UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC
Petitioner

v.

HEADWATER RESEARCH LLC
Patent Owner

Case No. IPR2026-00442
Patent 11,985,155

DECLARATION OF FRIEDHELM RODERMUND

GOOGLE EXHIBIT 1024
Google v. Headwater
IPR2026-00442

TABLE OF CONTENTS

Page

I. INTRODUCTION 1
II. QUALIFICATIONS 2
III. SUMMARY OF MY OPINIONS 7
IV. PUBLICATIONS OF 3GPP SPECIFICATIONS AND RELATED DOCUMENTS 8
A. General Practices 8
B. 3GPP TS 23.057 V7.0.0 (EX1021) 20
1. Authentication 20
2. Publication by 3GPP and ETSI 20
3. Conclusion 35
C. 3GPP TS 31.101 V7.0.1 (EX1018) 35
1. Authentication 35
2. Publication by 3GPP and ETSI 35
3. Conclusion 49
D. 3GPP TS 31.102 V8.0.0 (EX1019) 49
1. Authentication 49
2. Publication by 3GPP and ETSI 49
3. Conclusion 62
E. 3GPP TS 51.011 V4.10.0 (EX1020) 62
1. Authentication 62
2. Publication by 3GPP and ETSI 62
3. Conclusion 74
V. CONCLUSION 75

LIST OF APPENDICES

Appendix A	CV of Friedhelm Rodermund
Appendix B	3GPP working groups, as of 2005
Appendix C	3GPP specifications by series
Appendix D	3GPP 23-series
Appendix E	3GPP specification archive TS 51.011
Appendix F	3GPP portal TS 51.011
Appendix G	3GPP homepage, as of 2005
Appendix H	3GPP specifications page, as of 2005
Appendix I	3GPP specifications numbering scheme page, as of 2005
Appendix J	3GPP specifications series page, as of 2005
Appendix K	3GPP specification detail TS 51.011, as of 2005
Appendix L	3GPP specification archive TS 51.011, as of 2004
Appendix M	ETSI TS 151 011 V4.10.0
Appendix N	3GPP specification detail TS 23.057, as of 2007
Appendix O	3GPP specification archive TS 31.101
Appendix P	3GPP specification archive TS 31.101, as of 2007
Appendix Q	ETSI TS 131 101 V7.0.1
Appendix R	3GPP 31-series specifications, as of 2007
Appendix S	3GPP specification detail TS 31.101, as of 2007
Appendix T	3GPP specification archive TS 31.102

Appendix U	3GPP specification archive TS 31.102, as of 2008
Appendix V	3GPP portal TS 31.102
Appendix W	3GPP specification detail TS 31.102, as of 2008
Appendix X	3GPP specification archive TS 23.057
Appendix Y	3GPP specification archive TS 23.057, as of 2007
Appendix Z	ETSI TS 123 057 V7.0.0
Appendix AA	3GPP 23-series specifications, as of 2007
Appendix AB	3GPP portal TS 31.101

I, Friedhelm Rodermund, declare as follows:

I. INTRODUCTION

1. I have been retained as an independent expert witness on behalf of Petitioner, Google LLC for this *inter partes* review proceeding.

2. I am being compensated for my work in this matter at my accustomed hourly rate of €500 per hour. I am also being reimbursed for reasonable and customary expenses associated with my work and testimony in this investigation. My compensation is not contingent on the results of my study, the substance of my opinions, or the outcome of this matter.

3. In the preparation of this declaration I have reviewed the documents cited herein, each of which is a type of material that experts in my field would reasonably rely upon when forming their opinions, as well as all of the appendices attached hereto.

4. In forming the opinions expressed within this expert report, I have considered:

- The appendices listed above; and
- My own academic background, knowledge, and professional experiences in the field of wireless communications.

5. Although I have attempted to organize the information presented in this declaration into helpful sections and/or divisions, my opinions are supported by the information in the report in its entirety.

II. QUALIFICATIONS

6. I have 30 years of experience working with standards development organizations including the 3rd Generation Partnership Project ("3GPP"), the European Telecommunications Standards Institute ("ETSI"), and the Open Mobile Alliance ("OMA"). I have particular experience with the development of standards related to cellular telecommunications, including the standards for the Universal Mobile Telecommunications System ("UMTS"), Long Term Evolution ("LTE"), and 5G, which are all standards developed by the 3GPP.

7. I attended the University of Technology Aachen in Aachen, Germany, where I performed graduate studies in Electrical Engineering with a focus on telecommunications technologies ("Dipl.-Ing. TH" degree). I also attended the University of Technology Trondheim in Trondheim, Norway, and completed my Diploma thesis, "Design of a dual processor computer for digital signal processing in power electronics," in 1993.

8. From December 1993 to June 1998, I worked at Mannesmann Mobilfunk as a System Engineer and Project Manager in Quality Assurance and Technical Standards. One of my responsibilities was to ensure by managing and

performing related test activities that cellular network equipment was compatible with the Global System for Mobile Communications ("GSM") standard developed by ETSI. During that time, I also started working as a standards delegate. I attended my first ETSI meeting in 1996 (although I was already following ETSI developments from 1992 during my studies).

9. From June 1998 to December 2004, I worked at ETSI as a project manager for various ETSI Special Mobile Group ("SMG") and 3GPP working groups. First, I served as a secretary of SMG4 "Data Services" and SMG8 "Base Station Testing." Then, as a project manager with the ETSI Mobile Competence Center ("MCC"), I supported establishing 3GPP as the new international standards development organization for cellular telecommunications. One of my roles was acting as Secretary for 3GPP's Technical Specifications Group Terminals, Working Group ("T2"), the group which played a leading role in the creation of standards for Multimedia such as the Multimedia Messaging Service ("MMS"). Furthermore, T2 was also responsible for the development of the Mobile Execution Environment (MExE) standard of which the stage 2 was defined in TS 23.057.

10. In 2003, in addition to my roles in 3GPP, I was a member of the GSMA MMS Task Force where I was supporting the creation of interoperability guidelines for the introduction of MMS in cellular networks and devices.

11. During my time at ETSI, I acted also as the secretary of the highest-level Technical Specifications Group Terminals (TSG-T) which was, besides other things, responsible for the development of test specifications including tests for the radio interface. TSG-T was also the highest-level plenary to which the Terminals Working Group ("T3") reported, and therefore TSG-T was responsible for approving the working results of T3. T3 was responsible for SIM[1]-related aspects including TS 31.101, TS 31.102, and TS 51.011. Thus, as the TSG-T secretary I was well aware of the work performed on SIM-related aspects such as the SIM-terminal interface and the USIM[2] application. Furthermore, I attended and supported T3 working group meetings on several occasions.

12. I edited all technical specifications produced by my working groups and presented results to the parent body for approval. I attended all meetings (apart from a few sub-working group meetings) and was also responsible for compiling meeting reports, for handling all the meeting documents, and managing the work plan. It was also my role to guide the groups and to advise the chairmen regarding 3GPP working methods and procedures including document handling, and to make sure delegates

[1] Subscriber Identity Module also known as "SIM-card"

[2] Universal Subscriber Identity Module

were aware of their company's obligations under the 3GPP Intellectual Property Rights policy.

13. As part of my responsibilities at ETSI, I acted as a 3GPP custodian of records by personally managing 3GPP's public File Transfer Protocol (FTP) folders, which I used to make publicly accessible various 3GPP documents, including versions of 3GPP specifications, technical reports, liaison statements, change requests, contributions, agendas, meeting reports, and other 3GPP documents from my working groups. I am also knowledgeable about document management practices used in other working groups and within 3GPP in general with regard to making documents publicly accessible through the same public FTP server of 3GPP.

14. Since I left ETSI as a staff member in 2005, I have been continuously involved in standardization activities, including with OMA, ETSI, and 3GPP.

15. After I left ETSI, I worked from January 2005 to October 2014 at Vodafone, first as a Project Manager for Mobile Broadcast Standards, and then as Vice Chairman of the Device Management working group of the OMA, and then as a Senior Standards Strategist, all with responsibilities as described on my curriculum vitae. At Vodafone, I was deeply involved in standards work with 3GPP, ETSI and OMA, including as a delegate to 3GPP SA1 "Services." As part of my responsibilities, I attended standardization meetings, submitted documents to working group meetings, used 3GPP, ETSI and OMA resources (including 3GPP's

document server) extensively, and remained knowledgeable about 3GPP policies and procedures with regard to document management and public accessibility. At Vodafone, I was also involved in the creation of patents, defense activities related to patent litigations, and patent evaluation, mostly in the context of standards development.

16. Since leaving Vodafone in 2014, I have performed consulting work regarding Internet of Things (IoT) and Machine to Machine (M2M) technologies and standards, first at Friedhelm Rodermund Consulting and then as the Founder and Director of IOTECC GmbH. In connection with my work, I regularly deal with standards such as OMA's Lightweight M2M (LwM2M) and 3GPP's LTE, Narrowband IoT (NB-IoT) and 5G standards. And I have extensively used 3GPP resources and have remained knowledgeable about 3GPP policies and procedures with regard to document management and public accessibility.

17. I also provide consulting services related to patents, in particular around 3GPP Standard Essential Patents ("SEPs"), and I have worked as an expert witness on a number of occasions. Furthermore, I closely follow the maintenance of the ETSI IPR Policy as a delegate to the ETSI Intellectual Property Rights ("IPR") Special Committee. Furthermore, I am a guest lecturer at the Technical University of Ilmenau in Germany, teaching SEPs for the Internet of Things.

18. At the time of writing this declaration, I am following – including attending selected meetings – the following standards committees: ETSI oneM2M, ETSI IPR Special Committee, OMA, and 3GPP.

19. A copy of my curriculum vitae, which includes a detailed description of my experience and education, is attached as Appendix A. A list of litigation matters on which I have worked over the last five years is also included in my curriculum vitae.

III. SUMMARY OF MY OPINIONS

20. It is my opinion that EX1021 is an authentic copy of 3GPP Technical Specification TS 23.057 Version 7.0.0 entitled "Mobile Execution Environment (MExE); Functional description; Stage 2 (Release 7)" that was uploaded and made publicly available via the 3GPP FTP server by June 13, 2007 and not later than June 19, 2007.

21. It is my opinion that EX1018 is an authentic copy of 3GPP Technical Specification TS 31.101 Version 7.0.1 entitled "UICC-terminal interface; Physical and logical characteristics (Release 7)" that was uploaded and made publicly available via the 3GPP FTP server by June 20, 2007 and not later than June 21, 2007.

22. It is my opinion that EX1019 is an authentic copy of 3GPP Technical Specification TS 31.102 Version 8.0.0 entitled "Characteristics of the Universal

Subscriber Identity Module (USIM) application (Release 8)" that was uploaded and made publicly available via the 3GPP FTP server by December 21, 2007.

23. It is my opinion that EX1020 is an authentic copy of 3GPP Technical Specification TS 51.011 Version 4.10.0 entitled "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (Release 4)" that was uploaded and made publicly available via the 3GPP FTP server by January 12, 2004.

IV. PUBLICATIONS OF 3GPP SPECIFICATIONS AND RELATED DOCUMENTS

A. General Practices

24. Unless otherwise noted, the foregoing and following is an accurate description of 3GPP general practices from 1998 to the present, including in 2003-2007, regardless of whether I use the present or past tense to describe those practices.

25. 3GPP was established in 1998 by a group of telecommunications standard development organizations from Japan, Korea, China, Europe, and the United States to jointly develop worldwide standards for mobile telecommunications. Today, 3GPP consists of seven partners: Association of Radio Industries and Businesses, Japan ("ARIB"), Alliance for Telecommunications Industry Solutions, USA ("ATIS"), China Communications Standards Association ("CCSA"), European Telecommunications Standards Institute ("ETSI"),

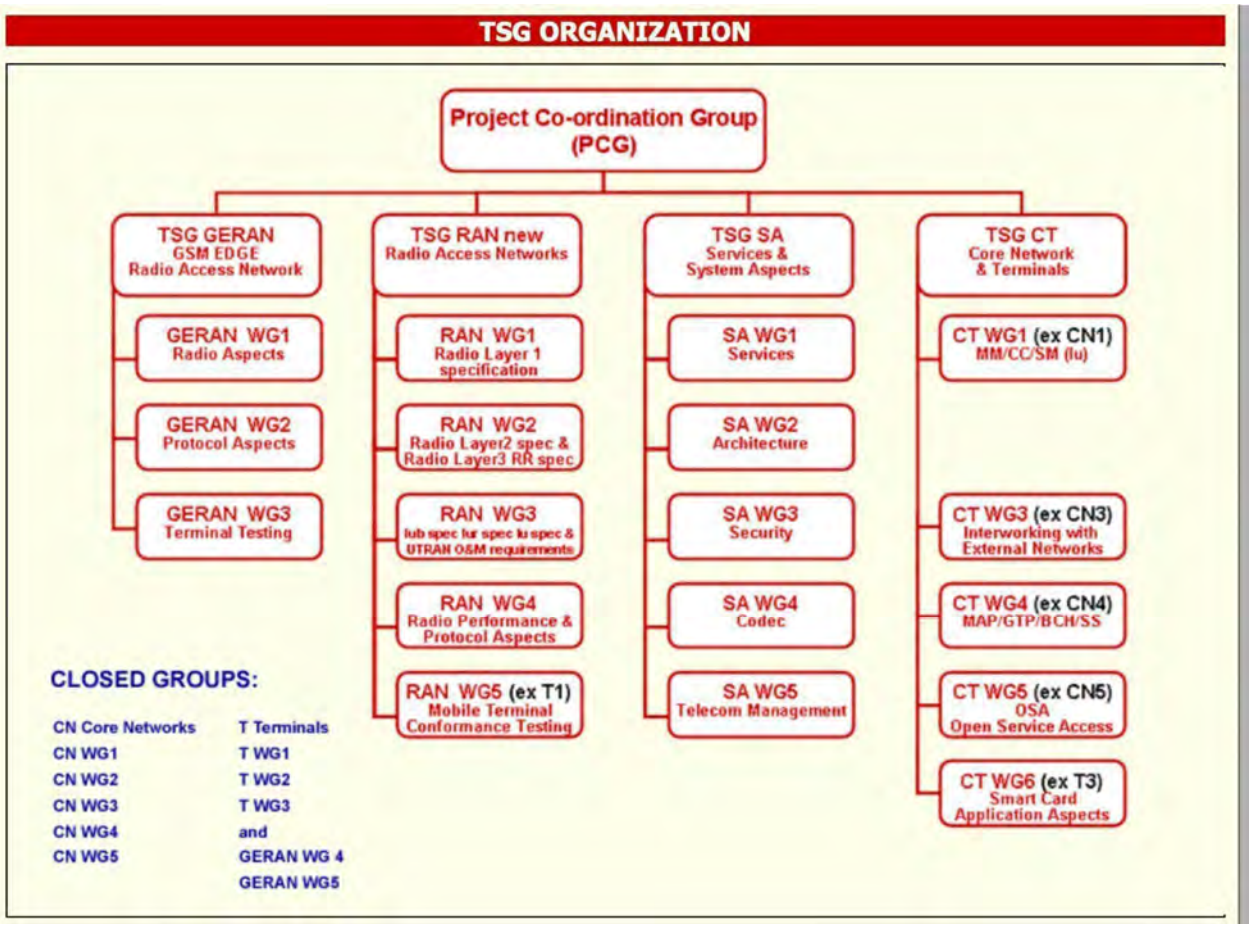
Telecommunications Standards Development Society, India ("TSDSI"), Telecommunications Technology Association, Korea ("TTA"), and Telecommunication Technology Committee, Japan ("TTC"). In addition to being one of the founding partners, ETSI hosts the Mobile Competence Centre ("MCC"), which provides administrative and technical support for the day-to-day work of 3GPP. Furthermore, ETSI manages 3GPP's IT services such as the 3GPP website, FTP server, and email exploders.

26. 3GPP is the world's leading organization for developing and maintaining cellular telecommunications standards, which it has done since it was founded in 1998. As noted above and in my curriculum vitae, I began working for 3GPP, as part of my work at ETSI, the European-based organizational partner of 3GPP.

27. In the ordinary course of its regularly conducted business activities, and pursuant to its standard business practices, 3GPP publishes technical specifications, proposals, reports, and other documents related to the development of cellular telecommunications standards. Such documents are published for the purposes of discussion and establishment of industry standards for cellular telecommunications. This has been 3GPP's ordinary course of business since I began working at ETSI in 1998.

28. In the ordinary course of 3GPP's regularly conducted business activities, and pursuant to its standard business practices, all draft technical specifications, proposals, reports, and other temporary documents to be discussed or considered in relation to 3GPP's telecommunications standards activities were, and continue to be, assigned a temporary document number and made publicly available, including on the FTP server associated with the 3GPP website, currently residing at ftp.3gpp.org. Such documents are referred to as "TDocs." Final versions of the technical specifications also were, and continue to be, publicly available on that same FTP server.

29. The names and the structure of 3GPP working groups, as of 2005, can be found at https://web.archive.org/web/20050805030338/http://www.3gpp.org:80/tb/home.htm (reproduced below and as Appendix B):



30. Each Technical Specification Group (TSG) or Working Group adopts a structured numbering system for the documents associated with their meetings, and those systems typically follow a consistent numbering system as shown in the following example: xminnzzzz. The numbering system normally comprises five logical elements: (1) x: a single letter corresponding to the TSG; wherein in 2005 x was one of R (Radio Access Network), C (Core and Terminals), S (Service and System Aspects), or G (GSM/EDGE Radio Access Network); (2) m: a single character corresponding to the Working Group identity (typically 1, 2, 3, etc.) or, in the case of the TSG itself, the letter “P”; (3) i: normally the hyphen character “-”;

(4) nn: the calendar year of the meeting to which the document was submitted; and (5) zzzz: a running number.

31. In the ordinary course of 3GPP's regularly conducted business activities, and pursuant to its standard business practices, from December 1998 onwards, 3GPP published all of its TDocs and all final versions of its technical specifications on its FTP server, which has always been easily and publicly accessible from its website and currently resides at ftp.3gpp.org.

32. By December 1998, including in 2005, 3GPP's FTP server was freely accessible to the general public with no login, password, or membership requirement.

33. By 1999, at least 100 companies were members of 3GPP (852 companies by August 2025), ranging from Bosch to Ericsson to Nokia to Samsung and generally including those interested in the discussion, creation, and adoption of cellular telecommunications standards, including GSM and UMTS. Each of these companies typically delegated multiple individuals to regularly participate in 3GPP meetings. Further, pursuant to 3GPP's standard business practices, 3GPP working groups sent emails notifying these individuals as soon as new or additional documents had been uploaded to 3GPP's FTP server. Thus, not only did the general public have access to the documents on the FTP server, but some of the interested members of the public—those working to develop standards for cellular

telecommunication or working to implement the standards—were personally informed of their availability by email. Based on my experience with 3GPP and the telecommunications industry, I would expect any person implementing a cellular network or device, e.g., a GSM or UMTS or LTE or 5G network or device - including any key component such as the SIM card and its respective interface to the device - to consult the corresponding specifications on the 3GPP FTP server, as well as other related documents. The purpose of 3GPP creating and making these documents available was so that engineers and other individuals would have ready access to them when developing and implementing cellular networks and devices.

34. By June 1999, 3GPP's FTP server was well-known to persons in the cellular telecommunications industry as a source of public information regarding industry standards and technological advances.

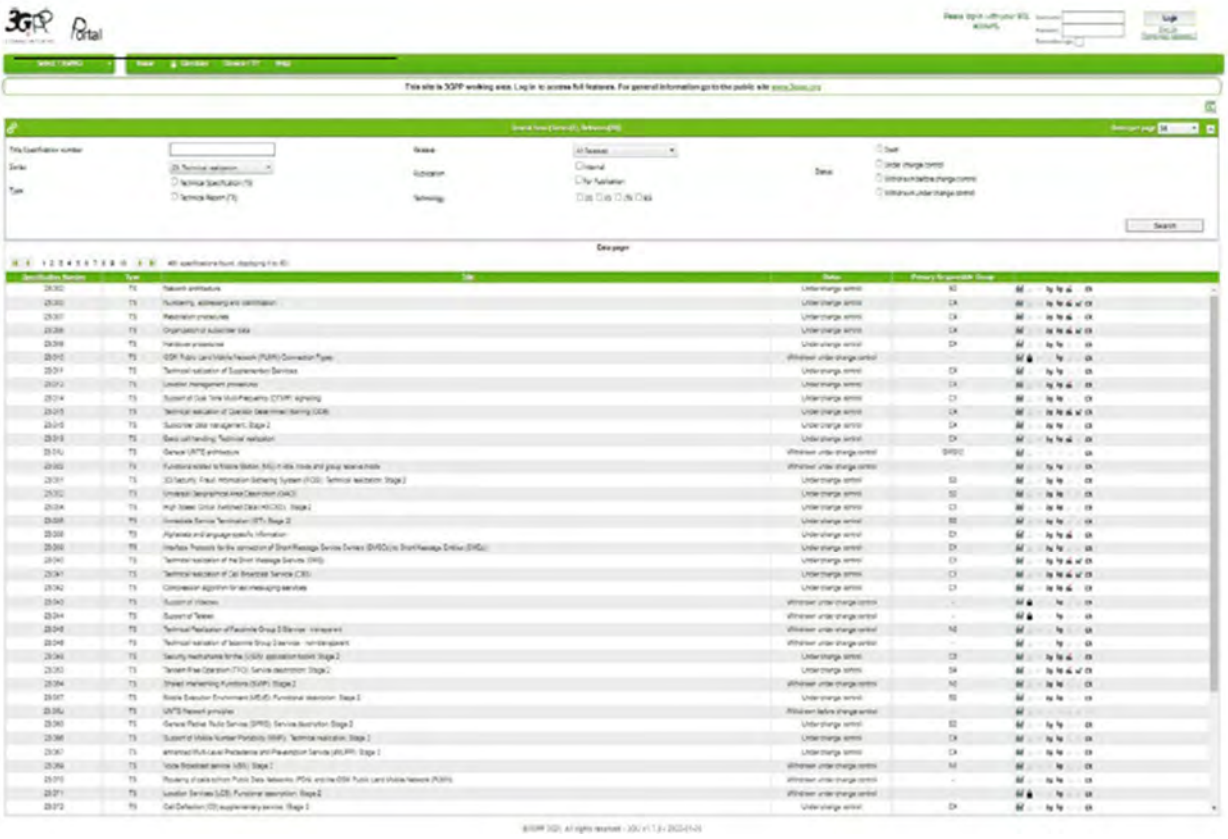
35. 3GPP specifications bear a specification number consisting of four or five digits, e.g., 09.02 or 29.002. The first two digits define the specification series which are defined to group the different aspects of the 3GPP system into, e.g., requirements, service aspects, radio aspects codecs, security aspects, and test specifications. The series digits are followed by two additional digits for the 01 to 13 series or three further digits for the 21 to 55 series. The subjects of the individual specification series are explained on 3GPP's website at

https://www.3gpp.org/specifications-technologies/specifications-by-series, and are reproduced below[3]:

[3] Full website available as Appendix C.

Subject of specification series	3G and beyond / GSM (R99 and later)	GSM only (Rel-4 and later)	GSM only (before Rel-4)
Requirements	21 series	41 series	01 series
Service aspects ("stage 1")	22 series	42 series	02 series
Technical realization ("stage 2")	23 series	43 series	03 series
Signalling protocols ("stage 3") - user equipment to network	24 series	44 series	04 series
Radio aspects	25 series	45 series	05 series
CODECs	26 series	46 series	06 series
Data	27 series	47 series (none exists)	07 series
Signalling protocols ("stage 3") -(RSS-CN) and OAM&P and Charging (overflow from 32.-range)	28 series	48 series	08 series
Signalling protocols ("stage 3") - intra-fixed-network	29 series	49 series	09 series
Programme management	30 series	50 series	10 series
Subscriber Identity Module (SIM / USIM), IC Cards. Test specs.	31 series	51 series	11 series
OAM&P and Charging	32 series	52 series	12 series
Access requirements and test specifications		13 series (1)	13 series (1)
Security aspects	33 series	(2)	(2)
UE and (U)SIM test specifications	34 series	(2)	11 series
Security algorithms (3)	35 series	55 series	(4)
LTE (Evolved UTRA), LTE-Advanced, LTE-Advanced Pro radio technology	36 series		
Multiple radio access technology aspects	37 series		
Radio technology beyond LTE	38 series		

36. Following a link for a series (e.g., “23 series” link) leads to a 3GPP web page providing access to all specifications in a series, as shown by the screenshot below[4]



37. In the ordinary course of 3GPP’s regularly conducted business activities, and pursuant to its standard business practices, 3GPP published and continues to publish all proposals, technical reports, technical specifications and other documents related to the development of cellular telecommunications

[4] Full website available as Appendix D.

standards to the 3GPP's publicly available, unrestricted, online FTP server: http://www.3gpp.org/ftp/. Draft proposals, technical reports, technical specifications, change requests, and other documents ("TDocs") were assigned a document number ("TDoc number") and uploaded to 3GPP's public FTP server before, during, and after meetings, making the documents publicly available. TDocs are usually uploaded to 3GPP's FTP server and website before the meeting where they are to be discussed. Documents created or revised during the course of a meeting are normally uploaded at the latest during the week following the meeting (e.g., the meeting report of the meeting is usually published for review during the week following the meeting and for approval at the next working group meeting).

38. In the ordinary course of 3GPP's regularly conducted business activities, and pursuant to its standard business practices, 3GPP maintains archives that include different versions of the specifications, as well as email communications to its membership, including emails announcing the uploading of new or additional documents to 3GPP's FTP server. These archives are created at the time the emails are initially sent.

39. The timestamp on 3GPP's FTP server shows the date when the document was uploaded the last time. Thus, the timestamp shows the latest possible date the document became publicly available and accessible on 3GPP's

FTP server. The given document might have been available earlier and the original timestamp might have been overwritten because the document was uploaded again. According to my experience, this is something which happened occasionally. Thus, the FTP timestamp is reliable as the latest possible upload date but one cannot determine whether it represents the first upload of a document to the FTP server.

40. 3GPP specifications are stored at different locations on ETSI's IT infrastructure which serves 3GPP delegates and anybody interested in developments around 3GPP standards. Specifications are stored in the "Specs" folder on the FTP server (www.3gpp.org/ftp/specs) from where they can be downloaded. Additionally, they are also available via the 3GPP portal (portal.3gpp.org). Usually, the specifications become available on different locations during the same day. However, occasionally it takes one or several days until specifications become accessible via the portal after being uploaded to the FTP server. This explains why the FTP specifications archive and the 3GPP portal screenshots in this declaration might show slightly different dates. However, it is the FTP server date stamp which represents the date a specification became available.

41. 3GPP's working practice to store their documents on its FTP server, as described above, has not changed over time. Starting from the first 3GPP meetings in 1998 until present, all WGs and plenary meetings are represented by

dedicated meeting folders on the FTP server. These meeting folders include the documents discussed at the meetings. Both the folders and the documents are accessible to the public. Almost every week, a new meeting folder with the respective documents is added. In addition to the plenary and WG meeting folders, and some other folders, there is also the “Specs” folder, which holds all 3GPP specifications including the aforementioned “snapshot” and archive folders. Since the early days of 3GPP, a new folder is added inside the “Specs” folder after each TSG plenary meeting, to hold the latest versions of specifications approved at those TSG plenary meetings. This is still 3GPP’s working practice today; thus, this practice has not changed over time.

42. 3GPP maintains a set of publicly accessible documents providing further details on its way of working:

- 3GPP Working Procedures
- Vocabulary for 3GPP Specifications 3GPP TR 21.905
- Working Methods 3GPP TR 21.900
- Specification Drafting Rules 3GPP TR 21.801

B. 3GPP TS 23.057 V7.0.0 (EX1021)

1. Authentication

43. EX1021 is a true and correct copy of 3GPP TS 23.057 V7.0.0, titled "Mobile Execution Environment (MExE); Functional description; Stage 2 (Release 7)". I obtained EX1021 from 3GPP's FTP server at the following location: https://www.3gpp.org/ftp/specs/archive/23_series/23.057[5]

2. Publication by 3GPP and ETSI

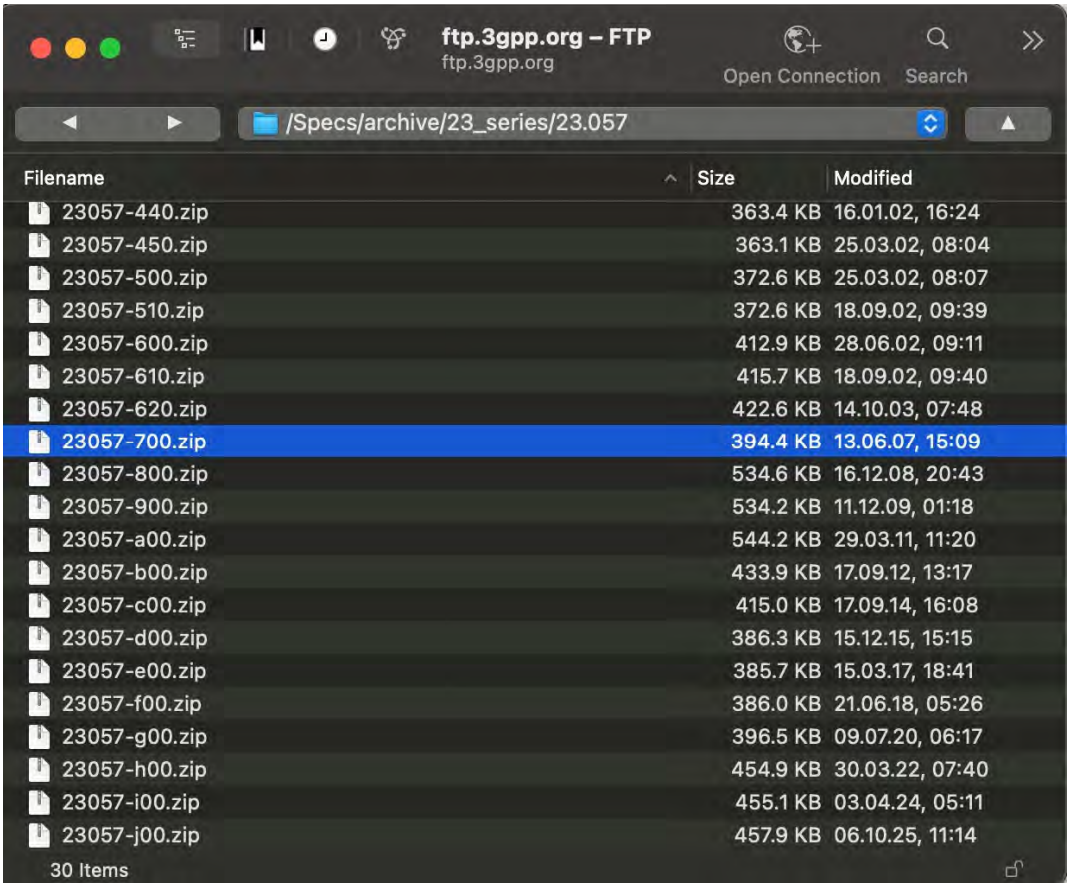
44. EX1021 shows on its cover page "2007-06" as the year (2007) and month (June) during which the document was released by 3GPP.

45. EX1021 was uploaded to the 3GPP FTP server on June 13, 2007, based on the upload date stamp shown on the historic 3GPP FTP server for the corresponding downloadable file ("23057-700.zip"), as maintained by the Internet Archive at https://web.archive.org/web/20071123021842/http://www.3gpp.org/ftp/Specs/archive/23_series/23.057/[6]. This information is also shown on the date stamp for the present-day listing of the same document on the 3GPP FTP server at

[5] Website available as Appendix X

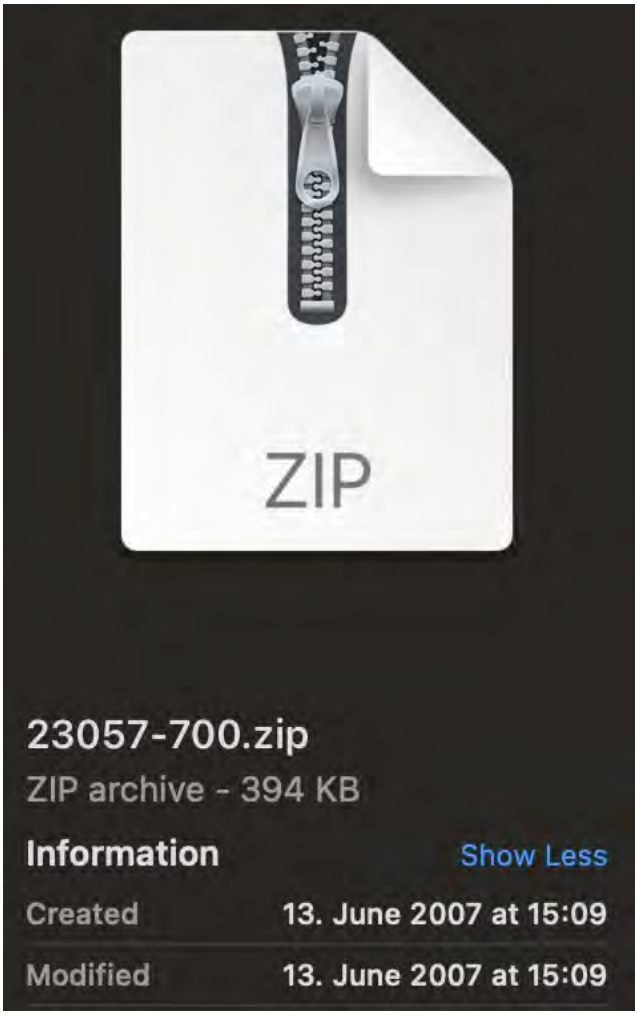
[6] Website available as Appendix Y.

https://www.3gpp.org/ftp/specs/archive/23_series/23.057 as shown in the screenshot below (listing date as “13.06.07”, or June 13, 2007):



46. Experts in the field of determining the public availability of 3GPP documents would reasonably rely upon the FTP server upload date on the current 3GPP FTP server as well as an archived version of the directory structure maintained by the Internet Archive to establish a date that a 3GPP document became available to the public via the 3GPP FTP server.

47. In addition, metadata information for the downloaded and extracted TDoc file states a last "Modified" date of "13. June 2007," as shown in the screenshot below:



48. This last modified date is consistent with the June 13, 2007, upload date of the document and the typical practice among 3GPP staff to upload technical specifications shortly after creating them.

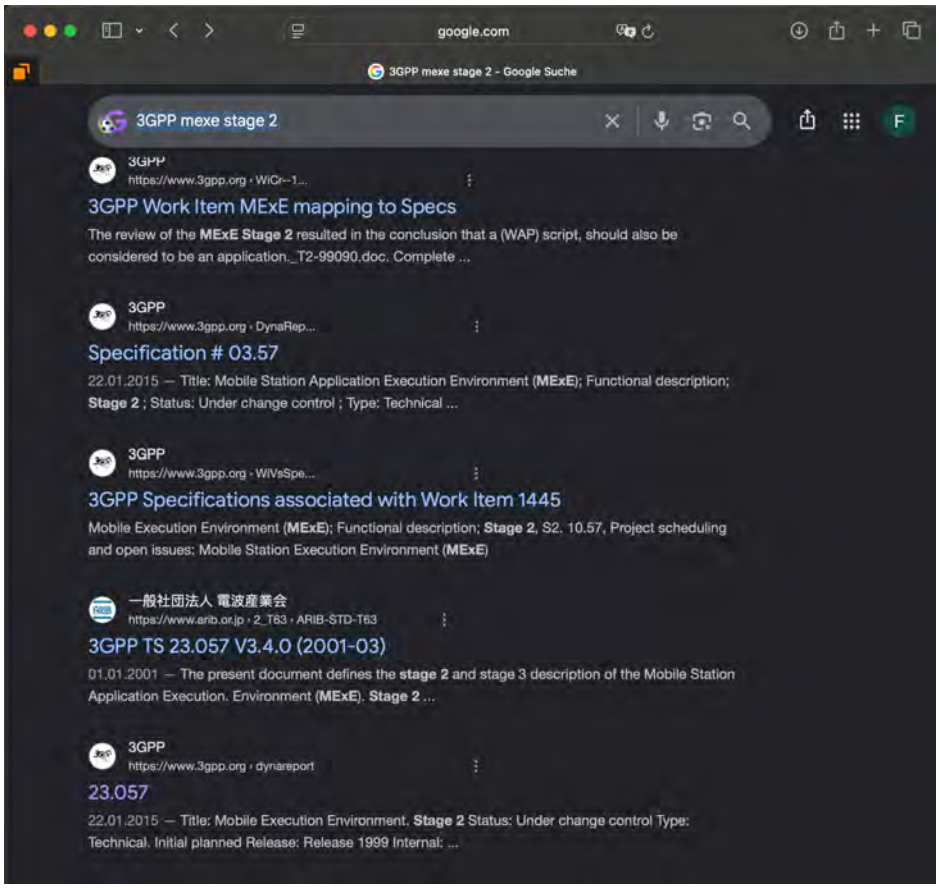
49. This publication date is further confirmed by the document history on the last page of the ETSI copy of TS 23.057 named "ETSI TS 123 057," which states that V7.0.0 was published in June 2007.[7] Upload to the ETSI website took place on June 21, 2007.[8] This is shortly after the upload to the 3GPP FTP server as it is common practice that the ETSI versions of 3GPP specifications are uploaded a few weeks after the 3GPP specifications were uploaded.

50. I believe that a person without prior knowledge of the technical specification (TS) number would have been able to also easily find the TS for download via internet search. For instance, a Google search for "3GPP mexe stage 2" provides the TS number "23.057" as one of the top results as can be seen in the screenshot below:

---

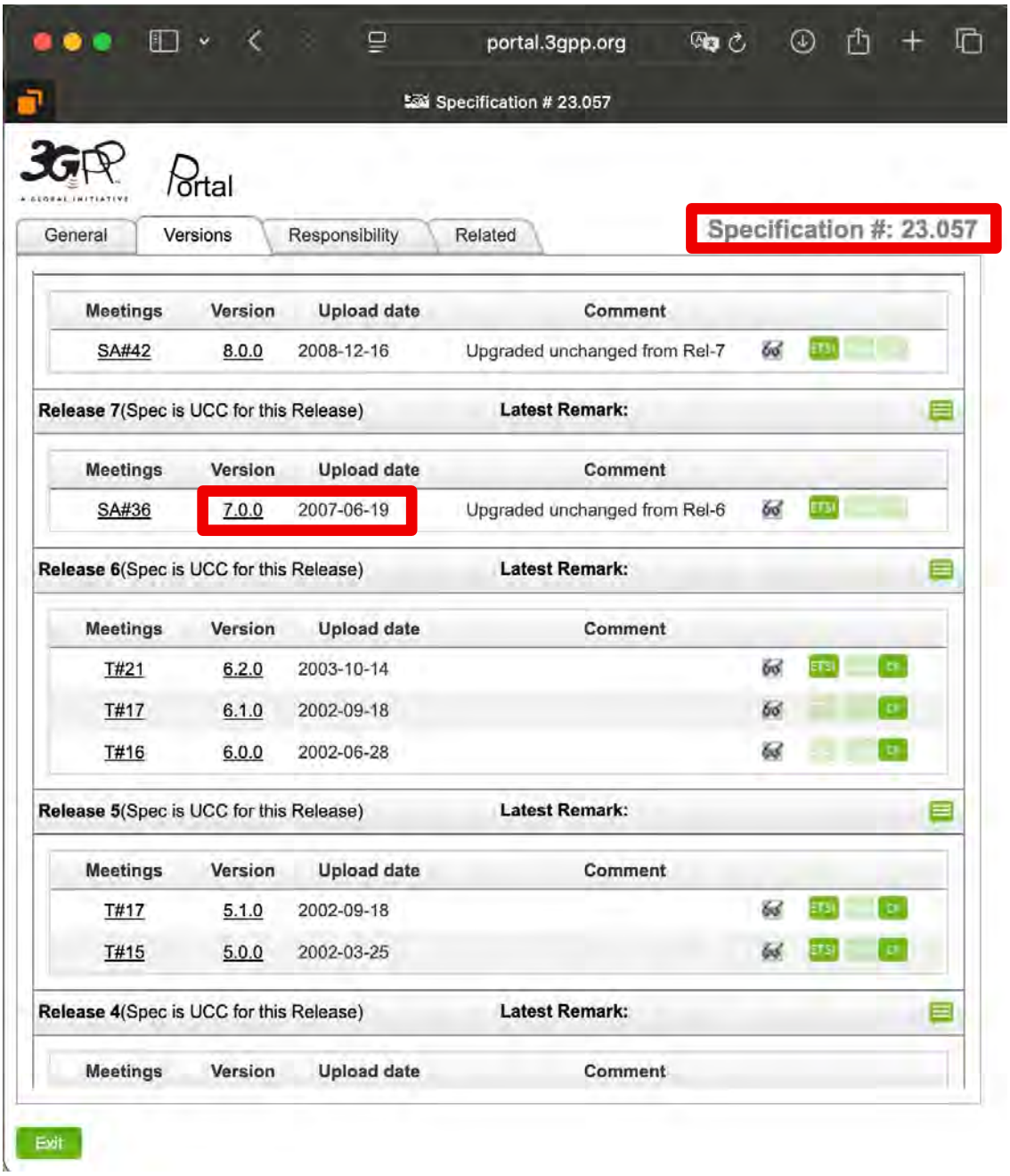
[7] https://www.etsi.org/deliver/etsi_ts/123000_123099/123057/07.00.00_60/ts_123057v070000p.pdf (Appendix Z)

[8] https://www.etsi.org/deliver/etsi_ts/123000_123099/123057/07.00.00_60/



51. Following the provided search result link “23.057” leads to a 3GPP web page offering under the tab “Versions” download links to all versions of TS 23.057 including version 7.0.0, as shown by the screenshot below[9]:

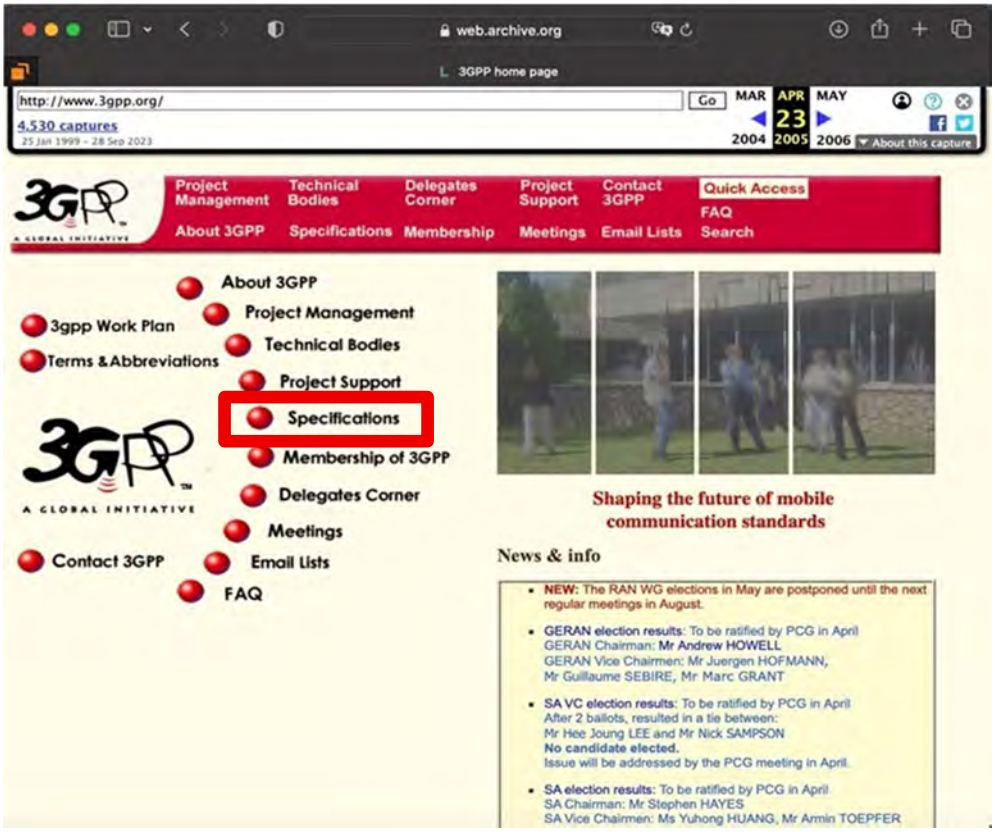
[9] Full website available as Appendix R.



52. The above example search illustrates that it is very easy for an interested member of the public without prior knowledge of the TS number to locate any version of TS 23.057, including version 7.0.0, for download.

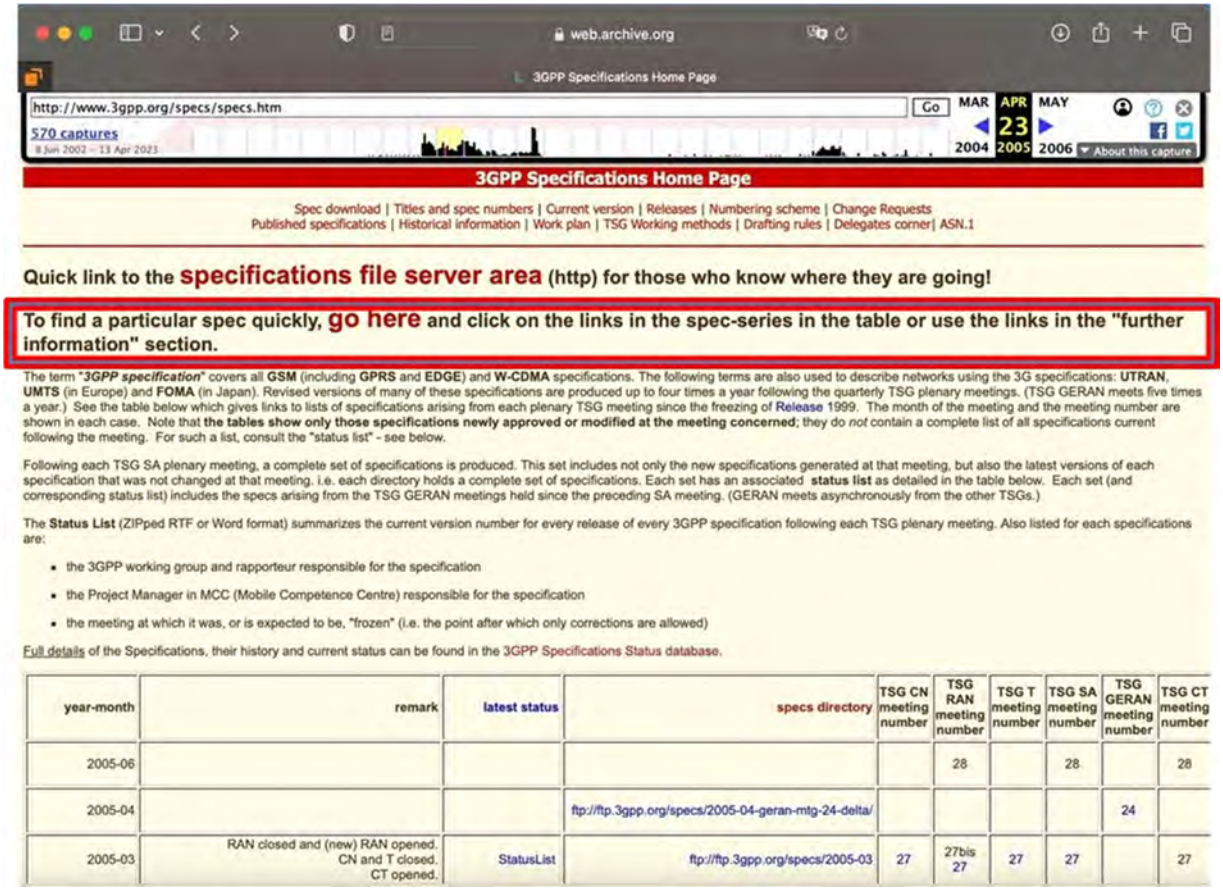
53. The above search was performed at the time of writing this declaration. According to my personal experience, similar searches done in 2007 or around that time would have similarly provided a path to download version 7.0.0 of TS 23.057 although the layout of the webpages was slightly different.

54. A similar search performed in 2007 could have looked like described in the following paragraphs. The 3GPP homepage from 2005 shown below included already a link to "Specifications"[10]:



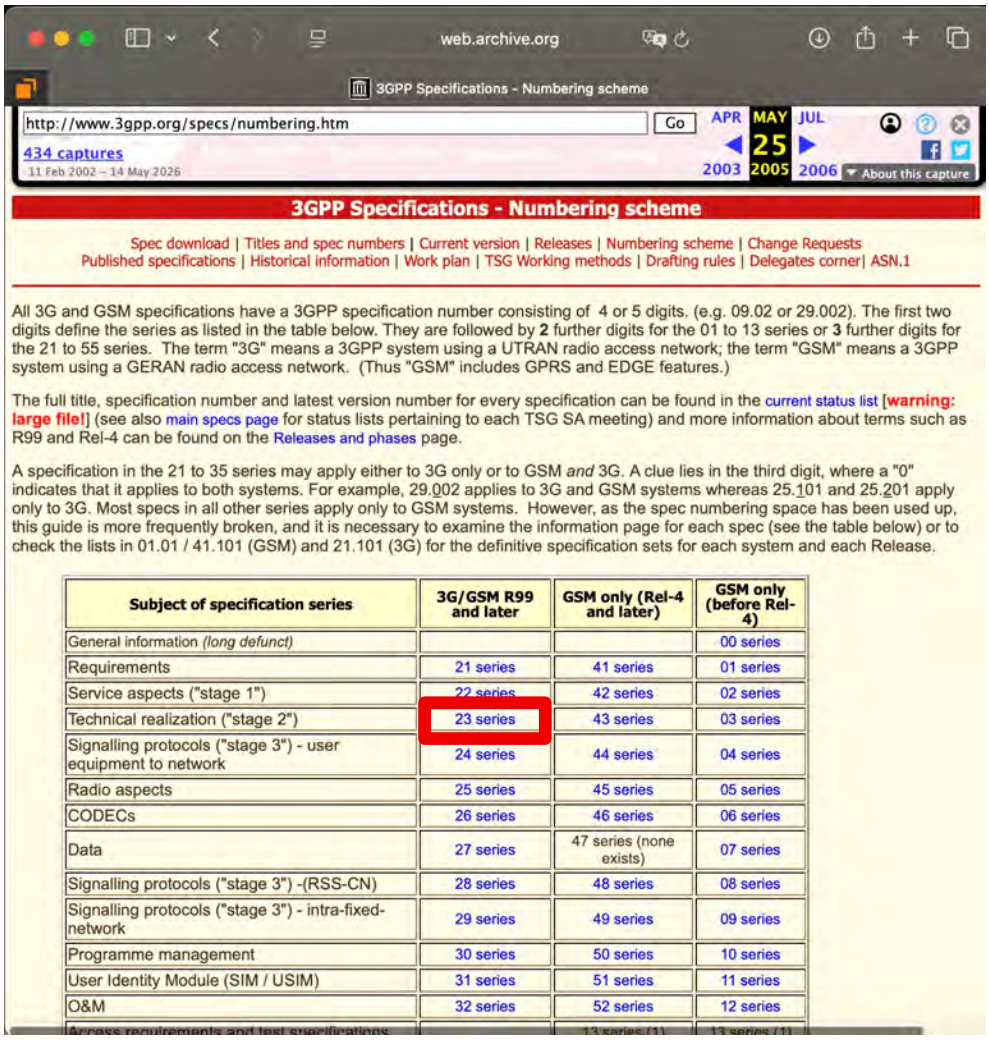
[10] Full website available as Appendix G.

55. Clicking on the "Specifications" link provided a specifications webpage with various paths for locating specific specifications, such as specification snapshots, e.g., "2005-03", a link to the "specifications file server area", or a link to the specifications series page ("To find a particular spec quickly, go here and click on the links in the spec-series in the table or use the links in the 'further information' section."), as shown below[11]:



[11] Full website available as Appendix H.

56. The subjects of the individual specification series for the 3GPP standards were explained on 3GPP's website by clicking on the "To find a particular spec quickly, go here …" link on the specifications webpage identified above. This link directed to the 3GPP specification numbering webpage shown below[12]:



[12] Full website available as Appendix I.

57. Following the link for the 23 series would have led to a 3GPP webpage providing access to all specifications in a series and providing a subject matter index to the list of specifications, as shown by an excerpt of the webpage below[13]:

[13] Full website available as Appendix AA.



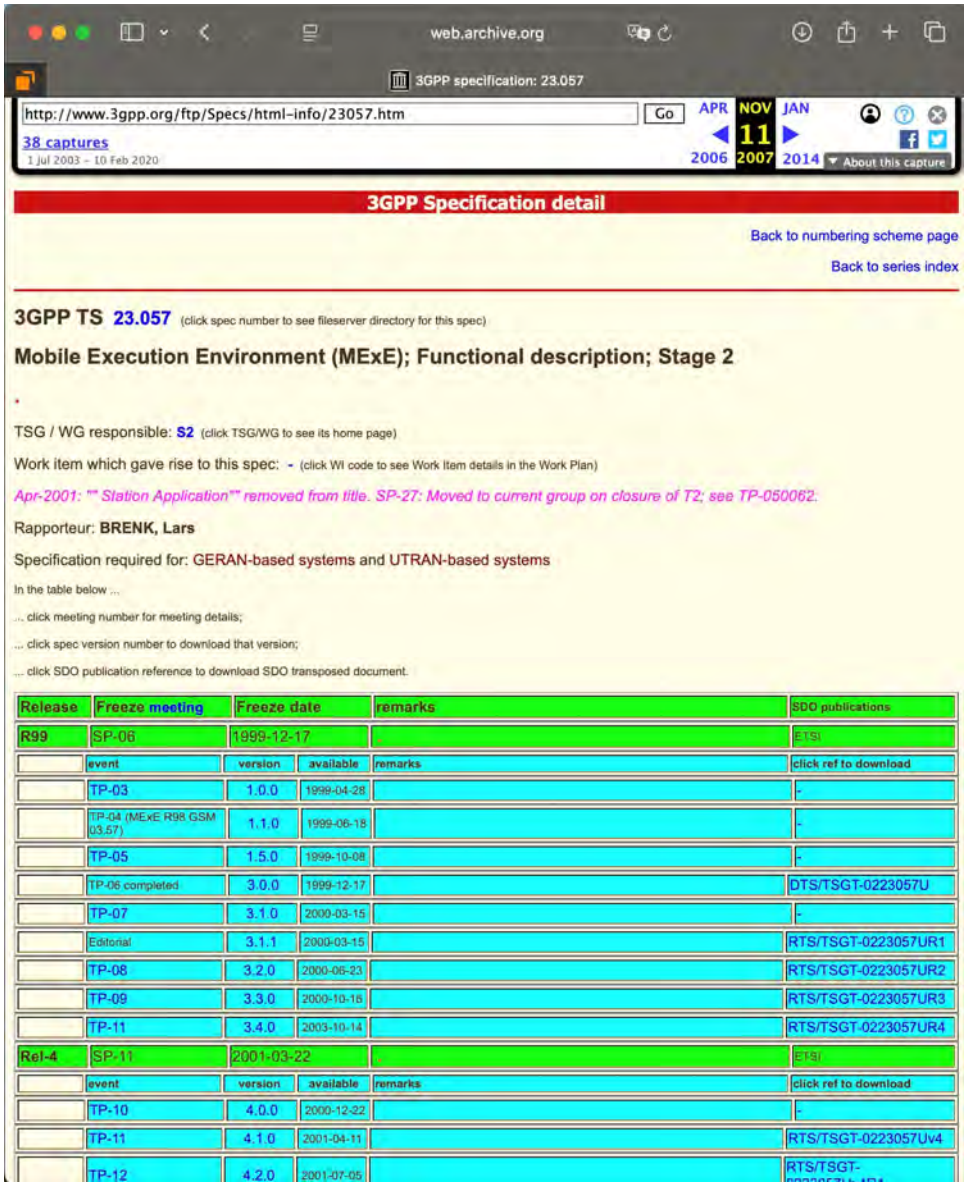
3GPP Specification series

Back to numbering scheme page

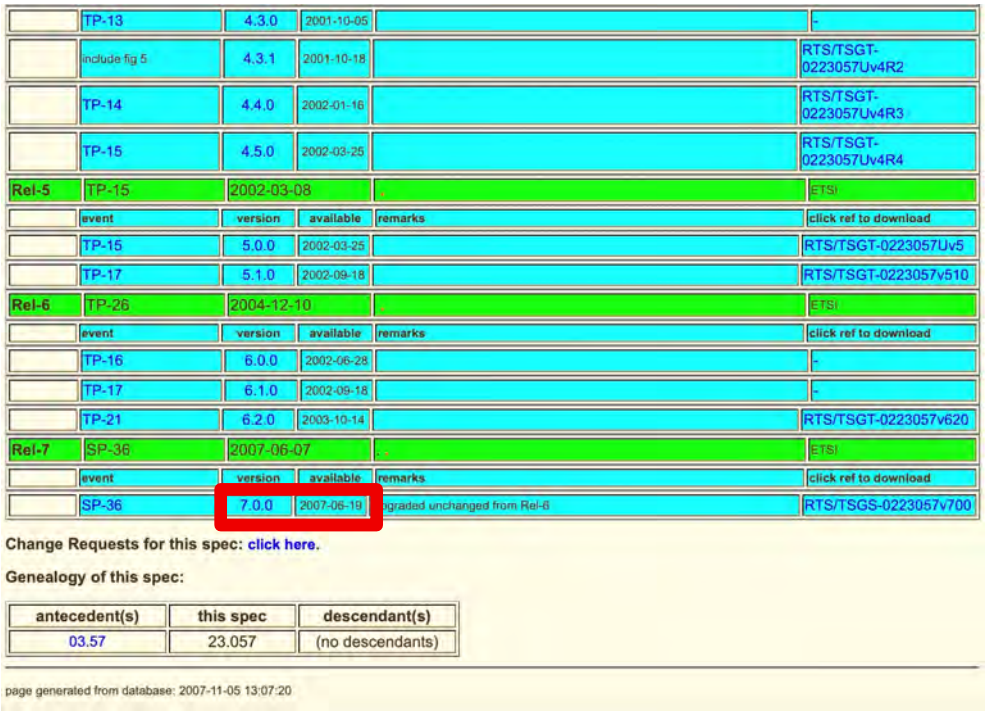
Click on spec number for details

TS 23.002	Network architecture	.
TS 23.003	Numbering, addressing and identification	.
TS 23.007	Restoration procedures	.
TS 23.008	Organization of subscriber data	.
TS 23.009	Handover procedures	.
TS 23.010	GSM Public Land Mobile Network (PLMN) Connection Types	SPECIFICATION WITHDRAWN
TS 23.011	Technical realization of Supplementary Services	.
TS 23.012	Location management procedures	.
TS 23.014	Support of Dual Tone Multi Frequency (DTMF) signalling	.
TS 23.015	Technical realization of Operator Determined Barring (ODB)	.
TS 23.016	Subscriber data management; Stage 2	.
TS 23.018	Basic call handling; Technical realization	.
TS 23.01U	General UMTS architecture	SPECIFICATION WITHDRAWN
TS 23.022	Functions related to Mobile Station (MS) in idle mode and group receive mode	SPECIFICATION WITHDRAWN
TS 23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	.
TS 23.032	Universal Geographical Area Description (GAD)	.
TS 23.034	High Speed Circuit Switched Data (HSCSD); Stage 2	.
TS 23.035	Immediate Service Termination (IST); Stage 2	.
TS 23.038	Alphabets and language-specific information	.
TR 23.039	Interface Protocols for the Connection of Short Message Service Centers (SMSCs) to Short Message Entities (SMEs)	.
TS 23.040	Technical realization of Short Message Service (SMS)	.
TS 23.041	Technical realization of Cell Broadcast Service (CBS)	.
TS 23.042	Compression algorithm for SMS	.
TS 23.043	Support of Videotex	SPECIFICATION WITHDRAWN
TS 23.044	Support of Teletex	SPECIFICATION WITHDRAWN
TS 23.045	Technical Realization of Facsimile Group 3 Service - transparent	SPECIFICATION WITHDRAWN
TS 23.046	Technical realisation of facsimile Group 3 service - non-transparent	SPECIFICATION WITHDRAWN
TS 23.048	Security mechanisms for the (U)SIM application toolkit; Stage 2	.
TS 23.053	Tandem Free Operation (TFO); Service description; Stage 2	.
TS 23.054	Shared Interworking Functions (SIWF); Stage 2	SPECIFICATION WITHDRAWN
TS 23.057	Mobile Execution Environment (MExE); Functional description; Stage 2	.
TS 23.05U	UMTS Network principles	SPECIFICATION WITHDRAWN
TS 23.060	General Packet Radio Service (GPRS); Service description; Stage 2	.
TS 23.066	Support of GSM Mobile Number Portability (MNP) stage 2	.

58. Following the link for TS 23.057 would have led to a 3GPP webpage providing access to all versions of TS 23.057 including V7.0.0 for download, as shown by annotated excerpts of the webpage below[14]:



[14] Full website available as Appendix N.



	TP-13	4.3.0	2001-10-05		-
	include fig 5	4.3.1	2001-10-18		RTS/TSGT-0223057Uv4R2
	TP-14	4.4.0	2002-01-16		RTS/TSGT-0223057Uv4R3
	TP-15	4.5.0	2002-03-25		RTS/TSGT-0223057Uv4R4
Rel-5	TP-15	2002-03-08			ETSI
	event	version	available	remarks	click ref to download
	TP-15	5.0.0	2002-03-25		RTS/TSGT-0223057Uv5
	TP-17	5.1.0	2002-09-18		RTS/TSGT-0223057v510
Rel-6	TP-26	2004-12-10			ETSI
	event	version	available	remarks	click ref to download
	TP-16	6.0.0	2002-06-28		-
	TP-17	6.1.0	2002-09-18		-
	TP-21	6.2.0	2003-10-14		RTS/TSGT-0223057v620
Rel-7	SP-36	2007-06-07			ETSI
	event	version	available	remarks	click ref to download
	SP-36	7.0.0	2007-06-19	igraded unchanged from Rel-6	RTS/TSGS-0223057v700

Change Requests for this spec: click here.

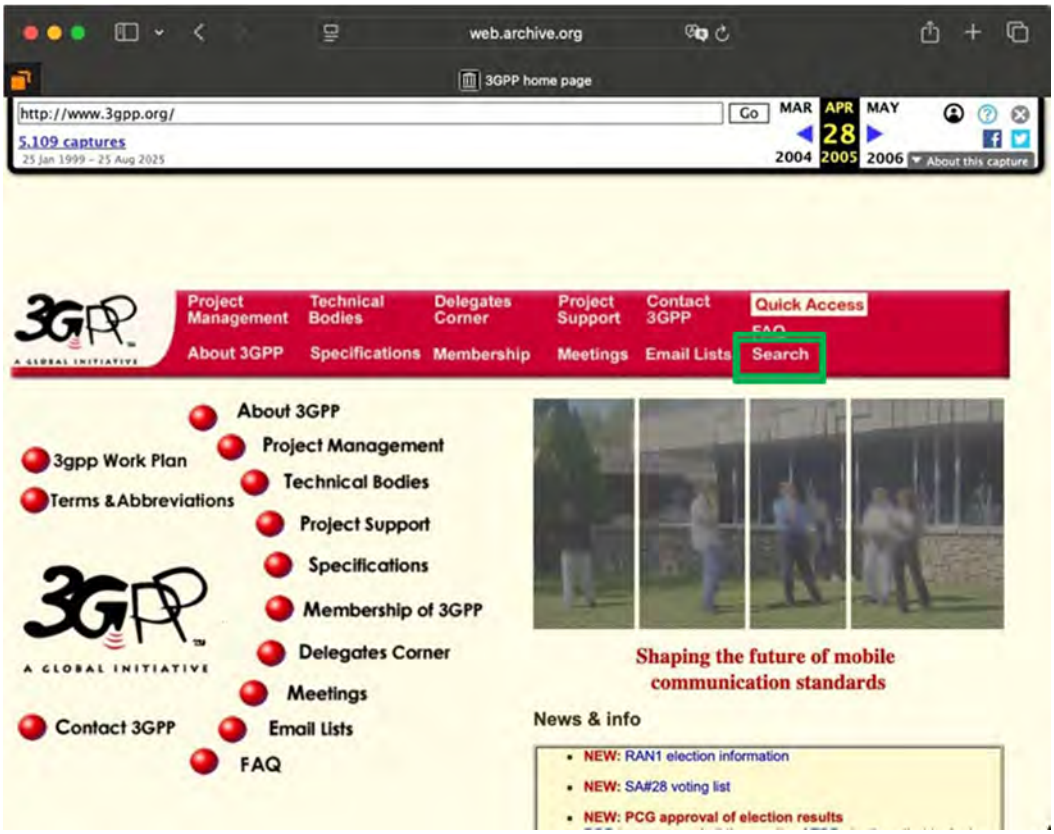
Genealogy of this spec:

antecedent(s)	this spec	descendant(s)
03.57	23.057	(no descendants)

page generated from database: 2007-11-05 13:07:20

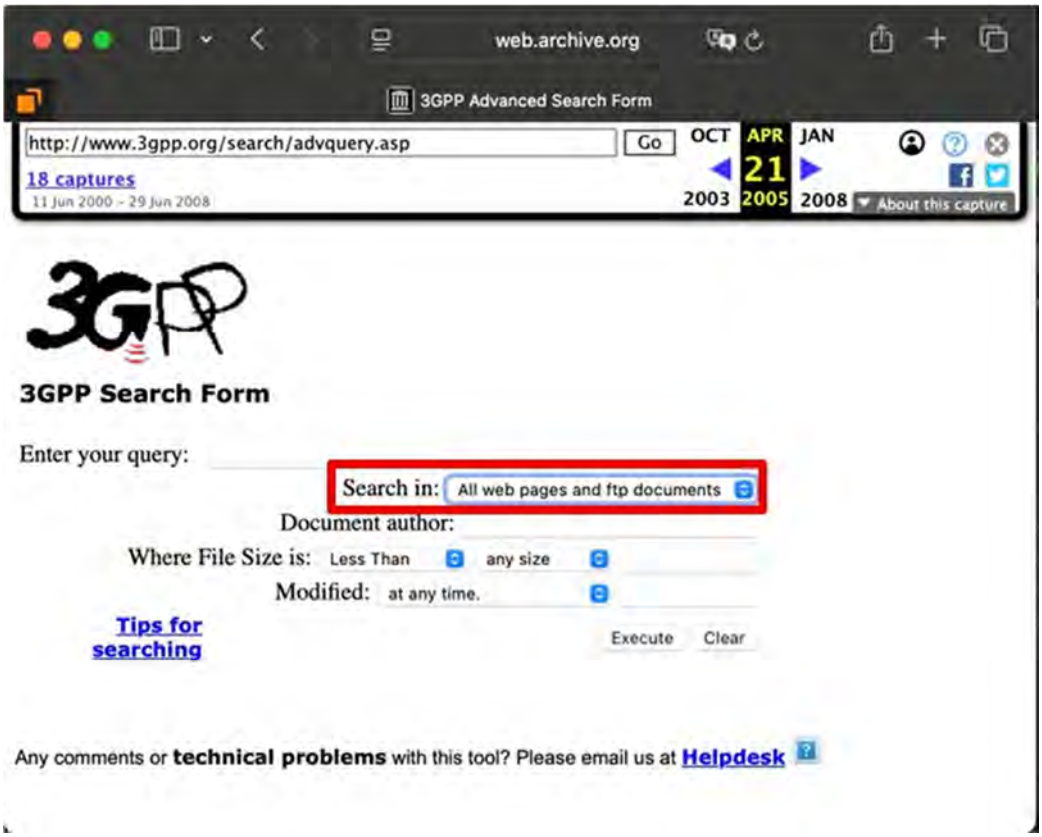
59. In summary, there are - and there were in 2007 - several paths to locate and download a specific 3GPP specification. Thus, it is - and was already in 2007 - straightforward for any interested person including members of the public to access 3GPP specifications such as TS 23.057 V7.0.0.

60. Furthermore, the 3GPP webpage included a search function already in 2005 as can be seen by the annotated screenshot from the Internet Archive below (https://web.archive.org/web/20050428075227/http://www.3gpp.org/):



61. The 3GPP search form allowed to search "All web pages and ftp documents" as can be seen by the annotated screenshot from the Internet Archive below[15]:

15 https://web.archive.org/web/20050421234921/http://www.3gpp.org/search/advquery.asp



62. Thus, in addition to the paths for downloading a specific Technical Specification (TS) described further above, it would have been possible to use the 3GPP web site's search function to find information and specific documents including technical specifications.

3. Conclusion

63. Thus, based on my personal knowledge and experience with ETSI's and 3GPP's standard business practices, this information tells me that EX1021 (3GPP TS 23.057 Version 7.0.0) was uploaded and made available via the 3GPP FTP server to 3GPP delegates and interested members of the public who would have been able to locate the reference exercising reasonable diligence by June 13, 2007 and not later than June 19, 2007.

C. 3GPP TS 31.101 V7.0.1 (EX1018)

1. Authentication

64. EX1018 is a true and correct copy of 3GPP TS 31.101 V7.0.1, titled "UICC-terminal interface; Physical and logical characteristics (Release 7)". I obtained EX1018 from 3GPP's FTP server at the following location: https://www.3gpp.org/ftp/specs/archive/31_series/31.101[16]

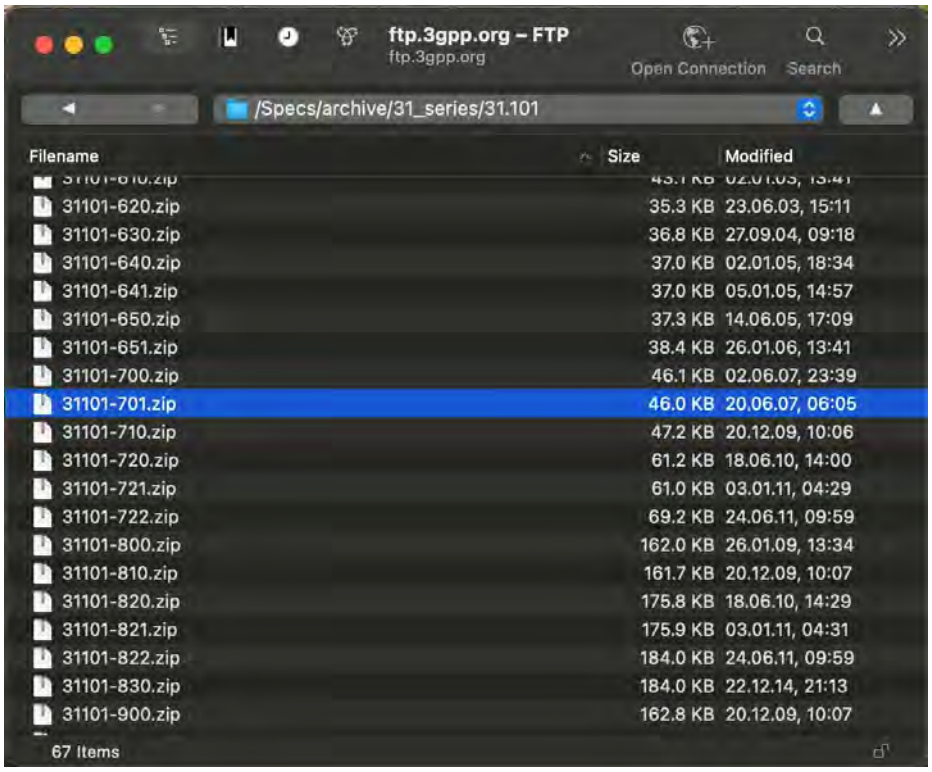
2. Publication by 3GPP and ETSI

65. EX1018 shows on its cover page "2007-06" as the year (2007) and month (June) during which the document was released by 3GPP.

[16] Website available as Appendix O

66. EX1018 was uploaded to the 3GPP FTP server on June 20, 2007, based on the upload date stamp shown on the historic 3GPP FTP server for the corresponding downloadable file ("31101-701.zip"), as maintained by the Internet Archive at https://web.archive.org/web/20071112060040/http://www.3gpp.org/ftp/Specs/archive/31_series/31.101/[17]. This information is also shown on the date stamp for the present-day listing of the same document on the 3GPP FTP server at https://www.3gpp.org/ftp/specs/archive/31_series/31.101 as shown in the screenshot below (listing date as "20.06.07", or June 20, 2007):

[17] Website available as Appendix P.



67. Experts in the field of determining the public availability of 3GPP documents would reasonably rely upon the FTP server upload date on the current 3GPP FTP server as well as an archived version of the directory structure maintained by the Internet Archive to establish a date that a 3GPP document became available to the public via the 3GPP FTP server.

68. In addition, metadata information for the downloaded and extracted TDoc file states a last “Modified” date of “20. June 2007,” as shown in the screenshot below:



69. This last modified date is consistent with the June 20, 2007, upload date of the document and the typical practice among 3GPP staff to upload technical specifications shortly after creating them.

70. This publication date is further confirmed by the document history on the last page of the ETSI copy of TS 31.101 named “ETSI TS 131 101,” which

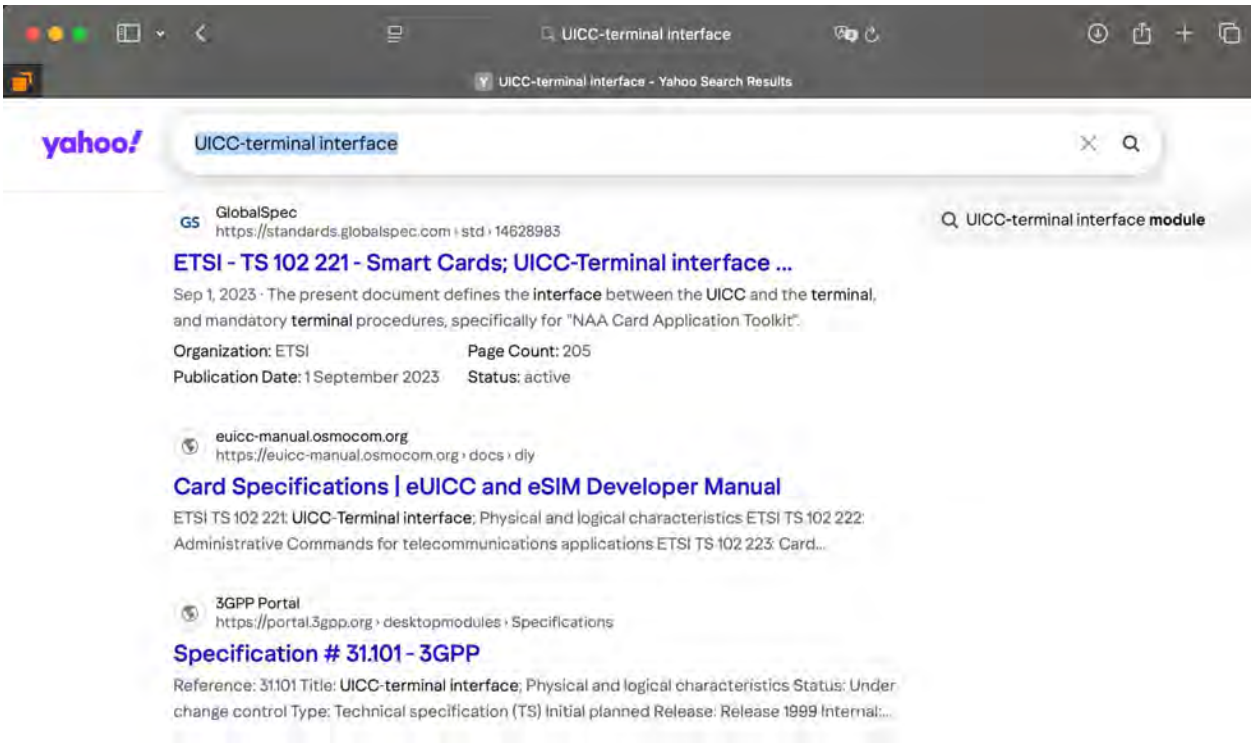
states that V7.0.1 was published in June 2007.[18] Upload to the ETSI website took place on July 19, 2007.[19] This is shortly after the upload to the 3GPP FTP server as it is common practice that the ETSI versions of 3GPP specifications are uploaded a few weeks after the 3GPP specifications were uploaded.

71. I believe that a person without prior knowledge of 3GPP and/or the technical specification (TS) number would have been able to also easily find the TS for download via internet search. For instance, a Yahoo search for "UICC-terminal interface" provides the TS number "31.101" as one of the top results as can be seen in the screenshot below:

---

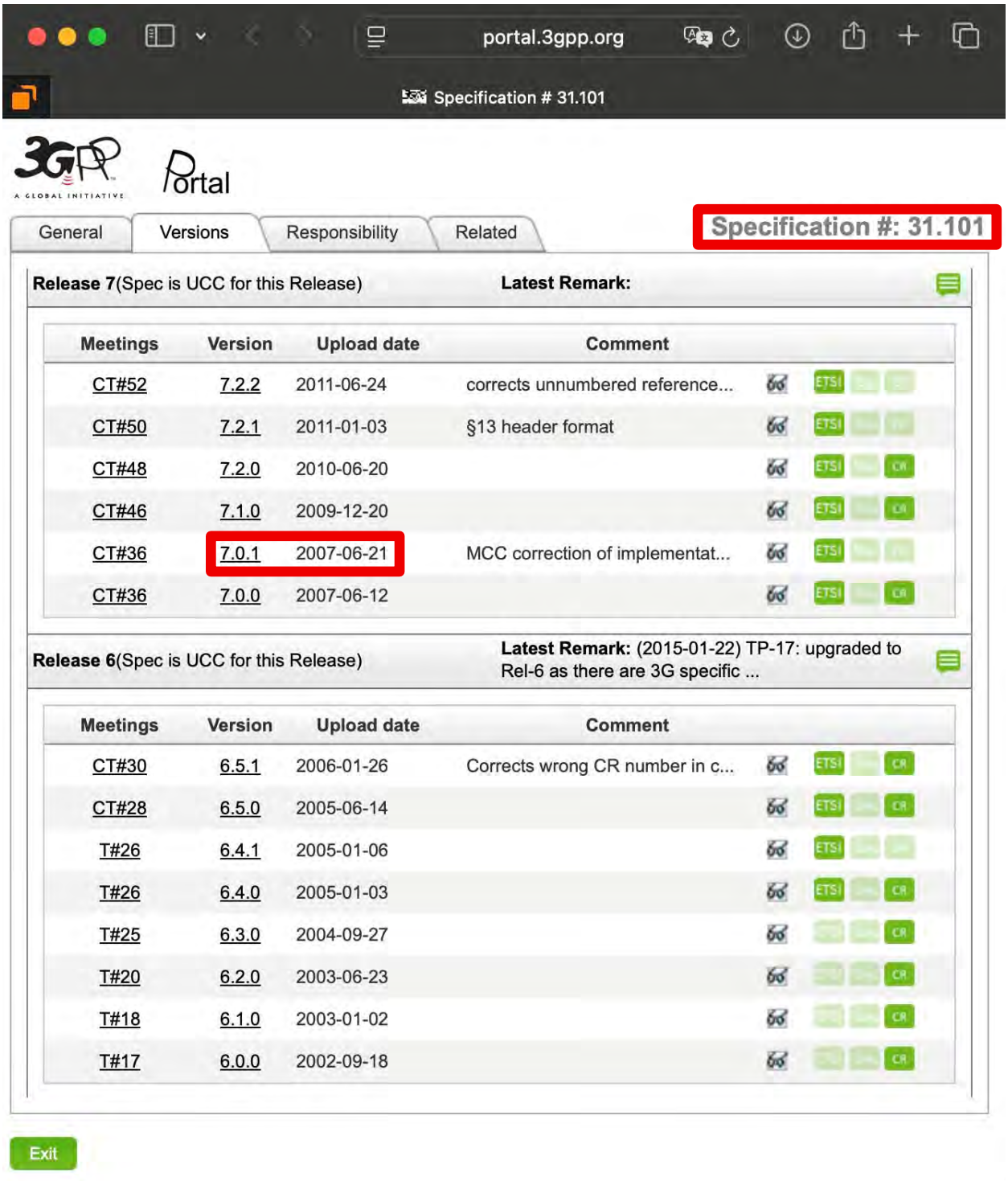
[18] https://www.etsi.org/deliver/etsi_ts/131100_131199/131101/07.00.01_60/ts_131101v070001p.pdf (Appendix Q)

[19] https://www.etsi.org/deliver/etsi_ts/131100_131199/131101/07.00.01_60/



72. Following the provided search result link “Specification # 31.101 – 3GPP” leads to a 3GPP web page offering under the tab “Versions” download links to all versions of TS 31.101 including version 7.0.1, as shown by the screenshot below[20]:

[20] Full website available as Appendix AB.



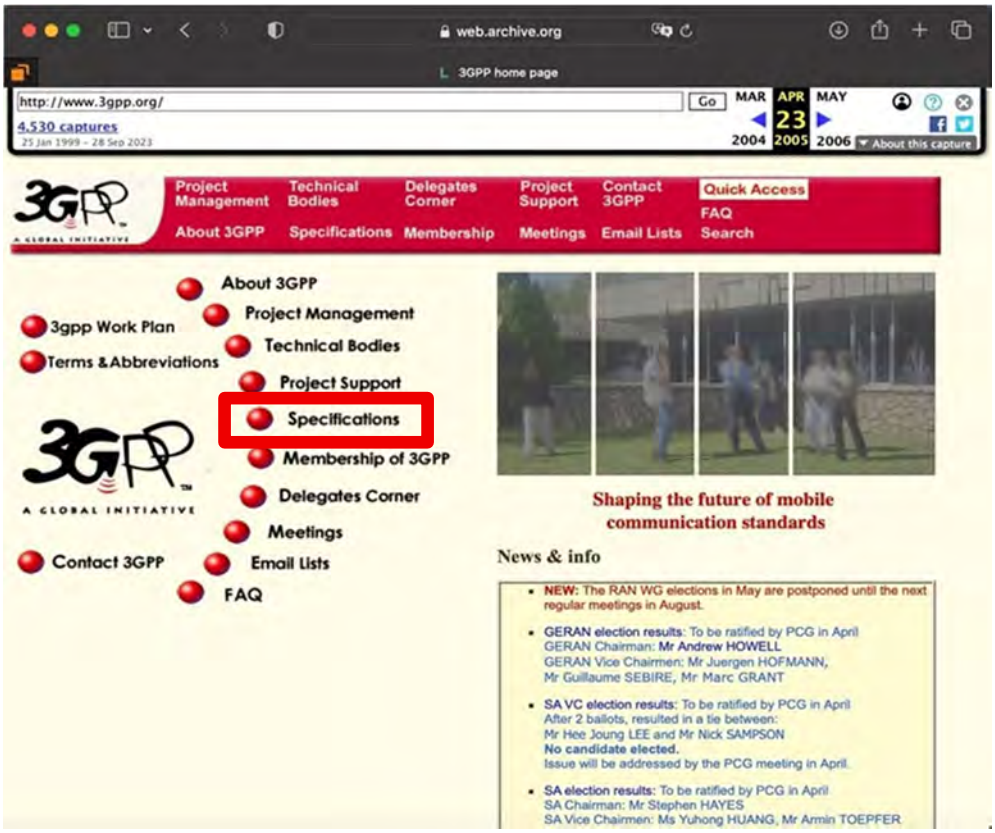
73. The above example search illustrates that it is very easy for an interested member of the public without prior knowledge of the TS number and

even without prior knowledge of 3GPP to locate any version of TS 31.101, including version 7.0.1, for download.

74. The above search was performed at the time of writing this declaration. According to my personal experience, similar searches done in 2007 or around that time would have similarly provided a path to download version 7.0.1 of TS 31.101 although the layout of the webpages was slightly different.

