMV-based payments are the ultimate target and clearly the preferred option from Mobey's perspective. This was suggested already in the PPA 1.0.

The migration path in Chapter 8 describes how to get there from today's technological environment and user habits. The choices made are to start by utilising the existing magnetic stripe infrastructure. Then, to add the payment card data as an digital image in a secure bank-controlled storage within the phone, and to allow transmitting the payment card data to the POS securely and to process the payment further from there as a normal transaction today. This storage can in the beginning be, for example, a RF-ID Tag placed inside the phone cover, but is expected to soon convert to a more integrated solution. During the first stage, the PIN is given – as today – at the POS or ATM through, for example, a PIN pad there. The user

is thus in the beginning only initiating the payment with the mobile, by waving it at the POS or ATM.

Within 1-2 years the local payment application could be placed on the same bank-issued (dual-interface) multi-application chip card besides the WIM application within a dual chip mobile phone. Within this next step in the development, Mobey prefers to move the PIN entry to the mobile device. To reach this target, both technical and process development is required. Rules as to how to enter the PIN code at the mobile so that it is technically secure and acceptable to all interested bodies, are to be agreed next.

By 2005, EMV is expected to be a reality in most parts of the world. By that time, the target is to have the full EMV solution available for mobile local payments. This is expected to happen by placing the bank-issued EMV payment application on the multi-application chip card in the second slot within the phone. Major work areas to achieve this target include agreeing on the potential EMV (self-)certification rules for the mobile phones, and technical work required for optimising the implementation of EMV standard over local wireless protocols. Banks and card associations have made major investments in EMV and certainly want to ensure that local mobile payments, predicted to be a reasonable share of transactions in ten years, will utilise the EMV processes.

1 Introduction

The mobile local payment environment is an area that still needs a significant amount of work in terms of research and understanding. With the variety of Personal Trusted Devices (PTDs) set to increase (mobile phones, PDAs, Smart-phones, etc.) and mobile commerce set to rise, an 'open framework' on which to build upon would be in the best interests of all concerned. This document is intended to provide a standard on which major parties – including handset manufacturers, suppliers of payment equipment, card issuers and credit authorities – can agree on in order to minimise confusion for the public and enable an open-standard environment in which to develop.

It is widely expected that mobile phones will become payment vehicles both in remote and local environments. Consumer convenience, having the required change and a ubiquitous payment mechanism always with you, is expected to be the driver for this habit change. An important driver from banks' and merchants' perspectives are the obvious cost savings and additional revenues the accelerated card-based transactions bring. In some countries still, 60-80% of transactions are made with cash or checks. The cost element this evolves has seldom been calculated, but we can make some estimations of it. Finland is one of the economies with small amounts of cash payments (cash in circulation is only 1.8% of BKT; electronic transfers are 91% of all banks' payment transfers. Source: The Finnish Bankers' Association, April 2002). Still there are some 2000 people employed by the Finnish banks to clear the cash, that is, to receive it from the merchants, count it and send it back to the ATMs. Another 2000 people are employed on the merchants' side to count the cash and to send it back to the banks. We can only guess what these figures are in countries like UK or in the US. Where is the sense in this process? Usually in an economy the least costly option wins – at least in the long run.

Mobile Financial services consist of at least four separate application areas, of which local payment is one. The other areas are ATM withdrawals, remote payments (e.g. WAP shopping), remote banking and ID services. Cash withdrawals and payments at local stores form an elementary part of consumers' everyday payment habits today. Banking service is perhaps the next one in terms of frequency of usage – usually performed on a weekly or bi-weekly basis. Generally, remote payments might be the least used of these services for the wider public.

Habit creation is of key importance in order for mobile commerce to kick off. When considered from the viewpoint of habit creation and speedy market adoption, it is necessary that the sequences of all these services are as similar as possible. It would be preferable from the user perspective to use, for example, the same PIN code for all of these services. It is more realistic to expect the wider public to start looking at their mobile phones as payment vehicles if you start from an area that is familiar to consumers and change only a little fraction of their payment habits in the beginning. Eventually you can introduce the less frequently used services like remote payments.

In order to establish a preferred architecture for the Local Payment scenario, certain requirements have to be met.

1.1 Requirements

The major requirements concerning Mobey that form the basis of this work are as follows:

- Ease of use for the consumer / convenience.
- Added value for the user compared to conventional payment mechanisms.
- Ability to securely establish connection between mobile devices and POS.
- Speed of transaction time.

- Simple, inexpensive, standardised solutions for merchants, in order to achieve widespread acceptance.
- Utilising existing and emerging payment protocols and technologies whenever possible.
- Brand recognition of bank / card brand at POS and in the payment process (e.g. customers pay with card brand, not with handset)
- Need for interchange (interoperability).

1.2 Local Payment Model

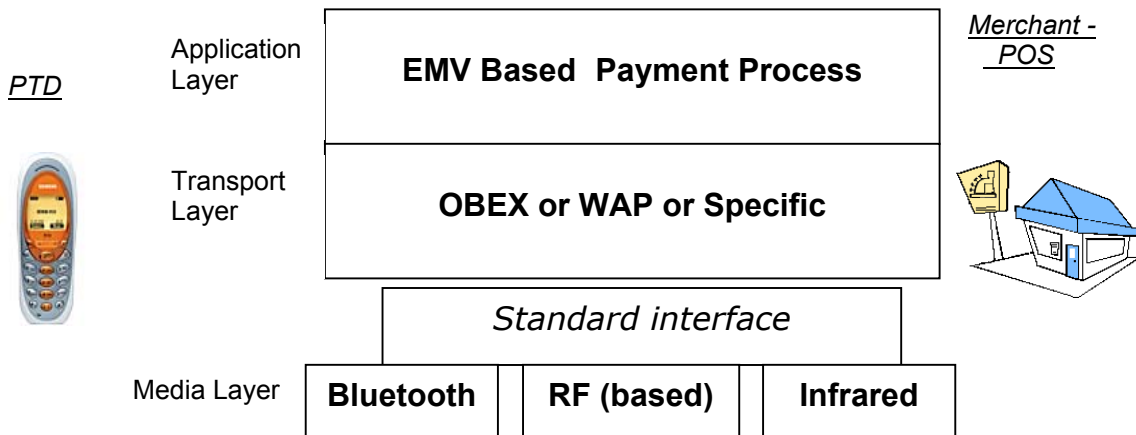


Figure 1 – Local Payment Model

The intention is to use the above model (*Figure 1*) in the Local Payment Environment. The idea is to standardise the Application (Business logic) and Transport (transport mechanism) layers in applications that can then communicate using the desired choice of media. If the interface is well standardised, the media layer implementations may vary, as long as interoperability is guaranteed.

Another way of understanding this would be through using an analogy of transporting people from Place 'A' to Place 'B'. The Application Layer would act as the people being transported between the two places. The fewer people to transport the easier/faster it becomes. The type of vehicle used to transport the people would act as the Transport Layer, i.e. car, truck, etc. Finally, the type of road used to deliver the people (fast speed highways, country roads, etc) would act as the type of media used.

2 Mobile Local Payments- Overview

2.1 The Local Payment Environment – Mobey Focus

A key advantage for the success of mobile payment lies with the fact that the groundwork has already been laid. Figures from a 2001 Forrester report show 59% of Europeans carried a mobile phone at the end of 2000, with two-thirds reporting that they never leave their home without it, figures that have surely increased since then across the world. This is unlike when credit cards first came into use and people had to get used to the concept of carrying one around, the trust issues around it and developing the user habit. Mobile phones have now been around for a number of years, gradually increasing in functionality from being simply a communication tool to offering a variety of features that adds value to the device for the user.

Potential mobile payments within a Local Environment fall into various distinct categories:

- **Payments for products and services purchased in the real world.** In this category, consumers use their mobile phones (containing a bank-issued payment chip card) to pay for anything they would use cash, checks or credit and debit cards to pay for in the physical locations, at a face-to-face retail point-of-sale.
- **Transactions at ATM.** Consumers could use their phone (containing a bank-issued payment chip card) if they needed cash for a specific purpose to withdraw or make any other transaction at an ATM (balance enquiry, order statements, etc). Ideally the phone could eventually act also as a PIN entry device communicating over the desired choice of media.
- **Payments for products at a vending machine.** With the same equipment consumers would be able to initiate payment for their desired product at a vending machine without having to carry cash / coins or cards. This could be for a variety of products, for example, from food and drink to ticketing and car park payments.

There are many scenarios where Mobile Payment can be used within a Local Payment Environment. These are 'generally' grouped with regard to the amount spent; 'Micro' for under 10 euros, 'mini' for between 10–100 euros and 'macro' for greater than 100 euros. Mini- and macro- payments are sometimes hard to separate and for them both usually same rules apply. This yields two main mobile payment segments within the local environment.

Proximity Payments with Mobile Phone	
Low-value (micro) payment (e.g. < 10 Euros)	Vending machines, parking meters, transportation, other face-to-face merchants enabled to accept mobile phone payments
Medium- High value (mini, macro) payment (e.g. > 10 Euros)	ATM withdrawals, Petrol stations, parking garages, restaurants, taxis, other face-to-face merchants enabled to accept mobile payments

Table 1 – Value of mobile transaction

There are a growing number of groups currently looking into Local Payment methods for mobile payments (see Chapter 7). Where Mobey can add most value to the equation is through the banks' interest to start from higher value transactions – in particular POS and ATM operations – where cash, checks and debit/credit cards are currently used today. Banks are also keen to offer more convenient, secure and cost-efficient mobile payment mechanisms for smaller payments in the Local Environment. This would include vending-type merchants, for example, once the transaction costs come down through more flexible card payment process requirements.

2.2 Overview of Local Payment Transactions

Introducing the mobile phone as the next step in the evolution of payment mechanisms (cash, cheque, card, etc) could have many advantages, including the ones outlined below:

- Cardholder convenience.
- Personal card reader in everybody's pocket (not required on the terminal).
- Increased speed of payment transactions.
- Increased electronic transaction volume; reducing the volume of expensive and outdated payment mechanisms like cheques.
- Decreasing the number of cards in circulation over time.
- Cardholder confirmation and choice via mobile device display.
- Introducing new functionality to a user's familiar mobile phone.
- Additional services can later be offered to the cardholder on the same device.
- Decreased transaction risk and cost compared to, for example, SMS-based or cash payments.
- New access channel to card payments with increased acceptance.
- Increased operator revenues, through additional usage of online services as well (due to mobile-payment habit creation).
- Increased handset vendor revenues, through increased phone purchases due to new functionality.
- Less cash transactions.

The overall Local Payment scenario offers a few business and technological choices that must be made with reference to their actual implementation on mobile phones and the connectivity type. At the time of writing, the PPA-compliant choices that are presented to us are outlined in Table 2 below. These alternatives are evaluated in this document and choices are suggested in Chapter 8.

Mobile Implementation	Payment Methods	Transport Protocol	Connectivity
Bank Issued Chip	EMV (possible relevant sub-set)	OBEX	Infrared
	WIM Signature	WAP	Bluetooth
	Magnetic-stripe Image	Contactless Protocol ISO 7816 APDU	RF (contactless) ISO 14443

Table 2 – Technology Alternatives

Although there are SIM chips in mobile phones today, these cannot be considered as alternatives for bank-issued payment applications for local use. First of all, payment associations' rules prevent banks from placing payment applications on a non-bank issued platform. Secondly, placing all of the bank-issued debit, credit, e-purse, etc. applications on an operator chip would require very heavy logistical co-operation. Payment applications are usually personalised before enrolment. SIM chips are pre-personalised. Matching the different applications and controlling the change management would be a logistical nightmare.

