



The Preferred Payment Architecture Executive Summary

Requirements for manufacturers and standardisation bodies

Version 1.0

**Approved by the Mobey BoD on
25.06.2001**

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

Legal Notice

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

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

1	INTRODUCTION.....	4
2	SCOPE.....	5
3	BUSINESS REQUIREMENTS.....	6
3.1	PAYMENT OPPORTUNITIES.....	6
3.2	REQUIREMENTS	6
3.3	SECURITY	7
4	THE MOBEY PREFERRED PAYMENT ARCHITECTURE	8
4.1	THE PREFERRED ARCHITECTURE FOR REMOTE PAYMENTS	8
4.1.1	The Server Wallet concept	8
4.2	THE PREFERRED ARCHITECTURE FOR LOCAL PAYMENTS	9
4.3	THE MISSING PIECES IN THE LOCAL PAYMENTS ARCHITECTURE.....	10
4.3.1	Issues to be solved with an EMV-based solution for Local Payments.....	10
5	CONCLUSIONS.....	12
6	NEXT STEPS	13

Editor's Preamble

These documents have been created with teamwork to ensure that different viewpoints and opinions are covered as much as possible. To this end, the following have contributed in creating these documents:

- Ben Arber from HSBC has contributed to the Executive Summary and Business documentation.
- Petri Pirhonen from Nokia has contributed, particularly to Chapter 3 of this document.
- Mike Thomas from Barclays, Alan Mullet and Tim Tompkins from Barclaycard have contributed to Chapters 4 and 5 of this document.
- Olle Melin from Handelsbanken, Jan Bartelen and Leonard Franken from ABN Amro have contributed to Chapter 4 of this document.
- Ville Vakkilainen from Sampo Bank has contributed to Chapter 4 of the Technical document.
- Jouni Jaakkonen from Nordea has contributed to Chapter 4 of the Technical document.
- Liisa Kanninen from Mobey Forum / Nordea has contributed to various chapters of this document.

As editor of this document I would like to take this opportunity to thank all Mobey Forum members for their valuable contributions in the process of creating this document.

Helsinki 25.06.2001

Liisa Kanninen

1 Introduction

This Executive Summary outlines the findings of the Mobey Forum business and technical documentation.

The purpose of these papers is to substantiate the Mobey Forum's viewpoint on mobile payments through creating business and technical requirements, evaluating potential business models and technical solutions, and making recommendations to standardisation bodies, handset manufacturers, payment schemes, network operators and technology suppliers to implement the required solutions.

This document forms a basis for discussing with and advising technology suppliers, network operators, standards bodies and other interested parties in the m-commerce arena. The target audience for this document are members of standardisation bodies such as the WAP Forum, handset and middleware manufacturers, financial services providers along with other companies interested in mobile commerce.

The business documentation consists of consolidated consumer experience and financial institution business criteria for mobile payments. It also addresses the requirements related to trust infrastructure. The technical documentation evaluates various potential technical solutions for the payee's and payer's architectures related to mobile payments and the required trust infrastructure. It also addresses the technical requirements such as interoperability and security related to these solutions.

The goal of the Mobey Forum is to see its preferred payment architecture used whenever mobile phones are used for banking or payments. However, the vision does not mean replacing existing payment or banking methods overnight.

The mission of the Mobey Forum is to encourage the use of mobile technology in financial services - such as payment, remote banking and brokerage. It aims to do this by:

- Raising the awareness of mobile financial service implementations
- Facilitating the open provisioning of mobile financial services
- Identifying business considerations and working to obtain the interoperability of the technical and security requirements for the mobile finance industry, in order to promote competition
- Acting as an active liaison between various standardisation fora/forums in both the mobile and financial industries, so as to promote competition.

Founder members are ABN AMRO Bank, Banco Santander Central Hispano, BNP Paribas, Barclays Bank, Deutsche Bank, HSBC Holdings, Nordea, SEB - Skandinaviska Enskilda Banken, UBS, Visa International, Ericsson, Nokia and Siemens.

More information about the Mobey Forum can be found on its website:

www.mobeyforum.org

2 Scope

The scope of the collective documents is to devise a Mobey Forum preferred international mass-market solution for mobile payments.