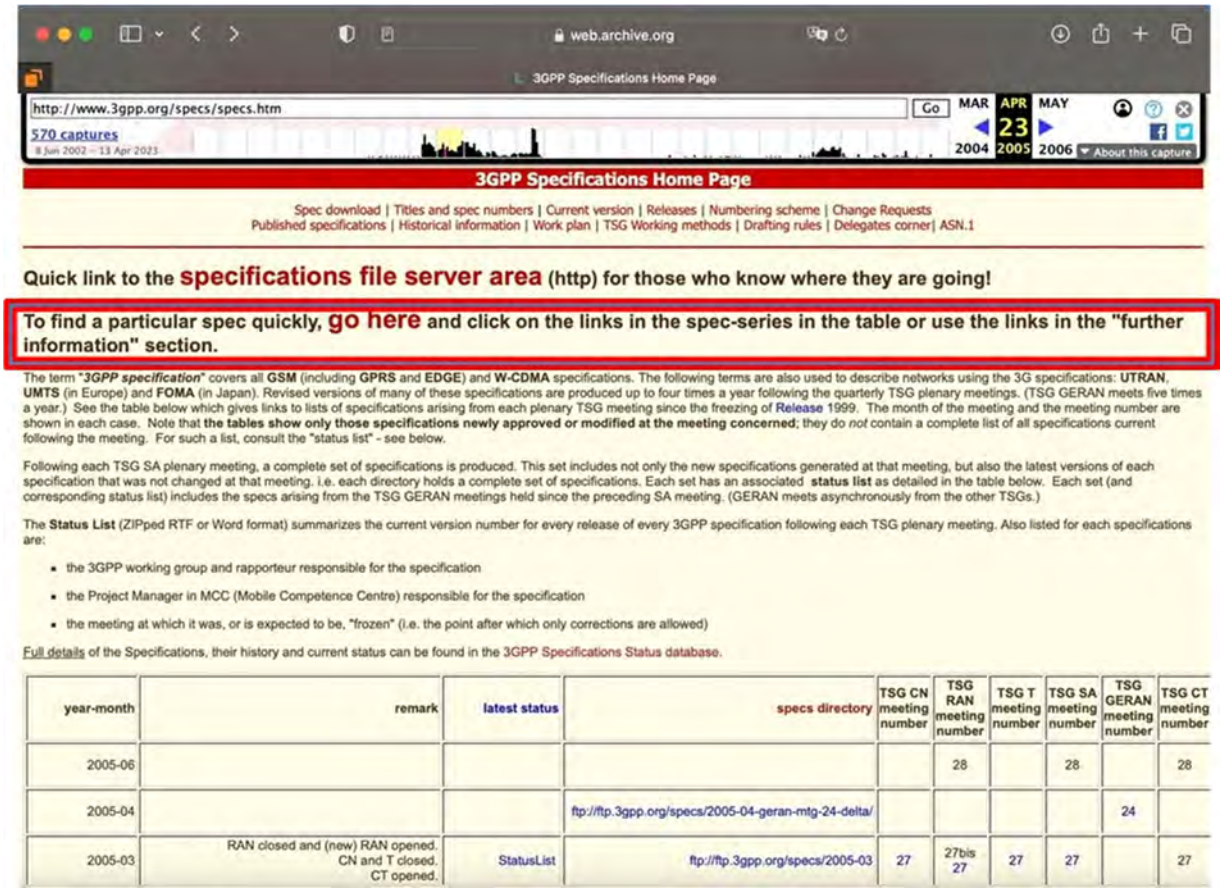
75. A similar search performed in 2007 could have looked like described in the following paragraphs. The 3GPP homepage from 2005 shown below included already a link to “Specifications”[21]:

[21] Full website available as Appendix G.



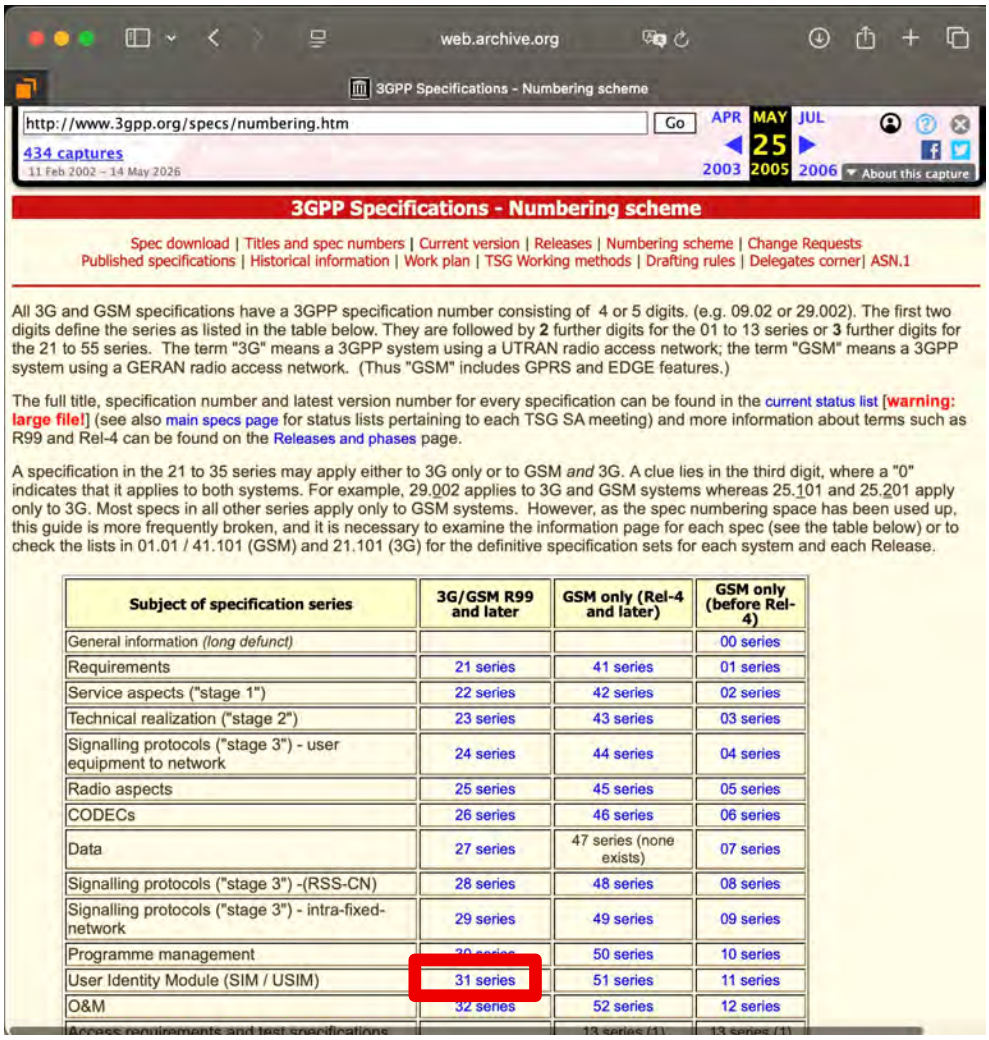
76. Clicking on the “Specifications” link provided a specifications webpage with various paths for locating specific specifications, such as specification snapshots, e.g., “2005-03”, a link to the “specifications file server area”, or a link to the specifications series page (“To find a particular spec quickly, go here and click on the links in the spec-series in the table or use the links in the ‘further information’ section.”), as shown below[22]:

[22] Full website available as Appendix H.



77. The subjects of the individual specification series for the 3GPP standards were explained on 3GPP's website by clicking on the "To find a particular spec quickly, go here …" link on the specifications webpage identified above. This link directed to the 3GPP specification numbering webpage shown below[23]:

[23] Full website available as Appendix I.



78. Following the link for the 31 series would have led to a 3GPP webpage providing access to all specifications in a series and providing a subject matter index to the list of specifications, as shown by an excerpt of the webpage below[24]:

[24] Full website available as Appendix R.



3GPP Specification series

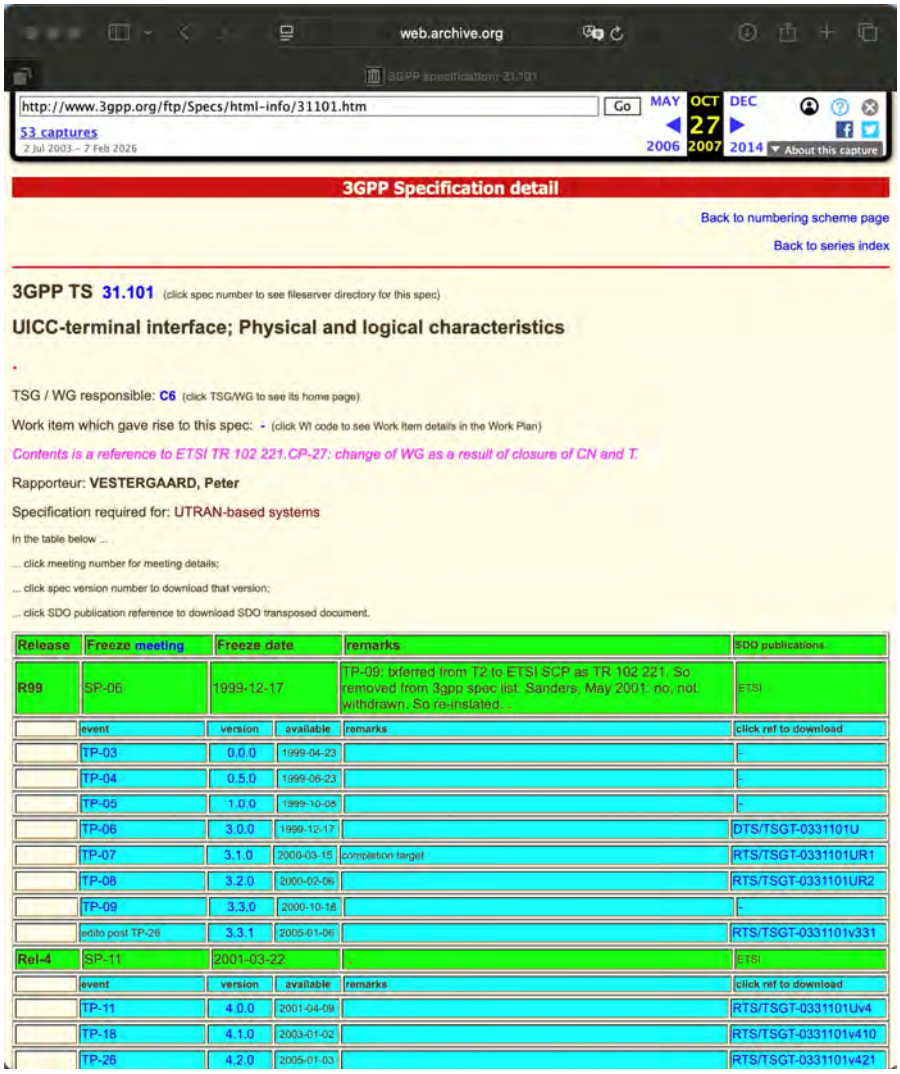
Back to numbering scheme page

Click on spec number for details

TS 31.048	Security mechanisms for the (U)SIM application toolkit; Test specification	
TS 31.101	UICC-terminal interface; Physical and logical characteristics	
TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application	
TS 31.103	Characteristics of the IP Multimedia Services Identity Module (ISIM) application	
TS 31.110	Numbering system for telecommunication IC card applications	
TS 31.111	Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)	
TS 31.112	Universal Subscriber Identity Module Application Toolkit (USAT) interpreter architecture description; Stage 2	
TS 31.113	Universal Subscriber Identity Module Application Toolkit (USAT) interpreter byte codes	
TS 31.114	Universal Subscriber Identity Module Application Toolkit (USAT) interpreter protocol and administration	
TS 31.115	Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications	
TS 31.116	Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications	
TS 31.120	UICC-terminal interface; Physical, electrical and logical test specification	
TS 31.121	UICC-terminal interface; Universal Subscriber Identity Module (USIM) application test specification	
TS 31.122	Universal Subscriber Identity Module (USIM) conformance test specification	
TS 31.123	(Universal) Subscriber Interface Module ((U)SIM) toolkit interpreter test	SPECIFICATION WITHDRAWN
TS 31.124	Mobile Equipment (ME) conformance test specification; Universal Subscriber Interface Module Application Toolkit (USAT) conformance test specification	
TS 31.130	(U)SIM Application Programming Interface (API); (U)SIM API for Java Card	
TS 31.131	C-language binding for (Universal) Subscriber Identity Module ((U)SIM) API	
TS 31.133	IP Multimedia Services Identity Module (ISIM) Application Programming Interface (API); ISIM API for Java Card™	
TS 31.213	Test specification for subscriber (U)SIM; Application Programming Interface (API) for Java Card™	
TS 31.50U	Essential requirements for UMTS Mobile Stations (ME) operating within frequency bands 1885-1980, 2010-2025 and 2110-2200 MHz	SPECIFICATION WITHDRAWN
TS 31.60U	Essential requirements for UMTS Mobile Earth Stations (MES) operating within frequency bands 1980- 2010 and 2170-2200 MHz	SPECIFICATION WITHDRAWN
TR 31.900	SIM/USIM internal and external interworking aspects	
TR 31.919	2G/3G Java Card™ Application Programming Interface (API) based applet interworking	

page generated from database: 2007-08-23 08:41:07

79. Following the link for TS 31.101 would have led to a 3GPP webpage providing access to all versions of TS 31.101 including V7.0.1 for download, as shown by annotated excerpts of the webpage below[25]:



web.archive.org

http://www.3gpp.org/ftp/Specs/html-info/31101.htm

53 captures

2 Jul 2003 - 7 Feb 2026

MAY OCT DEC

2006 27 2007 2014

About this capture

3GPP Specification detail

Back to numbering scheme page

Back to series index

3GPP TS 31.101 (click spec number to see fileserver directory for this spec)

UICC-terminal interface; Physical and logical characteristics

TSG / WG responsible: **C6** (click TSG/WG to see its home page)

Work item which gave rise to this spec: - (click WI code to see Work Item details in the Work Plan)

Contents is a reference to ETSI TR 102 221.CP-27: change of WG as a result of closure of CN and T.

Rapporteur: **VESTERGAARD, Peter**

Specification required for: UTRAN-based systems

In the table below ...

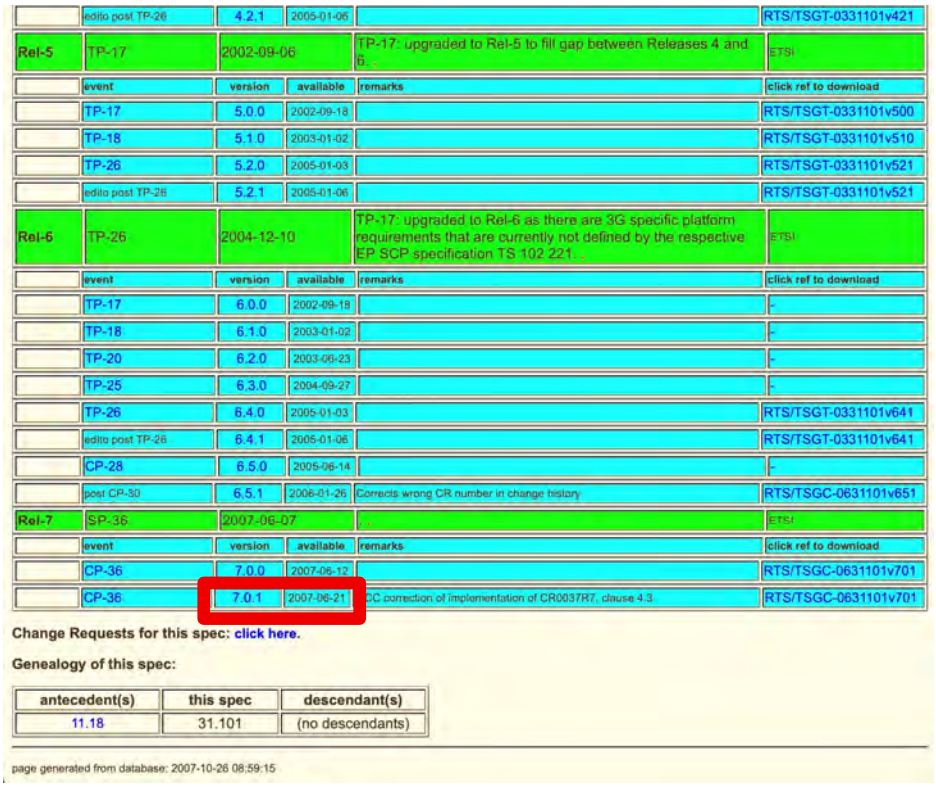
... click meeting number for meeting details;

... click spec version number to download that version;

... click SDO publication reference to download SDO transposed document.

Release	Freeze meeting	Freeze date	remarks	SDO publications
R99	SP-06	1999-12-17	TP-09: txferred from T2 to ETSI SCP as TR 102 221. So removed from 3gpp spec list. Sanders, May 2001: no, not withdrawn. So re-instated. .	ETSI
	event	version	available	remarks	click ref to download
	TP-03	0.0.0	1999-04-23		-
	TP-04	0.5.0	1999-06-23		-
	TP-05	1.0.0	1999-10-05		-
	TP-06	3.0.0	1999-12-17		DTS/TSGT-0331101U
	TP-07	3.1.0	2000-03-15	completion target	RTS/TSGT-0331101UR1
	TP-08	3.2.0	2000-02-06		RTS/TSGT-0331101UR2
	TP-09	3.3.0	2000-10-16		-
	edito post TP-26	3.3.1	2005-01-06		RTS/TSGT-0331101v331
Rel-4	SP-11	2001-03-22			ETSI
	event	version	available	remarks	click ref to download
	TP-11	4.0.0	2001-04-09		RTS/TSGT-0331101Uv4
	TP-18	4.1.0	2003-01-02		RTS/TSGT-0331101v410
	TP-26	4.2.0	2005-01-03		RTS/TSGT-0331101v421

[25] Full website available as Appendix S.



	edito post TP-26	4.2.1	2005-01-06		RTS/TSGT-0331101v421
Rel-5	TP-17	2002-09-06		TP-17: upgraded to Rel-5 to fill gap between Releases 4 and 6	ETSI
	event	version	available	remarks	click ref to download
	TP-17	5.0.0	2002-09-18		RTS/TSGT-0331101v500
	TP-18	5.1.0	2003-01-02		RTS/TSGT-0331101v510
	TP-26	5.2.0	2005-01-03		RTS/TSGT-0331101v521
	edito post TP-26	5.2.1	2005-01-06		RTS/TSGT-0331101v521
Rel-6	TP-26	2004-12-10		TP-17: upgraded to Rel-6 as there are 3G specific platform requirements that are currently not defined by the respective EP SCP specification TS 102 221	ETSI
	event	version	available	remarks	click ref to download
	TP-17	6.0.0	2002-09-18		-
	TP-18	6.1.0	2003-01-02		-
	TP-20	6.2.0	2003-06-23		-
	TP-25	6.3.0	2004-09-27		-
	TP-26	6.4.0	2005-01-03		RTS/TSGT-0331101v641
	edito post TP-26	6.4.1	2005-01-06		RTS/TSGT-0331101v641
	CP-28	6.5.0	2005-06-14		-
	post CP-30	6.5.1	2006-01-26	Corrects wrong CR number in change history	RTS/TSGC-0631101v651
Rel-7	SP-36	2007-06-07			ETSI
	event	version	available	remarks	click ref to download
	CP-36	7.0.0	2007-06-12		RTS/TSGC-0631101v701
	CP-36	7.0.1	2007-06-21	CC correction of implementation of CR0037R7, clause 4.3	RTS/TSGC-0631101v701

Change Requests for this spec: click here.

Genealogy of this spec:

antecedent(s)	this spec	descendant(s)
11.18	31.101	(no descendants)

page generated from database: 2007-10-26 08:59:15

80. In summary, there are - and there were in 2007 - several paths to locate and download a specific 3GPP specification. Thus, it is - and was already in 2007 - straightforward for any interested person including members of the public to access 3GPP specifications such as TS 31.101 V7.0.1.

3. Conclusion

81. Thus, based on my personal knowledge and experience with ETSI's and 3GPP's standard business practices, this information tells me that EX1018 (3GPP TS 31.101 Version 7.0.1) was uploaded and made available via the 3GPP FTP server to 3GPP delegates and interested members of the public who would have been able to locate the reference exercising reasonable diligence by June 20, 2007 and not later than June 21, 2007.

D. 3GPP TS 31.102 V8.0.0 (EX1019)

1. Authentication

82. EX1019 is a true and correct copy of 3GPP TS 31.102 V8.0.0, titled "Characteristics of the Universal Subscriber Identity Module (USIM) application (Release 8)". I obtained EX1019 from 3GPP's FTP server at the following location: https://www.3gpp.org/ftp/specs/archive/31_series/31.102[26]

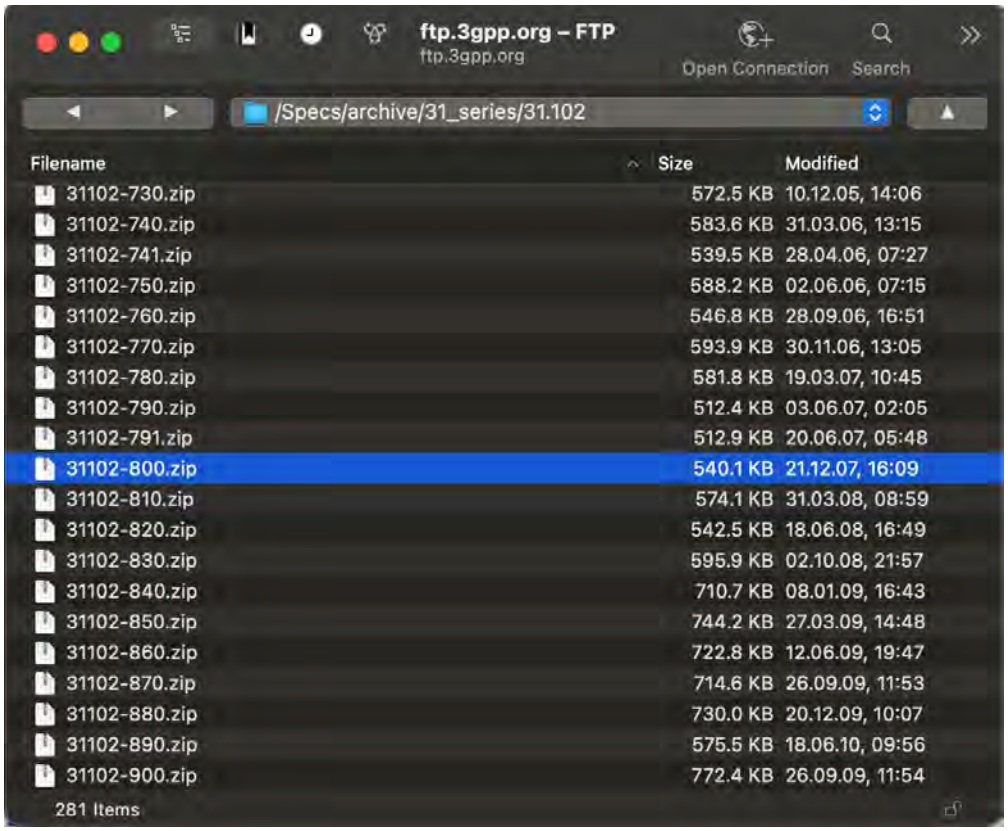
2. Publication by 3GPP and ETSI

83. EX1019 shows on its cover page "2007-12" as the year (2007) and month (December) during which the document was released by 3GPP.

[26] Website available as Appendix T

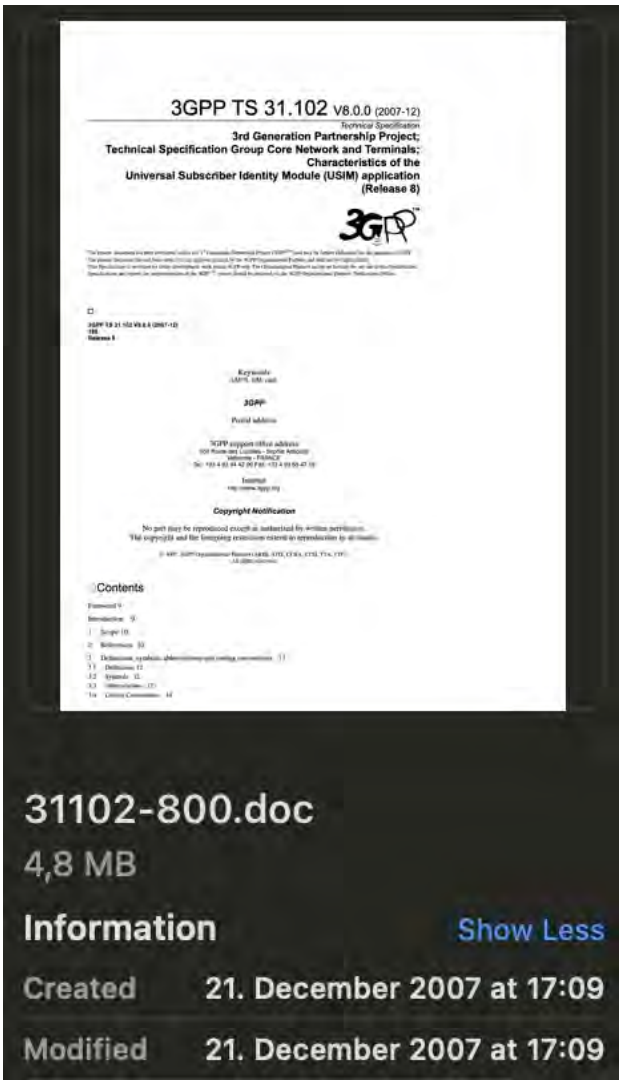
84. EX1019 was uploaded to the 3GPP FTP server on December 21, 2007, based on the upload date stamp shown on the historic 3GPP FTP server for the corresponding downloadable file ("31102-800.zip"), as maintained by the Internet Archive at https://web.archive.org/web/20080108151031/http://www.3gpp.org/ftp/Specs/archive/31_series/31.102/[27]. This information is also shown on the date stamp for the present-day listing of the same document on the 3GPP FTP server at https://www.3gpp.org/ftp/specs/archive/31_series/31.102 as shown in the screenshot below (listing date as "21.12.07", or December 21, 2007):

[27] Website available as Appendix U.



85. Experts in the field of determining the public availability of 3GPP documents would reasonably rely upon the FTP server upload date on the current 3GPP FTP server as well as an archived version of the directory structure maintained by the Internet Archive to establish a date that a 3GPP document became available to the public via the 3GPP FTP server.

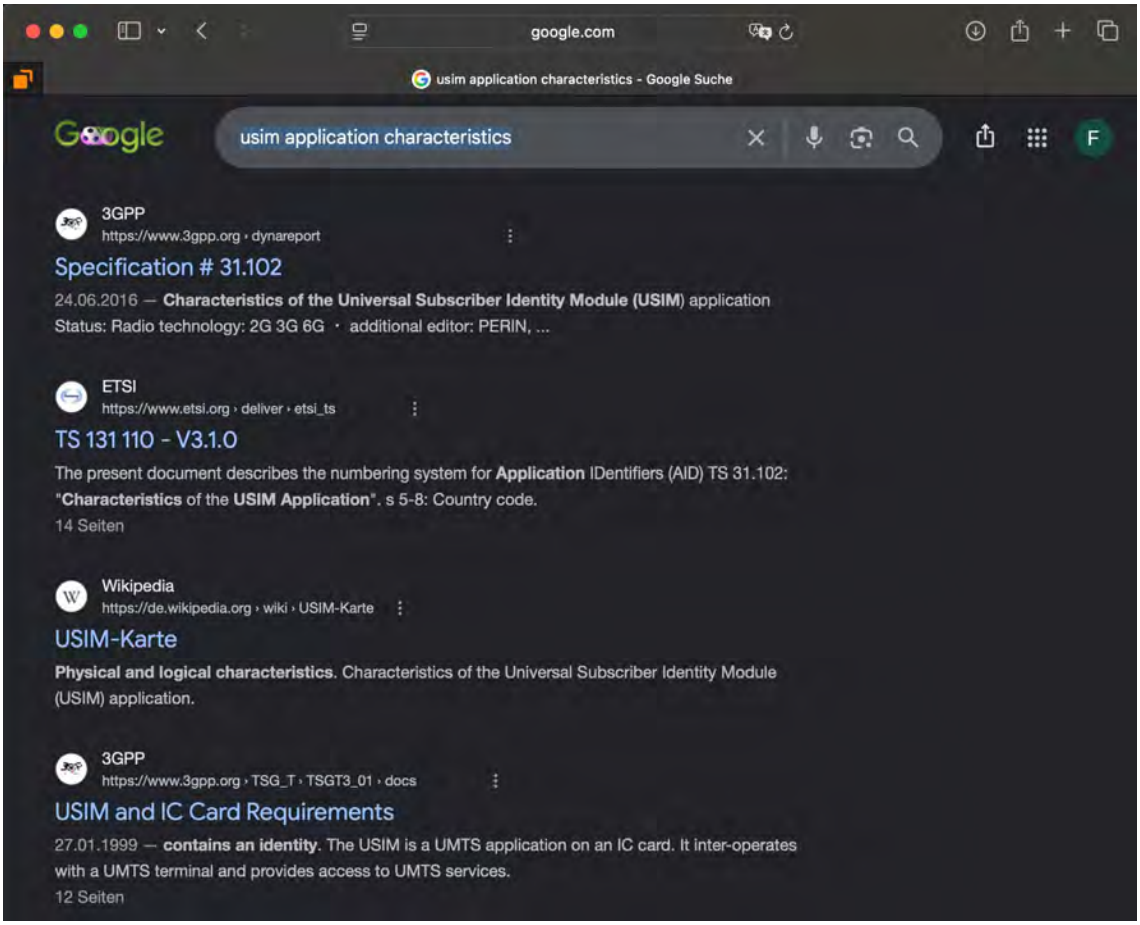
86. In addition, metadata information for the downloaded and extracted TDoc file states a last “Modified” date of “21. December 2007,” as shown in the screenshot below:



87. This last modified date is consistent with the December 21, 2007, upload date of the document and the typical practice among 3GPP staff to upload technical specifications shortly after creating them.

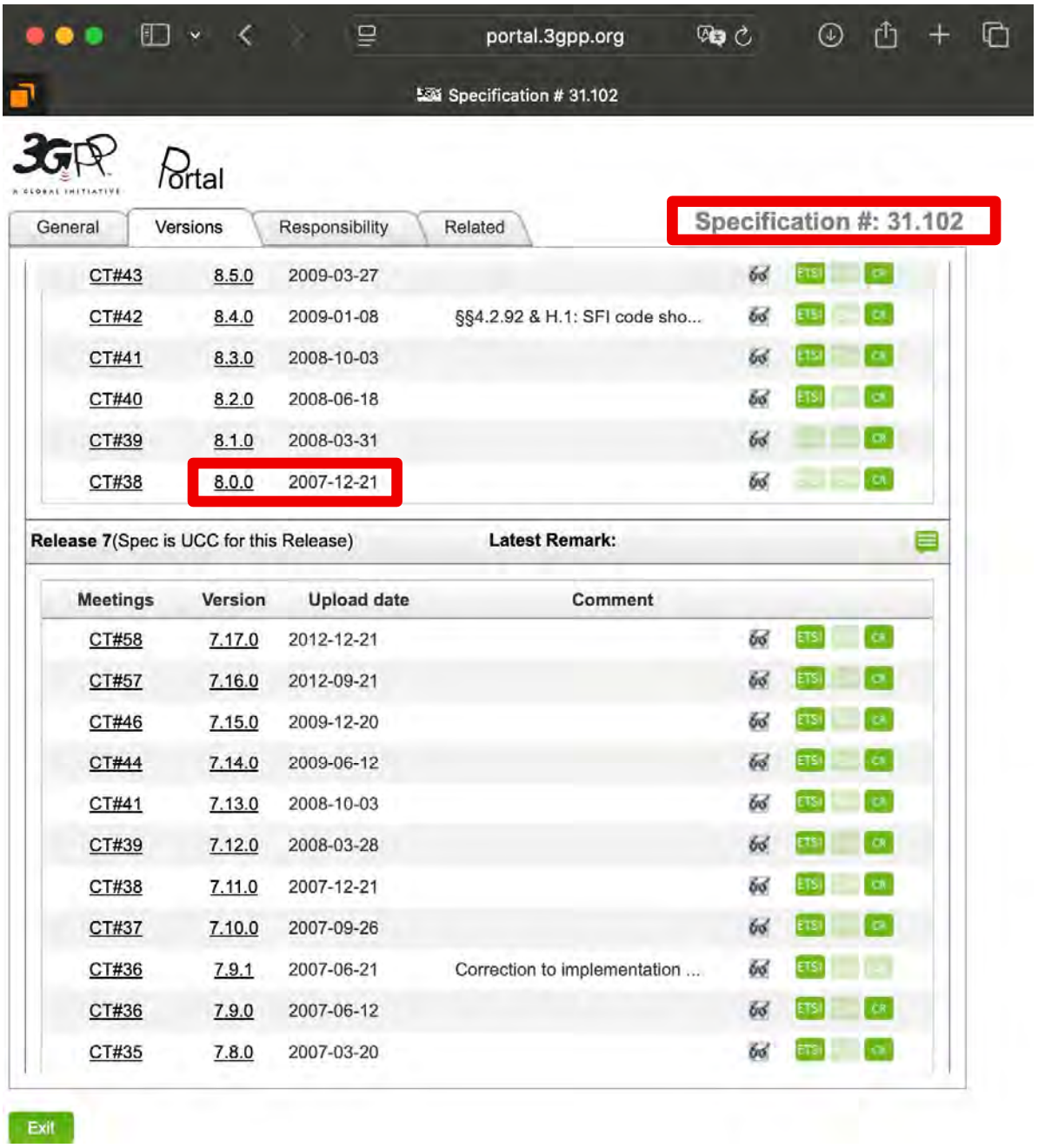
88. I believe that a person without prior knowledge of 3GPP and/or the technical specification (TS) number would have been able to also easily find the TS for download via internet search. For instance, a Google search for “usim

application characteristics" provides the TS number "31.102" as one of the top results as can be seen in the screenshot below:



89. Following the provided search result link "Specification # 31.102 – 3GPP" leads to a 3GPP web page offering under the tab "Versions" download links to all versions of TS 31.102 including version 8.0.0, as shown by the screenshot below[28]:

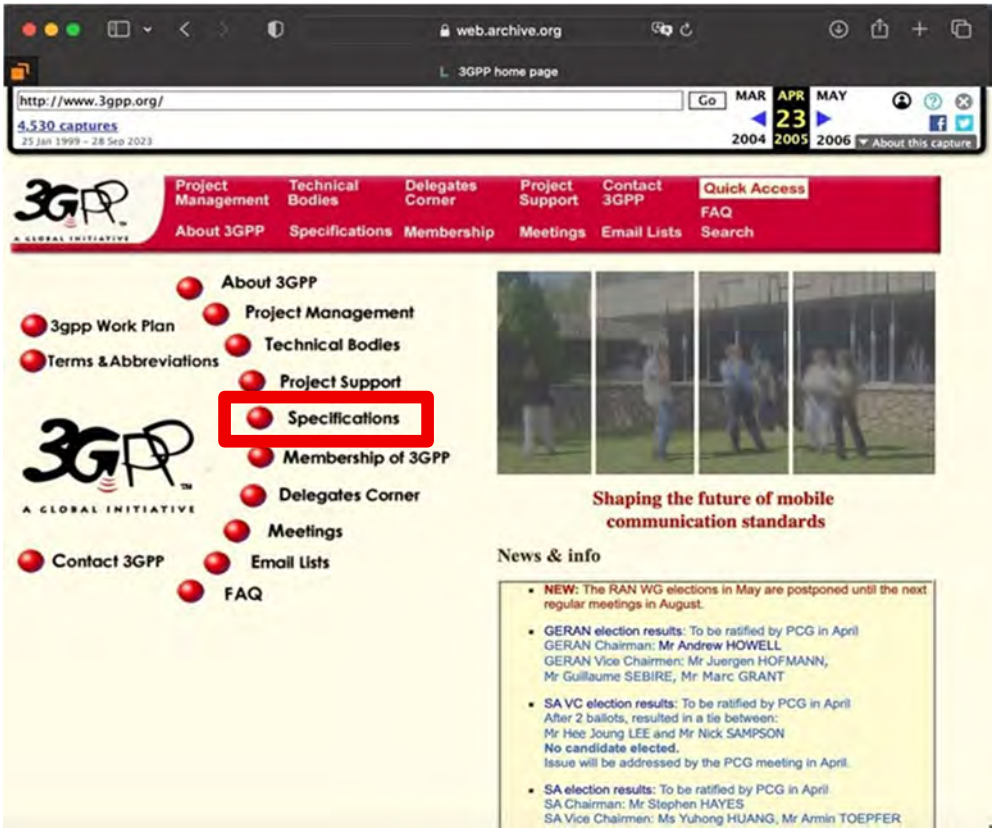
[28] Full website available as Appendix V.



90. The above example search illustrates that it is very easy for an interested member of the public without prior knowledge of the TS number and even without prior knowledge of 3GPP to locate any version of TS 31.102, including version 8.0.0, for download.

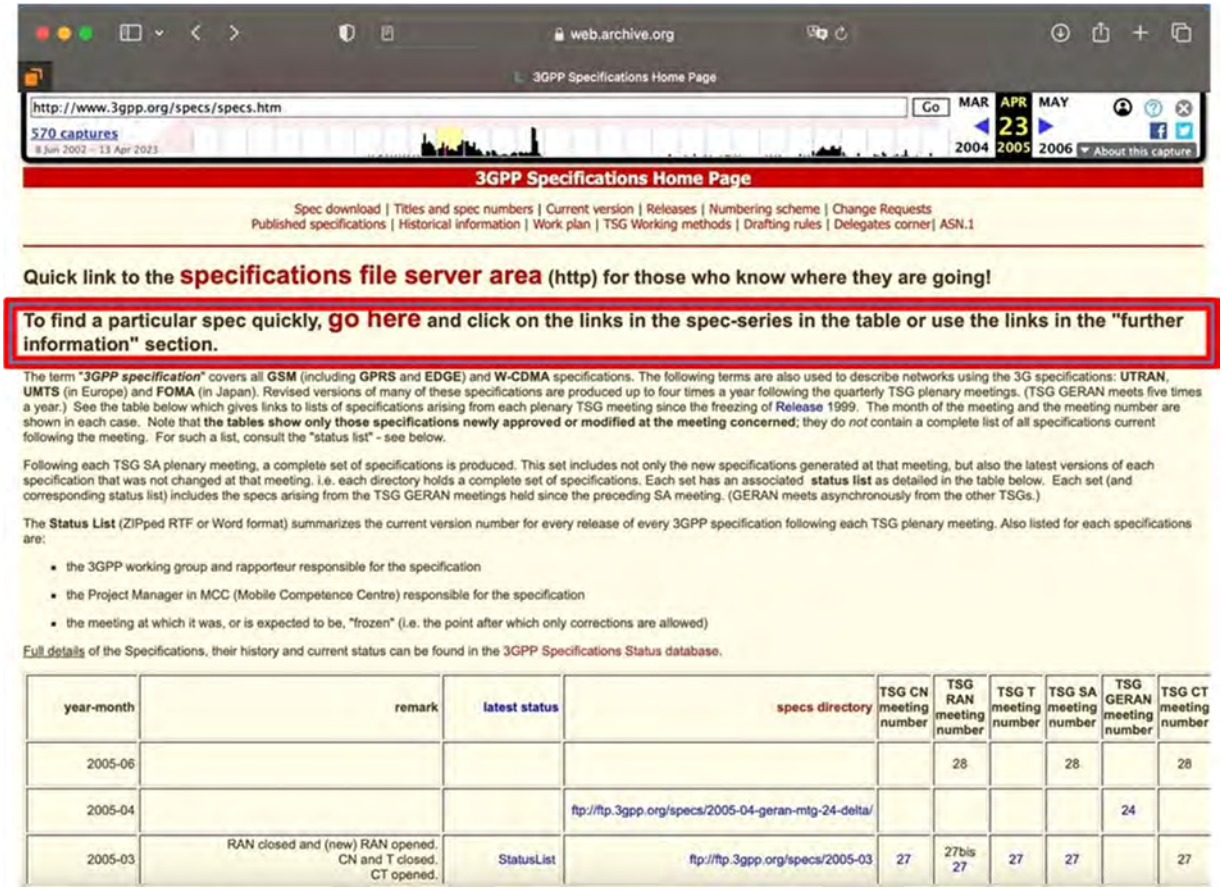
91. The above search was performed at the time of writing this declaration. According to my personal experience, similar searches done in 2007 or around that time would have similarly provided a path to download version 8.0.0 of TS 31.102 although the layout of the webpages was slightly different.

92. A similar search performed in 2007 could have looked like described in the following paragraphs. The 3GPP homepage from 2005 shown below included already a link to "Specifications"[29]:



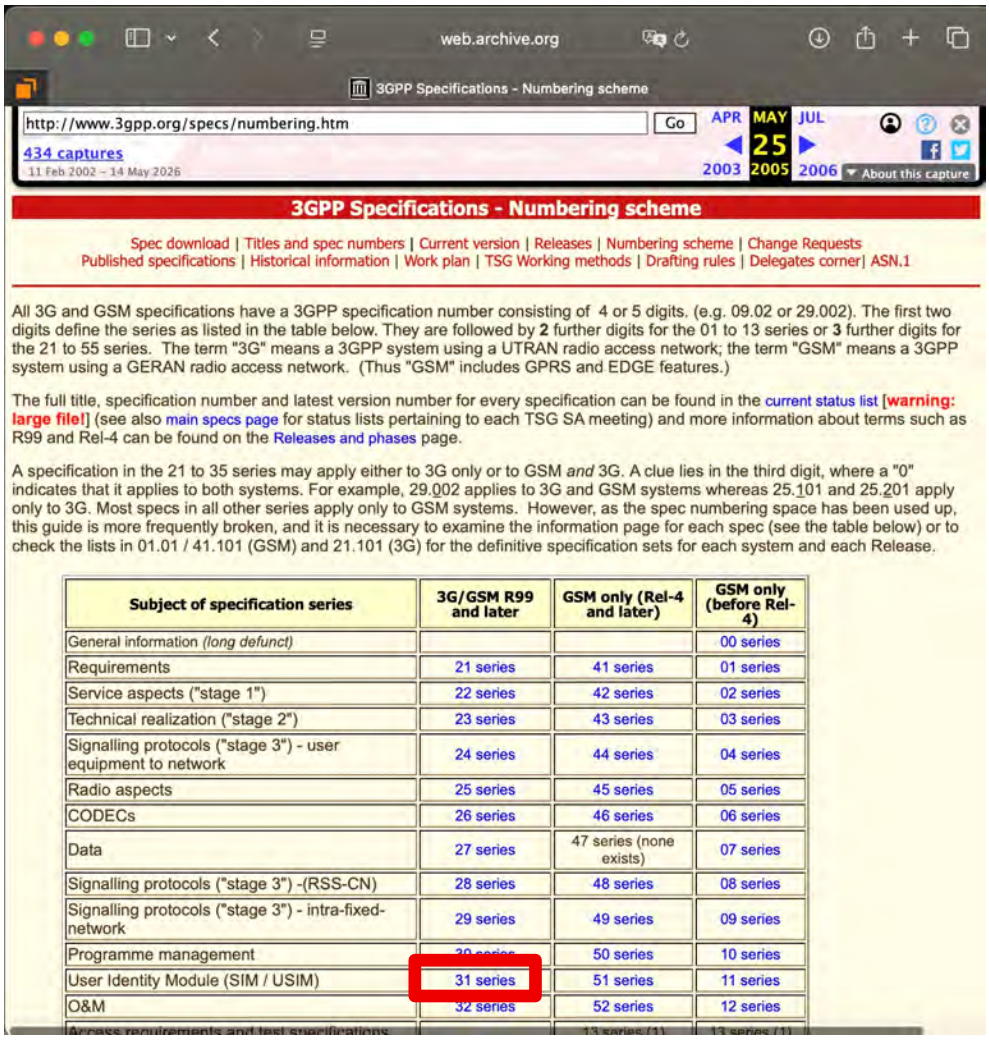
[29] Full website available as Appendix G.

93. Clicking on the "Specifications" link provided a specifications webpage with various paths for locating specific specifications, such as specification snapshots, e.g., "2005-03", a link to the "specifications file server area", or a link to the specifications series page ("To find a particular spec quickly, go here and click on the links in the spec-series in the table or use the links in the 'further information' section."), as shown below[30]:



[30] Full website available as Appendix H.

94. The subjects of the individual specification series for the 3GPP standards were explained on 3GPP's website by clicking on the "To find a particular spec quickly, go here …" link on the specifications webpage identified above. This link directed to the 3GPP specification numbering webpage shown below[31]:



[31] Full website available as Appendix I.

95. Following the link for the 31 series would have led to a 3GPP webpage providing access to all specifications in a series and providing a subject matter index to the list of specifications, as shown by an excerpt of the webpage below[32]:

[32] Full website available as Appendix R.



3GPP Specification series

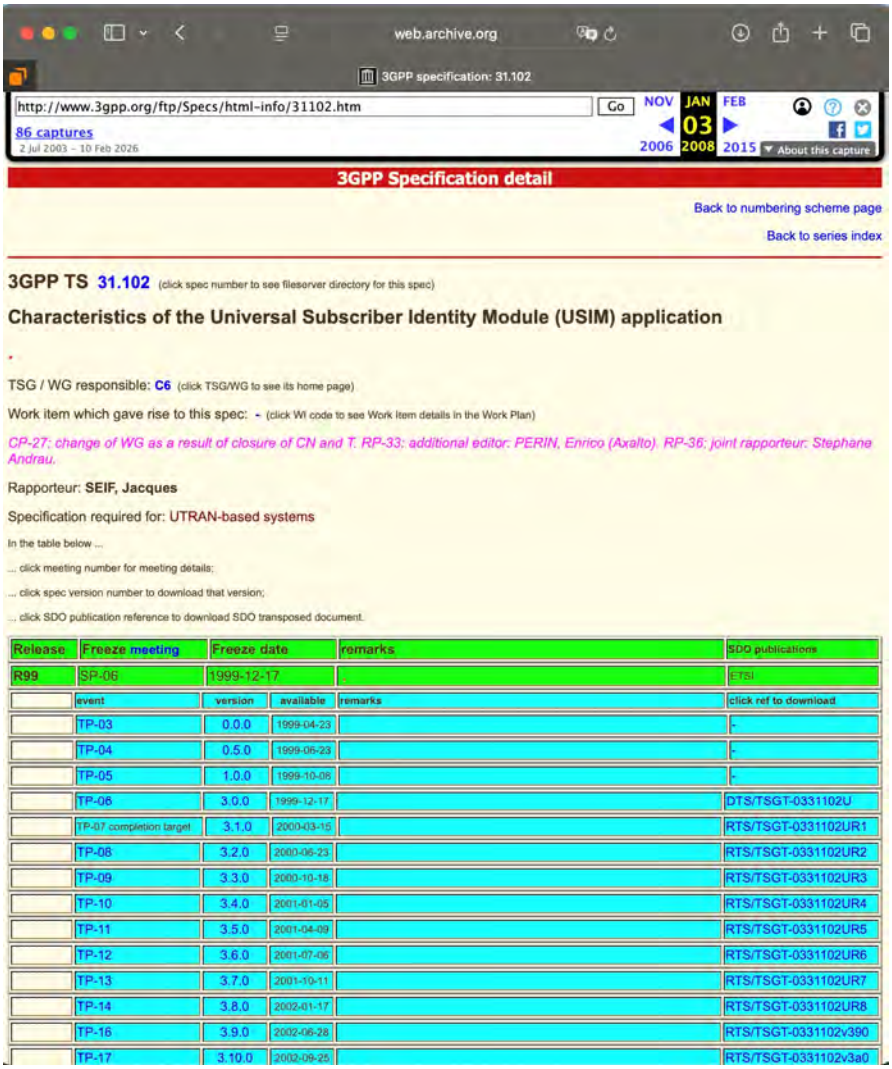
Back to numbering scheme page

Click on spec number for details

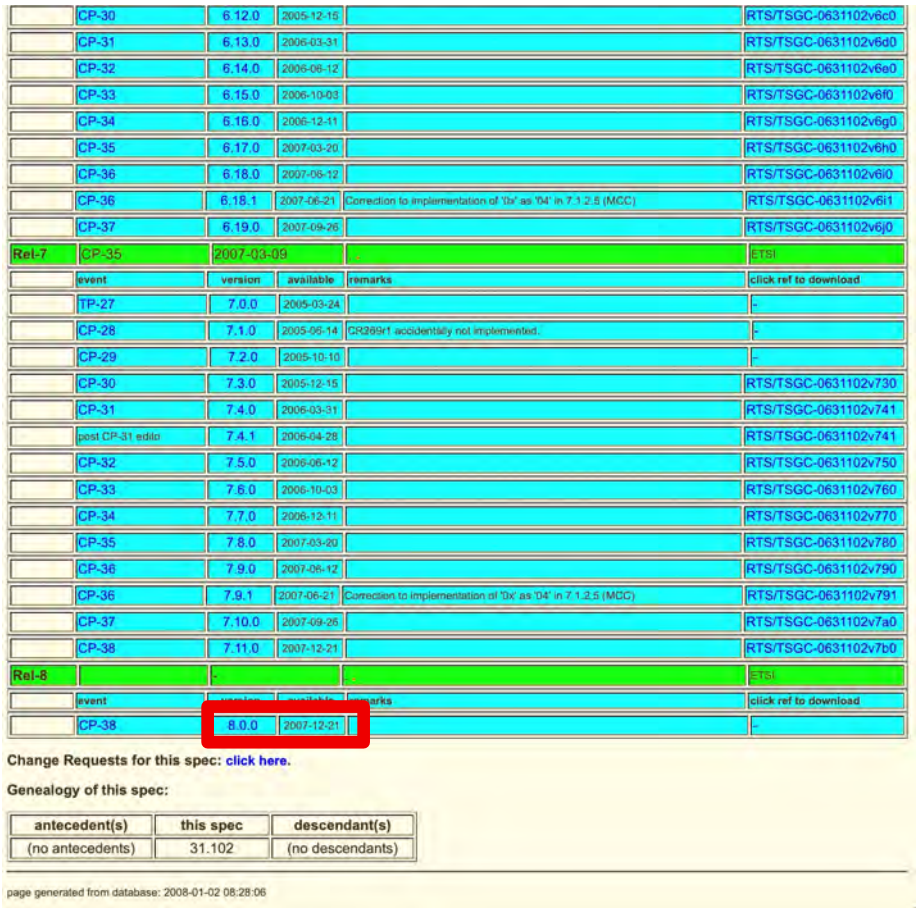
TS 31.048	Security mechanisms for the (U)SIM application toolkit; Test specification	
TS 31.101	UICC-terminal interface; Physical and logical characteristics	
TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application	
TS 31.103	Characteristics of the IP Multimedia Services Identity Module (ISIM) application	
TS 31.110	Numbering system for telecommunication IC card applications	
TS 31.111	Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)	
TS 31.112	Universal Subscriber Identity Module Application Toolkit (USAT) interpreter architecture description; Stage 2	
TS 31.113	Universal Subscriber Identity Module Application Toolkit (USAT) interpreter byte codes	
TS 31.114	Universal Subscriber Identity Module Application Toolkit (USAT) interpreter protocol and administration	
TS 31.115	Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications	
TS 31.116	Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications	
TS 31.120	UICC-terminal interface; Physical, electrical and logical test specification	
TS 31.121	UICC-terminal interface; Universal Subscriber Identity Module (USIM) application test specification	
TS 31.122	Universal Subscriber Identity Module (USIM) conformance test specification	
TS 31.123	(Universal) Subscriber Interface Module ((U)SIM) toolkit interpreter test	SPECIFICATION WITHDRAWN
TS 31.124	Mobile Equipment (ME) conformance test specification; Universal Subscriber Interface Module Application Toolkit (USAT) conformance test specification	
TS 31.130	(U)SIM Application Programming Interface (API); (U)SIM API for Java Card	
TS 31.131	C-language binding for (Universal) Subscriber Identity Module ((U)SIM) API	
TS 31.133	IP Multimedia Services Identity Module (ISIM) Application Programming Interface (API); ISIM API for Java Card™	
TS 31.213	Test specification for subscriber (U)SIM; Application Programming Interface (API) for Java Card™	
TS 31.50U	Essential requirements for UMTS Mobile Stations (ME) operating within frequency bands 1885-1980, 2010-2025 and 2110-2200 MHz	SPECIFICATION WITHDRAWN
TS 31.60U	Essential requirements for UMTS Mobile Earth Stations (MES) operating within frequency bands 1980- 2010 and 2170-2200 MHz	SPECIFICATION WITHDRAWN
TR 31.900	SIM/USIM internal and external interworking aspects	
TR 31.919	2G/3G Java Card™ Application Programming Interface (API) based applet interworking	

page generated from database: 2007-08-23 08:41:07

96. Following the link for TS 31.102 would have led to a 3GPP webpage providing access to all versions of TS 31.102 including V8.0.0 for download, as shown by annotated excerpts of the webpage below[33]:



[33] Full website available as Appendix W.



	CP-30	6.12.0	2005-12-15		RTS/TSGC-0631102v6c0
	CP-31	6.13.0	2006-03-31		RTS/TSGC-0631102v6d0
	CP-32	6.14.0	2006-06-12		RTS/TSGC-0631102v6e0
	CP-33	6.15.0	2006-10-03		RTS/TSGC-0631102v6f0
	CP-34	6.16.0	2006-12-11		RTS/TSGC-0631102v6g0
	CP-35	6.17.0	2007-03-20		RTS/TSGC-0631102v6h0
	CP-36	6.18.0	2007-06-12		RTS/TSGC-0631102v6i0
	CP-36	6.18.1	2007-06-21	Correction to implementation of '0x' as '04' in 7.1.2.6 (MCC)	RTS/TSGC-0631102v6i1
	CP-37	6.19.0	2007-09-26		RTS/TSGC-0631102v6j0
Rel-7	CP-35	2007-03-09	-		ETSI
	event	version	available	remarks	click ref to download
	TP-27	7.0.0	2005-03-24		-
	CP-28	7.1.0	2005-06-14	CR289r1 accidentally not implemented.	-
	CP-29	7.2.0	2005-10-10		-
	CP-30	7.3.0	2005-12-15		RTS/TSGC-0631102v730
	CP-31	7.4.0	2006-03-31		RTS/TSGC-0631102v741
	post CP-31 editd	7.4.1	2006-04-28		RTS/TSGC-0631102v741
	CP-32	7.5.0	2006-06-12		RTS/TSGC-0631102v750
	CP-33	7.6.0	2006-10-03		RTS/TSGC-0631102v760
	CP-34	7.7.0	2006-12-11		RTS/TSGC-0631102v770
	CP-35	7.8.0	2007-03-20		RTS/TSGC-0631102v780
	CP-36	7.9.0	2007-06-12		RTS/TSGC-0631102v790
	CP-36	7.9.1	2007-06-21	Correction to implementation of '0x' as '04' in 7.1.2.6 (MCC)	RTS/TSGC-0631102v791
	CP-37	7.10.0	2007-09-26		RTS/TSGC-0631102v7a0
	CP-38	7.11.0	2007-12-21		RTS/TSGC-0631102v7b0
Rel-8		-	-		ETSI
	event	[illegible]	[illegible]	[illegible]marks	click ref to download
	CP-38	8.0.0	2007-12-21		-

Change Requests for this spec: click here.

Genealogy of this spec:

antecedent(s)	this spec	descendant(s)
(no antecedents)	31.102	(no descendants)

page generated from database: 2008-01-02 08:28:06

97. In summary, there are - and there were in 2007 - several paths to locate and download a specific 3GPP specification. Thus, it is - and was already in 2007 - straightforward for any interested person including members of the public to access 3GPP specifications such as TS 31.102 V8.0.0.

3. Conclusion

98. Thus, based on my personal knowledge and experience with ETSI's and 3GPP's standard business practices, this information tells me that EX1019 (3GPP TS 31.102 Version 8.0.0) was uploaded and made available via the 3GPP FTP server to 3GPP delegates and interested members of the public who would have been able to locate the reference exercising reasonable diligence by December 21, 2007.

E. 3GPP TS 51.011 V4.10.0 (EX1020)

1. Authentication

99. EX1020 is a true and correct copy of 3GPP TS 51.011 V4.10.0, titled "Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface (Release 4)". I obtained EX1018 from 3GPP's FTP server at the following location: https://www.3gpp.org/ftp/specs/archive/51_series/51.011[34]

2. Publication by 3GPP and ETSI

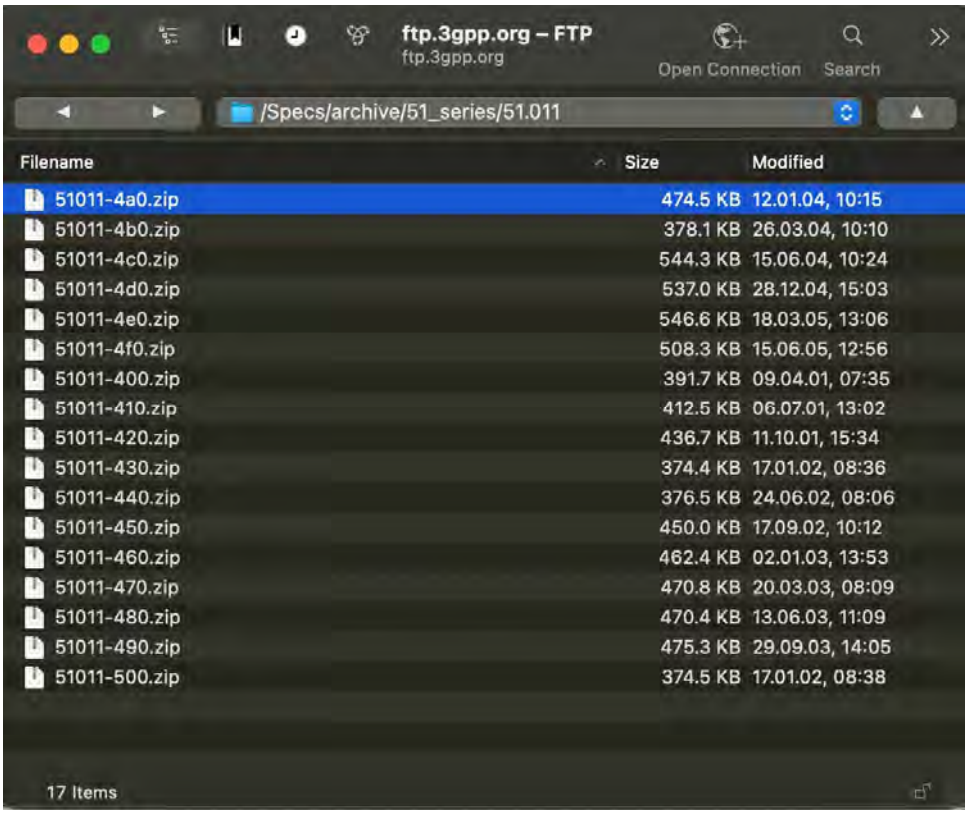
100. EX1020 shows on its cover page "2003-12" as the year (2003) and month (December) during which the document was released by 3GPP. TS 51.011

[34] Website available as Appendix E

V4.10.0 was released by the 3GPP TSG-T #22 meeting held December 10-12, 2003, in Maui, US, which I personally attended.

101. EX1020 was uploaded to the 3GPP FTP server on January 12, 2004, based on the upload date stamp shown on the historic 3GPP FTP server for the corresponding downloadable file ("51011-4a0.zip"), as maintained by the Internet Archive at https://web.archive.org/web/20040516210013/http://www.3gpp.org/ftp/specs/archive/51_series/51.011/[35]. This information is also shown on the date stamp for the present-day listing of the same document on the 3GPP FTP server at https://www.3gpp.org/ftp/specs/archive/51_series/51.011 as shown in the screenshot below (listing date as "12.01.04", or January 12, 2004):

[35] Website available as Appendix L.



102. Experts in the field of determining the public availability of 3GPP documents would reasonably rely upon the FTP server upload date on the current 3GPP FTP server as well as an archived version of the directory structure maintained by the Internet Archive to establish a date that a 3GPP document became available to the public via the 3GPP FTP server.

103. In addition, metadata information for the downloaded and extracted TDoc file states a last “Modified” date of “12. January 2004,” as shown in the screenshot below:



104. This last modified date is consistent with the upload date of the document and the typical practice among 3GPP staff to upload technical specifications shortly after creating them.

105. This publication date is further confirmed by the publication history of the ETSI copy of TS 51.011 named “ETSI TS 151 011,” which states that V4.10.0

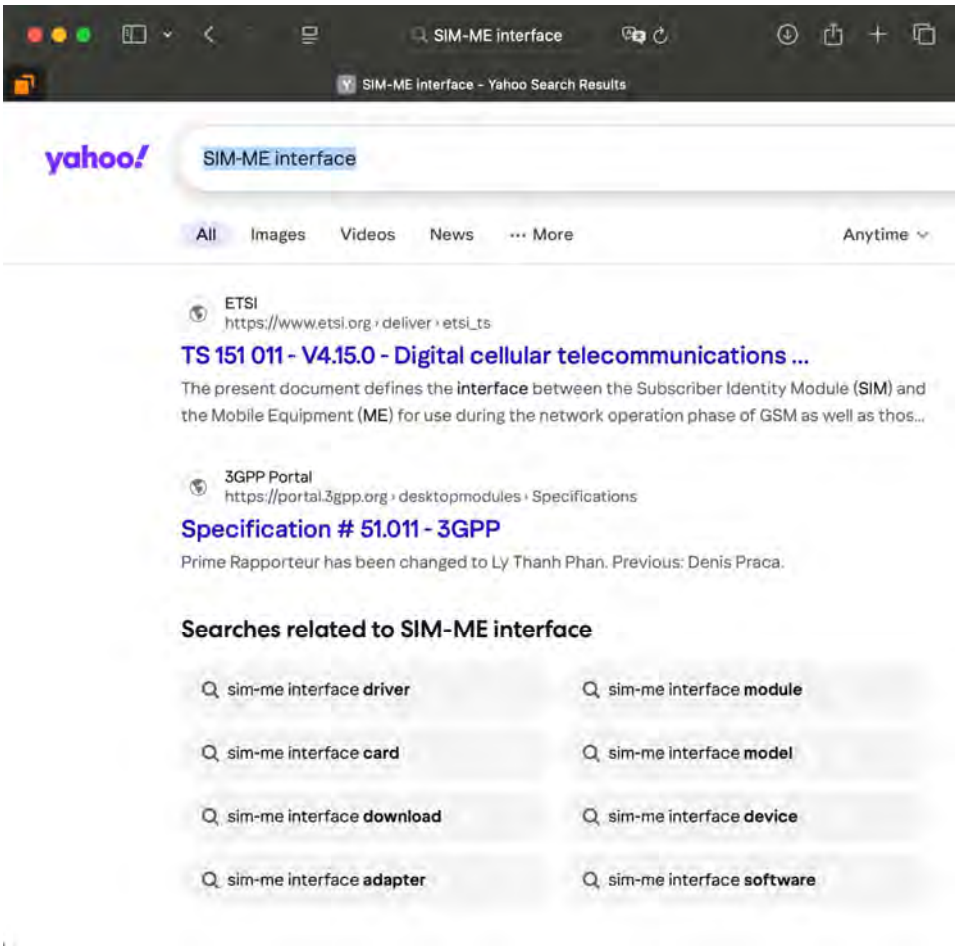
was published in December 2003.[36] December 2003 reflects the month the document was released by 3GPP and the upload to the ETSI website took place on January 19, 2004.[37] This is one week after the upload to the 3GPP FTP server as it is common practice that the ETSI versions of 3GPP specifications are uploaded a few weeks after the 3GPP specifications are uploaded.

106. I believe that a person without prior knowledge of 3GPP and/or the technical specification (TS) number would have been able to also easily find the TS for download via internet search. For instance, a Yahoo search for "SIM-ME interface" provides the TS number "51.011" as one of the top results as can be seen in the screenshot below:

---

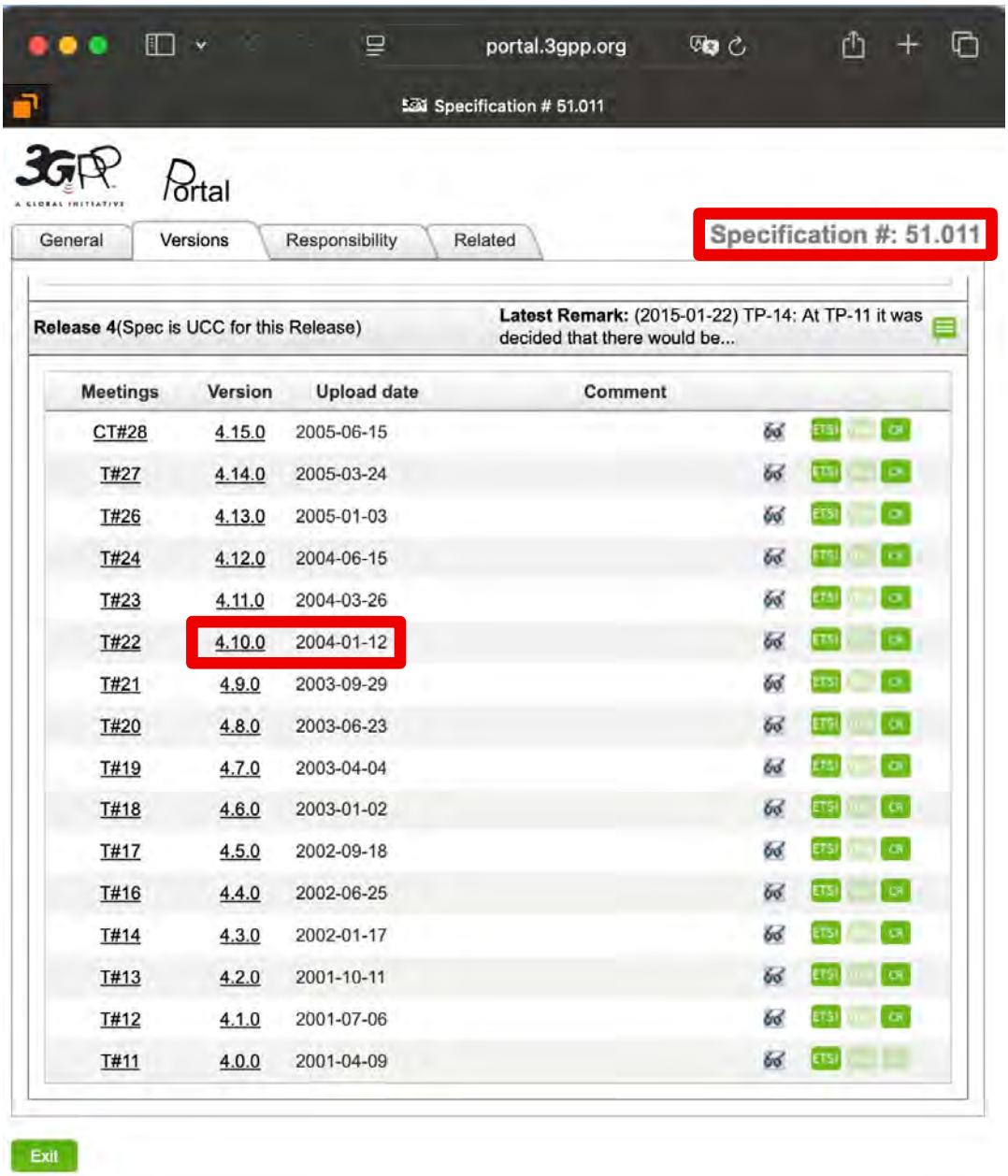
36 https://www.etsi.org/deliver/etsi_ts/151000_151099/151011/04.10.00_60/ts_151011v041000p.pdf (Appendix M)

37 https://www.etsi.org/deliver/etsi_ts/151000_151099/151011/04.10.00_60/



107. Following the provided search result link “Specification # 51.011 – 3GPP” leads to a 3GPP web page offering under the tab “Versions” download links to all versions of TS 51.011 including version 4.10.0, as shown by the screenshot below[38]:

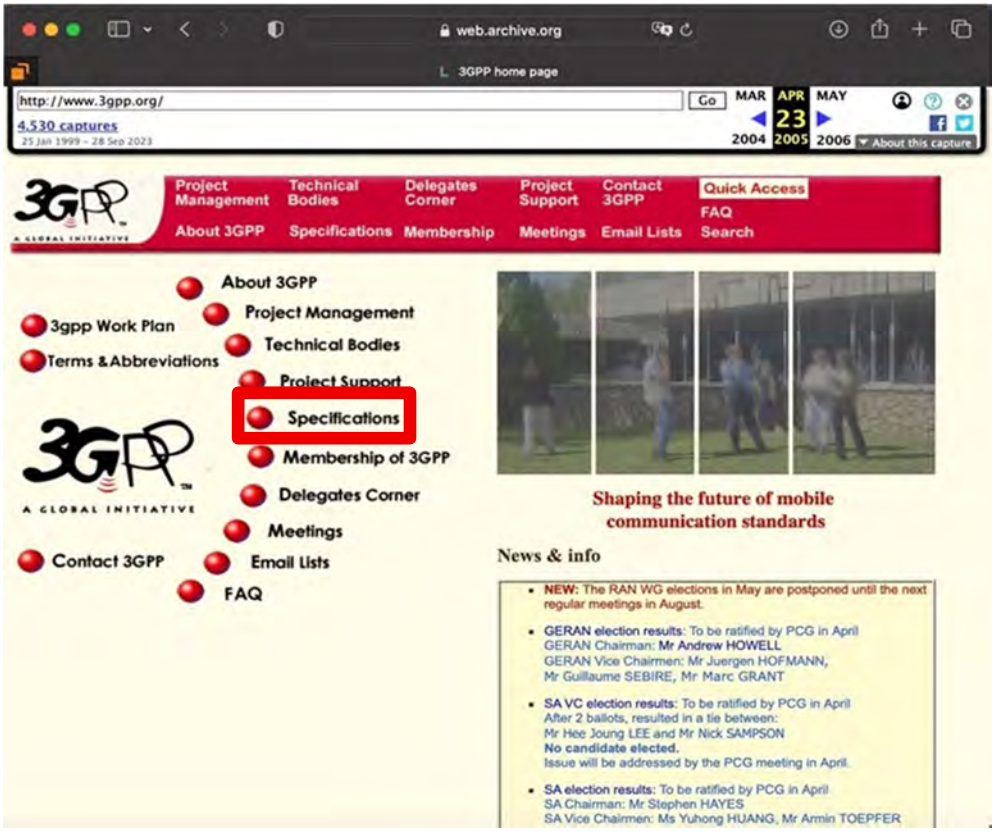
[38] Full website available as Appendix F.



108. The above example search illustrates that it is very easy for an interested member of the public without prior knowledge of the TS number and even without prior knowledge of 3GPP to locate any version of TS 51.011, including version 4.10.0, for download.

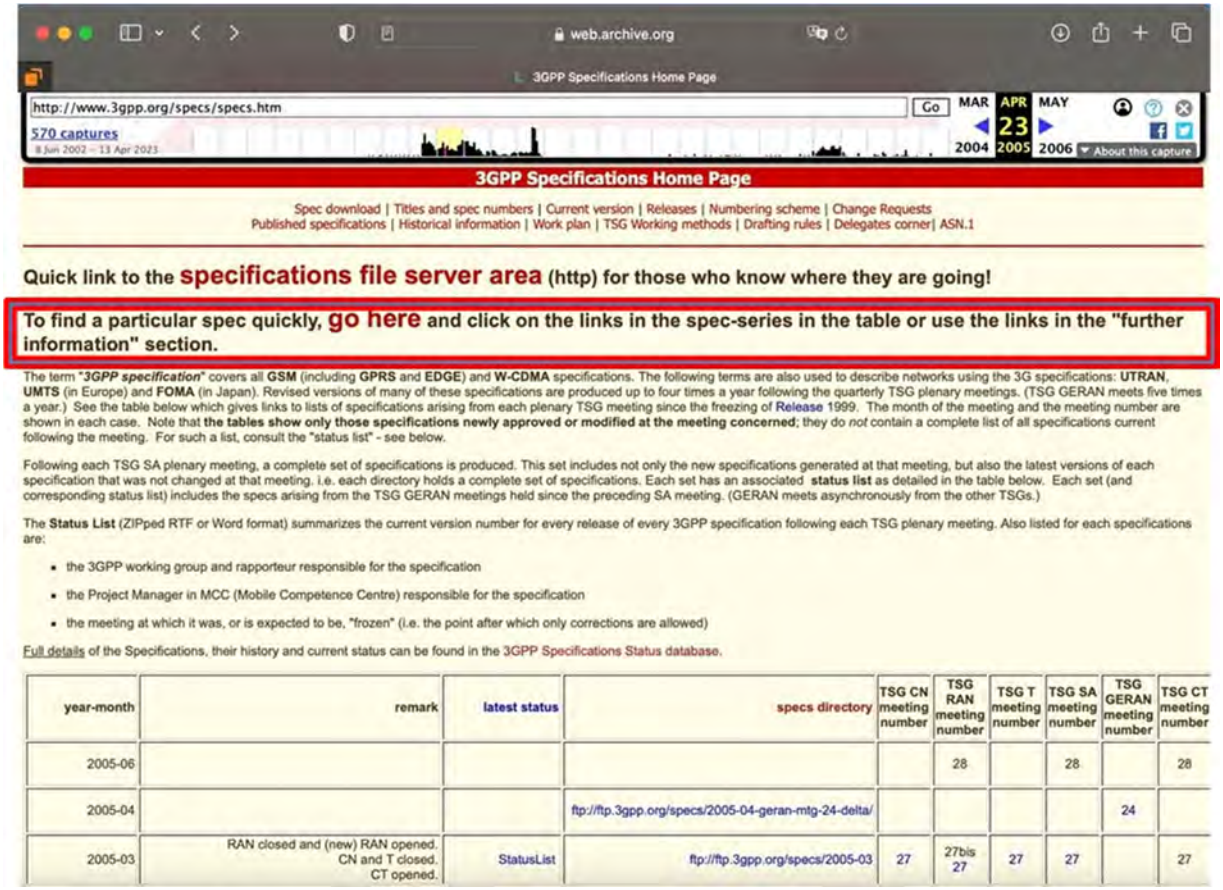
109. The above search was performed at the time of writing this declaration. According to my personal experience, similar searches done in 2005 or around that time would have similarly provided a path to download version 4.10.0 of TS 51.011 although the layout of the webpages was slightly different.

110. A similar search performed in 2005 could have looked like described in the following paragraphs. The 3GPP homepage from 2005 shown below included a link to "Specifications"[39]:



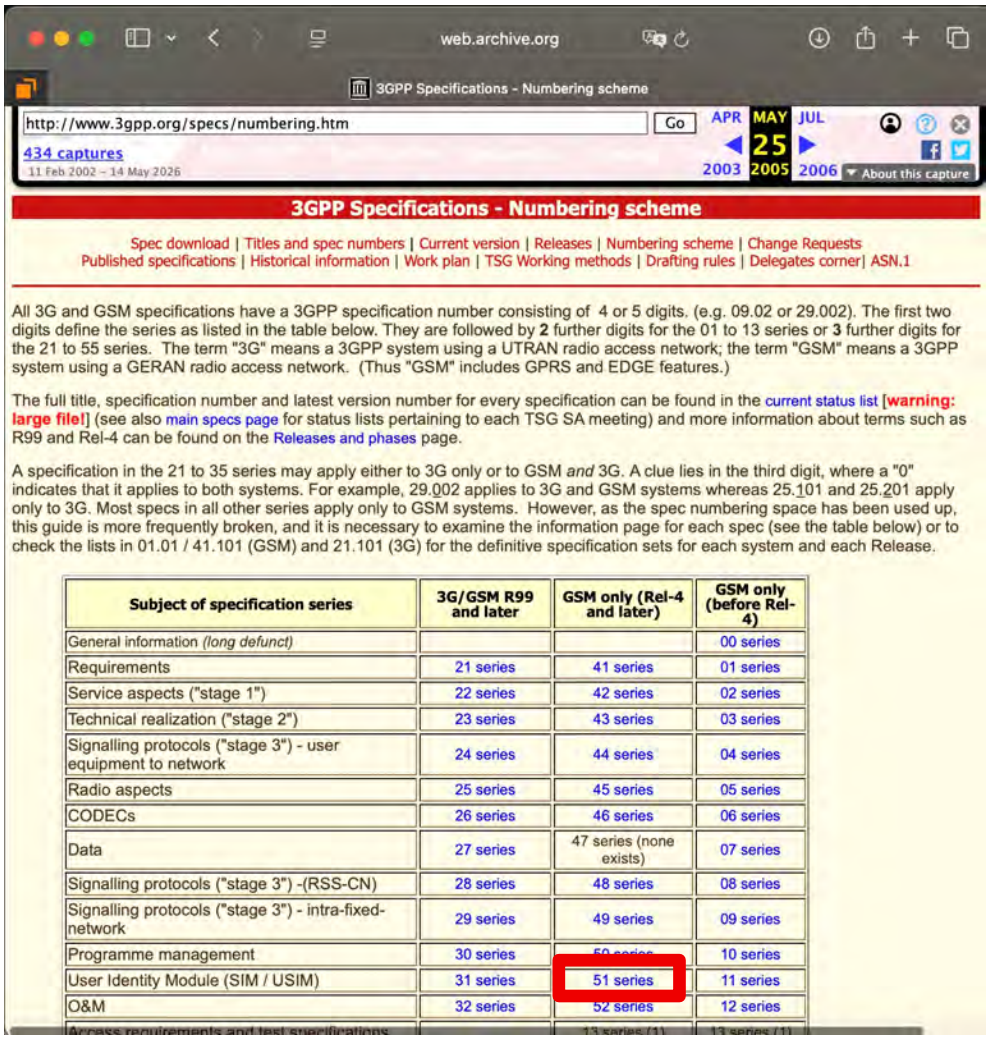
[39] Full website available as Appendix G.

111. Clicking on the "Specifications" link provided a specifications webpage with various paths for locating specific specifications, such as specification snapshots, e.g., "2005-03", a link to the "specifications file server area", or a link to the specifications series page ("To find a particular spec quickly, go here and click on the links in the spec-series in the table or use the links in the 'further information' section."), as shown below[40]:



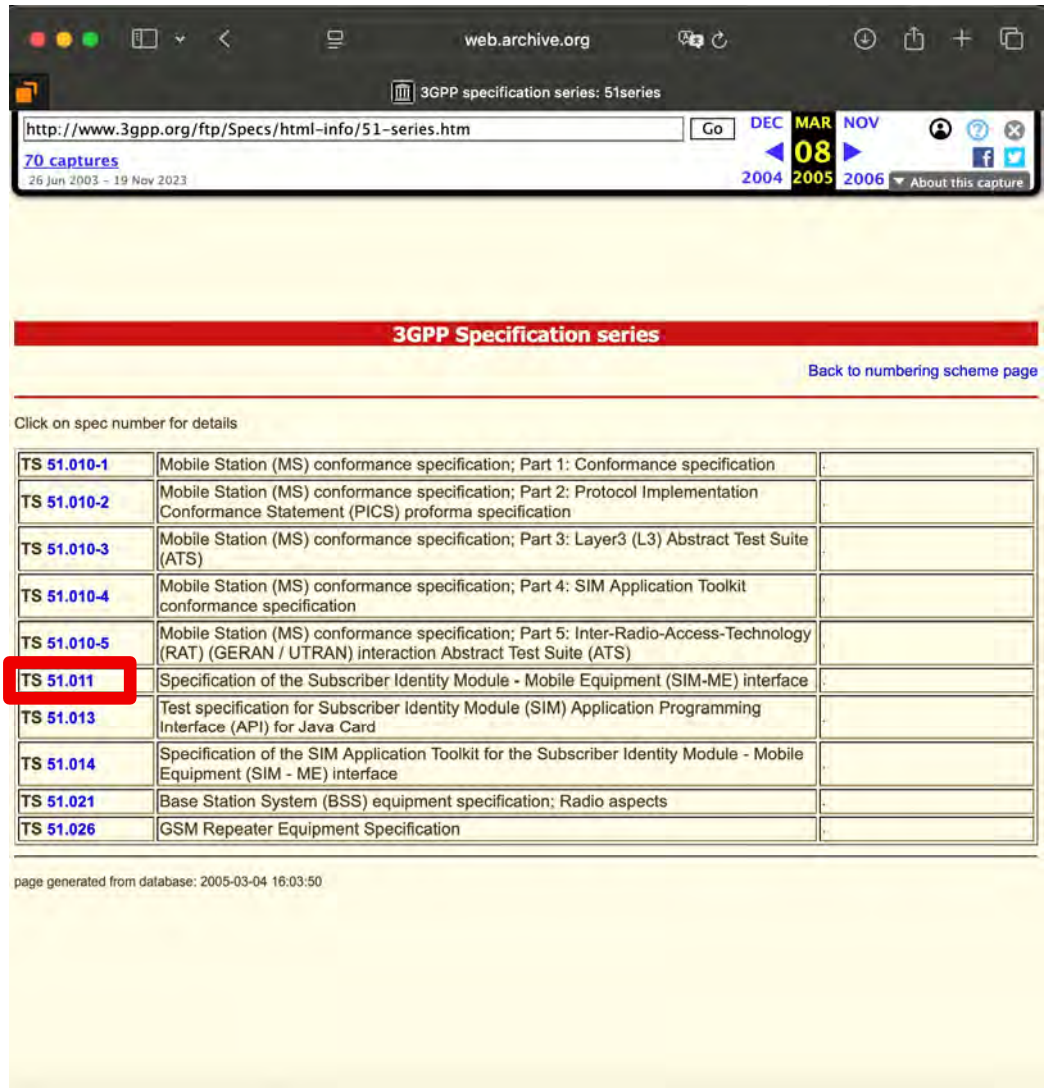
[40] Full website available as Appendix H.

112. The subjects of the individual specification series for the 3GPP standards were explained on 3GPP's website by clicking on the "To find a particular spec quickly, go here …" link on the specifications webpage identified above. This link directed to the 3GPP specification numbering webpage shown below[41]:



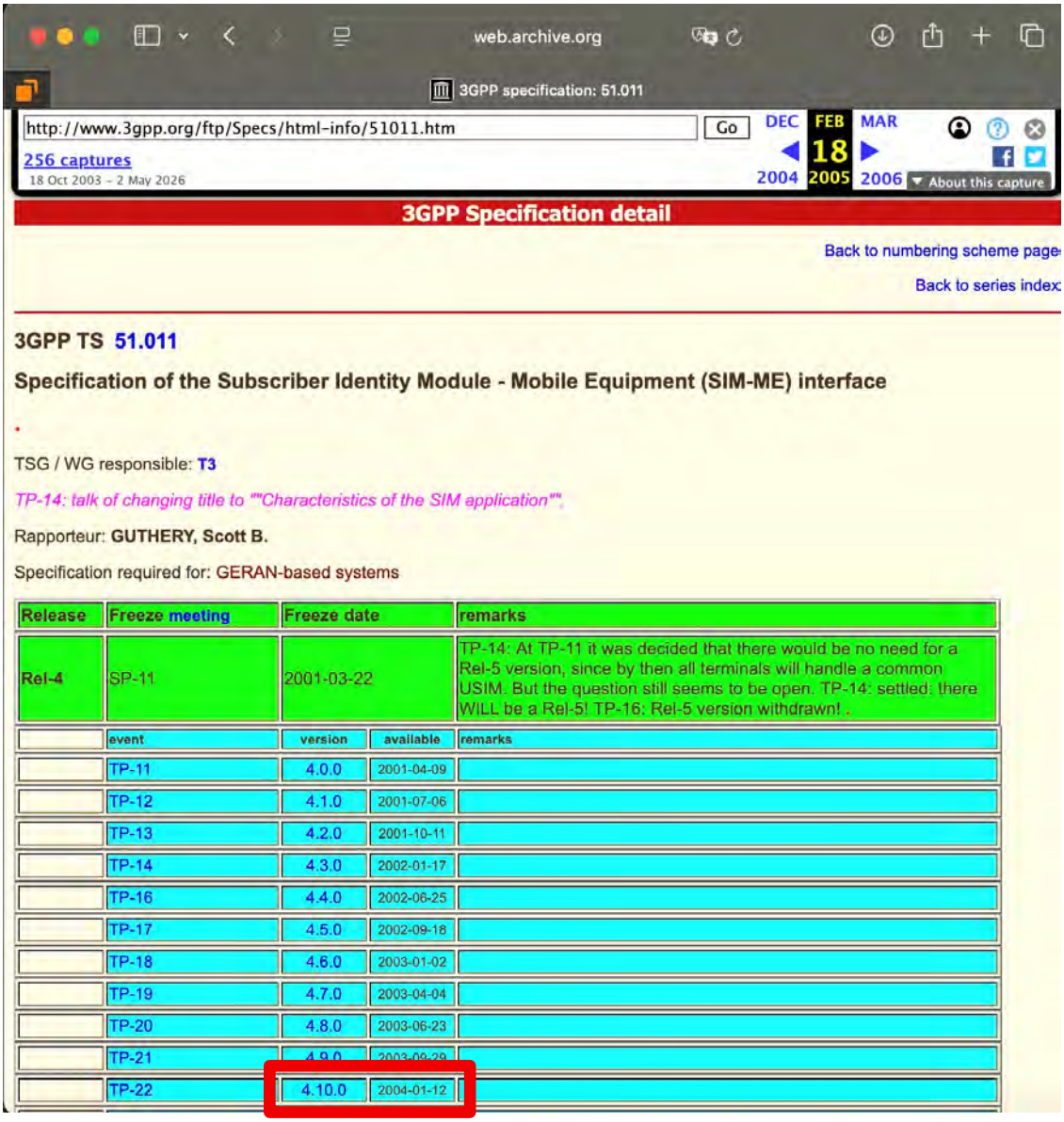
[41] Full website available as Appendix I.