2.3 Mobile Payment Opportunities

2.3.1 Proximity Payments

Local payments are expected to penetrate first to those industries where it is providing clear benefit either for end-customers or merchants. Benefits are, for example: convenience, faster through put time and savings in cash management.

According to an example research study from Forrester; consumer, provider, and technology factors will act differently in each segment of mobile payment, leading the payment mix to swing dramatically over time. Not considering Top-Up mobile content that dominated last year's market, leadership will shift to local low-value payment in 2003 and finally to local high-value payment in 2005, which coincides with the liability shift of an EMV-based standard across the world.

Local low-value payments are expected to penetrate niches fast - then plateau. Niches like ticketing, parking, vending machines and courier services will host mobile payments through 2003, offering obvious value to consumers and retailers. Some of the early trials in this area have been based on sending regular SMS messages with a predefined content structure or calling a premium number. The charging has often been based on operator billing. The main benefit for end customers has been cashless payments. However, these network-based solutions have not really taken off on a large scale possibly due to there not being one coherent payment mechanism which consumers can relate to. It might also be due to the rather high additional charges the new entrants in the market have been requesting.

It is expected that future solutions will support direct communication over a proximity interface enabling faster and more convenient transactions. Some of the first trials in cafeterias and fast food restaurants have been based on RF-ID technology where an RF tag is embedded into an exchangeable phone cover. Local payment solutions over a proximity interface typically require some terminal and infrastructure investments. Therefore, the expected speed of the investment cycle is not following what it has been typically in the mobile telecommunication industry, but will be a bit slower.

Local high-value payments are expected to develop slowly. Consumer trust in local payments and transaction convenience will be crucial to the take off of local high-value payments. No single player will be capable of meeting high-value payments' stringent demands, including security, capacity, non-repudiation and reliability. The progress might be accelerated by partnerships between financial firms, merchants and device manufacturers.

Some of the issues posted by the various players in this scenario are outlined in Table 3 below.

POS Terminal manufacturers (NCR)
▪ POS infrastructure: backwards and forwards compatible.
▪ EMV+PIN infrastructure roll-out (timing, differing from market to market.)
▪ Integrated or separate device.
▪ Fragmentation to be avoided (media, transport and application layers need to be standardised.)
▪ Is re-certification needed?
▪ Added costs (with regard to the media layer) to be kept to a minimum.

Merchants
▪ Transaction time - is it speeding up?
▪ Costs to be kept to a minimum (both investment and usage.)
▪ Not changes / new devices every year.
▪ Not to generate new payment mechanisms but to leverage on existing ones and to offer new convenient and speedy access mechanisms to them.
▪ Charge-back / customer service to be enhanced.
▪ Possibility of adding loyalty schemes.
▪ Giving the same payment guarantee as other methods?
▪ Trust / security as a payment media.

▪ EMV liability shift, 2005
▪ User adoption - is there mass-market potential?
▪ Cross-channel support integration.

Handset manufacturers
▪ Large market adoption.
▪ Non-fragmented solutions (global approach.)
▪ As cost-efficient as possible.
▪ Time-to-market (as light certification as possible / no certification.)
▪ Multi-application capability.
▪ New relationships with banks.
▪ Add value to the handset for the consumer.

Network operators
▪ Potential to add value.
▪ Level of involvement.
▪ Roles clarified between operators, handset vendors and banks (customer support issues.)
▪ Endorsement of the whole solution.

Consumer
▪ User experience as simple as possible.
▪ Enrolment optimal compared to existing options.
▪ Convenience.
▪ Additional value created.
▪ Trust and security (both perceived and technical.)
▪ Retain the charge-back rights.
▪ Wide acceptance / amount of fragmentation.
▪ Additional cost of usage (once-off and continuous)
▪ Flexibility of choosing payment products and supporting various payment types and amounts.
▪ Consumer acceptance.
▪ Interoperability between phones, operators, and banks.

Banks and card issuers
▪ Branding.
▪ Justifying the business case.
▪ Ownership of the payment application.
▪ Liability of the transaction vs. control of the security.
▪ Impact of the solution to the back office and the business rules (is it a new txn type? What is the impact?)
▪ Personalisation / card issuing process needs to be similar to existing one.
▪ Single chip / phone memory: who personalises it / how is it done?
▪ Cardholder enrolment process.
▪ Has to be at least as secure / apply for the same rules as current alternatives.
▪ Is PIN needed? The value of the transactions?
▪ Potential to create new additional business.
▪ Management of the multi-application process.
▪ New types of partners to take in consideration.
▪ Potential also to use for remote payment.
▪ Reducing / increasing fraud - risk management.

Acquirer bank
▪ Use of existing infrastructure.
▪ Just like any other transaction.
▪ Minimising the additional POS costs.
▪ Good value proposition to the merchants.

▪ Certification of the POS terminals.
▪ New relationships involving handset vendors? (Division of roles not agreed today)
▪ Impact of the solution to the back office and the business rules (What is the impact?)

Table 3 – Stakeholders Concerns for mobile local payments

It is generally agreed that new payment mechanisms should not be created, but rather existing ones should be fully leveraged and accessed through the mobile channel.

Card manufacturers' concerns should also be taken into account.

The average lifecycle for a POS terminal is approximately seven years. Since POS terminals need to be redesigned for EMV by 2005, there are issues concerning any interim solution causing any extra costs for merchant equipment. With our goal firmly fixed on an EMV based solution there should not be any concerns or discussion of re-certification of POS terminals for accepting mobile payments.

Mobey is keen to address these issues and to contribute to the development going on in the industry and feels that it is necessary to facilitate this process to the correct direction.

3 Application–Layer Alternatives

The Application layer contains 3 key areas central to Local Payments. These are:

1. Business Logic
2. Risk Management
3. Digital Signature.

These three areas can be broken down as follows, to identify how each contributes to a given transaction:

APPLICATION LAYER	Example
Business Logic	Identify and make clear to the user that in order to continue the transaction a 'PIN Number' is needed. User input to be requested.
Risk Management	Depending on amount of payment, card makes decision as to whether feasible or needs authorisation. Authentication method to be decided by issuer according to risk level.
Digital Signature	Legally binding signature performed by PIN code authorisation.

From these areas we can analyse the various options presented and select the preferred method based on our requirements.

3.1 EMV in the mobile environment

Jointly developed by Europay (E), MasterCard (M) and Visa (V), EMV is an agreed specification for the interoperability of smart cards and terminals equipped with smart card readers for debit and credit schemes, regardless of the card's manufacturer, the issuing institution, or location of the EMV terminal.

The standard migration from magnetic-stripe to EMV has already begun and is due to be accepted over the majority of the world by 2003 (*Figure 4*). Figures (2, 3 and 4) below from Europay highlight the EMV migration process further on a global scale.

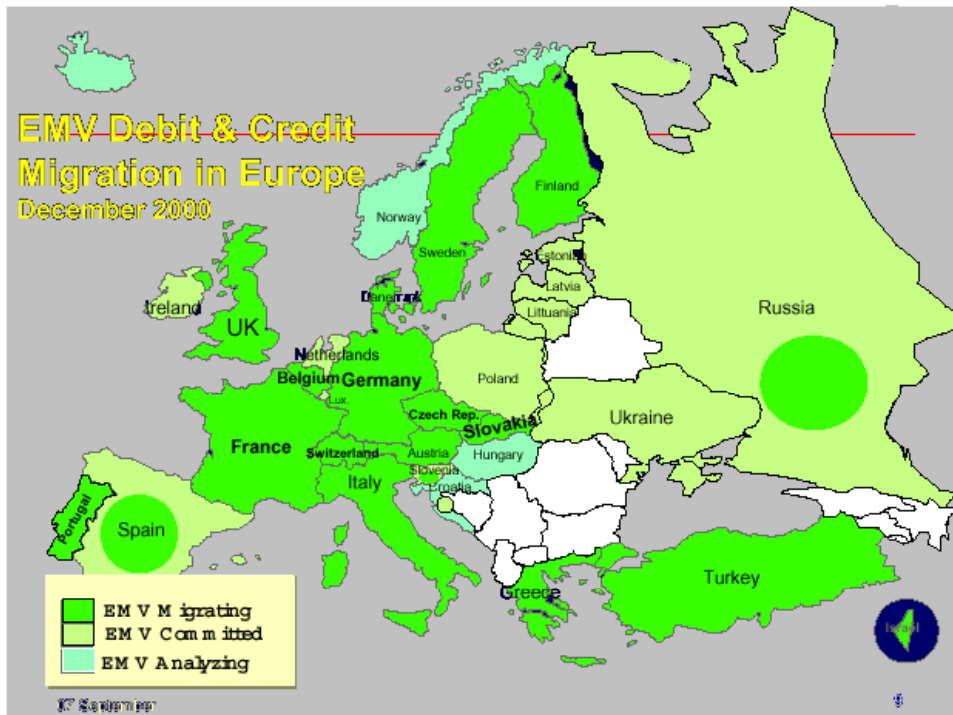


Figure 2: EMV Debit & Credit Migration in Europe (Source: Europay)

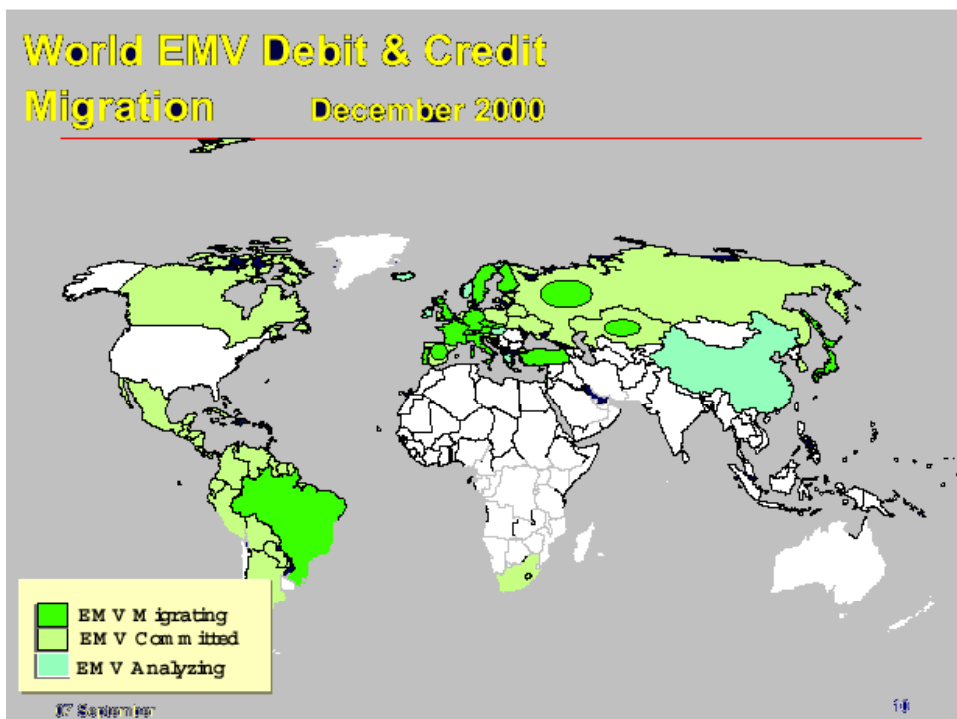


Figure 3: World EMV Debit & Credit Migration 2000 (Source: Europay)

