S3-000448

MExE

Mobile Execution Environment

mcatald1@email.mot.com
+44 (0)777 5582288

Agenda

- MExE timetable
- 2G and 3G Services
- MExE overview
- MExE functionality
- MExE domains and security
- MExE Release 2000
- MExE conformance

MExE Timetable

MExE

- MExE (Release 98)
  - WAP and PersonalJava classmarks
  - approved 2Q99
- MExE (Release 99)
  - SIM security enhancements
  - Quality of Service management
  - approved 4Q99
- MExE (Release 2000)
  - Java CLDC/MIDP classmark
  - other updates/additions
  - approval expected 4Q2000

Agenda

- MExE timetable
- 2G and 3G Services
- MExE overview
- MExE functionality
- MExE domains and security
- MExE Release 2000
- MExE conformance

2G mobile services

MExE

- core network supplementary services (e.g. call forwarding, call barring, call diversion etc.)
- all operators with same bland standardised services
- little scope for operators to differentiate
- tariffs are principle differentiators
- *one size fits all !!*

3G mobile multimedia services

MExE

- mobile phones fully internet integrated
- internet and multimedia services, *on the move*
- operator and third party multimedia services
- generally no services standardised, but enabled using services toolkits (e.g. MExE, CAMEL, USAT, OSA etc.)
- new multimedia services rapidly developed to differentiate from competitors, reduce “churn”
- *“mass market of one”*

Agenda

- MExE timetable
- 2G and 3G Services
- MExE overview
- MExE functionality
- MExE domains and security
- MExE Release 2000
- MExE conformance

MExE Overview

MExE

- standardised execution environments in a mobile phone
  - WAP
  - Personal Java
  - Java CLDC/MIDP (Release 2000)
- standardised negotiation of capabilities with servers
  - i.e. screen size, memory, bearers etc.
- independently developed multimedia services
  - write once, execute on many devices
- transfer of multimedia services
  - uploading/downloading, network and 3rd party services, MExE-to-MExE services

Agenda

- MExE timetable
- 2G and 3G Services
- MExE overview
- MExE functionality
- MExE domains and security
- MExE Release 2000
- MExE conformance

MExE functionality (1)

MExE

- standardised set of MExE classmarks
  - WAP, WAP/PersonalJava
- multimedia services supported by all devices of a given classmark (CM)
  - CM1 devices support CM1 applications, CM2 devices support CM2 applications etc.
- wide variety of multimedia services
  - with no standardised 3G services, MExE enables multimedia service delivery to users
- a more sophisticated user interface
  - advanced services presentation
  - Graphical User Interface (GUI)

MExE functionality (2)

MExE

- customisation and personalisation
  - services “look and feel”
  - user interface and services personalisation
  - services communication with network/non-network nodes
  - operator branding and differentiation
- user services management
  - services download
  - services/data management
  - determine active services

MExE functionality (3)

MExE

- re-use of existing technologies
  - software industry expertise, development tools
  - WAP, Internet and Intranet
  - existing APIs, (i.e. WAP, PersonalJava, Java MIDP/CLDC...)
- capability negotiation
  - allows servers and MExE mobile phones to determine the most suitable content format for the device (e.g. depending on screen size, memory, colour capabilities etc.)