113. Following the link for the 51 series would have led to a 3GPP webpage providing access to all specifications in a series and providing a subject matter index to the list of specifications, as shown by an excerpt of the webpage below[42]:



[42] Full website available as Appendix J.

114. Following the link for TS 51.011 would have led to a 3GPP webpage providing access to all versions of TS 51.011 including V4.10.0 for download, as shown by annotated excerpts of the webpage below[43]:



[43] Full website available as Appendix K.

115. In summary, there are - and there were in 2005 - several paths to locate and download a specific 3GPP specification. Thus, it is - and was already in 2005 - straightforward for any interested person including members of the public to access 3GPP specifications such as TS 51.011 V4.10.0.

3. Conclusion

116. Thus, based on my personal knowledge and experience with ETSI's and 3GPP's standard business practices, this information tells me that EX1020 (3GPP TS 51.011 Version 4.10.0) was uploaded and made available via the 3GPP FTP server to 3GPP delegates and interested members of the public who would have been able to locate the reference exercising reasonable diligence by January 12, 2004.

V. CONCLUSION

117. In signing this Declaration, I recognize that the Declaration will be filed as evidence in a case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that, if required, I will make myself available for cross-examination to take place within the United States, during the time allotted for cross-examination.

118. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: August 11, 2026



Friedhelm Rodermund

APPENDIX A

CURRICULUM VITAE

I. PERSONAL DATA

Name: **Friedhelm RODERMUND**

Mailing address: Am Steiner Graben 18
56077 Koblenz, Germany

Phone: +49 172 2606489

Email: fred@iotecc.com

II. PROFESSIONAL EXPERIENCE

Summary

Senior expert in telecommunications, Internet of Things (IoT) technology and related standard essential patents (SEPs). More than 30 years of experience within the mobile communications industry, and several years in the IoT domain in various roles such as project management, technology innovation and evolution, standards development, technology strategy, patent creation and patent litigations, and development/introduction of new services.

Recognized standards expert who was actively involved in leading roles in the development of key standards for mobile telephony/data and service anablers across standards development organizations such as 3GPP, ETSI, GSMA, IETF, OMA, and oneM2M. Currently focussing on standards for the Internet of Things including ETSI and 3GPP standards such as 5G and 6G, and OMA Lightweight M2M (LwM2M).

Founder and director of IOTECC GmbH which provides consulting services around technologies and standards enabling the Internet of Things, and consulting and expert services related to patents for mobile telcommunications and IoT.

01/2015 – present **IOTECC GmbH** **Koblenz, Germany**

Founder and CEO

- Mobile telecommunications, Internet of Things (IoT) technology and standards consulting
- Telecommunications and IoT patent consulting
  - Consulting services around telecommunications and IoT patents in particular related to 3GPP, ETSI and OMA standards
  - State of the art/prior art research services related to patent filing e.g. for 5G and 6G
  - Prior art research, essentiality assessment, patent infringement analysis related to litigations and validity actions
  - Advising on IP strategy
  - Advising on Standards Development Organisations (SDO) e.g. ETSI and 3GPP working processes and IPR policy
  - Conducting seminar on Standards Essential Patents (SEPs) for the Internet of Things at the Technical University of Ilmenau, Germany
  - Experienced expert witness (please see section III for a list of supported actions)

11/2014 – 12/2014 **Friedhelm Rodermund Consulting** **Koblenz, Germany**

Internet of Things (IoT) Consultant

- IoT standards development and introduction of new IoT services

01/2011 – 10/2014 **Vodafone Germany / Vodafone Group R&D** **Düsseldorf, Germany**

Senior Standards Strategist
- Representing Vodafone in various standardisation bodies
- Creating technical standards for the Internet of Things
- Work item lead, technical editor and key contributor of Open Mobile Alliance (OMA) "Lightweight M2M (LwM2M)" – the new standard for the Internet of Things
- Advising and supporting various IoT/M2M projects related to e.g. smart metering
- Advising on the introduction of new IoT/M2M technologies and services
- Leading Proof of Concepts of emerging technologies
- Involved in innovation projects
- Supporting the creation and protection of Intellectual Property

01/2009 – 12/2010 **Vodafone Germany** **Düsseldorf, Germany**

Vice Chairman Open Mobile Alliance (OMA) Device Management (DM)
- Responsible for Vodafone's Device Management standardisation
- As OMA DM Vice Chairman, co-leading the group, chairing committee meetings and web conferences, steering the technical direction, management of the different work items
- Editor of several specifications, rapporteur of various work items
- Support of projects for the introduction of device management
- Delegate to 3GPP SA1 with responsiblity for the introduction of MTC (machine type communications) related service/network requirements

01/2005 – 12/2008 **Vodafone Germany** **Düsseldorf, Germany**

Project Manager Mobile Broadcast Standards
- Responsible for Mobile Broadcast standardisation across different broadcast systems/standards bodies and across all Vodafone local operations
- Responsible for Mobile Broadcast standardisation strategy development and implementation
- Delegation Lead for the Open Mobile Alliance (OMA) BCAST working group
- Initiated and managed the BCAST device profile development in the BMCO Forum
- Leading the "Service Protection" (pay-TV) stream of the German DVB-H Consortium
- Filed several patents
- Supporting patent litigations and patent portfolio evaluation (various technical areas)

04/2003 – 12/2003 **GSM Association** **London, United Kingdom**

Member of the MMS Task Force
- Verification of the MMS operator interworking framework
- Supporting the definition and specification of the MMS functional evolution
- Acting as a "link" between 3GPP and GSMA in the area of MMS

06/1998 – 12/2004 **European Telecommunications Standards Institute (ETSI)**
Sophia Antipolis, France

01/2002 – 12/2004: Secretary 3GPP Technical Specifications Group *"Terminals"* and Terminals Working Group 2 *"Terminal Services and Capabilities"*

01/1999 – 12/2001: Secretary 3GPP Terminals Working Group 2 *"Terminal Services and Capabilities"* and GERAN 3 *"Base Station Testing"*

06/1998 – 03/1999: Secretary ETSI SMG4 *"Data Services"* and SMG8 *"Base Station Testing"*

- Supported the establishment of 3GPP (3rd Generation Partnership Project) as the leading standards organization for mobile telecommunications
- Project manager and secretary of TSG "Terminals" reponsbile for Terminal Conformance Testing, Terminal Services and Capabilities, Universal Subscriber Identity Module (USIM)
- Project manager and secretary of Terminals Working Group 2 "Terminal Services and Capabilities" that was responsible for Terminal Execution Environments, Messaging including Short Message Service (SMS), Cell Broadcast Service (CBS), Enhanced Messaging Service (EMS), Multimedia Messaging Service (MMS), Terminal Interfaces incl. AT-commands, Generic User Profile, Data Synchronization and others
- Establishment and management of the Work Plan and follow-up and report on the progress of the related work items
- Advising the chairmen and the standards groups on technical, procedural and political issues
- Editorship of various GSM and UMTS technical specifications
- Responsible for presenting the technical results of the working groups to the parent body
- Responsible for the communication with other standards bodies inside and outside 3GPP
- PR activities (articles, interviews)

12/1993 – 06/1998 Mannesmann Mobilfunk GmbH Düsseldorf, Germany

System Engineer and Project Manager in Quality Assurance and Technical Standards

- Leadership and management of acceptance test projects in the area of GSM Base Station Controller (BSC) and GSM Base Station (BTS) hardware and software.
- Leading project teams of around 15 people
- Responsible for the clearance of releasing new software/hardware into the network
- Supported Request for Quotations, supplier evaluation and pre-selection, project manager of System Verification as a central part of the supplier selection process.
- Representation of Mannesmann Mobilfunk to the ETSI standardization group "Standardization Technical Committee SMG3 System Architecture"
- Conduction of product and hardware development quality audits
- Representative of Mannesmann Mobilfunk in A-interface interoperability testing activities
- Member of BSS product planning group which was defining operator requirements for future BSS releases
- Development of process improvements for type acceptance

III. LIST OF SUPPORTED PATENT LITIGATIONS AND VALIDITY ACTIONS

2025

Hannibal IP LLC v. Samsung Electronics Co. Ltd., Samsung Electronics America Inc.
Inter Partes Review matters
On behalf of Samsung
Counsel: Finnegan L.L.P.
Role: Expert witness and consulting services

2025

Pantech Corp. v. OnePlus Technology Co., Ltd.
Inter Partes Review matters
On behalf of OnePlus
Counsel: Bayes PLLC
Role: Expert witness and consulting services

2025

Pantech Corp. v. OnePlus Technology Co., Ltd.
Inter Partes Review matters
On behalf of OnePlus
Counsel: Leydig, Voit & Mayer, Ltd.
Role: Expert witness and consulting services

2025

Apex Beam Technologies LLC v. Apple Inc.
Inter Partes Review matters
On behalf of Apple
Counsel: Fish&Richardson P.C.
Role: Expert witness and consulting services

2024

Pantech Corporation v. Oppo Mobile Telecommunications Corp., Ltd.
Inter Partes Review matters
On behalf of Oppo
Counsel: Bayes PLLC
Role: Expert witness and consulting services

2024

Pantech Corp. et al. v. LG Electronics Inc. et al.
Civil Action No. 5:22-cv-00113-RWS-JBB (E.D.Tx.)
On behalf of LG Electronics
Counsel: Ropes & Gray LLP
Role: Expert witness and consulting services

2024

Ericsson v. Lenovo
Inter Partes Review matters
On behalf of Lenovo
Counsel: Kirkland & Ellis LLP
Role: Expert witness and consulting services

2024

Pantech Corp. et al. v. OnePlus Technology Co., Ltd.
Civil Action No. 5:22-cv-00069-RWS (E.D.Tx.)
On behalf of OnePlus
Counsel: Leydig, Voit & Mayer, Ltd.
Role: Expert witness and consulting services

2024

G+ Communications, LLC, v. Samsung Electronics Co., Ltd.

Civil Action No. 2:22-CV-78 (E.D.Tx.)
On behalf of Samsung
Counsel: Fish&Richardson P.C.
Role: Expert witness and consulting services

2023

Unified Patents, LLC v. Helios Streaming LLC
Inter Partes Review matters
On behalf of Unified Patents
Counsel: Akin
Role: Expert witness and consulting services

2023

Unified Patents, LLC v. SLS Manager Technologies
Inter Partes Review matters
On behalf of Unified Patents
Counsel: Unified Patents
Role: Expert witness and consulting services

2023

Headwater Research LLC v. Samsung Electronics Co., Ltd.
Inter Partes Review matters
On behalf of Samsung
Counsel: Fish&Richardson P.C.
Role: Expert witness and consulting services

2023

Pantech Corp. et al. v. LG Electronics Inc. et al.
Inter Partes Review matters
On behalf of LG Electronics
Counsel: Ropes & Gray LLP
Role: Expert witness and consulting services

2023

Apple Computer Trading (Shanghai) Co., Ltd, Apple Electronics Products Commerce (Beijing) Co., Ltd. v. Optis Cellular Technology LLC
Shenzhen, China, Intermediate People's Court
On behalf of Apple
Counsel: WilmerHale
Role: Expert witness and consulting services

2023

Huawei Technologies Co., Ltd. v. MediaTek Inc.
Inter Partes Review matters
On behalf of MediaTek
Counsel: Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.
Role: Expert witness and consulting service

2023

Apex Beam Technologies LLC v. Samsung
Inter Partes Review matters
On behalf of Samsung
Counsel: Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.
Role: Expert witness and consulting services

2022

Constellation Designs LLC v. LG Electronics, Inc.
Inter Partes Review matters
On behalf of LG Electronics
Counsel: Fish&Richardson P.C.
Role: Expert witness and consulting services

2022

Unified Patents, LLC v. Togail Technologies LTD.
Inter Partes Review matters
On behalf of Unified Patents
Counsel: Duane Morris LLP
Role: Expert witness and consulting services

2022

Ericsson v. Apple
Certain Mobile Telephones, Tablet Computers With Cellular Connectivity, And Smart Watches With Cellular Connectivity, Components Thereof, And Products Containing Same, Inv. No. 337-TA-1299 (U.S.I.T.C.)
On behalf of Apple
Counsel: WilmerHale
Role: Expert and consulting services

2022

Ericsson v. Apple
Civil Action No. 2:21-cv-376 (E.D.Tex.)
On behalf of Apple
Counsel: WilmerHale
Role: Expert and consulting services

2022

Intellectual Ventures II LLC v. Toyota Motor Cooperation.
Inter Partes Review matters
On behalf of Toyota
Counsel: Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.
Role: Expert witness and consulting services

2022

Ericsson v. Apple
2nd Business Court, Rio de Janeiro, Brazil
On behalf of Apple
Counsel: WilmerHale
Role: Expert and consulting services

2022

Ericsson v. Apple
Civil Court, Bogotá, Columbia
On behalf of Apple
Counsel: WilmerHale
Role: Expert and consulting services

2022

Proven Networks LLC. v. NetApp Inc.
Inter Partes Review matters
On behalf of NetApp
Counsel: Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., Ropes & Gray LLP
Role: Expert witness and consulting services

2022

Ericsson v. Apple
Inter Partes Review matters
On behalf of Apple
Counsel: Fish&Richardson, Erise IP
Role: Expert witness and consulting services

2021

AEGIS 11 LLC v. Hisense Company, Ltd. and Hisense USA Corporation
Inter Partes Review matters
On behalf of Hisense

Counsel: Orrik Herrington & Sutcliffe LLP
Role: Expert witness and consulting services

2021

Nokia v. Lenovo
Certain Electronic Devices, Including Computers, Tablet Computers, and Components and Modules Thereof, Inv. No. 337-TA-1208 (U.S.I.T.C.)
On behalf of Lenovo
Counsel: WilmerHale
Role: Expert witness and consulting services

2021

Optis Cellular Technology LLC et al. v. Apple
Claim No. HP-2019-000006 (High Court of Justice, Business and Property Courts of England and Wales)
On behalf of Apple
Counsel: WilmerHale
Role: Expert witness and consulting services

2021

Ericsson v. Samsung
Inter Partes Review matters
On behalf of Samsung
Counsel: Kirkland&Ellis LLP, Fish&Richardson
Role: Expert witness and consulting services

2020

Panoptis Patent Management LLC et al. v. Apple Inc.
Civil Action No. 2:19-cv-66 (E.D. Tex.)
On behalf of Apple
Counsel: WilmerHale
Role: Expert witness at bench trial

2020

Sol IP, LLC v. AT&T Mobility, LLC et al.
Civil Action No. 2:18-cv-526 (E.D. Tex.)
On behalf of AT&T, Verizon, Sprint
Counsel: Gibson Dunn
Role: Expert witness and consulting services

2020

Bell Northern Research LLC v. LG Electronics Inc. et al.
Civil Action No. 18-CV-2864-CAB-BLM (S.D. Cal.)
On behalf of LG Electronics Inc.
Counsel: Fish&Richardson
Role: Expert witness and consulting services

2019

Conversant Wireless Licensing S.a.r.l. v. LG Electronics Deutschland GmbH
Civil Action No. 7 O 3277/18 (Landgericht Munich, Germany)
On behalf of LG Electronics Deutschland GmbH
Counsel: Wildanger Kehrwald Graf von Schwerin & Partner mbB
Role: Expert witness and consulting services

2019

Bell Northern Research, LLC v. Huawei Device Co., Ltd, et al.
Civil Action No. 3:18-cv-01784-CAB-BLM
On behalf of Huawei
Counsel: Fish&Richardson
Role: Expert witness and consulting services

2019

Uniloc USA, Inc., et al. v. Samsung Electronics America, Inc. and Samsung Electronics Co. Ltd.
Civil Action Nos. 2:18-cv-00040-JRG, 2:18-cv-00041-JRG, 2:18-cv-00042-JRG and 2:18-cv-00044-JRG (United States District Court for the Eastern District of Texas)
On behalf of Samsung
Counsel: Greenberg Traurig
Role: Expert witness and consulting services

2019

Uniloc USA, Inc., et al. v. Huawei Device USA, Inc. et al.
Civil Action No. 2:18-cv- 00072-JRG-RSP (E.D. Tex.)
On behalf of Huawei
Counsel: McGuireWoods
Role: Expert witness and consulting services

2019

Microsoft Corporation v. Uniloc 2017 LLC
Inter Partes Review of U.S. Pat. No. 7,167,487
Inter Partes Review of U.S. Pat. No. 7,075,917
On behalf of Microsoft and on behalf of Apple as joinder petitioner
Counsel: Klarquist Sparkman (Microsoft), Erise IP (Apple)
Role: Expert witness and consulting services

2019

Qualcomm v. KFTC
South Korean Case, Seoul High Court
On behalf of intervenor Apple supporting the KFTC
Counsel: Boies Schiller Flexner
Role: Expert witness

2018/19

Evolved Wireless, LLC v. Apple, Inc.
Civil Action No. 1:15-cv-00542-JFB-SRF
On behalf of Apple
Counsel: DLA Piper
Role: Expert witness and consulting services

2018/19

Cisco Systems Inc. v. Traxcell Technologies
Inter Partes Review of Traxcell Technologies patents
On behalf of Cisco
Counsel: King&Spalding
Role: Expert witness and consulting services

2018/19

Qualcomm Inc. v. Apple Inc.
Civil Action No. 3:17- cv-02398-DMS-MDD (United States District Court for the Southern District of California)
Civil Action No. 3:17-cv-02402-WQH-MDD
Certain Mobile Electronic Devices and Radio Frequency and Processing Components Thereof (II), Inv. No. 337-TA-1093
Inter Partes Review of U.S. PATENT NO. 9,154,356
Cases IPR2019-00047, IPR2019-00048, IPR2019-00049, IPR2019-00128, IPR2019-00129
On behalf of Apple and Intel
Counsel: WilmerHale
Role: Expert witness and consulting services

2018/19

Apple Inc. v. Qualcomm Inc.
Civil Action No. 3:17-CV-00108-GPC-MDD (United States District Court for the Southern District of California)
On behalf of Apple

Counsel: Fish&Richardson, Boies Schiller Flexner
Role: Expert witness and consulting services

2018

3G Licensing, S.A. et al. v. LG Electronics Inc. et al
Inter Partes Review of U.S. Patent No. 7,995,091
On behalf of LG Electronics
Counsel: Fish&Richardson
Role: Expert witness

2017

Huawei Technologies Co. LTD. v. T-Mobile US, Inc. & T-Mobile USA, Inc.
E.D. Tex. Case Nos. 2:16-cv-00052-JRG-RSP; 2:16-cv-00055-JRG-RSP; 2:16-cv-00056-JRG-RSP; and 2:16-cv-00057-JRG-RSP
On behalf of T-Mobile
Counsel: Gibson Dunn
Role: Expert witness and consulting services

2016

Koninklijke KPN N.V. v. Samsung Electronics America, Inc. et al.
Civil Action No. 14-cv-1165
On behalf of Samsung Electronics
Counsel: Baker Botts
Role: Expert witness and consulting services

2016

SSH v. Sony
OLG Düsseldorf, Germany
On behalf of SSH
Counsel: Cohausz&Florack
Role: Technical expert support

2015/16

LG Electronics v. Core Wireless Licensing S.A.R.L.
Inter Parles Review of U.S. Patent No. 8,165,049
On behalf of LG Electronics
Counsel: Greenberg Traurig
Role: Expert witness

2015/16

Core Wireless Licensing S.A.R.L. v. LG Electronics Inc. and LG Electronics MobileComm U.S.A., Inc
Civil Action No. 2:14-cv-911 (lead case) and Civil Action No. 2:14-cv-912 (consolidated)
On behalf of LG Electronics
Counsel: Greenberg Traurig, Sidley Austin
Role: Expert witness

2015

Intellectual Ventures I LLC v. T-Mobile USA, Inc. & T-Mobile US, Inc.
D. Del. Case No. 1:13-cv-01632
Intellectual Ventures II LLC v. T-Mobile USA, Inc. & T-Mobile US, Inc.
D. Del. Case No. 1:13-cv-01633
On behalf of T-Mobile
Counsel: Gibson Dunn
Role: Technical expert support

IV. EDUCATION

10/1984 – 10/1993 University of Technology Aachen Aachen, Germany

Graduate of Electrical Engineering with a focus on telecommunications technologies (Dipl.-Ing. TH)

10/1992 – 04/1993 **University of Technology Trondheim** **Trondheim, Norway**
Diploma Thesis "Design of a dual processor computer for digital signal processing in power electronics"

V. LANGUAGES

German, English, French

VI. PUBLICATIONS (selection)

- ”Standardessentielle Patente (SEPs) für das Internet der Dinge (IoT)”, PATINFO 2025 Proceedings, May 2025
- “The need for standardisation in the M2M services layer”, Global Telecoms Business, February 2014
- Co-authored white paper “Lightweight M2M: Enabling device management and applications for the internet of things”, Open Mobile Alliance, March 2014
- “Objects are a new way to create M2M applications”, Global Telecoms Business, April 2014
- “The need for standardisation in the M2M services layer”, M2M Now, July 2015
- “Objects are a new way to create M2M applications”, Global Telecoms Business, April 2014
- Co-authored white paper “Lightweight M2M: Enabling device management and applications for the internet of things”, Open Mobile Alliance, March 2014
- “The need for standardisation in the M2M services layer”, Global Telecoms Business, February 2014
- ”Unlocking the internet of things and driving the need for interoperability”, Global Telecoms Business, December 2013

APPENDIX AA

http://www.3gpp.org/ftp/Specs/html-info/23-series.htm Go
193 captures
30 Jun 2003 - 8 Jun 2024
APR JUL AUG
2006 2007 2008
About this capture

3GPP Specification series

Back to numbering scheme page

Click on spec number for details

TS 23.002	Network architecture	.
TS 23.003	Numbering, addressing and identification	.
TS 23.007	Restoration procedures	.
TS 23.008	Organization of subscriber data	.
TS 23.009	Handover procedures	.
TS 23.010	GSM Public Land Mobile Network (PLMN) Connection Types	SPECIFICATION WITHDRAWN
TS 23.011	Technical realization of Supplementary Services	.
TS 23.012	Location management procedures	.
TS 23.014	Support of Dual Tone Multi Frequency (DTMF) signalling	.
TS 23.015	Technical realization of Operator Determined Barring (ODB)	.
TS 23.016	Subscriber data management; Stage 2	.
TS 23.018	Basic call handling; Technical realization	.
TS 23.01U	General UMTS architecture	SPECIFICATION WITHDRAWN
TS 23.022	Functions related to Mobile Station (MS) in idle mode and group receive mode	SPECIFICATION WITHDRAWN
TS 23.031	Fraud Information Gathering System (FIGS); Service description; Stage 2	.
TS 23.032	Universal Geographical Area Description (GAD)	.
TS 23.034	High Speed Circuit Switched Data (HSCSD); Stage 2	.
TS 23.035	Immediate Service Termination (IST); Stage 2	.
TS 23.038	Alphabets and language-specific information	.
TR 23.039	Interface Protocols for the Connection of Short Message Service Centers (SMSCs) to Short Message Entities (SMEs)	.
TS 23.040	Technical realization of Short Message Service (SMS)	.
TS 23.041	Technical realization of Cell Broadcast Service (CBS)	.
TS 23.042	Compression algorithm for SMS	.
TS 23.043	Support of Videotex	SPECIFICATION WITHDRAWN
TS 23.044	Support of Teletex	SPECIFICATION WITHDRAWN
TS 23.045	Technical Realization of Facsimile Group 3 Service - transparent	SPECIFICATION WITHDRAWN
TS 23.046	Technical realisation of facsimile Group 3 service - non-transparent	SPECIFICATION WITHDRAWN
TS 23.048	Security mechanisms for the (U)SIM application toolkit; Stage 2	.
TS 23.053	Tandem Free Operation (TFO); Service description; Stage 2	.
TS 23.054	Shared Interworking Functions (SIWF); Stage 2	SPECIFICATION WITHDRAWN
TS 23.057	Mobile Execution Environment (MExE); Functional description; Stage 2	.
TS 23.05U	UMTS Network principles	SPECIFICATION WITHDRAWN
TS 23.060	General Packet Radio Service (GPRS); Service description; Stage 2	.
TS 23.066	Support of GSM Mobile Number Portability (MNP) stage 2	.
TS 23.067	Enhanced Multi-Level Precedence and Pre-emption Service (eMLPP); Stage 2	.
TS 23.069	Voice Broadcast service (VBS); Stage 2	SPECIFICATION WITHDRAWN
TS 23.070	Routeing of calls to/from Public Data Networks (PDN) and the GSM Public Land Mobile Network (PLMN)	SPECIFICATION WITHDRAWN
TS 23.071	Location Services (LCS); Functional description; Stage 2	SPECIFICATION WITHDRAWN
TS 23.072	Call Deflection Supplementary Service; Stage 2	.
TS 23.073	Support of Localised Service Area (SoLSA); Stage 2	SPECIFICATION WITHDRAWN

TS 23.078	Customized Applications for Mobile network Enhanced Logic (CAMEL) Phase X; Stage 2	.
TS 23.079	Support of Optimal Routeing (SOR); Technical realization; Stage 2	.
TS 23.081	Line Identification supplementary services; Stage 2	.
TS 23.082	Call Forwarding (CF) Supplementary Services; Stage 2	.
TS 23.083	Call Waiting (CW) and Call Hold (HOLD) Supplementary Service; Stage 2	.
TS 23.084	MultiParty (MPTY) Supplementary Service; Stage 2	.
TS 23.085	Closed User Group (CUG) Supplementary Service; Stage 2	.
TS 23.086	Advice of Charge (AoC) Supplementary Service; Stage 2	.
TS 23.087	User-to-User Signalling (UUS) supplementary service; Stage 2	.
TS 23.088	Call Barring (CB) Supplementary Service; Stage 2	.
TS 23.090	Unstructured Supplementary Service Data (USSD); Stage 2	.
TS 23.091	Explicit Call Transfer (ECT) Supplementary Service; Stage 2	.
TS 23.093	Technical realization of Completion of Calls to Busy Subscriber (CCBS); Stage 2	.
TS 23.094	Follow Me Stage 2	.
TS 23.096	Name identification supplementary service; Stage 2	.
TS 23.097	Multiple Subscriber Profile (MSP) Phase 1; Stage 2	.
TS 23.101	General UMTS Architecture	.
TS 23.107	Quality of Service (QoS) concept and architecture	.
TS 23.108	Mobile radio interface layer 3 specification core network protocols; Stage 2 (structured procedures)	.
TS 23.10U	UMTS Access Stratum; Services and Functions	SPECIFICATION WITHDRAWN
TS 23.110	UMTS Access Stratum Services and Functions	.
TS 23.116	Super-Charger technical realization; Stage 2	.
TS 23.119	Gateway Location Register (GLR); Stage2	.
TS 23.121	Architectural requirements for Release 1999	.
TS 23.122	Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode	.
TS 23.125	Overall high level functionality and architecture impacts of flow based charging; Stage 2	.
TS 23.127	Virtual Home Environment (VHE) / Open Service Access (OSA)	.
TS 23.135	Multicall supplementary service; Stage 2	.
TS 23.140	Multimedia Messaging Service (MMS); Functional description; Stage 2	.
TS 23.141	Presence service; Architecture and functional description; Stage 2	.
TS 23.146	Technical realization of facsimile Group 3 service - non-transparent	.
TS 23.153	Out of band transcoder control; Stage 2	.
TS 23.167	IP Multimedia Subsystem (IMS) emergency sessions	.
TS 23.171	Location Services (LCS); Functional description; Stage 2 (UMTS)	.
TS 23.172	Technical realization of Circuit Switched (CS) multimedia service; UDI/RDI fallback and service modification; Stage 2	.
TS 23.174	Push service; stage 2	.
TS 23.178	customized Applications for Mobile network Enhanced Logic (CAMEL) - IP Multimedia System (IMS) interworking; Stage 2	SPECIFICATION WITHDRAWN
TS 23.195	Provision of User Equipment Specific Behaviour Information (UESBI) to network entities	.
TS 23.198	Open Service Access (OSA); Stage 2	.
TS 23.202	Circuit switched data bearer services	.
TS 23.203	Policy and charging control architecture	.
TS 23.204	Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access; Stage 2	.
TS 23.205	Bearer-independent circuit-switched core network; Stage 2	.
TS 23.206	Voice Call Continuity (VCC) between Circuit Switched (CS) and IP Multimedia Subsystem (IMS); Stage 2	.
TS 23.207	End-to-end Quality of Service (QoS) concept and architecture	.
TS 23.209	Policy control over Gq interface	SPECIFICATION WITHDRAWN
TS 23.20U	Evolution of the GSM platform towards UMTS	SPECIFICATION WITHDRAWN
TS 23.218	IP Multimedia (IM) session handling; IM call model; Stage 2	.
TS 23.221	Architectural requirements	.

TS 23.226	Global text telephony (GTT); Stage 2: Architecture	.
TS 23.227	Application and user interaction in the UE; Principles and specific requirements	.
TS 23.228	IP Multimedia Subsystem (IMS); Stage 2	.
TS 23.234	3GPP system to Wireles Local Area Network (WLAN) interworking; System description	.
TS 23.236	Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes	.
TS 23.240	3GPP Generic User Profile (GUP) requirements; Architecture (Stage 2)	.
TS 23.241	3GPP Generic User Profile (GUP); Stage 2; Data Description Method (DDM)	SPECIFICATION WITHDRAWN
TS 23.246	Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description	.
TS 23.251	Network sharing; Architecture and functional description	.
TS 23.258	reserved for: All-IP network (AIPN); Stage 2	.
TS 23.259	Personal Network Management (PNM); Procedures and information flows	.
TS 23.271	Functional stage 2 description of Location Services (LCS)	.
TS 23.278	Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 4; Stage 2; IM CN Interworking	.
TS 23.279	Combining Circuit Switched (CS) and IP Multimedia Subsystem (IMS) services; Stage 2	.
TS 23.333	Multimedia Resource Function Controller (MRFC) - Multimedia Resource Function Processor (MRFP) Mp interface; Procedures descriptions	.
TS 23.340	(reserved for:"" IP Multimedia Subsystem (IMS) messaging; Stage 2"")	SPECIFICATION WITHDRAWN
TS 23.401	General Packet Radio Service (GPRS) enhancements for Long Term Evolution (LTE) access	.
TS 23.402	3GPP System Architecture Evolution (SAE): Architecture enhancements for non-3GPP accesses	.
TS 23.40U	UMTS Network Aspects; Relationship with UPT	SPECIFICATION WITHDRAWN
TS 23.50U	UMTS Network Aspects; IN and B-ISDN concepts in a UMTS environment	SPECIFICATION WITHDRAWN
TS 23.60U	UMTS Network Aspects; UMTS data organization	SPECIFICATION WITHDRAWN
TS 23.70U	UMTS Network Aspects; UMTS operations and procedures	SPECIFICATION WITHDRAWN
TR 23.801	Potential mechanisms for Circuit Switched (CS) domain video and voice service improvements	.
TR 23.802	Architectural enhancements for end-to-end Quality of Service (QoS)	.
TR 23.803	Evolution of policy control and charging	SPECIFICATION WITHDRAWN
TR 23.804	Support of SMS and MMS over generic 3GPP IP access	.
TR 23.805	Selective disabling of User Equipment (UE) capabilities; Report on technical options and conclusions	.
TR 23.806	Voice call continuity between Circuit Switched (CS) and IP Multimedia Subsystem (IMS) Study	.
TR 23.807	Feasibility study for enhancement of radio performance for Voice over IP Multimedia Subsystem (VoIMS); Report on technical options and conclusions	.
TR 23.808	Supporting Globally Routable User Agent URI in IMS; Report and conclusions	.
TR 23.809	One Tunnel solution for Optimisation of Packet Data Traffic	.
TS 23.80U	UMTS Network Aspects; Signalling requirements for UMTS	SPECIFICATION WITHDRAWN
TR 23.810	Study on architecture impacts of Service Brokering	.
TR 23.814	Separating RR and MM specific parts of the MS Classmark	.
TR 23.815	Charging implications of IMS architecture	.
TR 23.816	Identification of communication services in IMS	.
TR 23.817	Feasibility study on enhancement of radio performances for Voice over IMS (VoIMS); Report on Technical options and conclusions	.
TR 23.818	Optimisations and Enhancements for Realtime IMS Communication	.
TR 23.819	Terminating session handling	.
TR 23.820	Study of IMS restoration procedures	.
TR 23.821	Architecture Principles for Reelase 2000	SPECIFICATION WITHDRAWN
TR 23.825	Overall architecture aspects of IP flow based bearer level charging; Stage 2	SPECIFICATION WITHDRAWN
TR 23.826	Feasibility study on Voice Call Continuity (VCC) support for emergency calls	.
TR 23.827	Feasbility study of mobility between 3GPP-WLAN interworking and 3GPP systems	.
TR 23.835	Study into applicability of Galileo in Location Services (LCS)	.

TR 23.836	Quality of Service (QoS) and policy aspects of 3GPP - Wirless Local Area Network (WLAN) interworking	.
TR 23.837	Location Services (LCS) architecture for 3GPP system - Wireless Local Area Network (WLAN) interworking	.
TR 23.840	Study into routeing of MT-SMs via the HPLMN	.
TR 23.841	Presence service architecture	.
TR 23.846	Multimedia Broadcast/Multicast Service (MBMS); Stage 2	.
TR 23.847	Enhancements to IMS service functionalities facilitating multicast bearer services	.
TR 23.851	Network sharing; Architecture and functional description	.
TR 23.864	Commonality and interoperability between IP Multimedia System (IMS) core networks	.
TR 23.867	Internet Protocol (IP) based IP Multimedia Subsystem (IMS) emergency sessions	.
TR 23.871	Enhanced support for user privacy in Location Services (LCS)	.
TR 23.873	Feasibility study for transport and control separation in the PS CN domain	.
TR 23.874	Feasibility study of architecture for network requested PDP context activation with User-ID	SPECIFICATION WITHDRAWN
TR 23.875	Support of Push service	.
TR 23.876	Push architecture	SPECIFICATION WITHDRAWN
TR 23.877	Architectural aspects of speech-enabled services	.
TR 23.878	Impacts of speech-enabled services on IMS, PS and CS domains	SPECIFICATION WITHDRAWN
TR 23.879	Study on Circuit Switched (CS) domain services over evolved Packet Switched (PS) access	.
TR 23.881	Interworking aspects and migration scenarios for IPv4-based IP Multimedia Subsystem (IMS) implementations	SPECIFICATION WITHDRAWN
TR 23.882	3GPP system architecture evolution (SAE); Report on technical options and conclusions	.
TR 23.892	IP Multimedia System (IMS) centralized services	.
TR 23.893	Feasibility study on multimedia session continuity	.
TR 23.895	Provision of UE specific behaviour information to network entities	.
TR 23.898	Access Class Barring and Overload Protection (ACBOP)	.
TR 23.899	Combining Circuit Switched (CS) bearers with IP Multimeida Subsystem (IMS)	SPECIFICATION WITHDRAWN
TR 23.903	Redial solution for voice-video switching	.
TR 23.904	Support of SMS and MMS over generic 3GPP IP access	SPECIFICATION WITHDRAWN
TR 23.907	Quality of Service (QoS) concept	SPECIFICATION WITHDRAWN
TR 23.908	Technical report on Pre-Paging	.
TR 23.909	Technical report on the Gateway Location Register	.
TS 23.90U	UMTS Network Aspects; Network performance requirements	SPECIFICATION WITHDRAWN
TR 23.910	Circuit switched data bearer services	.
TR 23.911	Technical report on Out-of-band transcoder control	.
TR 23.912	Technical report on Super-Charger	.
TR 23.913	UMTS Turbo-Charger	SPECIFICATION WITHDRAWN
TR 23.915	Charging implications of IMS architecture	SPECIFICATION WITHDRAWN
TR 23.917	Dynamic policy control enhancements for end-to-end Quality of Service (QoS)	SPECIFICATION WITHDRAWN
TR 23.919	Direct tunnel deployment guideline	.
TS 23.920	Evolution of the GSM platform towards UMTS	SPECIFICATION WITHDRAWN
TR 23.922	Architecture for an All IP network	SPECIFICATION WITHDRAWN
TR 23.923	Combined GSM and Mobile IP mobility handling in UMTS IP CN	.
TR 23.925	UMTS Core network based ATM transport	SPECIFICATION WITHDRAWN
TR 23.927	VHE, Open Service Architecture (OSA)	SPECIFICATION WITHDRAWN
TR 23.930	Iu principles	.
TR 23.934	3GPP system to Wireless Local Area Network (WLAN) interworking; Functional and architectural definition	.
TR 23.937	Feasbility study of mobility between 3GPP-WLAN interworking and 3GPP systems	SPECIFICATION WITHDRAWN
TR 23.941	3GPP Generic User Profile (GUP); Stage 2; Data Description Method (DDM)	.
TR 23.955	Virtual Home Environment (VHE) concepts	SPECIFICATION WITHDRAWN
TS 23.95U	UMTS Network Aspects; Network functions relevant to satellites	SPECIFICATION WITHDRAWN
TR 23.960	Framework of network functions to support multimedia services	SPECIFICATION WITHDRAWN
TR 23.964	Commonality and interoperability between IP Multimedia System (IMS) core networks	SPECIFICATION WITHDRAWN

TR 23.972	Circuit switched multimedia telephony	.
TR 23.974	Support of push service	SPECIFICATION WITHDRAWN
TR 23.976	Push architecture	.
TR 23.977	Bandwidth And Resource Savings (BARS) and speech enhancements for Circuit Switched (CS) networks	.
TR 23.979	3GPP enablers for Open Mobile Alliance (OMA) Push-to-talk over Cellular (PoC) services; Stage 2	.
TR 23.981	Interworking aspects and migration scenarios for IPv4-based IP Multimedia Subsystem (IMS) implementations	.
TR 23.982	IP Multimedia System (IMS) centralized services	SPECIFICATION WITHDRAWN

APPENDIX AB

Specification #: 31.101

Meetings	Version	Upload date	Comment
CT#52	7.2.2	2011-06-24	corrects unnumbered reference...
CT#50	7.2.1	2011-01-03	§13 header format
CT#48	7.2.0	2010-06-20	
CT#46	7.1.0	2009-12-20	
CT#36	7.0.1	2007-06-21	MCC correction of implementat...
CT#36	7.0.0	2007-06-12	

Release 6(Spec is UCC for this Release)

Latest Remark: (2015-01-22) TP-17: upgraded to Rel-6 as there are 3G specific ...

Meetings	Version	Upload date	Comment
CT#30	6.5.1	2006-01-26	Corrects wrong CR number in c...
CT#28	6.5.0	2005-06-14	
T#26	6.4.1	2005-01-06	
T#26	6.4.0	2005-01-03	
T#25	6.3.0	2004-09-27	
T#20	6.2.0	2003-06-23	
T#18	6.1.0	2003-01-02	
T#17	6.0.0	2002-09-18	

Release 5(Spec is UCC for this Release)

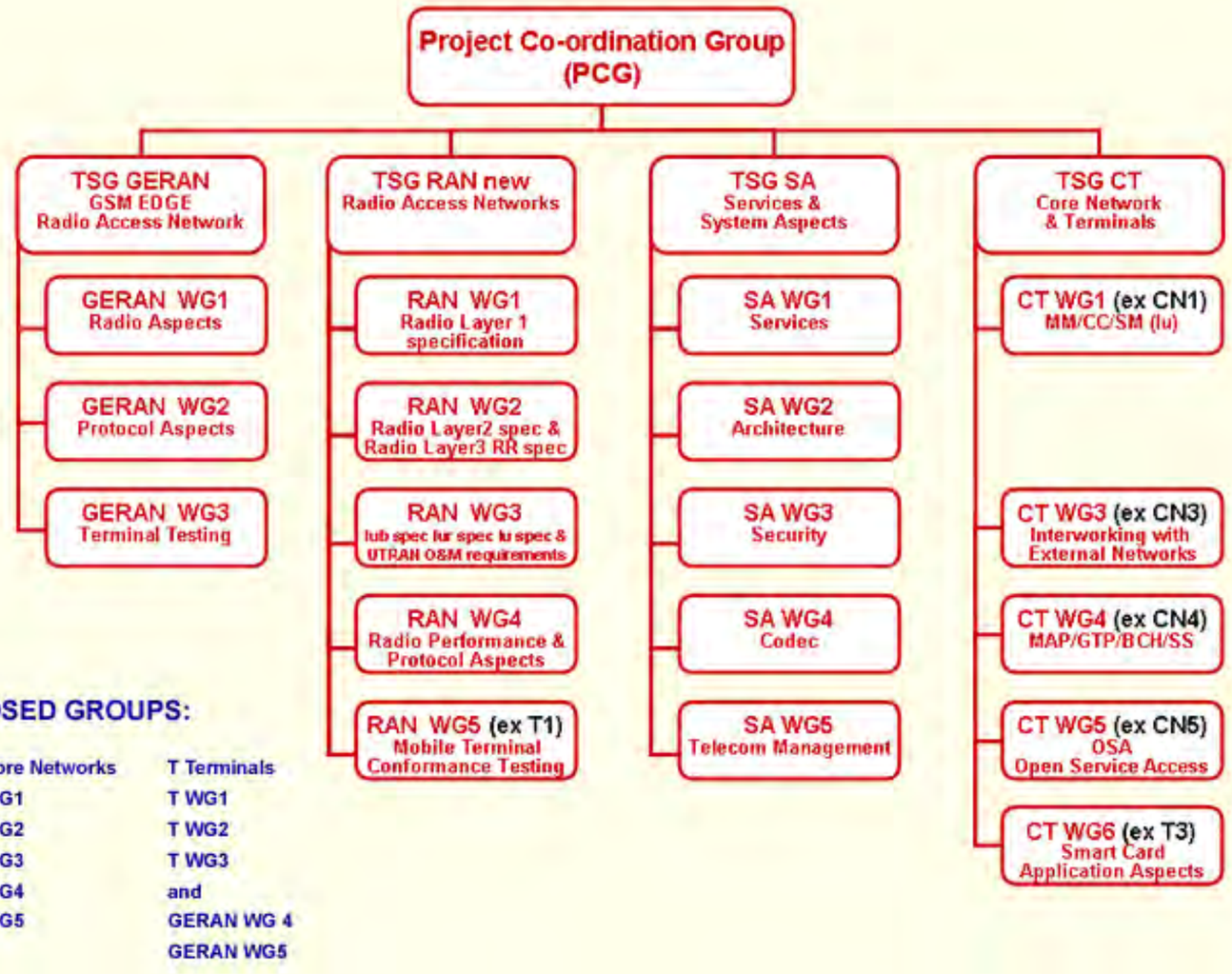
Latest Remark: (2015-01-22) TP-17: upgraded to Rel-5 to fill gap between Relea...

Exit

APPENDIX B

INTERNET ARCHIVE
WayBackMachine
http://www.3gpp.org/tb/home.htm
Go
JUN AUG OCT
247 captures
14 Dec 2001 – 6 Oct 2022
2004 05 2005 2006
About this capture

TSG ORGANIZATION



MCC Task Forces

last updated:
2005-06-22: new org chart removing closed working groups from main body of chart
2005-03-14: Complete update
2005-01-31: New TSG structure.

APPENDIX C

Specifications by Series



All 3GPP specifications have a specification number consisting of 5 digits, in a seriesinspired by the pre-1998 GSM series of specification numbering – with its4 digits. In both cases, the first two digits define the series number.

These series are commonly used to describe the work. An example would be the '38 series' can be used in the project to describe radio studies and specifications for 5G NR.

The links in the table below will take you to listings of the specifications and reports in each series.

Subject of specification series	3G and beyond / GSM (R99 and later)	GSM only (Rel-4 and later)	GSM only (before Rel-4)
Requirements	21 series	41 series	01 series
Service aspects ("stage 1")	22 series	42 series	02 series
Technical realization ("stage 2")	23 series	43 series	03 series
Signalling protocols ("stage 3") - user equipment to network	24 series	44 series	04 series
Radio aspects	25 series	45 series	05 series
CODECs	26 series	46 series	06 series

Data	27 series	47 series (none exists)	07 series
Signalling protocols ("stage 3") -(RSS-CN) and OAM&P and Charging (overflow from 32.- range)	28 series	48 series	08 series
Signalling protocols ("stage 3") - intra-fixed-network	29 series	49 series	09 series
Programme management	30 series	50 series	10 series
Subscriber Identity Module (SIM / USIM), IC Cards. Test specs.	31 series	51 series	11 series
OAM&P and Charging	32 series	52 series	12 series
Access requirements and test specifications		13 series [1]	13 series [1]
Security aspects	33 series	[2]	[2]
UE and (U)SIM test specifications	34 series	[2]	11 series
Security algorithms [3]	35 series	55 series	[4]
LTE (Evolved UTRA), LTE-Advanced, LTE-Advanced Pro radio technology	36 series		
Multiple radio access technology aspects	37 series		
Radio technology beyond LTE	38 series		

Note (1): *The 13 series GSM specifications relate to European Union specific regulatory standards. On the closure of ETSI TC SMG, responsibility for these specifications was transferred to ETSI TC MSG, (Mobile Specification Group) and they do not appear on the 3GPP file server.*

Note (2): *The specifications of these aspects are spread throughout several series.*

Note (3): *Algorithms may be subject to export licensing conditions. See the relevant 3GPP page. See also the relevant ETSI pages.*

Note (4): *The original GSM algorithms are not published and are controlled by the GSM Association.*

The links in the table above take you to the 3GPP Portal 'Specifications' section. From there you can download the specification and see full details of the history and ownership of the spec.(via the binocular icon...).

Numbering Technical Reports (two classes):

SDO Transposition	Not intended for publication
TRs Intended to be transposed and issued by the Organizational Partners as their own publications:	3GPP internal, documenting, planning and scheduling of work, interim results of feasibility studies:
Numbers of the form: xx.9xx	Numbers of the form: xx.8xx (feasibility study reports, etc) or, more rarely, 30.xxx / 50.xxx (planning and scheduling) For some specification series, the stock of xx.8xx TRs has been exhausted. In these cases, further internal TRs are allocated xx.7xx numbers.

Latest versions

- The latest versions of the approved specifications areplaced in the "latest" directory of the ftp area: https://www.3gpp.org/ftp/Specs/latest.
- The latest version of draft specifications (i.e. those not yet under change control) are in the "latest-drafts" directory (https://www.3gpp.org/ftp/Specs/latest-drafts)

Old (archived) specifications

All older versions of specifications (where available) are stored in the archive subdirectory. All versions of all releases of a given specification are placed directly under the name of the specification.

Specs related to a particular working group

Each 3GPP TSG Working Group has a home page, with a link to the list of specifications under its responsibility. See the 3GPP Group section of our website and navigate the WG or TSG of interest.

Official SDO Publications

The 3GPP Technical Specifications (TS) and Technical Reports (TR) become "official" when transposed into corresponding publications of the 3GPP Organizational Partner or the body acting as publisher for the Partner.

Once a Release is frozen (see definition in TR 21.900), 3GPP specifications are officially transposed and published by the Organizational Partners, as a part of their standards series.

More information about specifications:

3GPP Specification Status Report	https://www.3gpp.org/DynaReport/status-report.htm
'Missing Specs' following the most recent round of TSG meetings.	https://www.3gpp.org/DynaReport/MissingSpecs.htm
Specifications Per TSG (Plenary) Round	https://www.3gpp.org/specifications-technologies/specifications-by-series/specifications-per-tsg-round
Issuing new TS/TR numbers.	https://www.3gpp.org/specifications-technologies/specifications-by-series/issuing-new-ts-and-tr-numbers
Search for references to a given specificationor references in a specification.	https://portal.3gpp.org/3gppreferences/SearchReferences.aspx
TS or TR Proposed for withdrawal.	https://www.3gpp.org/specifications-technologies/specifications-by-series/ts-or-tr-proposed-for-withdrawal
Version numbering scheme	https://www.3gpp.org/specifications-technologies/specifications-by-series/version-numbering-scheme

Specification and TR file name conventions	https://www.3gpp.org/specifications-technologies/specifications-by-series/file-name-conventions
GSM Specifications – a short history	https://www.3gpp.org/specifications-technologies/specifications-by-series/gsm-specifications
ASN.1 Object Identifiers	https://www.3gpp.org/specifications-technologies/specifications-by-series/asn-1-object-identifiers
Confidentiality Algorithms	https://www.3gpp.org/specifications-technologies/specifications-by-series/confidentiality-algorithms
ETSI publications relating to core functions of the fixed IP Multimedia Subsystem (IMS)	https://www.3gpp.org/ftp/webExtensions/TISPAN_transfers/TISPAN_doc.pdf

Previous Next

Get news. Get knowledge. Get involved

Subscribe to 3GPP Newsletter

Join us and get involved

Browse our Technologies



The 5G Standard

3GPP General Enquiries:
info@3gpp.org

Connect:

Quick Links

- Home
- About 3GPP
- Specification Groups
- Specifications & Technologies
- Delegates Corner
- Get Involved
- News & Events
- Contact Us
- Unsubscribe
- Subscribe

Copyright 2023 © 3GPP

Legal Notice | Privacy | Terms of Use

Website by Alchemy Interactive

Cookie policy

APPENDIX D

Please log-in with your EOL account.

Username:

Password:

Keep me signed in (more info)

Login

Sign Up

Forgot your password ?

Select TSG/WG | Home | Directory | Browse FTP | Help

This site is 3GPP working area. Log in to access full features. For general information go to the public site www.3gpp.org

Search form (Series(1), Releases(26)) — Items per page 50

Title/Specification number

Series: 23. Technical realization

Type: Technical Specification (TS); Technical Report (TR)

Release: All Releases

Publication: Internal; For Publication

Technology: 2G; 3G; LTE; 5G

Status: Draft; Under change control; Withdrawn before change control; Withdrawn under change control

Search

Data pager

1 **2** 3 4 5 6 7 8 9 10 — 476 specifications found, displaying 51 to 100

Specification Number	Type	Title	Status	Primary Responsible Group	
23.100	TS	UMTS Access Stratum; Services and Functions	change control		
23.110	TS	Universal Mobile Telecommunications System (UMTS) access stratum; Services and functions	Under change control	S2	2g 3g lte CR
23.116	TS	Super-Charger technical realization; Stage 2	Under change control	C4	2g 3g CR
23.119	TS	Gateway Location Register (GLR); Stage 2	Under change control	C4	3g lte CR
23.121	TS	Architectural requirements for Release 1999	Under change control	S2	2g 3g CR
23.122	TS	Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode	Under change control	C1	2g 3g lte 5g CR
23.125	TS	Overall high level functionality and architecture impacts of flow based charging; Stage 2	Under change control	S2	3g lte CR
23.127	TS	Virtual Home Environment (VHE) / Open Service Access (OSA)	Under change control	S2	2g 3g CR
23.135	TS	Multicall supplementary service; Stage 2	Under change control	C4	3g lte CR
23.139	TS	3GPP system - fixed broadband access network interworking; Stage 2	Under change control	S2	2g 3g lte CR
23.140	TS	Multimedia Messaging Service (MMS); Functional description; Stage 2	Under change control	CP	2g 3g CR
23.141	TS	Presence service; Architecture and functional description	Under change control	S2	IMS 3g lte CR
23.142	TS	Value-added Services for SMS (VAS4SMS); Interface and signalling flow	Under change control	C4	2g 3g lte 5g CR
23.146	TS	Technical realization of facsimile Group 3 non-transparent	Under change control	C3	3g CR
23.153	TS	Out of band transcoder control; Stage 2	Under change control	C4	2g 3g lte CR
23.161	TS	Network-Based IP Flow Mobility (NBIFOM); Stage 2	Under change control	S2	3g lte CR
23.167	TS	IP Multimedia Subsystem (IMS) emergency sessions	Under change control	S2	IMS 3g lte CR
23.168	TS	reerved for: Earthquake and Tsunami Warning System Specification (ETWS)	Withdrawn before change control	S2	2g 3g lte

©3GPP 2023. All rights reserved - 3GU v1.8.4 - 2023-05-09

APPENDIX E

www.3gpp.org / ftp / specs / archive / 51_series / 51.011

Download

	sort by name/desc	sort by date/desc	sort by size/desc
	51011-400.zip	2001/04/09 7:35	382,5 KB
	51011-410.zip	2001/07/06 13:02	402,7 KB
	51011-420.zip	2001/10/11 15:34	426,4 KB
	51011-430.zip	2002/01/17 8:36	365,5 KB
	51011-440.zip	2002/06/24 8:06	367,6 KB
	51011-450.zip	2002/09/17 10:12	439,4 KB
	51011-460.zip	2003/01/02 13:53	451,5 KB
	51011-470.zip	2003/03/20 8:09	459,7 KB
	51011-480.zip	2003/06/13 11:09	459,4 KB
	51011-490.zip	2003/09/29 14:05	464,2 KB
	51011-4a0.zip	2004/01/12 10:15	463,3 KB
	51011-4b0.zip	2004/03/26 10:10	369,2 KB
	51011-4c0.zip	2004/06/15 10:24	531,5 KB
	51011-4d0.zip	2004/12/28 15:03	524,4 KB
	51011-4e0.zip	2005/03/18 13:06	533,7 KB
	51011-4f0.zip	2005/06/15 12:56	496,3 KB
	51011-500.zip	2002/01/17 8:38	365,7 KB

17 items.

APPENDIX F

3GPP A GLOBAL INITIATIVE Portal

General | Versions | Responsibility | Related

Specification #: 51.011

Release 5(Spec is Withdrawn from this Release at T#17) **Latest Remark:** (2015-01-22) TP-16: Rel-5 version withdrawn.

Meetings	Version	Upload date	Comment
T#14	5.0.0	2002-01-17	TP-16: Rel-5 version withdraw...

Release 4(Spec is UCC for this Release) **Latest Remark:** (2015-01-22) TP-14: At TP-11 it was decided that there would be...

Meetings	Version	Upload date	Comment
CT#28	4.15.0	2005-06-15	
T#27	4.14.0	2005-03-24	
T#26	4.13.0	2005-01-03	
T#24	4.12.0	2004-06-15	
T#23	4.11.0	2004-03-26	
T#22	4.10.0	2004-01-12	
T#21	4.9.0	2003-09-29	
T#20	4.8.0	2003-06-23	
T#19	4.7.0	2003-04-04	
T#18	4.6.0	2003-01-02	
T#17	4.5.0	2002-09-18	
T#16	4.4.0	2002-06-25	
T#14	4.3.0	2002-01-17	

Exit

APPENDIX G

http://www.3gpp.org/ Go MAR APR MAY
4,530 captures
25 Jan 1999 - 28 Sep 2023
2004 2005 2006
About this capture

About 3GPP
Project Management
3gpp Work Plan
Technical Bodies
Terms &Abbreviations
Project Support
Specifications
Membership of 3GPP
Delegates Corner
Meetings
Contact 3GPP
Email Lists
FAQ



Shaping the future of mobile communication standards

News & info

- **NEW:** The RAN WG elections in May are postponed until the next regular meetings in August.
- GERAN election results: To be ratified by PCG in April
  GERAN Chairman: Mr Andrew HOWELL
  GERAN Vice Chairmen: Mr Juergen HOFMANN, Mr Guillaume SEBIRE, Mr Marc GRANT
- SA VC election results: To be ratified by PCG in April
  After 2 ballots, resulted in a tie between:
  Mr Hee Joung LEE and Mr Nick SAMPSON
  No candidate elected.
  Issue will be addressed by the PCG meeting in April.
- SA election results: To be ratified by PCG in April
  SA Chairman: Mr Stephen HAYES
  SA Vice Chairmen: Ms Yuhong HUANG, Mr Armin TOEPFER
- CT election results: To be ratified by PCG in April
  CT Chairman: Mr Hannu HIETALAHTI
  CT Vice Chairmen: Mr Akishige NODA, Mr Gary JONES, Mr Steve MECROW
- RAN election results: To be ratified by PCG in April
  RAN Chairman: Mr Francois COURAU
  RAN Vice Chairmen: Mr Don ZELMER, Mr Hyeon Woo LEE, Mr Takehiro NAKAMURA
- Mobile industry applauds latest 3G specifications
- What is UMTS? (overview of the content of Releases 99 to 5)
- 3GPP IETF Dependencies and Priorities
- Liaison statements

Click here for access to the 3GPP ftp site

Last update: 2005-04-22

Legal notice

APPENDIX H

http://www.3gpp.org/specs/specs.htm Go MAR APR MAY
570 captures
8 Jun 2002 - 13 Apr 2023
2004 23 2005 2006 About this capture

Quick link to the specifications file server area (http) for those who know where they are going!

To find a particular spec quickly, go here and click on the links in the spec-series in the table or use the links in the "further information" section.

The term "***3GPP specification***" covers all **GSM** (including **GPRS** and **EDGE**) and **W-CDMA** specifications. The following terms are also used to describe networks using the 3G specifications: **UTRAN**, **UMTS** (in Europe) and **FOMA** (in Japan). Revised versions of many of these specifications are produced up to four times a year following the quarterly TSG plenary meetings. (TSG GERAN meets five times a year.) See the table below which gives links to lists of specifications arising from each plenary TSG meeting since the freezing of Release 1999. The month of the meeting and the meeting number are shown in each case. Note that **the tables show only those specifications newly approved or modified at the meeting concerned**; they do *not* contain a complete list of all specifications current following the meeting. For such a list, consult the "status list" - see below.

Following each TSG SA plenary meeting, a complete set of specifications is produced. This set includes not only the new specifications generated at that meeting, but also the latest versions of each specification that was not changed at that meeting. i.e. each directory holds a complete set of specifications. Each set has an associated **status list** as detailed in the table below. Each set (and corresponding status list) includes the specs arising from the TSG GERAN meetings held since the preceding SA meeting. (GERAN meets asynchronously from the other TSGs.)

The **Status List** (ZIPped RTF or Word format) summarizes the current version number for every release of every 3GPP specification following each TSG plenary meeting. Also listed for each specifications are:

- the 3GPP working group and rapporteur responsible for the specification
- the Project Manager in MCC (Mobile Competence Centre) responsible for the specification
- the meeting at which it was, or is expected to be, "frozen" (i.e. the point after which only corrections are allowed)

Full details of the Specifications, their history and current status can be found in the 3GPP Specifications Status database.

year-month	remark	latest status	specs directory	TSG CN meeting number	TSG RAN meeting number	TSG T meeting number	TSG SA meeting number	TSG GERAN meeting number	TSG CT meeting number
2005-06					28		28		28
2005-04			ftp://ftp.3gpp.org/specs/2005-04-geran-mtg-24-delta/					24	
2005-03	RAN closed and (new) RAN opened. CN and T closed. CT opened.	StatusList	ftp://ftp.3gpp.org/specs/2005-03	27	27bis 27	27	27		27
2005-01			ftp://ftp.3gpp.org/specs/2005-01-geran-mtg-23-delta/					23	
2004-12		StatusList	ftp://ftp.3gpp.org/specs/2004-12	26	26	26	26		
2004-11			ftp://ftp.3gpp.org/specs/2004-11-geran-mtg-22-delta/					22	
2004-09		StatusList	ftp://ftp.3gpp.org/specs/2004-09/	25	25	25	25		
2004-08			ftp://ftp.3gpp.org/specs/2004-08-geran-mtg-21-delta/					21	
2004-06			ftp://ftp.3gpp.org/specs/2004-06-geran-mtg-20-delta/					20	
2004-06		StatusList	ftp://ftp.3gpp.org/specs/2004-06/	24	24	24	24		
2004-04			ftp://ftp.3gpp.org/specs/2004-04-geran-mtg-19-delta/					19	
2004-03		StatusList	ftp://ftp.3gpp.org/specs/2004-03/	23	23	23	23		
2004-02			ftp://ftp.3gpp.org/specs/2004-02-geran-mtg-18-delta					18	
2003-12		StatusList	ftp://ftp.3gpp.org/specs/2003-12/	22	22	22	22		

2003-11			ftp://ftp.3gpp.org/specs/2003-11-geran-mtg-17-delta					17	
2003-09		StatusList	ftp://ftp.3gpp.org/specs/2003-09/	21	21	21	21		
2003-09			ftp://ftp.3gpp.org/specs/2003-09-geran-mtg-16-delta					16	
2003-06			ftp://ftp.3gpp.org/specs/2003-06-geran-mtg-15-delta					15	
2003-06		StatusList	ftp://ftp.3gpp.org/specs/2003-06/	20	20	20	20		
2003-04			ftp://ftp.3gpp.org/specs/2003-04-geran-mtg-14-delta					14	
2003-02		StatusList	ftp://ftp.3gpp.org/specs/2003-03/	19	19	19	19		
2003-02			ftp://ftp.3gpp.org/specs/2003-02-geran-mtg-13-delta					13	
2002-12 2002-11		StatusList	ftp://ftp.3gpp.org/specs/2002-12/	18	18	18	18	12	
2002-09		StatusList	ftp://ftp.3gpp.org/specs/2002-09/	17	17	17	17	11	
2002-06	Rel-5 GERAN features content functionally frozen		ftp://ftp.3gpp.org/specs/2002-06-geran-mtg-10-delta/					10	
2002-06	Rel-5 features content functionally frozen (remainder, non-GERAN)	StatusList	ftp://ftp.3gpp.org/specs/2002-06/	16	16	16	16		
2002-04			ftp://ftp.3gpp.org/specs/2002-04-geran-mtg-09-delta/					9	
2002-03	Rel-5 features content functionally frozen (part)	StatusList	ftp://ftp.3gpp.org/specs/2002-03/	15	15	15	15		
2002-02								8	
2001-12		StatusList	ftp://ftp.3gpp.org/specs/2001-12/	14	14	14	14		
2001-11								7	
2001-09		StatusList	ftp://ftp.3gpp.org/specs/2001-09/	13	13	13	13		
2001-08								6	
2001-06		StatusList	ftp://ftp.3gpp.org/specs/2001-06/	12	12	12	12	5	
2001-06	Rel-4 GERAN features content functionally frozen							4	
2001-03	Rel-4 non-GERAN features content functionally frozen	StatusList	ftp://ftp.3gpp.org/specs/2001-03/	11	11	11	11		
2001-01								3	
2000-12 2000-11		StatusList	ftp://ftp.3gpp.org/specs/2000-12/	10	10	10	10	2	
2000-11									
2000-09		StatusList	ftp://ftp.3gpp.org/specs/2000-09/	9	9	9	9	1	
2000-06		StatusList	ftp://ftp.3gpp.org/specs/2000-06/	8	8	8	8		
2000-03				7	7	7	7		
1999-12	R99 features content functionally frozen			6	6	6	6		
1999-10				5	5	5	5		
1999-06					4	4	4		
1999-05				4					
1999-04				3	3	3	3		
1999-03				2	2	2	2		
1998-12				1	1	1	1		

If you plan to download a large number of specifications and are using MS Explorer 4.0 or earlier, it may be worthwhile acquiring an FTP client software tool such as:

- Ipswitch WS_FTP Pro® : This general purpose file transfer program simplifies the process of downloading large numbers of files from an FTP site.
- FTPSync®: This tool allow the user to specify a directory on their local disk and synchronize it with a directory on an FTP site.

For additional information relating to 3GPP Specifications, their creation and maintenance, etc, **go here**.



This page maintained by Specifications Manager.

last updated
2005-04-21: GP-24 directory included.
2005-04-19: Hyperlink for GP-24 list added.
2005-04-04: All TSG links changed as to point to auto pages.
2005-04-01: Links for TSGs#27 changed to point to experimental pages automatically generated from status database rather than manually maintained pages.
2005-03-29: early TSG meeting entries added; GERAN#24 and other TSGs#28 entries added (no hyperlinks); column for TSG CT added
2005-03-21: TSGs#27 added, charts updated
2005-02-01: GERAN#23 added
2005-01-26: broken link to chart fixed
2005-01-19: charts updated
2004-12-23: TSGs#25 added
2004-11-19: GERAN#22 added
2004-11-03: charts updated
2004-09-28: TSGs#25 added, link to 2004-06 status list corrected.
2004-09-01: GERAN#21 added
2004-08-02: Spec availability chart updated.
2004-07-01: GERAN#20 added
2004-06-18: TSGs 24 added
2004-05-07: GP-19 added; clarifications to introductory text above the table of meetings.
2004-04-14: Specs delivery chart updated.
2004-03-26: minor errors in hyperlinks fixed.
2004-03-22: table entry for TSGs 23 added.
2004-02-18: table entry for GP-18 added.
2004-01-27: chart of spec delivery added.
2004-01-05: table entry for TSGs 22 added.
2003-12-03: table entry for GP-17 added.
2003-10-21: "further information" section moved to the "numbering" page.
2003-09-26: table entries for GP-16 and other TSGs 'P-21 added
2003-08-18: broken link repaired, links to cited spec pages made relative.
2003-07-02: typo corrected
2003-06-26: Further GERAN#15 info added; minor cosmetic improvements to text; hyperlinks for identified specs are now to their info page, not their archive storage directory
2003-06-23 - CN, RAN, T, SA #20 info and preliminary GERAN#15 info added
2003-04-25 - GERAN#14 info added
2003-04-24 - quick link to spec series table page added near top; from this it is possible to get to lists of specs in each series, and thence to details of the individual specs.
2003-03-25 - table entry for TSGs#19 added
2003-02-24 - table entry for GERAN#13 added
2003-01-13 - link to CR trends page added.
2002-12-15 - TSGs#18 (GERAN#12) line added; quick link to specs file at top of page added.
2002-10-18 - reference to 3GPP Specifications Status database added.

APPENDIX I

http://www.3gpp.org/specs/numbering.htm
Go
MAR APR MAY
443 captures
11 Feb 2002 - 8 Jul 2023
2004 22 2005 2006
About this capture

3GPP Specifications - Numbering scheme

Spec download | Titles and spec numbers | Current version | Releases | Numbering scheme | Change Requests
Published specifications | Historical information | Work plan | TSG Working methods | Drafting rules | Delegates corner | ASN.1

All 3G and GSM specifications have a 3GPP specification number consisting of 4 or 5 digits. (e.g. 09.02 or 29.002). The first two digits define the series as listed in the table below. They are followed by **2** further digits for the 01 to 13 series or **3** further digits for the 21 to 55 series. The term "3G" means a 3GPP system using a UTRAN radio access network; the term "GSM" means a 3GPP system using a GERAN radio access network. (Thus "GSM" includes GPRS and EDGE features.)

The full title, specification number and latest version number for every specification can be found in the current status list [**warning: large file!**] (see also main specs page for status lists pertaining to each TSG SA meeting) and more information about terms such as R99 and Rel-4 can be found on the Releases and phases page.

A specification in the 21 to 35 series may apply either to 3G only or to GSM *and* 3G. A clue lies in the third digit, where a "0" indicates that it applies to both systems. For example, 29.002 applies to 3G and GSM systems whereas 25.101 and 25.201 apply only to 3G. Most specs in all other series apply only to GSM systems. However, as the spec numbering space has been used up, this guide is more frequently broken, and it is necessary to examine the information page for each spec (see the table below) or to check the lists in 01.01 / 41.101 (GSM) and 21.101 (3G) for the definitive specification sets for each system and each Release.

Subject of specification series	3G/GSM R99 and later	GSM only (Rel-4 and later)	GSM only (before Rel-4)
General information *(long defunct)*			00 series
Requirements	21 series	41 series	01 series
Service aspects ("stage 1")	22 series	42 series	02 series
Technical realization ("stage 2")	23 series	43 series	03 series
Signalling protocols ("stage 3") - user equipment to network	24 series	44 series	04 series
Radio aspects	25 series	45 series	05 series
CODECs	26 series	46 series	06 series
Data	27 series	47 series (none exists)	07 series
Signalling protocols ("stage 3") -(RSS-CN)	28 series	48 series	08 series
Signalling protocols ("stage 3") - intra-fixed-network	29 series	49 series	09 series
Programme management	30 series	50 series	10 series
User Identity Module (SIM / USIM)	31 series	51 series	11 series
O&M	32 series	52 series	12 series
Access requirements and test specifications		13 series (1)	13 series (1)
Security aspects	33 series	(2)	(2)
SIM and test specifications	34 series	(2)	*11 series*
Security algorithms (3)	35 series	55 series	(4)

Note (1): The 13 series GSM specifications relate to European-Union-specific regulatory standards. On the closure of ETSI TC SMG, responsibility for these specifications was transferred to ETSI TC MSG, (Mobile Specification Group) and they do not appear on the 3GPP file server.

Note (2): The specification of these aspects are spread throughout several series.

Note (3): Algorithms may be subject to export licencing conditions. See the relevant 3GPP page. See also the relevant ETSI pages.

Note (4): The original GSM algorithms are not published and are controlled by the GSM Association.

The 3GPP Specifications are stored on the file server as zipped MS-Word files. The filenames have the following structure:

SM[-P[-Q]]-V.zip

where the character fields have the following significance ...

S = series number - 2 characters (see the table above)
M = mantissa (the part of the spec number after the series number) - 2 or 3 characters (see above)
P = optional part number - 1 or 2 digits if present
Q = optional sub-part number - 1 or 2 digits if present
V = version number, without separating dots - 3 digits

So for example:
21900-320.zip is 3GPP TR 21.900 version 3.2.0
0408-6g0.zip is 3GPP TS 04.08 version 6.16.0
32111-4-410 is 3GPP TS 32.111 part 4 version 4.1.0
29998-04-1-100 is 3GPP TS 29.998 part 4 sub-part 1 version 1.0.0

Further information:

Latest version

The latest versions of the approved specifications in the "latest" directory. The latest version of draft specs (i.e. those not yet under change control) are in the "latest-drafts" directory.

Particular version

All older versions of specifications (where available) are stored in the archive subdirectory. All versions of all releases of a given specification are placed directly under the name of the specification.

Title or subject

If you only know the **title** or the subject, but not the specification number, the best place to start looking is the complete list of all 3GPP specification numbers and titles. This list also shows the most recent version in each Release.

Specs related to a particular working group

Each 3GPP TSG Working Group has a home page, which lists the specifications under its responsibility. Follow the links from here....

Official versions published by recognized Standards Development Organizations

The 3GPP Technical Specifications (and Technical Reports) which are publicly available from this site have, in themselves, no legal standing. They only become "official" when transposed into corresponding publications of the Partner Organizations. If you are looking for the **official versions**, see the official publications page.

Yet more information:

- **Work plan.** The 3GPP Work plan describes the new functionality currently being elaborated in the TSG working groups. It also indicates the expected timescales for their finalization.
- **Releases (and phases, stages).** An introduction to the 3GPP mechanism for specifications releases can be found here.
- **Historical information.** If you need to look for old / superseded specifications or change requests, start here.
- **TSG working methods.** The procedures for creating, enhancing and maintaining specifications are described in TR 21.900. A presentation outlining the release and change request process can be found here.
- **3GPP Drafting rules.** The rules for drafting specifications are described in TR 21.801.
- **Change Requests (CRs).** The change request mechanism is used when a correction or new functionality is required for an existing specification. Here you can find all information related to change requests.

---

last updated:
2004-08-02: missing bracket inserted
2004-03-02: typo in hyperlink to 45-series specs corrected.
2003-10-21: "further information" section originally in main specs page transferred to this page; sundry editorial improvements.
2003-09-10: links to current status list and to spec numbering system added.
2003-07-10: minor editorial clarifications
2003-06-27: 00.-series added to table; URLs to spec lists made relative rather than absolute (to aid site mirroring)
2003-09-26: minor corrections and clarifications
2003-04-24: links to specs series indexes added
2002-10-10: mention of 55 series specs added, plus notes 3 & 4.

APPENDIX J

http://www.3gpp.org/ftp/Specs/html-info/51-series.htm Go
70 captures
26 Jun 2003 - 19 Nov 2023
DEC 2004 MAR 08 2005 NOV 2006
About this capture

3GPP Specification series

Back to numbering scheme page

Click on spec number for details

TS 51.010-1	Mobile Station (MS) conformance specification; Part 1: Conformance specification	.
TS 51.010-2	Mobile Station (MS) conformance specification; Part 2: Protocol Implementation Conformance Statement (PICS) proforma specification	.
TS 51.010-3	Mobile Station (MS) conformance specification; Part 3: Layer3 (L3) Abstract Test Suite (ATS)	.
TS 51.010-4	Mobile Station (MS) conformance specification; Part 4: SIM Application Toolkit conformance specification	.
TS 51.010-5	Mobile Station (MS) conformance specification; Part 5: Inter-Radio-Access-Technology (RAT) (GERAN / UTRAN) interaction Abstract Test Suite (ATS)	.
TS 51.011	Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface	.
TS 51.013	Test specification for Subscriber Identity Module (SIM) Application Programming Interface (API) for Java Card	.
TS 51.014	Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface	.
TS 51.021	Base Station System (BSS) equipment specification; Radio aspects	.
TS 51.026	GSM Repeater Equipment Specification	.

APPENDIX K

http://www.3gpp.org/ftp/Specs/html-info/51011.htm Go
256 captures
18 Oct 2003 - 2 May 2026
DEC FEB MAR
2004 18 2005 2006
About this capture

3GPP Specification detail

Back to numbering scheme page

Back to series index

3GPP TS 51.011

Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface

.

TSG / WG responsible: **T3**

TP-14: talk of changing title to ""Characteristics of the SIM application"".

Rapporteur: **GUTHERY, Scott B.**

Specification required for: GERAN-based systems

Release	Freeze meeting	Freeze date	remarks
Rel-4	SP-11	2001-03-22	TP-14: At TP-11 it was decided that there would be no need for a Rel-5 version, since by then all terminals will handle a common USIM. But the question still seems to be open. TP-14: settled: there WILL be a Rel-5! TP-16: Rel-5 version withdrawn! .

	event	version	available	remarks
	TP-11	4.0.0	2001-04-09	
	TP-12	4.1.0	2001-07-06	
	TP-13	4.2.0	2001-10-11	
	TP-14	4.3.0	2002-01-17	
	TP-16	4.4.0	2002-06-25	
	TP-17	4.5.0	2002-09-18	
	TP-18	4.6.0	2003-01-02	
	TP-19	4.7.0	2003-04-04	
	TP-20	4.8.0	2003-06-23	
	TP-21	4.9.0	2003-09-29	
	TP-22	4.10.0	2004-01-12	
	TP-23	4.11.0	2004-03-26	
	TP-24	4.12.0	2004-06-15	
	TP-26	4.13.0	2005-01-03	
Rel-5	TP-15	2002-03-08	TP-16: Rel-5 version withdrawn. **RELEASE WITHDRAWN**	
	event	**version**	**available**	**remarks**
	TP-14	5.0.0	2002-01-17	TP-16: Rel-5 version withdrawn!

Change Requests for this spec: click here.

Genealogy of this spec:

antecedent(s)	this spec	descendant(s)
11.11	51.011	(no descendants)

APPENDIX L

http://www.3gpp.org/ftp/specs/archive/51_series/51.011/ Go
123 captures
20 Dec 2001 - 18 Jun 2025
DEC MAY SEP
2003 16 2004 2005
About this capture

www.3gpp.org - /ftp/Specs/archive/51_series/51.011/

[To Parent Directory]

09 April 2001	08:35	391714	51011-400.zip
06 July 2001	14:02	412456	51011-410.zip
11 October 2001	16:34	436693	51011-420.zip
17 January 2002	09:36	374369	51011-430.zip
24 June 2002	09:06	376481	51011-440.zip
17 September 2002	11:12	449988	51011-450.zip
02 January 2003	14:53	462367	51011-460.zip
20 March 2003	09:09	470779	51011-470.zip
13 June 2003	12:09	470435	51011-480.zip
29 September 2003	15:05	475342	51011-490.zip
12 January 2004	11:15	474462	51011-4a0.zip
26 March 2004	11:10	378110	51011-4b0.zip
17 January 2002	09:38	374531	51011-500.zip

APPENDIX M

ETSI TS 151 011 V4.10.0 (2003-12)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Specification of the Subscriber Identity Module -
Mobile Equipment (SIM-ME) interface
(3GPP TS 51.011 version 4.10.0 Release 4)



Reference
RTS/TSGT-0351011v4a0

Keywords
GSM

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2003.
All rights reserved.

DECT™, **PLUGTESTS**™ and **UMTS**™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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 (http://webapp.etsi.org/IPR/home.asp).

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 .

Contents

Intellectual Property Rights 2
Foreword 2
Foreword 9
1 Scope 10
2 References 10
3 Definitions, abbreviations and symbols 12
3.1 Definitions 12
3.2 Abbreviations 13
3.3 Symbols 15
4 Physical characteristics 15
5 Electronic signals and transmission protocols 15
5.1 Electrical specifications 16
5.2 Initial communication establishment procedures 16
5.2.1 Error handling for speed enhancement 16
5.3 Transmission protocols 16
5.4 Clock 17
6 Application and File structure 17
6.1 SIM Application structure 17
6.2 Void 18
6.3 Void 18
6.4 File types 18
6.4.1 Dedicated files 18
6.4.2 Elementary files 18
6.4.2.1 Cyclic EF 18
6.5 Methods for selecting a file 18
7 Security features 18
7.1 Authentication and cipher key generation procedure 18
7.2 Algorithms and processes 19
7.3 File access conditions 19
8 Void 20
9 Description of the commands 20
9.1 Mapping principles 20
9.2 Coding of the commands 22
9.2.1 SELECT 23
9.2.2 STATUS 25
9.2.3 READ BINARY 25
9.2.4 UPDATE BINARY 25
9.2.5 READ RECORD 26
9.2.6 UPDATE RECORD 26
9.2.7 SEEK 26
9.2.8 INCREASE 27
9.2.9 VERIFY CHV 27
9.2.10 CHANGE CHV 27
9.2.11 DISABLE CHV 28
9.2.12 ENABLE CHV 28
9.2.13 UNBLOCK CHV 28
9.2.14 INVALIDATE 28
9.2.15 REHABILITATE 29
9.2.16 RUN GSM ALGORITHM 29
9.2.17 SLEEP 29

9.2.18 GET RESPONSE....29
9.2.19 TERMINAL PROFILE....29
9.2.20 ENVELOPE....30
9.2.21 FETCH....30
9.2.22 TERMINAL RESPONSE....30
9.3 Definitions and coding....30
9.4 Status conditions returned by the card....31
9.4.1 Responses to commands which are correctly executed....31
9.4.2 Responses to commands which are postponed....31
9.4.3 Memory management....32
9.4.4 Referencing management....32
9.4.5 Security management....32
9.4.6 Application independent errors....32
9.4.7 Commands versus possible status responses....32
10 Contents of the Elementary Files (EF)....33
10.1 Contents of the EFs at the MF level....34
10.1.1 EF_{ICCID} (ICC Identification)....34
10.1.2 EF_{PL} (Preferred language)....34
10.2 DFs at the GSM application level....34
10.3 Contents of files at the GSM application level....34
10.3.1 EF_{LP} (Language preference)....34
10.3.2 EF_{IMSI} (IMSI)....35
10.3.3 EF_{Kc} (Ciphering key Kc)....36
10.3.4 $EF_{PLMNsel}$ (PLMN selector)....37
10.3.5 EF_{HPPLMN} (Higher Priority PLMN search period)....37
10.3.6 EF_{ACMmax} (ACM maximum value)....38
10.3.7 EF_{SST} (SIM service table)....39
10.3.8 EF_{ACM} (Accumulated call meter)....41
10.3.9 EF_{GID1} (Group Identifier Level 1)....42
10.3.10 EF_{GID2} (Group Identifier Level 2)....42
10.3.11 EF_{SPN} (Service Provider Name)....43
10.3.12 EF_{PUCT} (Price per unit and currency table)....44
10.3.13 EF_{CBMI} (Cell broadcast message identifier selection)....45
10.3.14 EF_{BCCH} (Broadcast control channels)....45
10.3.15 EF_{ACC} (Access control class)....46
10.3.16 EF_{FPLMN} (Forbidden PLMNs)....46
10.3.17 EF_{LOCI} (Location information)....47
10.3.18 EF_{AD} (Administrative data)....48
10.3.19 EF_{Phase} (Phase identification)....50
10.3.20 EF_{VGCS} (Voice Group Call Service)....50
10.3.21 EF_{VGCSS} (Voice Group Call Service Status)....52
10.3.22 EF_{VBS} (Voice Broadcast Service)....53
10.3.23 EF_{VBSS} (Voice Broadcast Service Status)....55
10.3.24 EF_{eMLPP} (enhanced Multi Level Pre-emption and Priority)....55
10.3.25 EF_{AAeM} (Automatic Answer for eMLPP Service)....56
10.3.26 EF_{CBMID} (Cell Broadcast Message Identifier for Data Download)....57
10.3.27 EF_{ECC} (Emergency Call Codes)....57
10.3.28 EF_{CBMIR} (Cell broadcast message identifier range selection)....59
10.3.29 EF_{DCK} De-personalization Control Keys....59
10.3.30 EF_{CNL} (Co-operative Network List)....60
10.3.31 EF_{NIA} (Network's Indication of Alerting)....61
10.3.32 EF_{KcGPRS} (GPRS Ciphering key KcGPRS)....61
10.3.33 $EF_{LOCIGPRS}$ (GPRS location information)....62
10.3.34 EF_{SUME} (SetUpMenu Elements)....63
10.3.35 $EF_{PLMNwAcT}$ (User controlled PLMN Selector with Access Technology)....64
10.3.36 $EF_{OPLMNwAcT}$ (Operator controlled PLMN Selector with Access Technology)....65
10.3.37 $EF_{HPLMNwAcT}$ (HPLMN Selector with Access Technology)....66
10.3.38 EF_{CPBCCH} (CPBCCH Information)....66
10.3.39 $EF_{InvScan}$ (Investigation Scan)....67
10.3.40 Void....68
10.3.41 EF_{PNN} (PLMN Network Name)....68

10.3.42 EF_{OPL} (Operator PLMN List) 68
10.3.43 EF_{MBDN} (Mailbox Dialling Numbers) 69
10.3.44 EF_{MBI} (Mailbox Identifier) 70
10.3.45 EF_{MWIS} (Message Waiting Indication Status) 71
10.3.46 EF_{CFIS} (Call Forwarding Indication Status) 72
10.3.47 EF_{EXT5} (Extension5) 73
10.3.48 EF_{EXT6} (Extension6) 73
10.3.49 EF_{EXT7} (Extension7) 73
10.3.50 EF_{SPDI} (Service Provider Display Information) 73
10.3.51 EF_{MMSN} (MMS Notification) 74
10.3.52 EF_{EXT8} (Extension 8) 76
10.3.53 EF_{MMSICP} (MMS Issuer Connectivity Parameters) 76
10.3.54 EF_{MMSUP} (MMS User Preferences) 78
10.3.55 EF_{MMSUCP} (MMS User Connectivity Parameters) 79
10.4 Contents of DFs at the GSM application level 80
10.4.1 Contents of files at the GSM SoLSA level 80
10.4.1.1 EF_{SAI} (SoLSA Access Indicator) 80
10.4.1.2 EF_{SLL} (SoLSA LSA List) 81
10.4.1.3 LSA Descriptor files 83
10.4.2 Contents of files at the MExE level 84
10.4.2.1 $EF_{MExE-ST}$ (MExE Service table) 84
10.4.2.2 EF_{ORPK} (Operator Root Public Key) 85
10.4.2.3 EF_{ARPK} (Administrator Root Public Key) 87
10.4.2.4 EF_{TPRPK} (Third Party Root Public key) 87
10.4.2.5 Trusted Key/Certificates Data Files 88
10.5 Contents of files at the telecom level 88
10.5.1 EF_{ADN} (Abbreviated dialling numbers) 88
10.5.2 EF_{FDN} (Fixed dialling numbers) 92
10.5.3 EF_{SMS} (Short messages) 92
10.5.4 Capability configuration parameters 93
10.5.4.1 EF_{CCP} (Capability configuration parameters) 93
10.5.4.2 EF_{ECCP} (Extended Capability Configuration Parameters) 94
10.5.5 EF_{MSISDN} (MSISDN) 94
10.5.6 EF_{SMSP} (Short message service parameters) 95
10.5.7 EF_{SMSS} (SMS status) 96
10.5.8 EF_{LND} (Last number dialled) 97
10.5.9 EF_{SDN} (Service Dialling Numbers) 98
10.5.10 EF_{EXT1} (Extension1) 98
10.5.11 EF_{EXT2} (Extension2) 100
10.5.12 EF_{EXT3} (Extension3) 100
10.5.13 EF_{BDN} (Barred Dialling Numbers) 100
10.5.14 EF_{EXT4} (Extension4) 101
10.5.15 EF_{SMSR} (Short message status reports) 101
10.5.16 EF_{CMI} (Comparison Method Information) 102
10.6 DFs at the telecom level 103
10.6.1 Contents of files at the telecom graphics level 103
10.6.1.1 EF_{IMG} (Image) 103
10.6.1.2 Image Instance Data Files 105
10.7 Files of GSM 105

11 Application protocol 107
11.1 General procedures 109
11.2 SIM management procedures 109
11.2.1 SIM initialization 109
11.2.2 GSM session termination 111
11.2.3 Emergency Call Codes 112
11.2.4 Language preference 112
11.2.5 Administrative information request; 112
11.2.6 SIM service table request 112
11.2.7 SIM phase request 112
11.2.8 SIM Presence Detection and Proactive Polling 112
11.2.9 Preferred Language 112

11.3 CHV related procedures 112
11.3.1 CHV verification 113
11.3.2 CHV value substitution 113
11.3.3 CHV disabling 113
11.3.4 CHV enabling 113
11.3.5 CHV unblocking 114
11.4 GSM security related procedures 114
11.4.1 GSM algorithms computation 114
11.4.2 IMSI request 114
11.4.3 Access control request 114
11.4.4 Higher Priority PLMN search period request 114
11.4.5 Location information 114
11.4.6 Cipher key 114
11.4.7 BCCH information 114
11.4.8 Forbidden PLMN 115
11.4.9 LSA information 115
11.4.10 GPRS Location information 115
11.4.11 GPRS Cipher key 115
11.5 Subscription related procedures 115
11.5.1 Dialling numbers 115
11.5.2 Short messages 118
11.5.3 Advice of Charge (AoC) 118
11.5.4 Capability configuration parameters 118
11.5.5 PLMN selector 119
11.5.6 Cell broadcast message identifier 119
11.5.7 Group identifier level 1 119
11.5.8 Group identifier level 2 119
11.5.9 Service Provider Name 119
11.5.10 Voice Group Call Services 119
11.5.11 Voice Broadcast Services 119
11.5.12 Enhanced Multi Level Pre-emption and Priority Service 120
11.5.13 Cell Broadcast Message range identifier 120
11.5.14 Depersonalisation Control Keys 120
11.5.15 Short message status report 120
11.5.16 Network's indication of alerting 120
11.5.17 User controlled PLMN Selector with Access Technology 121
11.5.18 Operator controlled PLMN Selector with Access Technology 121
11.5.19 HPLMN Selector with Access Technology 121
11.5.20 CPBCCH information 121
11.5.21 Investigation Scan 121
11.5.22 Void 121
11.5.23 PLMN Network Name 121
11.5.24 Operator PLMN List 121
11.5.25 Message Waiting Indication 121
11.5.26 Call Forwarding Indication Status 122
11.5.27 Service Provider Display Information 122
11.5.28 MMS Notifications 122
11.5.29 MMS Issuer Connectivity Parameters 122
11.5.30 MMS User Preferences 123
11.5.31 MMS User Connectivity Parameters 123
11.6 SIM Application Toolkit related procedures 123
11.6.1 Initialization procedure 123
11.6.2 Proactive polling 123
11.6.3 Support of commands 123
11.6.4 Support of response codes 123
11.6.5 Command-response pairs 124
11.6.6 Independence of normal GSM and SIM Application Toolkit tasks 124
11.6.7 Use of BUSY status response 124
11.6.8 Use of NULL procedure byte 124
11.6.9 Using the TERMINAL PROFILE, ENVELOPE, and TERMINAL RESPONSE commands 124
11.6.10 Using the FETCH command 124
11.6.11 Data Download via SMS-CB 125

11.6.12 Data Download via SMS-PP 125
11.6.13 Menu selection 125
11.6.14 Call Control 125
11.6.15 Proactive SIM 125
11.6.16 Mobile Originated Short Message control by SIM 125
11.6.17 SIM data download error 125
11.6.18 Image Request 125
11.7 MExE related procedures 126
11.7.1 MExE ST 126
11.7.2 Operator root public key 126
11.7.3 Administrator root public key 126
11.7.4 Third Party root public key(s) 126

Annex A (normative): Void 127

Annex B (normative): Void 128

Annex C (informative): FDN/BDN Procedures 129

Annex D (informative): Suggested contents of the EFs at pre-personalization 134

Annex E (informative): SIM application Toolkit protocol diagrams 137

Annex F (informative): Examples of coding of LSA Descriptor files for SoLSA 144

Annex G (normative): Image Coding Schemes 145

G.1 Basic Image Coding Scheme 145

G.2 Colour Image Coding Scheme 146

Annex H (normative): Coding of EFs for NAM and GSM-AMPS Operational Parameters 148

H.1 Elementary File Definitions and Contents 148
H.1.1 EF_{MIN} (Mobile Identification Number) 148
H.1.2 EF_{ACCOLC} (Access Overload Class) 148
H.1.3 EF_{SID} (System ID Of Home System) 149
H.1.4 EF_{IPC} (Initial Paging Channel) 149
H.1.5 EF_{GPI} (Group ID) 150
H.1.6 $EF_{S\text{-}ESN}$ (SIM Electronic Serial Number) 150
H.1.7 EF_{COUNT} (Call Count) 151
H.1.8 EF_{PSID} (Positive/Favoured SID list) 151
H.1.9 EF_{NSID} (Negative/Forbidden SID List) 152
H.1.10 EF_{SPL} (Scanning Priority List) 153
H.1.11 EF_{NETSEL} (Network Selection Activation Flag) 154
H.1.12 EF_{CSID} (Current/Last Registered SID) 155
H.1.13 $EF_{REG\text{-}THRESH}$ (Registration Threshold) 155
H.1.14 EF_{CCCH} (Current Control Channel) 156
H.1.15 EF_{LDCC} (Latest DCC) 156
H.1.16 $EF_{GSM\text{-}RECON}$ (GSM Reconnect Timer) 156
H.1.17 $EF_{AMPS\text{-}2\text{-}GSM}$ (AMPS to GSM Rescan Timing Table) 157
H.1.18 EF_{*FC1} (Feature Activation Codes) 157
H.1.19 $EF_{AMPS\text{-}UI}$ (AMPS USAGE INDICATORS) 158

H.2 Authentication Functionality 159
H.2.1 A-KEY (ANSI-41 Authentication Key) 159
H.2.2 SSD (Shared Secret Data) 159

H.3 Authentication commands 159
H.3.1 Generation of Authentication Signature Data and Ciphering Keys 160
H.3.2 Validation and Storage of Entered A-Key's 161
H.3.3 Ask Random Task 161
H.3.4 Update Shared Secret Data 162
H.3.5 Confirm Shared Secret Data 162

H.3.6 CMEA Encryption of Voice Channel Data Digits 162
H.3.7 SIM Status Codes 163

Annex I (informative): EF changes via Data Download or SIM Toolkit applications 164

Annex J (informative): Tags defined in the present document 167

Annex K (informative): Example of MMS coding 168
K.1 Coding example for MMS User Preferences 168
K.2 Coding Example for MMS Issuer/User Connectivity Parameters 168

Annex L (informative): Change history 170

History 173

Foreword

This Technical Specification 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 interface between the Subscriber Identity Module (SIM) and the Mobile Equipment (ME) for use during the network operation phase of GSM as well as those aspects of the internal organization of the SIM which are related to the network operation phase. This is to ensure interoperability between a SIM and an ME independently of the respective manufacturers and operators. The concept of a split of the Mobile Station (MS) into these elements as well as the distinction between the GSM network operation phase, which is also called GSM operations, and the administrative management phase are described in the TS 02.17 [6]. The requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols are all defined in accordance with the TS 31.101 [55] except when stated otherwise in the present document.