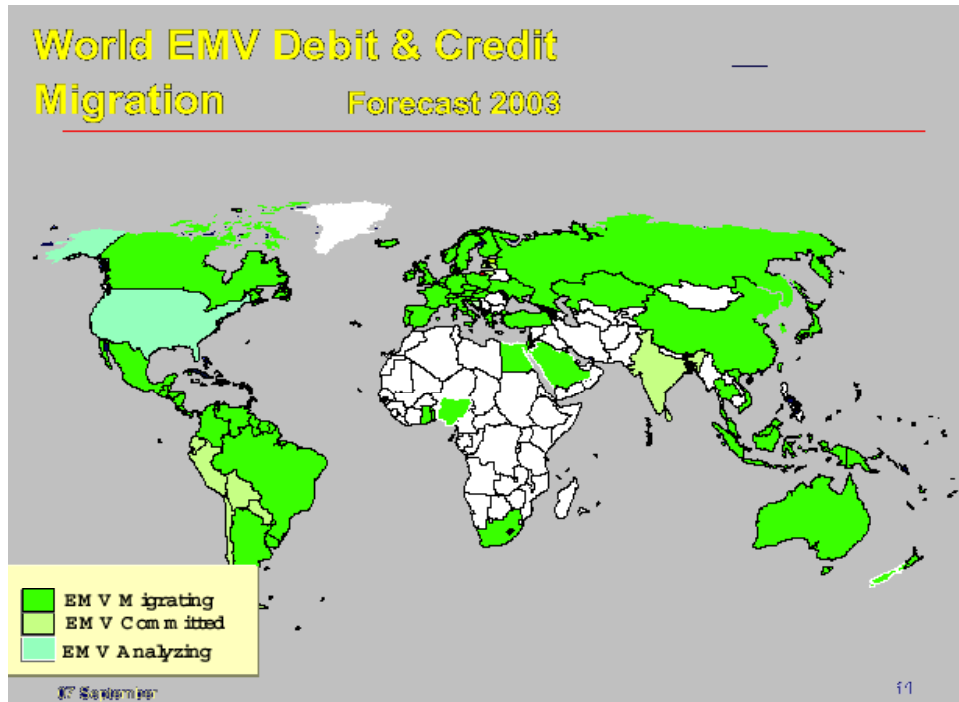


Figure 4: World EMV Debit & Credit Migration Forecast 2003 (Source: Europay)

Despite some merchants' reluctance to roll out smart card terminals, the main justification for EMV implementation is to cut fraud. Visa EU believes it can cut fraud losses from magnetic-stripe card counterfeiting by €700 million over the next four years with the rollout of EMV-compliant credit and debit smart cards. This is alongside requiring cardholders to enter PINs.

Under the Visa EU incentive program, merchants could receive money through banks to install terminals. Visa EU also will use money to encourage card issuers to accelerate their rollout schedules, earmarking cash to cover the cost difference between EMV-compliant chip cards and magnetic-stripe cards. The faster the banks move, the more their chip card costs will be covered, says Waqar Qureshi, head of chip and infrastructure at Visa EU.

The key deadline for EMV implementation is January 2005, when banks will become liable "for fraudulent transactions if they have not implemented chip cards and it can be demonstrated that chip cards would have prevented the fraudulent transaction from occurring".

Each regular EMV transaction consists of a maximum of 11 phases. The typical flow of an EMV transaction is outlined below and some possible methods of optimising EMV for mobile applications suggested.

Phases in EMV Transaction (1)

1: Application Selection
Terminal selects application on card

2: Initiate Processing

Terminal reads all necessary card data

A potential issue is to have magnetic-stripe data also being present on the EMV chip card. This can be used for the transition period and in case of partial grade (Europay) or early compliance (VISA) situations.

3: Offline Data Authentication

Terminal determines authenticity of card

Two methods for offline authentication:

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA or CDA+)
- If card and terminal support both, then DDA or CDA+ should always prevail, as this is more secure.

4: Processing Restrictions

Terminal checks validity of the card

The terminal compares various aspects of the card and terminal data like the application version number, expiry and effective date, and application usage control.

5: Cardholder Verification

Cardholder identifies himself as genuine owner of the card

Cardholder input (PIN code) to be requested at this stage.

6: Terminal Risk Management

Terminal determines transaction risk by performing checks on card data to protect acquirer, issuer and system from fraud

7: Terminal Action Analysis

Terminal makes decision about transaction

Terminal risk management results are compared with Terminal and Issuer Action Codes. Transaction can be rejected or sent online on the basis of:

- Unsuccessful data authentication performed
- Card appears on exception / black list
- Expired card / card not yet effective
- Lower / upper consecutive offline limit exceeded, etc.

8: Card Action Analysis

Card makes decision about transaction

The card can also perform its own risk management and take different considerations into account.

9: Completion

Completion of transaction on card and terminal

For offline completion, cards must either accept or reject the transaction. A cryptogram is stored in the terminal for clearing and settlement at a later stage.

10: Online Processing

Issuer makes decision about transaction

For online transactions the Authorisation Request Cryptogram (ARQC) is sent to the issuer. The issuer then makes the decision and responds with the Authorisation Response Cryptogram (ARPC) and Authorisation Response code (ARC). The terminal forwards ARPC to the card for issuer authentication and the transaction completes with the card providing a second cryptogram (TC).

11: Issuer Script Processing

Update card status or card data

By utilising scripts the issuer can:

- Ensure extra security, in blocking or unblocking applications, or block the card, which is irreversible.
- Provide extra possibilities though PIN unblock / change facilities and update of data.

The protocol as it currently stands would probably be too slow to work with a mobile phone. This is mainly due to the amount of logic the protocol uses. Some thoughts as to how EMV could be optimised within an environment for mobile payments come from Jouni Jaakkonen (Nordea):

1. Offline Data Authentication (SDA/DDA/CDA+) (step 3).

This can be done when the handset is powered on and the EMV chip is inside it, not when payment happens. This saves RSA calculations, but requires that the issuer's public root key reside in the handset. It also requires that issuers and acquirers establish trust with phone manufacturers, or then the root key may be stored at the bank-issued WIM. This would also mean that the responsibility of the off-line data authentication shifts from the acquirer domain to the issuer domain.

2. More offline transactions (step 9).

The more the EMV payment application in the chip accepts offline transactions, the faster the payment is.

3. Payment instrument negotiation.

If there is only one payment application on the chip, there is no need to negotiate. POS rejects the transaction if the Application Identifier (AID) is not valid.

4. Implementing as much application logic into the handset as possible.

MasterCard International (MCI) view EMV Co and Simon Pugh's MasterCard International team based out of Purchase, NY as the two primary groups focussing on optimising EMV for mobiles. The latter is a technology R&D team responsible in the past for the GMCIG (Global Mobile Commerce Interoperability Group), which is being dissolved to make way for the Mobile Payments Forum in conjunction with Visa and Amex, and defining technology models for mobile payments.

However, MasterCard's general position seems now to be one of pragmatism and concentrating on "here-and-now" opportunities. They also seem to feel that all EMV functionality is not necessarily required to be optimised for mobile devices. They do, however, share the belief that from a standpoint of a basic customer experience, EMV should work in mobile the same way as in the physical and virtual worlds.

3.2 Magnetic-stripe image

Storing your current card information on the phone would be a quick win for enabling an 'e-wallet' on your PTD. Here card details would be stored, for example, in an encrypted part of the phone memory and accessed via a PIN code. This would be a good first step to introduce the concept of PTD payments. However, in the mid to long-term there will be issues, which would mean this solution has limited value. For example, ensuring security from the financial institutions' perspective and proving non-repudiation through means of a digital signature is challenging in a software-only solution.

The solution, that alleviates the potential security problem in the phone memory storage option, can base on the use of an RF (contactless) chip, embedded in the PTD. The chip, that can be implemented using tamper-resistant technology, provides additional physical security to the image of the magnetic stripe. The usability is actually improving as the contactless interface provides fast and convenient method to communicate with the content of the chip. Further, if a dual interface (contact and contactless) chip is used, the content can be protected by means of a PIN code given through the phone User Interface (UI) while the chip can potentially store more than one image, reflecting the concept of multi-card wallet.

An optimal solution (proposed by Nordea) is to store the magnetic-stripe image as an additional application into a separate multi-application chip issued by the bank (EMV, WIM, etc.). The additional security features of the chip (in comparison to magnetic-stripe) can be used for storing the magnetic-stripe information as a digital image.

The most important security features of the chip are:

- Only the chip issuer can personalise the chip application (or authorise the personalisation.)
- PIN check may be performed off-line by the chip application.
- Chip application stores secret (DES) key that is used to sign off-line PIN check response to a POS.
- It may also store keys for signing authorisation messages and encrypt PIN when checking on-line to issuer.
- The drawback of using DES keys off-line is that the POS must also have equivalent keys in a Security Module (SAM)

If the separate chip lacks processing capabilities, for example if a simple RFID tag is used, the magnetic stripe image is still a potential solution. A first and quick to market step may be even preferred. The magnetic stripe image is in this particular case stored on the RFID tag and the usual swiping of the magnetic-stripe card can be replaced by a simple waving of a phone. This has the advantage of no magnetic stripes and readers and related sources of faults are in the process involved. Still a PIN can be requested on the POS or Vending machine. The sequence is the same for the magnetic-stripe card and the RFID tag:

- Wave / swipe + "yes" or
- Wave / swipe + PIN or
- Wave / swipe + handwritten signature or
- Plain wave (no user authentication).

The choice of authentication is depending on the POS interface and the issuer decision. The role of the PIN is to authenticate the cardholder and it may be replaced by a hand-made signature at manned point-of-sales.

The magnetic-stripe image application is expected to be a parallel application to the full-sized card, at least for a transition period. There are several ways to keep track of the different transactions. The user may be issued with two separate card numbers. A possible scenario might be that a consumer has a full-sized debit card in his physical wallet and another copy stored on his phone as well. There are similar scenarios today when issuing multiple magnetic-stripe cards. This solution could be managed by issuing phone based magnetic card data so that the use of different methods can be tracked, for example, much like the card sequence number on magnetic track data. When the consumer then uses his physical card in one terminal (Card sequence #1) and then the phone card details (Card Sequence #2) in another terminal, the usage can easily be tracked and separated.

3.3 WIM Signature added to a magnetic-stripe image

The Wireless Identity Module is an application storing user's private keys. WIM can reside on a tamper-proof device, for example a chip card, providing PKI-based authentication and digital-signature capability for WAP and m-commerce services. WIM is included in the WAP 1.2.1 specifications and can – according to the standard – be implemented in three ways: on the GSM SIM card, or on a separate chip card (for example dual chip / PPA model), or on another tamperproof hardware. Today there are public implementations of the first two alternatives. For financial applications like mobile banking the WIM would need to be a bank-issued one.