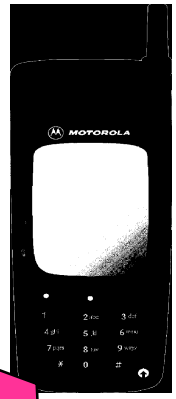
Agenda

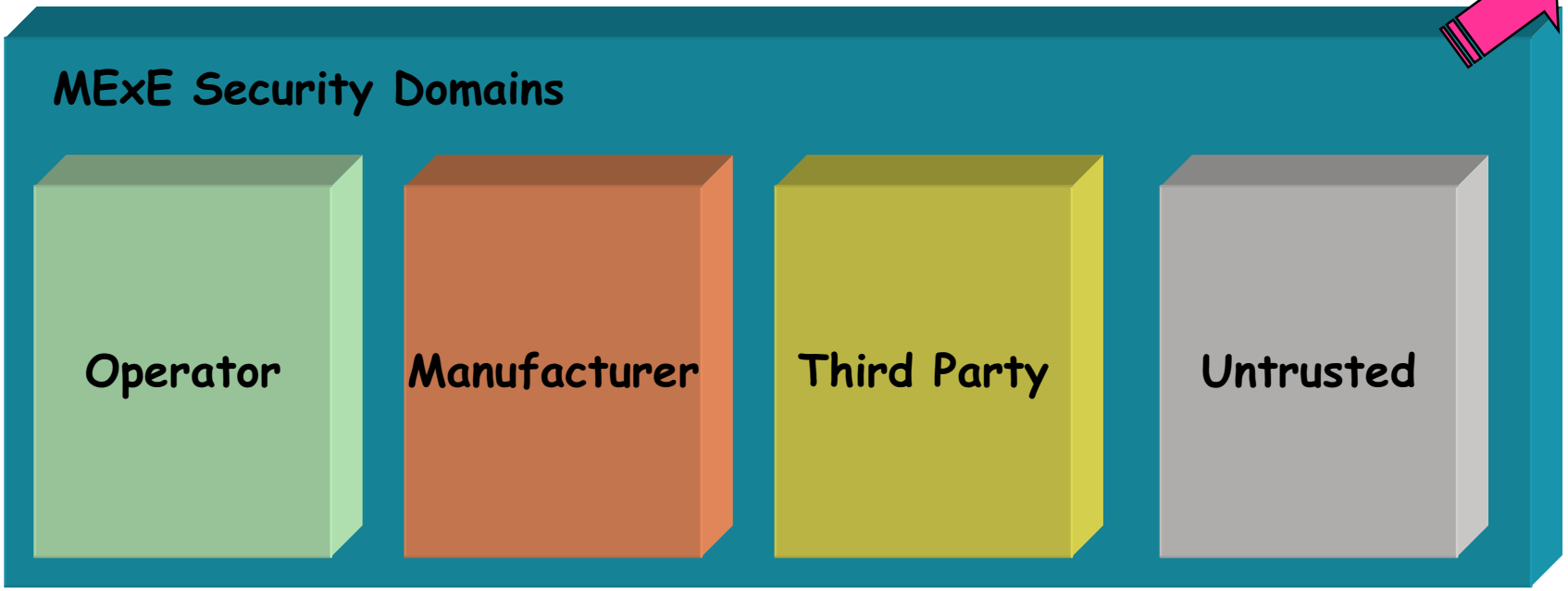
- MExE timetable
- 2G and 3G Services
- MExE overview
- MExE functionality
- MExE domains and security
- MExE Release 2000
- MExE conformance

MExE Security Domains (WAP and PJava classmarks)

MExE

- secure environment for multimedia services
- 3 security domains (using PKI certificates)
- 1 untrusted sandbox





Operator's Domain (WAP and PJava classmarks)

MExE

- only operator PKI authenticated multimedia services permitted
- operators provide existing services and new multimedia services
  - branded services
  - franchised services
  - customer support
  - service personalisation
- defined set of mandatory security restrictions on downloaded applications

Handset Manufacturer's Domain (WAP and PJava classmarks)

MExE

- only manufacturer's PKI authenticated multimedia services permitted
- permits mobile phone upgrades
  - "provisioned applications" upgrade
- user interface upgrades
- software updates
- manufacturer's multimedia services
- defined set of mandatory security restrictions on downloaded applications

Third Party Domain (WAP and PJava classmarks)

MExE

- "Administrator" determines whether Third Party domain is controlled by the operator or user
  - Operator controlled: operator decides which (if any) PKI authenticated third party services
  - User controlled: user decides which PKI authenticated third party services
- defined set of mandatory security restrictions on downloaded applications

Untrusted Sandbox (WAP and PJava classmarks)