The mobile handset is likely to become a payment device. However, this provides a challenge to banks who will need to migrate (or follow) their customers to this new payment vehicle and adapt their offerings to support it — whilst also promoting open solutions.

This solution encompasses a recommended technical architecture that meets the stated Mobey business requirements from the perspective of financial institutions, handset manufacturers and payment associations.

The proposed solution was reached by undertaking the following process:

1. Defining the requirements from a user and financial institution perspective.
2. Fully evaluating all existing payment models and technical options.
3. Design an architecture catering for the aforementioned requirements taking advantage of the most fit-for-purpose technical options.

This process is fully described in the two related documents, however the business document formulates these requirements. The scope of the business documentation can be summarised thus:

- To describe, in detail, the different experiences involved in making a mobile payment transaction from the user's standpoint.
- To design consolidated requirements for mobile payments from the perspective of consumers, financial institutions and merchants.
- To prioritise and address the key issues involved in facilitating mobile financial transactions.

The technical document takes the business requirements as a starting point, examines the possible technical alternatives both from a payer's and a payee's standpoint and recommends an overall architectural solution.

3 Business requirements

In general, the business documentation assessed the following three key areas.

1. How are mobile payments likely to evolve from a user perspective and are remote or local payments likely to be most common initially?
2. What are the related business requirements?
3. What level of security is required to execute mobile payment transactions?

3.1 Payment Opportunities

With regard to the first key issue, it is important to clarify the concepts of remote and local mobile payments. Remote usage consists of, for instance, a telephone order (attended or assisted) or a web-shop purchase (unattended or unassisted). Local usage would be shopping face-to-face or at a self-service site. Remote mobile shopping is already happening, offering a variety of opportunities, but it is expected to grow rapidly once convenient authentication methods towards server wallets are available. The breakthrough of local wireless shopping will probably be slower than remote shopping, due mainly to the slower development cycle of the required technology. But in reality, local payments have the potential to be widely popular in the long run.

Local payments will in the long term offer benefits for merchants in terms of cost savings if manned POS terminals can be turned into non-manned terminals or if customer throughput time can be increased. Likewise, acquiring new customers and additional sales with a more convenient service is also possible.

A payment standard needs to be implemented into mobile phones to enable local payments. Enabling local payments with a mobile-optimised but existing standard, for instance EMV will add significant value for banks, such as in situations where off-line payments are supported by POS terminals.

3.2 Requirements

Four principal categories were identified when substantiating business requirements for mobile payment transactions. These are, in order of importance, **customer proposition, business priorities, technical issues** and **implementation issues**.

The main elements within each principal category were assessed on their relative level of importance, in an overall mobile payments architectural solution, from the point of view of Mobey members. The categories are explained in the order of priority in the business documentation.

The customer proposition was considered to be the most important major category; simply on the understanding that if a mobile payment service was not easy-to-use, did not provide value-for-money and was not convenient, it would not succeed.

Other than security (see below), the main business requirements are the concept of personal trust coupled with ease-of-use for customers and the belief that the customer should not be forced to select a specific operator to take advantage of the service. As every bank cannot be expected to forge bilateral agreements with all operators in their specific markets, operator-independence is a necessity for a global solution.

3.3 Security

In terms of the security level, customer authentication is envisaged to be the most important security feature from the perspective of a financial institution. It is the belief of the Mobey Forum that strong authentication is preferred for macro-payments; while for transactions of a smaller amount (e.g., under EUR100) could use a less robust form of authentication.

The level of security will also depend on the type of purchase. For example, some local self-service or Internet micro-payments require only minimum security, as far as the product or service is not re-sellable. On the other hand, purchasing some low-value re-sellable items may require strong security.

Ease of use and implementation are key: the highest security level includes the use of mobile PKI by the issuing bank, for example with a bank-issued WIM application and certificates in the handset. The user confirms the transactions by a PIN-code, which is checked off-line by the bank-issued card. Using this solution with a strong level of security is still consumer friendly, since the same PIN code is used frequently.

The decisions, when and how the security levels are adjusted for physical and digital goods, or micro-, mini- and macro payments, are strictly under control of the financial institution assuming liability for the transaction.