There are some parties that have suggested WIM to be combined with a payment mechanism to be considered globally as an intermediate solution. This is mainly due to the roll out of the standard version of EMV taking so long (for example, EU countries by 2005 followed by USA/ Asia).

The idea is that the WIM signature is combined with an existing payment mechanism, like magnetic-stripe transaction. This alternative has not been tested anywhere in practice, but is evaluated within this document.

WIM signatures have been used in remote mobile payment services. The demonstration at CeBit (2000) showed through the use of Wireless Application Protocol (WAP) 1.2 and WAP Identity Module (WIM) in mobile e-commerce, how a secure encrypted session to a mobile commerce server is established, using strong user and client authentication enabled by WAP/WIM. In addition, it also showed how mobile payments could be completed using a Visa card and Secure Electronic Transaction (SET). More recently, the EMPS pilot run by Nokia, Nordea and VISA using a dual chip phone and a bank-issued WIM has demonstrated this. There are also other pilots that have successfully tested the same capabilities in the remote payment area. WIM has also been proven to be a very convenient and secure access method to mobile banking services where it can also be used for confirming transactions.

However, with POS terminals moving towards EMV standards, it would seem very inconvenient from merchants' points of view to implement a totally different method for mobile local payment transactions. For example, if WIM is used, POS would always need an online connection (capable of handling WIM signatures) all the way back to the issuing bank. This alternative would also require parallel infrastructure to be built within the whole financial industry.

4 Transport Layer Alternatives

Within this chapter the transport layer alternatives are described. In our earlier analogy this was referred to as the type of car used to transfer people from place A to place B.

4.1 Object Exchange Protocol (OBEX)

In 1999 the Infrared Data Association (IrDA) announced that IrDA's Object Exchange Protocol (IrOBEX) was to be adopted as the framework for wireless Object Exchange for Bluetooth technology. IrDA's OBEX protocol was the first API Session layer common to the two wireless specifications.

By adopting common usage models and then exploiting the unique advantages of each organisation's technology, the combination of Bluetooth and IrDA together create the only short-range wireless standards that can meet user needs, varying from wireless voice transmission to high-speed (16Mbps) robust data transfer.

IrDA's OBEX specification consists of a protocol and application framework. It is a session-level protocol that specifies the structure for the conversation between devices and it also contains a model for representing objects. The OBEX application framework is built on top of the OBEX protocol, which facilitates interoperability between devices.

IrOBEX provides object-exchange services similar to HTTP. However, OBEX works for the many devices that cannot afford the substantial resources required by a HTTP server and it also targets devices with different usage models than the web. The major use of OBEX is a "Push" or "Pull" application, allowing rapid communications among portable devices in dynamic environments.

OBEX is not limited to quick connect-transfer-disconnect scenarios. It also allows sessions in which transfers take place over a period of time, maintaining the connection even when it is idle. PCs, pagers, PDAs, phones, cameras, printers, auto-tellers, information kiosks, calculators, data collection devices, home electronics, medical instruments, automobiles, office equipment, toys and even watches are all candidates for using OBEX.

OBEX can be used to perform complex tasks such as database transactions and synchronisation. OBEX was designed to be application friendly and provide cross-platform interoperability. It is compact, flexible, extensive, minimises strain on resources of small devices and it maps easily into Internet data-transfer protocols.

As OBEX is written in binary (http), the protocol is good for phones with limited memory. Work has been carried out by LINUX in a University in Norway just over a year ago using this protocol. The protocol is relatively new, only infrared has been tested and supported. Nokia, Ericsson, Microsoft, Motorola, etc. use OBEX in their infrared devices. The main reason why it is suitable for different forms of media is due to the architecture of the protocol coming in two parts:

- 1- Application Framework: the data for transmission.
- 2- Session Framework: does not care what kind of data is transported, as it handles it all as objects. Therefore, the data packages can then be sent over various forms of media.

OBEX uses a MD5 algorithm (freely available) and a shared secret, such as a password or pin number, for sender and receiver authentication. Standard OBEX does not include encryption, but it is one of the proposed additions to OBEX. Currently, the overall reception using Bluetooth and OBEX has been positive, with Nokia recently carrying out a local project using this combination without experiencing any major problems. Nokia also use OBEX in

their Bluetooth development kit and according to what has been tested so far – transferring calendar data from PC to Nokia 6310 phone, for example – it works.

4.2 WAP as transport protocol

The Wireless Application Protocol (WAP) is an open, global specification that empowers the mobile user with a PTD to easily access and interact with wireless Internet services. Usage of WAP is evaluated here in the context of whether it could also be used as a transport protocol for local services, e.g. to access POS services instantly. The obvious benefit would be that WAP is well standardised and it is already widely used within the telecommunications industry.

Unlike the OBEX protocol, the previous version of WAP 1.1 does not offer any separation in architecture (application / session framework). Ericsson has recently completed a study with Bluetooth and WAP 1.1 with mixed success. The main issues were concerning its stability. Now with WAP 2.0 they are replacing WML with XHTML with a view of becoming more robust and open. Nokia are starting to look into WAP 2.0 but suggest it could take up to 2003 before it will be fully ready. They state the first commercial implementations (read browsers), which will use WAP 2.0 should be out 4Q/2002. This is quite an optimistic schedule, due to the WAP 2.0 standard not being fully complete (e.g. wmlscript support).

4.3. Contactless Protocol with ISO 7816 APDUs

The contactless protocol (as specified by ISO 14443) defines radio technology that in this case can be used to carry APDUs (application protocol data units) on top of the block exchange protocol. The generic format of interoperable APDUs is defined by ISO 7816 (specifically parts 4-9), defining two types of APDUs: command APDU that is sent from the reader to the card / device and response APDU that is sent back.

Each APDU acts as a frame (envelope) to convey information between the reader (usually stationary) and the contactless device (usually the card). The envelope holds data, provides space for its type, status and certain control codes, as well as for active application in case of multi-application contactless cards/devices. The set of most common commands is also standardised (following the standardisation of most common elements of the card architecture), leaving space for application-specific extensions.

The use of contactless protocol to carry APDUs is extremely popular and thoroughly standardised, being the most common method to interact with contactless cards and other contactless devices.

4.4 Specific

It is also necessary to consider POS vendors who may also have solutions for the transport between chip card reader, PIN-PAD and POS terminal. Using that also in a wireless environment one single POS terminal could communicate with wired and wireless card readers as well, bringing obvious benefits to the merchant environment.

5 Media Layer Alternatives

So far we have looked at the application layer model (the business logic, etc.) and at the transport mechanism, the method of getting a message from 'A' to 'B'. Now we will turn our attention to the media that is used to establish our protocol. Here we will focus, as previously mentioned, at the retail POS terminal for our transactions.

5.1 Bluetooth

Bluetooth is an open specification for omni-directional wireless communication of data and voice. The PTD will be equipped with a microchip transceiver that transmits and receives in a previously unused frequency band of 2.45 GHz that is available globally (with some variation of bandwidth in different countries). In addition to data, up to three voice channels are available. Each device has a unique 48-bit address from the IEEE 802 standard. Connections can be point-to-point or multipoint. The maximum range is 10 meters. Data can be exchanged at a rate of 1 megabit per second (MBPS) (up to 2 MBPS in the second generation of the technology). A frequency hop scheme allows devices to communicate even in areas with a great deal of electromagnetic interference. Built-in encryption and verification is also provided.

Payments over Bluetooth would work by users selecting via their PTD user interface that they would like to pay for goods. The user will then be prompted (e.g. verbally) to search and lock into the POS terminal via Bluetooth and to initiate a transaction. Alternatively the POS terminal can search and lock into the respective PTD by PTD device name. Transaction details are then sent to and from the PTD and POS as described in the PPA and as applicable to the payment protocol in question (e.g. EMV).

The main concerns with Bluetooth at this stage are the connection times and costs. Currently it takes between 7-10 seconds to establish a connection with another Bluetooth device, which is far from ideal in a local payment environment. Work is currently in progress to find ways of getting around this, reducing the connection times. In a Stockholm pilot, users establish a connection and are given a token as they enter the shop. By the time they are at the point-of-sale, the connection is already established and when locking onto the POS their token is immediately transferred.

Costs are also due to come down in the near future as Bluetooth becomes more popular, with phone manufacturers in particular. It is currently understood that Nokia and Sony-Ericsson are both building a complete Bluetooth platform (based on a Bluetooth Master Server). The target is to implement a "BT product package"; firstly in large markets and then in shopping centres. Here, the 'payment' feature will be only one part of the Bluetooth platform, with other services such as identification of current location, notification of special offers, etc. also being part of the whole package.

There are still major security concerns in Bluetooth that have not yet been resolved. The operational range of Bluetooth is typically longer than the 10 cm range found in ISO 14443, which increases the possibilities for eavesdropping. Also, the discovery problem has not yet been solved.

5.2 Radio Frequency – Contactless

This describes a technology in which a device (namely the card) has no power supply of its own, but receives power when it enters the radio frequency (RF) field generated by a polling reader. The device is fitted with the coil antenna. Communication from the reader to the device is by modulation of the RF field and in the reverse direction by load modulation in the device.

There are a number of proprietary schemes, but standard approaches can be found in ISO 14443 and ISO 15693. The latter describes a “vicinity” card system, not suitable for financial transactions due to a working range of up to one meter.

ISO 14443 is the mature standard of choice for several recent and planned deployments. It describes a “proximity” card system with a range in the order of 10 cm, providing bi-directional, half duplex information exchange at a speed of 106Kbit/s. The standard defines two variants of the radio modulation, A and B. For interoperability reasons and to claim compliance to 14443, a reader must support Type A and B, plus any options. Compatible cards (devices) must support Type A or B, plus any options.

The original intent of ISO 14443 was to define a system where the contactless device is a standard-sized card fitted with the coil connected to the embedded chip. The standard, however, can be applied for devices of any form factor, providing the antenna coil can be made large enough to deliver the necessary power. Further, as the standard defines only the radio interface, it can be also used for devices with its own power supply or for devices where the chip is not dedicated for the contactless communication.

Contactless technology is specifically fitted for solutions that require very fast turnover. The typical transaction time observed in installed systems is around 100ms.

The development of contactless technology has recently embraced dual interface cards: cards where the chip is connected not only to the coil antenna (as with regular contactless cards) but it is also available through regular ISO 7816 contacts. Both interfaces to the card may provide identical or different command sets, depending on the design of the card.

Even though the technology does not provide any transport level security, it is generally perceived secure due to an extremely limited operational range. Application-level security seems to be sufficient for existing applications. Even though existing systems usually operate symmetric cryptography, it is already possible to use asymmetric cryptography if required.

Being passive, the contactless device responds to every communication as long as the reader is close enough to the card. The inconvenience of unintentional communication can be partly solved by providing, for example, a button at the reader to activate reader function at the user's convenience. The risk of hostile communication can be solved, for example, by fitting readers with unique identifiers and keeping a limited transaction log within the card so that a limited audit trail is available.

The introduction of dual interface cards, combined with the ability to store the card in the phone, allows the user to temporary lock/unlock the card depending on needs (e.g. by delivering PIN code to the card and time-out card activities), significantly reducing the risk of unintentional or hostile communications. Such interaction with the user can be further accepted as user authentication or authorisation.