MExE

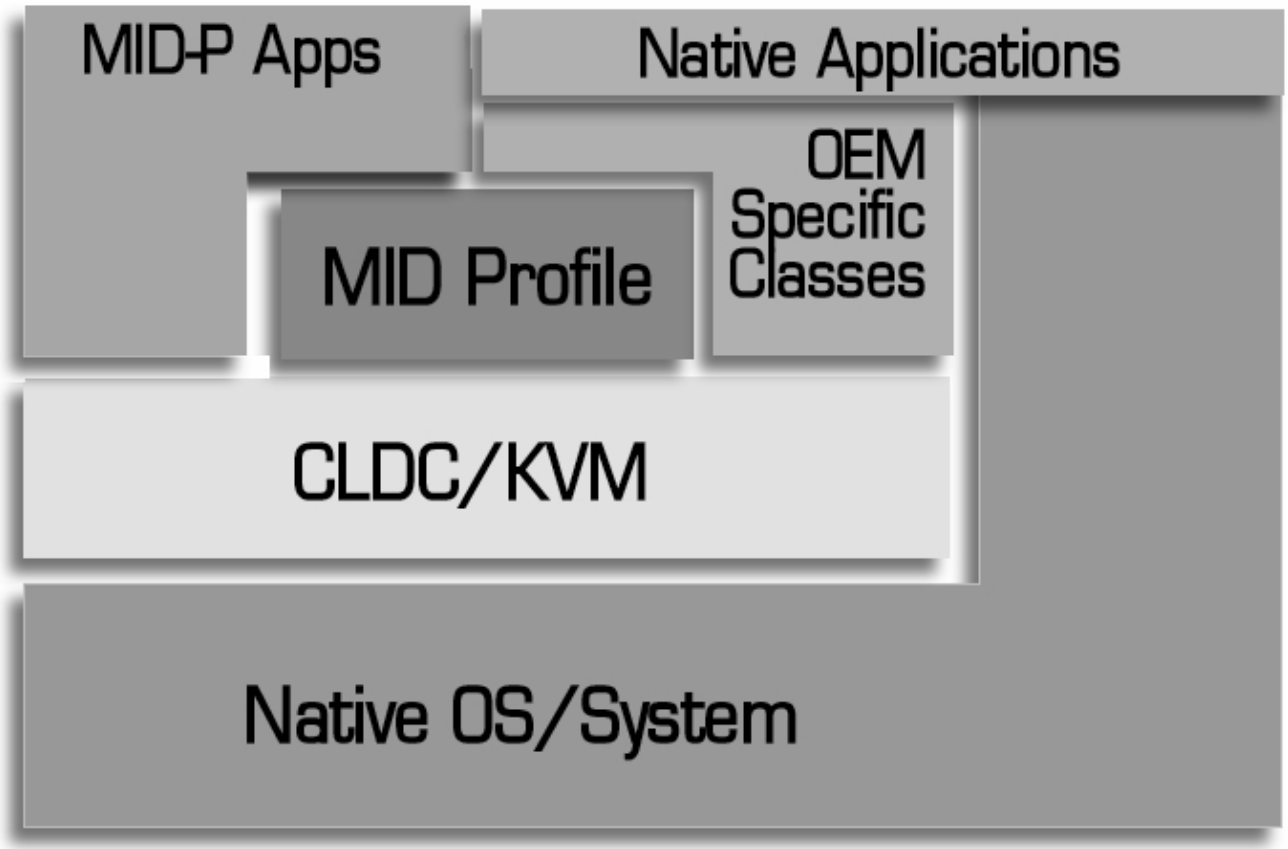
- user in control of the untrusted domain
- user downloads any multimedia service as desired
- downloaded multimedia services have limited permissions (only with explicit user authorisation)
  - call origination
  - screen access
  - sending DTMF
  - add phonebook entry
- defined set of mandatory security restrictions on downloaded applications

Agenda

- MExE timetable
- 2G and 3G Services
- MExE overview
- MExE functionality
- MExE domains and security
- MExE Release 2000
- MExE conformance

New CLDC/MIDP classmark (1)

Architecture of a Classmark 3 Device



Mobile Information Device Profile

- Designed to operate on top of CLDC
- MIDP applications (MIDlets) makes use of APIs supported by CLDC and MIDP specifications
- Supports third party applications for mobile information devices
- Supports a subset of HTTP over TCP/IP, WAP
- Requires a minimum set of device capabilities in
  - Display characteristics
  - Input characteristics
  - Memory
  - Networking

New CLDC/MIDP classmark (3)

MExE

- CLDC/MIDP only permits a “sandbox” security model
- user downloads any service/content as desired
- downloaded multimedia services have limited permissions
- design of MIDP does not allow any sensitive APIs to be exposed to applications (i.e. contained)
  - applications can only execute in their own space
  - applications cannot access device data or resources
  - access to input/output
- tighter MExE security restrictions than CM1/CM2