The selection of a local payment protocol and standard Interoperability Domain security protocols, be it 3D SET, 3D Secure, SPA-UCAF or any other, is crucial when designing the preferred payment architecture. Mobey Forum stresses the need to create standards for this area, which should happen within a cross-industry effort.

Other key security components include confidentiality, integrity and non-repudiation and these are studied in depth in the documentation.

4 The Mobey Preferred Payment Architecture

The preferred technical architecture is the optimum solution that fulfils the consolidated requirements of Mobey banks in the short and long term. The requirements for the user's system (handset), the issuer's or acquirer's infrastructure, and merchant's systems are all addressed.

The technical documentation concentrates on one key question:

- What might a generic mass-market mobile payment architecture, applicable across multiple markets, look like?

The preferred payment architecture consists of both payer's and payee's architectures. Furthermore, this architecture consists of various components that include alternative authentication methods and different payment models suited to different scenarios such as micro, mini and macro payments in remote and local environments.

The Mobey business documentation identifies two basic payment scenarios, remote and local, as well as 11 overall payment opportunities. The architecture is suitable for all types of usage with the possible exception of mobile person to person (P2P). However, Mobile person-to-person payments are already possible via use of WAP banking, which allows a mobile user to transfer money to another person by direct account transfer.

Taking the requirements of Mobey banks into account, it was recognised that the preferred solution should be:

- Operator independent
- Be based on a bank-issued second chip
- Suitable for mass-market

These requirements indicated that a dual-chip handset would be the best solution; it is the most probable scenario when taking both business and technical issues into consideration.

The dual-chip solution is also the preferred solution of the handset manufacturers that are members of the Mobey Forum.

4.1 The Preferred Architecture for Remote Payments

The preferred architecture for Remote payments is explained within this Chapter in high level.

4.1.1 *The Server Wallet concept*

The preferred architecture for Remote payments includes a Server Based Wallet (SBW), an interoperability domain security protocol and an end user authentication method.

A bank usually operates the Server Wallet - or a third party, if so requested by the issuing bank.

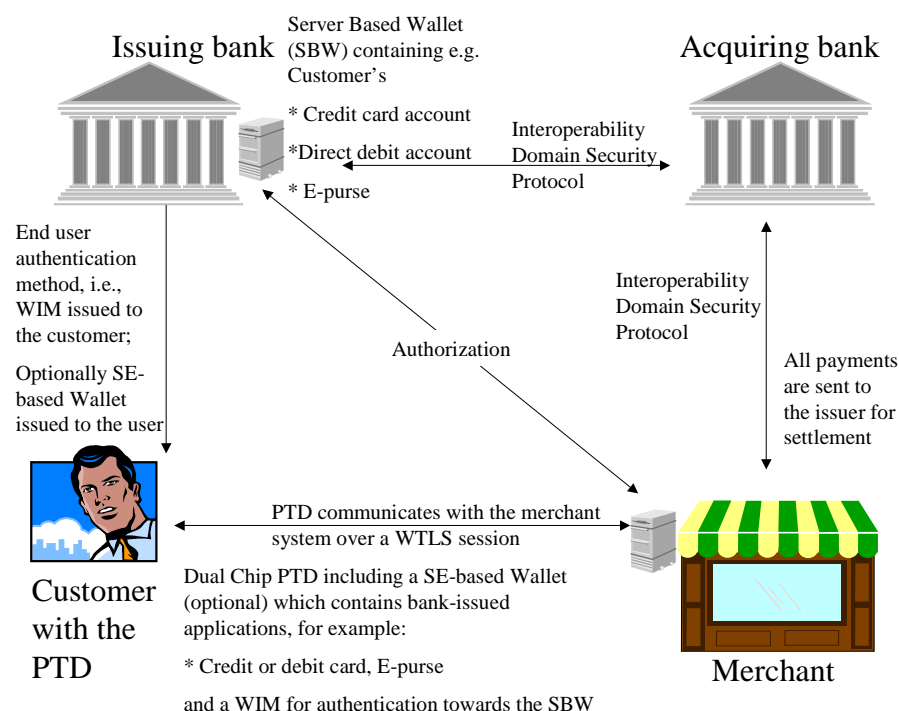
The selection of the interoperability domain security protocol - 3D Secure, 3D SET, SPA or another - is up to the issuer and may vary depending on the situation. Mobey Forum stresses the need to create standards for this area, which should be formulated by a cross-industry initiative, including all associated organisations.