The present document defines:

- the model which shall be used as a basis for the design of the logical structure of the SIM;
- the security features;
- the interface functions;
- the commands;
- the contents of the files required for the GSM application;
- the application protocol.

The present document does not specify any aspects related to the administrative management phase. Any internal technical reallocation of either the SIM or the ME are only specified where these reflect over the interface. It does not specify any of the security algorithms which may be used.

The present document defines the SIM/ME interface for GSM Phase 2. While all attempts have been made to maintain phase compatibility, any issues that specifically relate to Phase 1 should be referenced from within the relevant Phase 1 specification.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[3] Void.

[4] 3GPP TS 02.09: "Security aspects".

[5] 3GPP TS 22.011: "Service accessibility".

[6] 3GPP TS 42.017: "Subscriber Identity Modules (SIM); Functional characteristics".

[7] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[8] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[9] 3GPP TS 22.086: "Advice of Charge (AoC) Supplementary Services - Stage 1".

[10] 3GPP TS 23.003: "Numbering, addressing and identification".

[11] 3GPP TS 43.020: "Security related network functions".

[12] 3GPP TS 23.038: "Alphabets and language-specific information".

[13] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[14] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[15] Void.

[16] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[17] GSM 09.91: "Digital cellular telecommunications system (Phase 2); Interworking aspects of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface between Phase 1 and Phase 2".

[18] ITU-T Recommendation E.118: "The international telecommunication charge card".

[19] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[20] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange".

[21] ISO/IEC 7810 (1995): "Identification cards - Physical characteristics".

[22] ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing".

[23] ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".

[24] ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".

[25] ISO/IEC 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and locations of the contacts".

[26] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".

[27] 3GPP TS 51.014: "Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[28] GSM 11.12: "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[29] 3GPP TS 22.022: "Personalization of Mobile Equipment (ME); Mobile functionality specification".

[30] ISO 639 (1988): "Code for the representation of names of languages".

[31] ISO/IEC 10646-1 (1993): "Information technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane".

[32] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[33] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2".

[34] GSM 11.19: "Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile Station".

[35] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

[36] TIA/EIA-136-005: "Introduction, Identification, and Semi-Permanent Memory, November 1998".

[37] TIA/EIA-136-123-A: "Digital Control Channel Layer 3, November 1998".

[38] TIA/EIA-136-140-A: "Analogue Control Channel, November 1998".

[39] TIA/EIA-136-510-A: "Authentication, Encryption of Signaling Information/User Data and Privacy, November 1998".

[40] ANSI TIA/EIA-41: "Cellular Radio Telecommunications Intersystem Operations".

[41] EIA/TIA-553: "Mobile Station - Land Station Compatibility Specification".

[42] 3GPP TS 22.067: "enhanced Multi Level Precedence and Pre-emption service (eMLPP) - Stage 1".

[43] TR45 AHAG "Common Cryptographic Algorithms, Revision C," October 27, 1998.

[44] ETS 300 812: "Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM - ME) interface".

[45] 3GPP TS 03.22: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[46] 3GPP TS 05.05: "Radio transmission and reception".

[47] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[48] 3GPP TS 04.18: "Mobile radio interface layer 3 specification; Radio Resource Control Protocol".

[49] 3GPP TS 04.60: "General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/ Medium Access Control (RLC/MAC) protocol".

[50] 3GPP TS 23.057: "Mobile Execution Environment (MExE); Functional description; Stage 2".

[51] 3GPP TS 23.122: "NAS Functions related to Mobile Station (MS) in idle mode".

[52] 3GPP TS 31.102: "Characteristics of the USIM Application".

[53] 3GPP TS 22.101: "Service aspects; Service principles".

[54] 3GPP TS 23.097: "Multiple Subscriber Profile (MSP) (Phase 2) - Stage 2".

[55] 3GPP TS 31.101: "UICC-Terminal interface; Physical and logical characteristics"

[56] ISO/IEC 8825 (1990): "Information technology; Open Systems Interconnection; Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)"

[57] ETSI TS 102 221: "UICC-Terminal interface; Physical and logical characteristics"

[58] 3GPP TS 23.140: "Multimedia Messaging Service (MMS); Functional description; stage 2".

[59] 3GPP TS 44.018: "Mobile Radio Interface Layer 3 Specification; Radio Resource Control Protocol".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

access conditions: set of security attributes associated with a file

application: application consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols)

application protocol: set of procedures required by the application

card session: link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card

current directory: latest MF or DF selected

current EF: latest EF selected

data field: obsolete term for Elementary File

Dedicated File (DF): file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files (DFs)

directory: general term for MF and DF

Elementary File (EF): file containing access conditions and data and no other files

file: directory or an organized set of bytes or records in the SIM

file identifier: 2 bytes which address a file in the SIM

GSM, DCS 1800 or PCS 1900 application: set of security mechanisms, files, data and protocols required by GSM, DCS 1800 or PCS 1900

GSM session: that part of the card session dedicated to the GSM operation

IC card SIM: obsolete term for ID-1 SIM

ID-1 SIM: SIM having the format of an ID-1 card (see ISO 7816-1 [24])

Master File (MF): unique mandatory file containing access conditions and optionally DFs and/or EFs

normal GSM operation: relating to general, CHV related, GSM security related and subscription related procedures

padding: one or more bits appended to a message in order to cause the message to contain the required number of bits or bytes

plug-in SIM: Second format of SIM (specified in clause 4)

proactive SIM: SIM which is capable of issuing commands to the ME. Part of SIM Application Toolkit (see clause 11)

record: string of bytes within an EF handled as a single entity (see clause 6)

record number: number which identifies a record within an EF

record pointer: pointer which addresses one record in an EF

root directory: obsolete term for Master File

SIM application toolkit procedures: defined in TS 51.014 [27]

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply, in addition to those listed in TR 21.905 [2]:

A3	Algorithm 3, authentication algorithm; used for authenticating the subscriber
A38	A single algorithm performing the functions of A3 and A8
A5	Algorithm 5, cipher algorithm; used for enciphering/deciphering data
A8	Algorithm 8, cipher key generator; used to generate K_c
ACM	Accumulated Call Meter
ADM	Access condition to an EF which is under the control of the authority which creates this file

ADN	Abbreviated Dialling Number
AHAG	Ad-Hoc Authentication Group
A-Key	Authentication Key
ALW	ALWays
AMPS	Analogue Mobile Phone System
ANSI	American National Standards Institute
AoC	Advice of Charge
APDU	Application Protocol Data Unit
ATR	Answer To Reset
BCCH	Broadcast Control CHannel
BCD	Binary Coded Decimal
BDN	Barred Dialling Number
BTS	Base Transmitter Station
CB	Cell Broadcast
CBMI	Cell Broadcast Message Identifier
CCP	Capability/Configuration Parameter
CHV	Card Holder Verification information; access condition used by the SIM for the verification of the identity of the user
CLA	CLAss
CNL	Co-operative Network List
CPBCCH	COMPACT Packet BCCH
CTS	Cordless Telephony System
DCK	De-personalization Control Keys
DCS	Digital Cellular System
DF	Dedicated File (abbreviation formerly used for Data Field)
DTMF	Dual Tone Multiple Frequency
ECC	Emergency Call Code
EF	Elementary File
EIA	Electronics Industries Alliance (North America)
eMLPP	enhanced Multi-Level Precedence and Pre-emption Service
ETSI	European Telecommunications Standards Institute
etu	elementary time unit
FDN	Fixed Dialling Number
GSM	Global System for Mobile communications
HPLMN	Home PLMN
IC	Integrated Circuit
ICC	Integrated Circuit(s) Card
ID	IDentifier
IEC	International Electrotechnical Commission
IEI	Information Element Identifier
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
Kc	Cryptographic key; used by the cipher A5
Ki	Subscriber authentication key; the cryptographic key used by the authentication algorithm, A3, and cipher key generator, A8
LAI	Location Area Information; information indicating a cell or a set of cells
lgth	The (specific) length of a data unit
LND	Last Number Dialled
LSA	Localised Service Area
LSA ID	Localised Service Area Identity
LSB	Least Significant Bit
MCC	Mobile Country Code
ME	Mobile Equipment
MF	Master File
MMI	Man Machine Interface
MNC	Mobile Network Code
MS	Mobile Station
MSB	Most Significant Bit
MSISDN	Mobile Station international ISDN number
NAM	Numeric Assignment Module
NET	NETwork
NEV	NEVer

NPI	Numbering Plan Identifier
OFM	Operational Feature Monitor
OPLMN	Operator Controlled PLMN (Selector List)
OTA	Over The Air
PDC	Personal Digital Communications
PIN/PIN2	Personal Identification Number / Personal Identification Number 2 (obsolete terms for CHV1 and CHV2, respectively)
PLMN	Public Land Mobile Network
PPS	Protocol and Parameter Select (response to the ATR)
PUK/PUK2	PIN Unblocking Key / PIN2 Unblocking Key (obsolete terms for UNBLOCK CHV1 and UNBLOCK CHV2, respectively)
RAND	A RANDom challenge issued by the network
RFU	Reserved for Future Use
SDN	Service Dialling Number
SID	System IDentity
SIM	Subscriber Identity Module
SMS	Short Message Service
SoLSA	Support of Localised Service Area
SRES	Signed RESponse calculated by a SIM
SSC	Supplementary Service Control string
SW1/SW2	Status Word 1 / Status Word 2
TETRA	TErrestrial Trunk RAdio
TIA	Telecommunications Industries Association (North America)
TMSI	Temporary Mobile Subscriber Identity
TON	Type Of Number
TP	Transfer layer Protocol
TPDU	Transfer Protocol Data Unit
TS	Technical Specification
UNBLOCK CHV1/2	value to unblock CHV1/CHV2
VBS	Voice Broadcast Service
VGCS	Voice Group Call Service
VPLMN	Visited PLMN

3.3 Symbols

For the purposes of the present document, the following symbols apply:

'0' to '9' and 'A' to 'F'	the sixteen hexadecimal digits
Vcc	Supply voltage
Vpp	Programming voltage

4 Physical characteristics

Two physical types of SIM are specified. These are the "ID-1 SIM" and the "Plug-in SIM".

The physical characteristics of both types of SIM shall be in accordance with those specified for the UICC in TS 31.101 [55]

5 Electronic signals and transmission protocols

The present document contains references to the 3GPP UICC/Terminal interface specification, TS 31.101 [55]. For the requirements of TS 31.101 [55] which are referenced by the present specification, the usage of the term "UICC" shall be equivalent to the term "SIM".

5.1 Electrical specifications

Electrical specifications of the SIM – ME interface shall be in accordance with TS 31.101 [55] with the following limitations:

4MHz shall be the maximum clock speed specified for SIMs for 3V and below.

Power consumption during a SIM session and initial communication establishment i.e during the ATR shall not exceed the values defined for the ATR in TS 31.101 [55].

5.2 Initial communication establishment procedures

Initial communication establishment procedures shall be in accordance with TS 31.101 [55] with the following limitations.

Since 4MHz is the maximum clock speed specified for SIMs for 3V and below, the respective limitations on power consumption given in TS 31.101 [55] apply.

ATR content: The ME shall invoke the error handling as defined in TS 31.101 [55] if a SIM indicates other values than 0 or 255 in TC1. T=15 global interface parameters are optional. The coding of the historical bytes may not follow TS 31.101 [55] and need not to be interpreted by the ME.

PPS proceedures: Speed enhancement is optional for the SIM. However if speed enhancement is implemented at least F=512 and D=8 shall be supported.

Reset procedures: The SIM shall behave as a "Type 1 UICC".

Clock stop mode: The clock shall only be switched off subject to the conditions specified in the file characteristics (see clause 9.2.1). It is mandatory for a SIM operating at Class B or C operating conditions as defined in TS 31.101 [55] to support clock stop mode.

5.2.1 Error handling for speed enhancement

If the SIM does not answer the PPS request within the initial waiting time the ME shall reset the SIM. After two failed PPS attempts using F=512 and D=8 or values indicated in TA1, (no PPS response from the SIM) the ME shall initiate PPS procedure using default values. If this also fails (no PPS response from the SIM) the ME may proceed using default values without requesting PPS.

If the SIM does not support the values requested by the ME, the SIM shall respond to the PPS request indicating the use of default values.

5.3 Transmission protocols

Physical and Data link layer of the Transmission Protocols shall be in accordance with TS 31.101 [55] with the following limitations.

The support of the Transmission Protocol T=0 is mandatory for ME and the SIM. All other protocols are optional. Use of other protocols than T=0 is not defined in the present document.

In addition to the requirements specified in TS 31.101 [55], SIM cards and terminals compliant with the present document shall be ready to receive data no more than 12 etus after the leading edge of the start bit of the last outgoing character of any transmission that it originates. For the purpose of the present document, SIM cards and terminals only need to wait for 12 etus after the leading edge of the start bit of the last character received before transmitting data.

Procedure bytes '61' and '6C' shall not be used with GSM commands. Status byte '9F' is returned instead by the SIM to control exchanges between the Transport Layer of the terminal and the SIM.

5.4 Clock

If a frequency of 13/4 MHz is needed by the SIM to run the authentication procedure in the allotted time (see TS 03.20 [11]), or to process an ENVELOPE command used for SIM Data Download, bit 2 of byte 1 in the file characteristics shall be set to 1. Otherwise a minimum frequency of 13/8 MHz may be used.

6 Application and File structure

This clause describes the logical structure for a SIM if different from that specified in TS 31.101 [55], the code associated with it, and the structure of files used.

A file is associated with attributes that depending of the file type indicates how data is to be accessed e.g. file size, record length etc. Although in the present document some files and data structures stored in a file are indicated as having a fixed length; when reading such structures the terminal shall derive the length of the structure from the attributes provided in the file information i.e. not use the fixed value specified for the file in the present document. Although the terminal is able to read the entire structure it should only use those elements from the structure which is recognised by the terminal.

6.1 SIM Application structure

Figure 3 shows the general structural relationships which may exist between files. The files are organized in a hierarchical structure and are of one of the types as defined in TS 31.101 [55]. These files may be either administrative or application specific. The operating system handles the access to the data stored in different files.

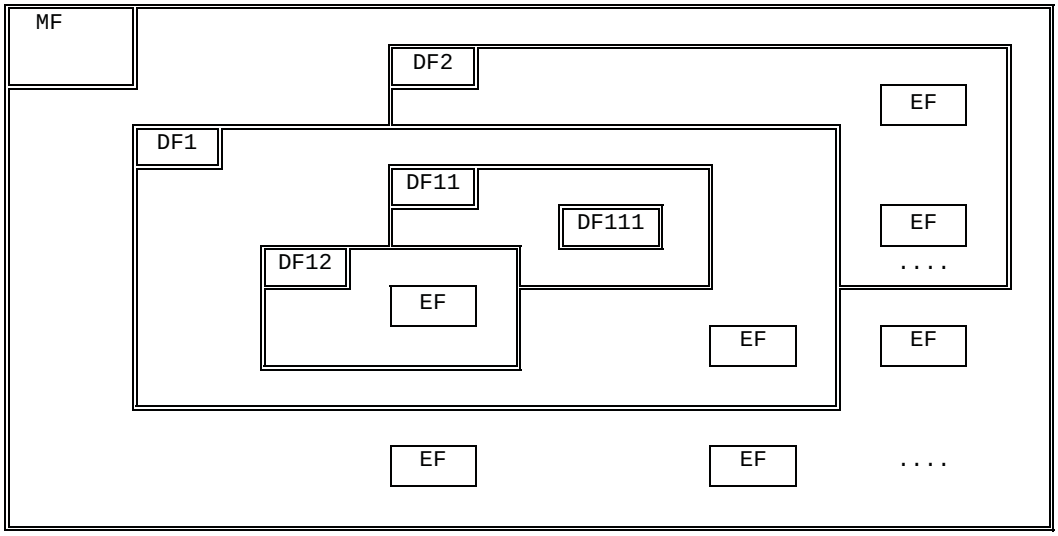


Figure 3: Organization of memory

Files are composed of a header, which is internally managed by the SIM, and optionally a body part. The information of the header is related to the structure and attributes of the file and may be obtained by using the commands GET RESPONSE or STATUS. This information is fixed during the administrative phase. The body part contains the data of the file.

6.2 Void

6.3 Void

6.4 File types

The SIM shall support the file types as defined in TS 31.101 [55] with the following limitations.

6.4.1 Dedicated files

The SIM does not support the operations that can be performed on an ADF as defined in TS 31.101 [55], although the SIM application DF is considered to be an ADF according to the definitions in TS 31.101 [55].

6.4.2 Elementary files

The SIM supports the elementary files as defined in TS 31.101 [55] with the following limitations

6.4.2.1 Cyclic EF

After selection of a cyclic file (for either operation), the record pointer shall address the record updated or increased last. If an action following selection of a record is aborted, then the record pointer shall remain set at the record at which it was set prior to the action.

6.5 Methods for selecting a file

After the Answer To Reset (ATR), the Master File (MF) is implicitly selected and becomes the Current Directory. Each file may then be selected by using the SELECT function as specified in TS 31.101 [55] with the following exception:

- Only support selection by file ID referencing and the command parameters as specified in the present document.

7 Security features

The security aspects of GSM are described in the normative references TS 02.09 [4] and TS 03.20 [11]. This clause gives information related to security features supported by the SIM to enable the following:

- authentication of the subscriber identity to the network;
- data confidentiality over the radio interface;
- file access conditions.

7.1 Authentication and cipher key generation procedure

This clause describes the authentication mechanism and cipher key generation which are invoked by the network. For the specification of the corresponding procedures across the SIM/ME interface see clause 11.

The network sends a Random Number (RAND) to the MS. The ME passes the RAND to the SIM in the command RUN GSM ALGORITHM. The SIM returns the values SRES and Kc to the ME which are derived using the algorithms and processes given below. The ME sends SRES to the network. The network compares this value with the value of SRES which it calculates for itself. The comparison of these SRES values provides the authentication. The value Kc is used by the ME in any future enciphered communications with the network until the next invocation of this mechanism.

A subscriber authentication key Ki is used in this procedure. This key Ki has a length of 128 bits and is stored within the SIM for use in the algorithms described below.

7.2 Algorithms and processes

The names and parameters of the algorithms supported by the SIM are defined in TS 03.20 [11]. These are:

- Algorithm A3 to authenticate the MS to the network;
- Algorithm A8 to generate the encryption key.

These algorithms may exist either discretely or combined (into A38) within the SIM. In either case the output on the SIM/ME interface is 12 bytes. The inputs to both A3 and A8, or A38, are Ki (128 bits) internally derived in the SIM, and RAND (128 bits) across the SIM/ME interface. The output is SRES (32 bits)/Kc (64 bits) the coding of which is defined in the command RUN GSM ALGORITHM in clause 9.

7.3 File access conditions

Every file has its own specific access condition for each command. The relevant access condition of the last selected file shall be fulfilled before the requested action can take place.

For each file:

- the access conditions for the commands READ and SEEK are identical;
- the access conditions for the commands SELECT and STATUS are ALWays.

No file access conditions are currently assigned by GSM to the MF and the DFs.

The access condition levels are defined in the following table:

Table 7: Access condition level coding

Level	Access Condition
0	ALWays
1	CHV1
2	CHV2
3	Reserved for GSM Future Use
4 to 14	ADM
15	NEVer

The meaning of the file access conditions is as follows:

ALWAYS: The action can be performed without any restriction;

CHV1 (card holder verification 1): The action shall only be possible if one of the following three conditions is fulfilled:

- a correct CHV1 value has already been presented to the SIM during the current session;
- the CHV1 enabled/disabled indicator is set to "disabled";

NOTE: Some Phase 1 and Phase 2 SIMs do not necessarily grant access when CHV1 is "disabled" and "blocked".

- UNBLOCK CHV1 has been successfully performed during the current session;

CHV2: The action shall only be possible if one of the following two conditions is fulfilled:

- a correct CHV2 value has already been presented to the SIM during the current session;
- UNBLOCK CHV2 has been successfully performed during the current session;

ADM: Allocation of these levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority

The definition of access condition ADM does not preclude the administrative authority from using ALW, CHV1, CHV2 and NEV if required.

NEVER: The action cannot be performed over the SIM/ME interface. The SIM may perform the action internally.

Condition levels are not hierarchical. For instance, correct presentation of CHV2 does not allow actions to be performed which require presentation of CHV1. A condition level which has been satisfied remains valid until the end of the GSM session as long as the corresponding secret code remains unblocked, i.e. after three consecutive wrong attempts, not necessarily in the same card session, the access rights previously granted by this secret code are lost immediately. A satisfied CHV condition level applies to both DF_{GSM} and $DF_{TELECOM}$.

The ME shall determine whether CHV2 is available by using the response to the STATUS command. If CHV2 is "not initialized" then CHV2 commands, e.g. VERIFY CHV2, shall not be executable.

8 Void

9 Description of the commands

The command description and structure is defined in TS 31.101 [55]. The coding of the CLA, INS and parameter bytes are according to TS 31.101 [55] with the limitations stated in the command description in the present document.This clause states the general principles for mapping the commands and responses onto Application Protocol Data Units which are used by the transmission protocol.

9.1 Mapping principles

The mapping of protocol T=0 with respect to the TPDU level is according to TS 31.101 [55] with the following exceptions:

- The use of procedure byte '6C' for Case 2 commands as defined in TS 31.101 [55] shall be replaced by the usage of '9F' as described in case 2b below. According to the present document the status byte '9F' triggers a GET RESPONSE command whereas the procedure byte '6C' in TS 31.101 [55] triggers re-issuing of the same command.

- The use of procedure byte '61' for Case 4 commands as defined in TS 31.101 [55] shall be replaced by the usage of '9F' as described in case 4 below. According to the present document the status byte '9F' triggers one GET RESPONSE command, which is optional for the ME, whereas the procedure byte '61' in TS 31.101 [55] triggers one or more GET RESPONSE commands depending upon the procedure bytes following the GET RESPONSE command.

For some commands described in the present document it is necessary for T=0 to use a supplementary transport service command (GET RESPONSE) to obtain the output data. For example, the SELECT function needs the following two commands:

- the first command (SELECT) has both parameters and data serving as input for the function;

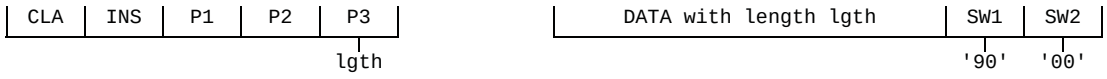
- the second command (GET RESPONSE) has a parameter indicating the length of the data to be returned.

If the length of the response data is not known beforehand, then its correct length may be obtained by applying the first command and interpreting the status words. SW1 shall be '9F' and SW2 shall give the total length of the data. Other status words may be present in case of an error. The various cases are:

Case 1: No input / No output

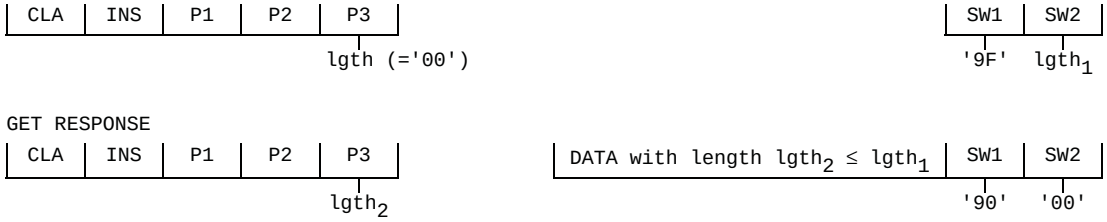


Case 2a: No input / Output of known length

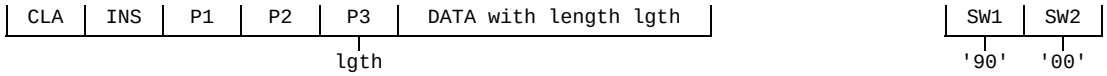


NOTE: lgth='00' causes a data transfer of 256 bytes.

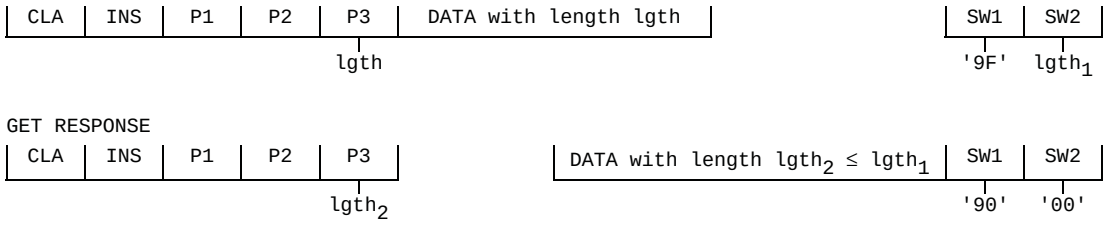
Case 2b: No Input / Output of unknown length



Case 3: Input / No output



Case 4: Input / Output of known or unknown length



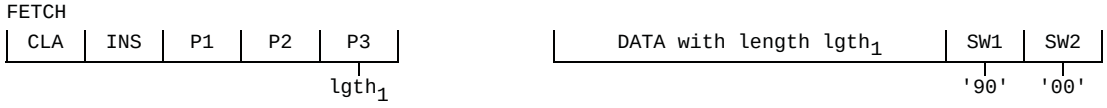
For case 4, in case of an ENVELOPE for SIM data download, SW1/SW2 may also indicate that there is response data with the value '9EXX', and the ME shall then send a GET RESPONSE command to get this response data.

The following diagrams show how the five cases of transmission protocol identified in the above diagrams can all be used to send pro-active SIM commands. For further information on the diagrams below see TS 51.014 [27].

Case 1: No input / "OK" response with no output, plus additional command from SIM

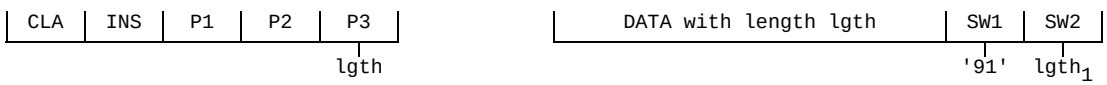


[Possible "normal GSM operation" command/response pairs]



NOTE: $lgth_1$='00' causes a data transfer of 256 bytes.

Case 2a: No input / "OK" response with data of known length, plus additional command from SIM

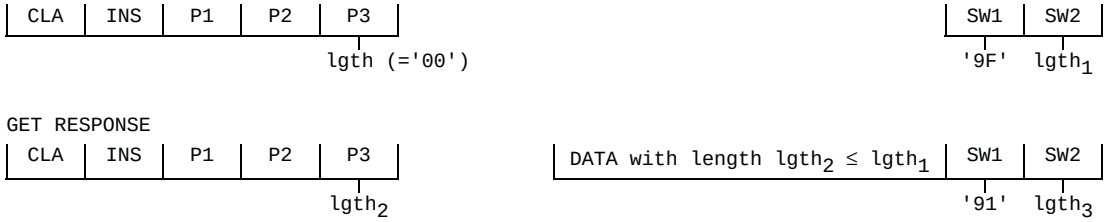


[Possible "normal GSM operation" command/response pairs]



NOTE: lgth='00' causes a data transfer of 256 bytes. The same applies to $lgth_1$.

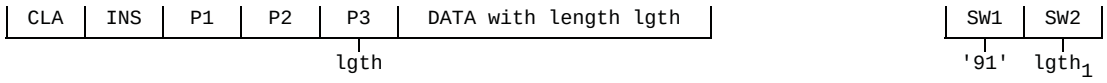
Case 2b: No Input / "OK" response with data of unknown length, plus additional command from SIM



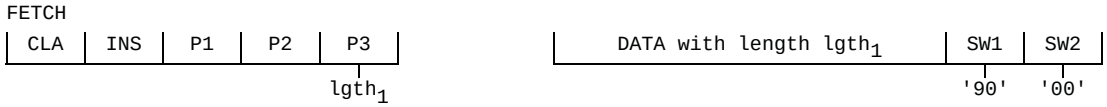
[Possible "normal GSM operation" command/response pairs]



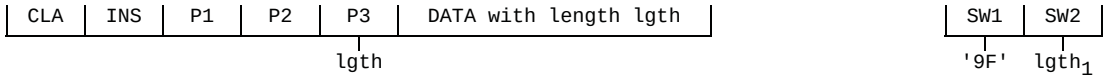
Case 3: Input / "OK" response with no output data, plus additional command from SIM



[Possible "normal GSM operation" command/response pairs]

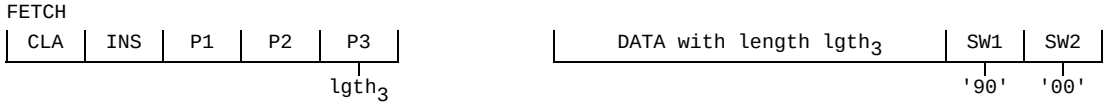


Case 4: Input / "OK" response with data of known or unknown length, plus additional command from SIM





[Possible "normal GSM operation" command/response pairs]



9.2 Coding of the commands

The commands are coded as specified in TS 31.101 [55] with the class byte set to 'A0'. In addition to the instruction codes specified TS 31.101 [55] the following codes are reserved:

GSM operational phase:

'1X' with X even, from X=6 to X=E.

Administrative management phase:

'2A', 'D0', 'D2', 'DE', 'C4', 'C6', 'C8', 'CA', 'CC', 'B4', 'B6', 'B8', 'BA' and 'BC'.

NOTE: This reservation may not be respected by other applications residing on a UICC or further evoluation of TS 31.101 [55].

9.2.1 SELECT

The SELECT command is coded as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1, P2 = '00'
- P3 = '02'

The response to the SELECT command with the parameters as specified is as follows:

Response parameters/data in case of an MF or DF:

Byte(s)	Description	Length
1 - 2	RFU	2
3 - 4	Total amount of memory of the selected directory which is not allocated to any of the DFs or EFs under the selected directory	2
5 - 6	File ID	2
7	Type of file (see clause 9.3)	1
8 - 12	RFU	5
13	Length of the following data (byte 14 to the end)	1
14 - 34	GSM specific data	21

GSM specific data:

Byte(s)	Description	Length
14	File characteristics (see detail 1)	1
15	Number of DFs which are a direct child of the current directory	1
16	Number of EFs which are a direct child of the current directory	1
17	Number of CHVs, UNBLOCK CHVs and administrative codes	1
18	RFU	1
19	CHV1 status (see detail 2)	1
20	UNBLOCK CHV1 status (see detail 2)	1
21	CHV2 status (see detail 2)	1
22	UNBLOCK CHV2 status (see detail 2)	1
23	RFU	1
24 - 34	Reserved for the administrative management	$0 \leq lgth \leq 11$

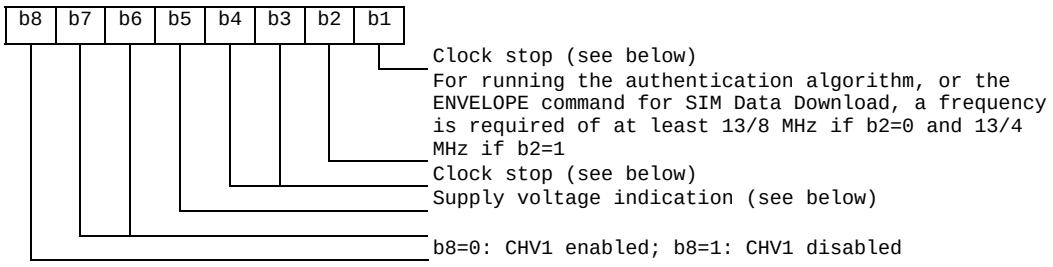
Bytes 1 - 22 are mandatory and shall be returned by the SIM. Bytes 23 and following are optional and may not be returned by the SIM.

NOTE 1: Byte 35 and following are RFU.

NOTE 2: The STATUS information of the MF, DF_{GSM} and $DF_{TELECOM}$ provide some identical application specific data, e.g. CHV status. On a multi-application card the MF should not contain any application specific data. Such data is obtained by terminals from the specific application directories. ME manufacturers should take this into account and therefore not use application specific data which may exist in the MF of a mono-application SIM.

Similarly, the VERIFY CHV command should not be executed in the MF but in the relevant application directory (e.g. DF_{GSM}).

Detail 1: File characteristics



The coding of the conditions for stopping the clock is as follows:

Bit b1	Bit b3	Bit b4	
1	0	0	clock stop allowed, no preferred level
1	1	0	clock stop allowed, high level preferred
1	0	1	clock stop allowed, low level preferred
0	0	0	clock stop not allowed
0	1	0	clock stop not allowed, unless at high level
0	0	1	clock stop not allowed, unless at low level

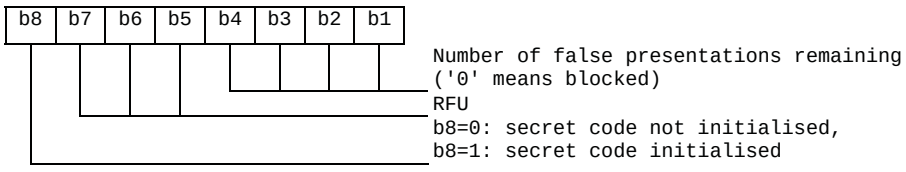
If bit b1 (column 1) is coded 1, stopping the clock is allowed at high or low level. In this case columns 2 (bit b3) and 3 (bit b4) give information about the preferred level (high or low, respectively) at which the clock may be stopped.

If bit b1 is coded 0, the clock may be stopped only if the mandatory condition in column 2 (b3=1, i.e. stop at high level) or column 3 (b4=1, i.e. stop at low level) is fulfilled. If all 3 bits are coded 0, then the clock shall not be stopped.

The coding of the conditions for the supply voltage indication is as follows:

SIM Supply Voltage	Bit 7	Bit 6	Bit 5
5V only SIM	0 (RFU) [1]	0 (RFU) [1]	0 (RFU) [1]
3V Technology SIM	0 (RFU) [1]	0 (RFU) [1]	1
1.8V Technology SIM	0 (RFU) [1]	1	1
Future Class	1	1	1
NOTE 1 The bits marked (RFU) are set to '0' and reserved for future use in the SIMs. The coding schemes relies on the fact that RFU bits are set to '0'.			

Detail 2: Status byte of a secret code



Response parameters/data in case of an EF:

Byte(s)	Description	Length
1 - 2	RFU	2
3 - 4	File size (for transparent EF: the length of the body part of the EF) (for linear fixed or cyclic EF: record length multiplied by the number of records of the EF)	2
5 - 6	File ID	2
7	Type of file (see 9.3)	1
8	see detail 3	1
9 - 11	Access conditions (see 9.3)	3
12	File status (see 9.3)	1
13	Length of the following data (byte 14 to the end)	1
14	Structure of EF (see 9.3)	1
15	Length of a record (see detail 4)	1
16 and following	RFU	-

Bytes 1-14 are mandatory and shall be returned by the SIM.

Byte 15 is mandatory in case of linear fixed or cyclic EFs and shall be returned by the SIM.

Byte 15 is optional in case of transparent EFs and may not be returned by the SIM.

Byte 16 and following (when defined) are optional and may not be returned by the SIM.

Detail 3: Byte 8

For transparent and linear fixed EFs this byte is RFU. For a cyclic EF all bits except bit 7 are RFU; b7=1 indicates that the INCREASE command is allowed on the selected cyclic file.

Detail 4: Byte 15

For cyclic and linear fixed EFs this byte denotes the length of a record. For a transparent EF, this byte shall be coded '00', if this byte is sent by the SIM.

9.2.2 STATUS

The STATUS command is coded as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1, P2 = '00'

The response parameters/data are identical to the response parameters/data of the SELECT command in case of an MF or DF.

9.2.3 READ BINARY

The READ BINARY command is coded as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- B8 in P1 shall be set to '0'

The response is according to the command parameters as defined in TS 31.101 [55].

9.2.4 UPDATE BINARY

The UPDATE BINARY command is coded as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'

- B8 in P1 shall be set to '0'

The response is according to the command parameters as defined in TS 31.101 [55].

9.2.5 READ RECORD

The READ RECORD command is coded as specified in TS 31.101 [55] with the following limitations:

Class = 'A0'

P2 = '02', '03', '04'

9.2.6 UPDATE RECORD

The UPDATE RECORD command is coded as specified in TS 31.101 [55] with the following limitations:

Class = 'A0'

P2 = '02', '03', '04'

The response is according to the command parameters, as defined in TS 31.101 [55]

9.2.7 SEEK

The instruction code 'A2' identifies the SEARCH RECORD command as defined in TS 31.101 [55]. In the present document the instruction code 'A2' is defined for the SEEK command for class 'A0'.

This function searches through the current linear fixed EF to find a record starting with the given pattern. This function shall only be performed if the READ access condition for this EF is satisfied. Two types of SEEK are defined:

Type 1 The record pointer is set to the record containing the pattern, no output is available.

Type 2 The record pointer is set to the record containing the pattern, the output is the record number.

NOTE: A Phase 1 SIM only executes type 1 of the SEEK function.

The SIM shall be able to accept any pattern length from 1 to 16 bytes inclusive. The length of the pattern shall not exceed the record length.

Four modes are defined:

- from the beginning forwards;
- from the end backwards;
- from the next location forwards;
- from the previous location backwards.

If the record pointer has not been previously set (its status is undefined) within the selected linear fixed EF, then the search begins:

- with the first record in the case of SEEK from the next location forwards; or
- with the last record in the case of SEEK from the previous location backwards.

After a successful SEEK, the record pointer is set to the record in which the pattern was found. The record pointer shall not be changed by an unsuccessful SEEK function.

COMMAND	CLASS	INS	P1	P2	P3
SEEK	'A0'	'A2'	'00'	Type/Mode	lgth

Parameter P2 specifies type and mode:

- 'x0' = from the beginning forward;
- 'x1' = from the end backward;
- 'x2' = from the next location forward;
- 'x3' = from the previous location backward;

with x='0' specifies type 1 and x='1' specifies type 2 of the SEEK command.

Command parameters/data:

Byte(s)	Description	Length
1 - lgth	Pattern	lgth

There are no response parameters/data for a type 1 SEEK. A type 2 SEEK returns the following response parameters/data:

Byte(s)	Description	Length
1	Record number	1

9.2.8 INCREASE

The INCREASE command is coded as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1,P2 = '00'
- P3 = '03'

The response is according to the command parameters, as defined in TS 31.101 [55]

9.2.9 VERIFY CHV

The VERIFY CHV is identical to the VERIFY PIN command as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1 = '00'
- P3 = '08'

NOTE: The functionality of the VERIFY CHV command is limited to CHV verification and can not be used to retrieve the retry counter value as specified in TS 31.101 [55].

Parameter P2 specifies the CHV:

- '01' = CHV1;
- '02' = CHV2.

The response is according to the command parameters, as defined in TS 31.101 [55].

9.2.10 CHANGE CHV

The CHANGE CHV is identical to the CHANGE PIN command as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1 = '00'

Parameter P2 specifies the CHV:

- '01' = CHV1;
- '02' = CHV2.

The response is according to the command parameters, as defined in TS 31.101 [55].

9.2.11 DISABLE CHV

The DISABLE CHV is identical to the DISABLE PIN command as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1 = '00'
- P2 = '01'

NOTE: The functionality of the DISABLE CHV command is limited to CHV disabling and can not be used to indicate the use of an alternative CHV (global key reference) as specified in TS 31.101 [55].

The response is according to the command parameters, as defined in TS 31.101 [55].

9.2.12 ENABLE CHV

The ENABLE CHV is identical to the ENABLE PIN command as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1 = '00'
- P2 = '01'

The response is according to the command parameters, as defined in TS 31.101 [55].

9.2.13 UNBLOCK CHV

The UNBLOCK CHV is identical to the UNBLOCK PIN command as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1 = '00'

Parameter P2 specifies the CHV:

- 00 = CHV1;
- 02 = CHV2.

NOTE: The coding '00' for CHV1 differs from the coding of CHV1 used for other commands.

The response is according to the command parameters, as defined in TS 31.101 [55].

9.2.14 INVALIDATE

The INVALIDATE command is identical to the DEACTIVATE command as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1,P2 = '00'

The response is according to the command parameters, as defined in TS 31.101 [55].

9.2.15 REHABILITATE

The REHABILITATE command is identical to the ACTIVATE command as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1,P2 = '00'

The response is according to the command parameters, as defined in TS 31.101 [55].

9.2.16 RUN GSM ALGORITHM

The RUN GSM ALGORITHM is identical to the AUTHENTICATE command as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'
- P1,P2 = '00'
- P3 = '10'

The structure of the Command parameters/data is as follows only for the specified parameters::

Byte(s)	Description	Length
1 - 16	RAND	16

The structure of the Response parameters/data is as follows only for the specified parameters:

Byte(s)	Description	Length
1 - 4	SRES	4
5 - 12	Cipher Key Kc	8

The most significant bit of SRES is coded on bit 8 of byte 1. The most significant bit of Kc is coded on bit 8 of byte 5.

9.2.17 SLEEP

This is an obsolete function used by Phase 1 MEs.

In order to achieve phase compatibility, a SIM of Phase 2 or later shall always send the status information "normal ending of the command" after the successful interpretation of the command SLEEP received from a Phase 1 ME. An ME of Phase 2 or later shall not send a SLEEP command;

COMMAND	CLASS	INS	P1	P2	P3
SLEEP	'A0'	'FA'	'00'	'00'	'00'

9.2.18 GET RESPONSE

The GET RESPONSE command is coded as specified in TS 31.101 [55] with the following limitations:

Class = 'A0'

Since the MF is implicitly selected after activation of the SIM, GET RESPONSE is also allowed as the first command after activation.

9.2.19 TERMINAL PROFILE

The TERMINAL PROFILE command is coded as specified in TS 31.101 [55] with the following limitations:

- Class = 'A0'

9.2.20 ENVELOPE

The ENVELOPE command is coded as specified in TS 31.101 [55] with the following limitations:

Class = 'A0'

9.2.21 FETCH

The FETCH command is coded as specified in TS 31.101 [55] with the following limitations:

Class = 'A0'

9.2.22 TERMINAL RESPONSE

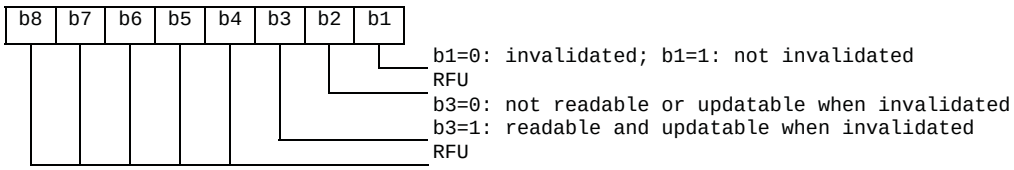
The TERMINAL RESPONSE command is coded as specified in TS 31.101 [55] with the following limitations:

Class = 'A0'

9.3 Definitions and coding

The coding conventions defined in TS 31.101 [55] applies with the following exceptions

File status



Bit b3 may be set to 1 in special circumstances when it is required that the EF can be read and updated even if the EF is invalidated, e.g. reading and updating the EF_{ADN} when the FDN feature is enabled, or reading and updating the EF_{BDN} when the BDN feature is disabled.

Structure of file

- '00' transparent;
- '01' linear fixed;
- '03' cyclic.

Type of File

- '00' RFU;
- '01' MF;
- '02' DF;
- '04' EF.

Coding of CHVs and UNBLOCK CHVs

A CHV is coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in ITU-T T.50 [20] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the ME shall pad the presented CHV with 'FF' before sending it to the SIM.

The coding of the UNBLOCK CHVs is identical to the coding of the CHVs. However, the number of (decimal) digits is always 8.

Coding of Access Conditions

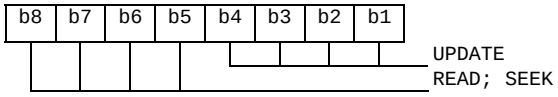
The access conditions for the commands are coded on bytes 9, 10 and 11 of the response data of the SELECT command if class byte 'A0' is usedEach condition is coded on 4 bits as shown in table 10.

Table 10: Access conditions

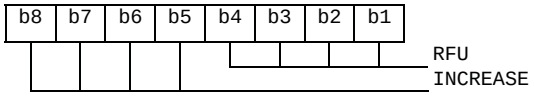
ALW	'0' *
CHV1	'1' *
CHV2	'2' *
RFU	'3'
ADM	'4'
.....	..
ADM	'E'
NEW	'F' *

Entries marked "*" in the table above, are also available for use as administrative codes in addition to the ADM access levels '4' to 'E' (refer to clause 7.3) if required by the appropriate administrative authority. If any of these access conditions are used, the code returned in the Access Condition bytes in the response data shall be the code applicable to that particular level.

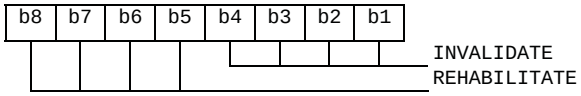
Byte 9:



Byte 10:



Byte 11:



9.4 Status conditions returned by the card

This clause specifies the coding of the status words SW1 and SW2.

9.4.1 Responses to commands which are correctly executed

SW1	SW2	Description
'90'	'00'	- normal ending of the command
'91'	'XX'	- normal ending of the command, with extra information from the proactive SIM containing a command for the ME. Length 'XX' of the response data
'9E'	'XX'	- length 'XX' of the response data given in case of a SIM data download error
'9F'	'XX'	- length 'XX' of the response data

9.4.2 Responses to commands which are postponed

SW1	SW2	Error description
'93'	'00'	- SIM Application Toolkit is busy. Command cannot be executed at present, further normal commands are allowed.

9.4.3 Memory management

SW1	SW2	Error description
'92'	'0X'	- command successful but after using an internal update retry routine 'X' times
'92'	'40'	- memory problem

9.4.4 Referencing management

SW1	SW2	Error description
'94'	'00'	- no EF selected
'94'	'02'	- out of range (invalid address)
'94'	'04'	- file ID not found - pattern not found
'94'	'08'	- file is inconsistent with the command

9.4.5 Security management

SW1	SW2	Error description
'98'	'02'	- no CHV initialized
'98'	'04'	- access condition not fulfilled - unsuccessful CHV verification, at least one attempt left - unsuccessful UNBLOCK CHV verification, at least one attempt left - authentication failed (see note)
'98'	'08'	- in contradiction with CHV status
'98'	'10'	- in contradiction with invalidation status
'98'	'40'	- unsuccessful CHV verification, no attempt left - unsuccessful UNBLOCK CHV verification, no attempt left - CHV blocked - UNBLOCK CHV blocked
'98'	'50'	- increase cannot be performed, Max value reached

NOTE: A Phase 1 SIM may send this error code after the third consecutive unsuccessful CHV verification attempt or the tenth consecutive unsuccessful unblocking attempt.

9.4.6 Application independent errors

SW1	SW2	Error description
'67'	'XX'	- incorrect parameter P3 (see note)
'6B'	'XX'#	- incorrect parameter P1 or P2 (see ##)
'6D'	'XX'#	- unknown instruction code given in the command
'6E'	'XX'#	- wrong instruction class given in the command
'6F'	'XX'#	- technical problem with no diagnostic given
NOTE 1: # These values of 'XX' are specified by ISO/IEC; at present the default value 'XX'='00' is the only one defined. NOTE 2: ## When the error in P1 or P2 is caused by the addressed record being out of range, then the return code '94 02' shall be used.		

NOTE: 'XX' gives the correct length or states that no additional information is given ('XX' = '00').

9.4.7 Commands versus possible status responses

The following table shows for each command the possible status conditions returned (marked by an asterisk *).

Table 11: Commands and status words

	OK				Busy	Mem Sta		Refer. Status				Security Status						Application Independent Errors				
	90	91	9E	9F	93	92	92	94	94	94	94	98	98	98	98	98	98	67	6B	6D	6E	6F
	00	XX	XX	XX	00	0X	40	00	02	04	08	02	04	08	10	40	50	XX	XX	XX	XX	XX
Commands																						
Select				*			*			*								*	*		*	*
Status	*	*					*											*	*		*	*
Update Binary	*	*				*	*	*			*		*		*			*	*		*	*
Update Record	*	*				*	*	*	*		*		*		*			*	*		*	*
Read Binary	*	*					*	*			*		*		*			*	*		*	*
Read Record	*	*					*	*	*		*		*		*			*	*		*	*
Seek	*			*			*	*		*	*		*		*		*	*	*		*	*
Increase				*		*	*	*			*		*		*		*	*	*		*	*
Verify CHV	*	*				*	*					*	*	*		*		*	*		*	*
Change CHV	*	*				*	*					*	*	*		*		*	*		*	*
Disable CHV	*	*				*	*					*	*	*		*		*	*		*	*
Enable CHV	*	*				*	*					*	*	*		*		*	*		*	*
Unblock CHV	*	*				*	*					*	*	*		*		*	*		*	*
Invalidate	*	*				*	*	*					*		*			*	*		*	*
Rehabilitate	*	*				*	*	*					*		*			*	*		*	*
Run GSM Algorithm				*			*				*		*					*	*		*	*
Sleep	*																	*	*		*	*
Get Response	*	*					*											*	*		*	*
Terminal Profile	*	*				*	*											*	*		*	*
Envelope	*	*	*	*	*	*	*											*	*		*	*
Fetch	*						*											*	*		*	*
Terminal Response	*	*				*	*											*	*		*	*

The responses '91 XX', and '93 00' and '9E XX' can only be given by a SIM supporting SIM Application Toolkit, to an ME also supporting SIM Application Toolkit.

For the SEEK command the response '91 XX' can be given directly after a Type 1 SEEK command. Following the Type 2 SEEK command the SIM can give the response '91 XX' only after the GET RESPONSE command.

10 Contents of the Elementary Files (EF)

This clause specifies the EFs for the GSM session defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity, e.g. the alpha tag in a EF_{ADN} record.

EFs or data items having an unassigned value, or, which during the GSM session, are cleared by the ME, shall have their bytes set to 'FF'. After the administrative phase all data items shall have a defined value or have their bytes set to 'FF'. If a data item is 'deleted' during a GSM session by the allocation of a value specified in another GSM TS, then this value shall be used, and the data item is not unassigned; e.g. for a deleted LAI in EF_{LOCI} the last byte takes the value 'FE' (TS 24.008 [47] refers).

EFs are mandatory (M) or optional (O). The file size of an optional EF may be zero. All implemented EFs with a file size greater than zero shall contain all mandatory data items. Optional data items may either be filled with 'F', or, if located at the end of an EF, need not exist.

When the coding is according to ITU-T T.50 [20], bit 8 of every byte shall be set to 0.

For an overview containing all files see figure 8.

10.1 Contents of the EFs at the MF level

The present document specifies only two Efs at the MF level. The presence of EF_{DIR} on a SIM is optional. The present document does not specify the mechanism to select a SIM application using EF_{DIR}.

10.1.1 EF_{ICCID} (ICC Identification)

This EF provides a unique identification number for the SIM. The structure of this EF is as defined in TS 31.101 [55]. Network operators who have already issued Phase 1 SIM cards with an identification number length of 20 digits may retain this length. Network operators who have already issued Phase 1 SIM cards where the digits within a byte are not swapped may retain this configuration.

10.1.2 EF_{PL} (Preferred language)

The structure of this data field is as defined in TS 31.101 [55]. The presence of this file is optional for a SIM.

This information may be used by the ME for MMI purposes. This information may also be used for the screening of Cell Broadcast messages in a preferred language, as follows.

When the CB Message Identifier capability is both allocated and activated, the ME selects only those CB messages the language of which corresponds to an entry in this EF or in EF_{LP}, whichever of these EFs is used (see clause 11.2.1). The CB message language is defined by the Data Coding Scheme (DCS: see TS 23.038 [12]) received with the CB message. The ME shall be responsible for translating the language coding indicated in the Data Coding Scheme for the Cell Broadcast Service (as defined in TS 23.038 [12]) to the language coding as defined in ISO 639 [30] if it is necessary to check the language coding in EF_{PL}.

NOTE: This file is called EF_{ELP} (Extended Langueage preference) in previous releases of the present document, i.e. TS 11.11.

10.2 DFs at the GSM application level

For compatibility with other systems based on the GSM switching platform and for special GSM services, DFs may be present as child directories of DF_{GSM}. The following have been defined:

$DF_{IRIDIUM}$	'5F30'
$DF_{GLOBALSTAR}$	'5F31'
DF_{ICO}	'5F32'
DF_{ACeS}	'5F33'
DF_{MExE}	'5F3C'
$DF_{EIA/TIA-553}$	'5F40'
DF_{CTS}	'5F60'
DF_{SoLSA}	'5F70'

Only the contents of DF_{SoLSA} and DF_{MExE} are specified in the present document. For details of the EFs contained in the DF_{CTS}, see TS 11.19 [34].

10.3 Contents of files at the GSM application level

The EFs in the Dedicated File DF_{GSM} contain network related information.

10.3.1 EF_{LP} (Language preference)

This EF contains the codes for one or more languages. This information, determined by the user/operator, defines the preferred languages of the user in order of priority. This information may be used by the ME for MMI purposes.

This information may also be used for the screening of Cell Broadcast messages in a preferred language, as follows. When the CB Message Identifier capability is both allocated and activated, the ME selects only those CB messages the language of which corresponds to an entry in this EF or in EF_{ELP}, whichever of these EFs is used (see clause 11.2.1). The CB message language is defined by the Data Coding Scheme (DCS: see TS 23.038 [12]) received with the CB message. The ME shall be responsible for translating the language coding indicated in the Data Coding Scheme for the Cell Broadcast Service (as defined in TS 23.038 [12]) to the language coding as defined in ISO 639 [30] if it is necessary to check the language coding in EF_{PL}.

Identifier: '6F05'	Structure: transparent	Mandatory
File size: 1 to n bytes	Update activity: low	
Access Conditions: READ ALW UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	1st language code (highest prior.)	M	1 byte
2	2nd language code	O	1 byte
n	nth language code (lowest prior.)	O	1 byte

Coding: according to language codings contained in the Data Coding Scheme (see TS 23.038 [12]).

Using the command GET RESPONSE, the ME can determine the size of the EF.

10.3.2 EF_{IMSI} (IMSI)

This EF contains the International Mobile Subscriber Identity (IMSI).

Identifier: '6F07'	Structure: transparent	Mandatory
File size: 9 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE CHV1		

Bytes	Description	M/O	Length
1	length of IMSI	M	1 byte
2 to 9	IMSI	M	8 bytes

- length of IMSI

  Contents:

  The length indicator refers to the number of significant bytes, not including this length byte, required for the IMSI.

  Coding: according to TS 24.008 [47].

- IMSI

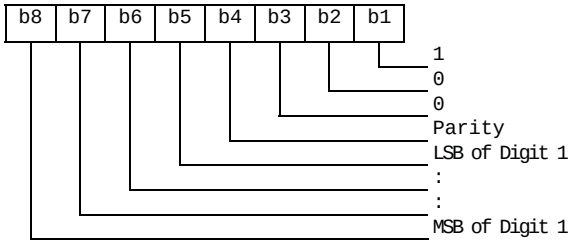
  Contents:

  International Mobile Subscriber Identity.

  Coding:

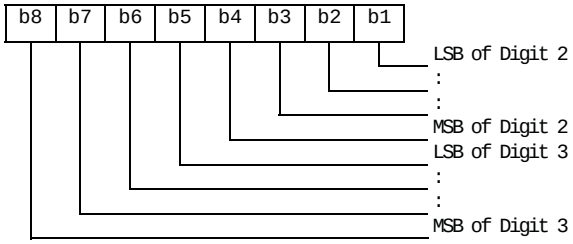
  This information element is of variable length. If a network operator chooses an IMSI of less than 15 digits, unused nibbles shall be set to 'F'.

Byte 2:



For the parity bit, see TS 24.008 [47].

Byte 3:



etc.

10.3.3 EF_{Kc} (Ciphering key Kc)

This EF contains the ciphering key Kc and the ciphering key sequence number n.

Identifier: '6F20'	Structure: transparent	Mandatory
File size: 9 bytes	Update activity: high	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 8	Ciphering key Kc	M	8 bytes
9	Ciphering key sequence number n	M	1 byte

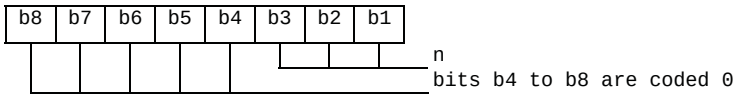
- Ciphering key Kc

  Coding:

  The least significant bit of Kc is the least significant bit of the eighth byte. The most significant bit of Kc is the most significant bit of the first byte.

- Ciphering key sequence number n

  Coding:



NOTE: TS 24.008 [47] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

10.3.4 $EF_{PLMNsel}$ (PLMN selector)

This EF contains the coding for n PLMNs, where n is at least eight. This information determined by the user/operator defines the preferred PLMNs of the user in priority order.

Identifier: '6F30'	Structure: transparent	Optional
File size: 3n (n ≥ 8) bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
22 to 24	8th PLMN	M	3 bytes
25 to 27	9th PLMN	O	3 bytes
(3n-2) to 3n	nth PLMN (lowest priority)	O	3 bytes

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

  according to TS 24.008 [47].

  If storage for fewer than the maximum possible number n is required, the excess bytes shall be set to 'FF'.

  For instance, using 246 for the MCC and 81 for the MNC and if this is the first and only PLMN, the contents reads as follows:

  Bytes 1-3: '42' 'F6' '18'

  Bytes 4-6: 'FF' 'FF' 'FF'

  etc.

10.3.5 EF_{HPPLMN} (Higher Priority PLMN search period)

This EF contains the interval of time between searches for a higher priority PLMN (see TS 22.011 [5]).

Identifier: '6F31'	Structure: transparent	Mandatory
File size: 1 byte	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Time interval	M	1 byte

- Time interval

  Contents:

  The time interval between two searches.

Coding:

The time interval is coded in integer multiples of n minutes. The range is from n minutes to a maximum value. The value '00' indicates that no attempts shall be made to search for any higher priority PLMN. The encoding is:

- '00': No higher priority PLMN search attempts
- '01': n minutes
- '02': 2n minutes
- : :
- 'YZ': (16Y+Z)n minutes (maximum value)

All other values shall be interpreted by the ME as a default period.

For specification of the integer timer interval n, the maximum value and the default period refer to TS 22.011 [5].

10.3.6 EF_{ACMmax} (ACM maximum value)

This EF contains the maximum value of the accumulated call meter. This EF shall always be allocated if EF_{ACM} is allocated.

Identifier: '6F37'	Structure: transparent	Optional
File size: 3 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1/CHV2 (fixed during administrative management)
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 3	Maximum value	M	3 bytes

- Maximum value

Contents:

maximum value of the Accumulated Call Meter (ACM)

Coding:

First byte:

b8	b7	b6	b5	b4	b3	b2	b1
2^{23}	2^{22}	2^{21}	2^{20}	2^{19}	2^{18}	2^{17}	2^{16}

Second byte:

b8	b7	b6	b5	b4	b3	b2	b1
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}

Third byte:

b8	b7	b6	b5	b4	b3	b2	b1
2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}

For instance, '00' '00' '30' represents 2^5+2^4.

All ACM data is stored in the SIM and transmitted over the SIM/ME interface as binary.

ACMmax is not valid, as defined in TS 22.024 [7], if it is coded '000000'.

10.3.7 EF_{SST} (SIM service table)

This EF indicates which services are allocated, and whether, if allocated, the service is activated. If a service is not allocated or not activated in the SIM, the ME shall not select this service.

Identifier: '6F38'	Structure: transparent	Mandatory
File size: X bytes, X ≥ 2	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Services n°1 to n°4	M	1 byte
2	Services n°5 to n°8	M	1 byte
3	Services n°9 to n°12	O	1 byte
4	Services n°13 to n°16	O	1 byte
5	Services n°17 to n°20	O	1 byte
6	Services n°21 to n°24	O	1 byte
7	Services n°25 to n°28	O	1 byte
8	Services n°29 to n°32	O	1 byte
etc.			
X	Services (4X-3) to (4X)	O	1 byte

-Services

Contents:		
	Service n°1:	CHV1 disable function
	Service n°2:	Abbreviated Dialling Numbers (ADN)
	Service n°3:	Fixed Dialling Numbers (FDN)
	Service n°4:	Short Message Storage (SMS)
	Service n°5:	Advice of Charge (AoC)
	Service n°6:	Capability Configuration Parameters (CCP)
	Service n°7:	PLMN selector
	Service n°8:	RFU
	Service n°9:	MSISDN
	Service n°10:	Extension1
	Service n°11:	Extension2
	Service n°12:	SMS Parameters
	Service n°13:	Last Number Dialled (LND)
	Service n°14:	Cell Broadcast Message Identifier
	Service n°15:	Group Identifier Level 1
	Service n°16:	Group Identifier Level 2
	Service n°17:	Service Provider Name
	Service n°18:	Service Dialling Numbers (SDN)
	Service n°19:	Extension3
	Service n°20:	RFU
	Service n°21:	VGCS Group Identifier List (EF_{VGCS} and EF_{VGCSS})
	Service n°22:	VBS Group Identifier List (EF_{VBS} and EF_{VBSS})
	Service n°23:	enhanced Multi-Level Precedence and Pre-emption Service
	Service n°24:	Automatic Answer for eMLPP
	Service n°25:	Data download via SMS-CB
	Service n°26:	Data download via SMS-PP
	Service n°27:	Menu selection
	Service n°28:	Call control
	Service n°29:	Proactive SIM
	Service n°30:	Cell Broadcast Message Identifier Ranges
	Service n°31:	Barred Dialling Numbers (BDN)
	Service n°32:	Extension4
	Service n°33:	De-personalization Control Keys
	Service n°34:	Co-operative Network List
	Service n°35:	Short Message Status Reports
	Service n°36:	Network's indication of alerting in the MS
	Service n°37:	Mobile Originated Short Message control by SIM
	Service n°38:	GPRS
	Service n°39:	Image (IMG)
	Service n°40:	SoLSA (Support of Local Service Area)
	Service n°41:	USSD string data object supported in Call Control
	Service n°42:	RUN AT COMMAND command
	Service n°43:	User controlled PLMN Selector with Access Technology
	Service n 44:	Operator controlled PLMN Selector with Access Technology
	Service n 45:	HPLMN Selector with Access Technology
	Service n 46:	CPBCCH Information
	Service n 47:	Investigation Scan
	Service n°48:	Extended Capability Configuration Parameters
	Service n°49:	MExE
	Service n°50:	Reserved and shall be ignored
	Service n°51:	PLMN Network Name
	Service n°52:	Operator PLMN List
	Service n°53:	Mailbox Dialling Numbers
	Service n°54:	Message Waiting Indication Status
	Service n°55:	Call Forwarding Indication Status
	Service n°56:	Service Provider Display Information
	Service n°57:	Multimedia Messaging Service (MMS)
	Service n°58:	Extension 8
	Service n°59:	MMS User Connectivity Parameters

For a phase 2 SIM, the EF shall contain at least two bytes which correspond to the Phase 1 services. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the responsibility of ETSI.

NOTE 1: Service N°8 was used in Phase 1 for Called Party Subaddress. To prevent any risk of incompatibility Service N°8 should not be reallocated.

NOTE 2: As the BDN service relies on the Call Control feature, service n°31 (BDN) should only be allocated and activated if service n°28 (Call control) is allocated and activated.

Coding:

2 bits are used to code each service:

first bit = 1: service allocated

first bit = 0: service not allocated

where the first bit is b1, b3, b5 or b7;

second bit = 1: service activated

second bit = 0: service not activated

where the second bit is b2, b4, b6 or b8.

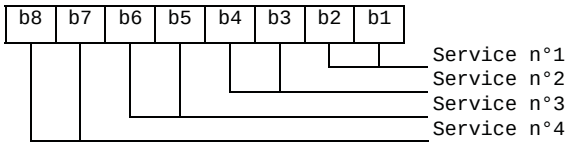
Service allocated means that the SIM has the capability to support the service. Service activated means that the service is available for the card holder (only valid if the service is allocated).

The following codings are possible:

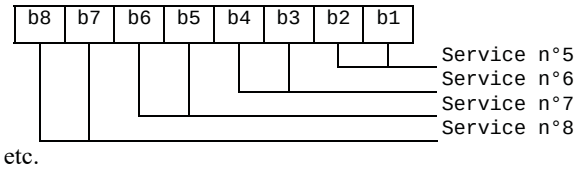
- first bit = 0: service not allocated, second bit has no meaning;
- first bit = 1 and second bit = 0: service allocated but not activated;
- first bit = 1 and second bit = 1: service allocated and activated.

The bits for services not yet defined shall be set to RFU. For coding of RFU see clause 9.3.

First byte:

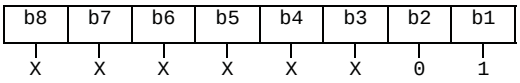


Second byte:



etc.

The following example of coding for the first byte means that service n°1 "CHV1-Disabling" is allocated but not activated:



If the SIM supports the FDN feature (FDN allocated and activated) a special mechanism shall exist in the SIM which invalidates both EF_{IMSI} and EF_{LOCI} once during each GSM session. This mechanism shall be invoked by the SIM automatically if FDN is enabled. This invalidation shall occur at least before the next command following selection of either EF. FDN is enabled when the ADN is invalidated or not activated.

If the SIM supports the BDN feature (BDN allocated and activated) a special mechanism shall exist in the SIM which invalidates both EF_{IMSI} and EF_{LOCI} once during each GSM session and which forbids the REHABILITATE command to rehabilitate both EF_{IMSI} and EF_{LOCI} until the PROFILE DOWNLOAD procedure is performed indicating that the ME supports the "Call control by SIM" facility. This mechanism shall be invoked by the SIM automatically if BDN is enabled. The invalidation of EF_{IMSI} and EF_{LOCI} shall occur at least before the next command following selection of either EF. BDN is enabled when the EF_{BDN} is not invalidated.

10.3.8 EF_{ACM} (Accumulated call meter)

This EF contains the total number of units for both the current call and the preceding calls.

NOTE: The information may be used to provide an indication to the user for advice or as a basis for the calculation of the monetary cost of calls (see TS 22.086 [9]).

Identifier: '6F39'	Structure: cyclic	Optional
Record length: 3 bytes	Update activity: high	

Access Conditions:

READ	CHV1
UPDATE	CHV1/CHV2 (fixed during administrative management)
INCREASE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 3	Accumulated count of units	M	3 bytes

- Accumulated count of units

  Contents: value of the ACM

  Coding: see the coding of EF_{ACMmax}

10.3.9 EF_{GID1} (Group Identifier Level 1)

This EF contains identifiers for particular SIM-ME associations. It can be used to identify a group of SIMs for a particular application.

Identifier: '6F3E'	Structure: transparent	Optional
File size: 1 to n bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to n	SIM group identifier(s)	O	n bytes

10.3.10 EF_{GID2} (Group Identifier Level 2)

This EF contains identifiers for particular SIM-ME associations. It can be used to identify a group of SIMs for a particular application.

Identifier: '6F3F'	Structure: transparent	Optional
File size: 1 to n bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to n	SIM group identifier(s)	O	n bytes

NOTE: The structure of EF_{GID1} and EF_{GID2} are identical. They are provided to allow the network operator to enforce different levels of security dependant on application.

10.3.11 EF_{SPN} (Service Provider Name)

This EF contains the service provider name and appropriate requirements for the display by the ME.

Identifier: '6F46'	Structure: transparent	Optional
File Size: 17 bytes	Update activity: low	
Access Conditions: READ ALWAYS UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

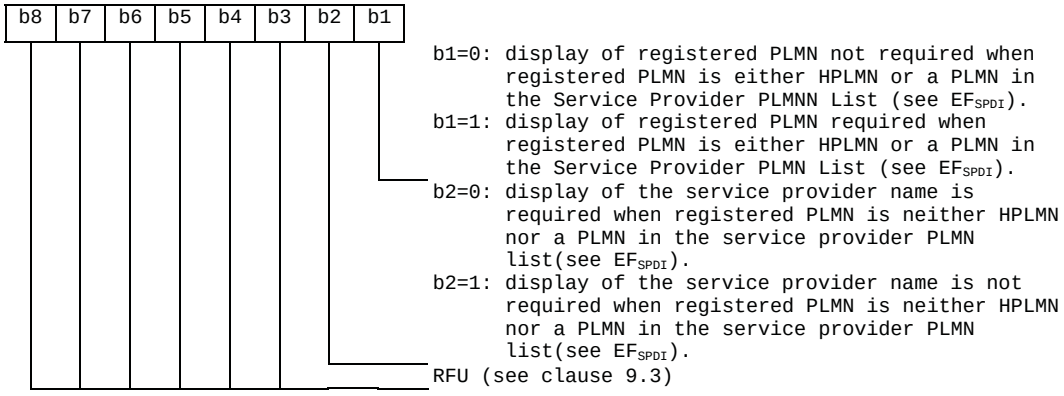
Bytes	Description	M/O	Length
1	Display Condition	M	1 byte
2 to 17	Service Provider Name	M	16 bytes

- Display Condition

  Contents: display condition for the service provider name in respect to the registered PLMN (see TS 22.101 [53]).

  Coding: see below

  Byte 1:



- Service Provider Name

  Contents: service provider string

  Coding: the string shall use either

  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [12] with bit 8 set to 0. The string shall be left justified. Unused bytes shall be set to 'FF'; or

  - one of the UCS2 code options defined in annex B.

10.3.12 EF_{PUCT} (Price per unit and currency table)

This EF contains the Price per Unit and Currency Table (PUCT). The PUCT is Advice of Charge related information which may be used by the ME in conjunction with EF_{ACM} to compute the cost of calls in the currency chosen by the subscriber, as specified in TS 22.024 [7]. This EF shall always be allocated if EF_{ACM} is allocated.

Identifier: '6F41'	Structure: transparent	Optional
File size: 5 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1/CHV2 (fixed during administrative management)
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 3	Currency code	M	3 bytes
4 to 5	Price per unit	M	2 bytes

- Currency code

  Contents:

  the alpha-identifier of the currency code.

  Coding:

  bytes 1, 2 and 3 are the respective first, second and third character of the alpha identifier. This alpha-tagging shall use the SMS default 7-bit coded alphabet as defined in TS 23.038 [12] with bit 8 set to 0.

- Price per unit

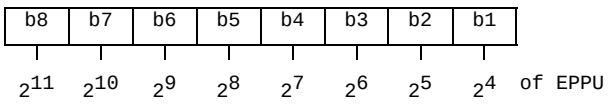
  Contents:

  price per unit expressed in the currency coded by bytes 1-3.

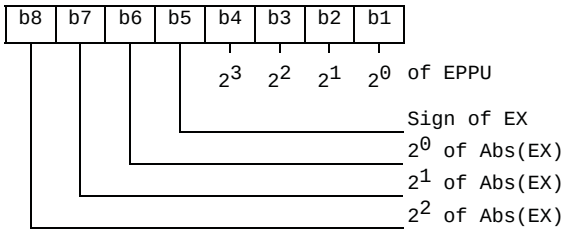
  Coding:

  Byte 4 and bits b1 to b4 of byte 5 represent the Elementary Price per Unit (EPPU) in the currency coded by bytes 1-3. Bits b5 to b8 of byte 5 are the decimal logarithm of the multiplicative factor represented by the absolute value of its decimal logarithm (EX) and the sign of EX, which is coded 0 for a positive sign and 1 for a negative sign.

  Byte 4:



  Byte 5:



  The computation of the price per unit value is made by the ME in compliance with TS 22.024 [7] by the following formula:

price per unit = EPPU * 10^{EX}.

The price has to be understood as expressed in the coded currency.

10.3.13 EF_{CBMI} (Cell broadcast message identifier selection)

This EF contains the Message Identifier Parameters which specify the type of content of the cell broadcast messages that the subscriber wishes the MS to accept.

Any number of CB Message Identifier Parameters may be stored in the SIM. No order of priority is applicable.

Identifier: '6F45'	Structure: transparent	Optional
File size: 2n bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 2	CB Message Identifier 1	O	2 bytes
3 to 4	CB Message Identifier 2	O	2 bytes
2n-1 to 2n	CB Message Identifier n	O	2 bytes

- Cell Broadcast Message Identifier

  Coding:

  as in TS 23.041, "Message Format on BTS-MS Interface - Message Identifier".

  Values listed show the types of message which shall be accepted by the MS.

  Unused entries shall be set to 'FF FF'.

10.3.14 EF_{BCCH} (Broadcast control channels)

This EF contains information concerning the BCCH according to TS 44.018 [59].

BCCH storage may reduce the extent of a Mobile Station's search of BCCH carriers when selecting a cell. The BCCH carrier lists in an MS shall be in accordance with the procedures specified in TS 44.018 [59]. The MS shall only store BCCH information from the System Information 2 message and not the 2bis extension message.

Identifier: '6F74'	Structure: transparent	Mandatory
File size: 16 bytes	Update activity: high	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 16	BCCH information	M	16 bytes

- BCCH information

  Coding:

  The information is coded as octets 2-17 of the "neighbour cells description information element" in TS 44.018 [59].

10.3.15 EF_{ACC} (Access control class)

This EF contains the assigned access control class(es). TS 22.011 [5] refers. The access control class is a parameter to control the RACH utilization. 15 classes are split into 10 classes randomly allocated to normal subscribers and 5 classes allocated to specific high priority users. For more information see TS 22.011 [5].

Identifier: '6F78'	Structure: transparent	Mandatory
File size: 2 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 2	Access control classes	M	2 bytes

- Access control classes

  Coding:

  Each ACC is coded on one bit. An ACC is "allocated" if the corresponding bit is set to 1 and "not allocated" if this bit is set to 0. Bit b3 of byte 1 is set to 0.

  Byte 1:

b8	b7	b6	b5	b4	b3	b2	b1	
15	14	13	12	11	10	09	08	Number of the ACC (except for bit b3)

  Byte 2:

b8	b7	b6	b5	b4	b3	b2	b1	
07	06	05	04	03	02	01	00	Number of the ACC

10.3.16 EF_{FPLMN} (Forbidden PLMNs)

This EF contains the coding for four Forbidden PLMNs (FPLMN). It is read by the ME as part of the SIM initialization procedure and indicates PLMNs which the MS shall not automatically attempt to access.

A PLMN is written to the EF if a network rejects a Location Update with the cause "PLMN not allowed". The ME shall manage the list as follows.

When four FPLMNs are held in the EF, and rejection of a further PLMN is received by the ME from the network, the ME shall modify the EF using the UPDATE command. This new PLMN shall be stored in the fourth position, and the existing list "shifted" causing the previous contents of the first position to be lost.

When less than four FPLMNs exist in the EF, storage of an additional FPLMN shall not cause any existing FPLMN to be lost.

Dependent upon procedures used to manage storage and deletion of FPLMNs in the EF, it is possible, when less than four FPLMNs exist in the EF, for 'FFFFFF' to occur in any position. The ME shall analyse all the EF for FPLMNs in any position, and not regard 'FFFFFF' as a termination of valid data.

Identifier: '6F7B'	Structure: transparent	Mandatory
File size: 12 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 3	PLMN 1	M	3 bytes
4 to 6	PLMN 2	M	3 bytes
7 to 9	PLMN 3	M	3 bytes
10 to 12	PLMN 4	M	3 bytes

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

  according to TS 24.008 [47].

  For instance, using 246 for the MCC and 81 for the MNC and if this is stored in PLMN 3 the contents is as follows:

  Bytes 7-9:'42' 'F6' '18'

  If storage for fewer than 4 PLMNs is required, the unused bytes shall be set to 'FF'.

10.3.17 EF_{LOCI} (Location information)

This EF contains the following Location Information:

- Temporary Mobile Subscriber Identity (TMSI);
- Location Area Information (LAI);
- TMSI TIME;
- Location update status.

In the case when updating EF_{LOCI} with data containing the TMSI value and the card reports the error '92 40' (Memory Problem), the ME shall terminate GSM operation.

Identifier: '6F7E'	Structure: transparent	Mandatory
File size: 11 bytes	Update activity: high	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	CHV1

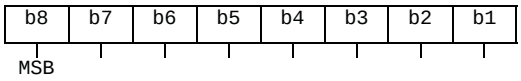
Bytes	Description	M/O	Length
1 to 4	TMSI	M	4 bytes
5 to 9	LAI	M	5 bytes
10	TMSI TIME	M	1 byte
11	Location update status	M	1 byte

- TMSI

Contents: Temporary Mobile Subscriber Identity

Coding: according to TS 24.008 [47].

Byte 1: first byte of TMSI

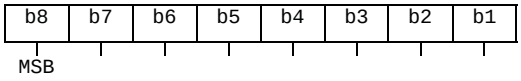


- LAI

Contents: Location Area Information

Coding: according to TS 24.008 [47].

Byte 5: first byte of LAI



- TMSI TIME

Contents: Current value of Periodic Location Updating Timer (T3212).

This byte is used by Phase 1 MEs, but it shall not be used by Phase 2 MEs.

- Location update status

Contents: status of location update according to TS 24.008 [47].

Coding:

Byte 11:

Bits:	b3	b2	b1	
0	0	0	:	updated
0	0	1	:	not updated
0	1	0	:	PLMN not allowed
0	1	1	:	Location Area not allowed
1	1	1	:	reserved

Bits b4 to b8 are RFU (see clause 9.3).

10.3.18 EF_{AD} (Administrative data)

This EF contains information concerning the mode of operation according to the type of SIM, such as normal (to be used by PLMN subscribers for GSM operations), type approval (to allow specific use of the ME during type approval procedures of e.g. the radio equipment), cell testing (to allow testing of a cell before commercial use of this cell), manufacturer specific (to allow the ME manufacturer to perform specific proprietary auto-test in its ME during e.g. maintenance phases).

It also provides an indication of whether some ME features should be activated during normal operation as well as information about the length of the MNC, which is part of the International Mobile Subscriber Identity (IMSI).

Identifier: '6FAD'	Structure: transparent	Mandatory
File size: 3+X bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	MS operation mode	M	1 byte
2 to 3	Additional information	M	2 bytes
4	length of MNC in the IMSI	O	1 byte
5 to 3+X	RFU	O	(X-1) bytes

NOTE: If X=0 no optional field is present;
If X=1 byte 4 is present but no RFU field is present;
When the RFU field is present (X ≥2) then byte 4 shall be present.