Nokia are currently undergoing handset trials in the U.S with contactless chips included within the handset. This proves to be a fast and convenient way of delivering the contactless solution within the mobile phone, specifically for rapid and small value transactions.

Note however, that the contactless technology may not cope well with transactions where the application logic and security are complex. If security between the device and the reader must be complex due to complex asymmetric key cryptography like TSL, for example, there might be some issues to solve due to very limited power available to the card. On the other hand, if the application logic is complex, which means that the interaction with the user requires several presentations of the device to the reader as well as user interaction with the device, usability might not be optimal.

5.3 Infrared

Infrared communication involves a transceiver (a combination transmitter and receiver) in both devices that communicate. Special microchips provide this capability. In addition, one or both devices may require special software so that the communication can be synchronised. An example is the special support for IR in Microsoft's Windows 95 operating system. In the IrDA-1.1 standard, the maximum data size that may be transmitted is 2048 bytes and the maximum transmission rate is 4 MBPS.

Infrared also seems to be well suited for local transactions. However, as Infrared is a cable replacement technology, it is dependent upon line of sight between devices and intended for short-range (<1 Meter) transactions. Although this limits usability, it may also increase the security level.

IrDA device discovery uses a polling scheme to collect responses from all devices in line-of sight within a one-meter range. The device-performing discovery is called the primary device and the devices that respond are called secondary devices. The primary device broadcasts a message to initiate device discovery. This message identifies the number of discovery time slots in which the secondary device may respond.

Device discoveries may contain 1, 6, 8, or 16 time slots. Each secondary device generates a random number specifying the slot in which it will respond. The primary device sends out a device discovery packet at the beginning of each time slot. If the time slot number matches the random number chosen by the secondary device, it will send a discovery response packet to the primary device. Each time slot must last at least 25 milliseconds, with each response beginning within 10 milliseconds and completing within 70 milliseconds of the end of the primary's device discovery packet. If a device discovery is performed using the maximum number of slots (16 slots), the device discovery time will be 1.12 seconds.

In an average theoretical case, an IrDA-enabled PTD will discover an IrDA-enabled POS in approximately 0.5 seconds, significantly shorter than Bluetooth as shown above.

6 Analysis

6.1 EMV in the mobile environment

This alternative is included as the preferred option in the original PPA published by the Mobey Forum in June 2001. The main idea of this alternative technology is to benefit from the emerging EMV infrastructure and to allow the offering of highly secure, personalised off-line and on-line payments in the local environment through the mobile devices, with a flexible new standard payment protocol.

6.1.1 Business

- **Timeframes**

Whilst EMV is being adopted on an ever-increasing scale, many issuer and acquirer infrastructures and networks are not yet equipped to deal with EMV transactions. The various Visa regions; Asia-Pacific, Central Europe-Middle East & Africa, European Union (EU), Latin America and USA have different implementation plans for the adoption of EMV. However, the Visa EU region has mandates in place to complete migration by 2005. Solutions will require the development and dissemination of new mobile devices. These factors are likely to delay these parties in officially recommending a mobile version of an EMV solution; it will be some years for development and for full acceptance across the EU region. At present there is no specification for this approach and such documentation is a prerequisite.

The choice of a banking-only chip or a combined phone/bank chip is unlikely to impact upon these timescales. In any case the chip has to be bank-issued in order to fulfil the rules of payment associations. Bank-only chips will be readily available, whilst inter-industry chips will require the business interests to be resolved first.

- **Costs**

Given that the infrastructure will exist to support EMV functionality, the infrastructure and network incremental costs are likely to be minimal.

There will be development costs for the mobile devices and POS terminals. The incremental costs for a new mobile device are unknown, but include the new functionality and any specific PIN handling requirements, which with certification may be appreciable. An extra certification phase could cause delays for new mobile device models, and would be expensive for the mobile device manufacturers. Existing POS terminals will have an upgrade cost to equip with non-contact capability and a transport protocol communication.

6.1.2 Technology

- **Availability**

There are currently no Mobile Device/POS functional specifications, security requirements or descriptions regarding certification processes for mobile devices. These would need to be developed before the deployment.

The EMV infrastructure and EMV chips will be available as chip technology before the payment industry is rolled out.

IrFM specifications being defined by the Infrared Data Association (IrDA) at present address the communication framework for the magnetic-stripe world and also for the EMV payments.

The Bluetooth specifications version 1.1 is currently available; however, they are not tailor-made for financial transactions to a physical POS terminal.

Specifications for the RF contactless technology are mature and use low-level APDU command/response transfers. A higher-level financial protocol might be needed for this media protocol.

- **Suitability**
Mobile EMV can work with either OBEX or WAP as transport protocols and can use Infrared, Bluetooth or RF contactless as connectivity protocols. All of following combinations are (in theory) possible with EMV:
 - Infrared and OBEX
 - Bluetooth and OBEX
 - Bluetooth and WAP
 - Bluetooth and APDUs
 - RF contactless and OBEX
 - RF contactless and APDUs

6.1.3 Deployment

- **Terminal Changes**
The POS terminals would need to be retrofitted to accept payment data received from the mobile device (originating from a chip semi-permanently installed within the phone) using non-contact communication. This will involve retrofitting the existing point-of-sale terminals with mobile adapters and installing higher-level functionality at the merchant's location depending upon the choice of the solution adopted or deployment of new POS terminals with the capabilities built-in.
- **System Changes**
It can be assumed that the infrastructure will be upgraded to support EMV data, however a new indicator for mobile local transactions will need to be accommodated. Visa has already defined use of an existing field and value to indicate that a transaction was conducted over a wireless interface. This is expected to help the implementation.
- **Mobile device upgrade**
Under the Mobey PPA, mobile devices will need to accommodate a separate banking chip (dual chip). For this a considerable implementation effort for EMV application is needed. EMV PIN pads are typically single function devices dedicated to EMV applications. Mobile devices on the other hand need to handle several applications simultaneously including the telephony application, local connectivity, PIM (Personal Information Manager), etc. and this may cause problems for the EMV application. These issues need to be resolved.
- **Issuing**
Full-size EMV chips will be readily available from issuers under existing bank-card arrangements and it is only necessary for the chip to be punched out and installed in the mobile device. EMVCo has changed EMV specification to also cover low voltage (3 volts and 1.8 volts) chips and terminals, which reconcile better for mobile usage.

Multiple payment applications (debit, credit) eventually need to be placed on the same multi-application chip in order to offer the same payment functionality for the consumers as of today.

It can be assumed, that at least for a transition period, a full-sized card is needed in parallel.

- **Certification (functional testing):**
Some level of functional testing should be accomplished for EMV. Specific EMV certification may be required for the mobile phones and there will be associated costs. Multiple software versions are characteristic to mobile devices. The certification model where all software changes cause a new certification round is not applicable to mobile

devices, but a special process here is needed. It is also noticeable that mobile device business is very time-critical, putting high pressure on the certification process. Self-certification, which is based on mutually-agreed specifications and where results are accepted by a trusted third party, is an option worth considering. Work to agree on the terms of this and to create the resolution has to continue urgently between the key stakeholders, namely the card associations and the handset vendors.

6.1.4 Usability

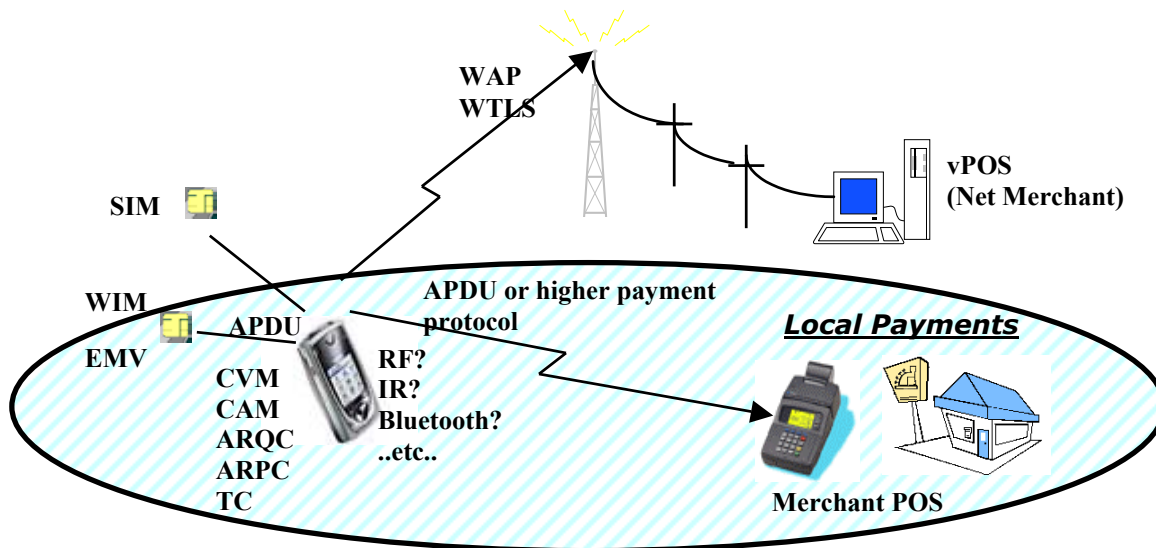


Figure 5: Example of a mobile optimised EMV transaction

- User Experience**
 The user making a financial transaction using a mobile device should be able to find this solution easy and convenient to use. In addition, the solution should be equally secure and consistent with the experience of conducting a financial transaction using a card today at a point-of-sale terminal. In addition, combining the user experience of on-line financial services will further increase the consumer convenience and speed up the mass-market adoption. Users must always have added value in mobile payments when compared to the traditional payment mechanisms.
- Speed**
 In general an EMV transaction takes a little longer than the magnetic-stripe equivalent (offline or on-line). However, the speed also depends upon the Cardholder Verification Method and the media protocol used.

6.1.5 Market Acceptance

- Probability Opinion**
 The EMV infrastructure will evolve in Europe and an approach which levers on this capability will have greater appeal than alternatives that require parallel developments.

6.2 Magnetic-stripe image

The main idea of this technology alternative is to leverage on the existing magnetic stripe payment infrastructure and to allow quick time to market and the beginning of the user habit creation as early as possible.

6.2.1 Business

- **Timeframes**

The issuer and acquirer networks and infrastructure to support magnetic-stripe are in place and no modifications would be required, except for the possibility of an indicator in the messages to show that the data came from a mobile device. POS terminals will need to be modified to accept messages from the handset and the functionality included to select and accept this alternative form of data entry. The time to do this will be the dominant aspect in terms of timescale.

- **Costs**

Processing magnetic-stripe transactions will require minimal upgrades to the current infrastructure. However, cost will be a consideration in terms of whether it is just retrofitting the existing POS terminals with a connectivity interface supporting PTDs, installation of WAP servers and other middleware in a connectivity interface environment or deployment of new terminals with connectivity interface capability built-in. Furthermore, there will be some requirements for functional testing that would need to be accomplished.

6.2.2 Technology

- **Availability**

The magnetic-stripe card-based payment method is existing and well established, but the security of magnetic-stripe cards is weak in comparison to EMV and the development is finished.

There are specifications being defined by Infrared Data Association (IrDA) in an effort to standardise transmission of payment data from the handheld to the point-of-sale (POS) terminal. The IrDA working group called "Infrared Financial Messaging- IrFM" has released a white paper in January 2002.

