MeT White Paper on Secure Services Architecture for Mobile Commerce

Approved 22-09-2003

Mobile electronic Transactions Ltd

MeT-WPSSAforMC-v1_0-20030922

Disclaimer:

This document is subject to change without notice.

www.mobiletransaction.org

Contents

1. Scope

This document constitutes a white paper on a secure services architecture for mobile commerce. The white paper should be read together with MeT Wallet Concept Description Version 1.0.

2. Document status

The current version of this document is approved.

2.1 Version History

Version	Date	Task Force or Working Group	Description
1.0	22-09-2003	MeT BoD	First public release

2.2 Errata

3. References

MeT Ltd specifications http://www.mobiletransaction.org.

MeT Wallet Concept Description Version 1.0 http://www.mobiletransaction.org.

4. Introduction

MeT Ltd. is the industry Mobile Commerce forum open to Mobile Terminal Manufacturers; Ericsson, NEC, Nokia, Panasonic and Siemens are current members. MeT are pleased to announce their new architecture for secure mobile commerce services enabled by the mobile terminal.

Realising that terminal manufactures are best placed to provide secure services for mobile commerce within the terminal, MeT has been working to define an open platform for mobile commerce centred on the User's need to:

- **Purchase goods and services** either from the mobile internet or from a local point of sale such as a petrol pump, drive-thru service point or parking meter
- **Store private and valuable information** such as passwords, PINs, e-money and electronic payment credentials in a 'Terminal Wallet'.
- **Prove their identity** to banks and mobile service providers
- **Seamlessly buy new content from within terminal applications** such a music player or game

5. Our belief

MeT members understand that for mobile commerce to succeed, mobile terminals need to enable and liberate all viable business models including those yet to be designed. Critically, our Users must be able to expect compatibility and interoperability from any terminal they choose to buy.

MeT has devised an Open platform and architecture enabling third parties and Mobile Network Operators to develop and deploy secure applications and services, extending those already supplied by the manufacturer.

6. Benefiting all

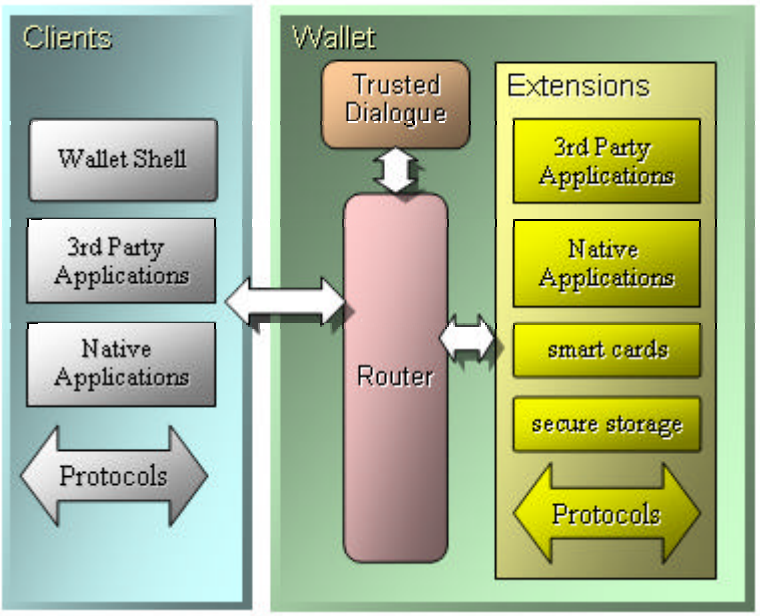
The benefits from leading terminal vendors working together with a shared vision reach far beyond the terminal User. A secure and flexible architecture, implemented in volume provides a strong platform for mobile commerce growth and success:

- **Merchants and Service Providers** can deploy secure 'shopping' applications to the terminal with controlled access to the resident terminal wallet if authorised by the User. The presence of up-to-date loyalty points in the wallet will encourage Users to spend. Ticketing operators will at last have an interoperable specification with which to sell, deliver and redeem tickets.
- **Financial Institutions** can authenticate their customers knowing that their communication is secure and that their terminal wallet will help Users identify when dangerous software is impersonating the bank illegally.
- **3rd Party Developers** can deploy mobile commerce applications and services written for common industry environments to terminals 'owning space' in the customer's wallet.
- **Mobile Network Operators** can extend their service portfolio onto the phone supporting their branding and customer experience programmes. Terminal wallets can redirect local Point of Sale transactions when the Merchant is acquired by an inter-operator payment scheme - in or out of coverage.
- **Terminal Manufacturers** can benefit froma shared-effort approach reducing research and development costs and avoiding market fragmentation risks. Enabling Users to confidently and safely purchase content and services via their mobile terminal can only increase demand for terminals able to consume increasing rich and complex content.

