ETSI TS 123 057 V14.0.0 (2017-05)

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
Mobile Execution Environment (MExE);
Functional description;
Stage 2
(3GPP TS 23.057 version 14.0.0 Release 14)**

3GPP A GLOBAL INITIATIVE
GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Reference
RTS/TSGS-0223057ve00

Keywords
GSM,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2017.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
oneM2M logo is protected for the benefit of its Members
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights 2
Foreword 2
Modal verbs terminology 2
Foreword 7
1 Scope 8
2 References 8
3 Definitions and abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 12
4 MExE basic principles 14
4.1 Generic MExE aspects 14
4.2 High level architecture 14
4.3 Multiple classmark support 15
4.3.1 Classmark 1 service support in non-Classmark 1 MExE devices 15
4.3.2 Classmark 2 service support in non-Classmark 2 MExE devices 16
4.3.3 Classmark 3 service support in non-Classmark 3 MExE devices 16
4.3.4 Classmark 4 service support in non-Classmark 4 MExE devices 16
5 Generic MExE functions (excluding security) 16
5.1 User profile 16
5.1.1 Location of, access to, and security of, the user profile 16
5.1.2 Support of the user profile 17
5.1.3 User interface personalisation 18
5.1.3.1 MExE user interface personalisation 18
5.1.3.2 Support of MExE user interface personalisation 18
5.1.4 Virtual home environment 19
5.2 Capability and content negotiation 19
5.2.1 User profile and capability negotiation relationship 20
5.2.2 Capability negotiation characteristics 20
5.2.3 Client content capability report 22
5.2.4 Server role in capability negotiation 22
5.2.5 Client-driven negotiation 22
5.3 Provisioning and management of services 22
5.3.1 Service discovery 22
5.3.2 Service transfer 23
5.3.3 Service installation and configuration 23
5.3.4 Service management 23
5.3.5 Service termination 23
5.3.6 Service deletion 23
5.4 User control of application connections 24
5.4.1 Journaling of network events 24
5.4.2 User notification 24
5.5 Quality of service 24
5.5.1 Introduction 26
5.5.2 MExE QoS support 26
5.5.3 MExE QoS manager 27
5.5.4 Network control API 27
5.5.5 MExE QoS API 27
5.5.6 Sources of bearer service parameters 28
5.5.7 QoS streams 28
5.5.8 QoS security 28
5.6 Charging 28
5.6.1 Generic charging support 29

6 Generic MExE Security 29
6.1 Introduction 29
6.2 MExE executable integrity 29
6.2.1 Full signature verification 30
6.2.2 Optimised pre-launch signature verification 30
6.3 MExE executable permissions 30
6.3.1 MExE executable permissions for operator, manufacturer and third party security domains 30
6.3.2 MExE executable permissions for untrusted MExE executables 34
6.4 Handling of MExE executables when their valid root public key is not available 35
6.4.1 Launching of MExE executables when their valid RPK is not available 36
6.4.2 Currently executing secure MExE executables when their valid RPK is no longer available 36
6.5 User permission types 36
6.6 Root Public keys 37
6.6.1 Operator root public key 37
6.6.1.1 Caching of root public keys 38
6.6.1.2 MExE device actions on detection of valid (U)SIM application and/or power up 38
6.6.2 Manufacturer root public key 40
6.6.3 Third party root public key 40
6.7 Certification and authorisation architecture 41
6.7.1 Certification requirements 41
6.7.1.1 MExE terminal requirements for certificate processing 41
6.7.2 Certification administration requirements 42
6.7.3 Example certification process 42
6.7.4 Certificate Chain Verification 43
6.8 Usage of Signed Content 45
6.8.1 Signed packages used for installation 45
6.8.2 Installation of root certificates in a signed data package 46
6.8.3 Installation of other signed data 46
6.9 Certificate Format 47
6.9.1 Certificate extension for removal of network access 47
6.9.1.1 X.509 version 3 47
6.10 Certificate management 47
6.10.1 Certificate configuration message (CCM) 48
6.10.1.1 CCM numbering convention 51
6.10.1.2 CCM order of transmission 51
6.10.1.3 CCM field mapping convention 51
6.10.1.4 Authorised CCM download mechanisms 51
6.11 Separation of I/O streams 51
6.12 Core software download 52
6.13 Administrator Concept 52
6.13.1 Administrator root public key 52
6.13.2 Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device 53
6.13.3 MExE administrator determination mechanism 53
6.13.3.1 Determining the administrator of the MExE device 53
6.13.3.2 Determining the administrator of the MExE device, for MExE-(U)SIM supporting third party certificates 54
6.13.3.2.1 Administrator of the MExE device is the user 54
6.13.3.2.2 Administrator of the MExE device is not the user 55
6.13.4 Administrator root certificate download mechanism 56

7 MExE Classmark 1 (WAP environment) 57
7.1 Introduction 57
7.1.1 WAP MExE devices 57
7.1.2 High level architecture 57
7.2 Non Security 57
7.2.1 WAP components 57
7.2.2 Services 58
7.2.2.1 User interface 58
7.2.2.2 Access points 58
7.2.2.3 Transferring 59
7.2.2.3.1 WSP and HTTP/1.1 Proxy Function 59