- MS operation mode

  Contents: mode of operation for the MS

  Coding:

  Initial value

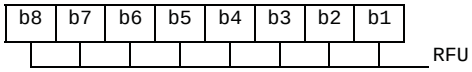
  - normal operation '00'
  - type approval operations '80'
  - normal operation + specific facilities '01'
  - type approval operations + specific facilities '81'
  - maintenance (off line) '02'
  - cell test operation '04'

- Additional information

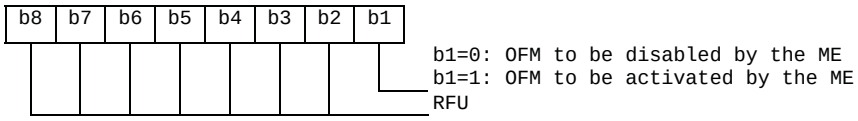
  Coding:

  - specific facilities (if b1=1 in byte 1);

  Byte 2 (first byte of additional information):



  Byte 3:



  The OFM bit is used to control the Ciphering Indicator as specified in TS 22.101 [53]

  - ME manufacturer specific information (if b2=1 in byte 1).

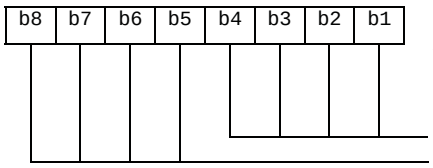
- Length of MNC in the IMSI :

  Contents:

  The length indicator refers to the number of digits, used for extracting the MNC from the IMSI

  Coding:

Byte 4:



10.3.19 EF_{Phase} (Phase identification)

This EF contains information concerning the phase of the SIM.

Identifier: '6FAE'	Structure: transparent	Mandatory
File size: 1 byte	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	SIM Phase	M	1 byte

- SIM Phase

  Coding:

  '00': phase 1

  '02': phase 2

  '03': phase 2 and PROFILE DOWNLOAD required (see TS 51.014 [27]).

  All other codings are reserved for specification by ETSI TC SMG. Codings '04' to '0F' indicate that the SIM supports, as a minimum, the mandatory requirements defined in this specification.

This phase identification does not preclude a SIM to support some features of a phase later than the one indicated in EF_{Phase}. For example : if EF_{Phase} is coded '00', it may be assumed by the ME that some Phase 2 or Phase 2+ features are supported by this SIM; if EF_{Phase} is coded '02' or '03', it may be assumed by the ME that some Phase 2+ features are supported by this SIM.

However, the services n°3 (FDN) and/or n°5 (AoC) shall only be allocated and activated in SIMs of phase 2 or later with EF_{Phase} being coded '02' or greater. Similarly, service n°31 (BDN) shall only be allocated and activated in SIMs with EF_{Phase} being coded '03' or greater.

If EF_{Phase} is coded '03' or greater, an ME supporting SIM Application Toolkit shall perform the PROFILE DOWNLOAD procedure, as defined in TS 51.014 [27].

10.3.20 EF_{VGCS} (Voice Group Call Service)

This EF contains a list of those VGCS group identifiers the user has subscribed to. The elementary file is used by the ME for group call establishment and group call reception.

Identifier: '6FB1'	Structure: transparent	Optional
File size: 4n bytes (n <= 50)	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 4	Group ID 1	M	4 bytes
5 to 8	Group ID 2	O	4 bytes
:	:	:	:
(4n-3) to 4n	Group ID n	O	4 bytes

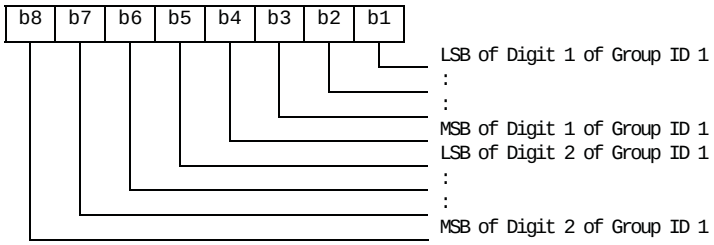
- Group ID

  Contents: VGCS Group ID, according to TS 23.003 [10]

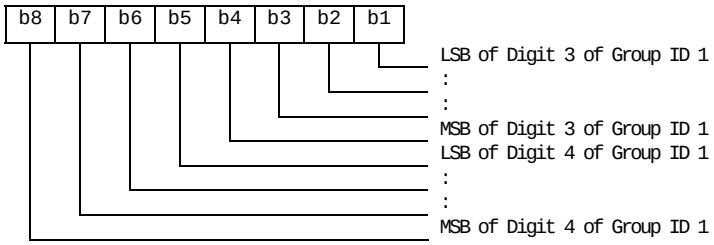
  Coding:

  The VGCS Group ID is of a variable length with a maximum length of 8 digits. Each VGCS Group ID is coded on four bytes, with each digit within the code being coded on four bits corresponding to BCD code. If a VGCS Group ID of less than 8 digits is chosen, then the unused nibbles shall be set to 'F'. VGCS Group ID Digit 1 is the most significant digit of the Group ID.

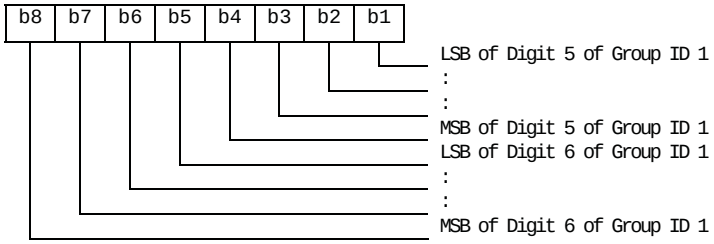
  Byte 1:



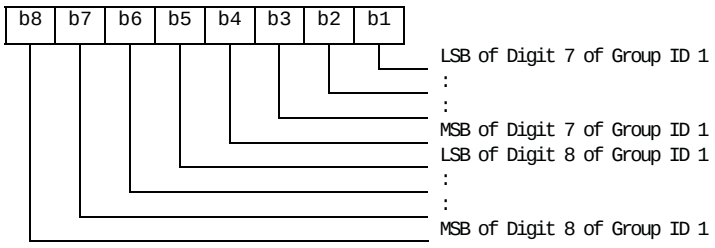
  Byte 2:



  Byte 3:

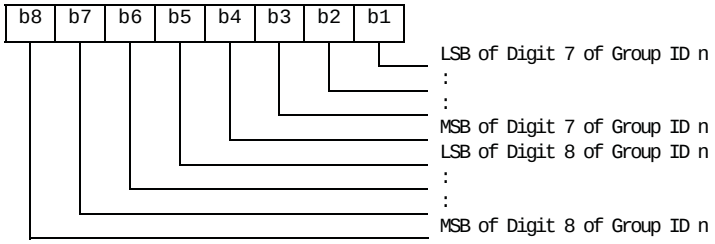


Byte 4:



:
: etc.....

Byte (4n-3) to 4n:



If storage for fewer than the maximum possible number *n* of VGCS Group IDs, is required, the excess bytes shall be set to 'FF'.

10.3.21 EF_{vgcss} (Voice Group Call Service Status)

This EF contains the status of activation for the VGCS group identifiers. The elementary file is directly related to the EF_{VGCS}. This EF shall always be allocated if EF_{VGCS} is allocated.

Identifier: '6FB2'	Structure: transparent	Optional
File size: 7 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 7	Activation/Deactivation Flags	M	7 bytes

- Activation/Deactivation Flags

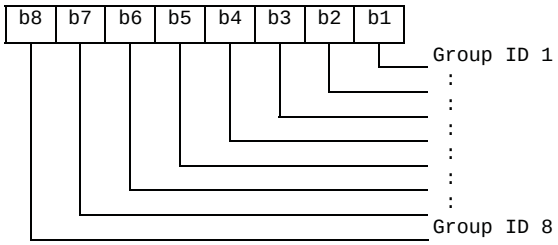
  Contents: Activation/Deactivation Flags of the appropriate Group IDs

  Coding:

  bit = 0 means - Group ID deactivated

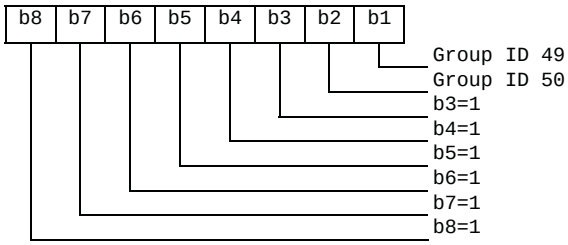
  bit = 1 means - Group ID activated

  Byte 1:



etc : : : : : : : :

Byte 7:



10.3.22 EF_{VBS} (Voice Broadcast Service)

This EF contains a list of those VBS group identifiers the user has subscribed to. The elementary file is used by the ME for broadcast call establishment and broadcast call reception.

Identifier: '6FB3'	Structure: transparent	Optional
File size: 4n bytes (n <= 50)	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 4	Group ID 1	M	4 bytes
5 to 2	Group ID 2	O	4 bytes
:	:	:	:
(4n-3) to 4n	Group ID n	O	4 bytes

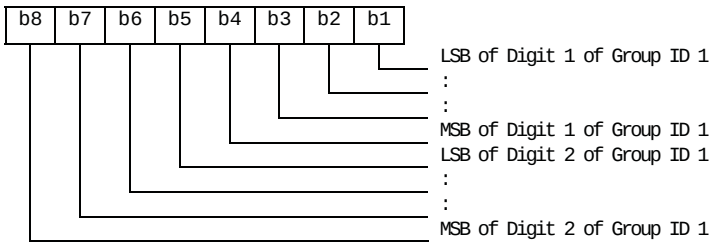
- Group ID

  Contents: VBS Group ID, according to TS 23.003 [10]

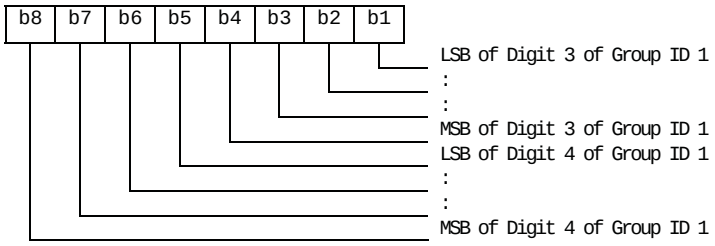
  Coding:

  The VBS Group ID is of a variable length with a maximum length of 8 digits. Each VBS Group ID is coded on four bytes, with each digit within the code being coded on four bits corresponding to BCD code. If a VBS Group ID of less than 8 digits is chosen, then the unused nibbles shall be set to 'F'. VBS Group ID Digit 1 is the most significant digit of the Group ID.

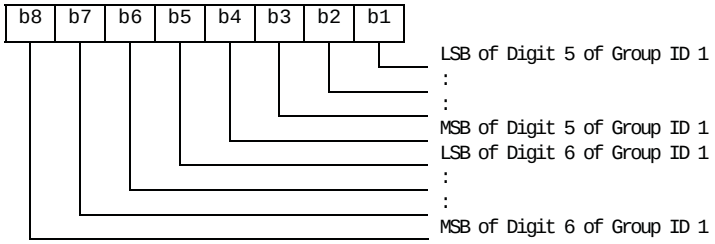
Byte 1:



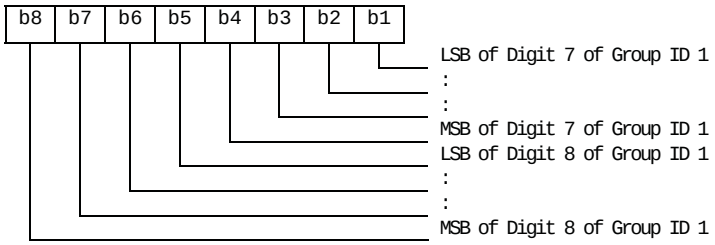
Byte 2:



Byte 3:

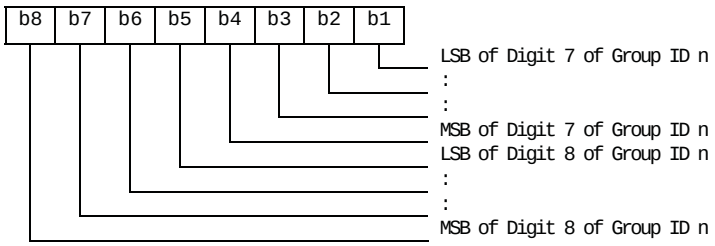


Byte 4:



:
: etc.....

Byte (4n-3) to 4n:



If storage for fewer than the maximum possible number *n* of VBS Group IDs, is required, the excess bytes shall be set to 'FF'.

10.3.23 EF_{VBSS} (Voice Broadcast Service Status)

This EF contains the status of activation for the VBS group identifiers. The elementary file is directly related to the EF_{VBS}. This EF shall always be allocated if EF_{VBS} is allocated.

Identifier: '6FB4'	Structure: transparent	Optional
File size: 7 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 7	Activation/Deactivation Flags	M	7 bytes

- Activation/Deactivation Flags

  Contents: Activation/Deactivation Flags of the appropriate Group IDs

  Coding:

  see coding of EF_{VGCSS}

10.3.24 EF_{eMLPP} (enhanced Multi Level Pre-emption and Priority)

This EF contains information about priority levels and fast call set-up conditions for the enhanced Multi Level Pre-emption and Priority service that which can be used by the subscriber.

Identifier: '6FB5'	Structure: transparent	Optional
File size: 2 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

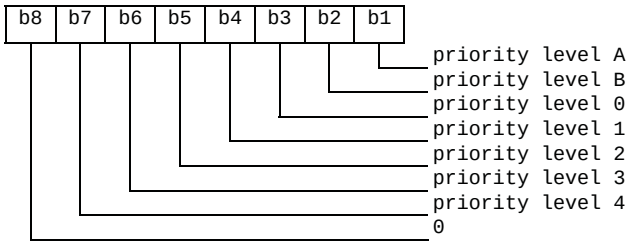
Bytes	Description	M/O	Length
1	Priority levels	M	1 byte
2	Fast call set-up conditions	M	1 byte

- Priority levels

  Contents: The eMLPP priority levels subscribed to.

  Coding: Each eMLPP priority level is coded on one bit. Priority levels subscribed to have their corresponding bits set to 1. Priority levels not subscribed to have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

  Byte 1:



NOTE: Priority levels A and B can not be subscribed to (see TS 22.067 [42] for details).

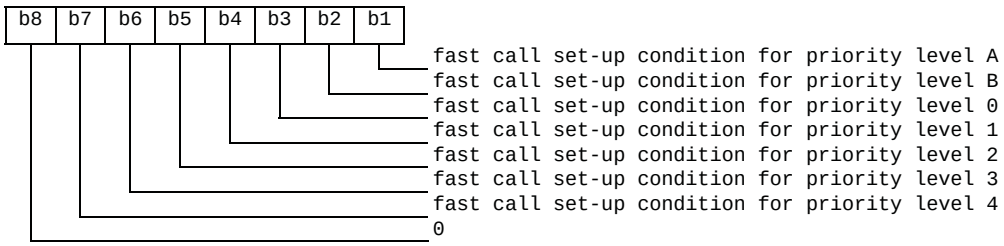
EXAMPLE 1: If priority levels 0, 1 and 2 are subscribed to, EF_{eMLPP} shall be coded '1C'.

- Fast call set-up conditions

  Contents: For each eMLPP priority level, the capability to use a fast call set-up procedure.

  Coding: Each eMLPP priority level is coded on one bit. Priority levels for which fast call set-up is allowed have their corresponding bits set to 1. Priority levels for which fast call set-up is not allowed have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

  Byte 2: fast call set-up condition for:



EXAMPLE 2: If fast call set-up is allowed for priority levels 0 and 1, then byte 2 of EF_{eMLPP} is coded '0C'.

10.3.25 EF_{AAeM} (Automatic Answer for eMLPP Service)

This EF contains those priority levels (of the Multi Level Pre-emption and Priority service) for which the mobile station shall answer automatically to incoming calls.

Identifier: '6FB6'	Structure: transparent	Optional
File size: 1 byte	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Automatic answer priority levels	M	1 byte

- Automatic answer priority levels

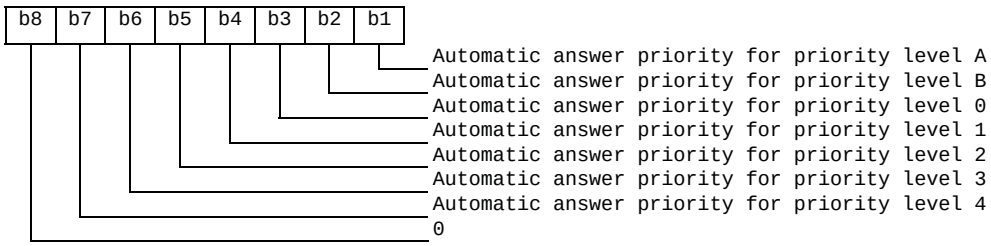
  Contents:

  For each eMLPP priority level, the capability for the mobile station to answer automatically to incoming calls (with the corresponding eMLPP priority level).

  Coding:

  Each eMLPP priority level is coded on one bit. Priority levels allowing an automatic answer from the mobile station have their corresponding bits set to 1. Priority levels not allowing an automatic answer from the mobile station have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

Byte 1:



EXAMPLE: If automatic answer is allowed for incoming calls with priority levels A, 0 and 1, then $EF_{AAeMLPP}$ is coded '0D'.

10.3.26 EF_{CBMID} (Cell Broadcast Message Identifier for Data Download)

This EF contains the message identifier parameters which specify the type of content of the cell broadcast messages which are to be passed to the SIM.

Any number of CB message identifier parameters may be stored in the SIM. No order of priority is applicable.

Identifier: '6F48'	Structure: transparent	Optional
File size: 2n bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 2	CB Message Identifier 1	O	2 bytes
3 to 4	CB Message Identifier 2	O	2 bytes
2n-1 to 2n	CB Message Identifier n	O	2 bytes

- Cell Broadcast Message Identifier

  Coding:

  as in TS 23.041 [14]. Values listed show the identifiers of messages which shall be accepted by the MS to be passed to the SIM.

  Unused entries shall be set to 'FF FF'.

10.3.27 EF_{ECC} (Emergency Call Codes)

This EF contains up to 5 emergency call codes.

Identifier: '6FB7'	Structure: transparent	Optional
File size: 3n (n ≤ 5) bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 3	Emergency Call Code 1	O	3 bytes
4 to 6	Emergency Call Code 2	O	3 bytes
(3n-2) to 3n	Emergency Call Code n	O	3 bytes

- Emergency Call Code

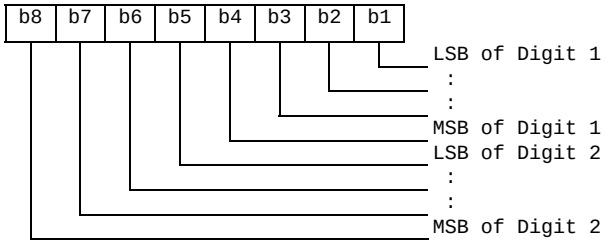
Contents:

Emergency Call Code

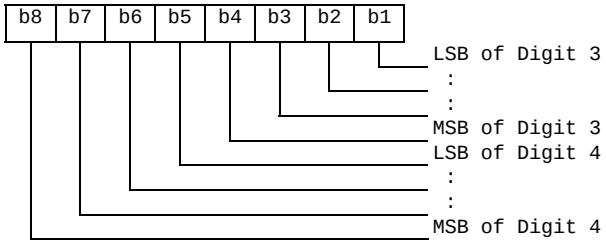
Coding:

The emergency call code is of a variable length with a maximum length of 6 digits. Each emergency call code is coded on three bytes, with each digit within the code being coded on four bits as shown below. If a code of less that 6 digits is chosen, then the unused nibbles shall be set to 'F'.

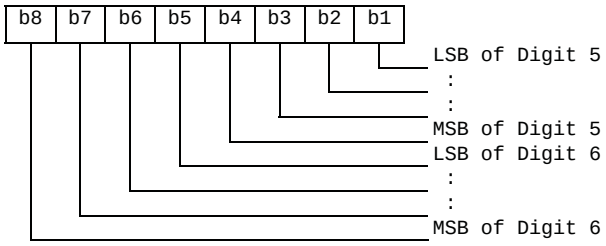
Byte 1:



Byte 2:



Byte 3:



10.3.28 EF_{CBMIR} (Cell broadcast message identifier range selection)

This EF contains ranges of cell broadcast message identifiers that the subscriber wishes the MS to accept.

Any number of CB Message Identifier Parameter ranges may be stored in the SIM. No order of priority is applicable.

Identifier: '6F50'	Structure: transparent	Optional
File size: 4n bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 4	CB Message Identifier Range 1	O	4 bytes
5 to 8	CB Message Identifier Range 2	O	4 bytes
(4n-3) to 4n	CB Message Identifier Range n	O	4 bytes

- Cell Broadcast Message Identifier Ranges

  Contents:

  CB Message Identifier ranges:

  Coding:

  bytes one and two of each range identifier equal the lower value of a cell broadcast range, bytes three and four equal the upper value of a cell broadcast range, both values are coded as in TS 23.041 [14] "Message Format on BTS-MS Interface - Message Identifier". Values listed show the ranges of messages which shall be accepted by the MS.

  Unused entries shall be set to 'FF FF FF FF'.

10.3.29 EF_{DCK} De-personalization Control Keys

This EF provides storage for the de-personalization control keys associated with the OTA de-personalization cycle of TS 22.022.

Identifier: '6F2C'	Structure: transparent	Optional
File size: 16 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 4	8 digits of network de-personalization control key	M	4 bytes
5 to 8	8 digits of network subset de-personalization control key	M	4 bytes
9 to 12	8 digits of service provider de-personalization control key	M	4 bytes
13 to 16	8 digits of corporate de-personalization control key	M	4 bytes

Empty control key records shall be coded 'FFFFFFFF'.

10.3.30 EF_{CNL} (Co-operative Network List)

This EF contains the Co-operative Network List for the multiple network personalization services defined in TS 22.022.

Identifier: '6F32'	Structure: transparent	Optional
File size: 6n bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 6	Element 1 of co-operative net list	O	6 bytes
6n-5 to 6n	Element n of co-operative net list	O	6 bytes

- Co-operative Network List

  Contents:

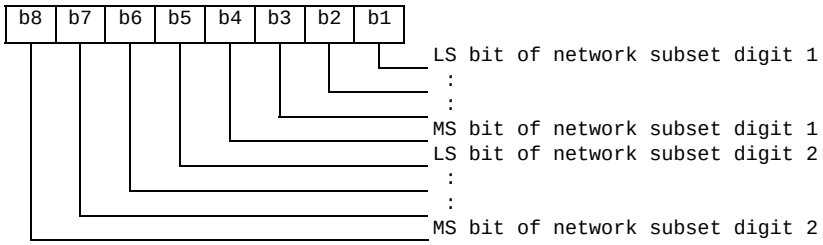
  PLMN network subset, service provider ID and corporate ID of co-operative networks.

  Coding:

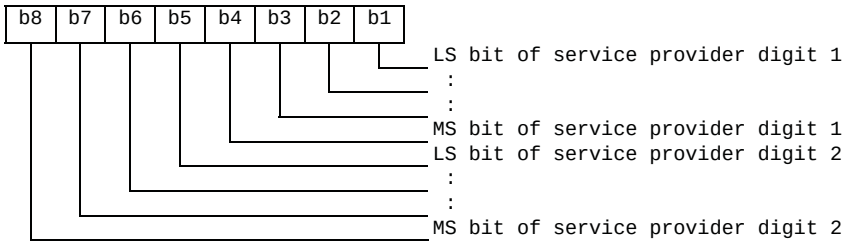
  For each 6 byte list element

  Byte 1 to 3 : PLMN (MCC + MNC) : according to TS 24.008 [47].

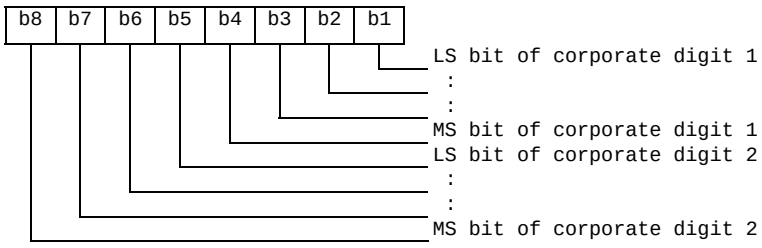
  Byte 4:



  Byte 5:



  Byte 6:



Empty fields shall be coded with 'FF'.

The end of the list is delimited by the first MCC field coded 'FFF'.

10.3.31 EF_{NIA} (Network's Indication of Alerting)

This EF contains categories and associated text related to the Network's indication of alerting in the MS service defined in TS 22.101 [53].

Identifier: '6F51'	Structure: linear fixed	Optional
Record length : X+1 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Alerting category	M	1 byte
2 to X+1	Informative text	M	X bytes

- Alerting category

  Contents:

  category of alerting for terminating traffic.

  Coding:

  according to TS 24.008 [47]. Value 'FF' means that no information on alerting category is available.

- Informative text

  Contents:

  text describing the type of terminating traffic associated with the category.

  Coding:

  see the coding of the Alpha Identifier item of the EF_{ADN} (clause 10.5.1). The maximum number of characters for this informative text is indicated in TS 22.101 [53].

10.3.32 EF_{KcGPRS} (GPRS Ciphering key KcGPRS)

This EF contains the ciphering key KcGPRS and the ciphering key sequence number n for GPRS (see TS 23.060 [32]).

Identifier: '6F52'	Structure: transparent	Optional
File size: 9 bytes	Update activity: high	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 8	Ciphering key KcGPRS	M	8 bytes
9	Ciphering key sequence number n for GPRS	M	1 byte

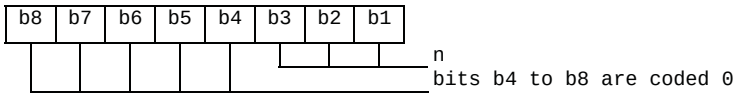
- Ciphering key KcGPRS

  Coding:

The least significant bit of KcGPRS is the least significant bit of the eighth byte. The most significant bit of KcGPRS is the most significant bit of the first byte.

- Ciphering key sequence number n for GPRS

  Coding:



NOTE: TS 24.008 [47] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

10.3.33 $EF_{LOCIGPRS}$ (GPRS location information)

This EF contains the following Location Information:

- Packet Temporary Mobile Subscriber Identity (P-TMSI);
- Packet Temporary Mobile Subscriber Identity signature value (P-TMSI signature value);
- Routing Area Information (RAI);
- Routing Area update status.

Identifier: '6F53'	Structure: transparent	Optional
File size: 14 bytes	Update activity: high	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

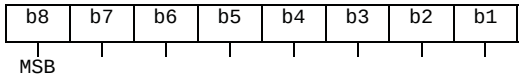
Bytes	Description	M/O	Length
1 to 4	P-TMSI	M	4 bytes
5 to 7	P-TMSI signature value	M	3 bytes
8 to 13	RAI	M	6 bytes
14	Routing Area update status	M	1 byte

- P-TMSI

  Contents: Packet Temporary Mobile Subscriber Identity

  Coding: according to TS 24.008 [47].

  Byte 1: first byte of P-TMSI

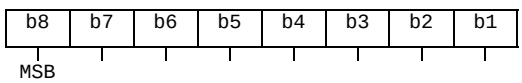


- P-TMSI signature value

  Contents: Packet Temporary Mobile Subscriber Identity signature value

  Coding: according to TS 24.008 [47].

  Byte 5: first byte of P-TMSI signature value

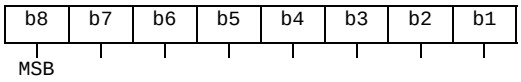


- RAI

  Contents: Routing Area Information

  Coding: according to TS 24.008 [47].

  Byte 8: first byte of RAI



- Routing area update status

  Contents: status of routing area update according to TS 24.008 [47].

  Coding:

  Byte 14:

  Bits: b3 b2 b1

  0 0 0 : updated
  0 0 1 : not updated
  0 1 0 : PLMN not allowed
  0 1 1 : Routing Area not allowed
  1 1 1 : reserved

  Bits b4 to b8 are RFU (see clause 9.3).

10.3.34 EF_{SUME} (SetUpMenu Elements)

This EF contains Simple TLVs related to the menu title to be used by a SIM card supporting the SIM API when issuing a SET UP MENU proactive command.

Identifier: '6F54'	Structure: transparent	Optional
File size: X+Y bytes	Update activity: low	

Access Conditions:

READ	ADM
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Title Alpha Identifier	M	X bytes
1+X to X+Y	Title Icon Identifier	O	Y bytes

- Title Alpha Identifier

  Contents:

  this field contains the Alpha Identifier Simple TLV defining the menu title text.

  Coding:

  according to TS 51.014 [27].

- Title Icon Identifier

  Contents:

  this field contains the Icon Identifier Simple TLV defining the menu title icon.

  Coding:

  according to TS 51.014 [27].
  If not present the field shall be set to 'FF'.

Unused bytes of this file shall be set to 'FF'.

10.3.35 $EF_{PLMNwAcT}$ (User controlled PLMN Selector with Access Technology)

This EF contains coding for n PLMNs, where n is at least eight. This information, determined by the user, defines the preferred PLMNs of the user in priority order. The EF also contains the Access Technologies for each PLMN in this list. (see TS 23.122 [51]).

Identifier:'6F60'	Structure: transparent	Optional
File size: 5n (n ≥ 8) bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes
6 to 8	2nd PLMN	M	3 bytes
9 to 10	2nd PLMN Access Technology Identifier	M	2 bytes
:	:		
36 to 38	8th PLMN	M	3 bytes
39 to 40	8th PLMN Access Technology Identifier	M	2 bytes
41 to 43	9th PLMN	O	3 bytes
44 to 45	9th PLMN Access Technology Identifier	O	2 bytes
:	:		
(5n-4) to (5n-2)	Nth PLMN (lowest priority)	O	3 bytes
(5n-1) to 5n	Nth PLMN Access Technology Identifier	O	2 bytes

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

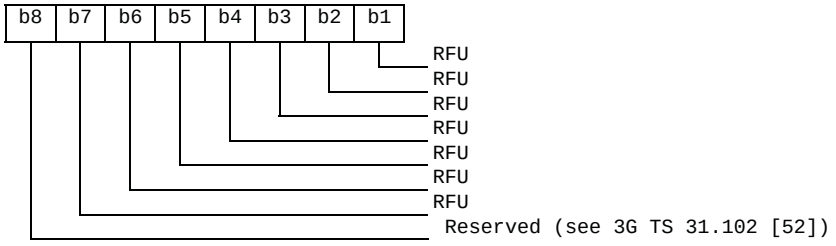
  according to TS 24.008 [47].

- Access Technologies

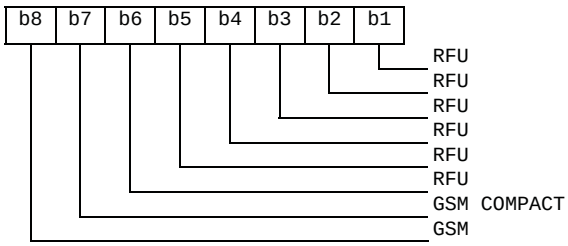
  Contents: The Access Technologies of a PLMN that the MS will assume when searching for a listed PLMN.

  Coding:
  - 2 bytes are used to select the access technology where the meaning of each bit is as follows:
    - bit = 1: access technology selected;
    - bit = 0: access technology not selected.

Byte 5n-1:



Byte 5n:



The RFU bits are coded with '0' in the bit positions.

10.3.36 $EF_{OPLMNwAcT}$ (Operator controlled PLMN Selector with Access Technology)

This EF contains coding for n PLMNs, where n is at least eight. This information, determined by the operator, defines the preferred PLMNs of the operator in priority order. The EF also contains the Access Technologies for each PLMN in this list (see TS 23.122 [51]).

Identifier: '6F61'	Structure: transparent	Optional
File size: 5n (n ≥ 8) bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes
:	:		
36 to 38	8th PLMN	M	3 bytes
39 to 40	8th PLMN Access Technology Identifier	M	2 bytes
41 to 43	9th PLMN	O	3 bytes
44 to 45	9th PLMN Access Technology Identifier	O	2 bytes
:	:		
(5n-4) to (5n-2)	Nth PLMN (lowest priority)	O	3 bytes
(5n-1) to 5n	Nth PLMN Access Technology Identifier	O	2 bytes

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

  according to TS 24.008 [47].

- Access Technologies

  Contents: The Access Technologies of a PLMN that the MS will assume when searching for a listed PLMN.

  Coding: See $EF_{PLMNwAcT}$ for coding.

10.3.37 $EF_{HPLMNwAcT}$ (HPLMN Selector with Access Technology)

The HPLMN Selector with access technology data field shall contain the HPLMN code, or codes together with the respective access technology in priority order (see TS 23.122 [51]).

Identifier: '6F62'	Structure: transparent	Optional
File size: 5n (n ≥ 1) bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 3	1st PLMN (highest priority)	M	3 bytes
4 to 5	1st PLMN Access Technology Identifier	M	2 bytes
6 to 8	2nd PLMN	O	3 bytes
9 to 10	2nd PLMN Access Technology Identifier	O	2 bytes
:	:		
(5n-4) to (5n-2)	nth PLMN (lowest priority)	O	3 bytes
(5n-1) to 5n	nth PLMN Access Technology Identifier	O	2 bytes

- PLMN
  Contents:
  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).
  Coding:
  according to TS 24.008 [47].

- Access Technology

  Contents: The Access Technology of the HPLMN that the MS will assume when searching for the HPLMN, in priority order. The first Access Technology in the list has the highest priority.

  Coding: See $EF_{PLMNwAcT}$ for coding.

10.3.38 EF_{CPBCCH} (CPBCCH Information)

This EF contains information concerning the CPBCCH according to TS 04.18 [48] and TS 03.22 [45].

CPBCCH storage may reduce the extent of a Mobile Station's search of CPBCCH carriers when selecting a cell. The CPBCCH carrier lists shall be in accordance with the procedures specified in TS 04.18 [48], TS 04.60 [49] and TS 03.22 [45]. The MS stores CPBCCH information from the System Information 19 message, Packet System Information 3, and Packet System Information 3 bis on the SIM. The same CPBCCH carrier shall never occur twice in the list.

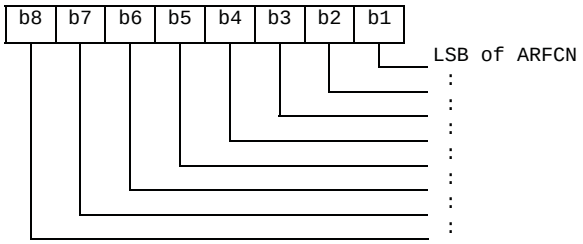
Identifier: '6F63'	Structure: transparent	Optional
File size: 2n bytes	Update activity: high	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 2	Element 1 of CPBCCH carrier list	M	2 bytes
2n-1 to 2n	Element n of CPBCCH carrier list	M	2 bytes

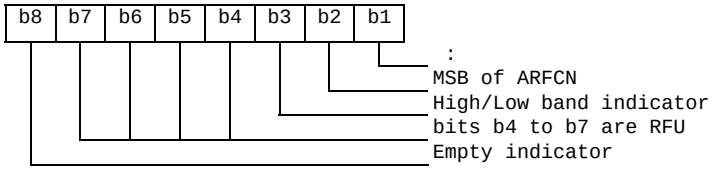
- Element in CPBCCH carrier list

Coding:

Byte 1: first byte of CPBCCH carrier list element



Byte 2: second byte of CPBCCH carrier list element



- ARFCN (10 bits) as defined in TS 05.05 [46].
- High/Low band indicator: If the ARFCN indicates possibly a channel in the DCS 1800 or a channel in the PCS 1900 band, if the bit is set to '1' the channel is in the higher band (GSM 1900). If the bit is set to '0', the lower band (GSM 1800) is indicated. If ARFCN indicates a unique channel, this indicator shall be set to '0'.
- Empty indicator: If this bit is set to '1', no CPBCCH carrier is stored in this position. If the Empty Indicator is set to '1', the content of the CPBCCH carrier field shall be ignored. The empty indicator shall also be used, and set to '1', if storage of fewer than maximum number n, of CPBCCH carrier fields is required.

10.3.39 $EF_{InvScan}$ (Investigation Scan)

This EF contains two flags used to control the investigation scan for higher prioritized PLMNs not offering voice services.

Identifier: '6F64'	Structure: transparent	Optional
File size: 1 byte	Update activity: low	

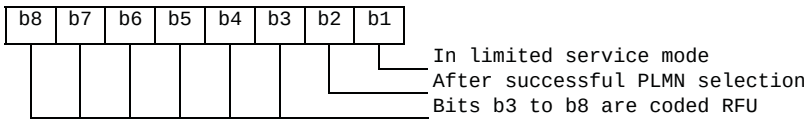
Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Investigation scan flags	M	1 bytes

- Investigation scan flags

Coding:



A '1' in a bit position indicates that the investigation scan shall be performed for the condition corresponding to that bit position and a '0' that it shall not be performed.

If this elementary file is not present, no investigation scan shall be performed.

10.3.40 Void

10.3.41 EF_{PNN} (PLMN Network Name)

This EF contains the full and short form versions of the network name for the registered PLMN. The ME shall use these versions in place of its own versions of the network name for the PLMN (stored in the ME's memory list), and also in place of the versions of the network name received when registered to the PLMN, as defined by 3G TS 24.008 [47].

The first record in this EF is used for the default network name when registered to the HPLMN. Subsequent records are to be used for other network names.

Identifier: '6FC5'	Structure: linear fixed	Optional
Record length: X bytes; X ≥ 3	Update activity: low	

Access Conditions:

READ	ALWAYS
UPDATE	ADM
ACTIVATE	ADM
DEACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Network name TLV objects	M	X bytes

- Network Name TLV objects.
  The content and coding (Full name for network and Short name for network) is defined below, where the fields within the objects are defined in 3G TS 24.008 [47]:

Coding of the Network Name TLV objects

Length	Description	Status
1 byte	Full name for network IEI (This shall be the same as that used in the MM information message).	M
1 byte	Length of Full name for network Name contents	M
Y bytes	Full name for network contents (Octets 3 to n of network name information element)	M
1 byte	Short name for network IEI (This shall be the same as that used in the MM information message).	O
1 byte	Length of Short name for network	C1
Z bytes	Short name for network contents (Octets 3 to n of network name information element)	C1
C1: this field shall be present if the short name for network IEI is present		

Unused bytes shall be set to 'FF'.

10.3.42 EF_{OPL} (Operator PLMN List)

This EF contains a prioritised list of Location Area Information (LAI) identities that are used to associate a specific operator name contained in EF_{PNN} with the LAI. The ME shall use this EF in association with the EF_{PNN} in place of any network name stored within the ME's internal list and any network name received when registered to the PLMN, as defined by 3G TS 24.008 [47].

If the EF_{PNN} is not present then this file shall not be present.

Identifier: '6FC6'	Structure: linear fixed	Optional
Record length: X bytes, X >= 8	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 7	Location Area Identity	M	7 bytes
8	PLMN Network Name Record Identifier	M	1 byte

- Location Area Identity

  Contents:

  Location Area Information, this comprises of the MCC, MNC and two LACs

  Coding:

  PLMN: according to TS 24.008 [47]

  A BCD value of 'D' in any of the MCC and/or MNC digits shall be used to indicate a "wild" value for that corresponding MCC/MNC digit

  LAC : according to 3G TS 24.008 [47]

  Two values for the LAC are stored in order to allow a range of LAC values to be specified for a given PLMN. A value of '0000' stored in bytes 4 to 5 and a value of 'FFFE' stored in bytes 6 to 7 shall be used to indicate the entire range of LACs for the given PLMN. In the case where only a single LAC value is to be specified then the value stored in bytes 4 to 5 shall be identical to the value stored in bytes 6 to 7 for the given PLMN. If a range of LAC values are to be specified, then the value stored in bytes 4 to 5 shall be the start of the LAC range and the value stored in bytes 6 to 7 shall be the end of the LAC range for the given PLMN.

- PLMN Network Name Record Identifier

  Contents:

  Identifier of operator name to be displayed

  Coding:

  A value of '00' indicates that the name is to be taken from other sources, see 3G TS 22.101 [53]

  A value in the range '01' to 'FE' indicates the record number in EF_{PNN} that shall be displayed as the registered PLMN name

NOTE: The intent of this file is to provide exceptions to the other sources of a network name. Care should be taken not to introduce too many PLMN entries. An excessive number of entries could result in a longer initialisation period.

10.3.43 EF_{MBDN} (Mailbox Dialling Numbers)

This EF contains dialling numbers to access mailboxes associated with Voicemail, Fax, Electronic Mail and other messages. It may also contain associated alpha-tags for each supported mailbox. Each dialling number shall be associated with a message waiting indication group type using EF_{MBI} (see 3G TS 23.038 [12] for message waiting indication group types).

This EF is mandatory if EF_{SST} indicates that the Mailbox Dialling Numbers service is available.

Identifier: '6FC7'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1/ADM (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC contents	M	10 bytes
X+13	Extended Capability Configuration Parameters	M	1 byte
X+14	Extension 6 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (clause 10.5.1), with the exception that extension records are stored in the EF_{EXT6} and with the exception that Capability/Configuration parameters are stored in the EF_{ECCP}

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

10.3.44 EF_{MBI} (Mailbox Identifier)

This EF contains information to associate mailbox dialling numbers in EF_{MBDN} with a message waiting indication group type and subscriber profile (as defined in 3G TS 23.097 [54]). A message waiting indication group type may either be Voicemail, Fax, Electronic Mail or Other (as defined in 3G TS 23.038 [12] for Data Coding Scheme).

This EF contains as many records as there are subscriber profiles (shall be record to subscriber profile). Each record contains references to mailbox dialling numbers in EF_{MBDN} (one reference for each message waiting indication group type).

This EF is mandatory if EF_{SST} indicates that the Mailbox Dialling Numbers service is available.

Identifier: '6FC9'	Structure: linear fixed	Optional
Record length: X bytes, X>=4	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1/ADM (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Mailbox Dialling Number Identifier – Voicemail	M	1 byte
2	Mailbox Dialling Number Identifier – Fax	M	1 byte
3	Mailbox Dialling Number Identifier – Electronic Mail	M	1 byte
4	Mailbox Dialling Number Identifier – Other	M	1byte

- Mailbox Dialling Number Identifier (message waiting group type = Voicemail, Fax, Electronic Mail or Other).
  Contents:
  Identifies the mailbox dialling number to be associated with message waiting type.

  Coding:
  '00' – no mailbox dialling number associated with message waiting indication group type
  'xx' – record number in EF_{MBDN} associated with message waiting indication group type

10.3.45 EF_{MWIS} (Message Waiting Indication Status)

This EF contains the status of indicators that define whether or not a Voicemail, Fax, Electronic Mail or Other message is waiting (as defined in 3G TS 23.038 [12] for message waiting indication group types). The ME uses the status after re-activation to determine whether or not to display the respective message-waiting indication on its display.

This EF contains as many records as there are subscriber profiles (shall be record to subscriber profile) as defined in 3G TS 23.097 [54] for MSP.

Identifier: '6FCA'	Structure: Linear fixed	Optional
Record length: X bytes, X >= 5	Update activity: high	

Access Conditions:

READ	CHV1
UPDATE	CHV1
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Message Waiting Indicator Status	M	1 byte
2	Number of Voicemail Messages Waiting	M	1 byte
3	Number of Fax Messages Waiting	M	1 byte
4	Number of Electronic Mail Messages Waiting	M	1 byte
5	Number of Other Messages Waiting	M	1 byte

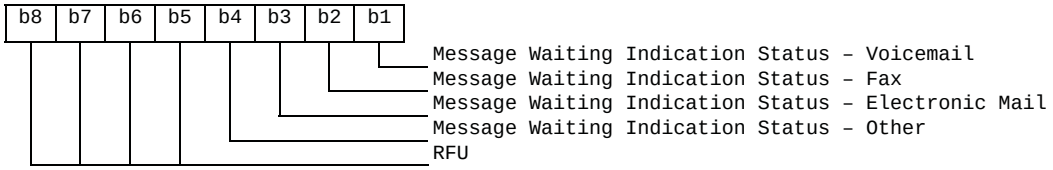
Message Waiting Indication Status

Contents:

Indicates the status of the message-waiting indication.

Coding:

The indicator status for each indicator type is 1 bit long and set as follows:
bit = 1: Set Indication Active
bit = 0: Set Indication Inactive



Number of Voicemail Messages Waiting

Contents:

Contains the number of voicemail messages waiting (see 3G TS 23.040 [13]).

Coding:

Binary.

Number of Fax Messages Waiting

Contents:

Contains the number of fax messages waiting (see 3G TS 23.040 [13]).

Coding:

Binary.

Number of Electronic Mail Messages Waiting

Contents:

Contains the number of electronic mail messages waiting (see 3G TS 23.040 [13])

Coding:

Binary.

Number of Other Messages Waiting

Contents:

Contains the number of other messages waiting (see 3G TS 23.040 [13]).

Coding:

Binary.

10.3.46 EF_{CFIS} (Call Forwarding Indication Status)

This EF contains the status of indicators that are used to record whether call forward is active. The ME uses the status after re-activation to determine whether or not to display the respective Call Forwarding indicator on its display.

This EF contains as many records as there are subscriber profiles (shall be record to subscriber profile) as defined in 3G TS 23.097 [54] for MSP.

Identifier: '6FCB'	Structure: Linear Fixed	Optional
Record length: 16 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	MSP number	M	1 byte
2	CFU indicator status	M	1 byte
3	Length of BCD number	M	1 byte
4	TON and NPI	M	1 byte
5 to 14	Dialling Number	M	10 bytes
15	Extended Capability Configuration Parameters	M	1 byte
16	Extension 7 Record Identifier	M	1 byte

NOTE: For contents and coding of data items not detailed below, see the respective data items of EF_{ADN} (subclause 10.5.1), with the exception that Capability/Configuration parameters are stored in the EF_{ECCP} and Extension 7 Record Identifier is used.

MSP number:

Contents:

The MSP number contains the Profile Identity of the subscriber profile. The Profile Identity shall be between 1and 4 as defined in 3G TS 23.097 [54] for MSP.

Coding:

Binary.

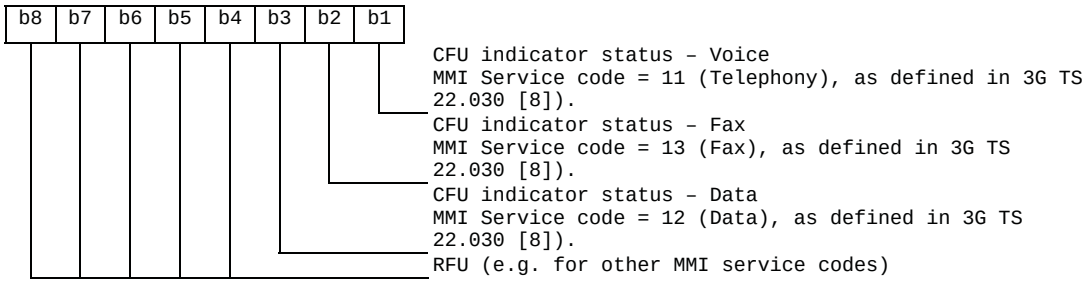
CFU indicator status:

Contents:

Indicates the status of the call forward unconditional indicator. Service code = 21 (CFU) or 002 (for CFU part of all CF), as defined in 3G TS 22.030 [8]

Coding:

The indicator status for each indicator type is 1 bit long and is set as follows:
bit = 1: Set indication active
bit = 0: Set indication inactive



10.3.47 EF_{EXT5} (Extension5)

This EF is not used

10.3.48 EF_{EXT6} (Extension6)

This EF contains extension data of an MBDN (see MBDN in 10.3.43).

Identifier: '6FC8'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1/ADM (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding, see clause 10.5.10 (EF_{EXT1}).

10.3.49 EF_{EXT7} (Extension7)

This EF contains extension data of a CFIS (Call Forwarding Indication Status - see 10.3.46).

Identifier: '6FCC'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see clause 10.5.10 (EF_{EXT1}).

10.3.50 EF_{SPDI} (Service Provider Display Information)

This EF contains information regarding the service provider display i.e. the service provider PLMN list.

Identifier: '6FCD'	Structure: transparent	Optional
File size: x bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to x	TLV object(s) containing Service Provider Information	M	x bytes

Tag Value	Tag Description
'A3'	Service Provider Display Information Tag
'80'	Service Provider PLMN List Tag

The Service Provider Display Information object is a constructed TLV.

- Service Provider PLMN List
  Contents:
  This TLV contains a list of n PLMNs in which the Service Provider Name shall be displayed, as defined in subclause 10.3.11 (EF_{SPN}).

  Coding:

Description	M/O	Length
Service Provider PLMN List tag	M	1 byte
Length (see note)	M	x bytes
1st PLMN entry	M	3 bytes
2nd PLMN entry	O	3 bytes
3rd PLMN entry	O	3 bytes
…		
nth PLMN entry	O	3 bytes
Note: the length is 3*n bytes, where n denotes the number of PLMN entries. The length can be coded on one or more bytes.		

  Each PLMN is coded as follows:
  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC) according to TS 24.008 [47].
  In case a PLMN entry is not used, it shall be set to 'FF FF FF'.

10.3.51 EF_{MMSN} (MMS Notification)

If service n°57 is "allocated and activated", this file shall be present.

This EF contains information in accordance with 3GPP TS 23.140 [58] comprising MMS notifications (and associated parameters) which have been received by the UE from the network.

Identifier: "6FCE"	Structure: Linear fixed	Optional
Record length: 4+X bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 2	MMS Status	M	2 bytes
3	MMS Implementation	M	1 byte
4 to X+3	MMS Notification	M	X bytes
X+4	Extension file record number	M	1 byte

- MMS Status

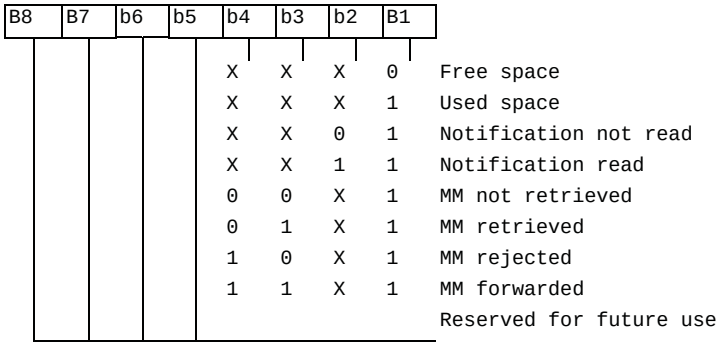
Content:

The status bytes contain the status information of the notification.

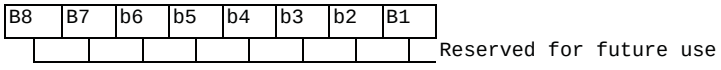
Coding:

b1 indicates whether there is valid data or if the location is free. b2 indicates whether the MMS notification has been read or not. Bits b3-b4 of the first byte indicate the MM retrieval, MM rejection, or MM forwarding status, Bits b5-b8 of the first byte and the entire second byte are reserved for future use.

First byte:



Second byte:



- MMS Implementation

Contents:

The MMS Implementation indicates the used implementation type, e.g. WAP.

Coding:

Allocation of bits:

Bit number	Parameter indicated
1	WAP implementation of MMS
2-8	Reserved for future use

Bit value Meaning

0 Implementation not supported.

1 Implementation supported.

- MMS Notification

  Contents:

  The MMS Notification contains the MMS notification.

  Coding:

  The MMS Notification is coded according to the MMS Implementation as indicated in Byte 3.

  Any unused byte shall be set to 'FF'.

- Extension file record number

  Contents:

  extension file record number. This byte identifies the number of a record in the EF_{EXT8} containing extension data for the notification information. The use of this byte is optional. If it is not used it shall be set to 'FF'.

  Coding:

  binary

10.3.52 EF_{EXT8} (Extension 8)

If service n°58 is "allocated and activated", this file shall be present.

This EF contains extension data of a MMS Notification (Multimedia Messaging Service - see 10.3.51).

Identifier: '6FCF'	Structure: linear fixed	Optional
Record length: X+2 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to X+1	Extension data	M	X bytes
X+2	Identifier	M	1 byte

For contents and coding see clause 10.5.10 (EF_{EXT1}).

10.3.53 EF_{MMSICP} (MMS Issuer Connectivity Parameters)

If service n°57 is "allocated and activated", this file shall be present.

This EF contains values for Multimedia Messaging Connectivity Parameters as determined by the issuer, which can be used by the ME for user assistance in preparation of connecting to the network for the MMS purpose network connection. This file may contain one or more sets of Multimedia Messaging Issuer Connectivity Parameters. The first set of Multimedia Messaging Issuer Connectivity Parameters is used as the default set. Each set of Multimedia Messaging Issuer Connectivity Parameters may consist of one or more Interface to Core Network and Bearer information TLV objects, but shall contain only one MMS implementation TLV object, one MMS Relay/Server TLV object and one Gateway TLV object. The order of the Interface to Core Network and Bearer information TLV objects in

the MMS Connectivity TLV object defines the priority of the Interface to Core Network and Bearer information, with the first TLV object having the highest priority.

Identifier: '6FD0'	Structure: Transparent	Optional
File Size: X_1+…+ X_n bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X_1	MMS Connectivity Parameters TLV object	M	X_1bytes
X_1+1 to X_1 + X_2	MMS Connectivity Parameters TLV object	O	X_2 bytes
…	…		
X_1+…+ X_{n-1}+1 to X_1+…+ X_n	MMS Connectivity Parameters TLV object	O	X_n bytes

- MMS Connectivity Parameters tags

Description	Tag Value
MMS Connectivity Parameters Tag	'AB'
MMS Implementation Tag	"80"
MMS Relay/Server Tag	"81"
Interface to Core Network and Bearer Information Tag	'82'
Gateway Tag	'83'

- MMS Connectivity Parameters contents

Description	Value	M/O	Length (bytes)
MMS Connectivity Parameters Tag	'AB'	M	1
Length	Note 1	M	Note 2
MMS Implementation Tag	'80'	M	1
Length	1	M	Note 1
MMS Implementation Information	--	M	1
MMS Relay/Server Tag	'81'	M	1
Length	X	M	Note 2
MMS Relay/Server Address	--	M	X
1st Interface to Core Network and Bearer Information Tag (highest priority)	'82'	M	1
Length	Y1	M	Note 2
1st Interface to Core Network and Bearer information	--	M	Y1
2nd Interface to Core Network and Bearer Information Tag	'82'	O	1
Length	Y2	O	Note 2
2nd Interface to Core Network and Bearer information	--	O	Y2
…	…	…	…
nth Interface to Core Network and Bearer Information Tag (lowest priority)	'82'	O	1
Length	Y3	O	Note 2
Interface to Core Network and Bearer information	--	O	Y3
Gateway Tag	'83'	O	1
Length	Z	O	Note 2
Gateway Information	--	O	Z
Note 1: This is the total size of the constructed TLV object Note 2: The length is coded according to ISO/IEC 8825 [56]			

- MMS Implementation Tag '80'

  See section 10.3.51 for contents and coding.

- MMS Relay/server Tag '81'

  Contents:

  The MMS relay/server contains the address of the associated MMS relay/server.

  Coding:

  The MMS relay/server address is coded according to the guideline provided in 3GPP TS 23.140 [58].

- Interface to Core Network and Bearer Information Tag '82'

  Contents:

  The Interface to Core Network and Bearer Information may contain the following information to set up the bearer: Bearer, Address, Type of address, Speed, Call type, Authentication type, Authentication id, Authentication password.

  Coding:

  The coding is according to the guideline provided in 3GPP TS 23.140 [58].

- Gateway Tag '83'

  Contents:

  The Gateway may contain the following information; Address, Type of address, Port, Service, Authentication type, Authentication id and Authentication password.

  Coding:

  The coding is according to the guideline provided in 3GPP TS 23.140 [58].

  Unused bytes shall be set to 'FF'.

An Example for the coding of these parameters can be found in Annex K.2.

10.3.54 EF_{MMSUP} (MMS User Preferences)

If service n°57 is "allocated and activated", this file shall be present.

This EF contains values for Multimedia Messaging Service User Preferences, which can be used by the ME for user assistance in preparation of mobile multimedia messages (e.g. default values for parameters that are often used).

Identifier: '6FD1'	Structure: Linear Fixed	Optional
Record Length: X bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X	MMS User Preference TLV Objects	M	X bytes

- MMS User Preference tags

Description	Tag Value
MMS Implementation Tag	'80'
MMS User preference profile name Tag	'81'
MMS User Preference information Tag	'82'

- MMS User Preference information

Description	Value	M/O	Length (bytes)
MMS Implementation Tag	'80'	M	1
Length	1	M	Note
MMS Implementation information	--	M	1
MMS User preference profile name Tag	'81'	M	1
Length	X	M	Note
MMS User profile name	--	M	X
MMS User Preference information Tag	'82'	M	1
Length	Y	M	Note
MMS User Preference information	--	M	Y
Note: The length is coded according to ISO/IEC 8825 [56]			

- MMS Implementation Tag '80'

  For contents and coding see 10.3.51

- MMS User preference profile name Tag '81'

  Contents:

  Alpha-tagging of the MMS user preference profile.

  Coding:

  this alpha-tagging shall use either:

  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [12] with bit 8 set to 0. The alpha identifier shall be left justified.

  or:

  - one of the UCS2 coded options as defined in the annex of TS 102 221 [55].

- MMS User Preference information Tag '82'

  Contents:

  The following information elements may be coded; Sender Visibility, Delivery Report, Read-Reply, Priority, Time of Expiry and Earliest Delivery Time.

  Coding:

  Depending upon the MMS implementation as indicated in Tag '80'.

An Example for the coding of these parameters can be found in Annex K.1.

10.3.55 EF_{MMSUCP} (MMS User Connectivity Parameters)

If service n°57 and n°59 are "allocated and activated", this file shall be present. The file shall provide the possibility to store at least 5 user connectivity parameter sets.

This EF contains values for Multimedia Messaging Connectivity Parameters as determined by the user, which can be used by the ME for MMS network connection. This file may contain one or more sets of Multimedia Messaging User Connectivity Parameters. Each set of Multimedia Messaging User Connectivity Parameters may consist of one or more

Interface to Core Network and Bearer information TLV objects, but shall contain only one MMS implementation TLV object, one MMS Relay/Server TLV object and one Gateway TLV object. The order of the Interface to Core Network and Bearer information TLV objects in the MMS Connectivity TLV object defines the priority of the Interface to Core Network and Bearer information, with the first TLV object having the highest priority.

Identifier: '6FD2'	Structure: Transparent	Optional
File Size: X_1+…+ X_n bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1/CHV2 (fixed during administrative management)
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to X_1	MMS Connectivity Parameters TLV objects	O	X_1bytes
X_1+1 to X_1 + X_2	MMS Connectivity Parameters TLV object	O	X_2 bytes
…	…		
X_1+…+ X_{n-1}+1 to X_1+…+ X_n	MMS Connectivity Parameters TLV object	O	X_n bytes

For the contents and coding see 10.3.53.

10.4 Contents of DFs at the GSM application level

10.4.1 Contents of files at the GSM SoLSA level

This clause specifies the EFs in the dedicated file DF_{SoLSA}. It only applies if the SoLSA feature is supported (see TS 23.073 [33]).

The EFs contain information about the users subscribed local service areas.

10.4.1.1 EF_{SAI} (SoLSA Access Indicator)

This EF contains the 'LSA only access indicator'. This EF shall always be allocated if DF_{SoLSA} is present.

If the indicator is set, the network will prevent terminated and/or originated calls when the MS is camped in cells that are not included in the list of allowed LSAs in EF_{SLL}. Emergency calls are, however, always allowed.

The EF also contains a text string which may be displayed when the MS is out of the served area(s).

Identifier: '4F30'	Structure: transparent	Optional
File size: X + 1 bytes	Update activity: low	

Access Conditions:

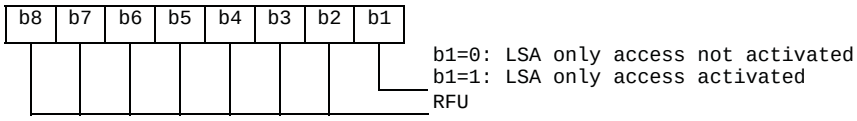
READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	LSA only access indicator	M	1 byte
2 to X+1	LSA only access indication text	M	X bytes

- LSA only access indicator

Contents: indicates whether the MS is restricted to use LSA cells only or not.

Coding:



- LSA only access indication text

  Contents: text to be displayed by the ME when it's out of LSA area.

  Coding: the string shall use either

  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [12] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or
  - one of the UCS2 coded options as defined in annex B.

10.4.1.2 EF_{SLL} (SoLSA LSA List)

This EF contains information describing the LSAs that the user is subscribed to. This EF shall always be allocated if DF_{SoLSA} is present.

Each LSA is described by one record that is linked to a LSA Descriptor file. Each record contains information of the PLMN, priority of the LSA, information about the subscription and may also contain a text string and/or an icon that identifies the LSA to the user. The text string can be edited by the user.

Identifier: '4F31'	Structure: linear fixed	Optional
Record length: X + 10 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to X	LSA name	O	X bytes
X+1	Configuration parameters	M	1 byte
X+2	RFU	M	1 byte
X+3	Icon Identifier	M	1 byte
X+4	Priority	M	1 byte
X+5 to X+7	PLMN code	M	3 bytes
X+8 to X+9	LSA Descriptor File Identifier	M	2 byte
X+10	LSA Descriptor Record Identifier	M	1 byte

- LSA name

  Contents: LSA name string to be displayed when the ME is camped in the corresponding area, dependant on the contents of the LSA indication for idle mode field.

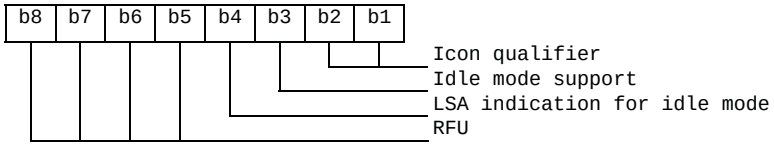
  Coding: the string shall use either

  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [12] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or
  - one of the UCS2 coded options as defined in annex B.

- Configuration parameters

  Contents: Icon qualifier, control of idle mode support and control of LSA indication for idle mode.

Coding:



Icon qualifier:

Contents: The icon qualifier indicates to the ME how the icon is to be used.

b2, b1: 00: icon is not to be used and may not be present
01: icon is self-explanatory, i.e. if displayed, it replaces the LSA name
10: icon is not self-explanatory, i.e. if displayed, it shall be displayed together with the LSA name
11: RFU

Idle mode support:

Contents: The idle mode support is used to indicate whether the ME shall favour camping on the LSA cells in idle mode.

b3 = 0: Idle mode support disabled
b3 = 1: Idle mode support enabled

LSA indication for idle mode:

Contents: The LSA indication for idle mode is used to indicate whether or not the ME shall display the LSA name when the ME is camped on a cell within the LSA.

b4 = 0: LSA indication for idle mode disabled
b4 = 1: LSA indication for idle mode enabled

Bits b5 to b8 are RFU (see clause 9.3).

- Icon Identifier

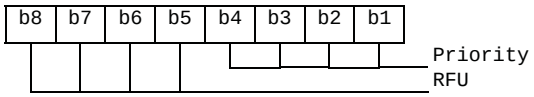
Contents: The icon identifier addresses a record in EF_{IMG}.

Coding: binary.

- Priority

Contents: Priority of the LSA which gives the ME the preference of this LSA relative to the other LSAs.

Coding:



'0' is lowest priority, 'F' is highest.

- PLMN code

Contents: MCC + MNC for the LSA.

Coding: according to TS 24.008 [47] and EF_{LOCI}.

- LSA Descriptor File Identifier:

Contents: these bytes identify the EF which contains the LSA Descriptors forming the LSA.

Coding: byte X+8: high byte of the LSA Descriptor file;
byte X+9: low byte of the LSA Descriptor file.

- LSA Descriptor Record Identifier:

Contents: this byte identifies the number of the first record in the LSA Descriptor file forming the LSA.

Coding: binary.

10.4.1.3 LSA Descriptor files

Residing under DF_{SoLSA}, there may be several LSA Descriptor files. These EFs contains one or more records again containing LSA Descriptors forming the LSAs. LSAs can be described in four different ways. As a list of LSA IDs, as a list of LAC + CIs, as a list of CIs or as a list of LACs. As the basic elements (LSA ID, LAC + CI, CI and LAC) of the four types of lists are of different length, they can not be mixed within one record. Different records may contain different kinds of lists within the EFs. Examples of codings of LSA Descriptor files can be found in annex F.

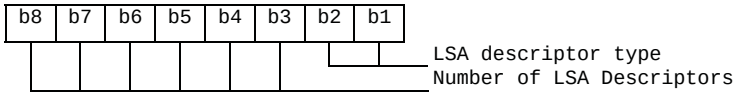
Identifier: '4FXX'	Structure: linear fixed	Optional
Record length: n*X+2 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	LSA descriptor type and number	M	1 byte
2 to X+1	1st LSA Descriptor	M	X bytes
X+2 to 2X+1	2nd LSA Descriptor	M	X bytes
(n-1)*X+2 to n*X+1	nth LSA Descriptor	M	X bytes
n*X+2	Record Identifier	M	1 byte

- LSA descriptor type and number:

  Contents: The LSA descriptor type gives the format of the LSA descriptor and the number of valid LSA Descriptors within the record.

  Coding:



  LSA descriptor type:

  Contents: Gives the format of the LSA Descriptors.

  b2, b1: 00: LSA ID.
  01: LAC + CI
  10: CI
  11: LAC

  Number of LSA Descriptors:

  Contents: Gives the number of valid LSA Descriptors in the record.

  Coding: binary, with b8 as MSB and b3 as LSB leaving room for 64 LSA Descriptors per record.

- LSA Descriptor

  Contents: Dependant of the coding indicated in the LSA descriptor type:

  - in case of LSA ID the field length 'X' is 3 bytes;
  - in case of LAC + CI the field length 'X' is 4 bytes;

- in case of CI the field length 'X' is 2 bytes;
- in case of LAC the field length 'X' is 2 bytes.

Coding: according to TS 24.008 [47].

- Record Identifier:

  Contents: This byte identifies the number of the next record containing the LSA Descriptors forming the LSA.

  Coding: record number of next record. 'FF' identifies the end of the chain.

This file utilises the concept of chaining as for EF_{EXT1}.

The identifier '4FXX' shall be different from one LSA Descriptor file to the other and different from the identifiers of EF_{SAI} and EF_{SLL}. For the range of 'XX', see clause 6.6.

10.4.2 Contents of files at the MExE level

This clause specifies the EFs in the dedicated file DFMExE. It only applies if support of MExE by the SIM is supported (see TS 23.057 [50]).

The EFs in the Dedicated File DFMExE contain execution environment related information.

10.4.2.1 $EF_{MExE-ST}$ (MExE Service table)

This EF indicates which MExE services are allocated, and whether, if allocated, the service is activated. If a service is not allocated or not activated in the SIM, the ME shall not select this service.

Identifier: '4F40'	Structure: transparent	Optional
File size: X bytes, X ≥ 1	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°4	M	1 byte
2	Services n°5 to n°8	O	1 byte
etc.			
X	Services (4X-3) to (4X)	O	1 byte

-Services

Contents:
- Service n°1: Operator root public key
- Service n°2: Administrator root public key
- Service n°3: Third party root public key
- Service n°4: RFU

Coding:

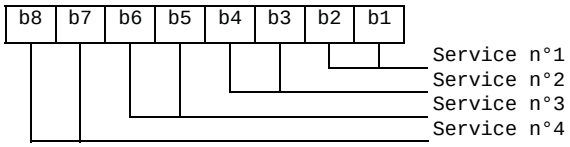
2 bits are used to code each service:
first bit = 1: service allocated
first bit = 0: service not allocated
where the first bit is b1, b3, b5 or b7;
second bit = 1: service activated
second bit = 0: service not activated
where the second bit is b2, b4, b6 or b8.

Service allocated means that the SIM has the capability to support the service. Service activated means that the service is available for the card holder (only valid if the service is allocated).

The following codings are possible:
- first bit = 0: service not allocated, second bit has no meaning;
- first bit = 1 and second bit = 0: service allocated but not activated;
- first bit = 1 and second bit = 1: service allocated and activated.

The bits for services not yet defined shall be set to RFU. For coding of RFU see clause 9.3.

First byte:



etc.

For an example of coding see clause 10.3.7

10.4.2.2 EF_{ORPK} (Operator Root Public Key)

This EF contains the descriptor(s) of certificates containing the Operator Root Public Key. This EF shall only be allocated if the operator wishes to verify applications and certificates in the MExE operator domain using a root public key held on the SIM. Each record of this EF contains one certificate descriptor.

For example, Operator may provide a second key for recover disaster procedure in order to limit OTA data to load.

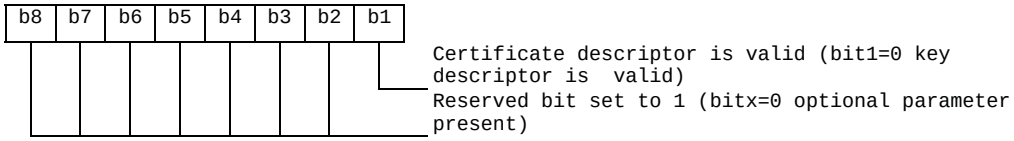
Identifier: '4F41'	Structure: linear fixed	Optional
Record length : X + 10 bytes, X ≥1	Update activity: low	

Access Conditions:

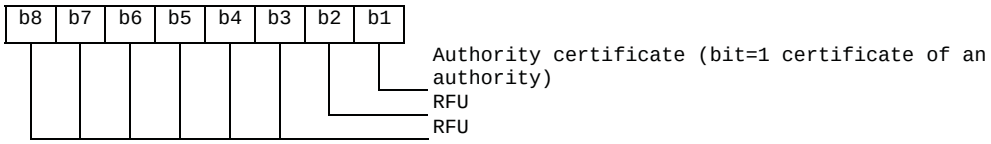
READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (X)	M	1 byte
11 to 10+X	Key identifier	M	X bytes

- Parameter indicator
  Contents:
  The parameter indicator indicates if record is full and which optional parameters are present
  Coding: bit string



- Flags
  Contents:
  The authority flag indicates whether the certificate identify an authority (i.e. CA or AA) or not.
  Coding: bit string



- Type of certificate
  Contents:
  This field indicates the type of certificate containing the key.
  Coding: binary :
  0 : WTLS
  1 : X509
  2 : X9.68
  Other values are reserved for further use

- Key/certificate File Identifier
  Contents:
  these bytes identify an EF which is the key/certificate data file (see clause 10.7.5), holding the actual key/certificate data for this record.
  Coding:
  byte 4: high byte of Key/certificate File Identifier;
  byte 5: low byte of Key/certificate File Identifier.

- Offset into Key/certificate File
  Contents:
  these bytes specify an offset into the transparent key/certificate data File identified in bytes 4 and 5.
  Coding:
  byte 6: high byte of offset into Key/certificate Data File;
  byte 7: low byte of offset into Key/certificate Data File

- Length of Key/certificate Data
  Contents:
  these bytes yield the length of the key/certificate data, starting at the offset identified in "Offset into Key/certificate File" field.
  Coding:
  byte 8: high byte of Key/certificate Data length;
  byte 9: low byte of Key/certificate Data length.

- Key identifier length
  Contents:
  This field gives length of key identifier
  Coding:
  binary

- Key identifier
  Contents:
  This field provides a means of identifying certificates that contain a particular public key (chain building) and linking the public key to its corresponding private key. For more information about value and using see TS 23.057 [50].
  Coding:
  octet string

NOTE: transparent key/certificate data longer than 256 bytes may be read using successive READ BINARY commands.

10.4.2.3 EF_{ARPK} (Administrator Root Public Key)

This EF contains the descriptor(s) of certificates containing the Administrator Root Public Key. This EF shall only be allocated if the SIM issuer wishes to control the Third Party certificates on the terminal using an Administrator Root Public Key held on the SIM. Each record of this EF contains one certificate descriptor.

This file shall contain only one record.

Identifier: '4F42'	Structure: linear fixed	Optional
Record length: X + 10 bytes, X ≥1	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (X)	M	1 byte
11 to 10+X	Key identifier	M	X bytes

For contents and coding of all data items see the respective data items of the EF_{ORPK} (clause 10.4.2.1).

10.4.2.4 EF_{TPRPK} (Third Party Root Public key)

This EF contains descriptor(s) of certificates containing the Third Party Root Public key (s). This EF shall only be allocated if the SIM issuer wishes to verify applications and certificates in the MExE Third Party domain using root public key(s) held on the SIM. This EF can contain one or more root public keys. Each record of this EF contains one certificate descriptor.

For example, an operator may provide several Third Party root public keys.

Identifier: '4F43'	Structure: linear fixed	Optional
Record length : X + Y + 11 bytes; X ≥ 1; Y ≥ 1	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (X)	M	1 byte
11 to 10+X	Key identifier	M	X bytes
11+X	Certificate identifier length (m)	M	1 byte
12+X to 11+X+Y	Certificate identifier	M	Y bytes

- Certificate identifier length
  Contents:
  This field gives length of certificate identifier
  Coding:
  binary

- Certificate identifier
  Contents:
  This field identify the issuer and provide a easy way to find a certificate. For more information about value and usage, see TS 23.057 [50].
  Coding:
  Octet string

For contents and coding of all other data items see the respective data items of the EF_{ORPK} (clause 10.7.1).

10.4.2.5 Trusted Key/Certificates Data Files

Residing under DF_{MExE}, there may be several key/certificates data files. These EFs containing key/certificates data shall have the following attributes:

Identifier: '4FXX'	Structure: transparent	Optional
Record length: Y bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to Y	Key/Certicates Data	M	Y bytes

Contents and coding:

Key/certificate data are accessed using the key/certificates descriptors provided by EF_{TPRPK} (see clause 10.4.2.4).

The identifier '4FXX' shall be different from one key/certificate data file to the other. For the range of 'XX', see clause 6.6. The length Y may be different from one key/certificate data file to the other.

10.5 Contents of files at the telecom level

The EFs in the Dedicated File $DF_{TELECOM}$ contain service related information.

10.5.1 EF_{ADN} (Abbreviated dialling numbers)

This EF contains Abbreviated Dialling Numbers (ADN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F3A'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	CHV2
REHABILITATE	CHV2

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte

- Alpha Identifier

  Contents:

  Alpha-tagging of the associated dialling number.

  Coding:

  this alpha-tagging shall use either

  - the SMS default 7-bit coded alphabet as defined in TS 23.038 [12] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or
  - one of the UCS2 coded options as defined in annex B.

NOTE 1: The value of X may be from zero to 241. Using the command GET RESPONSE the ME can determine the value of X.

- Length of BCD number/SSC contents

  Contents:

  this byte gives the number of bytes of the following two data items containing actual BCD number/SSC information. This means that the maximum value is 11, even when the actual ADN/SSC information length is greater than 11. When an ADN/SSC has extension, it is indicated by the extension1 identifier being unequal to 'FF'. The remainder is stored in the EF_{EXT1} with the remaining length of the additional data being coded in the appropriate additional record itself (see clause 10.5.10).

  Coding:

  according to TS 24.008 [47].

- TON and NPI

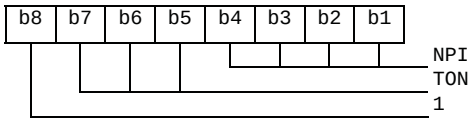
  Contents:

  Type of number (TON) and numbering plan identification (NPI).

  Coding:

  according to TS 24.008 [47]. If the Dialling Number/SSC String does not contain a dialling number, e.g. a control string deactivating a service, the TON/NPI byte shall be set to 'FF' by the ME (see note 2).

NOTE 2: If a dialling number is absent, no TON/NPI byte is transmitted over the radio interface (see TS 24.008 [47]). Accordingly, the ME should not interpret the value 'FF' and not send it over the radio interface.



- Dialling Number/SSC String

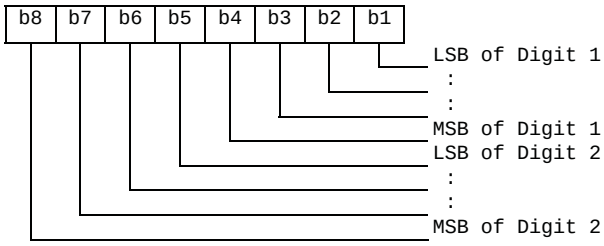
  Contents:

  up to 20 digits of the telephone number and/or SSC information.

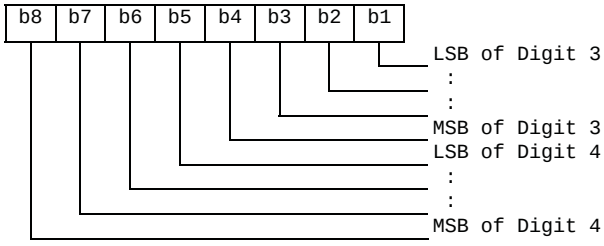
  Coding:

  according to TS 24.008 [47] , TS 22.030 [8] and the extended BCD-coding (see table 12). If the telephone number or SSC is longer than 20 digits, the first 20 digits are stored in this data item and the remainder is stored in an associated record in the EF_{EXT1}. The record is identified by the Extension1 Record Identifier. If ADN/SSC require less than 20 digits, excess nibbles at the end of the data item shall be set to 'F'. Where individual dialled numbers, in one or more records, of less than 20 digits share a common appended digit string the first digits are stored in this data item and the common digits stored in an associated record in the EF_{EXT1}. The record is identified by the Extension 1 Record Identifier. Excess nibbles at the end of the data item shall be set to 'F'.

  Byte X+3



  Byte X+4:



etc.

- Capability/Configuration Identifier

  Contents:

  capability/configuration identification byte. This byte identifies the number of a record in the EF_{CCP} containing associated capability/configuration parameters required for the call. The use of this byte is optional. If it is not used it shall be set to 'FF'.

  Coding:

  binary.

- Extension1 Record Identifier

  Contents:

  extension1 record identification byte. This byte identifies the number of a record in the EF_{EXT1} containing an associated called party subaddress or additional data. The use of this byte is optional. If it is not used it shall be set to 'FF'.

If the ADN/SSC requires both additional data and called party subaddress, this byte identifies the additional record. A chaining mechanism inside EF_{EXT1} identifies the record of the appropriate called party subaddress (see clause 10.5.10).

Coding:

binary.

NOTE 3: As EF_{ADN} is part of the $DF_{TELECOM}$ it may be used by GSM and also other applications in a multi-application card. If the non-GSM application does not recognize the use of Type of Number (TON) and Number Plan Identification (NPI), then the information relating to the national dialling plan must be held within the data item dialling number/SSC and the TON and NPI fields set to UNKNOWN. This format would be acceptable for GSM operation and also for the non-GSM application where the TON and NPI fields shall be ignored.

EXAMPLE: SIM storage of an International Number using E.164 [19] numbering plan.

	TON	NPI	Digit field
GSM application	001	0001	abc...
Other application compatible with GSM	000	0000	xxx...abc...

where "abc..." denotes the subscriber number digits (including its country code), and "xxx..." denotes escape digits or a national prefix replacing TON and NPI.

NOTE 4: When the ME acts upon the EF_{ADN} with a SEEK command in order to identify a character string in the alpha-identifier, it is the responsibility of the ME to ensure that the number of characters used as SEEK parameters are less than or equal to the value of X if the MMI allows the user to offer a greater number.

Table 12: Extended BCD coding

BCD Value	Character/Meaning
'0'	"0"
...	...
'9'	"9"
'A'	"*"
'B'	"#"
'C'	DTMF Control digit separator (TS 22.101 [53])
'D'	"Wild" value This will cause the MMI to prompt the user for a single digit (see TS 22.101 [53]).
'E'	Expansion digit ("Shift Key"). It has the effect of adding '10' to the following digit. The following BCD digit will hence be interpreted in the range of '10'-'1E'. The purpose of digits in this range is for further study.
'F'	Endmark e.g. in case of an odd number of digits

BCD values 'C', 'D' and 'E' are never sent across the radio interface.

NOTE 5: The interpretation of values 'D', 'E' and 'F' as DTMF digits is for further study.

NOTE 6: A second or subsequent 'C' BCD value will be interpreted as a 3 second PAUSE (see TS 22.101 [53]).

10.5.2 EF_{FDN} (Fixed dialling numbers)

This EF contains Fixed Dialling Numbers (FDN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F3B'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV2
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension2 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (clause 10.5.1), with the exception that extension records are stored in the EF_{EXT2}.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

10.5.3 EF_{SMS} (Short messages)

This EF contains information in accordance with TS 23.040 [13] comprising short messages (and associated parameters) which have either been received by the MS from the network, or are to be used as an MS originated message.

Identifier: '6F3C'	Structure: linear fixed	Optional
Record length: 176 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

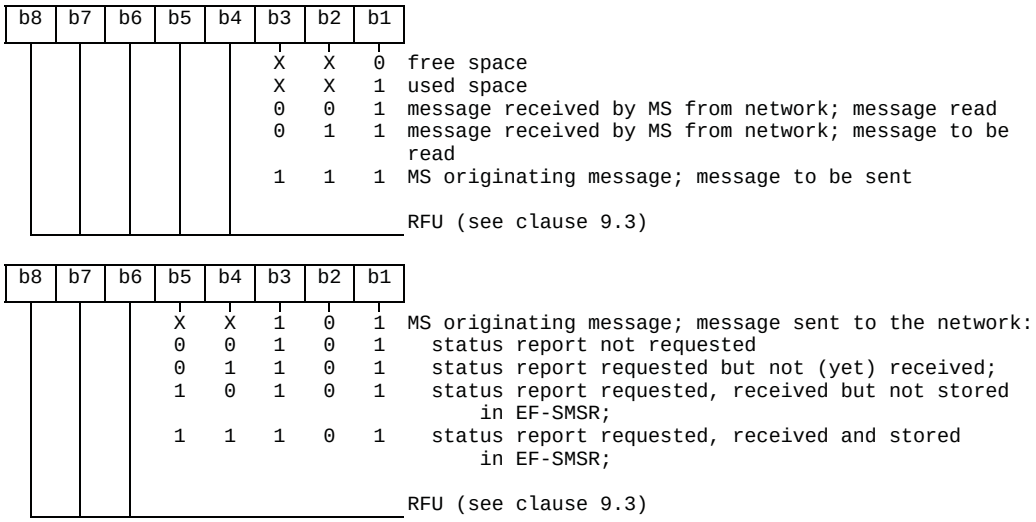
Bytes	Description	M/O	Length
1	Status	M	1 byte
2 to 176	Remainder	M	175 bytes

- Status

  Contents:

  Status byte of the record which can be used as a pattern in the SEEK command. For MS originating messages sent to the network, the status shall be updated when the MS receives a status report, or sends a successful SMS Command relating to the status report.

  Coding:



- Remainder

  Contents:

  This data item commences with the TS-Service-Centre-Address as specified in TS 24.011 [16]. The bytes immediately following the TS-Service-Centre-Address contain an appropriate short message TPDU as specified in TS 23.040 [13], with identical coding and ordering of parameters.

  Coding:

  according to TS 23.040 [13] and TS 24.011 [16]. Any TP-message reference contained in an MS originated message stored in the SIM, shall have a value as follows:

	Value of the TP-message-reference:
message to be sent:	'FF'
message sent to the network:	the value of TP-Message-Reference used in the message sent to the network.

  Any bytes in the record following the TPDU shall be filled with 'FF'.

  It is possible for a TS-Service-Centre-Address of maximum permitted length, e.g. containing more than 18 address digits, to be associated with a maximum length TPDU such that their combined length is 176 bytes. In this case the ME shall store in the SIM the TS-Service-Centre-Address and the TPDU in bytes 2-176 without modification, except for the last byte of the TPDU, which shall not be stored.

10.5.4 Capability configuration parameters

10.5.4.1 EF_{CCP} (Capability configuration parameters)

This EF contains parameters of required network and bearer capabilities and ME configurations associated with a call established using an abbreviated dialling number, a fixed dialling number, an MSISDN, a last number dialled, a service dialling number or a barred dialling number.

For compatibility reasons, this file may be present for release 98 or earlier MEs in order to support Capability Configuration Parameters service.

Identifier: '6F3D'	Structure: linear fixed	Optional
Record length: 14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 10	Bearer capability information element	M	10 bytes
11 to 14	Bytes reserved - see below	M	4 bytes

- Bearer capability information element

  Contents and Coding:

  - see TS 24.008 [47]. The Information Element Identity (IEI) shall be excluded. i.e. the first byte of the EF_{CCP} record shall be Length of the bearer capability contents.

  - Bytes 11-14 shall be set to 'FF' and shall not be interpreted by the ME.

10.5.4.2 EF_{ECCP} (Extended Capability Configuration Parameters)

This EF contains parameters of required network and bearer capabilities and ME configurations associated with a call established using an abbreviated dialling number, a fixed dialling number, an MSISDN, a last number dialled, a service dialling number, a barred dialling number, a mailbox dialling number or a call forwarding indication status number.

The number of records of the EF_{ECCP} shall be equal to the number of records of the EF_{CCP}. Each record of the EF_{CCP} shall have a corresponding record in the EF_{ECCP} with the same record number.

If an ME has to update a record, then the ME shall update each record of both files, EF_{CCP} with 10 bytes and EF_{ECCP} with X bytes (X≥15).