7. The Reference Architecture

The MeT secure services architecture is inspired by the concepts of the smart card and the firewall. Access to services and data is controlled by an access control 'Router'. Only Clients and Extensions authenticated and authorised may

access secure data. Only the Terminal Manufacturer can implement the Router and Native components ensuring security and providing access to lower level calls within the system.



7.1 Logical Components

The **Router** controls access between Clients, services and secure storage. Extensions register their presence (including name and corporate logo), capability, accessibility profile and secure data inventory with the router. Extensions do not publish secure data but references to that data so they can be accessed by authorised applications and the User. Extensions can publish links that call the Extension which are really adverts for the secure service.

Extensions provide secure services and access to secure data. They may also do management tasks such as backup and restore. Some will be provided by the terminal manufacturer and some can be downloaded at any time by 3rd parties. MeT hopes that 3rd parties will create enabling Extensions with published interfaces that can be used be even more mobile commerce Client applications. Examples of Extensions include:

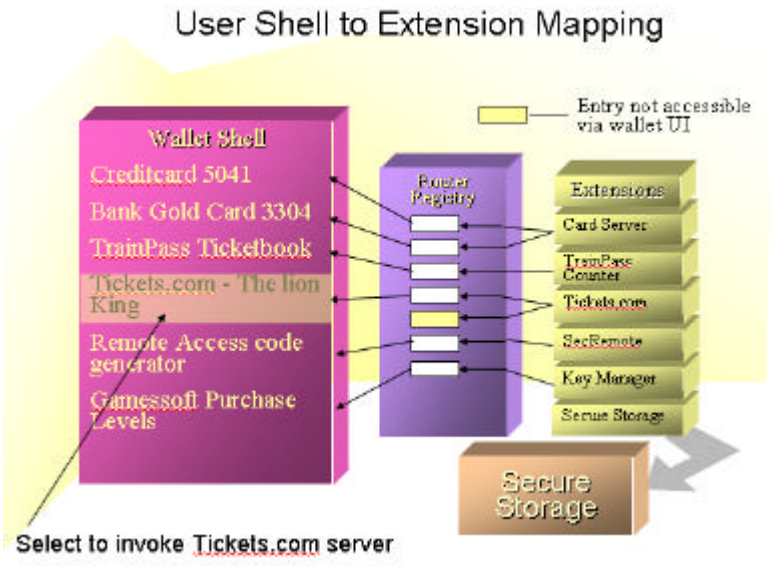
- Encryption Extensions
- Issuer developed virtual payment card Extensions
- Abstract payment card managers
- Logging and receipt management Extensions
- Generic secure data store
- Smart card interface Extension
- External secure memory storage Extensions
- Generic Ticketing Extension

Clients are applications or protocols that can interface secure services and data through the router. Examples would include browsers, shopping applications and games.

The **Trusted Dialog** is a User interface resource securely implemented by the Terminal Manufacturer. This allows the wallet to visually 'authenticate' itself to the User to prevent secure data being entered into rogue applications. Authorised Extensions and the Router can use this trusted dialog resource.

The **Wallet Shell** is the main user interface to the wallet. While this will normally be supplied by the Terminal Manufacturer, 3rd parties can replace or re-brand this shell. The shell reads the Extension registration information in the router and presents this to the User as a Terminal Wallet.

Secure Storage is implemented through Extensions. Software secure storage will be available in the Terminal. Secure storage in the form of secure memory cards is likely to become popular and will be supported, as will Smart Cards.



8. An invitation

MeT is pleased to invite all Mobile Terminal Manufacturers to join our programme to produce open specifications and deliver concrete proof-of-concept implementations around the world.

MeT is liaising with other industry organisations to ensure it is harmonised with the different stakeholders in the vast mobile commerce landscape. It is also working with standards and specification bodies to ensure that its platform and interfaces are as open and accepted as possible. MeT is software environment and bearer agnostic at the architectural level.