7.2.3 WAP charging support....60
7.2.4 CC/PP over WSP (Classmark 1)....60
7.3 Security....60
7.3.1 Call control....60
7.3.2 Local phonebook....60

8 MExE Classmark 2 (PersonalJava environment)....60
8.1 Introduction....60
8.1.1 Classmark 2 MExE devices....61
8.1.2 High level architecture....61
8.2 Non Security....61
8.2.1 High level functions....61
8.2.1.1 Optional Java packages....61
8.2.1.2 Required and optional PersonalJava APIs....62
8.2.1.3 Required and optional JavaPhone APIs....62
8.2.1.3.1 Application installation....63
8.2.1.3.2 Power....63
8.2.1.3.3 Datagram recipient addressing....63
8.2.1.4 Required and optional MExE PersonalJava APIs....63
8.2.1.5 Mandated services and applications....64
8.2.1.5.1 Network protocol support....64
8.2.2 CC/PP over HTTP (Classmark 2)....64
8.2.3 Java charging support....64
8.3 Security....64
8.3.1 PersonalJava security....64
8.3.1.1 Java applet certification in PersonalJava....64
8.3.1.2 Java application signature verification in PersonalJava....64
8.3.1.3 Java loading native libraries in PersonalJava....65
8.3.2 Installing MExE native libraries....65

9 MExE Classmark 3 (J2ME CLDC environment)....65
9.1 Introduction....65
9.1.1 Classmark 3 MExE devices....65
9.1.2 High level architecture....65
9.1.3 High level functionality....66
9.2 Non Security....66
9.2.1 Connected Limited Device Configuration (CLDC)....66
9.2.2 Mobile Information Device Profile (MIDP)....66
9.2.2.1 Networking....67
9.2.2.2 MID Applications (MIDlet)....67
9.2.2.3 MIDlet Suites....67
9.2.2.4 Record Storage....67
9.2.3 Required and optional MExE APIs....67
9.2.4 Service discovery and management....67
9.2.5 Transfer of capability negotiation information in Classmark 3....68
9.3 Security....68
9.3.1 CLDC security....68

10 MExE classmark 4 (CLI Compact environment)....68
10.1 Introduction....68
10.1.1 High level architecture....69
10.2 Non security....69
10.2.1 High level functionality....69
10.2.2 Network protocol support....70
10.2.3 Power Management....70
10.2.4 CLI charging support....70
10.2.5 CC/PP over HTTP or WSP (Classmark 4)....70
10.3 Security....71
10.3.1 CLI Security....71

Annex A (normative): MExE profile of PKCS#15....72

A.1 PKCS#15 certificate object attributes presentation....72

A.1.1 Object common attributes 72
A.1.2 Certificate common attributes 72
A.1.3 Certificate attributes 72
A.1.4 Specific X.509 certificate attributes 72
A.2 MExE profile of PKCS#15....72
A.3 Coding and storage in MExE-(U)SIM 73
Annex B (informative): PKCS#15 certificate objects ASN1 expanded syntax extract 74
Annex C (normative): Access restriction certificate extension 76
Annex D (informative): MExE executable life cycle....77
D.1 State of a MExE executable 77
D.2 Released state 79
D.3 Uninstalled Execution state 80
D.4 Verification....81
Annex E (informative): MExE conformance requirements 82
Annex F (informative): Change history 86
History 87

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the stage 2 and stage 3 description of the Mobile Execution Environment (MExE). Stage 2 identifies the functional capabilities and information flows needed to support the service described in stage 1.

The present document includes information applicable to network operators, service providers and terminal, switch and database manufacturers.

The present document contains the core functions for a Mobile Execution Environment (MExE) which are sufficient to provide a complete service.

MExE uses a number of technologies to realise the requirements of the stage 1 description (3GPP TS 22.057). The present document describes how the service requirements are realised with the selected technologies. The TS is devised into clauses each covering the aspects relating to particular MExE technologies, it is intended that this specification will evolve along with the MExE technologies. A generic clause of the specification covers areas of MExE common to all technologies.

Implementation of this specification outside the UE (User Equipment) is outside the scope of this specification.

2 References

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] Void.

[2] 3GPP TS 22.057: "Mobile Execution Environment (MExE); Stage 1".

[3] Personal Java 1.1.1 or higher: Sun Microsystems http://www.javasoft.com/products/personaljava/.

[4] JavaPhone API version 1.0: http://java.sun.com/products/javaphone/.

[5] Void.

[6] Wireless Application Protocol (WAP) June 2000 Conformance Release: http://www.wapforum.org.

[7] Void.

[8] Void.

[9] IETF RFC 2616:Hypertext Transfer Protocol – HTTP/1.1: http://www.w3.org/Protocols/rfc2616/rfc2616.

[10] Void.

[11] 3GPP TR 22.170: "Universal Mobile Telecommunications System (UMTS); Service aspects; Provision of Services in UMTS - The Virtual Home Environment".

[12] 3GPP TS 22.121: "The Virtual Home Environment; Stage 1".

[13] Void.

[14] 3GPP TS 22.101: "Service Aspects; Service Principles".

[15] CC/PP Exchange Protocol based on HTTP Extension Framework; W3C http://www.w3.org/Mobile/CCPP.