The Bluetooth specifications version 1.1 is currently available from the Bluetooth SIG; however, they are not tailor-made to financial transactions at a physical POS terminal.

- **Suitability**

Magnetic-stripe can work with either OBEX or WAP as transport protocols and can use Infrared, Bluetooth or RF contactless as connectivity protocols (although Bluetooth might not be an optimal media protocol). All of the following combinations are (in theory) possible with magnetic-stripe image:

- Infrared and OBEX
- Bluetooth and OBEX
- Bluetooth and WAP
- RF contactless and OBEX
- RF contactless and ISO 7816

6.2.3 Deployment

- **Terminal Changes**

The POS terminals would need to be retrofitted to accept payment data beamed from the mobile device using either Infrared, Bluetooth or RF contactless as a connectivity interface. This may involve retrofitting the existing point-of-sale terminals with connectivity adapters or other middleware at the merchant's location, depending upon the choice of the solution adopted or deployment of new POS terminals with the capabilities built-in.

- **System Changes**

The infrastructure for supporting magnetic-stripe data at the back-end exists today. However, a new indicator for mobile local transactions will need to be accommodated.

When the contactless chip (RFID tag) is used, from the POS perspective the sequence will remain the same as with today's magnetic stripe cards: instead of "swiping" the card consumer is "waving" it within the phone. When required, the user is authenticated either by typing the PIN code at a PIN pad connected to the POS or at manned POS with a handwritten signature.

- **Processing Capabilities**

In addition to being able to allow selection of a payment application and the transportation of payment data to the POS terminal, there will not be any additional requirements for processing on the cardholder device. If there is only one application on the chip, application selection capability is not required.

- **Certification (Functional Testing)**

Some level of functional testing will need to be accomplished to enable magnetic-stripe image payments. Generally issuers approve their applications for the Cardholder Verification Method (CVM) functionality (for example, PIN code).

- **Mobile device upgrade**

Mobile device needs to support a payment application to:

- Store a magnetic-stripe image securely.
- Provide access control mechanism (UI) for users.
- Support magnetic-stripe image transmission between the mobile device and the mobile adapter or the POS terminal.
- Support payment method selection.
- Eventually enable new payment method / magnetic-stripe image registration, activation and downloading.

Magnetic-stripe image needs to be stored securely, because it contains the card number, however it does not necessarily require a tamper-proof storage. Mobey-preferred options for storing the magnetic-stripe image are:

- Bank-issued chip card
- Bank-issued contactless chip (RF-ID tag)

If the payment data is stored in the phone memory, secure access control mechanism/environment to access the payment application (User Interface) needs to be established. There will be no support in the handset for an off-line banking PIN with magnetic-stripe data. Using the handset for on-line PIN support will impose onerous security requirements on the mobile device. If the magnetic-stripe image is stored in the phone memory, only non-PIN usage (MOTO) is enabled. Mobey Forum doesn't want to include the phone memory storage as a preferred option, since it feels that user authentication in terms of checking the PIN code has to be possible.

The best solution is to store the magnetic-stripe image as an additional application on a separate multi-application chip containing also the EMV and WIM applications, for example. If this is not yet possible, the image can - as on intermediary solution - be stored on a separate contactless chip (RF-ID tag) issued by a bank.

The additional security features of the chip can be used for storing and using the magnetic-stripe information and PIN-code. Magnetic-stripe application provides the same off-line banking PIN capability as an EMV application (see Chapter 3.2).

- **Enrolment**

Banks prefer the magnetic-stripe image solution because the application already exists and the issuing of the application and cardholder verification both stay under the control of the bank. It is good to remember that the rules of the payment associations prevent banks from placing their payment applications on a non-bank issued platform.

An optimal combination would be to have EMV and magnetic-stripe image applications on the same chip to make possible to use the same mobile phone (and payment chip card)

on both EMV and magnetic-stripe based POS terminals. In those areas where EMV infrastructure is not yet ready, it is enough to put only the magnetic-stripe image application on the chip because it works also on EMV terminals if the user travels in areas where EMV is already in use.

- **Payment method issuing**

Issuing of the payment application and the magnetic-stripe image is depending on the storage of the magnetic-stripe image. Three different options can be seen:

- Magnetic-stripe image is issued and pre-personalised together with the banking chip.
- Magnetic-stripe image can be downloaded over-the-air from the card issuer server to the banking chip (following special requirements).
- Magnetic-stripe images can be downloaded locally (e.g. at a bank branch) over RF-contactless interface to the RF-ID tag by the issuing bank.
- RF-ID tags can be pre-personalised with the magnetic-stripe image by the issuing bank.

6.2.4 Usability

- **User Experience**

The user making a financial transaction using a mobile device should be able to find this solution easy and convenient to use. In addition, the solution should be equally secure and consistent with the experience of conducting a financial transaction using a card at a point-of-sale terminal or a vending machine.

Today there are examples of payment situations where users are not requested to insert a PIN code although they might be spending at least medium size amounts, the Heathrow Express ticket (£23) is one example.

PIN Pads at POS's are becoming more commonplace (e.g. France), which will on the other hand help to create a more consistent user experience evolution path.

- **Speed**

The speed of completing a transaction initiated with a phone containing the magnetic-stripe image is likely to be at least as fast as using a normal magnetic-stripe card.

6.2.5 Market Acceptance

- **Probability Opinion**

There is minimal impact on the existing infrastructure and systems and thus it is a question of user convenience, although the security issues of accommodating the data in the handset and controlling user selection and access may give issuing banks some difficulties. Storing the application on a bank-issued chip platform will increase the security level of the solution. However, the enrolment process needs to be reasonable; in some options it may cause additional logistical challenges for issuing banks.

Magnetic-stripe image application stored on a chip card provides the same on-line and off-line banking PIN capability as an EMV application (See Chapter 3.2). This solution is preferred by the banks (certainly for the short term) due to the application already existing and since the application and cardholder verification both stay under the control of the issuing bank.

If PIN authentication is not used at POS-terminals, MOTO rules should be applied.

It is expected, that in the future there will be more flexible authentication rules for small payments processed through the card payment process, which will also help banks addressing smaller amount payments with the same card payment system.

6.3 WIM Signature

The main idea in this technology alternative is to increase the security level of the payment transaction and possibly unify user experiences in remote and local environments by utilising the WIM application to digitally sign a magnetic stripe payment transaction.

6.3.1 Business

- ***Timeframes***

The issuer and acquirer networks and infrastructure to support magnetic-stripe are in place and no modifications would be required, except for the possibility of an indicator in the messages to show that the payment is either signed or verified. WIM enabled phones with certificate storage and with proximity protocol support can be adapted to accommodate magnetic-stripe images in a fairly short space of time.

A new adapter or modification to POS terminals will be needed to accept messages from the handset using proximity protocol and the functionality included to select and accept this alternative form of data entry. The adapter needs to support PKI certificates (x.509) and signature validation based on a financial institution's public keys. Generally in PKI-based payment transactions the root keys used need to be originated from the card association in question.

Phone changes:

- Earliest pilot capability (phones) in 2002
- Commercial phones earliest in 2003

Mobile adapter:

- Pilot mobile adapter 1 year after the frozen specifications
- Commercial adapters in mass deployment will take years

Payment infrastructure:

- Only optional changes to the protocol
- Clearly not a limiting factor
- The mobile payment indicator may be updated within one year, but the signed magnetic-stripe information takes longer time (if it is even possible to do).

There is no specific WIM public key in use. The card schemes would need to specify the WIM root key and to install it in all local payment POS terminals. This would be a major effort and would at least delay the take-up of this solution.

- ***Costs***

Processing magnetic-stripe transactions with a WIM Signature will require some PKI upgrades capable of handling WIM signatures (x.509) to the current infrastructure. However, cost will be a consideration in terms of whether it is just retrofitting the existing POS terminals with mobile adapters, or deployment of new terminals with mobile and PKI capability built-in.

From a mobile phone perspective, magnetic-stripe transactions with WIM Signatures can be enabled utilising a separate multi-application / WIM chip, which may already be in the phone for user authentication over remote channels (dual chip). The same card can offer storage facility for the magnetic-stripe image.

6.3.2 Technology

- ***Availability***

WAP forum WIM specification has been frozen since 1999 and there are already commercial implementations on the market.

There are no specifications for payment transaction security with a WIM signature (responsibilities, fraud, non-repudiation etc). Neither do any technical specifications exist on how to sign a magnetic-stripe transaction by WIM.

- **Suitability**

WIM signature can work with WAP as the transport protocol and can use Bluetooth as the connectivity protocol. The following combination is possible with a WIM signature: Bluetooth and WAP.

Using other transport protocol such as OBEX or other connectivity protocol (i.e. Infrared or RF) would require extra specification and implementation effort.

6.3.3 Deployment

- **Terminal Changes**

The POS terminals would need to be retrofitted to accept payment data beamed from the mobile device using a proximity interface, or a new additional component, a mobile adapter, is needed to make mobile payments transparent for POS terminals. The terminal needs to support PKI validation.

- **System Changes**

The infrastructure for supporting magnetic-stripe data at the back-end exists today. However, adding a new data field for signed magnetic-stripe data might be a major change to the existing magnetic-stripe based payment protocol.

- **Mobile device upgrade**

Mobile devices will need to accommodate a separate banking chip containing the WIM application. In addition, the magnetic-stripe image requires a secure storage, which can well be the same chip card.

In order to transmit payment data over a proximity interface the mobile device needs to support Digital Signature functionality (WAP/WIM) over Bluetooth.

- **Access Control**

One advantage of the mobile solution is that access control to the payment application can be implemented. This prevents a lost phone being directly equivalent to a lost card. The WIM-NR PIN is used for the cardholder authentication and for card verification.

- **Issuing**

A payment method, which corresponds to a client certificate including a magnetic-stripe image, can be issued either together with the WIM card or can be downloaded over the air based on WAP Forum WPKI specifications.

6.3.4 Usability

- **User Experience**

The user making a financial transaction using a mobile device should be able to find this solution easy and convenient to use. A clear advantage of this solution is that it makes both remote and local payment user experience similar. However, the user needs to be educated for certificate usage, which might be a challenge. A certificate corresponds to a branded payment card.

- **Speed**

In general, WIM signature transactions take a little longer than the magnetic-stripe equivalent, but transactions are obviously faster than EMV transactions. However, the Bluetooth and WAP dependency may increase the actual user interaction times.

6.3.5 Market Acceptance

- **Probability Opinion**

Magnetic-stripe payments are largely and widely used around the globe. By adding additional security based on PKI signatures the method may address also financial institutions' security concerns. On the other hand, WIM/PKI technology is widely supported among mobile device vendors and has wider support also among the whole telecommunications industry.

WIM/PKI infrastructure will be at least as difficult as EMV to implement into the payment infrastructure. First EMV specifications were ready in 1996, and the specification work started long before that. The liability shift is planned for 2005. This is giving an indication of the time-cycles of developing new payment protocols. It might be difficult to motivate the payment industry to develop the magnetic-stripe payments any more. In any case this would be an intermediate step prior to full EMV.

Taking into account the lead-time for the required changes, this might not be the best option as an intermediary step.