The issuer also selects the end user authentication method, along with the requirements for the level of security (depending on the purchase in question). This authentication method may well be a password-based mechanism in the beginning, the upgrade path and preferred solution being a dual chip phone with WIM and digital signature capability.

E-purse is one viable option for remote payments, especially for micro transactions. Both server- and chip-based e-purses are included in the architecture.

The following diagram describes the preferred architecture for remote payments in high level. This architecture is explained in more detail within the Mobey Forum PPA Technical document.

Picture 1: The Preferred Architecture for Remote Payments



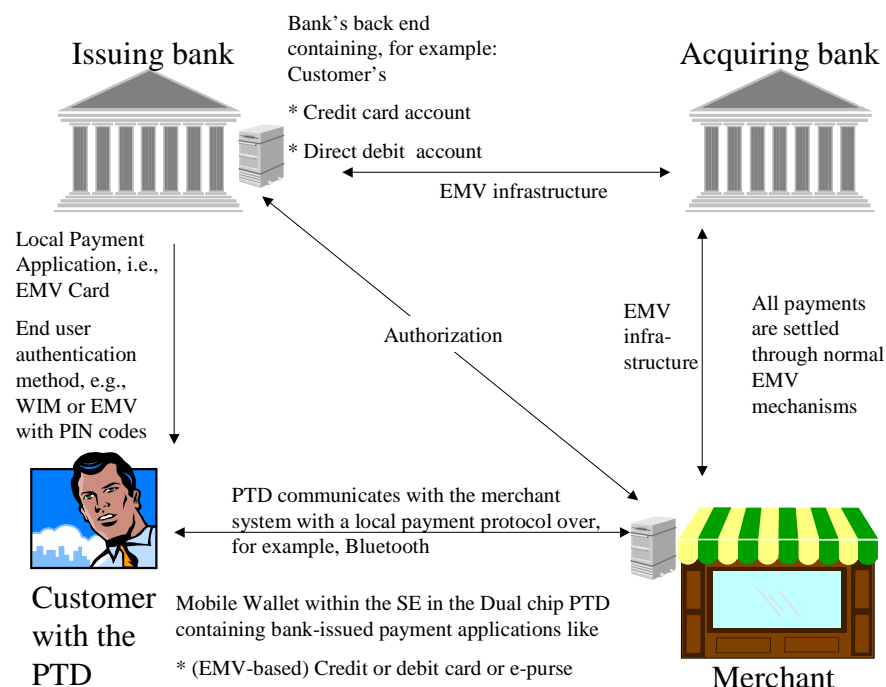
4.2 The Preferred Architecture for Local Payments

The preferred architecture for local payments is a solution based on a bank-issued card with the payment method embedded in or programmed on it. The preferred solution consists of a bank-issued EMV card in the customer's dual chip phone, which communicates with the POS over a local payment protocol. If the current issues with EMV aren't solved in the near future and a mobile optimised EMV isn't rolled out globally within the next 3-5 years, the bank-issued payment method on the chip card might be at first based on another method. In case an intermediary solution is required, alternative methods will be evaluated separately.

E-purse is one viable option for local payments, mainly in the form of a chip-based e-purse, since local transactions may be off-line and a server-based solution would thus not fulfil the requirement of a fast and cheap transaction.

The following picture describes the preferred architecture for local payments in high level. The architecture is explained in more details within the Technical documentation.

Picture 2: The Preferred Architecture for Local Payments



4.3 The Missing Pieces in the Local Payments Architecture

In all ideal solutions there will be technical details to be finalised – but these “blanks” are there to be discussed and finalised. After this chapter it should be clear what parts of the preferred architecture need future work within standardisation bodies, or with technology vendors.

There are problems with implementing EMV into mobile handsets – mainly certification requirements for handsets and the fact that EMV is not optimised for use with mobile handsets and networks. It is the Mobey Forum's viewpoint that work should be started immediately to solve these issues.

4.3.1 Issues to be solved with an EMV-based solution for Local Payments

There is a clear requirement from the financial industry to use EMV for Local Payments. The EMV protocol has to be optimised for mobile use. Specification of such a new protocol needs to be prepared by a cross-industry initiative, driven by payment associations, where all relevant parties participate. It is the task of payment associations to drive this work, however the Mobey Forum would like to speed up the process.