If an ME has to read a record, then the ME shall check the consistency between the record of the EF_{ECCP} and the corresponding record of the EF_{CCP} and update the record of the EF_{ECCP} with the value of the corresponding record of the EF_{CPP}.

Identifier: '6F4F'	Structure: linear fixed	Optional
Record length: X (X≥15)	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Bearer capability information element	M	X bytes

- Bearer capability information element

  Contents and Coding:

  see TS 24.008 [47]. The Information Element Identity (IEI) shall be excluded, i.e. the first byte of the EF_{ECCP} record shall be Length of the bearer capability contents.

  Unused bytes are filled with 'FF'.

10.5.5 EF_{MSISDN} (MSISDN)

This EF contains MSISDN(s) related to the subscriber. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F40'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of EF_{ADN}.

NOTE 1: If the SIM stores more than one MSISDN number and the ME displays the MSISDN number(s) within the initialization procedure then the one stored in the first record shall be displayed with priority.

NOTE 2: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

10.5.6 EF_{SMSP} (Short message service parameters)

This EF contains values for Short Message Service header Parameters (SMSP), which can be used by the ME for user assistance in preparation of mobile originated short messages. For example, a service centre address will often be common to many short messages sent by the subscriber.

The EF consists of one or more records, with each record able to hold a set of SMS parameters. The first (or only) record in the EF shall be used as a default set of parameters, if no other record is selected.

To distinguish between records, an alpha-identifier may be included within each record, coded on Y bytes.

The SMS parameters stored within a record may be present or absent independently. When a short message is to be sent from the MS, the parameter in the SIM record, if present, shall be used when a value is not supplied by the user.

Identifier: '6F42'	Structure: linear fixed	Optional
Record length: 28+Y bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to Y	Alpha-Identifier	O	Y bytes
Y+1	Parameter Indicators	M	1 byte
Y+2 to Y+13	TP-Destination Address	M	12 bytes
Y+14 to Y+25	TS-Service Centre Address	M	12 bytes
Y+26	TP-Protocol Identifier	M	1 byte
Y+27	TP-Data Coding Scheme	M	1 byte
Y+28	TP-Validity Period	M	1 byte

Storage is allocated for all of the possible SMS parameters, regardless of whether they are present or absent. Any bytes unused, due to parameters not requiring all of the bytes, or due to absent parameters, shall be set to 'FF'.

- Alpha-Identifier

  Contents:

Alpha Tag of the associated SMS-parameter.

Coding:

see clause 10.5.1 (EF_{ADN}).

NOTE: The value of Y may be zero, i.e. the alpha-identifier facility is not used. By using the command GET RESPONSE the ME can determine the value of Y.

- Parameter Indicators

Contents:

Each of the default SMS parameters which can be stored in the remainder of the record are marked absent or present by individual bits within this byte.

Coding:

Allocation of bits:

Bit number	Parameter indicated
1	TP-Destination Address
2	TS-Service Centre Address
3	TP-Protocol Identifier
4	TP-Data Coding Scheme
5	TP-Validity Period
6	reserved, set to 1
7	reserved, set to 1
8	reserved, set to 1

Bit value	Meaning
0	Parameter present
1	Parameter absent

- TP-Destination Address

Contents and Coding: As defined for SM-TL address fields in TS 23.040 [13].

- TP-Service Centre Address

Contents and Coding: As defined for RP-Destination address Centre Address in TS 24.011 [16].

- TP-Protocol Identifier

Contents and Coding: As defined in TS 23.040 [13].

- TP-Data Coding Scheme

Contents and Coding: As defined in TS 23.038 [12].

- TP-Validity Period

Contents and Coding: As defined in TS 23.040 [13] for the relative time format.

10.5.7 EF_{SMSS} (SMS status)

This EF contains status information relating to the short message service.

The provision of this EF is associated with EF_{SMS}. Both files shall be present together, or both absent from the SIM.

Identifier: '6F43'	Structure: transparent	Optional
File size: 2+X bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Last Used TP-MR	M	1 byte
2	SMS "Memory Cap. Exceeded" Not. Flag	M	1 byte
3 to 2+X	RFU	O	X bytes

- Last Used TP-MR.

  Contents:

  the value of the TP-Message-Reference parameter in the last mobile originated short message, as defined in TS 23.040 [13].

  Coding:

  as defined in TS 23.040 [13].

- SMS "Memory Capacity Exceeded" Notification Flag.

  Contents:

  This flag is required to allow a process of flow control, so that as memory capacity in the MS becomes available, the Network can be informed. The process for this is described in TS 23.040 [13].

  Coding:

  b1=1 means flag unset; memory capacity available

  b1=0 means flag set

  b2 to b8 are reserved and set to 1.

10.5.8 EF_{LND} (Last number dialled)

This EF contains the last numbers dialled (LND) and/or the respective supplementary service control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain associated alpha-tagging.

Identifier: '6F44'	Structure: cyclic	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INCREASE	NEVER
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte

For contents and coding, see clause 10.5.1 EF_{ADN}.

The value of X in EF_{LND} may be different to both the value of X in EF_{ADN} and of X in EF_{FDN}.

If the value of X in EF_{LND} is longer than the length of the α-tag of the number to be stored, then the ME shall pad the α-tag with 'FF'. If the value of X in EF_{LND} is shorter than the length of the α-tag of the number to be stored, then the ME shall cut off excessive bytes.

10.5.9 EF_{SDN} (Service Dialling Numbers)

This EF contains special service numbers (SDN) and/or the respective supplementary service control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain associated alpha-tagging.

Identifier: '6F49'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 bytes
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension3 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (clause 10.5.1), with the exception that extension records are stored in the EF_{EXT3}.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

10.5.10 EF_{EXT1} (Extension1)

This EF contains extension data of an ADN/SSC, an MSISDN, or an LND. Extension data is caused by:

- an ADN/SSC (MSISDN, LND) which is greater than the 20 digit capacity of the ADN/SSC (MSISDN, LND) Elementary File or where common digits are required to follow an ADN/SSC string of less than 20 digits. The remainder is stored in this EF as a record, which is identified by a specified identification byte inside the ADN/SSC (MSISDN, LND) Elementary File. The EXT1 record in this case is specified as additional data;
- an associated called party subaddress. The EXT1 record in this case is specified as subaddress data.

Identifier: '6F4A'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

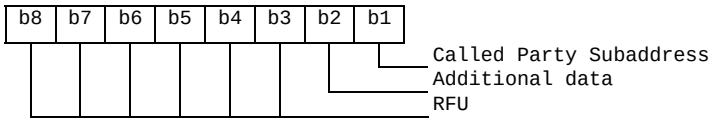
READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

- Record type

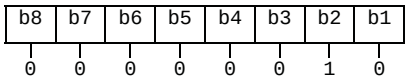
Contents: type of the record

Coding:



b3-b8 are reserved and set to 0;
a bit set to 1 identifies the type of record;
only one type can be set;
'00' indicates the type "unknown".

The following example of coding means that the type of extension data is "additional data":



- Extension data

Contents: Additional data or Called Party Subaddress depending on record type.

Coding:

Case 1, Extension1 record is additional data:

The first byte of the extension data gives the number of bytes of the remainder of ADN/SSC (respectively MSISDN, LND). The coding of remaining bytes is BCD, according to the coding of ADN/SSC (MSISDN, LND). Unused nibbles at the end have to be set to 'F'. It is possible if the number of additional digits exceeds the capacity of the additional record to chain another record inside the EXT1 Elementary File by the identifier in byte 13. In this case byte 2 (first byte of the extension data) of all records for additional data within the same chain indicates the number of bytes ('01' to '0A') for ADN/SSC (respectively MSISDN, LND) within the same record unequal to 'FF'.

Case 2, Extension1 record is Called Party Subaddress:

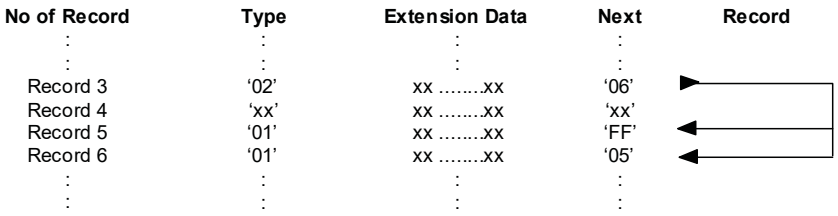
The subaddress data contains information as defined for this purpose in TS 24.008 [47]. All information defined in TS 24.008 [47], except the information element identifier, shall be stored in the SIM. The length of this subaddress data can be up to 22 bytes. In those cases where two extension records are needed, these records are chained by the identifier field. The extension record containing the first part of the called party subaddress points to the record which contains the second part of the subaddress.

- Identifier

Contents: identifier of the next extension record to enable storage of information longer than 11 bytes.

Coding: record number of next record. 'FF' identifies the end of the chain.

EXAMPLE: Of a chain of extension records being associated to an ADN/SSC. The extension1 record identifier (Byte 14+X) of EF_{ADN} is set to 3.



In this example ADN/SSC is associated to additional data (records 3 and 4) which represent the last 27 or 28 digits of the whole ADN/SSC (the first 20 digits are stored in EF_{ADN}) and a called party subaddress whose length is more than 11 bytes (records 6 and 1).

10.5.11 EF_{EXT2} (Extension2)

This EF contains extension data of an FDN/SSC (see EXT2 in clause 10.5.2).

Identifier: '6F4B'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV2
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see clause 10.5.10 EF_{EXT1}.

10.5.12 EF_{EXT3} (Extension3)

This EF contains extension data of an SDN (see EXT3 in clause 10.5.9).

Identifier: '6F4C'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see clause 10.5.10 EF_{EXT1}.

10.5.13 EF_{BDN} (Barred Dialling Numbers)

This EF contains Barred Dialling Numbers (BDN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F4D'	Structure: linear fixed	Optional
Record length: X+15 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV2
INVALIDATE	CHV2 / ADM (set at personalisation)
REHABILITATE	CHV2 / ADM (set at personalisation)

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension4 Record Identifier	M	1 byte
X+15	Comparison Method Pointer	M	1 byte

For contents and coding of all data items, except for the Comparison Method Pointer, see the respective data items of the EF_{ADN} (clause 10.5.1), with the exception that extension records are stored in the EF_{EXT4}. The Comparison Method Pointer refers to a record number in EF_{CMI}.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

10.5.14 EF_{EXT4} (Extension4)

This EF contains extension data of an BDN/SSC (see EXT4 in clause 10.5.13).

Identifier: '6F4E'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV2
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see clause 10.5.10 EF_{EXT1}.

10.5.15 EF_{SMSR} (Short message status reports)

This EF contains information in accordance with TS 23.040 [13] comprising short message status reports which have been received by the MS from the network.

Each record is used to store the status report of a short message in a record of EF_{SMS}. The first byte of each record is the link between the status report and the corresponding short message in EF_{SMS}.

Identifier: '6F47'	Structure: linear fixed	Optional
Record length: 30 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	SMS record identifier	M	1
2 to 30	SMS status report	M	29 bytes

- SMS record identifier

  Contents:

  This data item identifies the corresponding SMS record in EF_{SMS}, e.g. if this byte is coded '05' then this status report corresponds to the short message in record #5 of EF_{SMS}.

  Coding:

  '00' - empty record

  '01' - 'FF' - record number of the corresponding SMS in EF_{SMS}.

- SMS status report

  Contents:

  This data item contains the SMS-STATUS-REPORT TPDU as specified in TS 23.040 [13], with identical coding and ordering of parameters.

  Coding:

  according to TS 23.040 [13]. Any bytes in the record following the TPDU shall be filled with 'FF'.

10.5.16 EF_{CMI} (Comparison Method Information)

This EF contains a list of Comparison Method Identifiers and alpha-tagging associated with BDN entries (see EF_{BDN}). This EF shall always be present if EF_{BDN} is present.

Identifier: '6F58'	Structure: linear fixed	Optional
Record length: X+1 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	M	X bytes
X+1	Comparison Method Identifier	M	1 byte

- Alpha Identifier

  Contents:

  Alpha-tagging of the associated Comparison Method Identifier

  Coding:

  Same as the alpha identifier in EF_{ADN}.

- Comparison Method Identifier

  Contents:

  this byte describes the comparison method which is associated with a BDN record. Its interpretation is not specified but it shall be defined by the operators implementing the BDN feature.

  Coding:

  '00' - 'FE' = Comparison Method Identifier.

  'FF' = Default method.

10.6 DFs at the telecom level

DFs may be present as child directories of $DF_{TELECOM}$. The following has been defined.

$DF_{GRAPHICS}$ '5F50'

10.6.1 Contents of files at the telecom graphics level

The EFs in the Dedicated File $DF_{GRAPHICS}$ contain graphical information.

10.6.1.1 EF_{IMG} (Image)

Each record of this EF identifies instances of one particular graphical image, which graphical image is identified by this EF's record number.

Image instances may differ as to their size, having different resolutions, and the way they are coded, using one of several image coding schemes.

As an example, image k may represent a company logo, of which there are i instances on SIM, of various resolutions and perhaps encoded in several image coding schemes. Then, the i instances of the company's logo are described in record k of this EF.

Identifier: '4F20'	Structure: linear fixed	Optional
Record length: 9n+1 or 9n+2 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Number of Actual Image Instances	M	1 byte
2 to 10	Descriptor of Image Instance 1	M	9 bytes
11 to 19	Descriptor of Image Instance 2	O	9 bytes
:			
9 (n-1) + 2 to 9n + 1	Descriptor of Image Instance n	O	9 bytes
9n + 2	RFU	O	1 byte

- Number of Actual Image Instances

  Contents: this byte gives the number of actual image instances described in the following data items (i.e. unused descriptors are not counted).

  Coding: binary

- Image Instance Descriptor

Contents: a description of an image instance

Coding: see below

Byte 1: Image Instance Width

Contents:

this byte specifies the image instance width, expressed in raster image points.

Coding:

binary.

Byte 2: Image Instance Height

Contents:

this byte specifies the image instance height, expressed in raster image points.

Coding:

binary.

Byte 3: Image Coding Scheme

Contents:

this byte identifies the image coding scheme that has been used in encoding the image instance.

Coding:

'11' - basic image coding scheme as defined in annex G;

'21' - colour image coding scheme as defined in annex G;

other values are reserved for future use.

Bytes 4 and 5: Image Instance File Identifier

Contents:

these bytes identify an EF which is the image instance data file (see clause 10.6.1.2), holding the actual image data for this particular instance.

Coding:

byte 4: high byte of Image Instance File Identifier;

byte 5: low byte of Image Instance File Identifier.

Bytes 6 and 7: Offset into Image Instance File

Contents:

these bytes specify an offset into the transparent Image Instance File identified in bytes 4 and 5.

Coding:

byte 6: high byte of offset into Image Instance File;

byte 7: low byte of offset into Image Instance File

Bytes 8 and 9: Length of Image Instance Data

Contents:

these bytes yield the length of the image instance data, starting at the offset identified in bytes 6 and 7.

Coding:

byte 8: high byte of Image Instance Data length;

byte 9: low byte of Image Instance Data length.

NOTE: Transparent image instance data longer than 256 bytes may be read using successive READ BINARY commands.

10.6.1.2 Image Instance Data Files

Residing under $DF_{GRAPHICS}$, there may be several image instance data files. These EFs containing image instance data shall have the following attributes.

Identifier: '4FXX'	Structure: transparent	Optional
Record length: Y bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to Y	Image Instance Data	M	Y bytes

Contents and coding:

Image instance data are accessed using the image instance descriptors provided by EF_{IMG} (see clause 10.6.1.1).

The identifier '4FXX' shall be different from one image instance data file to the other. For the range of 'XX', see clause 6.6. The length Y may be different from one image instance data file to the other.

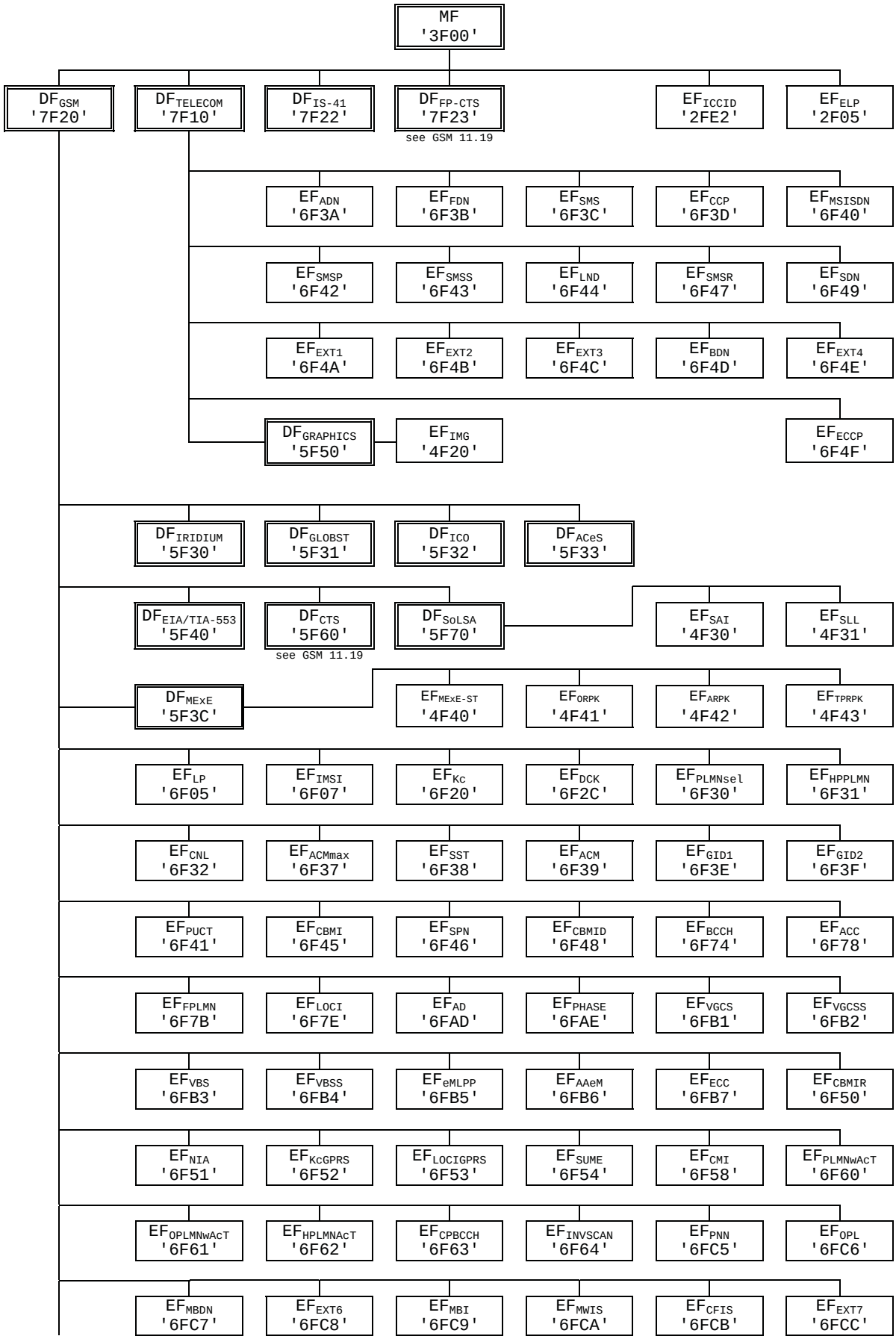
10.7 Files of GSM

This clause contains a figure depicting the file structure of the SIM. DF_{GSM} shall be selected using the identifier '7F20'. If selection by this means fails, then DCS 1800 MEs shall, and optionally GSM MEs may then select DF_{GSM} with '7F21'.

NOTE 1: The selection of the GSM application using the identifier '7F21', if selection by means of the identifier '7F20' fails, is to ensure backwards compatibility with those Phase 1 SIMs which only support the DCS 1800 application using the Phase 1 directory $DF_{DCS1800}$ coded '7F21'.

NOTE 2: To ensure backwards compatibility with those Phase 1 DCS 1800 MEs which have no means to select DF_{GSM} two options have been specified. These options are given in GSM 09.91 [17].

NOTE 3: The value '6F65' under DF_{GSM} was used in earlier versions of this specification, and should not be re-assigned in future versions.


MF '3F00'
DF GSM '7F20'
DF TELECOM '7F10'
DF IS-41 '7F22'
DF FP-CTS '7F23'
see GSM 11.19
EF ICCID '2FE2'
EF ELP '2F05'
EF ADN '6F3A'
EF FDN '6F3B'
EF SMS '6F3C'
EF CCP '6F3D'
EF MSISDN '6F40'
EF SMSP '6F42'
EF SMSS '6F43'
EF LND '6F44'
EF SMSR '6F47'
EF SDN '6F49'
EF EXT1 '6F4A'
EF EXT2 '6F4B'
EF EXT3 '6F4C'
EF BDN '6F4D'
EF EXT4 '6F4E'
DF GRAPHICS '5F50'
EF IMG '4F20'
EF ECCP '6F4F'
DF IRIDIUM '5F30'
DF GLOBST '5F31'
DF ICO '5F32'
DF ACeS '5F33'
DF EIA/TIA-553 '5F40'
DF CTS '5F60'
see GSM 11.19
DF SoLSA '5F70'
EF SAI '4F30'
EF SLL '4F31'
DF MExE '5F3C'
EF MExE-ST '4F40'
EF ORPK '4F41'
EF ARPK '4F42'
EF TPRPK '4F43'
EF LP '6F05'
EF IMSI '6F07'
EF Kc '6F20'
EF DCK '6F2C'
EF PLMNsel '6F30'
EF HPPLMN '6F31'
EF CNL '6F32'
EF ACMmax '6F37'
EF SST '6F38'
EF ACM '6F39'
EF GID1 '6F3E'
EF GID2 '6F3F'
EF PUCT '6F41'
EF CBMI '6F45'
EF SPN '6F46'
EF CBMID '6F48'
EF BCCH '6F74'
EF ACC '6F78'
EF FPLMN '6F7B'
EF LOCI '6F7E'
EF AD '6FAD'
EF PHASE '6FAE'
EF VGCS '6FB1'
EF VGCSS '6FB2'
EF VBS '6FB3'
EF VBSS '6FB4'
EF eMLPP '6FB5'
EF AAeM '6FB6'
EF ECC '6FB7'
EF CBMIR '6F50'
EF NIA '6F51'
EF KcGPRS '6F52'
EF LOCIGPRS '6F53'
EF SUME '6F54'
EF CMI '6F58'
EF PLMNwAcT '6F60'
EF OPLMNwAcT '6F61'
EF HPLMNAcT '6F62'
EF CPBCCH '6F63'
EF INVSCAN '6F64'
EF PNN '6FC5'
EF OPL '6FC6'
EF MBDN '6FC7'
EF EXT6 '6FC8'
EF MBI '6FC9'
EF MWIS '6FCA'
EF CFIS '6FCB'
EF EXT7 '6FCC'

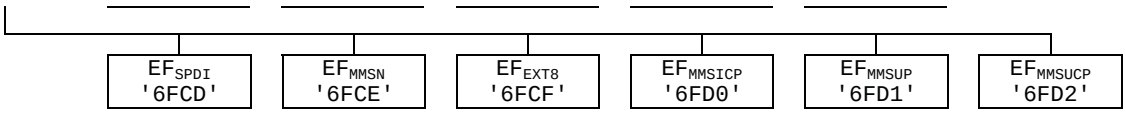


Figure 8: File identifiers and directory structures of GSM

11 Application protocol

When involved in GSM administrative management operations, the SIM interfaces with appropriate terminal equipment. These operations are outside the scope of the present document.

When involved in GSM network operations the SIM interfaces with an ME with which messages are exchanged. A message can be a command or a response.

- A GSM command/response pair is a sequence consisting of a command and the associated response.
- A GSM procedure consists of one or more GSM command/response pairs which are used to perform all or part of an application-oriented task. A procedure shall be considered as a whole, that is to say that the corresponding task is achieved if and only if the procedure is completed. The ME shall ensure that, when operated according to the manufacturer's manual, any unspecified interruption of the sequence of command/response pairs which realize the procedure, leads to the abortion of the procedure itself.
- A GSM session of the SIM in the GSM application is the interval of time starting at the completion of the SIM initialization procedure and ending either with the start of the GSM session termination procedure, or at the first instant the link between the SIM and the ME is interrupted.

During the GSM network operation phase, the ME plays the role of the master and the SIM plays the role of the slave.

The SIM shall execute all GSM and SIM Application Toolkit commands or procedures in such a way as not to jeopardise, or cause suspension, of service provisioning to the user. This could occur if, for example, execution of the RUN GSM ALGORITHM is delayed in such a way which would result in the network denying or suspending service to the user.

Some procedures at the SIM/ME interface require MMI interactions. The descriptions hereafter do not intend to infer any specific implementation of the corresponding MMI. When MMI interaction is required, it is marked "MMI" in the list given below.

Some procedures are not clearly user dependent. They are directly caused by the interaction of the MS and the network. Such procedures are marked "NET" in the list given below.

Some procedures are automatically initiated by the ME. They are marked "ME" in the list given below.

The list of procedures at the SIM/ME interface in GSM network operation is as follows:

General Procedures:

- Reading an EF ME
- Updating an EF ME
- Increasing an EF ME

SIM management procedures:

- SIM initialization ME
- GSM session termination ME
- Emergency call codes request ME
- Extended language preference request ME
- Language preference request ME

- Administrative information request ME
- SIM service table request ME
- SIM phase request ME

CHV related procedures:

- CHV verification MMI
- CHV value substitution MMI
- CHV disabling MMI
- CHV enabling MMI
- CHV unblocking MMI

GSM security related procedures:

- GSM algorithms computation NET
- IMSI request NET
- Access control information request NET
- Higher Priority PLMN search period request NET
- Location Information NET
- GPRS Location Information NET
- Cipher key NET
- GPRS Cipher key NET
- BCCH information NET
- Forbidden PLMN information NET
- LSA information NET

Subscription related procedures:

- Dialling Numbers (ADN, FDN, MSISDN, LND, SDN, BDN) MMI/ME
- Short messages (SMS) MMI
- Advice of Charge (AoC) MMI
- Capability Configuration Parameters (CCP) MMI
- PLMN Selector MMI
- HPLMN Selector with Access Technology MMI
- User controlled PLMN Selector with Access Technology MMI
- Operator controlled PLMN Selector with Access Technology MMI
- Investigation Scan request NET
- CPBCCH information NET
- Cell Broadcast Message Identifier (CBMI) MMI
- Group Identifier Level 1 (GID1) MMI/ME
- Group Identifier Level 2 (GID2) MMI/ME

- Service Provider Name (SPN) ME
- Voice Group Call Service (VGCS) MMI/ME
- Voice Broadcast Service (VBS) MMI/ME
- Enhanced Multi Level Pre-emption and Priority (eMLPP) MMI/ME
- Depersonalisation Control Keys ME
- Short message status reports (SMSR) MMI
- Network's indication of alerting ME

SIM Application Toolkit related procedures:

- Data Download via SMS-CB (CBMID) NET
- Data Download via SMS-PP NET
- Menu selection MMI
- Call Control MMI/ME/NET
- Proactive SIM MMI/ME/NET
- Mobile Originated Short Message control by SIM MMI/ME/NET
- Image Request MMI/ME

MExE related procedures:

- Reading of MExE_ST ME
- Reading of root public keys on the SIM (ORPK, ARPK,TPRPK) ME/NET

The procedures listed in clause 11.2 are basically required for execution of the procedures in clauses 11.3, 11.4 and 11.5. The procedures listed in clauses 11.3 and 11.4 are mandatory (see TS 02.17 [6]). The procedures listed in clause 11.5 are only executable if the associated services, which are optional, are provided in the SIM. However, if the procedures are implemented, it shall be in accordance with clause 11.5.

If a procedure is related to a specific service indicated in the SIM Service Table, it shall only be executed if the corresponding bits denote this service as "allocated and activated" (see clause 10.3.7). In all other cases this procedure shall not start.

11.1 General procedures

Procedures on different types of files shall be in accordance with TS 31.101 [55] with the limitation that the use of short file IDs is not supported by the SIM.

11.2 SIM management procedures

Phase 2 MEs shall support all SIMs which comply with the mandatory requirements of Phase 1, even if these SIMs do not comply with all the mandatory requirements of Phase 2. Furthermore, Phase 2 MEs shall take care of potential incompatibilities with Phase 1 SIMs which could arise through use of inappropriate commands or misinterpretation of response data. Particular note should be taken of making a false interpretation of RFU bytes in a Phase 1 SIM having contradictory meaning in Phase 2; e.g. indication of EF invalidation state.

11.2.1 SIM initialization

After SIM activation (see clause 4.3.2), the ME selects the Dedicated File DF_{GSM} and optionally attempts to select EF_{ECC} If EF_{ECC} is available, the ME requests the emergency call codes.

The ME requests the Extended Language Preference. The ME only requests the Language Preference (EF_{LP}) if at least one of the following conditions holds:

- EF_{PL} is not available;
- EF_{PL} does not contain an entry corresponding to a language specified in ISO 639[30];
- the ME does not support any of the languages in EF_{PL}.

If both EFs are not available or none of the languages in the EFs is supported then the ME selects a default language. It then runs the CHV1 verification procedure.

If the CHV1 verification procedure is performed successfully, the ME then runs the SIM Phase request procedure.

For a SIM requiring PROFILE DOWNLOAD, then the ME shall perform the PROFILE DOWNLOAD procedure in accordance with TS 51.014 [27]. When BDN is enabled on a SIM, the PROFILE DOWNLOAD procedure is used to indicate to the SIM whether the ME supports the "Call Control by SIM" facility. If so, then the SIM is able to allow the REHABILITATE command to rehabilitate EF_{IMSI} and EF_{LOCI}.

If the ME detects a SIM of Phase 1, it shall omit the following procedures relating to FDN and continue with the Administrative Information request. The ME may omit procedures not defined in Phase 1 such as Higher Priority PLMN Search Period request.

For a SIM of Phase 2 or greater, GSM operation shall only start if one of the two following conditions is fulfilled:

- if EF_{IMSI} and EF_{LOCI} are not invalidated, the GSM operation shall start immediately;
- if EF_{IMSI} and EF_{LOCI} are invalidated, the ME rehabilitates these two EFs.

  MEs without FDN capability but with Call control by SIM facility shall not rehabilitate EF_{IMSI} and/or EF_{LOCI} if FDN is enabled in the SIM and therefore have no access to these EFs. GSM operation will therefore be prohibited;

  MEs without FDN capability and without Call control by SIM facility shall not rehabilitate EF_{IMSI} and/or EF_{LOCI} and therefore have no access to these EFs. GSM operation will therefore be prohibited.

  It is these mechanisms which are used for control of services n°3 and n°31 by the use of SIMs for these services which always invalidate these two EFs at least before the next command following selection of either EF.

NOTE: When FDN and BDN are both enabled, and if the ME supports FDN but does not support the Call control by SIM facility, the rehabilitation of EF_{IMSI} and EF_{LOCI} will not be successful because of a restriction mechanism of the REHABILITATE command linked to the BDN feature.

When EF_{IMSI} and EF_{LOCI} are successfully rehabilitated, if the FDN capability procedure indicates that:

i) FDN is allocated and activated in the SIM; and FDN is set "enabled", i.e. ADN "invalidated" or not activated; and the ME supports FDN; or

ii) FDN is allocated and activated in the SIM; and FDN is set "disabled", i.e. ADN "not invalidated"; or

iii) FDN is not allocated or not activated;

then GSM operation shall start.

In all other cases GSM operation shall not start.

Afterwards, the ME runs the following procedures, subject to the service being supported both by the ME and the SIM:

- Administrative Information request;
- SIM Service Table request;
- IMSI request;
- Access Control request;
- Higher Priority PLMN Search Period request;

- Investigation scan request;
- PLMN selector request;
- HPLMN Selector with Access Technology request;
- User controlled PLMN Selector with Access Technology request;
- Operator controlled PLMN Selector with Access Technology request;
- Location Information request;
- GPRS Location Information request;
- Cipher Key request;
- GPRS Cipher Key request;
- BCCH information request;
- CPBCCH information request;
- Forbidden PLMN request;
- LSA information request;
- CBMID request;
- Depersonalisation Control Keys request;
- Network's indication of alerting request.

If the SIM service table indicates that the proactive SIM service is active, then from this point onwards, the ME, if it supports the proactive SIM service, shall send STATUS commands at least every 30s during idle mode as well as during calls, in order to enable the proactive SIM to respond with a command. The SIM may send proactive commands (see TS 51.014 [27]), including a command to change the interval between STATUS commands from the ME, when in idle mode. In-call requirements for STATUS for SIM Presence Detection are unchanged by this command.

After the SIM initialization has been completed successfully, the MS is ready for a GSM session.

11.2.2 GSM session termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in clause 4.3.2.

The GSM session is terminated by the ME as follows.

The ME runs all the procedures which are necessary to transfer the following subscriber related information to the SIM, subject to the service being supported both by the ME and the SIM:

- Location Information update;
- GPRS Location Information update;
- Cipher Key update;
- GPRS Cipher Key update;
- BCCH information update;
- CPBCCH information update;
- Advice of Charge increase;
- Forbidden PLMN update.

As soon as the SIM indicates that these procedures are completed, the ME/SIM link may be deactivated.

Finally, the ME deletes all these subscriber related information elements from its memory.

NOTE 2: If the ME has already updated any of the subscriber related information during the GSM Session, and the value has not changed until GSM session termination, the ME may omit the respective update procedure.

11.2.3 Emergency Call Codes

Request: The ME performs the reading procedure with EF_{ECC}.

Update: The ME performs the updating procedure with EF_{ECC}.

NOTE: The update procedure is only applicable when access conditions of ADM for update is set to ALW, CHV1 or CHV2.

11.2.4 Language preference

Request: The ME performs the reading procedure with EF_{LP}.

Update: The ME performs the updating procedure with EF_{LP}.

11.2.5 Administrative information request;

The ME performs the reading procedure with EF_{AD}.

11.2.6 SIM service table request

The ME performs the reading procedure with EF_{SST}.

11.2.7 SIM phase request

The ME performs the reading procedure with EF_{Phase}.

11.2.8 SIM Presence Detection and Proactive Polling

As an additional mechanism, to ensure that the SIM has not been removed during a card session, the ME sends, at frequent intervals, a STATUS command during each call. A STATUS command shall be issued within all 30 second periods of inactivity on the SIM-ME interface during a call. Inactivity in this case is defined as starting at the end of the last communication or the last issued STATUS command. If no response data is received to this STATUS command, then the call shall be terminated as soon as possible but at least within 5 seconds after the STATUS command has been sent. If the DF indicated in response to a STATUS command is not the same as that which was indicated in the previous response, or accessed by the previous command, then the call shall be terminated as soon as possible but at least within 5 seconds after the response data has been received. This procedure shall be used in addition to a mechanical or other device used to detect the removal of a SIM.

If the ME supports the proactive SIM service, and the SIM has this service activated in its Service Table, then during idle mode the ME shall send STATUS commands to the SIM at intervals no longer than the interval negotiated with the SIM (see TS 51.014 [27]).

11.2.9 Preferred Language

Request: The ME performs the reading procedure with EF_{PL}.

Update: The ME performs the updating procedure with EF_{PL}.

11.3 CHV related procedures

A successful completion of one of the following procedures grants the access right of the corresponding CHV for the GSM session. This right is valid for all files within the GSM application protected by this CHV.

After a third consecutive presentation of a wrong CHV to the SIM, not necessarily in the same GSM session, the CHV status becomes "blocked" and if the CHV is "enabled", the access right previously granted by this CHV is lost immediately.

An access right is not granted if any of the following procedures are unsuccessfully completed or aborted.

11.3.1 CHV verification

The ME checks the CHV status.

In the case of CHV1 the following procedure applies:

- if the CHV1 status is "blocked" and CHV1 is "enabled", the procedure ends and is finished unsuccessfully;
- if the CHV1 status is "blocked" but CHV1 is "disabled", the procedure ends and is finished successfully. The ME shall, however, accept SIMs which do not grant access rights when CHV1 is "blocked" and "disabled". In that case ME shall consider those SIMs as "blocked";
- if the CHV1 status is not "blocked" and CHV1 is "disabled", the procedure is finished successfully;
- if the CHV1 status is not "blocked" and CHV1 is "enabled", the ME uses the VERIFY CHV function. If the CHV1 presented by the ME is equal to the corresponding CHV1 stored in the SIM, the procedure is finished successfully. If the CHV1 presented by the ME is not equal to the corresponding CHV1 stored in the SIM, the procedure ends and is finished unsuccessfully.

In the case of CHV2 the following procedure applies:

- if the CHV2 status is "blocked", the procedure ends and is finished unsuccessfully;
- if the CHV2 status is not "blocked", the ME uses the VERIFY CHV function. If the CHV2 presented by the ME is equal to the corresponding CHV2 stored in the SIM, the procedure is finished successfully. If the CHV2 presented by the ME is not equal to the corresponding CHV2 stored in the SIM, the procedure ends and is finished unsuccessfully.

11.3.2 CHV value substitution

The ME checks the CHV status. If the CHV status is "blocked" or "disabled", the procedure ends and is finished unsuccessfully.

If the CHV status is not "blocked" and the enabled/disabled indicator is set "enabled", the ME uses the CHANGE CHV function. If the old CHV presented by the ME is equal to the corresponding CHV stored in the SIM, the new CHV presented by the ME is stored in the SIM and the procedure is finished successfully.

If the old CHV and the CHV in memory are not identical, the procedure ends and is finished unsuccessfully.

11.3.3 CHV disabling

Requirement: Service n°1 "allocated and activated".

The ME checks the CHV1 status. If the CHV1 status is "blocked", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked", the ME reads the CHV1 enabled/disabled indicator. If this is set "disabled", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked" and the enabled/disabled indicator is set "enabled", the ME uses the DISABLE CHV function. If the CHV1 presented by the ME is equal to the CHV1 stored in the SIM, the status of CHV1 is set "disabled" and the procedure is finished successfully. If the CHV1 presented by the ME is not equal to the CHV1 stored in the SIM, the procedure ends and is finished unsuccessfully.

11.3.4 CHV enabling

The ME checks the CHV1 status. If the CHV1 status is "blocked", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked", the ME reads the CHV1 enabled/disabled indicator. If this is set "enabled", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked" and the enabled/disabled indicator is set "disabled", the ME uses the ENABLE CHV function. If the CHV1 presented by the ME is equal to the CHV1 stored in the SIM, the status of CHV1 is set "enabled" and the procedure is finished successfully. If the CHV presented by the ME is not equal to the CHV1 stored in the SIM, the procedure ends and is finished unsuccessfully.

11.3.5 CHV unblocking

The execution of the CHV unblocking procedure is independent of the corresponding CHV status, i.e. being blocked or not.

The ME checks the UNBLOCK CHV status. If the UNBLOCK CHV status is "blocked", the procedure ends and is finished unsuccessfully.

If the UNBLOCK CHV status is not "blocked", the ME uses the UNBLOCK CHV function. If the UNBLOCK CHV presented by the ME is equal to the corresponding UNBLOCK CHV stored in the SIM, the relevant CHV status becomes "unblocked" and the procedure is finished successfully. If the UNBLOCK CHV presented by the ME is not equal to the corresponding UNBLOCK CHV stored in the SIM, the procedure ends and is finished unsuccessfully.

11.4 GSM security related procedures

11.4.1 GSM algorithms computation

The ME selects DF_{GSM} and uses the RUN GSM ALGORITHM function (see clause 8.16). The response SRES-Kc is sent to the ME when requested by a subsequent GET RESPONSE command.

11.4.2 IMSI request

The ME performs the reading procedure with EF_{IMSI}.

11.4.3 Access control request

The ME performs the reading procedure with EF_{ACC}.

11.4.4 Higher Priority PLMN search period request

The ME performs the reading procedure with EF_{HPPLMN}.

11.4.5 Location information

Request: The ME performs the reading procedure with EF_{LOCI}.

Update: The ME performs the updating procedure with EF_{LOCI}.

11.4.6 Cipher key

Request: The ME performs the reading procedure with EF_{Kc}.

Update: The ME performs the updating procedure with EF_{Kc}.

11.4.7 BCCH information

Request: The ME performs the reading procedure with EF_{BCCH}.

Update: The ME performs the updating procedure with EF_{BCCH}.

11.4.8 Forbidden PLMN

Request: The ME performs the reading procedure with EF_{PLMN}.

Update: The ME performs the updating procedure with EF_{PLMN}.

11.4.9 LSA information

Request: The ME performs the reading procedure with EF_{SAI}, EF_{SLL} and its associated LSA Descriptor files.

Update: The ME performs the updating procedure with EF_{SLL}.

11.4.10 GPRS Location information

Requirement: Service n°38 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{LOCIGPRS}$.

Update: The ME performs the updating procedure with $EF_{LOCIGPRS}$.

11.4.11 GPRS Cipher key

Requirement: Service n°38 "allocated and activated".

Request: The ME performs the reading procedure with EF_{KcGPRS}.

Update: The ME performs the updating procedure with EF_{KcGPRS}.

11.5 Subscription related procedures

11.5.1 Dialling numbers

The following procedures may not only be applied to EF_{ADN} and its associated extension files EF_{CCP} and EF_{EXT1} as described in the procedures below, but also to EF_{FDN}, EF_{MSISDN}, EF_{LND}, EF_{BDN}, EF_{SDN}, EF_{MBDN} and their associated extension files. If these files are not allocated and activated, as denoted in the SIM service table, the current procedure shall be aborted and the appropriate EFs shall remain unchanged.

As an example, the following procedures are described as applied to ADN.

Requirement: Service n°2 "allocated and activated"

(Service n°3 for FDN,

Service n°9 for MSISDN,

Service n°13 for LND,

Service n°18 for SDN,

Service n°31 for BDN,

Service n°53 for MBDN)

Update: The ME analyses and assembles the information to be stored as follows (the byte identifiers used below correspond to those in the description of the EFs in clauses 10.5.1, 10.5.4 and 10.5.10):

i) The ME identifies the Alpha-tagging, Capability/Configuration Identifier and Extension1 Record Identifier.

ii) The dialling number/SSC string shall be analysed and allocated to the bytes of the EF as follows:

- if a "+" is found, the TON identifier is set to "International";

- if 20 or less "digits" remain, they shall form the dialling number/SSC string;
- if more than 20 "digits" remain, the procedure shall be as follows:

  Requirement:

  Service n°10 "allocated and activated";

  (Service n°10 applies also for MSISDN and LND;

  Service n°11 for FDN;

  Service n°19 for SDN;

  Service n°32 for BDN;

  Service n°53 for MBDN).

  The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.

  The first 20 "digits" are stored in the dialling number/SSC string. The value of the length of BCD number/SSC contents is set to the maximum value, which is 11. The Extension1 record identifier is coded with the associated record number in the EF_{EXT1}. The remaining digits are stored in the selected Extension1 record where the type of the record is set to "additional data". The first byte of the Extension1 record is set with the number of bytes of the remaining additional data. The number of bytes containing digit information is the sum of the length of BCD number/SSC contents of EF_{ADN} and byte 2 of all associated chained Extension1 records containing additional data (see clauses 10.5.1 and 10.5.10).

iii) If a called party subaddress is associated to the ADN/SSC the procedure shall proceed as follows:

Requirement:
Service n°10 "allocated and activated"
(Service n°10 applies also for MSISDN and LND;
Service n°11 for FDN;
Service n°19 for SDN;
Service n°32 for BDN;
Service n°53 for MBDN).

If the length of the called party subaddress is less than or equal to 11 bytes (see TS 24.008 [47] for coding):

- the ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted;
- the ME stores the called party subaddress in the Extension1 record, and sets the Extension1 record type to "called party subaddress".

If the length of the called party subaddress is greater than 11 bytes (see TS 24.008 [47] for coding):

- the ME seeks for two free records in EF_{EXT1}. If no such two records are found, the ME runs the Purge procedure. If two Extension1 records are still unavailable, the procedure is aborted;
- the ME stores the called party subaddress in the two Extension1 records. The identifier field in the Extension1 record containing the first part of the subaddress data is coded with the associated EF_{EXT1} record number containing the second part of the subaddress data. Both Extension1 record types are set to "called party subaddress".

Once i), ii), and iii) have been considered the ME performs the updating procedure with EF_{ADN}. If the SIM has no available empty space to store the received ADN/SSC, or if the procedure has been aborted, the ME advises the user.

NOTE 1: For reasons of memory efficiency the ME is allowed to analyse all Extension1 records to recognize if the additional or subaddress data to be stored is already existing in EF_{EXT1}. In this case the ME may use the existing chain or the last part of the existing chain from more than one ADN (LND, MSISDN). The ME is only allowed to store extension data in unused records. If existing records are used for multiple access, the ME shall not change any data in those records to prevent corruption of existing chains.

Erasure: The ME sends the identification of the information to be erased. The content of the identified record in EF_{ADN} is marked as "free".

Request: The ME sends the identification of the information to be read. The ME shall analyse the data of EF_{ADN} (subclause 10.5.1) to ascertain, whether additional data is associated in EF_{EXT1} or EF_{CCP}. If necessary, then the ME performs the reading procedure on these EFs to assemble the complete ADN/SSC.

Purge: The ME shall access each EF which references EF_{EXT1} ($EF_{EXT2,}$ EF_{EXT6}) for storage and shall identify records in these files using extension data (additional data or called party subaddress). Note that existing chains have to be followed to the end. All referred Extension1 (Extension2, Extension6) records are noted by the ME. All Extension1 (Extension2, Extension6) records not noted are then marked by the ME as "free" by setting the whole record to 'FF'.

NOTE 2: Dependent upon the implementation of the ME, and in particular the possibility of erasure of ADN/SSC records by Phase 1 MEs, which have no knowledge of the EF_{EXT1}, it is possible for Extension1 records to be marked as "used space" (not equal to 'FF'), although in fact they are no longer associated with an ADN/SSC record.

The following three procedures are only applicable to service n°3 (FDN).

FDN capability request. The ME has to check the state of service n°3, i.e. if FDN is "enabled" or "disabled". In case of enabled FDN, the ME has to switch to a restrictive terminal mode (see TS 22.101 [53]). To ascertain the state of FDN, the ME checks in EF_{SST} whether or not ADN is activated. If ADN is not activated, service n°3 is enabled. If ADN is activated, the ME checks the response data of EF_{ADN}. If EF_{ADN} is invalidated, service n°3 is enabled. In all other cases service n°3 is disabled.

FDN disabling. The FDN disabling procedure requires that CHV2 verification procedure has been performed successfully and that ADN is activated. If not, FDN disabling procedure will not be executed successfully. To disable FDN capability, the ME rehabilitates EF_{ADN}. The invalidate/rehabilitate flag of EF_{ADN}, which is implicitly set by the REHABILITATE command, is at the same time the indicator for the state of the service n°3. If ADN is not activated, disabling of FDN is not possible and thus service n°3 is always enabled (see FDN capability request).

NOTE 3: If FDN is disabled (by rehabilitating EF_{ADN}) using an administrative terminal then the FDN disabling procedure of this administrative terminal need also to rehabilitate EF_{IMSI} and EF_{LOCI} to ensure normal operation of the SIM in a phase 1 ME or a phase 2 ME which does not support FDN.

FDN enabling. The FDN enabling procedure requires that CHV2 verification procedure has been performed successfully. If not, FDN enabling procedure will not be executed successfully. To enable FDN capability, the ME invalidates EF_{ADN}. The invalidate/rehabilitate flag of EF_{ADN}, which is implicitly cleared by the INVALIDATE command, is at the same time the indicator for the state of the service n°3 (see FDN capability request). If ADN is not activated, service n°3 is always enabled.

Invalidated ADNs may optionally still be readable and updatable depending on the file status (see clause 9.3)

The following three procedures are only applicable to service n°31 (BDN).

BDN capability request. The ME has to check the state of service n°31, i.e. if BDN is "enabled" or "disabled". BDN service is "enabled" only if service n°31 is allocated and activated, and EF_{BDN} is not invalidated. In all other cases, the BDN service is "disabled".

BDN disabling. The BDN disabling procedure requires that CHV2 verification procedure has been performed successfully. If not, BDN disabling procedure will not be executed successfully. To disable BDN capability, the ME invalidates EF_{BDN}. The invalidate/rehabilitate flag of EF_{BDN}, which is implicitly cleared by the INVALIDATE command, is at the same time the indicator for the state of the service n°31 (see BDN capability request).

BDN enabling. The BDN enabling procedure requires that CHV2 verification procedure has been performed successfully. If not, BDN enabling procedure will not be executed successfully. To enable BDN capability, the ME rehabilitates EF_{BDN}. The invalidate/rehabilitate flag of EF_{BDN}, which is implicitly set by the REHABILITATE command, is at the same time the indicator for the state of the service n°31 (see BDN capability request).

Invalidated BDNs (when BDN capability is disabled) may optionally still be readable and updatable depending on the file status (see clause 9.3).

11.5.2 Short messages

Requirement: Service n°4 "allocated and activated".

Request: The SIM seeks for the identified short message. If this message is found, the ME performs the reading procedure with EF_{SMS}.

If service n°35 is "allocated and activated" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the ME performs the reading procedure with the corresponding record in EF_{SMSR}. If the ME does not find a corresponding record in EF_{SMSR}, then the ME shall update the status of the SMS with '15' (status report requested, received but not stored in EF_{SMSR}).

If the short message is not found within the SIM memory, the SIM indicates that to the ME.

Update: The ME looks for the next available area to store the short message. If such an area is available, it performs the updating procedure with EF_{SMS}.

If there is no available empty space in the SIM to store the received short message, a specific MMI will have to take place in order not to loose the message.

Erasure: The ME will select in the SIM the message area to be erased. Depending on the MMI, the message may be read before the area is marked as "free". After performing the updating procedure with EF_{SMS}, the memory allocated to this short message in the SIM is made available for a new incoming message. The memory of the SIM may still contain the old message until a new message is stored in this area.

If service n°35 is "allocated and activated" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the ME performs the erasure procedure for EF_{SMSR} with the corresponding record in EF_{SMSR}.

11.5.3 Advice of Charge (AoC)

Requirement: Service n°5 "allocated and activated".

Accumulated Call Meter.

Request: The ME performs the reading procedure with EF_{ACM}. The SIM returns the last updated value of the ACM.

Initialization: The ME performs the updating procedure with EF_{ACM} using the new initial value.

Increasing: The ME performs the increasing procedure with EF_{ACM} sending the value which has to be added.

Accumulated Call Meter Maximum Value.

Request: The ME performs the reading procedure with EF_{ACMmax}.

Initialization: The ME performs the updating procedure with EF_{ACMmax} using the new initial maximum value.

Price per Unit and Currency Table (PUCT).

Request: The ME performs the reading procedure with EF_{PUCT}.

Update: The ME performs the updating procedure with EF_{PUCT}.

11.5.4 Capability configuration parameters

Requirement: Service n°6 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CCP}.

Update: The ME performs the updating procedure with EF_{CCP}.

Erasure: The ME sends the identification of the requested information to be erased. The content of the identified record in EF_{CCP} is marked as "free".

11.5.5 PLMN selector

Requirement: Service n°7 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{PLMNsel}$.

Update: The ME performs the updating procedure with $EF_{PLMNsel}$.

11.5.6 Cell broadcast message identifier

Requirement: Service n°14 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CBMI}.

Update: The ME performs the updating procedure with EF_{CBMI}.

11.5.7 Group identifier level 1

Requirement: Service n°15 "allocated and activated".

Request: The ME performs the reading procedure with EF_{GID1}.

11.5.8 Group identifier level 2

Requirement: Service n°16 "allocated and activated".

Request: The ME performs the reading procedure with EF_{GID2}.

11.5.9 Service Provider Name

Requirement: Service n°17 "allocated and activated".

Request: The ME performs the reading procedure with EF_{SPN}.

11.5.10 Voice Group Call Services

Requirement: Service n°21 "allocated and activated".

Voice Group Call Service

Request: The ME performs the reading procedure with EF_{VGCS}.

Voice Group Call Service Status

Request: The ME performs the reading procedure with EF_{VGCSS}.

Update: The ME performs the updating procedure with EF_{VGCSS}.

11.5.11 Voice Broadcast Services

Requirement: Service n°22 "allocated and activated".

Voice Broadcast Service

Request: The ME performs the reading procedure with EF_{VBS}.

Voice Broadcast Service Status

Request: The ME performs the reading procedure with EF_{VBSS}.

Update: The ME performs the updating procedure with EF_{VBSS}.

11.5.12 Enhanced Multi Level Pre-emption and Priority Service

Requirement: Service n°23 "allocated and activated".

Enhanced Multi Level Pre-emption and Priority

Request: The ME performs the reading procedure with EF_{eMLPP}.

Automatic Answer on eMLPP service

Request: The ME performs the reading procedure with EF_{AAeM}.

Update: The ME performs the updating procedure with EF_{AAeM}.

11.5.13 Cell Broadcast Message range identifier

Requirement: Service n°30 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CBMIR}.

Update: The ME performs the updating procedure with EF_{CBMIR}.

11.5.14 Depersonalisation Control Keys

Requirement: Service n°33 "allocated and activated".

Request: The ME performs the reading procedure with EF_{DCK}.

11.5.15 Short message status report

Requirement: Service n°35 "allocated and activated".

Request: If the status of a stored short message indicates that there is a corresponding status report, the ME performs the seek function with EF_{SMSR} to identify the record containing the appropriate status report. The ME performs the reading procedure with EF_{SMSR}.

Update: If a status report is received, the ME first seeks within the SMS record identifiers of EF_{SMSR} for the same record number it used for the short message in EF_{SMS}. If such a record identifier is found in EF_{SMSR}, it is used for storage. If such a record identifier is not found, then the ME seeks for a free entry in EF_{SMSR} for storage. If no free entry is found the ME runs the Purge procedure with EF_{SMSR}. If there is still no free entry, the status report is not stored.

If the ME found an appropriate record in EF_{SMSR} for storage, it updates the record with the status report setting the record identifier in EF_{SMSR} to the appropriate record number of the short message in EF_{SMS}.

The status in EF_{SMS} is updated accordingly (see clause 10.5.3) by performing the update procedure with EF_{SMS}.

Erasure: The ME runs the update procedure with EF_{SMSR} by at least storing '00' in the first byte of the record. The ME may optionally update the following bytes with 'FF'.

Purge: The ME shall read the SMS record identifier (byte 1) of each record of EF_{SMSR}. With each record the ME checks the corresponding short messages in EF_{SMS}. If the status (byte 1) of the corresponding SMS is not equal '1D' (status report requested, received and stored in EF_{SMSR}), the ME shall perform the erasure procedure with the appropriate record in EF_{SMSR}.

11.5.16 Network's indication of alerting

Requirement: Service n°36 "allocated and activated".

Request: The ME performs the reading procedure with EF_{NIA}.

11.5.17 User controlled PLMN Selector with Access Technology

Requirement: Service n°43"allocated and activated".

Request: The ME performs the reading procedure with $EF_{PLMNwAcT}$.

Update: The ME performs the updating procedure with $EF_{PLMNwAcT}$.

11.5.18 Operator controlled PLMN Selector with Access Technology

Requirement: Service n°44 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{OPLMNwAcT}$

11.5.19 HPLMN Selector with Access Technology

Requirement: Service n°45 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{HPLMNAcT}$.

11.5.20 CPBCCH information

Requirement: Service n°46 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CPBCCH}.

Update: The ME performs the updating procedure with EF_{CPBCCH}.

11.5.21 Investigation Scan

Requirement: Service n°47 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{InvScan}$.

11.5.22 Void

11.5.23 PLMN Network Name

Requirement: Service n°51 "allocated and activated".

Request: The ME performs the reading procedure with EF_{PNN}.

11.5.24 Operator PLMN List

Requirement: Service n°52 "allocated and activated".

Request: The ME performs the reading procedure with EF_{OPL}

11.5.25 Message Waiting Indication

Requirement: Service n°54 "allocated and activated".

Request: The ME performs the reading procedure with EF_{MWIS}.

Update: The ME performs the updating procedure with EF_{MWIS}.

11.5.26 Call Forwarding Indication Status

Requirement: Service n°55 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CFIS}.

Update: The ME performs the updating procedure with EF_{CFIS}.

11.5.27 Service Provider Display Information

Requirement: Services n°17 and 56 are "allocated and activated".

Request: The ME performs the reading procedure with EF_{SPDI}.

Update: The ME performs the updating procedure with EF_{SPDI}.

11.5.28 MMS Notifications

Requirement: Service n°57 "allocated and activated".

Request: The ME sends the identification of the information to be read, then the ME performs the reading procedure with $EF_{MMSN.}$ If Service n°58 is allocated and activated the ME shall analyse the data of EF_{MMSN} to ascertain, whether additional data is associated in EF_{EXT8}. If necessary, then the ME performs the reading procedure on EF_{EXT8} to assemble the complete MMS notification.

Update: The ME analyses and assembles the MMS notification to be stored as follows:

– if the MMS notification contains not more bytes than the maximum possible number for EF_{MMSN} then the ME looks for the next available area to store the MMS notification. If such an area is available, it performs the updating procedure with EF_{MMSN}.

– if the MMS notification contains more bytes than the maximum possible number for EF_{MMSN} then the ME seeks for a sufficient number of free records in EF_{EXT8} to store the complete MMS notification.

- If there is not a sufficient number of EF_{EXT8} records marked as "free" to store the complete MMS notification, the procedure is aborted.

- otherwise, the ME performs the updating procedure and stores as many bytes as possible in EF_{MMSN}. The Extension file record number of EF_{MMSN} is coded with the associated record number in the EF_{EXT8}. The remaining bytes are stored in the selected EF_{EXT8} record where the type of the record is then set to "additional data". The second byte of the EF_{EXT8} record is set with the number of bytes of the remaining additional data. It is possible, if the number of additional digits exceeds the capacity of the additional record, to chain another record inside the EF_{EXT8} by the identifier in the last byte of the record. In this case byte 2 of each record for additional data within the same chain indicates the number of bytes within the same record.

The ME is only allowed to store extension data in unused records of EF_{EXT8}

If there is no available empty space in the SIM to store the MMS notification, it is up to ME implementation how the notification is handled.

Erasure: The ME will select in the USIM the MMS notification to be erased. Depending on the MMI, the MMS notification may be read before the area is marked as "free". The memory of the SIM may still contain the old MMS notification until a new message is stored. If Service n°58 is allocated and activated all associated records in EF_{EXT8} are then marked by the ME as "free" by setting them to 'FF'.

11.5.29 MMS Issuer Connectivity Parameters

Requirement: Service n°57 "allocated and activated".

Request: The ME performs the reading procedure with EF_{MMSICP}.

Update: The ME performs the updating procedure with $EF_{MMSICP.}$

11.5.30 MMS User Preferences

Requirement: Service n°57 "allocated and activated".

Request: The ME performs the reading procedure with EF_{MMSUP}.

Update: The ME performs the updating procedure with $EF_{MMSUP.}$

11.5.31 MMS User Connectivity Parameters

Requirement: Services n°57 and n°59 "allocated and activated".

Request: The ME performs the reading procedure with EF_{MMSUCP}.

Update: The ME performs the updating procedure with $EF_{MMSUCP.}$

11.6 SIM Application Toolkit related procedures

SIM Application Toolkit is an optional feature. The higher level procedures, and contents and coding of the commands, are given in TS 51.014 [27]. Procedures relating to the transmission of commands and responses across the SIM/ME interface are given in this clause. A SIM or ME supporting SIM Application Toolkit shall conform to the requirements given in this clause.

11.6.1 Initialization procedure

A SIM supporting SIM Application Toolkit shall indicate this through relevant data in EF_{Phase} and EF_{SST}, as defined in the relevant clauses above.

An ME supporting SIM Application Toolkit shall perform initialization as defined in the SIM Initialization clause above.

11.6.2 Proactive polling

An ME supporting proactive SIM (part of SIM Application Toolkit) shall support the polling procedure as defined above.

11.6.3 Support of commands

A SIM or ME supporting SIM Application Toolkit shall support the commands TERMINAL PROFILE, ENVELOPE, FETCH and TERMINAL RESPONSE.

These commands shall never be used if either the SIM or ME does not support SIM Application Toolkit. Therefore standard SIMs and MEs do not need to support these commands.

11.6.4 Support of response codes

A SIM or ME supporting SIM Application Toolkit shall support the response status words (SW1 SW2) '91 XX', and '93 00' and '9E XX'. The SIM shall send '9E XX' only to an ME indicating in TERMINAL PROFILE that it supports the handling of these status words.

These responses shall never be used if either the SIM or ME does not support SIM Application Toolkit. Therefore standard SIMs and MEs do not need to support them.

11.6.5 Command-response pairs

Using the terminology where the ME issues a command and the SIM a response, ending in status words SW1 SW2, a command-response pair is considered as a single transaction. Each transaction is initiated by the ME and terminated by the SIM. One transaction must be completed before the next one can be initiated. This protocol applies to SIM Application Toolkit in the same way as it does to normal operation.

11.6.6 Independence of normal GSM and SIM Application Toolkit tasks

Normal GSM operation (relating to general, CHV related, GSM security related, and subscription related procedures) and SIM Application Toolkit operation shall be logically independent, both in the SIM and in the ME.

Specifically, this means:

- the currently selected EF and current record pointer in the normal GSM task shall remain unchanged, if still valid, as seen by the ME, irrespective of any SIM Application Toolkit activity;
- between successive SIM Application Toolkit related command-response pairs, other normal GSM related command-response pairs can occur. The SIM Application Toolkit task status shall remain unchanged by these command-response pairs.

11.6.7 Use of BUSY status response

If for any reason the SIM Application Toolkit task of the SIM cannot process an ENVELOPE command issued by the ME at present (e.g. other SIM Application Toolkit processes are already running, and this additional one would cause an overload), the SIM can respond with a status response of '93 00'. The ME may re-issue the command at a later stage.

The BUSY status response has no impact on normal GSM operation.

11.6.8 Use of NULL procedure byte

The NULL procedure byte provides a mechanism for the SIM to obtain more time before supplying the response part of a command-response pair, during which time the ME is unable to send further commands to the SIM.

If a SIM Application Toolkit activity in the SIM runs for too long, this may prevent the ME from sending "normal GSM" commands which are time-critical, e.g. RUN GSM ALGORITHM. A MORE TIME command is defined in TS 51.014 [27], which ensures that the SIM Application Toolkit task in the SIM gets more processing time, while at the same time freeing the SIM/ME interface. This should be used in preference to NULL procedure bytes ('60').

11.6.9 Using the TERMINAL PROFILE, ENVELOPE, and TERMINAL RESPONSE commands

These commands are part of the set used by SIM Application Toolkit. The use of the these commands, the occasions where they are required, and the command and response parameters associated with the commands, are specified in TS 51.014 [27]. The ME completes the command parameters/data of the relevant command and sends the command to the SIM. The transmitted data is processed by the SIM in a specific way depending on the tag value in the command parameters.

A SIM or ME not supporting SIM Application Toolkit does not need to support these commands.

11.6.10 Using the FETCH command

This command is used by SIM Application Toolkit. The use of the this command, the occasions where it is required, and the command and response parameters associated with the command, are specified in TS 51.014 [27]. It is similar in function to GET RESPONSE, in that it requests response parameters from the SIM, following a '91 XX' status response. The transmitted response data from the SIM is processed by the ME in a specific way depending on the tag value in the response parameters.

A SIM or ME not supporting SIM Application Toolkit does not need to support this command.

11.6.11 Data Download via SMS-CB

Requirement: Service n°25 "allocated and activated".

The ME shall perform the reading procedure with EF_{CBMID}. On receiving a cell broadcast message with an identifier which matches an identifier in EF_{CBMID}, the ME shall pass the CB message to the SIM using the ENVELOPE command. If a match is not found and service no. 14 is "allocated and activated", then the message identifier is checked against those in EF_{CBMI}.

11.6.12 Data Download via SMS-PP

Requirement: Service n°26 "allocated and activated".

The procedures and commands for Data Download via SMS-PP are defined in TS 51.014 [27].

11.6.13 Menu selection

Requirement: Service n°27 "allocated and activated".

The procedures and commands for Menu Selection are defined in TS 51.014 [27].

11.6.14 Call Control

Requirement: Service n°28 "allocated and activated".

The procedures and commands for Call Control are defined in TS 51.014 [27]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Call Control in the TERMINAL PROFILE command. When BDN is enabled, the Call control facility of the ME is used by the SIM to support the BDN service.

11.6.15 Proactive SIM

Requirement: Service n°29 "allocated and activated".

The procedures and commands for Proactive SIM, at the application level, are defined in TS 51.014 [27].

11.6.16 Mobile Originated Short Message control by SIM

Requirement: Service n°37 "allocated and activated".

The procedures and commands for Mobile Originated Short Message control by SIM are defined in TS 51.014 [27]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Mobile Originated Short Message control by SIM in the TERMINAL PROFILE command.

11.6.17 SIM data download error

In case of an ENVELOPE for SIM data download, the SIM can respond with the status words '9E XX' to indicate that response data is available. The ME shall use the GET RESPONSE command to get the response data. The ME shall then send transparently to the network this response data, using the error procedure of the transport mechanism.

11.6.18 Image Request

Requirement: Service n°39 "allocated and activated".

The ME sends the identification of the information to be read. The ME shall analyse the data of EF_{IMG} (clause 10.6.1.1) to identify the files containing the image's instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete image instance data.

11.7 MExE related procedures

MExE is an optional feature. The higher level procedures, and contents and coding of the commands, are given in TS 23.057 [50]. Procedures relating to the transmission of commands and responses across the SIM/ME interface are given in this clause. A SIM or ME supporting MExE shall conform to the requirements given in this clause.

11.7.1 MExE ST

Requirement: Service n°49 (MExE) "allocated and activated".
Request: The ME performs the reading procedure with EF_{MExE_ST}.

11.7.2 Operator root public key

Requirement: Service n°49 (MExE) "allocated and activated" and MExE ST service n°1 (EF_{ORPK})" allocated and activated".
Request: The ME performs the reading procedure with EF_{ORPK}. The ME shall analyse the data of EF_{ORPK} (clause 10.7.2) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

11.7.3 Administrator root public key

Requirement: Service n°49 (MExE) "allocated and activated" and MExE ST service n°2 (EF_{ARPK}) "allocated and activated".
Request: The ME performs the reading procedure with EF_{ARPK}. The ME shall analyse the data of EF_{ARPK} (clause 10.7.3) to identify the file containing the certificate instance. If necessary, then the ME performs READ BINARY commands on this file to assemble the complete certificate instance data.

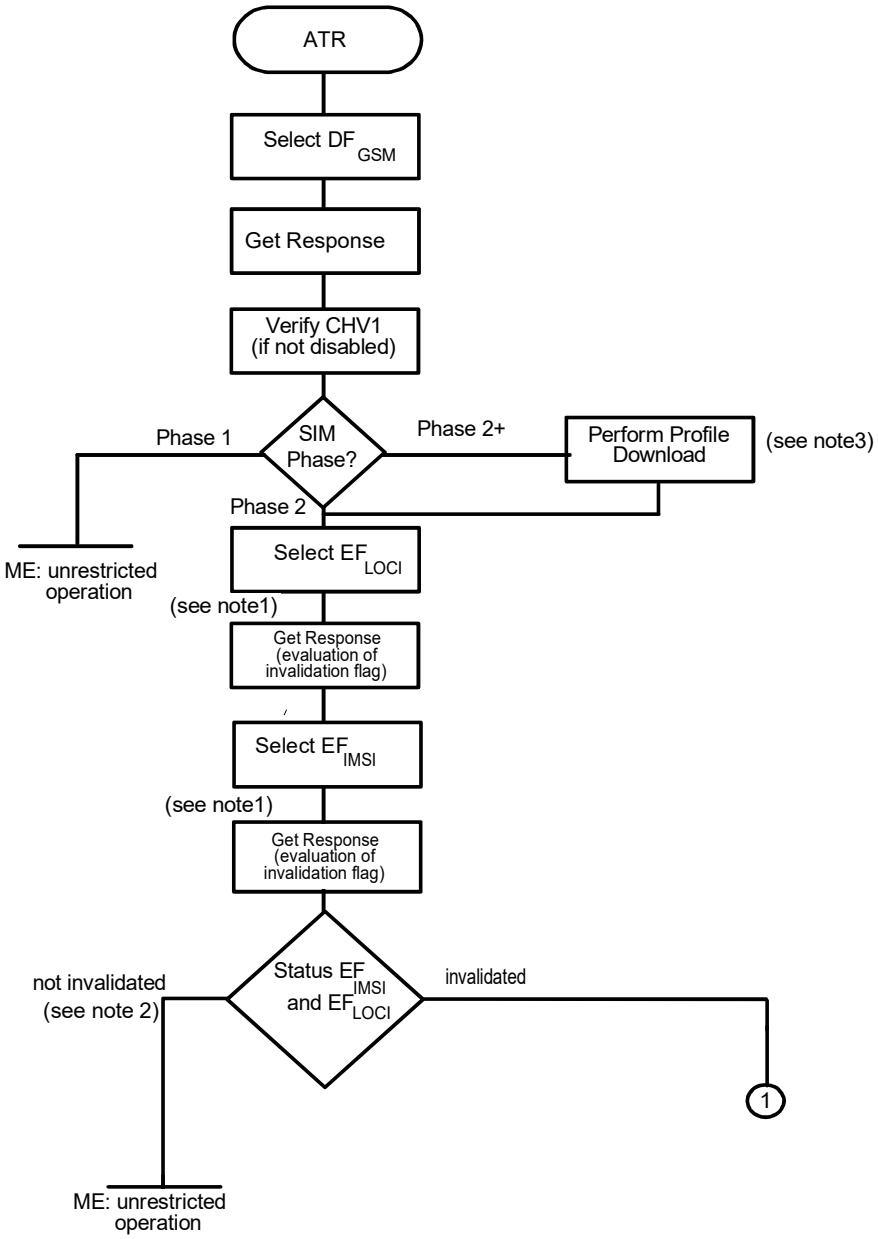
11.7.4 Third Party root public key(s)

Requirement: Service n°49 (MExE) "allocated and activated" and MExE ST service n°3 (EF_{TPRPK}) "allocated and activated".
Request: The ME performs the reading procedure with EF_{TPRPK}. The ME shall analyse the data of EF_{TPRPK} (clause 10.7.4) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

Annex A (normative):
Void

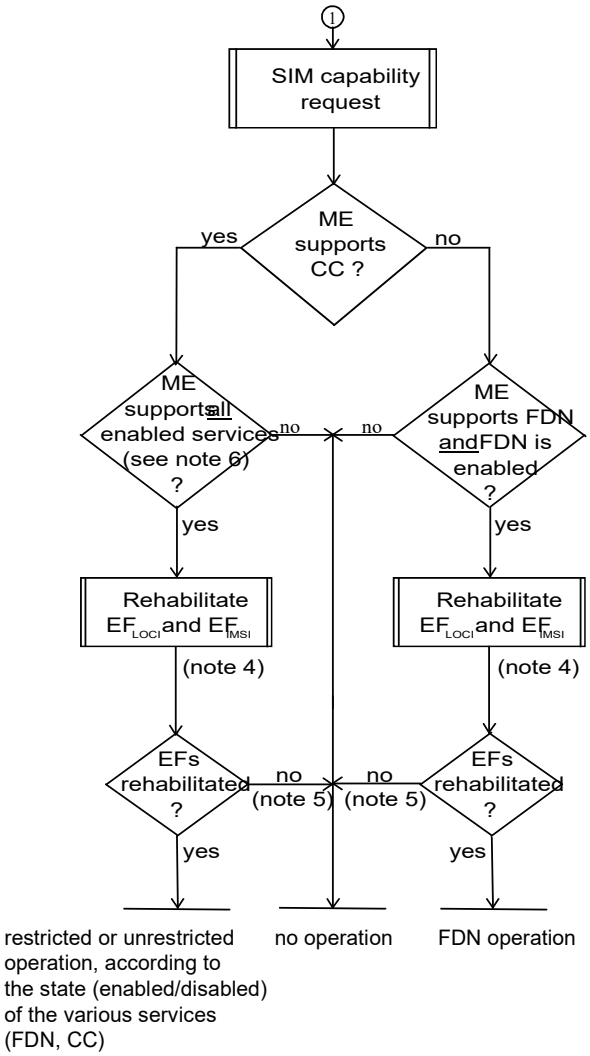
Annex B (normative): Void

Annex C (informative): FDN/BDN Procedures



NOTE 1: In case of enabled FDN and/or enabled BDN, the EF has been invalidated by the SIM at no later than this stage.
NOTE 2: Invalidation of only one of the two EFs is not allowed for FDN and BDN.
NOTE 3: For SIMs with enabled BDN this procedure is used to check whether the ME supports the Call Control by the SIM facility.

Figure C.1a: Example of an Initialization Procedure of a FDN/BDN SIM (see clause 11.2.1)



NOTE 4: In case of "BDN enabled", the SIM only allows rehabilitation of the EF_{IMSI} and EF_{LOCI}, if the ME has indicated its CC-capability to the SIM (by PROFILE_DOWNLOAD).

NOTE 5: Possibility for future "restricting" services to use the internal SIM mechanism of invalidation of EF_{IMSI} and EF_{LOCI}.

NOTE 6: If the ME does not support all enabled services (e.g. FDN, BDN), it does not operate. In case of enabled BDN, the support of the "Call Control Feature" by the ME is sufficient for operation. For future use, there may be additional "restricting" services, which are not known to the ME. In that case the ME will perform the subsequent rehabilitation procedure but will fail to rehabilitate EF_{IMSI} and EF_{LOCI} (see note 4).

Figure C.1b: Example of an Initialization Procedure of a FDN/BDN SIM (continued)

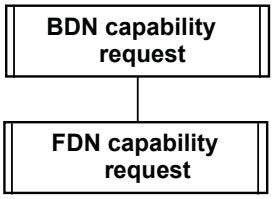


Figure C.2: SIM capability request

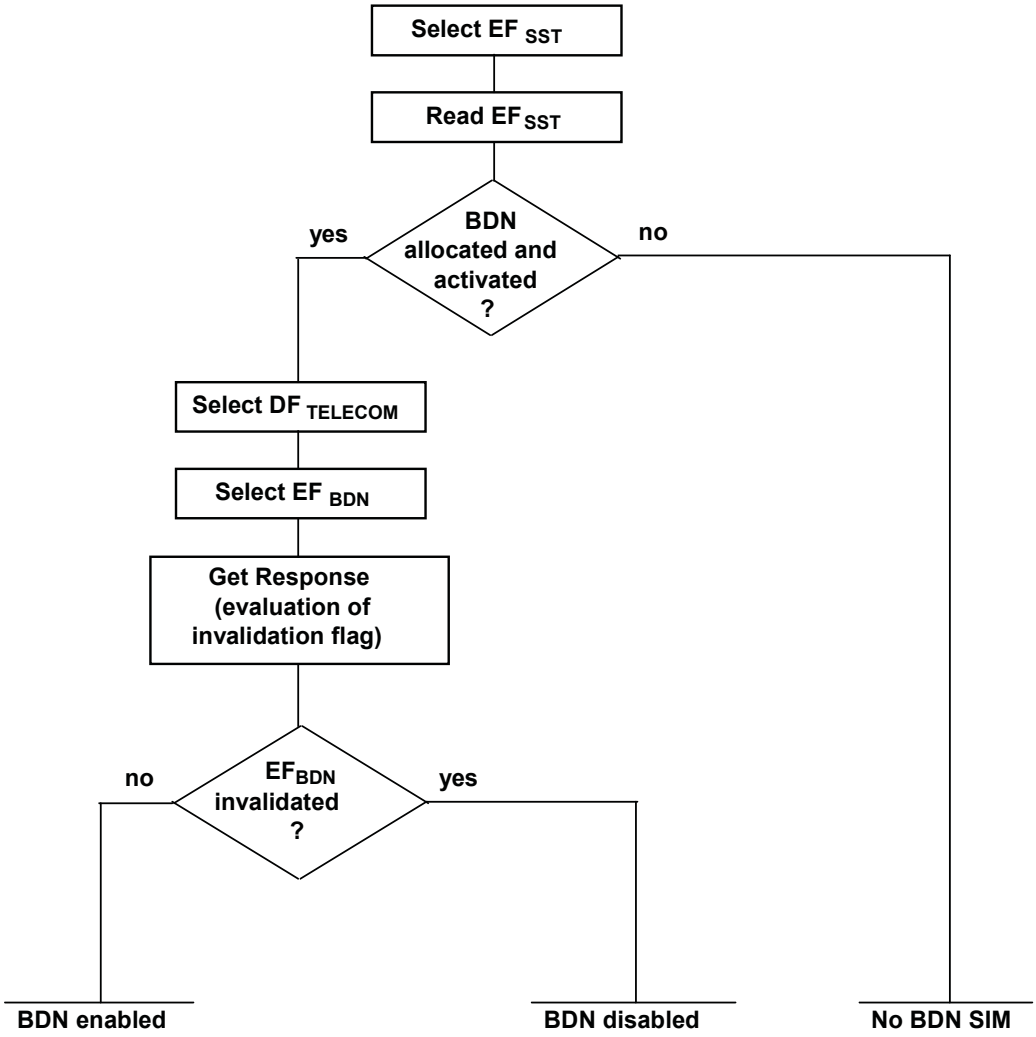
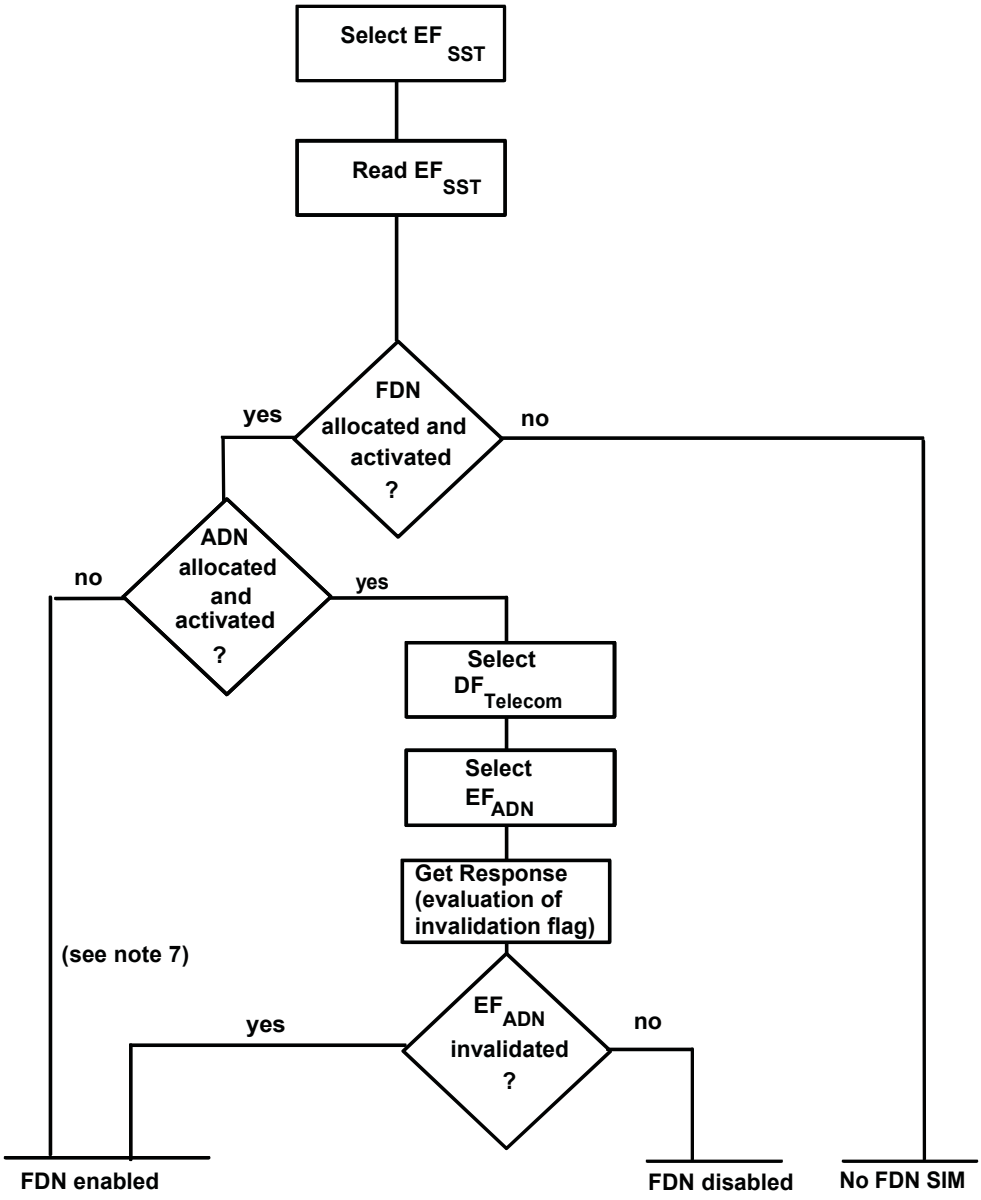
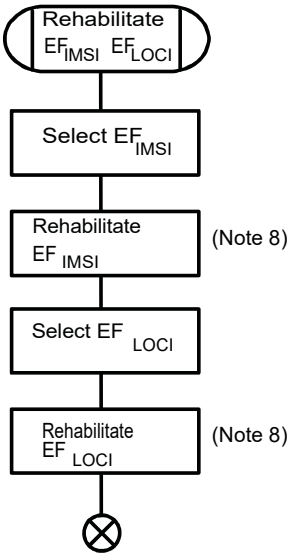


Figure C.3: BDN capability request (see clause 11.5.1)



NOTE 7: In this case FDN is enabled without the possibility of disabling.

Figure C.4: FDN capability request (see clause 11.5.1)



NOTE 8: If BDN is enabled in the SIM, and if the Profile download procedure has not indicated that the ME supports Call Control, the EF is not rehabilitated by the SIM.