6.4 Connectivity/Transport Protocol Comparison

The following table describes the possible connectivity/transport protocol combinations and their main characteristics regarding the local payment. The characteristics are listed based on the current understanding, and it is possible that some of them will be updated after more experience has been gathered about each connectivity/transport protocol combination.

Connectivity/ Transport Protocol	Confidentiality and Integrity	Usability	Reliability	Transaction time
Infrared/OBEX	Short distance/user control, possibly some additional security required	Reasonable	Poor	Good
Bluetooth/OBEX	BT Security, possibly some additional security required	Good	Good	Poor
Bluetooth/WAP	BT Security + WTLS/TLS	Poor	Good	Poor
RF/OBEX	Short distance/user control, possibly some additional security required	Good	Good	Excellent
RF/ISO 7816 APDU	Short distance/user control, possibly some additional security required	Good	Excellent	Excellent

Table 4 – Characteristics of transport and media layers

All of these media and transport level protocols will support application level encryption.

Infrared/OBEX solution does not provide any channel protection but because of the nature of Infrared line-of-sight distance connection it is rather difficult to eavesdrop the transaction without user perception. However, in some cases the Infrared reflections may be captured quite far from the devices. Therefore some additional application layer security may be needed to prevent eavesdropping of the card data.

Usability of an Infrared/OBEX solution is quite poor because the mobile device needs to be pointed towards the POS terminal to maintain Infrared connection all through the transaction. Otherwise the usability can be relatively good; the user activates the infrared and moves the mobile device close to the terminal, which activates the payment application. Infrared connection set-up and actual payment transaction time can also be relatively fast. Reliability in a bright/daylight environment and sensitivity to line-of-sight are the biggest problems of the infrared-based payment.

Bluetooth/OBEX solutions can utilise the underlying Bluetooth transport security (mutual authentication, integrity protection, and confidentiality). Some additional application layer security may be needed to prevent eavesdropping of the card data. Usability can be built to be relatively good; the user activates the payment application on the mobile device, which establishes the connection to the terminal. Bluetooth connection set-up time however is quite long. Very noisy Bluetooth environments may cause reliability problems in certain situations. The known Bluetooth problems include, for example, handshake challenges in typical merchant-store situations. For instance, if there are 10 customers trying to establish a connection with 5 POS terminals simultaneously, there has to be a robust mechanism for ensuring that devices are “locked” to talking only with their correct counter-parties.

The Bluetooth/WAP solution offers a good protection for eavesdropping since both Bluetooth transport security and WAP transport layer security (WTLS/TLS) can be used. The usability can be built to be optimal for payment situations where the user needs to make selections on the mobile device UI. However, creating a good usability for simple payments is challenging; the user activates the WAP browser and connects to the merchant payment service, selects the payment method and signs the transaction. Bluetooth and WAP connection times are relatively long. Very noisy Bluetooth environments may cause reliability problems in certain situations.

RF/OBEX solution provides a reasonably good eavesdropping/integrity protection because of the very low transmission power used by the reader, which limits the maximum connection distance to around 10 cm. Challenge-response (to be developed) combined with application-level security can be used to protect the transaction. Unintentional or hostile communication risk could be resolved with the introduction of dual interface chips.

The usability of the RF/OBEX-based payment solution can be quite good as the user brings the mobile device close to the reader, which activates the service. If the dual interface is used the user can make the necessary selections and approval on the device UI. Alternatively the user can use the reader (at POS) for this purpose. Note that if the transaction goes beyond the simple case, the multiple presentation of the device to the reader is needed.

The connection set-up time as well as the actual payment transaction time is very short. RF is considered to be a reliable connectivity method. OBEX reliability with RF bearer is not known.

The RF/ISO 7816 APDU solution provides the same security level as the RF/OBEX solution. The usability depends on the application. The simple RF/ISO 7816 APDU solution allows the user to approve the payment by bringing the mobile device close to the reader. Usability of a more advanced RF/ISO 7816 APDU model can be similar as in RF/OBEX solution and requires either dual interface chip or interaction with the POS. The connection set-up time and the payment transaction times are very short and the reliability is supposed to be very good.

7 Industry Bodies Developing Local Transaction Specifications*

There are four other leading industry groups that have already contributed with open standards for local transaction solutions today. These bodies, whose contributions have been evaluated by Mobey Forum, include:

- The Mobile Electronic Transaction Forum (MeT Forum).
- The Infrared Data Association's (IrDA) Infrared Financial Messaging Special Interest Group (IrFM SIG).
- The Bluetooth Special Interest Groups (Bluetooth SIG) Short-Range Financial Transaction Study Group (SRFT SG).
- The National Retail Federation (NRF).

Since the area is developing fast, there might be standards' bodies whose contributions were not yet ready at the time of writing, or with whom Mobey Forum has not had a chance to co-operate yet. Thus this list might not be all-inclusive.

There is close cooperation between the organisations listed above and a strong desire by all to create a single set of standards for worldwide compatibility of mobile local transaction solutions.

7.1 The MeT Forum

MeT (<http://www.mobiletransaction.org>) is an initiative started by Ericsson, Motorola and Nokia to establish a framework for secure mobile transactions – the ability to buy goods and services using a mobile device. One of the 3 missions of the MeT forum is to enable the physical or local transaction environment by enabling payment from a mobile terminal to a merchant at the point of sale. Today, the MeT forums' local transaction solution proposes the extension of a browser-based remote purchase model to the local environment using Bluetooth¹.

MeT is exploring the Local Transaction model more closely and some efforts are underway to share work between the IrFM SIG and the MeT forum.

7.2 The IrFM SIG

IrFM is a Special Interest Group formed by the IrDA (<http://www.irda.org>) to define transaction-usage models, profiles, and protocol layers to enable hardware, software, and systems designers to develop globally compatible IrFM-compliant products. Key participants within IrFM include Palm, VISA International, Verifone, Ingenico, Toshiba, In2M, Extended Systems, Zilog, C-SAM, Harex InfoTech, CrossCheck, and others.

The IrFM "Point and Pay Profile" defines a transaction infrastructure built on top of IrDA and the IrOBEX protocol for performing point-of-sale transactions, now also with chip cards. Currently, the IrFM SIG has a draft version of the specification that is being reviewed by the general membership of IrDA.

The following graphic (*Figure 6*) describes the current approach defined by IrFM and MeT.

* Taken primarily from in2M Publication Paper 'Infrared and Bluetooth Transactions at Point of Sale' (24/09/01)

¹ MeT Retail Shopping. Version A. (21 February 2001) <http://www.mobiletransaction.org/pdf/MeT-Retail-Shopping-20010221.pdf>

IrFM and MeT

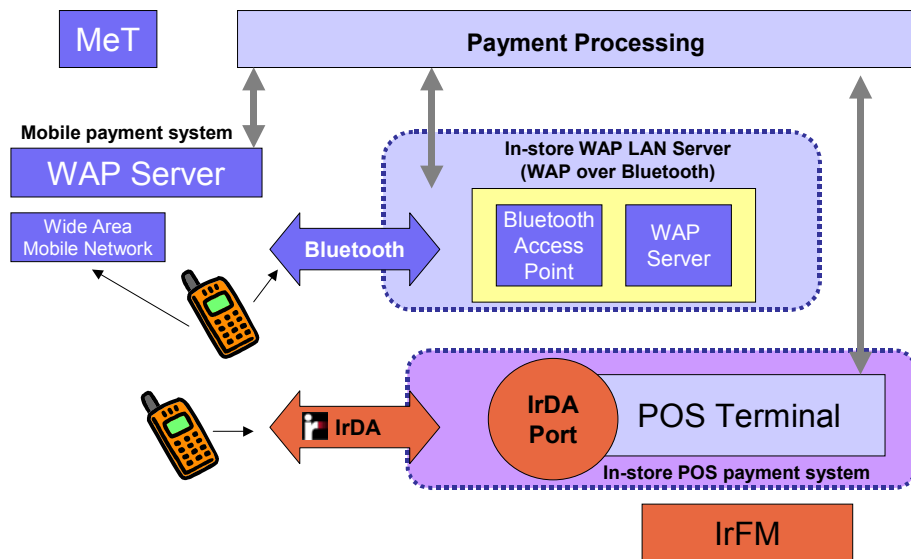


Figure 6: IrFM and MeT approaches

7.3 The Bluetooth SIG SRFT Study Group

The Bluetooth SIG SRFT Study Group is a research group examining the development of a profile that improves the device discovery and connection times for short-range financial transactions at the point-of-sale. Today, the group is co-chaired by Toshiba and In2M with participation from Toshiba Tech, Verifone, Panasonic and IBM.

Research results and any specifications from this group will be proposed to MeT for the enabling of a faster user experience with Bluetooth at the point-of-sale.

7.4 The National Retail Federation - ARTS

The Association for Retail Technology Standards (ARTS) of the National Retail Federation is a retailer-driven membership organisation dedicated to creating an international, barrier-free technology environment for retailers. ARTS was established in 1993 to ensure that technology works to enhance a retailer's ability to develop store level business solutions. It was also to avoid situations that limit a retailers' ability to implement change, while providing industry standards designed to provide greater value at lower costs.

ARTS has three standards:

- Standard Relational Data Model, supporting all retail applications.
- Unified Point of Service, POS device interface specification.
- IXRetail standard XML schemas to interface applications within the retail enterprise.

In January of 2002, ARTS accepted a proposed XML-schema for digital receipts by the Digital Receipt Alliance, which was formed and led by NCR Corporation. Other founding members of the Alliance included America Online; Microsoft; Office Depot; ValiCert, Inc. (formerly known as Receipt.com); RCS and VeriFone, a division of Hewlett Packard Company. Currently, both MeT and IrFM are working together with the IXRetail group to define a mobile receipt profile of the full Digital Receipt Alliance XML-schema.

7.5 Conclusions

Paying with your mobile phone or PDA is a vision that is quickly becoming a reality. A number of proprietary IrDA and Bluetooth payment solutions have risen in the last several years, but they have been more like technological demos rather than mass or even regional-market rollouts. With the industry standards mentioned in this document reaching completion by the first quarter of 2002, Local Transaction technology will gain a strong foothold and begin its rollout onto the world stage. The topic for debate will be whether Bluetooth, RF or IrDA will be the primary media technology for conducting these transactions.

Where other groups are lacking in knowledge is from the financial perspective. The majority of these groups concentrate on the optimal media layer. This is where the Mobey Forum can work with these groups and act as a major Financial Industry representative in ensuring our views in this business case are preserved.

We are entering a new era of payment technologies and solutions where the Mobile Electronic Wallet will one day supplement and perhaps replace your physical wallet. Local Payment is truly a disruptive technology poised to improve the way consumers purchase and merchants sell.

8 The Preferred Payment Solution for Local Payments

The Mobey Forum is now proposing a migration path, which will bring us to the ultimate target, enabling EMV-payments with mobile phones.

8.1 The First Step: Contactless Chip and Existing Infrastructure

The first step on this migration path is to store a Magnetic-stripe Image on a contactless chip card, or RF-ID tag, and to combine it with user authorisation in terms of a PIN code given at the POS. The next picture illustrates this solution.