New CLDC/MIDP classmark (4)

MExE

CLDC Security - addressed in two different levels

- **Low level security based on a classfile verifier (VM level)**
  - Ensures that a downloaded classfile does not execute in a way that is not permitted by the Virtual Machine
- **Application level security based on a Sandbox**
  - Ensures that only Java APIs defined by the CLDC, profiles and licensee open classes (OEM) are available to downloaded applications
  - The downloaded applications cannot delete or modify the system classes
  - The set of native functions accessible to the virtual machine is closed

All applications are untrusted as Classmark 3 devices does not support digital certificates

New CLDC/MIDP classmark (5)

MIDP Security - applicable to Java MIDlets

- All Java MIDlets will be treated as untrusted
- Will only have access to functions that are exposed as Java APIs
- Not all Original Equipment Manufacturer (OEM) classes will be exposed to Java MIDlets (need to make sure that OEM classes do not allow executables to bypass security restrictions)
- Java MIDlets will not have access to native functions

Other Release 2000 items (1)

MExE

- enhanced security
  - clarifications and corrections (if necessary)
- support of terminal parts of the VHE / User Profile
  - work with S1, S2 and CN5 to support VHE
- investigate and identify support for IP multimedia services
  - identify any additional support required for multimedia services (possibly none)
  - MExE intrinsically supports downloadable multimedia applications

Other Release 2000 items (2)

MExE

- investigate and identify secure download mechanisms and capabilities to support SDR concepts
  - co-operation with SDR Forum, which is re-using MExE technology
- investigate and identify support of AT commands
  - carried forward from Release 99: intended to securely enable selected AT command support to applications
- investigate and identify support of MP3/MPEG4 content
  - largely already supported by MExE; MExE intrinsically supports downloadable music/video applications

Other Release 2000 items (3)

MExE

- investigate and identify support of SIM toolkit / OSA / CAMEL interaction to provided advanced services
  - Work with S1, S3, T2, T3, and CN5 to support interworking between the toolkits

Agenda

- MExE timetable
- 2G and 3G Services
- MExE overview
- MExE functionality
- MExE domains and security
- MExE Release 2000
- MExE conformance

MExE Generic Conformance

MExE

Generic MExE conformance requirements	CM1	CM2	CM3
Support of WAP Forum's UAProf capability negotiation ▪ MExE-specific parameters ▪ direct and indirect referencing mechanisms to support the user profile	M	M	M
Support of HTTP/1.1or later version	O	O	O
Support of the user profile (*Note: not yet defined by 3GPP!*) ▪ services personalisation ▪ user interface personalisation preferences	M	M	M
Support of service management to:- (*CM3 applications are subject to MIDP restrictions*) ▪ discover applications ▪ control download, installation, configure and delete applications ▪ control execution (fine grain), suspend terminate applications	M	M	M
User control of downloaded applications' active connections ▪ terminate connections ▪ suspend connections ▪ obtain information on application connections	M	M	M
Support of journalling of network events ▪ activate/deactivate the journalling in a secure manner ▪ determine journalling status	M	M	M

MExE Security Conformance (1/3)

MExE

MExE security conformance requirements (1/3)	CM1	CM2	CM3
3 security domains (operator, manufacturer, trusted third party) (Note status for CM1 and CM2 may be changed in Release 2000)	M	M	O
Support of security restrictions when specific functionality is called by MExE executables (Note status for CM1 and CM2 may be changed in Release 2000) ▪ Support for permissions of operator, manufacturer and third party security domains ▪ Access to the user input/output by untrusted uninstalled MExE executables ▪ Separation of the user input and output between different MExE executables ▪ Access to files in the MExE executable's own area by untrusted MExE executables (MIDP provides a mechanism for MIDlets to persistently store and retrieve data, and share it between MIDlets in a suite) ▪ Conditional ability of untrusted MExE executables to initiate a connection, generate DTMF tones, add phonebook entries ▪ Prohibition for untrusted MExE executables to access any other functions ▪ Visual indication to user whenever user permission is sought by untrusted MExE application ▪ Ability of the user to request to see the "subject" field of the certificate of the signer ▪ Prompt for user permission related to all specified action groups by MExE executable	M	M	M
Support of permissions ▪ Blanket permission and single action permission (mandatory) ▪ Session permission (optional)	M/O	M/O	M/O