Figure C.5: Procedure to rehabilitate GSM files

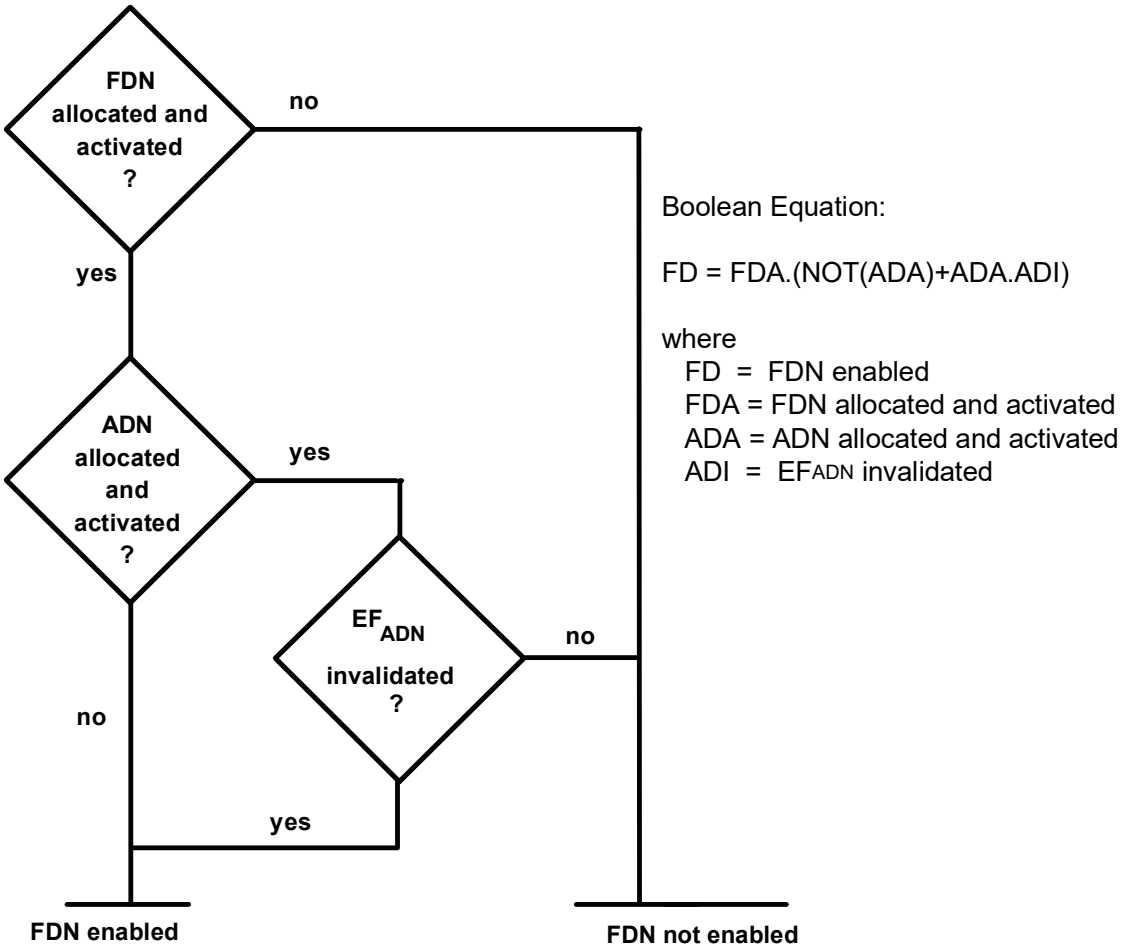


Figure C.6: Coding for state of FDN

Annex D (informative): Suggested contents of the EFs at pre-personalization

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'2FE2'	ICC identification	operator dependant (see 10.1.1)
'2F05'	Extended Language preference	'FF…FF'
'6F05'	Language preference	'FF'
'6F07'	IMSI	operator dependant (see 10.3.2)
'6F20'	Ciphering key Kc	'FF...FF07'
'6F30'	PLMN selector	'FF...FF'
'6F31'	Higher Priority PLMN search period	'FF'
'6F37'	ACM maximum value	'000000' (see note 1)
'6F38'	SIM service table	operator dependant (see 10.3.7)
'6F39'	Accumulated call meter	'000000'
'6F3E'	Group identifier level 1	operator dependant
'6F3F'	Group identifier level 2	operator dependant
'6F41'	PUCT	'FFFFFF0000'
'6F45'	CBMI	'FF...FF'
'6F46'	Service provider name	'FF...FF'
'6F48'	CBMID	'FF...FF'
'6F49'	Service Dialling Numbers	'FF...FF'
'6F74'	BCCH information	'FF...FF'
'6F78'	Access control class	operator dependant (see 10.3.15)
'6F7B'	Forbidden PLMNs	'FF...FF'
'6F7E	Location information	'FFFFFFFF xxxxxx 0000 FF 01' (see note 2)
'6FAD'	Administrative data	operator dependant (see 10.3.18)
'6FAE'	Phase identification	see 10.3.16
'6F3A'	Abbreviated dialling numbers	'FF...FF'
'6F3B'	Fixed dialling numbers	'FF...FF'
'6F3C'	Short messages	'00FF...FF'
'6F3D'	Capability configuration parameters	'FF...FF'
'6F40'	MSISDN storage	'FF...FF'
'6F42'	SMS parameters	'FF...FF'
'6F43'	SMS status	'FF...FF'
'6F44'	Last number dialled	'FF...FF'
'6F47'	Short message status reports	'00 FF…FF'
'6F4A'	Extension 1	'00 FF...FF'
'6F4B'	Extension 2	'00 FF...FF'
'6F4C'	Extension 3	'00 FF...FF'
'6F4D'	Barred dialling numbers	'FF...FF'
'6F4E'	Extension 4	'00 FF...FF'
'6F4F'	Extended capability configuration parameters	'FF...FF'
'6F51'	Network's indication of alerting	'FF...FF'
'6F52'	GPRS Ciphering key KcGPRS	'FF...FF07'
'6F53'	GPRS Location Information	'FFFFFFFF FFFFFF xxxxxx 0000 FF 01' (see note 2)
'6F54'	SetUpMenu Elements	operator dependant (see 10.3.34)
'6F58'	Comparison method information	'FF…FF'
'6F60'	User controlled PLMN Selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F61'	Operator controlled PLMN Selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F62'	HPLMN Selector with Access Technology	'FFFFFF0000..FFFFFF0000'
'6F63'	CPBCCH information	'FF..FF'
'6F64'	Investigation Scan	'00'

Continued

File Identification	Description	Value
'4F20'	Image data	'00FF...FF'
'4F30'	SoLSA Access Indicator)	'00FF...FF'
'4F31'	SoLSA LSA List	'FF...FF'
'6FC5'	PLMN Network Name	Operator dependant
'6FC6'	Operator PLMN List	Operator dependant
'6FC7'	Mailbox Dialling Numbers	Operator dependant
'6FC8'	Extension 6	'00 FF...FF'
'6FC9'	Mailbox Identifier	Operator dependant
'6FCA'	Message Waiting Indication Status	'00 00 00 00 00'
'6FCB'	Call Forwarding Indication Status	'xx 00 FF...FF'
'6FCC'	Extension 7	'00 FF...FF'
'6FCD'	Service Provider display Information	'FF...FF'
"6FCE"	MMS Notification	"00 00 00 FF…FF"
"6FCF"	Extension 8	'00 FF...FF'
"6FD0"	MMS Issuer Connectivity Parameters	"FF…FF"
"6FD1"	MMS User Preferences	"FF…FF"
"6FD2"	MMS User Connectivity Parameters	"FF…FF"

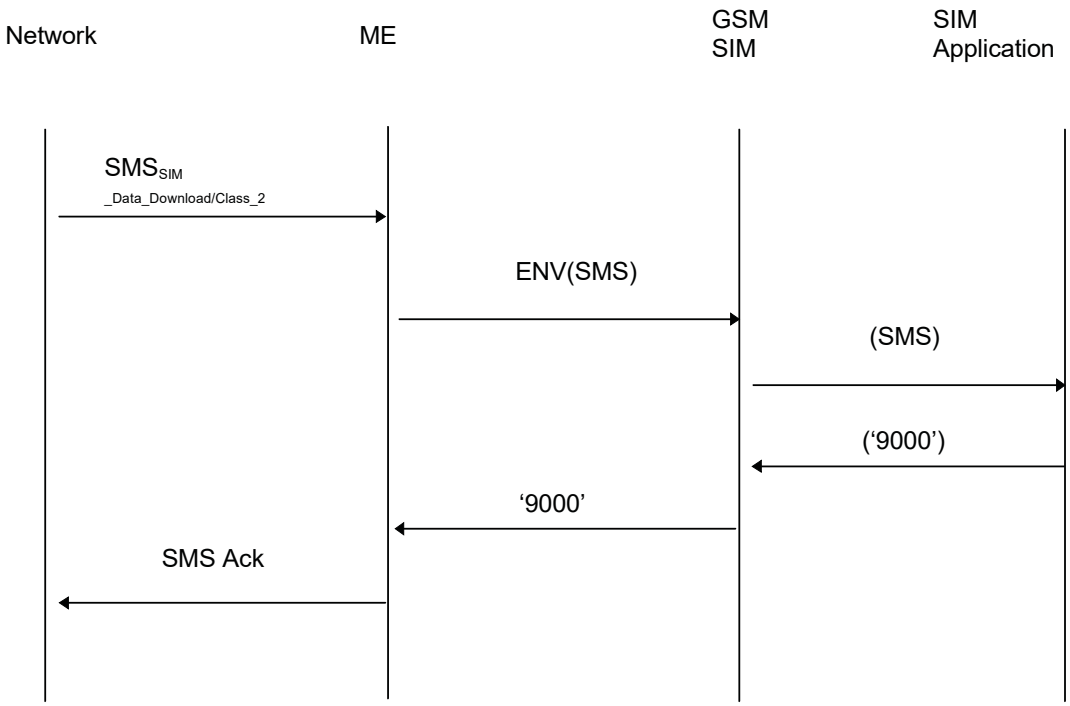
NOTE 1: The value '000000' means that ACMmax is not valid, i.e. there is no restriction on the ACM. When assigning a value to ACMmax, care should be taken not to use values too close to the maximum possible value 'FFFFFF', because the INCREASE command does not update EF_{ACM} if the units to be added would exceed 'FFFFFF'. This could affect the call termination procedure of the Advice of Charge function.

NOTE 2: xxxxxx stands for any valid MCC and MNC, coded according to TS 24.008 [47].

Annex E (informative): SIM application Toolkit protocol diagrams

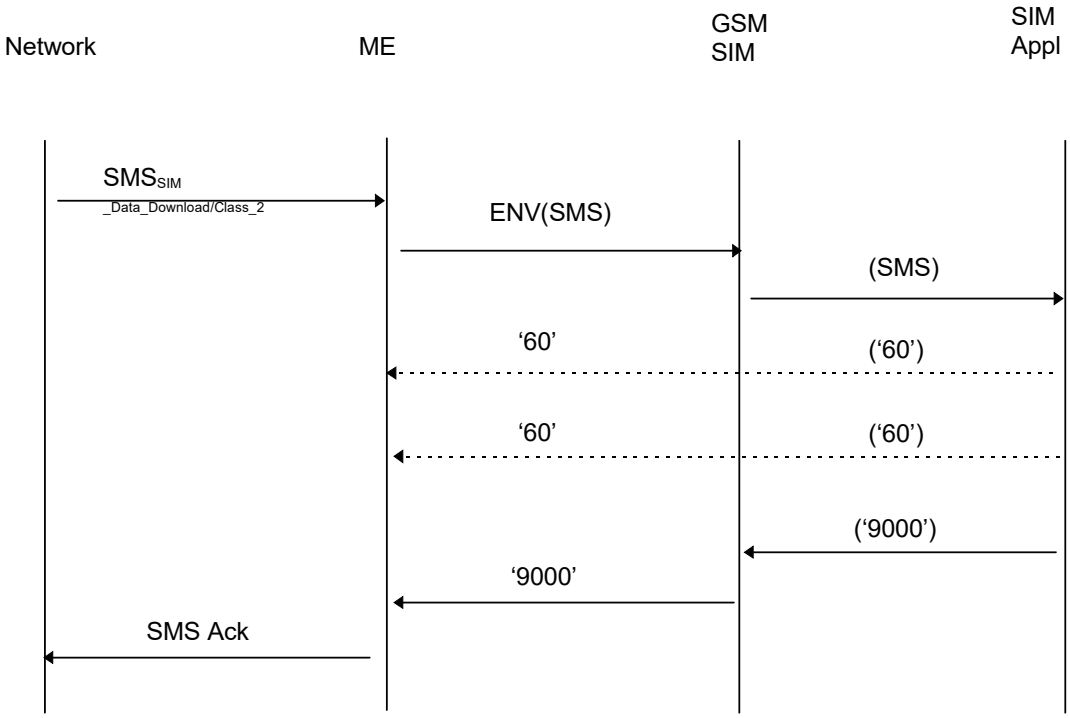
The diagrams in this annex are intended to illustrate the data protocols of the SIM toolkit application in various situations. The SIM application is shown as initiated by SMS Data Download messages. Other possibilities exist (as defined in TS 51.014) such as data entry from a menu selection.

Case 1: Simple



This shows the simple case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and processed immediately by the SIM application. This requires no ME action except to acknowledge the SMS.

Case 2: Simple with short delay

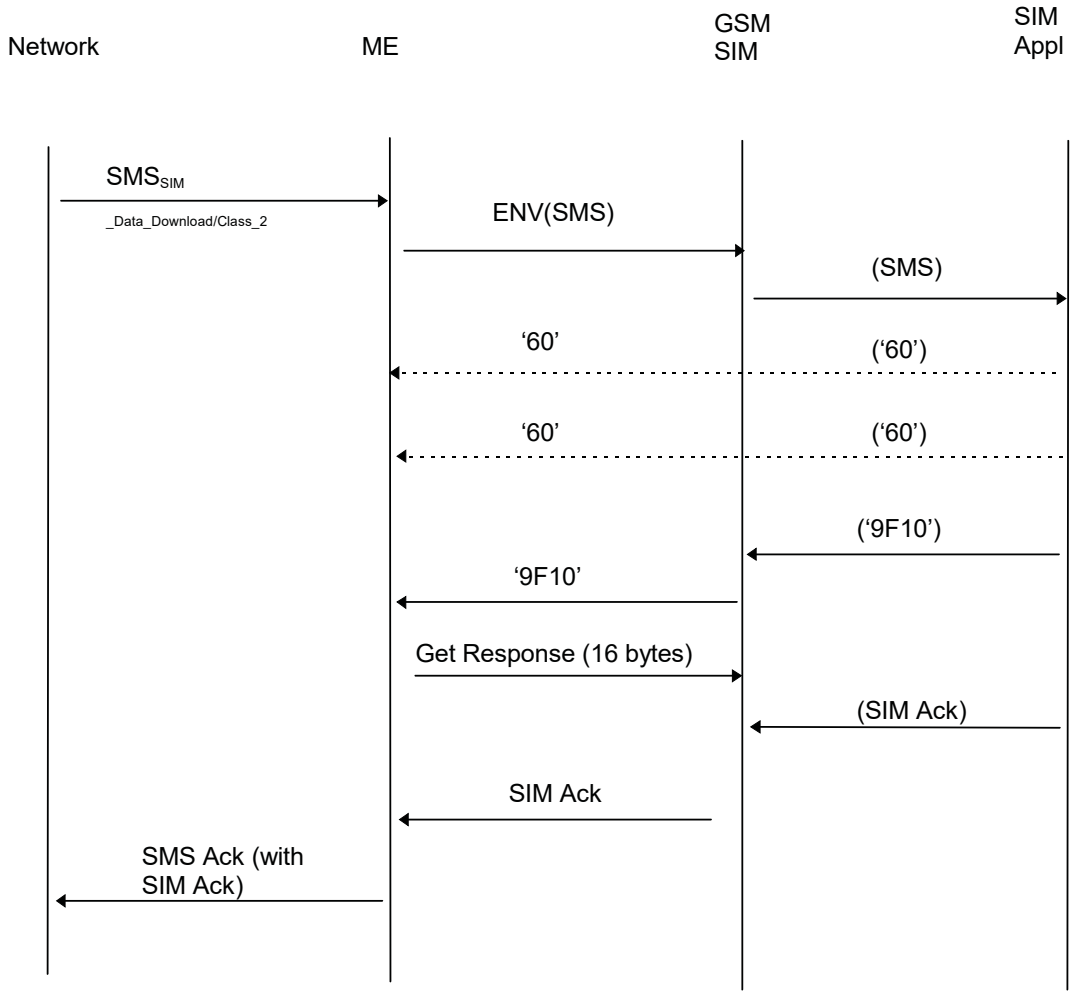


This shows the simple case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and which requires some time to process by the SIM application. The processing time is "not long" and is obtained by the SIM application sending "null procedure bytes" to the ME. Each byte has the effect of restarting the work waiting time so that the ME does not abort the transaction before the SIM application has finished processing the command(s) sent in the SMS.

Guidelines on timings:

1. The SMS Ack must be sent back before the network times out and sends the SMS again.
2. Use of null procedure bytes must not be excessive as during this time the ME is unable to issue normal GSM commands to the SIM.

Case 3: Simple with short delay and SIM Acknowledgement

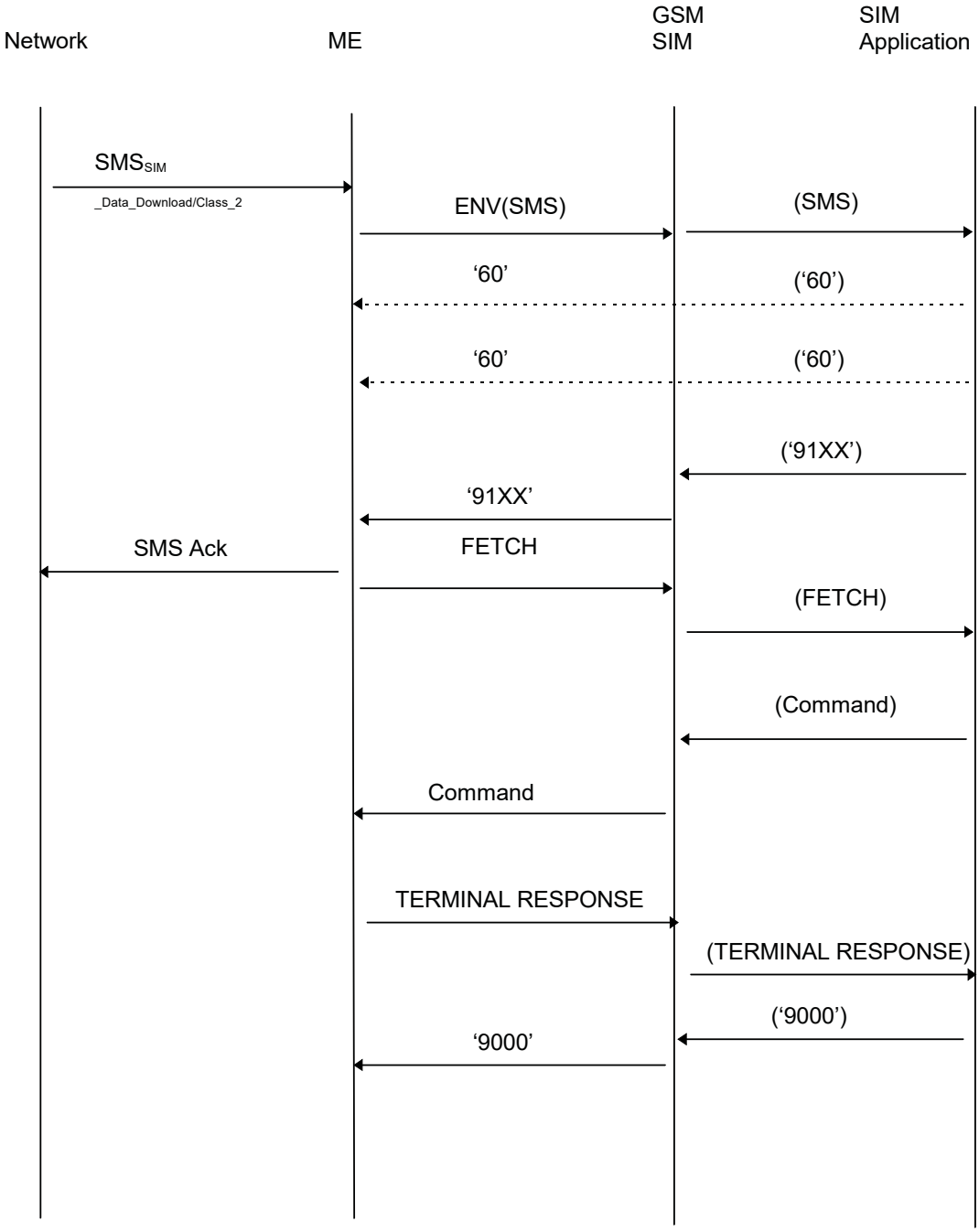


This shows the same case as previously where an SMS for SIM updating is received from the network, passed to the SIM by the ME and which requires some time to process by the SIM application. However in this case the SIM application has SIM acknowledgement data to include in the SMS acknowledgement being returned to the network by the ME.

Guideline on timings:

The SMS Ack must be sent back before the network times out and sends the SMS again.

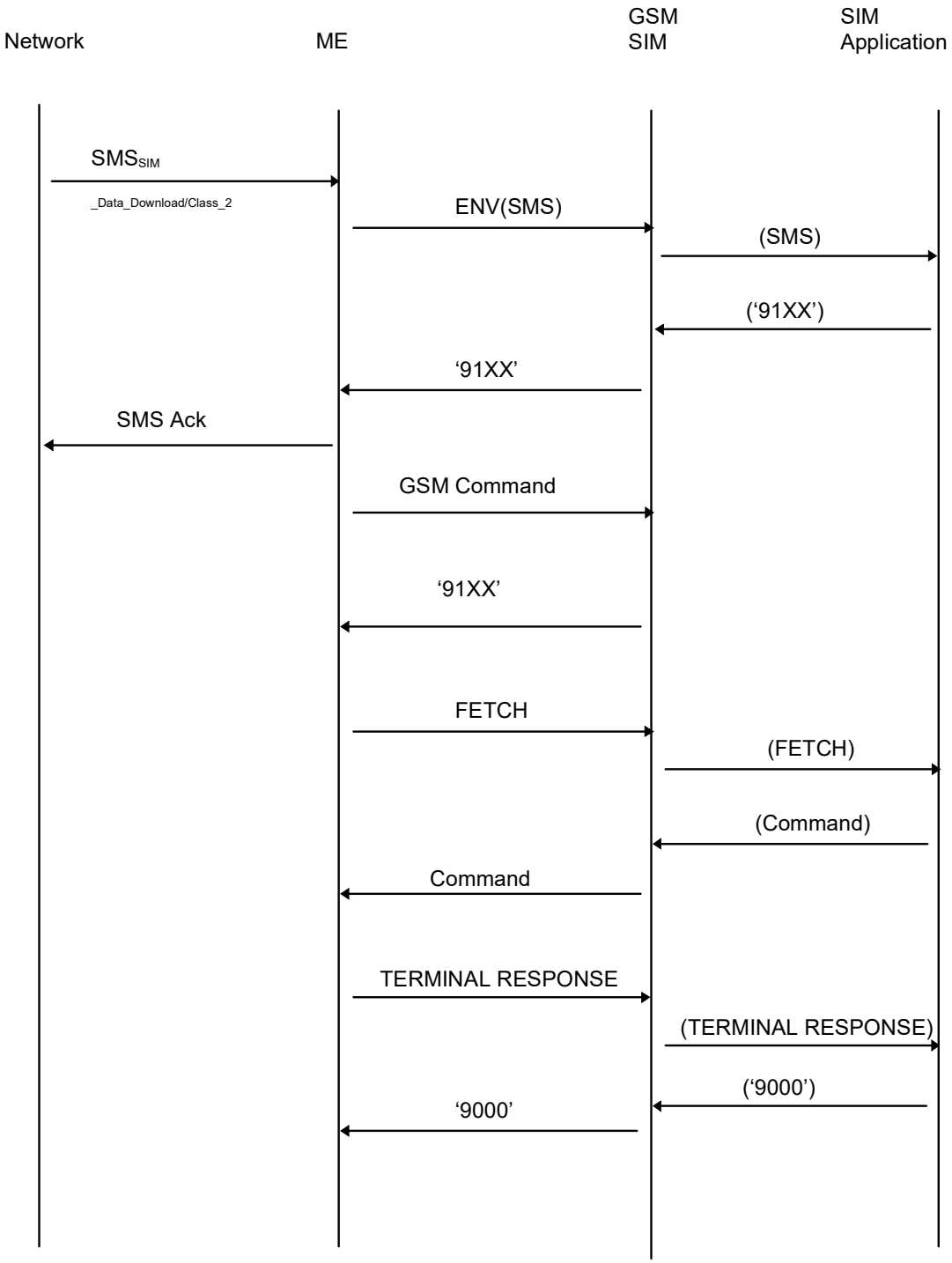
Case 4: A Toolkit command generated by the SIM application as a result of an SMS from the network



This shows the case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and processed by the SIM application which then generates a command for action by the ME (e.g. PLAYTONE).

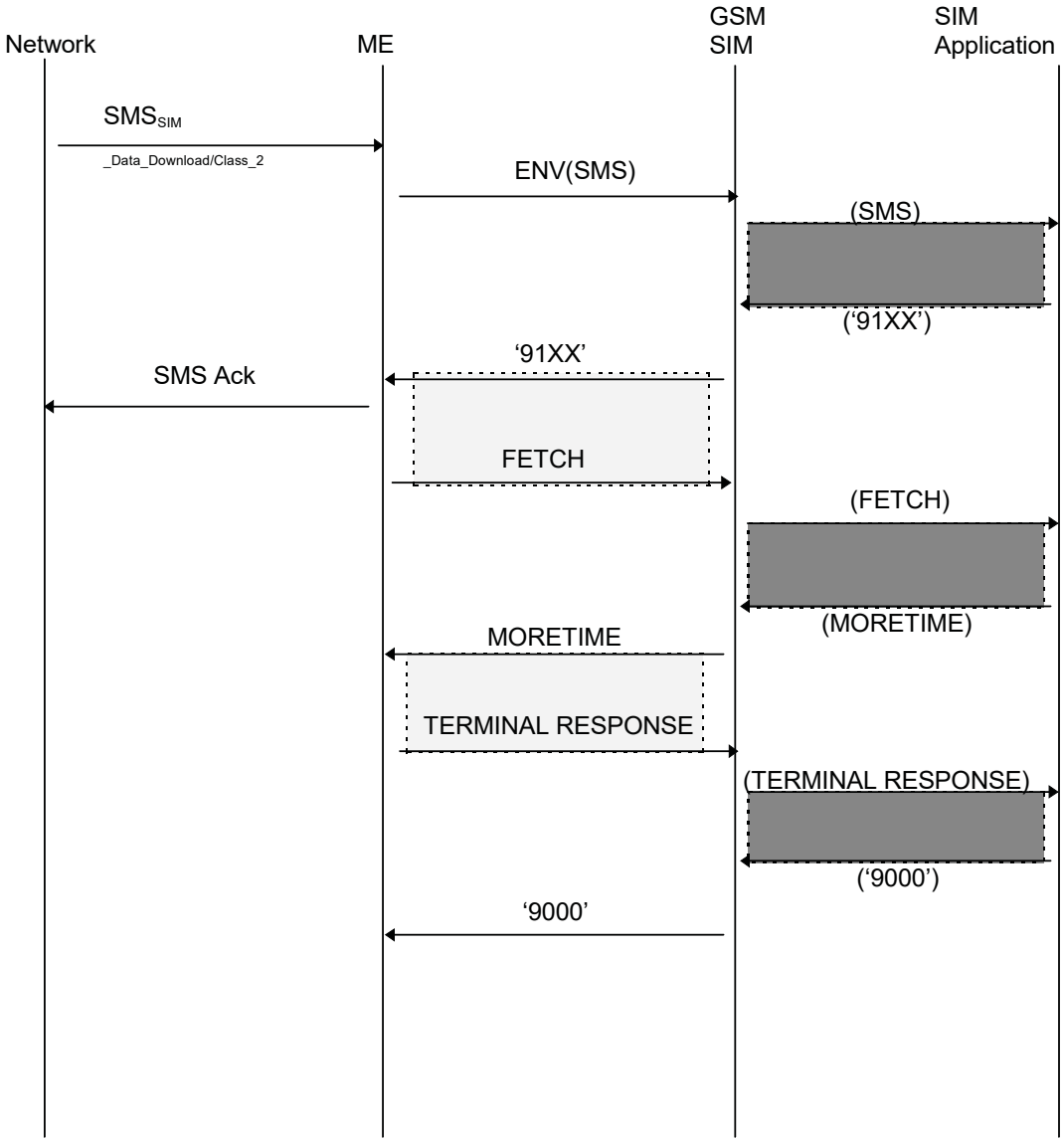
NOTE: If a positive acknowledgement to the network of completion of execution of the instructions given in the SMS message is required then the SIM application can issue a command to the ME to send a MO SMS.

Case 5: A normal GSM command requires processing before the ME can respond to the 91XX from the SIM



This shows the case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and processed by the SIM application which then generates a command for action by the ME (e.g. PLAYTONE). However a normal GSM command requires processing before the ME can FETCH the command which the SIM is waiting to give it. The response to the normal GSM command is '91XX' in this case to remind the ME of the outstanding SIM application command request.

Case 6: MORE TIME Command



This shows the case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and requires a considerable period of time to be processed by the SIM application. In this case the use of null procedure bytes only is inappropriate as the ME must be given the opportunity to process normal GSM commands. The opportunities gained by the SIM application for processing, and the opportunities for normal GSM commands are shown in the diagram above. The sequence of 91XX, FETCH and MORETIME commands can be repeated if required.

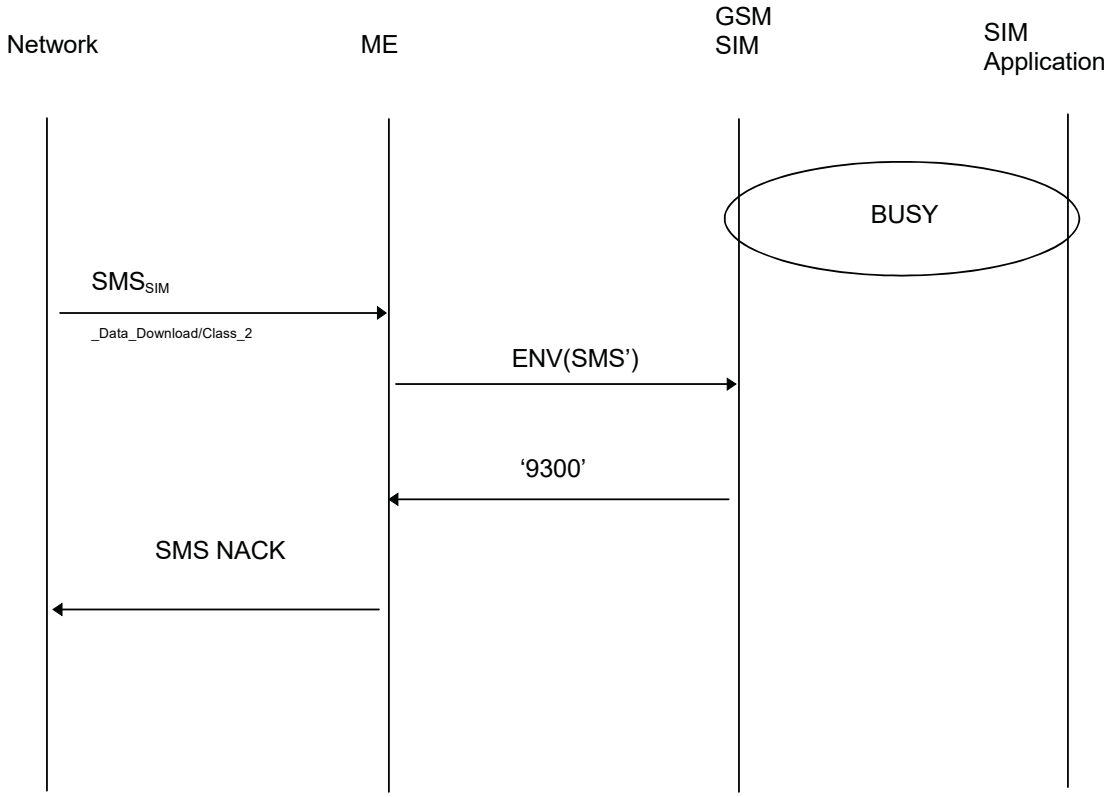
Opportunities to process normal GSM commands are shown thus:



Opportunities for SIM application processing are shown thus:



Case 7: SIM Application Busy



While the SIM application is busy processing a SMS for the SIM application arrives from the network and is sent to the SIM by the ME in the usual manner. The SIM operating system recognizes that the SIM application is busy, and it sends a busy response ('9300') to the ME. The ME then sends negative acknowledgement to the network. The responsibility for a retry rests with the network.

Annex F (informative): Examples of coding of LSA Descriptor files for SoLSA

The length of all the records is determined by the LSA descriptor containing the largest number of bytes. Combinations containing different numbers of LSA IDs, LAC+ CI and CI or LAC can therefore be done. Various examples are show. Due to the OTA management of the records it is recommended that the record length is maximum 100 bytes in order to leave room for command descriptor and signature information in the SMS.

This first example contains two LSAs, one described by two LSA IDs and another described by three Cell IDs, giving a record length of 8 bytes.

1st record:

LSA descriptor type = LSA ID and number = 2 (1 byte)	LSA ID (3 bytes)	LSA ID (3 bytes)	Identifier (1 byte)

2nd record:

LSA descriptor type = CI and number = 3 (1 byte)	CI (2 bytes)	CI (2 bytes)	CI (2 bytes)	Identifier (1 byte)

The second example contains two LSAs, one described by one LSA ID and one described by two Cell Ids, giving a record length of 6 bytes.

1st record:

LSA descriptor type = LSA ID and number = 1 (1 byte)	LSA ID (3 bytes)	'FF'	Identifier (1 byte)

2nd record:

LSA descriptor type = CI and number = 2 (1 byte)	CI (2 bytes)	CI (2 bytes)	Identifier (1 byte)

Annex G (normative): Image Coding Schemes

The following image coding schemes are applicable to rectangular raster images. Raster image points are assumed to be of square shape. They are numbered sequentially from 1 onwards, starting at the upper left corner, proceeding line by line downwards, each line in turn proceeding from left to right, and ending at the image's lower right corner.

The following example illustrates the numbering scheme for raster image points by showing how the corner points are numbered, assuming an image length of x points and an image height of y points.



G.1 Basic Image Coding Scheme

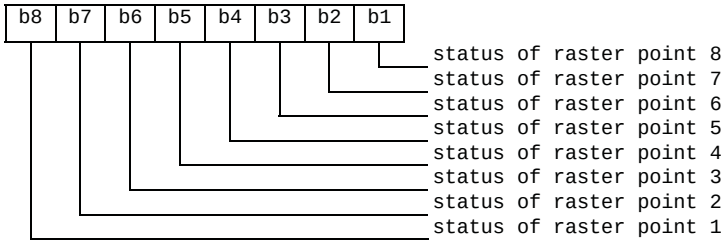
This coding scheme applies to rectangular raster images made up of raster points that are either set or not set. This coding scheme does not support any notion of colour. Image data are coded as follows:

Byte(s)	Description	Length
1	image width = X	1
2	image height = Y	1
3 to K+2	image body	K

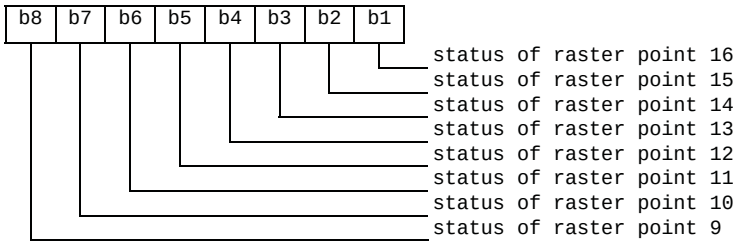
Coding of image body:

The status of each raster image point is coded in one bit, to indicate whether the point is set (status = 1) or not set (status = 0).

Byte 1:



Byte 2:



etc.

Unused bits shall be set to 1

G.2 Colour Image Coding Scheme

This coding scheme applies to coloured rectangular raster images. Raster image point colours are defined as references into a colour look-up table (CLUT), which contains a subset of the red-green-blue colour space. The CLUT in turn is located in the same transparent file as the image instance data themselves, at an offset defined within the image instance data.

Image data are coded as follows:

Byte(s)	Description	Length
1	Image width = X	1
2	Image height = Y	1
3	Bits per raster image point = B	1
4	Number of CLUT entries = C	1
5 to 6	Location of CLUT (Colour Look-up Table)	2
7 to K+6	Image body	K

- Bits per raster image point:

  Contents:

  The number B of bits used to encode references into the CLUT, thus defining a raster image point's colour.

  B shall have a value between 1 and 8.

  Coding:

  Binary.

- Number of entries in CLUT:

  Contents:

  The number C of entries in the CLUT which may be referenced from inside the image body. CLUT entries are numbered from 0 to C-1.

  C shall have a value between 1 and 2**B.

  Coding:

  Binary. The value 0 shall be interpreted as 256.

- Location of CLUT:

  Contents:

  This item specifies where the CLUT for this image instance may be found. The CLUT is always located in the same transparent file as the image instance data themselves, at an offset determined by these two bytes.

  Coding:

  Byte 1: high byte of offset into Image Instance File.

  Byte 2: low byte of offset into Image Instance File.

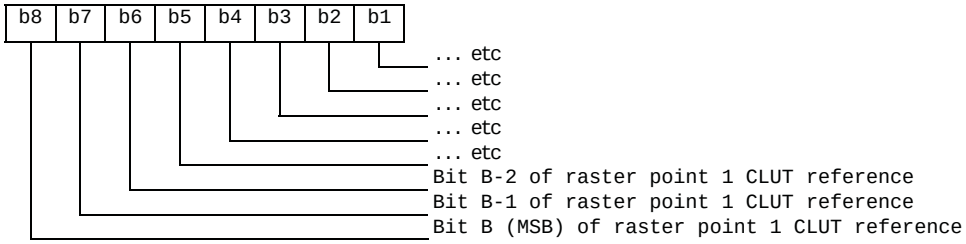
- Image body:

  Coding:

  Each raster image point uses B bits to reference one of the C CLUT entries for this image instance. The CLUT entry being thus referenced yields the raster image point's colour.

  The image body is arrayed as for the Basic Colour Image Coding Scheme, that is, starting with the highest bit of the first raster image point's colour information.

Byte 1:



etc.

Unused bits shall be set to 1.

The CLUT (Colour Look-up Table) for an image instance with C colours is defined as follows:

Contents:

C CLUT entries defining one colour each.

Coding:

The C CLUT entries are arranged sequentially:

Byte(s) of CLUT	CLUT Entry
1-3	entry 0
...	...
3*(C-1) +1 to 3*C	Entry C-1

Each CLUT entry in turn comprises 3 bytes defining one colour in the red-green-blue colour space:

Byte(s) of CLUT enty	Intensity of Colour
1	Red
2	Green
3	Blue

A value of 'FF' means maximum intensity, so the definition 'FF' '00' 00' stands for fully saturated red.

NOTE 1: Two or more image instances located in the same file can share a single CLUT.

NOTE 2: Most MEs capable of displaying colour images are likely to support at least a basic palette of red, green, blue and white.

Annex H (normative): Coding of EFs for NAM and GSM-AMPS Operational Parameters

If the EIA/TIA-553 DF is provisioned on the SIM, then EFs specified in this annex and indicated as mandatory under the DF shall be provided. TIA/EIA-41 [40] based radio access systems should use this DF for storage of NAM parameters.

All quantities shown in the EF descriptions abide by the following rules unless otherwise specified:

- all unused bits of allocated parameters shall be set by default to 0;
- all unused bytes in a series of values (e.g. Partner, Favoured, or Forbidden SID List) should be set by default to 'FF'.

H.1 Elementary File Definitions and Contents

H.1.1 EF_{MIN} (Mobile Identification Number)

This EF contains the Mobile Identification Number (MIN). The MIN is a 34-bit number used to address the mobile station across the AMPS and the TIA/EIA-136 air interfaces, and to identify the mobile station's home network. See TIA/EIA-136-005 [36] for further details on MIN.

Identifier: '4F88'	Structure: transparent	Mandatory
File size: 5 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	CHV2	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1 – 2	MIN2	M	2 bytes
3 – 5	MIN1	M	3 bytes

The MIN field is coded as follows:

- 6 most significant bits are unused;
- next 10 bits are MIN2;
- 24 least significant bits are MIN1;
- default MIN is '00 00 00 00 00' or 'FF FF FF FF FF'. In either case the ME shall interpret this as an invalid MIN and shall not transmit this value over the radio interface.

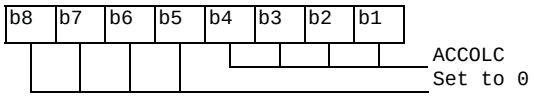
H.1.2 EF_{ACCOLC} (Access Overload Class)

This file contains the Access Overload Class (ACCOLC). The ACCOLC is a 4-bit indicator used to identify which overload class field controls the access attempts by the mobile station. See EIA/TIA-553 [41] for further details on ACCOLC.

Identifier: '4F89'	Structure: transparent	Mandatory
File size: 1 byte	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	CHV2	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1	ACCOLC (possible values from '00' to '0F')	M	1 byte

Byte 1:



Initial value shall be '00'.

H.1.3 EF_{SID} (System ID Of Home System)

This file contains the system identity of the home system. The SID is a 15-bit number that uniquely identifies an AMPS or TIA/EIA-41 system. See EIA/TIA-553 [41] for further details on Home SID.

Identifier: '4F80'	Structure: transparent	Mandatory
File size: 2 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	CHV2	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1-2	System ID of Home System (SID) (Most significant bit = 0)	M	2 bytes

The default value shall be '0000'.

H.1.4 EF_{IPC} (Initial Paging Channel)

The Initial (First) Paging Channel contains two 11-bit first paging channels (FIRSTCHP p-pri and FIRSTCHP p-sec) used to identify the channel number of the first paging channel when the mobile station is 'home'. See EIA/TIA-553 [41] for further details on First (Initial) Paging Channel.

Identifier: '4F82'	Structure: transparent	Mandatory
File size: 2-4 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	CHV2	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1 - 2	FIRSTCHPpri (Initial Paging Channel)	M	2 bytes
3 – 4	FIRSTCHPp-sec	O	2 bytes

- In the absence of the FIRSTCHPp-sec, the mobile station shall default to '02C4' if the primary channel = '014D' or '02E1' if the primary channel = '014E'

- A file size of 4 bytes may not be backwards compatible with the current dual-mode mobile equipment

The default of FISRTCHPpri value shall be '014D' for A systems, or '014E' for B systems.

H.1.5 EF_{GPI} (Group ID)

This file defines a subset of the most significant bits of the system identification (SID) that is used to identify a group of cellular systems for local control purposes. If the local control option is enabled within the mobile station and the bits of the home system identification that comprise the group identification match the corresponding bits of the SID read by the mobile station over the air, then the Local Control status shall be enabled. Otherwise, the Local Control status shall be disabled. Refer to EIA/TIA-553 [41] for additional details.

Identifier: '4F81'	Structure: transparent	Mandatory
File size: 1 byte	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	CHV2	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1	Group ID	M	1 byte

- Group ID default value for North America = '0A'.

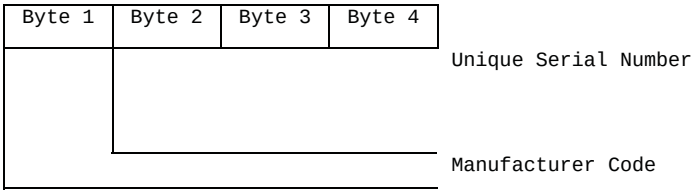
H.1.6 $EF_{S\text{-}ESN}$ (SIM Electronic Serial Number)

This file stores a 32-bit electronic serial number (ESN) that is unique to the GSM-ANSI-136 SIM. The S-ESN can be unrelated to the ESN of any host equipment to which the GSM-ANSI-136 SIM may be attached. The S-ESN can be used for registration in conjunction with the MIN. The S-ESN may also be used in conjunction with the A-key and CAVE algorithm for authentication. See the ANSI-136 Usage Indicator file for details on the ESN usage indicator which specifies to the mobile equipment how the S-ESN should be used. See EIA/TIA-553 [41] for details on the ESN as it applies to registration and authentication.

The contents of this EF shall not be changed by any over-the-air procedures.

Identifier: '4F8B'	Structure: transparent	Mandatory
File size: 4 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	NEVER	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1 – 4	SIM ESN	M	4 bytes



The default value shall be 'FF FF FF FF'.

H.1.7 EF_{COUNT} (Call Count)

This file contains the CALL COUNT parameter. The CALL COUNT is used as a simple 'clone' detector in TIA/EIA-136 and AMPS modes. During the network access signalling in AMPS and other TIA/EIA-41 based networks, the SIM reports its CALL COUNT value to the network. If the value is consistent with the network perception of the CALL COUNT for that SIM, then the network will likely grant access based on the authentication process. During an AMPS or other TIA/EIA-41 based systems call, the value of the CALL COUNT may be incremented upon a command from the network. The value of the CALL COUNT, when incremented, is incremented by 1 using the INCREASE command. See EIA/TIA-553 [41] for further details on COUNTs-p.

Identifier: '4F83'	Structure: Cyclic	Mandatory
File size: 3*N bytes	Update Activity: high	
Access Conditions:		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
Most Recent Record	CALL COUNT	M	3 bytes
---		…	…
Rec N	. . .	M	3 bytes

- File shall be initialised '00 00 00'
- Minimum file size is 2 records

H.1.8 EF_{PSID} (Positive/Favoured SID list)

This file contains a list of Favoured SIDs for use in identifying Favoured service providers while performing network selection (intelligent roaming).

Identifier: '4F85'	Structure: transparent	Optional
File size: 2*N bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1 – 2	Favoured SID 1	M	2 bytes
…	Favoured SID 2	O	…
(2N-1) – (2N)	Favoured SID N	O	2 bytes

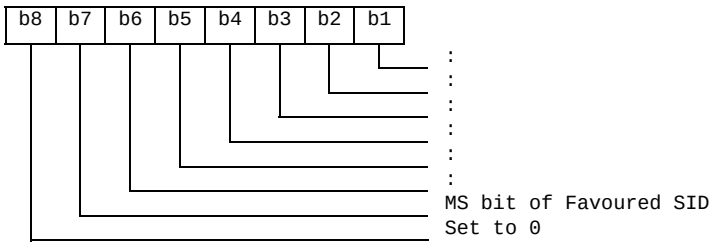
EOF (End of File) is indicated by 'FFFF'. An entry with all zeros is considered filler.

The most significant bit of the Favoured SID field is not used and it is set to 0.

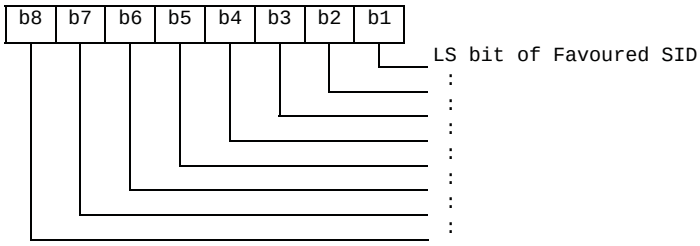
Coding of the Favoured SID field (2-byte coding)

The default value in the first two bytes shall be 'FFFF'.

Byte 1:



Byte 2:



H.1.9 EF_{NSID} (Negative/Forbidden SID List)

This file contains a list of Forbidden SIDs, for use in identifying Forbidden service providers while performing network selection (intelligent roaming).

Identifier: '4F84'	Structure: transparent	Optional
File size: 2*N bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1 – 2	Forbidden SID 1	M	2 bytes
…	Forbidden SID 2	O	…
(2N-1) – (2N)	Forbidden SID N	O	2 bytes

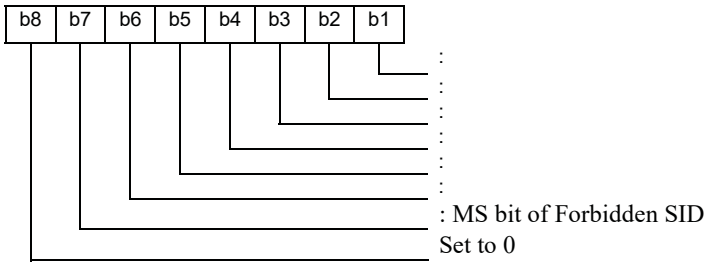
EOF (End of File) is indicated by 'FFFF.' An entry with all zeros is considered filler.

The most significant bit of the Forbidden SID field is not used and it is set to 0.

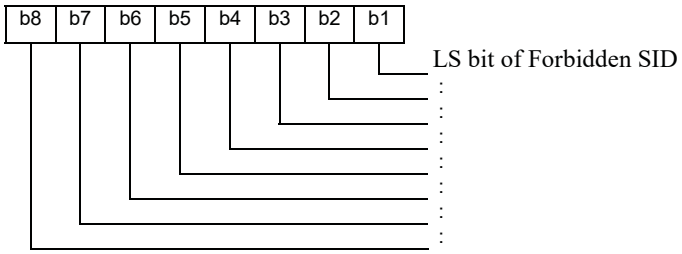
Coding of the Forbidden SID field (2-byte coding)

The default value in the first two bytes shall be 'FFFF'.

Byte 1:



Byte 2:



H.1.10 EF_{SPL} (Scanning Priority List)

This file contains the Scanning Priority List. The Scanning Priority List is an array that defines the various types of systems that can be found. It also acts as a reference table, pointing to the various data structures in the SIM. This file is for backwards compatibility with GSM/AMPS mobile equipment. A Mobile Station supporting both TIA/EIA-136 and EIA/TIA-553 [41] is not expected to support this EF for network selection.

Identifier: '4F87'	Structure: transparent	Optional
File size: 27 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1	Value 1	M	1 byte
2 – 3	Pointer 1	M	2 bytes
…			
…			
25	Value 9	M	1 byte
26 – 27	Pointer 9	M	2 bytes

- The position of the pointers is fixed in this file. Highest priority level is 1, lowest priority level is 7. No two entries can have the same priority level with the exception the last two fields (Forbidden PLMNs and Negative SIDs) which both will have a value of 0. Default values are in parentheses. The values 1 or 2 shall reside in the first position (Home PLMN), and the second position (Last registered PLMN) shall contain a higher priority than position 3 (Preferred PLMNs List) and 4 (Any Other PLMNs).

  Format:

Priority Value	Pointer	Reserved For
1 – 7 (2)	SIM ('6F07')	Home PLMN
1 – 7 (1)	SIM ('6F7E')	Last Registered PLMN
1 – 7 (3)	SIM ('6F30')	Preferred PLMNs List
1 – 7 (6)	0	Any Other PLMNs
1 – 7 (4)	SIM ('4F80')	Home SID
1 – 7 (5)	SIM ('4F85')	Positive SIDs List
1 – 7 (7)	0	Any Other SIDs
0	SIM ('6F7B')	Forbidden PLMNs List
0	SIM ('4F84')	Negative SIDs List

Constraints on the Priority List:

Mandatory PLMN priority order (highest to lowest):

Home PLMN or Last Registered PLMN, Preferred PLMNs, Any Other PLMNs

Mandatory SID priority order (highest to lowest):

Home SID, Positive SIs, Any Other SIDs.

H.1.11 EF_{NETSEL} (Network Selection Activation Flag)

This file contains the Network Selection Activation Flag. This flag is used to enable/disable the Manual Mode and some MMI functionality within the ME.

Identifier: '4F86'	Structure: transparent	Mandatory
File size: 1 byte	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1	Network Selection Activation Flag	M	1 byte

Enables / disables Manual Mode and some MMI functionality within the ME, in both AMPS and GSM modes.

Default value = 05 Hex.

Coding:

Bit 0 =0 GSM Manual Mode disabled

=1 GSM Manual Mode enabled (default)

Bit 1 =0 AMPS Manual Mode disabled (default)

=1 AMPS Manual Mode enabled

Bit 2 =0 Scanning Sequence Flags disabled

=1 Scanning Sequence Flags enabled (default)

Bit 3 =0 Disallow home only AMPS selection (default)

=1 Allow home only AMPS selection

Bits 4 through 7 are not used and set to zero.

H.1.12 EF_{CSID} (Current/Last Registered SID)

This file contains the SIDsp value. The most significant bit is unused and set to 0.

Identifier: '4F8C'	Structure: transparent	Optional
File size: 2 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1 -2	SIDsp	M	2 bytes

The default value shall be 'FFFF'.

H.1.13 $EF_{REG-THRESH}$ (Registration Threshold)

This file contains the NXTREGsp value, specified in EIA/TIA-553 [41]. The three most significant bits are unused and are set to 0.

Identifier: '4F8D'	Structure: transparent	Optional
File size: 3 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1 – 3	NXTREGsp value	M	3 bytes

- (Default value = '00 00 00')

H.1.14 EF_{CCCH} (Current Control Channel)

This file contains the Current Control Channel information related to the Last Paging Control Channel on which the AMPS phone camped on.

Identifier: '4F8E'	Structure: transparent	Optional
File size: 2 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1 – 2	Current Control Channel	M	2 bytes

- (Default value = '0000')

H.1.15 EF_{LDCC} (Latest DCC)

This file contains the DCC value associated with the saved Current Control Channel.

Identifier: '4F8F'	Structure: transparent	Optional
File size: 1 byte	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1	DCC (Default value = '00')	M	1 byte

H.1.16 $EF_{GSM\text{-}RECON}$ (GSM Reconnect Timer)

This file specifies, in seconds, the time the ME should remain scanning the GSM-1900 spectrum, after loss of service from a GSM-1900 system, before any scanning of the AMPS spectrum is allowed.

Identifier: '4F90'	Structure: transparent	Optional
File size: 2 bytes	Update Activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1-2	GSM Reconnect Timer (Default value = '00 3C' = 60 seconds)	M	2 bytes

H.1.17 $EF_{AMPS\text{-}2\text{-}GSM}$ (AMPS to GSM Rescan Timing Table)

The EF specifies, in minutes, a series of (typically increasing) intervals for scanning the GSM-1900 spectrum, used while in-service on an AMPS network while in Dual-Mode operation. The time is measured from the end of the last GSM-1900 scan to the start of the next GSM-1900 scan. If the table is not completely filled (i.e. the end-of-table value 'FF' is found), the last filled value may be repeated indefinitely. If a value of 'F0' is encountered, the table is terminated, as are all rescans to GSM until the current AMPS system is lost.

Identifier: '4F91'	Structure: transparent	Optional
File size: 10 bytes	Update Activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	First Rescan Attempt Interval (Default = '02')	M	1 byte
2	Second Rescan Attempt Interval (Default = '03')	M	1 byte
3	Third Rescan Attempt Interval (Default = '04')	M	1 byte
4	Fourth Rescan Attempt Interval (Default = '05')	M	1 byte
5	Fifth Rescan Attempt Interval (Default = '06')	M	1 byte
6	Sixth Rescan Attempt Interval (Default = 'FF')	M	1 byte
7	Seventh Rescan Attempt Interval (Default = 'FF')	M	1 byte
8	Eighth Rescan Attempt Interval (Default = 'FF')	M	1 byte
9	Ninth Rescan Attempt Interval (Default = 'FF')	M	1 byte
10	Tenth Rescan Attempt Interval (Default = 'FF')	M	1 byte

H.1.18 EF_{*FC1} (Feature Activation Codes)

This file contains the feature code table as specified in EIA/TIA-553 [41].

Identifier: '4F8A'	Structure: transparent	Optional
File size: 2 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1-2	Default value 'B990'.	M	2 bytes

H.1.19 $EF_{AMPS-UI}$ (AMPS USAGE INDICATORS)

This file contains usage indicators for local control and extended address method.

Identifier: 4F93	File Type: Transparent	Optional
File size: 2 bytes (minimum)	Update Activity: Low	
Access Conditions:		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1	Number of Services (S)	M	1 byte
2	Services n°1 to n°8	M	1 byte

-Services:

Contents

Service n°1 : Local Control Indicator (see Note 1)

Service n°2 : Extended Address Method indicator – included in any access attempts (see Note 2)

Services n3°-n°8 : RFU

- Number of Services

Contents:

This byte refers to the number of services defined in the following byte.

Coding:

This byte is coded as BCD

Services

Contents:

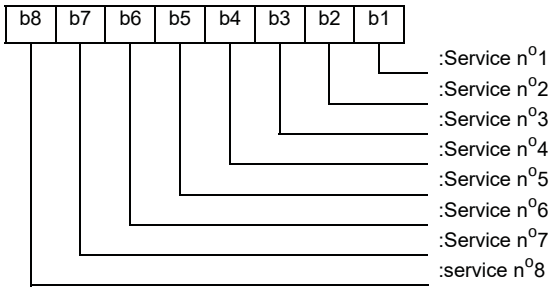
This byte describes the services

Coding:

- One bit is used to code each service
- If the bit = 0: service is not enabled
- If the bit = 1: service is enabled

- The bits for services not yet defined shall be set to RFU. For coding of RFU see clause 9.3.

Byte 2:



NOTE 1: The Local Control Indicator is a means provided within the mobile station to enable or disable the local control option. Local Control is a mechanism that allows a cellular system to customise operation for home mobile stations, and for those roaming mobile stations whose home systems are members of a group, by sending local orders with the order field set to local control (which informs the mobile station to examine the local control field), and by sending one or both of two local control global action overhead messages.

A group of systems could be formed by participating systems agreeing to a common set of local control protocols and whose system identifications (SID) are recognised by mobile stations as a common group.

NOTE 2: The Extended Address Method indicator determines if the extended address word must be included in all access attempts.

H.2 Authentication Functionality

H.2.1 A-KEY (ANSI-41 Authentication Key)

The A-Key is only accessible to the algorithm used for Key generation. The A-Key may be programmed into the SIM directly by the service provider, or it may be programmed into the SIM through a specific over the air procedure. The A-Key is not accessible by the mobile equipment, therefore the method of storage on the SIM is not specified in the present document. The SIM command A-KEY_VALIDATION is used to store the A-Key on the SIM.

H.2.2 SSD (Shared Secret Data)

The Shared Secret Data is accessible only to the Authentication and the Key Generation functions. SSD is not accessible by the mobile equipment, therefore the method of storage on the SIM is not specified in the present document.

An additional Status Code is defined for SSD updating as follows:

98, 34 Error, Update SSD order sequence not respected (should be used if SSD Update commands are received out of sequence).

H.3 Authentication commands

It is necessary to provide six interfaces to the CAVE Algorithm and Secret Data areas, as listed below:

- Generation of Authentication Signature data, and generation of ciphering keys.
- Validation and storage of entered A-Key's
- Ask Random task (generates RANDBS)

- Update Shared Secret Data (Generates SSD_A_NEW, SSD_B_NEW and AUTHBS values)
- Confirm Shared Secret Data (Updates SSD values)
- CMEA Encryption of voice channel data digits

NOTE: For each task, the expected normal (i.e. success) status code is listed in the status word description. A list of possible error codes that apply to all tasks can be found in the SIM Status Codes.

The interpretation of these instruction codes (INS in the table below) is valid only for class A0.

Task Name	CLA	INS	P1	P2	Lc
Internal_Authenticate	'A0'	'88'	'00'	'00'	'0F'
AKEY_validation	'A0'	'86'	'00'	'00'	'12'
Ask_Random	'A0'	'8A'	'00'	'00'	'04'
Update_SSD	'A0'	'84'	'00'	'00'	'0C'
Confirm_SSD	'A0'	'82'	'00'	'00'	'03'
CMEA_encrypt	'A0'	'8C'	'00'	'00'	'nn'

H.3.1 Generation of Authentication Signature Data and Ciphering Keys

This task produces an Authentication response, and shall be used during mobile Registrations, Originations, Terminations, R_Data messages, SPACH Confirmations, and for the Unique Challenge-Response Procedure. If Byte 0, Bit 1 is set, the SIM should also generate key bits after completing the Authentication function. Some of those ciphering octets may be passed back to the ME for use with supplementary crypto mechanisms which reside in the ME. This task requires the following input parameters:

Task Name	CLA	INS	P1	P2	Lc
Internal_Authenticate	'A0'	'88'	'00'	'00'	'0F'

Coding::

Byte 0 Process Control Byte

Bit 0 0=RANDs, 1= RANDU

Bit 1 Generate Key Bits flag (0= No, 1= Yes)

Bit 2 Load Internal key flag:

(0= pass all generated key bytes to handset, 1= load first 8 bytes of generated keys internally to SIM, pass all remaining key bytes to ME)

Bits 3-7 Unused, future expansion

Bytes 1-4 RANDs (for Registrations, Originations, and Terminations)

or

Bytes 1-3 RANDU (for Unique Challenge-Response Procedures)
Byte 4 = 0 (MIN2 will be filled in by SIM)

Byte 5 Digits Length (in bits, =0, 4, 8, 12, 16, 20 or 24,

= 4 x number of digits in bytes 6-8)

Bytes 6-8 =0,0,0 (for Registrations, Terminations, Unique Challenge Response Procedures)

= Last Dialed Digits, unused bits filled with 0's (for Originations). If more than 6 digits are dialed, these are the last 6 digits in the origination string. If less than 6 digits are dialed, MIN1 will be filled in by the SIM for the unused bits.

Byte 9 Use ME ESN (='00')

Bytes 10-13 ESN

Byte 14 Key_size (=0 if Byte 0, Bit 1= 0, =8 (or more) if Byte 0, Bit 1 = 1)

The output of this task shall be:

Status Bytes: SW1 (='9F' if success)

SW2 (='nn' if success)

('nn' is 03+Key_size if Byte 0, Bit 2 above =0, 03+Key_size-08 if Byte 0, Bit 2 above =1)

H.3.2 Validation and Storage of Entered A-Key's

With manual entry of the A-key, the input A-Key must be validated prior to its storage in the SIM. If successful, the A-key is saved in the SIM and the COUNTsp and Shared Secret Data (SSD) are reset to zero. This task requires the following input parameters:

Task Name	CLA	INS	P1	P2	Lc
AKEY_validation	'A0'	'86'	'00'	'00'	'12'

Coding:

Bytes 0 - 12

Authentication digits string (first digit in Most-Significant nibble of byte 0, last digit in Least-Significant nibble of Byte 12, for a total of 26 digits)

Byte 13 Use ME ESN (='00')

Bytes 14-17 ESN

The output of this task shall be:

Status Bytes: SW1 (='90' if success)

SW2 (='00' if success)

H.3.3 Ask Random Task

This task is used to generate the RANDBS random value. This task must be executed prior to updating the Shared Secret Data (SSD). The value RANDSeed must be generated by the ME prior to calling this task. This task requires the following input parameters:

Task Name	CLA	INS	P1	P2	Lc
Ask_Random	'A0'	'8A'	'00'	'00'	'04'

Coding:

Bytes 0-3 RANDSeed

The output of this task shall be:

Status Bytes: SW1 (='9F' if success)

SW2 (='04' if success)

H.3.4 Update Shared Secret Data

This task is used to generate the preliminary new Shared Secret Data (SSD_A_NEW, SSD_B_NEW) and the AUTHBS value. The Ask Random Task (see above) must be executed prior to this routine. The task requires the following input parameters:

Task Name	CLA	INS	P1	P2	Lc
Update_SSD	'A0'	'84'	'00'	'00'	'0C'

Coding:

Bytes 0-6 RANDSSD

Byte 7 Use ME ESN (='00')

Bytes 8-11 ESN

The output of this task shall be:

Status Bytes: SW1 (='90' if success, ='98' if failure)

SW2 (='00' if success, ='04' if failure)

H.3.5 Confirm Shared Secret Data

This task is used to validate the new Shared Secret Data (SSD_A_NEW, SSD_B_NEW) by comparing the internally computed AUTHBS with the AUTHBSs received from the system. If successful, the SSD_A and SSD_B values will be updated to match the SSD_A_NEW and SSD_B_NEW values, respectively The task requires the following input parameters:

Task Name	CLA	INS	P1	P2	Lc
Confirm_SSD	'A0'	'82'	'00'	'00'	'03'

Coding:

Bytes 0-2 AUTHBSs

The output of this task shall be:

Status Bytes: SW1 (='90' if success)

SW2 (='00' if success)

H.3.6 CMEA Encryption of Voice Channel Data Digits

This task is used when the MS is on a Voice Channel, to encrypt and decrypt some portions of digital messages transmitted to the BS. These will occur for the following messages:

- Called Address Message (in response to a hookflash, up to 4 bytes per word, 4 words, total of 16 bytes)

Task Name	CLA	INS	P1	P2	Lc
CMEA_encrypt	'A0'	'8C'	'00'	'00'	'nn'

where 'nn' is hex value of data length n

Coding:

Bytes 0 - (n-1) The n-byte data to be encoded, max. size = 32 bytes.

The output of this task shall be:

Status Bytes: SW1 (='9F' if success)

SW2 (='nn' if success) ('nn' is hex value of data length n)

H.3.7 SIM Status Codes

The following status codes, returned by the SIM in response to the execution of any of the tasks specified in the present document, are valid. The first hex value is returned in SW1, the second hex value in SW2.

Success Codes:

90, 00	Generic success code
9F, xx	Success, xx bytes of data available to be read via "Get_Response" task.

Error Codes:

92, 40	Error, memory problem
94, 08	Error, file is inconsistent with the command
98, 04	Error, no CHV1 has been presented successfully
98, 34	Error, Update SSD order sequence not respected (should be used if SSD Update commands are received out of sequence).
67, xx	Error, incorrect parameter P3 (ISO code)
6B, xx	Error, incorrect parameter P1 or P2 (ISO code)
6D, xx	Error, unknown instruction code given in the command (ISO code)
6E, xx	Error, wrong instruction class given in the command (ISO code)
6F, xx	Error, technical problem with no diagnostic given (ISO code)
6F, 00	Error, invalid input parameters to authentication computation

Annex I (informative): EF changes via Data Download or SIM Toolkit applications

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS), or by SIM Toolkit Application (e.g. by using the SIM API), is advisable. Updating of certain EFs, "over the air" such as EF_{ACC} could result in unpredictable behaviour of the MS; these are marked "Caution" in the table below. Certain EFs are marked "No"; under no circumstances should "over the air" changes of these EFs be considered.

File identification	Description	Change advised
'2F05'	Extended Language preference	Yes
'2FE2'	ICC identification	No
'4F20'	Image data	Yes
'4Fxx'	Image Instance data Files	Yes
'6F05'	Language preference	Yes
'6F07'	IMSI	Caution (note)
'6F20'	Ciphering key Kc	No
'6F2C'	De-personalization Control Keys	Caution
'6F30'	PLMN selector	Caution
'6F31'	Higher Priority PLMN search period	Caution
'6F32'	Co-operative network	Caution
'6F37'	ACM maximum value	Yes
'6F38'	SIM service table	Caution
'6F39'	Accumulated call meter	Yes
'6F3A'	Abbreviated dialling numbers	Yes
'6F3B'	Fixed dialling numbers	Yes
'6F3C'	Short messages	Yes
'6F3D'	Capability configuration parameters	Yes
'6F3E'	Group identifier level 1	Yes
'6F3F'	Group identifier level 2	Yes
'6F40'	MSISDN storage	Yes
'6F41'	PUCT	Yes
'6F42'	SMS parameters	Yes
'6F43'	SMS status	Yes
'6F44'	Last number dialled	Yes
'6F45'	CBMI	Caution
'6F46'	Service provider name	Yes
'6F47'	Short message status reports	Yes
'6F48'	CBMID	Yes
'6F49'	Service Dialling Numbers	Yes
'6F4A'	Extension 1	Yes
'6F4B'	Extension 2	Yes
'6F4C'	Extension 3	Yes
'6F4D'	Barred dialling numbers	Yes
'6F4E'	Extension 4	Yes
"6F4F"	Extended Capability configuration parameters	Yes
'6F50'	CBMIR	Yes
'6F51'	Network's indication of alerting	Caution
'6F52'	GPRS Ciphering key KcGPRS	No
'6F53'	GPRS Location Information	Caution
'6F58'	Comparison method information	
'6F60'	User controlled PLMN Selector with Access Technology	see 3GPP TS 22.011
'6F61'	Operator controlled PLMN Selector with Access Technology	Caution
'6F62'	HPLMN Selector with Access Technology	Caution
'6F63'	CPBCCH information	No
'6F64'	Investigation scan	Caution
'6F74'	BCCH information	No
'6F78'	Access control class	Caution
'6F7B'	Forbidden PLMNs	Caution
'6F7E'	Location information	No (note)
	Continued.....	

File identification	Description	Change advised
'6FAD'	Administrative data	Caution
'6FAE'	Phase identification	Caution
'6FB1'	Voice Group Call Service	Yes
'6FB2'	Voice Group Call Service Status	Yes
'6FB3'	Voice Broadcast Service	Yes
'6FB4'	Voice Broadcast Service Status	Yes
'6FB5'	Enhanced Multi Level Pre-emption and Priority	Yes
'6FB6'	Automatic Answer for eMLPP Service	Yes
'6FB7'	Emergency Call Codes	Caution
'6FC5'	PLMN Network Name	Yes
'6FC6'	Operator PLMN List	Yes
'6FC7'	Mailbox Dialling Numbers	Yes
'6FC8'	Extension 6	Yes
'6FC9'	Mailbox Identifier	Caution
'6FCA'	Message Waiting Indication Status	Caution
'6FCB'	Call Forwarding Indication Status	Caution
'6FCC'	Extension 7	Yes
'6FCD'	Service Provider Display Information	Yes
"6FCE"	MMS Notification	Yes
"6FCF"	Extension 8	Yes
"6FD0"	MMS Issuer Connectivity Parameters	Yes
"6FD1"	MMS User Preferences	Yes
"6FD2"	MMS User Connectivity Parameters	Yes
NOTE: If EF_{IMSI} is changed, the SIM should issue REFRESH as defined in TS 51.014 [27] and update EF_{LOCI} accordingly.		

Annex J (informative): Tags defined in the present document

Tag	Name of Data Element	Usage
'A3'	Service provider display information The following tags are encapsulated within 'A3': '80' Service provider PLMN list	Service Provider Display Information (EF_{SPDI})
"AB"	MMS Connectivity Parameters: The following are encapsulated under "AB": "80" MMS Implementation Tag "81" MMS Relay/Server Tag "82" Interface to core network and bearer Tag "83" Gateway Tag	MMS Connectivity Parameters (EF_{MMSICP} and EF_{MMSUCP})

NOTE: the value 'FF' is an invalid tag value. For ASN.1 tag assignment rules see ISO/IEC 8825 [56]

Annex K (informative): Example of MMS coding

This annex gives an example for the coding of MMS User Preferences, while the MMS User Information Preference parameters are coded according to the WAP implementation of MMS.

K.1 Coding example for MMS User Preferences

0x80 MMS Implementation Tag

0x01 (Length = "1")

0x01 (MMS implementation information = "WAP")

0x81 MMS User Preference Profile Name Tag

0x0E (Length = "14")

43 68 72 69 73 74 6D 61 73 20 43 61 72 64

(profile name = "Christmas Card"; 14 characters, 14 Bytes)

0x82 MMS User Information Preference Information Tag

0x19 (Length = "25")

0x14 0x80 (visibility: = "hide"; 2 Bytes)

0x06 0x80 (delivery report: = "yes"; 2 Bytes)

0x10 0x80 (read-reply: = "yes"; 2 Bytes)

0x0F 0x81 (priority: = "normal"; 2 Bytes)

0x07 0x07 0x80 0x05 0x11 0x22 0x33 0x44 0x55
(Delivery-Time-Tag, Value-Length, Absolute-Token-Tag, Date-Value-Length, Date-Value; 9 Bytes)

0x08 0x06 0x81 0x04 0x55 0x22 0x33 0x44
(Expiry Tag, Value-Length, Relative-Token-Tag, Delta-Second-Value-Length, Delta-Second-Value; 8 Bytes)

K.2 Coding Example for MMS Issuer/User Connectivity Parameters

0xAB MMS Connectivity Parameters Tag

0x9F (Length = "159")

0x80 MMS Implementation Tag

0x01 (Length = "1")

0x01 (MMS implementation information = "WAP"; 1 Byte)

0x81 MMS Relay/Server Tag

0x17 (Length = "23")

0x68 0x74 0x74 0x70 0x3A 0x2F 0x2F 0x6D 0x6D 0x73 0x2D 0x6F 0x70 0x65 0x72 0x61 0x74 0x6F 0x72 0x2E 0x63 0x6F 0x6D
(MMS Relay/Server information = "http://mms-operator.com"; 23 characters; 23 Bytes)

0x82 Interface to Core Network and Bearer Tag

0x32 (Length = "50")

0x10 0xAA (bearer = "GSM-CSD"; 2 Bytes)

0x08 0x2B 0x34 0x39 0x35 0x33 0x34 0x31 0x39 0x30 0x36 0x00
(address = "+495341906", 12 Bytes)

0x09 0x87 (type of address = "E164"; 2 Bytes)

0x25 0xC5 (speed = "autobauding"; 2 Bytes)

0x0A 0x90 (call type = "ANALOG_MODEM"; 2 Bytes)

0x0C 0x9A (authentication type = "PAP"; 2 Bytes)

0x0D 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x6E 0x61 0x6D 0x65 0x00
(authentication id = "dummy_name"; 12 Bytes)

0x0E 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x70 0x61 0x73 0x73 0x77 0x6F 0x72 0x64 0x00
(authentication pw = "dummy_password"; 16 Bytes)

0x83 Gateway Tag

0x36 (Length = "54")

0x20 0x31 0x37 0x30 0x2E 0x31 0x38 0x37 0x2E 0x35 0x31 0x2E 0x33 0x00
(address = "170.187.51.3"; 14 Bytes)

0x21 0x85 (type of address = "IPv4"; 2 Bytes)

0x23 0x39 0x32 0x30 0x33 0x00 (port = "9203"; 6 Bytes)

0x24 0xCB (service = "CO-WSP"; 2 Bytes)

0x19 0x9C (authentication type = "HTTP BASIC"; 2 Bytes)

0x1A 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x6E 0x61 0x6D 0x65 0x00
(authentication id = "dummy_name"; 12 Bytes)

0x1B 0x64 0x75 0x6D 0x6D 0x79 0x5F 0x70 0x61 0x73 0x73 0x77 0x6F 0x72 0x64 0x00
(authentication pw = "dummy_password"; 16 Bytes)

Annex L (informative): Change history

This annex lists all change requests approved for the present document since the first phase2+ version was approved by ETSI SMG.

Meeting	Plenary tdoc	WG tdoc	VERS	CR	RV	Release	CAT	SUBJECT	Resulting Version
s16	709/95	154/95	4.15.0	A008		R96	1	SIM Speed Enhancement	5.0.0
s17	062/96	147/95	5.0.0	A006		R96	B	Service Dialling Numbers	5.1.0
	060/96	06/96		A009		R96	B	ASCI for VGCS and VBS	
	060/96	06/96		A010		R96	B	ASCI for eMLPP	
	059/96	204/95r		A013		R96	C	Interaction between FDNs and ADNs	
	061/96	05/96		A014		R96	D	Correction of baud rate for SIM Speed enhancement	
s18	263/96	57/96	5.1.0	A011	3	R96	B	SIM Application Toolkit protocol enhancements	5.2.0
	260/96	45/96		A016		R96	A	SIM presence detection clarification	
	261/96	54/96		A018		R96	A	Reponse codes and coding of SIM service table	
	262/96	55/96		A020		R96	A	Reference to International Standards	
s19	374/96	102/96	5.2.0	A012		R96	C	Contacting elements	5.3.0
	373/96	105/96		A023		R96	A	Clarification of clock stop timing	
	409/96	107/96		A024	1	R96	B	Emergency Call Codes (ECC)	
	374/96	108/96		A025		R96	C	Using ranges of CBMIs	
s20	580/96	206/96	5.3.0	A021		R96	B	Barred Dialling Numbers	5.4.0
	734/96	197/96		A026		R96	B	Addition of Cooperative Network List EF	
	734/96	197/96		A027		R96	B	Addition of ME Depersonalisation feature and EF	
	702/96	207/96		A031		R96	D	RFU bit taken into use in GSM 11.12	
s21	101/97	97/079	5.4.0	A032	2	R96	D	Ammendment to BDN diagrams in Annex B	5.5.0
	101/97	97/086		A033	1	R96	B	DFs for MSS/ PCS1900/other use	
	101/97	97/056		A034		R96	C	Reading of EF_DCK during SIM initialisation	
	101/97	97/058		A036		R96	D	Administrative Access Conditions	
	101/97	97/059		A037		R96	B	Format of EF_CNL to include fields for Corporate Personal.	
	101/97	97/089		A041		R96	B	Administrative Data field	
s22	356/97	183/97	5.5.0	A042		R97	B	Extended language preference	5.6.0
	356/97	163/97		A044	1	R96	A	Clarification of electrical/mechanical SIM/ME interface	
	356/97	179/97		A045		R96	D	Security procedures for 2nd level; DFs located under DF_GSM	
	356/97	187/97		A047		R96	F	Number of bytes returned after a SELECT command	
	356/97	093/97		A048		R96	D	Serivce table and "radio interface"	
	356/97	109/97		A049		R96	F	Update Access condition of EF_DCK (aligns 11.11 & 02.22)	
s23	788/97	97/249	5.6.0	A046	2	R97	B	Short Message Status Reports	5.7.0
	788/97	97/243		A050		R96	F	Addition of SDN and BDN in the description of EFCCP	
	788/97	97/259		A051	1	R97	C	SIM and ME behaviour when SIM is disabled and blocked	
	788/97	97/262		A053		R96	F	Response data following an ENVELOPE command	
	788/97	97/260		A054		R96	F	Coding of EFPhase	
	788/97	97/271		A055		R97	C	Changes to Dialling Number Files and extensions	
	788/97	97/261		A056		R97	B	Network's indication of alerting in the MS	
s24	97-0886	97/365	5.7.0	A052	2	R97	b	Introduction of UCS2	5.8.0
	97-0886	97/383		A057		R97	c	MO SMS control by SIM	
At SMG #25, it was decided to create a version 6.0.0 of every specification that contained at least one release '97 work item and a version 7.0.0 of every specification that contained at least one release '98 work item.									
s25	98-0157	98p052	5.8.0	A058	2	R97	B	Addition of EFs for GPRS	6.0.0
	98-0157	98p108		A059		R97	F	Clarification regarding EF_CCP records	
	98-0157	98p094		A061	1	R96	A	Clarification of removal of the SIM	
s26	98-0398	98p228	6.0.0	A062	2	R98	B	Icons - addition of EF_IMG and DF_GRAPHICS	7.0.0
	98-0398	98p227		A064		R98	B	Operation of ME with multiple card readers	
	98-0400	98p237		A065		R98	F	Deletion of all release 97 markers from the R98 version	
	98-0398	98p240		A066		R97	F	RP-ACK RP-ERROR for SIM data download error	
	98-0398	98p263		A069		R97	D	Allocation of file ID for IS-41	

(continued)

Change History (continued)

Meeting	Plenary tdoc	WG tdoc	VERS	CR	RV	Release	CAT	SUBJECT	Resulting Version
s27	98-0671	98p339	7.0.0	A071		R98	C	Enhanced image coding schemes (colour icons)	7.1.0
	98-0671			A072	1	R98	D	Addition of reference to PCS 1900	
s28	P-99-185	9-99-076	7.1.0	A073	1	R98	F	Alignment with 2nd edition of ISO/IEC 7816-3 (1997)	7.2.0
	P-99-185	9-99-037		A074		R98	B	Addition of SoLSA data fields	
	P-99-185	9-99-066		A075	1	R98	B	Addition of CTS fields	
	P-99-185	9-99-095		A076	1	R98	B	Definition of a file containing the title of the main menu	
	P-99-185	9-99-072		A077		R98	C	USSD format indication in the SIM Service Table	
	P-99-185	0-99-093		A078		R98	B	Informative annex on EF changes	
	P-99-185	9-99-097		A080		R98	C	Additional GPRS field	
	P-99-188			A082		R98	D	Deletion of $(.....)$ release markers	
s29	P-99-412	9-99-163	7.2.0	A083	1	R98	C	EF_IMSI changes via data download or SIM toolkit	8.0.0
	P-99-412	9-99-180		A084		R98	F	Addition of RUN AT COMMAND to the SIM service table	
	P-99-412	9-99-208		A085		R99	C	Alignment of maximum of records in a linear fixed file in GSM	
s30	P-99-670	9-99-260	8.0.0	A089		R99	A	Correction for coding of SoLSA "Priority" field	8.1.0
	P-99-670	9-99-277		A090		R99	D	Clarification of the Ciphering Indicator disable bit in the EFad	
	P-99-670	9-99-281		A091		R99	F	Introduction of a new DF for the TIA/EIA-136 technology	
	P-99-670	9-99-294		A092	1	R99	B	Addition of EF definitions under the PCS 1900 DF	
	P-99-670	9-99-310		A093		R99	F	Clarification about "Memory Problem" error for EF_{LOCI} update	
	P-99-670	9-99-300		A094		R99	F	Execution time of SIM toolkit procedures	
	P-99-670	9-99-311		A095		R99	B	Introduction of a new DF for the TIA/EIA-95 technology	
	P-99-670	9-99-258		A097		R99	A	Clarification of Optional Status for GPRS files	
s31	P-00-137	9-00-0088	8.1.0	A098		R99	F	Clarification of interactions for CBS and the language files on	8.2.0
	P-00-137	9-00-0092		A101		R99	F	Correction to coding of ASCI EF eMLPP.	
	P-00-137	9-00-0095		A104		R99	F	Addition of coding for ASCI Efs (VGCS and VBS)	
	P-00-137	9-00-0098		A107		R99	F	Correction of the byte numbering related to EF LOCIGPRS	
	P-00-137	9-00-0133		A108		R99	F	Corrections and additions to DF-5F40	
	P-00-137	9-00-0146		A109	1	R99	F	Clarification of manual entry of the A-Key.	
	P-00-137	9-00-0151		A110		R99	D	Addition of reference to the File ID as used in the TETRA	
	P-00-137	9-00-0163		A111	1	R99	B	COMPACT Cell Selection	
	P-00-137	9-00-0155		A112		R99	B	COMPACT Cell Selection - Investigation Scan indicator for	
	P-00-139	9-00-0161		A113		R99	B	Enhancement to CCP coding (CR number incorrect in P-00-	
	P-00-139	9-00-0159		A114		R99	B	Enhancement of BDN feature (CR number incorrect in P-00-	
s32	P-00-296	9-00-0232	8.2.0	A120		R99	B	DFs for MexE	8.3.0
	P-00-296	9-00-0276		A122		R99	C	HPLM length	
	P-00-296	9-00-0275		A123		R99	A	LAI, RAI and CNL: alignment with GSM 04.08	
	P-00-296	9-00-0273		A124		R99	F	PLMN Selection Corrections regarding RFU bits	
	Following the closure of ETSI SMG and the agreement of the 3GPP in July 2000 to undertake responsibility for remaining GSM specifications, the change requests listed below were approved by 3GPP TSG-T. This change in responsibility also changed the specification number from "GSM 11.11" to "3GPP TS 11.11".								
TP-09	TP-000176	9-00-0253	8.3.0	A116		R99	F	PLMN Selection Corrections and additions for EDGE	8.4.0
	TP-000176	9-00-0269		A119		R99	C	Addition of RPLMN file	
	TP-000148	T3-000479		A126		R99	F	Standardise the current GAIT commands and reserving	
TP-11	TP-010038	T3-010047	8.4.0	A127		R99	F	Addition of file ID for indicating iDEN access technology	8.5.0
	TP-010038	T3-010045		A128		R99	F	Correction to default HPLMN RAT	
	At TSG-T #11, it was agreed that all existing release 99 specifications should be reissued as release 4 specifications so as to create a complete set of release 4 specifications. Further more, it was agreed to change the specification number of all GSM-only specifications from AA.BB to (AA+40).0BB. Thus GSM 11.11 changed to 3GPP TS 51.011. At the same time, the version numbering scheme was harmonised with 3G specifications so that all release 4 specifications have a version number 4.x.y. The contents of TS 51.011 v4.0.0 are identical to GSM 11.11 v8.5.0								4.0.0
TP-12	TP-010109	T3-010373	4.0.0	002		Rel-4	F	Introduction of selected USIM features in to the SIM	4.1.0
TP-13	TP-010203	T3-010583	4.1.0	003		Rel-4	F	EF_EXT1: Clarification of Length Indicator for Additional	4.2.0
TP-14	TP-010244	T3-010744	4.2.0	004		Rel-4	F	Collection of corrections	4.3.0
	TP-010244	T3-010747		005		Rel-4	F	Alignment of SPN feature between 2G and 3G	
	TP-010244	T3-010773		006		Rel-4	D	Restructuring of TS 51.011 to be based on TS 102 221	
	TP-010244	T3-010797		008		Rel-4	F	Correction to EF_OPL	
TP-16	TP-020121	T3-020338	4.3.0	009		Rel-4	F	The EF_CNL and EF_DCK are missed in the Figure "Files identifiers and directory structures of GSM"	4.4.0
	TP-020167			010		Rel-4	F	The identifier of EF_RPLMNAcT (RPLMN Last used Access Technology) is inconsistent within the specification	
TP-17	TP-020218	T3-020717	4.4.0	013		Rel-4	A	Inconsistent record length of EF_IMG	4.5.0

		T3-020640		011		Rel-4	F	Incomplete EF_ICCID description	
		T3-020670		012		Rel-4	F	Correction of references and clarification of Scope	
		T3-020719		014		Rel-4	F	Incomplete description of EF_ECCP	
		T3-020720rev1		015		Rel-4	B	Introduction of MMS files and procedures	
TP-18	TP-020278	T3-020918	4.5.0	016		Rel-4	A	Essential corrections of file size and record lengths in several EFs	4.6.0
								Editorial correction to the ranges in the file description as concluded at T3#25.	
TP-19	TP-030017	T3-030145	4.6.0	017		Rel-4	F	Correction of reference to GSM 11.14 (Rel-4 is TS 51.014)	4.7.0
		T3-030151		018		Rel-4	F	Example for MMS connectivity parameters	
TP-20	TP-030124	T3-030398	4.7.0	020		Rel-4	F	Correction of the MMS example	4.8.0
		T3-030402		022		Rel-4	F	Correction of inconsistencies within the document	
		T3-030412		023		Rel-4	F	Correction of pre-personalisation values	
		T3-030417		021		Rel-4	F	Essential correction on SIM/UICC interface compatibility	
TP-21	TP-030178	T3-030630	4.8.0	024		Rel-4	F	Correction on EF_VBSS Coding	4.9.0
		T3-030653		025		Rel-4	F	Correction to SMS	
	TP-030186	T3-030726		026		Rel-4	F	CR to delete Elementary File EFRPLMNAcT, in accordance with TP-020168 from T Plenary in Marco Island.	
TP-22	TP-030248	T3-030949		027	-	Rel-4	F	Correction to procedures for service no 21, 22 and 23	4.10.0
		TP-030305		028	1	Rel-4	A	Alignment of EF-HPLMN Search Period with 22.011 and 23.122	
		T3-031031		029	-	Rel-4	F	Removal of references to TS 02.07	
		T3-031032		030	-	Rel-4	F	Removal of references to TS 04.08	

History

Document history		
V4.0.0	July 2001	Publication
V4.1.0	September 2001	Publication
V4.2.0	September 2001	Publication
V4.3.0	December 2001	Publication
V4.4.0	June 2002	Publication
V4.5.0	September 2002	Publication
V4.6.0	December 2002	Publication
V4.7.0	April 2003	Publication
V4.8.0	June 2003	Publication
V4.9.0	September 2003	Publication
V4.10.0	December 2003	Publication

APPENDIX N

http://www.3gpp.org/ftp/Specs/html-info/23057.htm Go APR NOV JAN
38 captures 11
1 Jul 2003 – 10 Feb 2020 2006 2007 2014 About this capture

3GPP Specification detail

Back to numbering scheme page

Back to series index

3GPP TS 23.057 (click spec number to see fileserver directory for this spec)

Mobile Execution Environment (MExE); Functional description; Stage 2

.