Issues related to EMV certification of mobile phones have to be solved by the relevant parties, such as MeT and other bodies involved in payment schemes. Handsets need to be certified for relevant parts of EMV in a reasonable timeframe to acceptable costs, preferably with self-certification. The self-certification rules for mobile phone manufacturers have to be created and accepted by the relevant players.

The local payment standard, once specified, then needs to be rolled out globally and implemented on mobile phones to enable local payments.

In addition, a local payment protocol needs to be specified. This is to be used, e.g. over Bluetooth, but should be transparent to the transport layer, thus allowing its use over other connection methods such as infrared.

5 Conclusions

The Mobey Forum recommends a wide-ranging, multi-market and long-term technical solution that fulfils all the stated business criteria. This consists of remote and local architecture solutions, including a modular option approach.

For remote payments, server wallet architecture with a convenient and secure customer authentication method is the recommended scenario, although for micro-payments, server- and local purse solutions are expected to co-exist. The Mobey architecture supports both and aims to make them interoperable. For customer authentication the preferred solution is a dual chip phone with a WIM-based digital signature capability.

In terms of local payments the fast global adoption of a standard, optimised for the mobile environment within a dual-chip architecture and WIM-capable multi-application card, is the option that best fulfils the business requirements identified. A mobile-optimised EMV-based local payment standard needs to be rolled out globally and implemented on mobile phones to enable local payments. Other authentication methods will also be used and are included in the preferred architecture to cater for smaller transactions with moderate security needs.

6 Next Steps

The Mobey Forum recommends the following steps, in order of importance, for moving forward.

- Discuss the recommended payment architecture with as many parties involved in the mobile payments industry and obtain buy-in from key industry groups (particularly network operators, payment associations and associated fora/forums).
- Consider how to solve the problem of:
 - Integrating mobile payments into existing merchants' infrastructure
 - Assess merchants' requirements concerning the infrastructure and network
 - Positioning with regards to other payment methods
 - Cost incentives
 - Process changes
 - Confirmation/reconciliation
 - Market opportunities.
- Address the technical issues under section 4.3 — the “blanks” to be filled in by the relevant technical bodies.
- Assess ‘trust’ infrastructure issues, inter-bank interoperability and usage. Global Inter-operability of certificates and CA systems needs to be guaranteed in order that customers may use the services from different banks and maintain its general usage.

ABBREVIATIONS USED IN THE MOBEY DOCUMENTATION

3D Secure	A security protocol defined by Visa International.
3D SET	A security protocol defined by Visa International.
3G	3rd generation cellular standard.
ARQC	Authorization Request Cryptogram.
ATM	Automated Teller Machine, a bank-operated machine where consumers can withdraw cash with their bank-issued payment cards.
Bluetooth	A local cellular technology capable of connecting various devices to each other's.
CA	Certificate Authority, a party issuing certificates.
DC	Dual chip (see definitions).
DES	Data Encryption Standard.
DS	Dual slot (see definitions).
EBPP	Electronic Bill Payment and Presentment.
EFI	External Functionality Interface / WAP Forum.
EMV	A payment standard defined by Europay, Mastercard and Visa International.
GSM	Global System for Mobile Communications, a (2 nd generation) mobile network standard.
HW	Hardware.
IC	Integrated Circuit.
ICC	Integrated Circuit Card.
IrDA	An Infrared standard.
MB	Megabytes, amount of memory.
MeT	Mobile Electronic Transactions, a Forum of handset manufacturers.
MMCA	MultiMediaCard Association.
MSISDN	Mobile Subscriber Identification Service xxx Number.
OTA	Over the air.
PIN	Personal Identification Number.
PKI	Public Key Infrastructure.
POS	Point of sales (terminal).
PTD	Personal Trusted Device (see definitions).
R&T	(here) Mobey Forum Requirements & Technology workgroup.
SAT	SIM Application Toolkit (GSM 11.14).
SBW	Server Based Wallet.
SC	Smart Card, equal to chip card (see definitions).
SE	Security Element (see 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.
SPA	A security protocol defined by Mastercard.
SSL	Secure Socket Layer, a generic transport layer security protocol.
SW	Software.
UCAF	Universal Cardholder Authentication Code (SPA specifications / Mastercard).
URL	Universal Resource Location, a www address.
WAP	Wireless Application Protocol.
WIM	Wireless Identification Module / WAP Forum.
WTLS	Wireless Transport Layer Security (protocol) / WAP Forum.