Figure 7: Payment with Magnetic stripe image on a RF-ID Tag with PIN verification at POS

For quicker implementation within this phase in development, mobile phones are introduced with contactless chips that contain the image of the magnetic stripe comparable with the existing magnetic stripe card. The image can be transferred to the reader at POS similarly to the way the card is presented today; in practice consumers just wave their phone close to the POS or ATM to initiate the payment.

If the transaction requires authorisation in the form of PIN code, a separate PIN entry device connected to the POS terminal or ATM PIN pad can be used. For off-line transactions there is a provision for the PIN code being stored together with the smart card image. For online transactions there is a mechanism for checking the PIN as well. (See Chapter 3.2 for details.)

The following picture illustrates the withdrawal at an ATM with this solution.



Figure 8: ATM Withdrawal with the contactless chip within the phone

This step aims mostly at user education, as consumers that are not familiar with contactless technology or PIN entry – instead of the traditional hand-written signature – will be introduced to the concept. In addition, the usefulness and convenience of the solution can be quickly verified.

RF-ID has already become popular throughout the world where consumers wave their phones over RF readers at POS terminals to pay for goods or services. Existing solutions are mainly closed systems and they usually do not use any form of authentication or authorisation, only the physical presence of the chip is required to make a payment.

The Mobey banks suggest that there should be means for requesting user input/ authorisation of payment in an open payment system. However, in many cases, risk management can address the concern of user authorisation; several factors about the transaction can be taken into account. It is possible to combine an initiation of payment by waving the phone with the RF chip at the POS or ATM with performing the user authorisation at the POS or ATM. This is the option included in the Mobey-preferred solution for situations where user authorisation is requested for business reasons.

8.2 The Second Step: A More Integrated Solution – PIN Entry at Mobile

Initially, for quicker implementation, the magnetic-stripe information will be stored within a RF-ID tag in the phone cover and not being fully integrated into the mobile device. Gradually the dual interface chip is planned to be introduced. This – together with possible further integration to the phone functionality – will further increase the customer convenience by allowing the user to better control the activity of the chip and the transaction. Specifically, it is envisaged that PIN entry will be served ultimately by the mobile phone, not by the POS. This will be a rather visible step to the consumers.

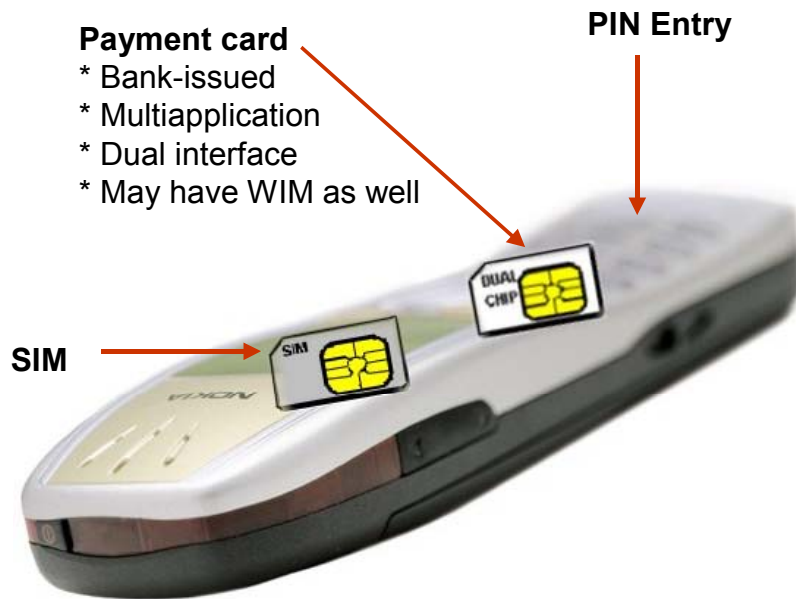


Figure 9: Further integration - PIN Entry moving to the mobile phone



Figure 10: Mobile Local Payment at POS with PIN-code entry through the mobile device

Parties may adopt the process at various stages throughout the road map. For example, there will be some who do not want to invest in a separate keypad at point of sale, but request to have user authorisation. They may wish to wait for the development to include the use of the mobile phone keypad for entering the payment application PIN code. This proposed road map

is designed to be a quick-to-market solution leveraging on the current infrastructure, and building user habit as soon as possible.

This step towards our initial requirements would ensure a great deal of user convenience and speed of transaction time. The introduction of dual interface cards and the close proximity of the device would also ensure the connection was secure with minimal interference from external parties. This would satisfy a number of the issues mentioned by the various stakeholders in Table 3.

8.3 Towards the Target Solution – Mobile EMV Payments

From the technical- and payment-industry perspective the second major step on the migration path is to switch from magnetic stripe payments to the EMV-based payment process. This shift will be gradual and it is not likely to be very visible to the consumers. The EMV-based solution optimised for use with mobile devices, where the application is placed on a semi-permanently installed bank-issued chip within the mobile device, is expected to be available around 2005. The final selection of transport and media protocols will be visible along the path when technology develops further and several technical solutions are better tested. Discussion within the industry is expected to continue on these details. While merchants', phone and POS manufacturers' viewpoints are an important element there, the solution needs also to fulfil the financial industry's specific and other practical requirements.

The EMV-based mobile local payments are the next logical step and our eventual goal. However, at this stage, due mainly to the technology still maturing, it is too early to predict how this will fully evolve. There are high-level recommendations made in section 3.1 as to how EMV could be optimised for use in the mobile environment. This work will continue over time together with analysis of the various forms of transport and media layers as they mature closer to the time. It is important to remember that this solution will be based on the current EMV specifications and is NOT a proposal to re-write the existing EMV specifications.

8.4 Conclusions – the Migration Path

From the user experience-creation viewpoint there are two stages: first, the user will only initiate the payment by waving her phone at the POS. At the second step, when consumers have become more familiar with the usage of PIN codes, they will gradually start to use their familiar and personal phones for inserting the PIN code.

From the technology perspective, the two steps are the RF-ID tag, a form factor of contactless chip, which at the second phase changes to a dual interface contactless chip, and can then also contain other applications, like the WIM application for remote usage. The final decisions on the media and transport protocols will be done after more practical experience is available on the usage of the proposed solutions.

From the payment-industry viewpoint there are also two steps: in the beginning, payments are performed through the magnetic stripe infrastructure, and at the second phase a gradual move towards EMV standard is included.

All of these steps are illustrated in the figure below.

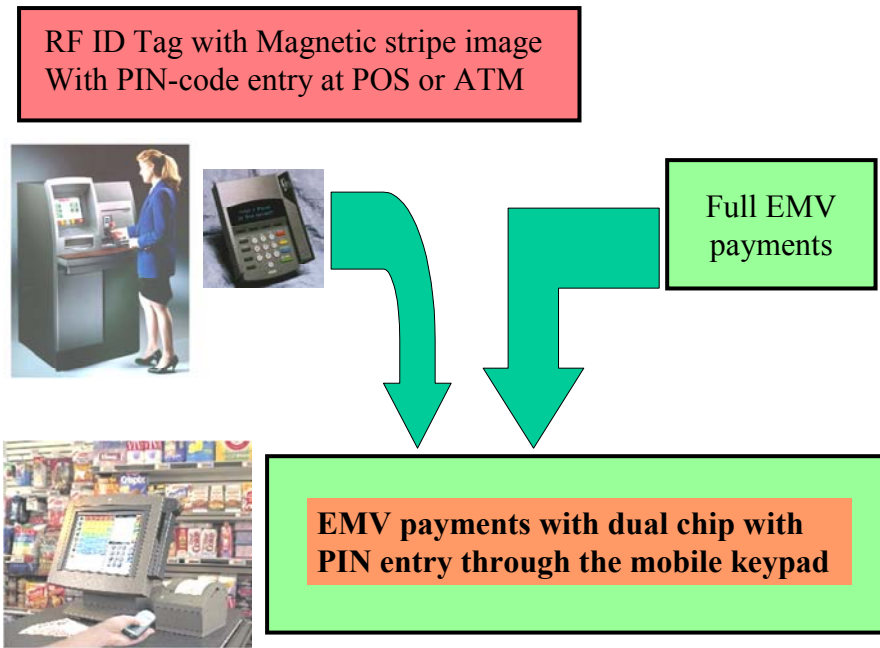


Figure 11: The migration path towards fully integrated EMV-based mobile payments with mobile PIN entry

The whole roadmap is illustrated in the figure below from the perspective of how it is expected to evolve along the time aspect.

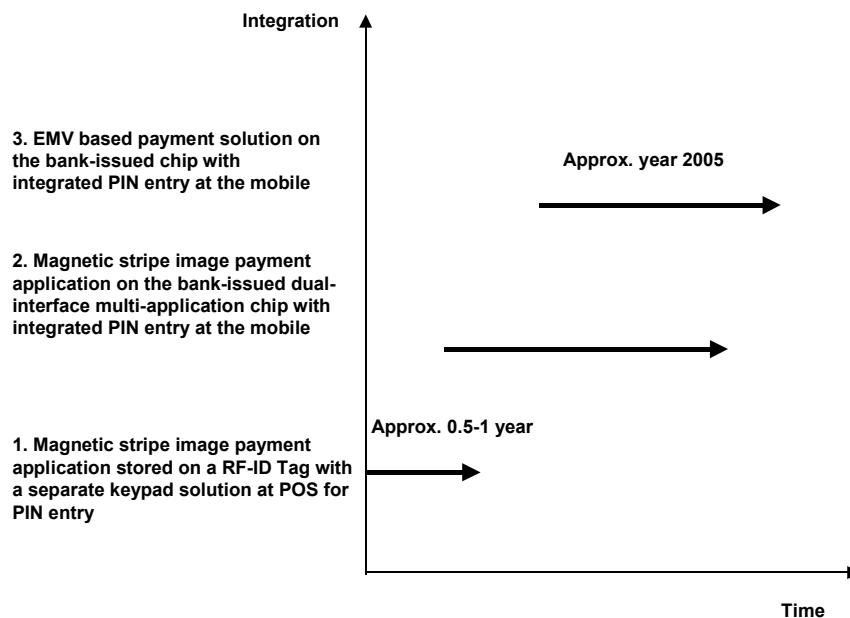


Figure 12: The migration path along time towards EMV-based mobile payments

In formulating this strategy a balance is made between a quick-to-market solution and one that will work in the foreseeable future with the introduction of EMV. Currently, there are many

proprietary mobile-payment solutions. Therefore, it is important that we establish a payment method using the fundamentals of the Mobey principles early on, before the market gets too saturated with different solutions confusing the consumer. Due to the early stage of EMV it is not, at the time of writing, possible to agree a mobile optimised version of EMV to adopt in mobile payments. However, it is agreed that this should be the next major migration step from the payment-industry viewpoint. This is because it will tie in with POS vendors and retailers upgrading their systems to accept the EMV protocol, facilitating the market adoption and thereby offering an unified payment protocol as an end result.

The immediate next steps of the Local Payments development within the Mobey Forum and within the Industry include: banks as owners of the service proposition working together with EMVCo and the supporters of the EMV-specifications, and handset and POS vendors to accommodate EMV specifications to optimise mobile usage. This work is urgent, since the liability shift of 2005 is getting closer and the mobile payment capability should optimally be included in the POS devices when merchants upgrade them for the EMV migration. In addition, the remaining issues (e.g. handset certification) need to be cleared at the earliest possible time, in order to speed up development of suitable handsets.