MExE Security Conformance (2/3)

MExE

MExE security conformance requirements (2/3)	CM1	CM2	CM3
Support for public key based solution (PKI) for content authentication (Note status for CM1 and CM2 may be changed in Release 2000) ▪ Support of certificate chains ▪ Support at least one level of certificate under operator, manufacturer or Third Party root public keys ▪ Secure installation of root public keys ▪ Prohibition to share public keys between domains ▪ Support the use and management of an operator root public key on the SIM ▪ Prohibition to the user to add or delete any type of operator public keys ▪ Support of the use and management of the operator, manufacturer, third party and administrator root public keys ▪ Support of the administrator designation mechanism ▪ Support of the certificate configuration management ▪ Use of the CCM by MExE device to determine the third party certificates that are trusted for the use on the MExE MS ▪ Support of authorised CCM download mechanisms ▪ Change of the CCM with the change of administrator ▪ Support of provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device ▪ Support for determining the administrator ▪ Use of a sandbox system to implement each MExE domain ▪ Verification of the certification of the application or applet ▪ Support of the JAR file format for securely downloading packaged objects ▪ Support for the case when a certificate containing an Administrator root public key is contained in a signed package ▪ Support for administrator root certificate mechanism	M	M	O

MExE Security Conformance (3/3)

MExE

MExE security conformance requirements (3/3)	CM1	CM2	CM3
Support for public key based solution (PKI) for content authentication (Note status for CM1 and CM2 may be changed in Release 2000) ▪ Installation of a disaster recovery root public keys ▪ User's ability to add/delete/mark trusted/mark untrusted/modify fine grain access permission for a given certificate ▪ Additional support of other means to enable/disable root certificates ▪ Support for trusted applets ▪ Java loading native libraries that are intrinsically part of the ME implementation, and MExE native libraries ▪ Support for other proprietary means of downloading and installing objects ▪ Support of MExE native library signed package installation ▪ Support of installation of other signed data ▪ Support of alternative methods to download an administrator root certificate ▪ Support of pre-verification of applications	N/A	O	O

MExE Classmark 1 Conformance

MExE

MExE WAP (CM1) conformance requirements	CM1	CM2	CM3
WAP version 1.1 or higher	M	M	?
Display an indicator whenever network activity is in progress	O	O	O
Capability to upgrade, replace preinstalled/preloaded WAP browser	O	M	?
Pre-installed or pre-loaded WAP browser Rendering tokenised WML documents ("WML decks") WMLscript bytecode Other WML formats (e.g. textual WML documents, textual WMLscripts) optional (Note: effectively means full support of WAE!)	M	M	?
Support of QoS API by MExE MS ▪ Support of a basic QoS operations ▪ Support of MExE QoS API by MExE QoS Manager ▪ Access to MExE QoS Manager through MMI ▪ QoS control by MExE QoS Manager, if QoS not provided in the network ▪ Support of a standard set of parameters by a QoS API ▪ MExE QoS Manager to deal independently with simultaneous QoS streams	M	M	M

MExE Classmark 2 Conformance

MExE

MExE PersonalJava (CM2) conformance requirements	CM1	CM2	CM3
PersonalJava MExE API	N/A	M	N/A
PersonalJava 1.1 or higher JavaPhone API specification Wireless Profile JAR file manifest entries: Implementation-Title, Main-Class, Class-Path event generation (“BatteryCritical”, “BatteryNormal” is mandatory minimum support)	N/A	M	N/A
PersonalJava network protocols:- ▪ HTTP/1.1 (mandatory) ▪ HTTPS (mandatory) ▪ Gopher (optional) ▪ ftp (optional) ▪ mailto (mandatory) ▪ file (optional)	N/A	M/O	N/A
Other Java APIs which comply with the MExE security requirements	N/A	O	O

MExE Classmark 3 Conformance

MExE

MExE CLDC/MIDP (CM3) conformance requirements	CM1	CM2	CM3
Support of the J2ME Connected Limited Device Configuration (CLDC) with the Mobile Information Device Profile (MIDP).	N/A	N/A	M
Support of network connectivity:- ▪ MIDP connectivity support with the HttpConnection API to set request header, parse response headers and perform HTTP specific functions. ▪ CLDC datagram support by use of DatagramConnection interface	N/A	N/A	M