DEFINITIONS USED IN THE MOBEY DOCUMENTATION

Acquirer	Acquiring bank, a bank with merchant relationship and responsible for capturing the transaction.
Attended (shopping)	Merchant service is attended when there is a person acting as sales clerk; this might be in the form of phone sales or face-to-face shopping.
Business requirements	(Here) General requirements from the point of view of all institutions with an interest in mobile payments and the facilitation thereof.
Cardholder	End user with a bank issued card-based payment method.
Chip based e-purse	An e-purse application residing on a chip card; usually a stored value solution.
Dual chip	A mobile phone with an additional SIM-size slot for an independent multi-application chip card, targeted for payments and other banking applications.
Dual slot	A mobile phone with an additional slot for inserting a full-sized chip card, e.g., for payments. Can in principle be independent or dependent (i.e., SAT DS) on the SIM card.
E-purse	An application handling tokens representing electronic money; usually prepaid.
External reader	A chip card reader for full-sized smart cards connected to mobile phones, e.g., by Bluetooth.
Face-to-face	The transaction happens between a customer and a sales clerk and they are physically in the same location when the transaction happens.
Issuer	Issuing bank, the bank having business relationship to the Cardholder
Local Payments	Customer is physically in the same environment with the merchant. Transaction can be conducted over a local protocol like Bluetooth or over a remote protocol (mobile internet).
Macro Payment	A transaction (here) above 100 euros.
Merchant	The party selling goods or services to the customer
Micro Payment	A transaction (here) below 10 euros.
Mini Payment	A transaction (here) between 10 and 100 euros.
MultiMediaCard	A memory card used (today) mainly for data storage in the high-end mobile phones.
Non-attended (Shopping)	Shopping is non-attended when customer deals with an automated merchant service, i.e. there is no sales clerk present. This may be Local (e.g., vending) or Remote (e.g., web purchases) Shopping.
Non-repudiation	The transaction cannot be denied afterwards.
Payer's subsystem	Customer's mobile payment solution, consisting usually of a handset and a Security Element, both capable for mobile payments.
Payee's subsystem	Mobile Payment Architecture consisting of Issuer and Acquirer banks' and Merchants' solutions.
Personal Trusted Device	A personal mobile phone with a Security Element and capable of performing legally binding transactions.
Remote Payments	The customer and the merchant are conducting the transaction over an open network, here mobile Internet.
Secure MultiMediaCard	A MultiMediaCard with an ICC-like design conforming to the MMCA standards
Security Element (SE)	(Here) a bank-issued token, usually with smart card form factor, that usually contains bank-issued security credentials like private keys and bank-issued payment applications.
Server Based e-purse	Customer's separate prepaid account on a (bank-operated) Wallet Server used usually for conducting micro transactions.

Server Based Wallet	Customer's payment methods like credit card numbers or a server-based e-purse is stored on a Wallet Server operated by e.g. a bank.
White card	An additional chip card in the mobile phone issued by a trusted third party like government authority.

REFERENCES

The following reference documents have been used in the production of these documents:

Title	Owner / location if publicly available
White Paper version 1.0	Mobey Forum / http://www.mobeyforum.org/
Payment Models Version 0.1	Mobey Forum
Payment Uses Cases Version 2.0	Mobey Forum
Generic Use Cases Version 1.0	Mobey Forum
[MeTCORE] MeT Core Specification	MeT / http://www.mobiletransaction.org/
[MeTPTD] MeT Personal Trusted Device Definition	MeT / http://www.mobiletransaction.org/
[MeTPTDSec] "MeT PTD Security Requirements" V0.	MeT / 1 http://www.mobiletransaction.org/
[MeTCUE] "MeT Consistent User Experience" V0.1	MeT / http://www.mobiletransaction.org/
[WPKI] "Wireless Public Key Infrastructure Specification",	WAP Forum / http://www.wapforum.org/