TSG / WG responsible: S2 (click TSG/WG to see its home page)

Work item which gave rise to this spec: - (click WI code to see Work Item details in the Work Plan)

Apr-2001: "" Station Application"" removed from title. SP-27: Moved to current group on closure of T2; see TP-050062.

Rapporteur: **BRENK, Lars**

Specification required for: GERAN-based systems and UTRAN-based systems

In the table below ...

... click meeting number for meeting details;

... click spec version number to download that version;

... click SDO publication reference to download SDO transposed document.

Release	Freeze meeting	Freeze date	remarks	SDO publications
R99	SP-06	1999-12-17	-	ETSI
	event	version	available	remarks	click ref to download
	TP-03	1.0.0	1999-04-28		-
	TP-04 (MExE R98 GSM 03.57)	1.1.0	1999-06-18		-
	TP-05	1.5.0	1999-10-08		-
	TP-06 completed	3.0.0	1999-12-17		DTS/TSGT-0223057U
	TP-07	3.1.0	2000-03-15		-
	Editorial	3.1.1	2000-03-15		RTS/TSGT-0223057UR1
	TP-08	3.2.0	2000-06-23		RTS/TSGT-0223057UR2
	TP-09	3.3.0	2000-10-16		RTS/TSGT-0223057UR3
	TP-11	3.4.0	2003-10-14		RTS/TSGT-0223057UR4
Rel-4	SP-11	2001-03-22	-	ETSI
	event	version	available	remarks	click ref to download
	TP-10	4.0.0	2000-12-22		-
	TP-11	4.1.0	2001-04-11		RTS/TSGT-0223057Uv4
	TP-12	4.2.0	2001-07-05		RTS/TSGT-0223057Uv4R1
	TP-13	4.3.0	2001-10-05		-
	include fig 5	4.3.1	2001-10-18		RTS/TSGT-0223057Uv4R2
	TP-14	4.4.0	2002-01-16		RTS/TSGT-0223057Uv4R3
	TP-15	4.5.0	2002-03-25		RTS/TSGT-0223057Uv4R4
Rel-5	TP-15	2002-03-08	-	ETSI
	event	version	available	remarks	click ref to download
	TP-15	5.0.0	2002-03-25		RTS/TSGT-0223057Uv5
	TP-17	5.1.0	2002-09-18		RTS/TSGT-0223057v510
Rel-6	TP-26	2004-12-10	-	ETSI
	event	version	available	remarks	click ref to download
	TP-16	6.0.0	2002-06-28		-
	TP-17	6.1.0	2002-09-18		-
	TP-21	6.2.0	2003-10-14		RTS/TSGT-0223057v620
Rel-7	SP-36	2007-06-07	-	ETSI
	event	version	available	remarks	click ref to download
	SP-36	7.0.0	2007-06-19	Upgraded unchanged from Rel-6	RTS/TSGS-0223057v700

Change Requests for this spec: click here.

Genealogy of this spec:

antecedent(s)	this spec	descendant(s)
03.57	23.057	(no descendants)

page generated from database: 2007-11-05 13:07:20

APPENDIX O

www.3gpp.org / ftp / specs / archive / 31_series / 31.101

Download

	sort by name/desc	sort by date/desc	sort by size/desc
	31101-050.zip	1999/07/20 6:46	161,2 KB
	31101-100.zip	1999/10/20 15:49	213,7 KB
	31101-300.zip	2000/01/12 13:43	192,2 KB
	31101-310.zip	2000/04/20 8:42	247,2 KB
	31101-320.zip	2000/07/21 14:25	256,1 KB
	31101-330.zip	2000/10/18 12:18	27,6 KB
	31101-331.zip	2005/01/06 10:04	29,3 KB
	31101-400.zip	2001/04/09 7:37	27,8 KB
	31101-410.zip	2003/01/02 13:40	36 KB
	31101-420.zip	2005/01/02 18:34	29,5 KB
	31101-421.zip	2005/01/06 10:05	30 KB
	31101-500.zip	2002/09/18 7:53	28,1 KB
	31101-510.zip	2003/01/02 13:41	36,2 KB
	31101-520.zip	2005/01/02 18:34	29,7 KB
	31101-521.zip	2005/01/06 10:06	30 KB
	31101-600.zip	2002/09/18 7:54	28,4 KB
	31101-610.zip	2003/01/02 13:41	42 KB
	31101-620.zip	2003/06/23 15:11	34,5 KB
	31101-630.zip	2004/09/27 9:18	35,9 KB
	31101-640.zip	2005/01/02 18:34	36 KB
	31101-641.zip	2005/01/05 14:57	36,1 KB
	31101-650.zip	2005/06/14 17:09	36,4 KB
	31101-651.zip	2006/01/26 13:41	37,5 KB
	31101-700.zip	2007/06/02 23:39	44,9 KB
	31101-701.zip	2007/06/20 6:05	44,8 KB

31101-710.zip	2009/12/20 10:06	46 KB
31101-720.zip	2010/06/18 14:00	59,7 KB
31101-721.zip	2011/01/03 4:29	59,5 KB
31101-722.zip	2011/06/24 9:59	67,5 KB
31101-800.zip	2009/01/26 13:34	158,1 KB
31101-810.zip	2009/12/20 10:07	157,9 KB
31101-820.zip	2010/06/18 14:29	171,6 KB
31101-821.zip	2011/01/03 4:31	171,8 KB
31101-822.zip	2011/06/24 9:59	179,7 KB
31101-830.zip	2014/12/22 21:13	179,7 KB
31101-900.zip	2009/12/20 10:07	158,9 KB
31101-910.zip	2010/06/18 14:52	171,6 KB
31101-911.zip	2011/01/03 4:32	171,8 KB
31101-912.zip	2011/06/24 9:59	179,7 KB
31101-920.zip	2014/12/22 21:17	179,7 KB
31101-a00.zip	2011/03/31 21:27	464,5 KB
31101-a01.zip	2011/06/24 9:59	471,5 KB
31101-a10.zip	2014/12/22 21:22	473,8 KB
31101-b00.zip	2012/09/29 8:42	472,3 KB
31101-b10.zip	2014/12/22 21:25	472,7 KB
31101-b20.zip	2015/03/21 6:09	472,9 KB
31101-c00.zip	2014/10/03 13:18	472,7 KB
31101-c10.zip	2014/12/22 21:30	472,9 KB
31101-c20.zip	2015/06/26 4:33	473,2 KB
31101-d00.zip	2015/09/28 1:28	473,6 KB
31101-d10.zip	2016/01/08 16:26	101,3 KB
31101-d20.zip	2016/06/24 20:49	102 KB
31101-e00.zip	2017/01/16 7:14	102,5 KB
31101-e10.zip	2017/03/17 13:10	102,5 KB
31101-e20.zip	2017/12/30 1:20	102,8 KB
31101-f00.zip	2018/07/02 7:05	68 KB

31101-f10.zip	2018/10/04 6:36	68,3 KB
31101-f20.zip	2019/09/26 11:58	72,5 KB
31101-f30.zip	2020/07/07 11:54	77,9 KB
31101-g00.zip	2020/07/07 11:55	80,9 KB
31101-g10.zip	2021/04/06 14:03	92 KB
31101-g20.zip	2021/06/25 5:37	91,5 KB
31101-h00.zip	2022/04/01 9:20	92,3 KB
31101-h10.zip	2022/06/24 10:46	94,7 KB
31101-i00.zip	2024/04/10 6:14	129,1 KB
31101-i10.zip	2024/06/28 8:40	131,1 KB
31101-j00.zip	2025/10/08 16:59	131,6 KB

67 items.

APPENDIX P

The Wayback Machine - https://web.archive.org/web/20071112060040/http://www.3gpp.org:80/ftp/Spe…

www.3gpp.org - /ftp/Specs/archive/31_series/31.101/

[To Parent Directory]

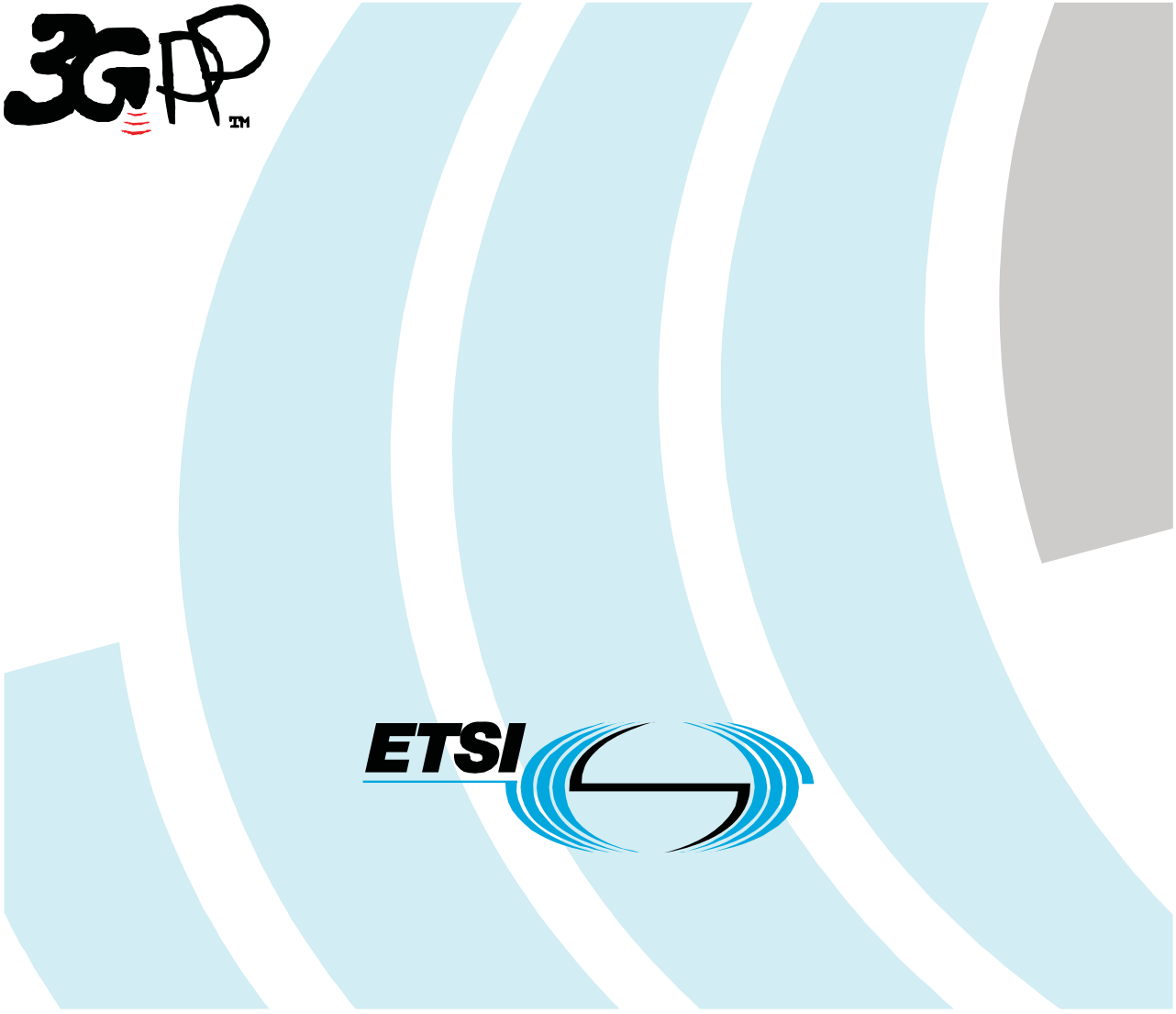
20 July 1999	06:46	165086	31101-050.zip
20 October 1999	15:49	218900	31101-100.zip
12 January 2000	13:43	196903	31101-300.zip
20 April 2000	08:42	253186	31101-310.zip
21 July 2000	14:25	262302	31101-320.zip
18 October 2000	12:18	28270	31101-330.zip
06 January 2005	10:04	30085	31101-331.zip
09 April 2001	07:37	28514	31101-400.zip
02 January 2003	13:40	36893	31101-410.zip
02 January 2005	18:34	30293	31101-420.zip
06 January 2005	10:05	30763	31101-421.zip
18 September 2002	07:53	28855	31101-500.zip
02 January 2003	13:41	37156	31101-510.zip
02 January 2005	18:34	30491	31101-520.zip
06 January 2005	10:06	30794	31101-521.zip
18 September 2002	07:54	29157	31101-600.zip
02 January 2003	13:41	43110	31101-610.zip
23 June 2003	15:11	35347	31101-620.zip
27 September 2004	09:18	36832	31101-630.zip
02 January 2005	18:34	36953	31101-640.zip
05 January 2005	14:57	37006	31101-641.zip
14 June 2005	17:09	37300	31101-650.zip
26 January 2006	13:41	38434	31101-651.zip
02 June 2007	23:39	46056	31101-700.zip
20 June 2007	06:05	45967	31101-701.zip

APPENDIX Q

ETSI TS 131 101 V7.0.1 (2007-06)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
UICC-terminal interface;
Physical and logical characteristics
(3GPP TS 31.101 version 7.0.1 Release 7)



Reference
RTS/TSGC-0631101v701

Keywords
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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2007.
All rights reserved.

DECT™, **PLUGTESTS**™ and **UMTS**™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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 (http://webapp.etsi.org/IPR/home.asp).

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.

Contents

Intellectual Property Rights 2
Foreword 2
Foreword 4
Introduction 4
1 Scope 5
2 References 5
3 Definitions, symbols, abbreviations and coding 5
4 General 3GPP platform requirements 6
4.1 GSM/USIM application interaction and restrictions 6
4.2 3GPP platform overview 6
4.3 TS 102 221 UICC/terminal interface 6
4.4 TS 102 600 Inter-Chip USB UICC/terminal interface 6
5 Physical and logical characteristics 7
5.1 Transmission speed 7
5.2 Voltage classes 7
5.3 File Control Parameters (FCP) 7
5.3.1 Minimum application clock frequency 7
5.4 Interface protocol 7
6 Application protocol 7
7 User verification and file access conditions 8
8 Files 9
8.1 Contents of the EFs at the MF level 9
Annex A (informative): Change history 10
History 11

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.

Introduction

The present document defines a generic Terminal/Integrated Circuit Card (ICC) interface for 3GPP applications. The present document is based on ETSI TS 102 221 [1], which defines a generic platform for any IC card application. The functionality provided by this platform may be operated either over the electrical interface specified in ETSI TS 102 221 [1], or by transporting APDUs over the Inter-Chip USB Terminal/ICC interface specified in ETSI TS 102 600 [7].

Requirements that are common to all 3GPP smart card based applications are also listed in this specification.

The aim of the present document is to ensure interoperability between an ICC and a terminal independently of the respective manufacturer, card issuer or operator. The present document does not define any aspects related to the administrative management phase of the ICC. Any internal technical realisation of either the ICC or the terminal is only specified where these are reflected over the interface.

Application specific details for applications residing on an ICC are specified in the respective application specific documents.

References to this document from 3GPP application specifications related to functionalities that are not described in the present document are to be considered as direct references to ETSI TS 102 221 [1].

1 Scope

The present document specifies the interface between the UICC and the Terminal for 3G telecom network operation.

The present document specifies:

- the requirements for the physical characteristics of the UICC;
- the electrical interface between the UICC and the Terminal;
- the initial communication establishment and the transport protocols;
- the model which serves as a basis for the logical structure of the UICC;
- the communication commands and the procedures;
- the application independent files and protocols.

The administrative procedures and initial card management are not part of the present document.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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] ETSI TS 102 221 Release 7: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics ".

[2] 3GPP TS 31.102: "Characteristics of the USIM Application".

[3] ETSI TS 101 220: "Smart cards; ETSI numbering system for telecommunication application providers".

[4] Void.

[5] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange".

[6] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[7] ETSI TS 102 600 Release 7: "Smart cards; UICC-Terminal interface; Characteristics of the USB interface".

3 Definitions, symbols, abbreviations and coding

All definitions, symbols, abbreviations applicable to the terminal are specified in ETSI TS 102 221 [1] and ETSI TS 102 600 [7].

The coding of Data Objects in the present document is according to ETSI TS 102 221 [1].

'XX': Single quotes indicate hexadecimal values. Valid elements for hexadecimal values are the numbers '0' to '9' and 'A' to 'F'.

4 General 3GPP platform requirements

4.1 GSM/USIM application interaction and restrictions

Activation of a USIM session excludes the activation of a GSM session. In particular, this implies that once a USIM application session has been activated, commands sent to the UICC with CLAss byte set to 'A0' shall return SW1SW2 '6E 00' (class not supported) to the terminal.

Similarly, activation of a GSM session excludes the activation of a USIM session.

At most one USIM session can be active at the same time.

4.2 3GPP platform overview

The UICC/terminal interface shall support the interface specified in ETSI TS 102 221 [1]. In addition, the UICC/terminal interface may support the Inter-Chip USB interface defined in ETSI TS 102 600 [7].

3GPP ICC based applications (e.g. USIM, USIM Application Toolkit, ISIM, SIM) are supported over both interfaces (see figure 1).

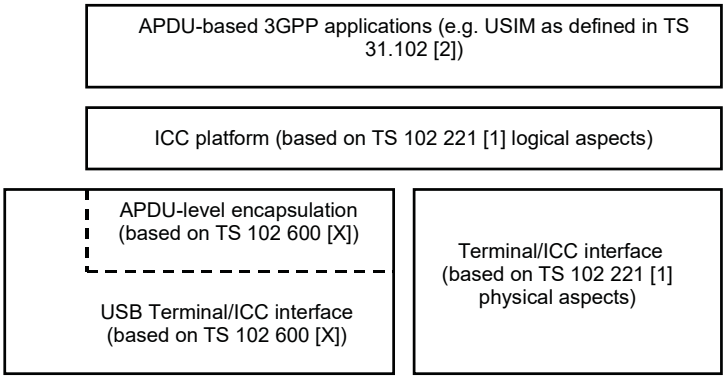


Figure 1: Terminal/UICC interface

4.3 TS 102 221 UICC/terminal interface

The UICC/terminal interface shall comply with all requirements stated in ETSI TS 102 221 [1]. Where options are indicated in ETSI TS 102 221 [1], the present document specifies which options are to be used for a TS 102 221 UICC/terminal interface where the UICC supports a 3GPP application.

4.4 TS 102 600 Inter-Chip USB UICC/terminal interface

If the Inter-Chip USB UICC/terminal interface is supported, it shall comply with ETSI TS 102 600 [7]. Where options are indicated in ETSI TS 102 600 [7], the present document specifies which options are to be used for an Inter-Chip USB UICC/terminal interface where the UICC supports a 3GPP application.

The protocol stack for APDU-level exchanges that are described in ETSI TS 102 600 [7] allow the transmission of APDUs. USB UICCs and USB UICC-enabled terminals shall comply with the functionality of the TS 102 221 interface. Where options are indicated in ETSI TS 102 221 [1], the present document specifies which options are to be used for APDU-based applications where the UICC supports a 3GPP application.

The mapping of APDU into TPDU (see ETSI TS 102 221 [1]) and transmission oriented commands (see ETSI TS 102 221 [1]) do not apply in the USB context as the APDU commands and responses are transmitted over USB as encoded at the application layer (i.e. C-APDU and R-APDU are directly encapsulated).

In the context of UICC applications running over USB, the card activation and deactivation process, the cold and warm reset procedures and the request for additional processing time as described in ETSI TS 102 221 [1] shall be performed by USB commands as described in ETSI TS 102 600 [7]. Any reference to the above procedures shall be interpreted in a USB context according to ETSI TS 102 600 [7]. When an ATR is received then the corresponding provisions and error handling procedures of ETSI TS 102 221 [1] apply.

5 Physical and logical characteristics

5.1 Transmission speed

Cards and terminals supporting an application based on the present specification shall support the transmission factor (F,D)=(512,32) in addition to those required by ETSI TS 102 221 [1].

It is recommended that terminals and cards supporting Multimedia Message storage functionality (see TS 31.102 [2]) support the transmission factor (F,D)=(512,64) in addition to those specified in the present document.

5.2 Voltage classes

A UICC holding a 3GPP application shall support at least two consecutive voltage classes as defined in ETSI TS 102 221 [1], e.g. AB or BC. If the UICC supports more than two classes, they shall all be consecutive, e.g. ABC.

5.3 File Control Parameters (FCP)

This clause defines the contents of the data objects which are part of the FCP information where there is a difference compared to the values as specified in ETSI TS 102 221 [1]. Where options are indicated in ETSI TS 102 221 [1], this clause specifies the values to be used in the FCP related to 3GPP applications.

5.3.1 Minimum application clock frequency

This data object is indicated by tag '82' in the proprietary constructed data object in the FCP information, identified by tag 'A5', as defined in ETSI TS 102 221 [1]. This data object specifies the minimum clock frequency to be provided by the terminal during the 3GPP application session. The value indicated in this data object shall not exceed 3 MHz, corresponding to '1E'. The terminal shall use a clock frequency between the value specified by this data object and the maximum clock frequency for the UICC as defined in ETSI TS 102 221 [1]. If this data object is not present in the FCP response or the value is 'FF' then the terminal shall assume that the minimum clock frequency is 1 MHz.

5.4 Interface protocol

No extra guard time, indicated in TC1 in the ATR, needs to be supported when sending characters from the terminal to the card. The terminal may reject a UICC indicating values other than 0 or 255 in TC1.

6 Application protocol

When involved in administrative management operations, a 3GPP application interfaces with appropriate equipment. These operations are outside the scope of the present document.

When involved in network operations a 3GPP application interfaces with a terminal with which messages are exchanged. A message can be a command or a response.

- A 3GPP Application command/response pair is a sequence consisting of a command and the associated response.

- A 3GPP Application procedure consists of one or more 3GPP Application command/response pairs which are used to perform all or part of an application-oriented task. A procedure shall be considered as a whole, that is to say that the corresponding task is achieved if and only if the procedure is completed. The terminal shall ensure that, when operated according to the manufacturer's manual, any unspecified interruption of the sequence of command/response pairs which realise the procedure, leads to the abortion of the procedure itself.

- A 3GPP application session is the interval of time starting at the completion of the 3GPP application initialisation procedure and ending either with the start of the 3GPP session termination procedure, or at the first instant the link between the UICC and the terminal is interrupted.

During the 3GPP network operation phase, the terminal plays the role of the master and the 3GPP application plays the role of the slave.

A 3GPP application specification may specify some commands defined in ETSI TS 102 221 [1] as optional or define additional commands. The 3GPP application shall execute all applicable commands in such a way as not to jeopardise, or cause suspension, of service provisioning to the user. This could occur if, for example, execution of the AUTHENTICATE is delayed in such a way which would result in the network denying or suspending service to the user.

7 User verification and file access conditions

A 3GPP application uses 2 PINs for user verification, PIN and PIN2. PIN2 is used only in the ADF. The PIN and PIN2 are mapped into key references as defined in ETSI TS 102 221 [1]. The Universal PIN shall be associated with a usage qualifier, and other key references may also be associated with a usage qualifier as defined in ETSI TS 102 221 [1]. The PIN status is indicated in the PS_DO, which is part of the FCP response when an ADF/DF is selected. The coding of the PS_DO is defined in ETSI TS 102 221 [1].

PIN and PIN2 are coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in CCITT T.50 [5] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the ME shall pad the presented PIN with 'FF' before sending it to the 3GPP application.

The coding of the UNBLOCK PINs is identical to the coding of the PINs. However, the number of (decimal) digits is always 8.

The security architecture as defined in ETSI TS 102 221 [1] applies to 3GPP applications with the following definitions and additions:

- A 3GPP application may reside on either a single-verification capable UICC or a multi-verification capable UICC.

- A 3GPP application residing on a multi-verification capable UICC shall support the replacement of its application PIN with the Universal PIN, key reference '11', as defined in ETSI TS 102 221 [1]. Only the Universal PIN is allowed as a replacement.

- A multi-verification capable UICC holding a 3GPP application shall support the referenced format using SEID as defined in ETSI TS 102 221 [1].

- Every file related to a 3GPP application shall have a reference to an access rule stored in EF_{ARR}.

- Disabling of PIN2 is allowed if supported by the 3GPP application, unless indicated otherwise.

The security architecture as defined in ETSI TS 102 221 [1] applies to terminals supporting 3GPP applications with the following definitions and requirements:

- A terminal shall support the use of level 1 and level 2 user verification requirements as defined in ETSI TS 102 221 [1].

- A terminal shall support the multi-application capabilities as defined in ETSI TS 102 221 [1].

- A terminal shall support the replacement of a 3GPP application PIN with the Universal PIN, key reference '11', as defined in ETSI TS 102 221 [1].

- A terminal shall support the security attributes defined using tag's '8C', 'AB' and '8B' as defined in ETSI TS 102 221 [1]. In addition both the referencing methods indicated by tag '8B' shall be supported as defined in ETSI TS 102 221 [1].

The access rule is referenced in the FCP using tag '8B'. The TLV object contains the file ID (the file ID of EF_{ARR}) and record number, or file ID (the file ID of EF_{ARR}), SEID and record number, pointer to the record in EF_{ARR} where the access rule is stored. Each SEID refers to a record number in EF_{ARR}. EFs having the same access rule use the same record reference in EF_{ARR}. For an example EF_{ARR}, see ETSI TS 102 221 [1].

8 Files

This clause specifies general requirements for EFs for 3GPP applications.

EFs contain data items. A data item is a part of an EF which represents a complete logical entity. The 3GPP application specification defines the access conditions, data items and coding for each file.

EFs or data items having an unassigned value, or which are cleared by the terminal, shall have their bytes set to 'FF'. After the administrative phase all data items shall have a defined value or have their bytes set to 'FF', unless specified otherwise in other 3GPP specifications. For example, for a deleted LAI in the EF_{LOCI} file defined in TS 31.102 [2], the last byte takes the value 'FE' (refer to TS 24.008 [6]). If a data item is modified by the allocation of a value specified in another 3GPP TS, then this value shall be used and the data item is not unassigned.

EFs are mandatory (M), optional (O), or conditional (C). A conditional file is mandatory if required by a supported feature, as defined by the 3GPP application.(e.g; PBR in TS 31.102 [2]). The file size of an optional EF may be zero. All implemented EFs with a file size greater than zero shall contain all mandatory data items. Optional data items may either be filled with 'F', or, if located at the end of an EF, need not exist.

When the coding is according to ITU-T Recommendation T.50 [5], bit 8 of every byte shall be set to 0.

8.1 Contents of the EFs at the MF level

There are four EFs at the Master File (MF) level specified in ETSI TS 102 221 [1] (EF_{ICCID}; EF_{DIR}, EF_{PL} and EF_{ARR}), which are all mandatory for 3GPP.

The EF_{DIR} file contains the Application Identifiers (AIDs) and the Application Labels of the 3GPP applications present on the card as mandatory elements. The AIDs of 3GPP applications are defined in ETSI TS 101 220 [3]. The 3GPP applications can only be selected by means of the AID selection. The EF_{DIR} entry shall not contain a path object for application selection. It is recommended that the application label does not contain more than 32 bytes.

Annex A (informative): Change history

Change history								
Date	Meeting	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New
2002-12	TP-18	TP-020279	0027	-	D	Gather all 3GPP-specific card platform requirements in TS 31.101.	6.0.0	6.1.0
2003-06	TP-20	TP-030120	0028	-	F	Clarification on the support of extra guardtime	6.1.0	6.2.0
2004-09	TP-25	TP-040180	0029	-	B	Requirement for higher UICC/Terminal interface speed	6.2.0	6.3.0
		TP-040180	0030	-	B	Move "GSM/USIM application interactions and restrictions" from ETSI TS 102 221	6.2.0	6.3.0
2004-12	TP-26	TP-040255	0033	-	F	Correction of non specific references	6.3.0	6.4.0
2004-12	TP-26					Reinstation of original bullets in reference clause	6.4.0	6.4.1
2005-06	CP-28	CP-050136	0034	-	F	ISO/IEC 7816-Series Revision	6.4.1	6.5.0
2006-01						Correction of CR-number from CP-28	6.5.0	6.5.1
2007-06	CP-36	CP-070480	0037	7	B	Introduction of the new High Speed ME-UICC Interface	6.5.1	7.0.0
2007-06	-	-	-	-	-	MCC correction of implementation of CR0037R7, clause 4.3	7.0.0	7.0.1

History

Document history		
V7.0.1	June 2007	Publication

APPENDIX R

http://www.3gpp.org/ftp/Specs/html-info/31-series.htm Go
89 captures
30 Jun 2003 - 19 Nov 2023
JAN AUG OCT
2006 2007 2008
About this capture

3GPP Specification series

Back to numbering scheme page

Click on spec number for details

TS 31.048	Security mechanisms for the (U)SIM application toolkit; Test specification	.
TS 31.101	UICC-terminal interface; Physical and logical characteristics	.
TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application	.
TS 31.103	Characteristics of the IP Multimedia Services Identity Module (ISIM) application	.
TS 31.110	Numbering system for telecommunication IC card applications	.
TS 31.111	Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)	.
TS 31.112	Universal Subscriber Identity Module Application Toolkit (USAT) interpreter architecture description; Stage 2	.
TS 31.113	Universal Subscriber Identity Module Application Toolkit (USAT) interpreter byte codes	.
TS 31.114	Universal Subscriber Identity Module Application Toolkit (USAT) interpreter protocol and administration	.
TS 31.115	Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications	.
TS 31.116	Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications	.
TS 31.120	UICC-terminal interface; Physical, electrical and logical test specification	.
TS 31.121	UICC-terminal interface; Universal Subscriber Identity Module (USIM) application test specification	.
TS 31.122	Universal Subscriber Identity Module (USIM) conformance test specification	.
TS 31.123	(Universal) Subscriber Interface Module ((U)SIM) toolkit interpreter test	SPECIFICATION WITHDRAWN
TS 31.124	Mobile Equipment (ME) conformance test specification; Universal Subscriber Interface Module Application Toolkit (USAT) conformance test specification	.
TS 31.130	(U)SIM Application Programming Interface (API); (U)SIM API for Java Card	.
TS 31.131	C-language binding for (Universal) Subscriber Identity Module ((U)SIM) API	.
TS 31.133	IP Multimedia Services Identity Module (ISIM) Application Programming Interface (API); ISIM API for Java Card™	.
TS 31.213	Test specification for subscriber (U)SIM; Application Programming Interface (API) for Java Card™	.
TS 31.50U	Essential requirements for UMTS Mobile Stations (ME) operating within frequency bands 1885-1980, 2010-2025 and 2110-2200 MHz	SPECIFICATION WITHDRAWN
TS 31.60U	Essential requirements for UMTS Mobile Earth Stations (MES) operating within frequency bands 1980- 2010 and 2170-2200 MHz	SPECIFICATION WITHDRAWN
TR 31.900	SIM/USIM internal and external interworking aspects	.
TR 31.919	2G/3G Java Card™ Application Programming Interface (API) based applet interworking	.

APPENDIX S

http://www.3gpp.org/ftp/Specs/html-info/31101.htm
Go
MAY OCT DEC
27
2006 2007 2014
53 captures
2 Jul 2003 - 7 Feb 2026
About this capture

3GPP Specification detail

Back to numbering scheme page

Back to series index

3GPP TS 31.101 (click spec number to see fileserver directory for this spec)

UICC-terminal interface; Physical and logical characteristics

.

TSG / WG responsible: C6 (click TSG/WG to see its home page)

Work item which gave rise to this spec: - (click WI code to see Work Item details in the Work Plan)

Contents is a reference to ETSI TR 102 221.CP-27: change of WG as a result of closure of CN and T.

Rapporteur: **VESTERGAARD, Peter**

Specification required for: UTRAN-based systems

In the table below ...

... click meeting number for meeting details;

... click spec version number to download that version;

... click SDO publication reference to download SDO transposed document.

Release	Freeze meeting	Freeze date	remarks	SDO publications
R99	SP-06	1999-12-17	TP-09: txferred from T2 to ETSI SCP as TR 102 221. So removed from 3gpp spec list. Sanders, May 2001: no, not withdrawn. So re-instated. .	ETSI
	event	version	available	remarks	click ref to download
	TP-03	0.0.0	1999-04-23		-
	TP-04	0.5.0	1999-06-23		-
	TP-05	1.0.0	1999-10-08		-
	TP-06	3.0.0	1999-12-17		DTS/TSGT-0331101U
	TP-07	3.1.0	2000-03-15	completion target	RTS/TSGT-0331101UR1
	TP-08	3.2.0	2000-02-06		RTS/TSGT-0331101UR2
	TP-09	3.3.0	2000-10-18		-
	edito post TP-26	3.3.1	2005-01-06		RTS/TSGT-0331101v331
Rel-4	SP-11	2001-03-22	.		ETSI
	event	version	available	remarks	click ref to download
	TP-11	4.0.0	2001-04-09		RTS/TSGT-0331101Uv4
	TP-18	4.1.0	2003-01-02		RTS/TSGT-0331101v410
	TP-26	4.2.0	2005-01-03		RTS/TSGT-0331101v421
	edito post TP-26	4.2.1	2005-01-06		RTS/TSGT-0331101v421
Rel-5	TP-17	2002-09-06	TP-17: upgraded to Rel-5 to fill gap between Releases 4 and 6. .		ETSI
	event	version	available	remarks	click ref to download
	TP-17	5.0.0	2002-09-18		RTS/TSGT-0331101v500
	TP-18	5.1.0	2003-01-02		RTS/TSGT-0331101v510
	TP-26	5.2.0	2005-01-03		RTS/TSGT-0331101v521
	edito post TP-26	5.2.1	2005-01-06		RTS/TSGT-0331101v521
Rel-6	TP-26	2004-12-10	TP-17: upgraded to Rel-6 as there are 3G specific platform requirements that are currently not defined by the respective EP SCP specification TS 102 221. .		ETSI
	event	version	available	remarks	click ref to download
	TP-17	6.0.0	2002-09-18		-
	TP-18	6.1.0	2003-01-02		-
	TP-20	6.2.0	2003-06-23		-
	TP-25	6.3.0	2004-09-27		-
	TP-26	6.4.0	2005-01-03		RTS/TSGT-0331101v641
	edito post TP-26	6.4.1	2005-01-06		RTS/TSGT-0331101v641
	CP-28	6.5.0	2005-06-14		-
	post CP-30	6.5.1	2006-01-26	Corrects wrong CR number in change history	RTS/TSGC-0631101v651
Rel-7	SP-36	2007-06-07	..		ETSI
	event	version	available	remarks	click ref to download
	CP-36	7.0.0	2007-06-12		RTS/TSGC-0631101v701
	CP-36	7.0.1	2007-06-21	MCC correction of implementation of CR0037R7, clause 4.3	RTS/TSGC-0631101v701

Change Requests for this spec: click here.

Genealogy of this spec:

antecedent(s)	this spec	descendant(s)
11.18	31.101	(no descendants)

APPENDIX T

www.3gpp.org / ftp / Specs / archive / 31_series / 31.102

Download

	sort by name/desc	sort by date/desc	sort by size/desc
	31102-050.zip	1999/07/20 6:46	149,1 KB
	31102-100.zip	1999/10/20 15:49	167,2 KB
	31102-300.zip	2000/01/12 13:43	206,6 KB
	31102-310.zip	2000/04/20 8:42	240,2 KB
	31102-320.zip	2000/07/21 14:25	309,6 KB
	31102-330.zip	2000/10/18 12:18	311,6 KB
	31102-340.zip	2001/01/05 6:09	325,6 KB
	31102-350.zip	2001/04/09 7:36	317,9 KB
	31102-360.zip	2001/07/06 13:41	319,1 KB
	31102-370.zip	2001/10/11 15:25	321,3 KB
	31102-380.zip	2002/01/17 8:26	320,1 KB
	31102-390.zip	2002/06/28 14:46	321,6 KB
	31102-3a0.zip	2002/09/25 13:55	323,4 KB
	31102-3b0.zip	2003/01/02 13:42	333,3 KB
	31102-3c0.zip	2003/03/31 12:59	326 KB
	31102-3d0.zip	2003/06/23 15:14	339,2 KB
	31102-3e0.zip	2003/09/30 9:48	338,7 KB
	31102-3f0.zip	2004/01/12 10:07	477,7 KB
	31102-3g0.zip	2004/03/24 20:59	464 KB
	31102-3h0.zip	2004/06/15 10:20	472,3 KB
	31102-3i0.zip	2005/06/14 17:15	470,7 KB
	31102-400.zip	2001/04/09 7:36	325,9 KB
	31102-410.zip	2001/07/20 8:43	331,1 KB

31102-420.zip	2001/10/11 15:23	341,2 KB
31102-430.zip	2002/01/17 8:28	344,6 KB
31102-440.zip	2002/03/26 10:24	407,3 KB
31102-450.zip	2002/06/28 14:46	403,6 KB
31102-460.zip	2002/09/25 13:54	408,8 KB
31102-470.zip	2003/01/02 13:43	418,3 KB
31102-480.zip	2003/03/31 13:31	359,1 KB
31102-490.zip	2003/06/23 15:13	423,7 KB
31102-4a0.zip	2003/09/30 9:48	425,4 KB
31102-4b0.zip	2004/01/09 12:56	506 KB
31102-4c0.zip	2004/03/24 21:06	483,5 KB
31102-4d0.zip	2004/06/15 10:21	502,1 KB
31102-4e0.zip	2005/01/04 16:00	508,1 KB
31102-4f0.zip	2005/06/14 17:20	497,8 KB
31102-500.zip	2002/03/26 10:27	403,6 KB
31102-510.zip	2002/06/28 14:46	404,2 KB
31102-520.zip	2002/09/25 13:55	409,5 KB
31102-530.zip	2003/01/02 13:43	417,6 KB
31102-540.zip	2003/03/31 13:37	362,7 KB
31102-550.zip	2003/06/13 11:08	425,9 KB
31102-560.zip	2003/09/30 9:49	423,7 KB
31102-570.zip	2004/01/12 10:08	504,2 KB
31102-580.zip	2004/03/24 21:15	483,4 KB
31102-590.zip	2004/06/15 10:21	504,6 KB
31102-5a0.zip	2004/09/23 15:27	509,5 KB
31102-5b0.zip	2005/01/06 10:07	510,4 KB
31102-5c0.zip	2005/03/18 11:37	482,9 KB
31102-5d0.zip	2005/06/15 12:38	490,9 KB
31102-5e0.zip	2005/10/10 11:46	487,5 KB

31102-5f0.zip	2012/09/21 8:21	380,8 KB
31102-600.zip	2003/01/02 13:44	414 KB
31102-610.zip	2003/03/31 13:41	355,7 KB
31102-620.zip	2003/06/23 15:15	418,2 KB
31102-630.zip	2003/09/30 9:50	418,8 KB
31102-640.zip	2004/01/12 10:09	477,6 KB
31102-650.zip	2004/03/25 13:55	447,9 KB
31102-660.zip	2004/06/24 7:32	530,5 KB
31102-670.zip	2004/10/07 12:59	520,9 KB
31102-680.zip	2005/01/05 14:43	512,6 KB
31102-690.zip	2005/03/18 11:37	552,3 KB
31102-6a0.zip	2005/06/14 17:21	522,3 KB
31102-6b0.zip	2005/10/10 11:47	522,1 KB
31102-6c0.zip	2005/12/10 14:05	568,9 KB
31102-6d0.zip	2006/03/30 15:15	573,3 KB
31102-6e0.zip	2006/06/02 7:11	577,2 KB
31102-6f0.zip	2006/09/28 16:47	541,3 KB
31102-6g0.zip	2006/11/30 13:02	542,2 KB
31102-6h0.zip	2007/03/19 10:31	567,6 KB
31102-6i0.zip	2007/06/03 0:23	555,7 KB
31102-6i1.zip	2007/06/18 13:53	549,4 KB
31102-6j0.zip	2007/09/21 14:17	512,4 KB
31102-6k0.zip	2008/03/28 13:50	520,3 KB
31102-6l0.zip	2008/10/02 20:55	522,8 KB
31102-6m0.zip	2012/09/21 8:33	395,6 KB
31102-6n0.zip	2012/12/21 8:54	398,9 KB
31102-700.zip	2005/03/18 11:37	501,4 KB
31102-710.zip	2005/06/14 17:23	515,1 KB
31102-720.zip	2005/10/10 11:47	518,9 KB

31102-730.zip	2005/12/10 14:06	559,1 KB
31102-740.zip	2006/03/31 13:15	569,8 KB
31102-741.zip	2006/04/28 7:27	526,8 KB
31102-750.zip	2006/06/02 7:15	574,4 KB
31102-760.zip	2006/09/28 16:51	533,9 KB
31102-770.zip	2006/11/30 13:05	579,9 KB
31102-780.zip	2007/03/19 10:45	568,1 KB
31102-790.zip	2007/06/03 2:05	500,4 KB
31102-791.zip	2007/06/20 5:48	500,8 KB
31102-7a0.zip	2007/09/21 14:52	561 KB
31102-7b0.zip	2007/12/21 16:07	527,7 KB
31102-7c0.zip	2008/03/28 14:08	519,2 KB
31102-7d0.zip	2008/10/02 21:03	523,6 KB
31102-7e0.zip	2009/06/12 13:52	523,9 KB
31102-7f0.zip	2009/12/20 10:07	531,8 KB
31102-7g0.zip	2012/09/21 8:47	403,6 KB
31102-7h0.zip	2012/12/21 10:19	404 KB
31102-800.zip	2007/12/21 16:09	527,4 KB
31102-810.zip	2008/03/31 8:59	560,6 KB
31102-820.zip	2008/06/18 16:49	529,7 KB
31102-830.zip	2008/10/02 21:57	581,9 KB
31102-840.zip	2009/01/08 16:43	694 KB
31102-850.zip	2009/03/27 14:48	726,7 KB
31102-860.zip	2009/06/12 19:47	705,9 KB
31102-870.zip	2009/09/26 11:53	697,8 KB
31102-880.zip	2009/12/20 10:07	712,8 KB
31102-890.zip	2010/06/18 9:56	561,9 KB
31102-8a0.zip	2010/10/02 13:33	567,1 KB
31102-8b0.zip	2011/01/02 17:11	567,5 KB

31102-8c0.zip	2011/06/21 13:05	568 KB
31102-8d0.zip	2011/10/03 16:49	568,6 KB
31102-8e0.zip	2012/01/06 14:26	568,6 KB
31102-8f0.zip	2012/09/21 8:53	571,1 KB
31102-8g0.zip	2012/12/21 10:29	571,7 KB
31102-8h0.zip	2013/06/28 13:32	569,1 KB
31102-8i0.zip	2015/06/26 4:47	573,1 KB
31102-8j0.zip	2016/01/12 10:44	573,5 KB
31102-8k0.zip	2016/03/18 15:39	603,7 KB
31102-8l0.zip	2017/03/17 16:44	595,1 KB
31102-8m0.zip	2017/12/30 1:42	564 KB
31102-900.zip	2009/09/26 11:54	754,3 KB
31102-910.zip	2009/12/20 10:07	765,1 KB
31102-920.zip	2010/04/13 13:36	730,1 KB
31102-930.zip	2010/06/18 9:56	574,9 KB
31102-940.zip	2010/10/02 14:22	569,7 KB
31102-950.zip	2011/01/02 17:35	578,1 KB
31102-960.zip	2011/04/01 5:17	582,8 KB
31102-970.zip	2011/06/21 16:08	584,3 KB
31102-980.zip	2011/10/03 16:49	585,3 KB
31102-990.zip	2012/01/06 14:26	582,8 KB
31102-9a0.zip	2012/06/29 14:59	587,2 KB
31102-9b0.zip	2012/09/21 9:04	587,9 KB
31102-9c0.zip	2012/12/21 13:20	586,1 KB
31102-9d0.zip	2013/06/28 13:32	585,8 KB
31102-9e0.zip	2013/09/20 18:50	586,4 KB
31102-9f0.zip	2015/06/26 5:16	587,3 KB
31102-9g0.zip	2016/01/08 18:11	590,3 KB
31102-9h0.zip	2016/03/18 15:47	622 KB

31102-9i0.zip	2017/03/17 16:19	613,9 KB
31102-9i1.zip	2017/04/11 16:05	619,1 KB
31102-9j0.zip	2017/12/30 1:41	582 KB
31102-a00.zip	2011/01/02 17:50	584,7 KB
31102-a10.zip	2011/04/01 7:15	609,2 KB
31102-a20.zip	2011/06/21 16:47	620,4 KB
31102-a30.zip	2011/10/03 16:49	622,3 KB
31102-a40.zip	2012/01/06 14:26	611,8 KB
31102-a50.zip	2012/03/23 19:18	623,5 KB
31102-a60.zip	2012/06/29 15:00	627 KB
31102-a70.zip	2012/09/21 9:10	628,4 KB
31102-a80.zip	2012/12/21 13:25	628,6 KB
31102-a90.zip	2013/06/28 13:31	626,2 KB
31102-aa0.zip	2013/09/20 18:49	628,4 KB
31102-ab0.zip	2015/06/26 5:15	628,5 KB
31102-ac0.zip	2016/01/08 18:27	630,3 KB
31102-ad0.zip	2016/03/18 17:06	664 KB
31102-ae0.zip	2017/03/17 16:24	654 KB
31102-ae1.zip	2017/04/11 16:11	661,6 KB
31102-af0.zip	2017/12/30 1:40	621,8 KB
31102-b00.zip	2011/10/03 16:49	622,5 KB
31102-b10.zip	2012/03/23 19:40	614,5 KB
31102-b20.zip	2012/06/29 15:00	629,6 KB
31102-b30.zip	2012/09/21 9:16	627,9 KB
31102-b40.zip	2012/12/21 13:49	619,5 KB
31102-b50.zip	2013/06/28 13:31	630,8 KB
31102-b60.zip	2013/09/20 18:48	629,1 KB
31102-b70.zip	2014/09/26 16:35	632,4 KB
31102-b80.zip	2015/06/26 5:15	631,5 KB

31102-b90.zip	2016/01/08 18:31	634,4 KB
31102-ba0.zip	2016/03/18 17:23	667,8 KB
31102-bb0.zip	2017/03/17 16:29	660 KB
31102-bc0.zip	2017/12/30 1:39	628,7 KB
31102-c00.zip	2013/06/28 13:31	631,5 KB
31102-c10.zip	2013/09/20 18:48	629,4 KB
31102-c20.zip	2013/12/20 15:34	633,9 KB
31102-c30.zip	2014/03/19 17:26	645,5 KB
31102-c40.zip	2014/07/02 15:17	659 KB
31102-c50.zip	2014/09/26 16:34	667,1 KB
31102-c60.zip	2015/01/06 15:13	678,6 KB
31102-c70.zip	2015/03/27 16:18	686,4 KB
31102-c80.zip	2015/06/26 5:35	699,9 KB
31102-c81.zip	2015/07/03 9:08	700,4 KB
31102-c90.zip	2015/09/25 14:28	691,3 KB
31102-ca0.zip	2016/01/12 10:45	699,8 KB
31102-cb0.zip	2016/03/18 18:05	741,9 KB
31102-cc0.zip	2017/03/17 16:34	733,4 KB
31102-cd0.zip	2017/12/30 1:38	691,9 KB
31102-d00.zip	2015/07/03 9:20	701,6 KB
31102-d10.zip	2015/09/25 14:48	685,6 KB
31102-d20.zip	2016/01/08 19:23	693,3 KB
31102-d30.zip	2016/03/25 23:21	771,4 KB
31102-d40.zip	2016/06/24 21:41	772,9 KB
31102-d50.zip	2016/10/07 21:37	645,9 KB
31102-d60.zip	2017/01/19 15:56	649,6 KB
31102-d70.zip	2017/03/17 16:41	680,9 KB
31102-d80.zip	2017/06/16 12:06	641,6 KB
31102-d81.zip	2018/01/11 11:28	649 KB

31102-d90.zip	2017/12/30 1:37	636,2 KB
31102-d91.zip	2018/01/11 11:34	649,4 KB
31102-e00.zip	2016/10/07 21:36	650,4 KB
31102-e10.zip	2017/01/19 17:01	641,3 KB
31102-e20.zip	2017/03/17 15:21	717,5 KB
31102-e30.zip	2017/06/16 12:04	669,7 KB
31102-e40.zip	2017/12/30 1:36	677,3 KB
31102-e50.zip	2018/04/03 17:01	722,7 KB
31102-e60.zip	2018/12/21 20:14	687,7 KB
31102-e61.zip	2019/04/26 9:45	733,9 KB
31102-e62.zip	2019/04/26 12:51	740,8 KB
31102-e70.zip	2019/03/24 19:16	676,7 KB
31102-e80.zip	2019/06/10 8:02	669,5 KB
31102-f00.zip	2018/04/03 16:58	720,6 KB
31102-f10.zip	2018/06/22 22:16	697,8 KB
31102-f20.zip	2018/10/04 6:36	757,7 KB
31102-f30.zip	2018/12/21 20:15	727,8 KB
31102-f40.zip	2019/02/21 13:14	739,8 KB
31102-f50.zip	2019/03/24 19:17	721,9 KB
31102-f60.zip	2019/06/10 8:04	837,1 KB
31102-f70.zip	2019/09/26 12:01	838,9 KB
31102-f80.zip	2020/01/08 11:11	842,9 KB
31102-f90.zip	2020/03/30 16:33	785,9 KB
31102-fa0.zip	2020/07/07 11:55	794,1 KB
31102-fb0.zip	2020/09/23 22:12	798 KB
31102-fc0.zip	2022/09/23 8:12	1160,3 KB
31102-fd0.zip	2026/06/29 16:12	1181,5 KB
31102-g00.zip	2019/06/10 8:05	839,6 KB
31102-g10.zip	2019/09/26 12:01	840,1 KB

31102-g20.zip	2020/01/08 11:11	849,8 KB
31102-g30.zip	2020/03/30 16:33	795,2 KB
31102-g40.zip	2020/07/07 11:56	790 KB
31102-g50.zip	2020/09/23 22:12	806,5 KB
31102-g60.zip	2020/12/11 10:55	807,9 KB
31102-g70.zip	2021/06/25 5:42	1185,3 KB
31102-g80.zip	2021/09/24 12:23	1196 KB
31102-g90.zip	2021/12/16 11:39	1203,5 KB
31102-ga0.zip	2022/05/10 13:38	1214,9 KB
31102-gb0.zip	2022/06/24 10:46	1214,1 KB
31102-gc0.zip	2022/09/23 8:13	1216,2 KB
31102-gd0.zip	2022/12/15 12:14	1219,2 KB
31102-ge0.zip	2024/04/10 5:44	1229,7 KB
31102-gf0.zip	2025/03/27 14:43	1230,5 KB
31102-gg0.zip	2026/06/29 16:12	1237,6 KB
31102-h00.zip	2020/12/11 10:56	815,1 KB
31102-h10.zip	2021/04/06 14:04	1194,8 KB
31102-h20.zip	2021/06/25 6:11	1199,1 KB
31102-h30.zip	2021/09/24 12:24	1223,9 KB
31102-h40.zip	2021/12/16 11:40	1220,2 KB
31102-h50.zip	2022/04/01 9:22	1294,9 KB
31102-h60.zip	2022/06/24 10:47	1334,7 KB
31102-h70.zip	2022/09/23 8:13	1336,8 KB
31102-h71.zip	2022/10/19 7:08	1337,6 KB
31102-h80.zip	2022/12/15 12:15	1340,3 KB
31102-h90.zip	2023/03/29 10:45	1344,4 KB
31102-ha0.zip	2023/06/26 13:57	1345,6 KB
31102-hb0.zip	2024/01/10 6:54	1346 KB
31102-hc0.zip	2024/04/10 5:45	1360 KB

31102-hd0.zip	2024/06/28 8:40	1373.7 KB
31102-he0.zip	2024/10/02 7:11	1354.8 KB
31102-he1.zip	2024/10/10 7:38	1352.8 KB
31102-he2.zip	2024/10/24 13:55	1355 KB
31102-hf0.zip	2025/01/03 12:47	1352.9 KB
31102-hg0.zip	2025/03/27 14:43	1367.3 KB
31102-hh0.zip	2026/06/29 16:13	1386.3 KB
31102-i00.zip	2023/03/30 17:10	1405.1 KB
31102-i10.zip	2023/06/26 13:59	1406.7 KB
31102-i20.zip	2023/09/22 17:25	1418.5 KB
31102-i30.zip	2024/01/10 6:54	1431.9 KB
31102-i40.zip	2024/04/12 8:45	1475.2 KB
31102-i50.zip	2024/06/28 8:41	1483.1 KB
31102-i60.zip	2024/10/02 7:12	1485.6 KB
31102-i61.zip	2024/10/10 7:40	1484.3 KB
31102-i62.zip	2024/10/24 13:56	1483.7 KB
31102-i70.zip	2025/01/03 12:47	1487 KB
31102-i80.zip	2025/03/27 14:44	1491.6 KB
31102-i90.zip	2025/06/13 7:39	1487.7 KB
31102-ia0.zip	2026/06/29 16:13	1496.6 KB
31102-j00.zip	2025/01/03 12:49	1490.6 KB
31102-j10.zip	2025/03/27 14:45	1490.1 KB
31102-j20.zip	2025/06/13 7:40	1539.1 KB
31102-j30.zip	2025/09/28 21:06	1553.9 KB
31102-j40.zip	2026/01/06 21:24	1548.1 KB
31102-j50.zip	2026/06/29 16:14	1558 KB

281 items.

APPENDIX U

INTERNET ARCHIVE Wayback Machine
http://www.3gpp.org/ftp/Specs/archive/31_series/31.102/
Go
105 captures
12 Jun 2002 – 17 Feb 2026
NOV JAN MAR
2005 08 2008 2014
About this capture

www.3gpp.org - /ftp/Specs/archive/31_series/31.102/

[To Parent Directory]

20 July 1999	06:46	152735	31102-050.zip
20 October 1999	15:49	171283	31102-100.zip
12 January 2000	13:43	211594	31102-300.zip
20 April 2000	08:42	246044	31102-310.zip
21 July 2000	14:25	317066	31102-320.zip
18 October 2000	12:18	319143	31102-330.zip
05 January 2001	06:09	333434	31102-340.zip
09 April 2001	07:36	325541	31102-350.zip
06 July 2001	13:41	326826	31102-360.zip
11 October 2001	15:25	329068	31102-370.zip
17 January 2002	08:26	327836	31102-380.zip
28 June 2002	14:46	329403	31102-390.zip
25 September 2002	13:55	331214	31102-3a0.zip
02 January 2003	13:42	341393	31102-3b0.zip
31 March 2003	12:59	333906	31102-3c0.zip
23 June 2003	15:14	347411	31102-3d0.zip
30 September 2003	09:48	346901	31102-3e0.zip
12 January 2004	10:07	489228	31102-3f0.zip
24 March 2004	20:59	475200	31102-3g0.zip
15 June 2004	10:20	483638	31102-3h0.zip
14 June 2005	17:15	482096	31102-3i0.zip
09 April 2001	07:36	333821	31102-400.zip
20 July 2001	08:43	339079	31102-410.zip
11 October 2001	15:23	349418	31102-420.zip
17 January 2002	08:28	352889	31102-430.zip
26 March 2002	10:24	417126	31102-440.zip
28 June 2002	14:46	413346	31102-450.zip
25 September 2002	13:54	418614	31102-460.zip
02 January 2003	13:43	428422	31102-470.zip
31 March 2003	13:31	367728	31102-480.zip
23 June 2003	15:13	433966	31102-490.zip
30 September 2003	09:48	435711	31102-4a0.zip
09 January 2004	12:56	518185	31102-4b0.zip
24 March 2004	21:06	495152	31102-4c0.zip
15 June 2004	10:21	514245	31102-4d0.zip
04 January 2005	16:00	520325	31102-4e0.zip
14 June 2005	17:20	509765	31102-4f0.zip
26 March 2002	10:27	413369	31102-500.zip
28 June 2002	14:46	413991	31102-510.zip
25 September 2002	13:55	419343	31102-520.zip
02 January 2003	13:43	427705	31102-530.zip
31 March 2003	13:37	371426	31102-540.zip
13 June 2003	11:08	436125	31102-550.zip
30 September 2003	09:49	433891	31102-560.zip
12 January 2004	10:08	516360	31102-570.zip
24 March 2004	21:15	495089	31102-580.zip
15 June 2004	10:21	516802	31102-590.zip
23 September 2004	15:27	521729	31102-5a0.zip
06 January 2005	10:07	522664	31102-5b0.zip
18 March 2005	11:37	494551	31102-5c0.zip
15 June 2005	12:38	502708	31102-5d0.zip
10 October 2005	11:46	499223	31102-5e0.zip
02 January 2003	13:44	424017	31102-600.zip
31 March 2003	13:41	364336	31102-610.zip
23 June 2003	15:15	428280	31102-620.zip
30 September 2003	09:50	428922	31102-630.zip
12 January 2004	10:09	489131	31102-640.zip
25 March 2004	13:55	458739	31102-650.zip
24 June 2004	07:32	543261	31102-660.zip
07 October 2004	12:59	533444	31102-670.zip
05 January 2005	14:43	524972	31102-680.zip
18 March 2005	11:37	565584	31102-690.zip
14 June 2005	17:21	534917	31102-6a0.zip
10 October 2005	11:47	534712	31102-6b0.zip
10 December 2005	14:05	582603	31102-6c0.zip
30 March 2006	15:15	587092	31102-6d0.zip
02 June 2006	07:11	591083	31102-6e0.zip
28 September 2006	16:47	554348	31102-6f0.zip
30 November 2006	13:02	555263	31102-6g0.zip
19 March 2007	10:31	581279	31102-6h0.zip
03 June 2007	00:23	569126	31102-6i0.zip
18 June 2007	13:53	562661	31102-6i1.zip
21 September 2007	14:17	524769	31102-6j0.zip
18 March 2005	11:37	513516	31102-700.zip
14 June 2005	17:23	527563	31102-710.zip
10 October 2005	11:47	531429	31102-720.zip
10 December 2005	14:06	572527	31102-730.zip
31 March 2006	13:15	583575	31102-740.zip
28 April 2006	07:27	539492	31102-741.zip
02 June 2006	07:15	588249	31102-750.zip
28 September 2006	16:51	546795	31102-760.zip
30 November 2006	13:05	593885	31102-770.zip
19 March 2007	10:45	581807	31102-780.zip
03 June 2007	02:05	512416	31102-790.zip
20 June 2007	05:48	512891	31102-791.zip
21 September 2007	14:52	574550	31102-7a0.zip
21 December 2007	16:07	540414	31102-7b0.zip
21 December 2007	16:09	540139	31102-800.zip

APPENDIX V

CT#43	8.5.0	2009-03-27			ETSI TDoc CR
CT#42	8.4.0	2009-01-08	§§4.2.92 & H.1: SFI code sho...		ETSI TDoc CR
CT#41	8.3.0	2008-10-03			ETSI TDoc CR
CT#40	8.2.0	2008-06-18			ETSI TDoc CR
CT#39	8.1.0	2008-03-31			ETSI TDoc CR
CT#38	8.0.0	2007-12-21			ETSI TDoc CR

Release 7(Spec is UCC for this Release) **Latest Remark:**

Meetings	Version	Upload date	Comment		
CT#58	7.17.0	2012-12-21			ETSI TDoc CR
CT#57	7.16.0	2012-09-21			ETSI TDoc CR
CT#46	7.15.0	2009-12-20			ETSI TDoc CR
CT#44	7.14.0	2009-06-12			ETSI TDoc CR
CT#41	7.13.0	2008-10-03			ETSI TDoc CR
CT#39	7.12.0	2008-03-28			ETSI TDoc CR
CT#38	7.11.0	2007-12-21			ETSI TDoc CR
CT#37	7.10.0	2007-09-26			ETSI TDoc CR
CT#36	7.9.1	2007-06-21	Correction to implementation ...		ETSI TDoc CR
CT#36	7.9.0	2007-06-12			ETSI TDoc CR
CT#35	7.8.0	2007-03-20			ETSI TDoc CR

Exit

APPENDIX W

http://www.3gpp.org/ftp/Specs/html-info/31102.htm
Go
NOV JAN FEB
86 captures
2 Jul 2003 - 10 Feb 2026
2006 03 2008 2015
About this capture

3GPP Specification detail

Back to numbering scheme page

Back to series index

3GPP TS 31.102 (click spec number to see fileserver directory for this spec)

Characteristics of the Universal Subscriber Identity Module (USIM) application

TSG / WG responsible: C6 (click TSG/WG to see its home page)

Work item which gave rise to this spec: - (click WI code to see Work Item details in the Work Plan)

CP-27: change of WG as a result of closure of CN and T. RP-33: additional editor: PERIN, Enrico (Axalto). RP-36: joint rapporteur: Stephane Andrau.

Rapporteur: **SEIF, Jacques**

Specification required for: UTRAN-based systems

In the table below ...

... click meeting number for meeting details;

... click spec version number to download that version;

... click SDO publication reference to download SDO transposed document.

Release	Freeze meeting	Freeze date	remarks	SDO publications
R99	SP-06	1999-12-17	.	ETSI
	event	version	available	remarks	click ref to download
	TP-03	0.0.0	1999-04-23		-
	TP-04	0.5.0	1999-06-23		-
	TP-05	1.0.0	1999-10-08		-
	TP-06	3.0.0	1999-12-17		DTS/TSGT-0331102U
	TP-07 completion target	3.1.0	2000-03-15		RTS/TSGT-0331102UR1
	TP-08	3.2.0	2000-06-23		RTS/TSGT-0331102UR2
	TP-09	3.3.0	2000-10-18		RTS/TSGT-0331102UR3
	TP-10	3.4.0	2001-01-05		RTS/TSGT-0331102UR4
	TP-11	3.5.0	2001-04-09		RTS/TSGT-0331102UR5
	TP-12	3.6.0	2001-07-06		RTS/TSGT-0331102UR6
	TP-13	3.7.0	2001-10-11		RTS/TSGT-0331102UR7
	TP-14	3.8.0	2002-01-17		RTS/TSGT-0331102UR8
	TP-16	3.9.0	2002-06-28		RTS/TSGT-0331102v390
	TP-17	3.10.0	2002-09-25		RTS/TSGT-0331102v3a0
	TP-18	3.11.0	2003-01-02		RTS/TSGT-0331102v3b0
	TP-19	3.12.0	2003-04-01		RTS/TSGT-0331102v3c0
	TP-20	3.13.0	2003-06-23		RTS/TSGT-0331102v3d0
	TP-21	3.14.0	2003-09-30		RTS/TSGT-0331102v3e0

	TP-22	3.15.0	2004-01-12		RTS/TSGT-0331102v3f0
	TP-23	3.16.0	2004-03-25		RTS/TSGT-0331102v3g0
	TP-24	3.17.0	2004-06-15		RTS/TSGT-0331102v3h0
	CP-28	3.18.0	2005-06-14		RTS/TSGC-0631102v3i0
Rel-4	SP-11	2001-03-22	.		ETSI
	event	**version**	**available**	**remarks**	**click ref to download**
	TP-11	4.0.0	2001-04-09		RTS/TSGT-0331102Uv4
	TP-12	4.1.0	2001-07-23		RTS/TSGT-0331102Uv4R1
	TP-13	4.2.0	2001-10-11		RTS/TSGT-0331102Uv4R2
	TP-14	4.3.0	2002-01-17		RTS/TSGT-0331102Uv4R3
	TP-15	4.4.0	2002-03-28		RTS/TSGT-0331102Uv4R4
	TP-16	4.5.0	2002-06-28		RTS/TSGT-0331102v450
	TP-17	4.6.0	2002-09-25		RTS/TSGT-0331102v460
	TP-18	4.7.0	2003-01-02		RTS/TSGT-0331102v470
	TP-19	4.8.0	2003-04-01		RTS/TSGT-0331102v480
	TP-20	4.9.0	2003-06-23		RTS/TSGT-0331102v490
	TP-21	4.10.0	2003-09-30		RTS/TSGT-0331102v4a0
	TP-22	4.11.0	2004-01-12		RTS/TSGT-0331102v4b0
	TP-23	4.12.0	2004-03-25		RTS/TSGT-0331102v4c0
	TP-24	4.13.0	2004-06-15		RTS/TSGT-0331102v4d0
	TP-26	4.14.0	2005-01-06		RTS/TSGT-0331102v4e0

	CP-28	4.15.0	2005-06-14		RTS/TSGC-0631102v4f0
Rel-5	TP-15	2002-03-08	.		ETSI
	event	**version**	**available**	**remarks**	**click ref to download**
	TP-15	5.0.0	2002-03-28		RTS/TSGT-0331102Uv5
	TP-16	5.1.0	2002-06-28		RTS/TSGT-0331102v510
	TP-17	5.2.0	2002-09-25		RTS/TSGT-0331102v520
	TP-18	5.3.0	2003-01-02		RTS/TSGT-0331102v530
	TP-19	5.4.0	2003-04-01		RTS/TSGT-0331102v540
	TP-20	5.5.0	2003-06-23		RTS/TSGT-0331102v550
	TP-21	5.6.0	2003-09-30		RTS/TSGT-0331102v560
	TP-22	5.7.0	2004-01-12		RTS/TSGT-0331102v570
	TP-23	5.8.0	2004-03-25		RTS/TSGT-0331102v580
	TP-24	5.9.0	2004-06-15		RTS/TSGT-0331102v590
	TP-25	5.10.0	2004-09-27		RTS/TSGT-0331102v5a0
	TP-26	5.11.0	2005-01-06		RTS/TSGT-0331102v5b0
	TP-27	5.12.0	2005-03-24		RTS/TSGC-0631102v5c0
	CP-28	5.13.0	2005-06-15		RTS/TSGC-0631102v5d0
	CP-29	5.14.0	2005-10-10		RTS/TSGC-0631102v5e0
Rel-6	TP-26	2004-12-10	TP-26: not yet ready to freeze. .		ETSI
	event	**version**	**available**	**remarks**	**click ref to download**
	TP-18	6.0.0	2003-01-02		-
	TP-19	6.1.0	2003-04-01		-
	TP-20	6.2.0	2003-06-23		-

	TP-21	6.3.0	2003-09-30		RTS/TSGT-0331102v630
	TP-22	6.4.0	2004-01-12		RTS/TSGT-0331102v640
	TP-23	6.5.0	2004-03-25		-
	TP-24	6.6.0	2004-06-24		-
	TP-25	6.7.0	2004-10-07		-
	TP-26	6.8.0	2005-01-06		RTS/TSGT-0331102v680
	TP-27	6.9.0	2005-03-24		RTS/TSGC-0631102v690
	CP-28	6.10.0	2005-06-14	CR269r1 accidentally implemented here (should have been Rel-7)	RTS/TSGC-0631102v6a0
	CP-29	6.11.0	2005-10-10		RTS/TSGC-0631102v6b0
	CP-30	6.12.0	2005-12-15		RTS/TSGC-0631102v6c0
	CP-31	6.13.0	2006-03-31		RTS/TSGC-0631102v6d0
	CP-32	6.14.0	2006-06-12		RTS/TSGC-0631102v6e0
	CP-33	6.15.0	2006-10-03		RTS/TSGC-0631102v6f0
	CP-34	6.16.0	2006-12-11		RTS/TSGC-0631102v6g0
	CP-35	6.17.0	2007-03-20		RTS/TSGC-0631102v6h0
	CP-36	6.18.0	2007-06-12		RTS/TSGC-0631102v6i0
	CP-36	6.18.1	2007-06-21	Correction to implementation of '0x' as '04' in 7.1.2.5 (MCC)	RTS/TSGC-0631102v6i1
	CP-37	6.19.0	2007-09-26		RTS/TSGC-0631102v6j0
Rel-7	CP-35	2007-03-09	. .		ETSI
	event	**version**	**available**	**remarks**	**click ref to download**
	TP-27	7.0.0	2005-03-24		-
	CP-28	7.1.0	2005-06-14	CR269r1 accidentally not implemented.	-
	CP-29	7.2.0	2005-10-10		-

	CP-30	7.3.0	2005-12-15		RTS/TSGC-0631102v730
	CP-31	7.4.0	2006-03-31		RTS/TSGC-0631102v741
	post CP-31 edito	7.4.1	2006-04-28		RTS/TSGC-0631102v741
	CP-32	7.5.0	2006-06-12		RTS/TSGC-0631102v750
	CP-33	7.6.0	2006-10-03		RTS/TSGC-0631102v760
	CP-34	7.7.0	2006-12-11		RTS/TSGC-0631102v770
	CP-35	7.8.0	2007-03-20		RTS/TSGC-0631102v780
	CP-36	7.9.0	2007-06-12		RTS/TSGC-0631102v790
	CP-36	7.9.1	2007-06-21	Correction to implementation of '0x' as '04' in 7.1.2.5 (MCC)	RTS/TSGC-0631102v791
	CP-37	7.10.0	2007-09-26		RTS/TSGC-0631102v7a0
	CP-38	7.11.0	2007-12-21		RTS/TSGC-0631102v7b0
Rel-8		-		. .	ETSI
	event	**version**	**available**	**remarks**	**click ref to download**
	CP-38	8.0.0	2007-12-21		-

Change Requests for this spec: click here.

Genealogy of this spec:

antecedent(s)	this spec	descendant(s)
(no antecedents)	31.102	(no descendants)

---

page generated from database: 2008-01-02 08:28:06

APPENDIX X

www.3gpp.org / ftp / specs / archive / 23_series / 23.057

Download

	sort by name/desc	sort by date/desc	sort by size/desc
	23057-150.zip	1999/10/25 12:58	177,9 KB
	23057-300.zip	2000/01/05 11:45	200,7 KB
	23057-320.zip	2000/07/10 15:05	207,1 KB
	23057-330.zip	2000/10/16 13:39	210,2 KB
	23057-340.zip	2001/03/27 9:49	217,1 KB
	23057-400.zip	2000/12/22 7:53	317,1 KB
	23057-410.zip	2001/04/10 16:29	316,8 KB
	23057-420.zip	2001/07/05 7:24	342,4 KB
	23057-430.zip	2001/10/05 12:46	345,6 KB
	23057-431.zip	2001/10/18 8:52	348,4 KB
	23057-440.zip	2002/01/16 16:24	354,8 KB
	23057-450.zip	2002/03/25 8:04	354,6 KB
	23057-500.zip	2002/03/25 8:07	363,8 KB
	23057-510.zip	2002/09/18 9:39	363,8 KB
	23057-600.zip	2002/06/28 9:11	403,2 KB
	23057-610.zip	2002/09/18 9:40	405,9 KB
	23057-620.zip	2003/10/14 7:48	412,6 KB
	23057-700.zip	2007/06/13 15:09	385,1 KB
	23057-800.zip	2008/12/16 20:43	522,1 KB
	23057-900.zip	2009/12/11 1:18	521,6 KB
	23057-a00.zip	2011/03/29 11:20	531,4 KB
	23057-b00.zip	2012/09/17 13:17	423,6 KB
	23057-c00.zip	2014/09/17 16:08	405,2 KB
	23057-d00.zip	2015/12/15 15:15	377,2 KB
	23057-e00.zip	2017/03/15 18:41	376,6 KB
	23057-f00.zip	2018/06/21 5:26	376,9 KB
	23057-g00.zip	2020/07/09 6:17	387,2 KB
	23057-h00.zip	2022/03/30 7:40	444,2 KB
	23057-i00.zip	2024/04/03 5:11	444,4 KB
	23057-j00.zip	2025/10/06 11:14	447,1 KB

30 items.

APPENDIX Y

INTERNET ARCHIVE
Wayback Machine
http://www.3gpp.org/ftp/Specs/archive/23_series/23.057/
Go
50 captures
11 Jan 2002 - 15 Jan 2026
MAY 2006 NOV 23 2007 JAN 2008
About this capture

www.3gpp.org - /ftp/Specs/archive/23_series/23.057/

[To Parent Directory]

25 October 1999	12:58	182178	23057-150.zip
05 January 2000	11:45	205561	23057-300.zip
10 July 2000	15:05	212136	23057-320.zip
16 October 2000	13:39	215251	23057-330.zip
27 March 2001	09:49	222391	23057-340.zip
22 December 2000	07:53	324777	23057-400.zip
10 April 2001	16:29	324428	23057-410.zip
05 July 2001	07:24	350686	23057-420.zip
05 October 2001	12:46	353992	23057-430.zip
18 October 2001	08:52	356832	23057-431.zip
16 January 2002	16:24	363405	23057-440.zip
25 March 2002	08:04	363125	23057-450.zip
25 March 2002	08:07	372627	23057-500.zip
18 September 2002	09:39	372609	23057-510.zip
28 June 2002	09:11	412929	23057-600.zip
18 September 2002	09:40	415670	23057-610.zip
14 October 2003	07:48	422604	23057-620.zip
13 June 2007	15:09	394398	23057-700.zip

APPENDIX Z

ETSI TS 123 057 V7.0.0 (2007-06)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Mobile Execution Environment (MExE);
Functional description;
Stage 2
(3GPP TS 23.057 version 7.0.0 Release 7)



Reference
RTS/TSGS-0223057v700

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2007.
All rights reserved.

DECT™, **PLUGTESTS**™ and **UMTS**™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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 (http://webapp.etsi.org/IPR/home.asp).

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.

Contents

Intellectual Property Rights 2
Foreword 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 33
6.4 Handling of MExE executables when their valid root public key is not available 34
6.4.1 Launching of MExE executables when their valid RPK is not available 35
6.4.2 Currently executing secure MExE executables when their valid RPK is no longer available 35
6.5 User permission types 35
6.6 Root Public keys 36
6.6.1 Operator root public key 36
6.6.1.1 Caching of root public keys 37
6.6.1.2 MExE device actions on detection of valid (U)SIM application and/or power up 37
6.6.2 Manufacturer root public key 39
6.6.3 Third party root public key 39
6.7 Certification and authorisation architecture 40
6.7.1 Certification requirements 40
6.7.1.1 MExE terminal requirements for certificate processing 40
6.7.2 Certification administration requirements 41
6.7.3 Example certification process 41
6.7.4 Certificate Chain Verification 42
6.8 Usage of Signed Content 44
6.8.1 Signed packages used for installation 44
6.8.2 Installation of root certificates in a signed data package 45
6.8.3 Installation of other signed data 45
6.9 Certificate Format 46
6.9.1 Certificate extension for removal of network access 46
6.9.1.1 X.509 version 3 46
6.10 Certificate management 46
6.10.1 Certificate configuration message (CCM) 47
6.10.1.1 CCM numbering convention 50
6.10.1.2 CCM order of transmission 50
6.10.1.3 CCM field mapping convention 50
6.10.1.4 Authorised CCM download mechanisms 50
6.11 Separation of I/O streams 50
6.12 Core software download 51
6.13 Administrator Concept 51
6.13.1 Administrator root public key 51
6.13.2 Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device 52
6.13.3 MExE administrator determination mechanism 52
6.13.3.1 Determining the administrator of the MExE device 52
6.13.3.2 Determining the administrator of the MExE device, for MExE-(U)SIM supporting third party certificates 53
6.13.3.2.1 Administrator of the MExE device is the user 53
6.13.3.2.2 Administrator of the MExE device is not the user 54
6.13.4 Administrator root certificate download mechanism 55

7 MExE Classmark 1 (WAP environment) 56
7.1 Introduction 56
7.1.1 WAP MExE devices 56
7.1.2 High level architecture 56
7.2 Non Security 56
7.2.1 WAP components 56
7.2.2 Services 57
7.2.2.1 User interface 57
7.2.2.2 Access points 57
7.2.2.3 Transferring 58
7.2.2.3.1 WSP and HTTP/1.1 Proxy Function 58
7.2.3 WAP charging support 59

7.2.4 CC/PP over WSP (Classmark 1) 59
7.3 Security 59
7.3.1 Call control 59
7.3.2 Local phonebook 59

8 MExE Classmark 2 (PersonalJava environment) 59
8.1 Introduction 59
8.1.1 Classmark 2 MExE devices 60
8.1.2 High level architecture 60
8.2 Non Security 60
8.2.1 High level functions 60
8.2.1.1 Optional Java packages 60
8.2.1.2 Required and optional PersonalJava APIs 61
8.2.1.3 Required and optional JavaPhone APIs 61
8.2.1.3.1 Application installation 62
8.2.1.3.2 Power 62
8.2.1.3.3 Datagram recipient addressing 62
8.2.1.4 Required and optional MExE PersonalJava APIs 62
8.2.1.5 Mandated services and applications 63
8.2.1.5.1 Network protocol support 63
8.2.2 CC/PP over HTTP (Classmark 2) 63
8.2.3 Java charging support 63
8.3 Security 63
8.3.1 PersonalJava security 63
8.3.1.1 Java applet certification in PersonalJava 63
8.3.1.2 Java application signature verification in PersonalJava 63
8.3.1.3 Java loading native libraries in PersonalJava 64
8.3.2 Installing MExE native libraries 64

9 MExE Classmark 3 (J2ME CLDC environment) 64
9.1 Introduction 64
9.1.1 Classmark 3 MExE devices 64
9.1.2 High level architecture 64
9.1.3 High level functionality 65
9.2 Non Security 65
9.2.1 Connected Limited Device Configuration (CLDC) 65
9.2.2 Mobile Information Device Profile (MIDP) 65
9.2.2.1 Networking 66
9.2.2.2 MID Applications (MIDlet) 66
9.2.2.3 MIDlet Suites 66
9.2.2.4 Record Storage 66
9.2.3 Required and optional MExE APIs 66
9.2.4 Service discovery and management 66
9.2.5 Transfer of capability negotiation information in Classmark 3 67
9.3 Security 67
9.3.1 CLDC security 67

10 MExE classmark 4 (CLI Compact environment) 67
10.1 Introduction 67
10.1.1 High level architecture 68
10.2 Non security 68
10.2.1 High level functionality 68
10.2.2 Network protocol support 69
10.2.3 Power Management 69
10.2.4 CLI charging support 69
10.2.5 CC/PP over HTTP or WSP (Classmark 4) 69
10.3 Security 70
10.3.1 CLI Security 70

Annex A (normative): MExE profile of PKCS#15 71

A.1 PKCS#15 certificate object attributes presentation 71
A.1.1 Object common attributes 71

A.1.2 Certificate common attributes 71
A.1.3 Certificate attributes 71
A.1.4 Specific X.509 certificate attributes 71
A.2 MExE profile of PKCS#15 71
A.3 Coding and storage in MExE-(U)SIM 72
Annex B (informative): PKCS#15 certificate objects ASN1 expanded syntax extract 73
Annex C (normative): Access restriction certificate extension 75
Annex D (informative): MExE executable life cycle 76
D.1 State of a MExE executable 76
D.2 Released state 78
D.3 Uninstalled Execution state 79
D.4 Verification 80
Annex E (informative): MExE conformance requirements 81
Annex F (informative): Change history 85
History 86

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] Hypertext Transfer Protocol – HTTP/1.1, IETF document RFC2616, 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.

[16] Composite Capability/Preference Profiles (CC/PP):A user side framework for content negotiation; http://www.w3.org/Mobile/CCPP.

[17] UAProf Specification http://www.wapforum.org/what/technical.htm.

[18] JDK 1.1 security http://www.javasoft.com/products/jdk/1.1/docs/guide/security/index.html.

[19] Java 2 security http://www.javasoft.com/products/jdk/1.2/docs/guide/security/index.html.

[20] Java security tutorial http://java.sun.com/docs/books/tutorial/security1.2/overview/index.html.

[21] OCF 1.1.: "Smartcard API specified by OpenCard Consortium http://www.opencard.org.

[22] RFC 1738: "Uniform Resource Locators (URL)" http://www.w3.org/pub/WWW/Addressing/rfc1738.txt.

[23] The MD5 Message Digest Algorithm", Rivest, R., RFC 1321, April 1992. URL: ftp://ftp.isi.edu/in-notes/rfc1321.txt.

[24] ISO/IEC 10118-3 (1996): "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions".

[25] IETF RFC 2368: "The mailto URL scheme".

[26] ITU-T Recommendation X.509: "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".

[27] 3GPP TS 51.011: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM - ME) interface".

[28] 3GPP TS 23.107: "QoS Concept and Architecture".

[29] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General Aspects".

[30] 3GPP TS 24.008: "Mobile radio interface layer 3 specification, Core Network Protocols; Stage 3".

[31] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[32] PKCS #15 "Cryptographic Token Information Syntax Standard" version 1.1, RSA Laboratories, June 2000
URL: ftp://ftp.rsa.com/pub/pkcs/pkcs-15/pkcs-15v1_1.doc.

[33] RFC 2510 (1999): "Internet X.509 Public Key Infrastructure Certificate Management Protocols".

[34] Connected Limited Device configuration, J2ME version 1.0, http://java.sun.com/j2me/docs/.

[35] Mobile Information Device Profile, J2ME version 1.0, http://java.sun.com/j2me/docs/.

[36] eXtensible Markup Language (XML) 1.0, W3C Recommendation.
URL: http://www.w3.org/XML.

[37] Resource Definition Framework (RDF) Model and Syntax, W3C Recommendation.
URL: http://www.w3.org/RDF.

[38] UML Partners: Unified Modelling Language. URL: http://www.omg.org.

[39] 3GPP TS 31.102: "Characteristics of the USIM applications".

[40] RFC 2396 (1998): "Uniform Resource Identifiers (URI): Generic Syntax". T. Berners-Lee, R. Fielding, L. Masinter.

[41] RFC 2616 (1999): "Hypertext Transfer Protocol -- HTTP/1.1". R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee.

[42] Description of the "JAR Manifest" file encoding, Sun Microsystems. URL: http://java.sun.com/j2se/1.3/docs/guide/jar/jar.html

[43] RFC 2459 (1999): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". R. Housley, W. Ford, W. Polk, D. Solo.

[44] 3GPP TR 21.905: Vocabulary for 3GPP Specifications.

[45] WAP Binary XML Content Format Specification (WBXML), http://www.wapforum.org/what/technical.htm.

[46] RFC 1766: "Tags for the Identification of Languages".

[47] WAP Certificate and CRL Profiles, WAP-211-WAPCert http://www.wapforum.org/what/technical.htm.

[48] 3GPP TS 23.227 “Applications and User interaction in the UE-Principles and specific requirements”.

[49] PKCS#1 “RSA Cryptographic Standard” " version 2.0, RSA Laboratories, October 1998 URL: http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html.

[50] Common Language Infrastructure, ECMA specification ECMA-335, http://www.ecma.ch/ecma1/STAND/ecma-335.htm.

[51] Simple Object Access Protocol version 1.1, (SOAP), URL : http://www.w3.org/TR/2000/NOTE-SOAP-20000508/.

[52] PKCS#7 “Cryptographic Message Syntax Standard” " version 1.5, RSA Laboratories, November 1993 URL: http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

administrator: administrator of the MExE device is the entity that has the control of the third party trusted domain, and all resources associated with the domain

NOTE 1: The administrator of the MExE device could be the user, the operator, the manufacturer, the service provider, or a third party as designated by the owner of the MExE device.

best effort QoS (Quality of Service): best effort QoS refers to the lowest of all QoS traffic classes

NOTE 2: If the guaranteed QoS cannot be delivered, the bearer network delivers the QoS which can also be called best effort QoS [28].

certificate: entity that contains the issuer's public key, identification of the issuer, identification of the signer, and possibly other relevant information

NOTE 3: Also, a certificate contains a signed hash of the contents. The signer can be a 3rd. party other than the issuer.

delivered QoS: actual QoS parameter values with which the content was delivered over the lifetime of a QoS session [28].

End Entity: user of PKI certificates and/or end user system that is the subject of a certificate.

fine grain: refers to the capabilities of the Java security system to allow applications, sections of code or Java classes to be assigned permissions to perform a specific set of privileged operations

NOTE 4: The smallest programming element that can be given permission attributes is a Java class [19].

key pair: key pairs are matching private and public keys

NOTE 5: If a block of data is encrypted using the private key, the public key from the pair can be used to decrypt it. The private key is never divulged to any other party, but the public key is available, e.g. in a certificate.

Operator: term operator as used in this specification refers to the term Home Environment, defined as "Home Environment: The home environment is responsible for enabling a user to obtain UMTS services in a consistent manner regardless of the user's location or terminal used (within the limitations of the serving network and current terminal)" in [44].

negotiated QoS: response to a QoS request, the network shall negotiate each QoS attribute to a level that is in accordance with the available network resources

NOTE 6: After QoS negotiation, the bearer network shall always attempt to provide adequate resources to support all of the negotiated QoS profiles [31].

personal certificate: certificate loaded by the user or a user application which is limited to the application that it is intended for, and is not a MExE Certificate

NOTE 7: E.g. an e-mail application could load certificates for its usage. Personal certificates are out of scope for MExE.

phonebook: dataset of personal or entity attributes

NOTE 8: The simplest form is a set of name-number pairs as defined by GSM SIMs. A phonebook may also be supported on a (U)SIM.

Mobile Execution Environment (MExE): is defined in detail in the present document, but the scope of MExE does not include the operating system, or the manufacturer's execution environment

MExE API: consists of interfaces present in the MExE device and exposed to MExE executables

NOTE 9: The APIs which are outside of the scope of this specification, are not part of MExE API.

MExE certificate: used in the realisation of MExE security domains

NOTE 10: A MExE Certificate can be used to verify downloaded MExE executables. Use of the word "certificate" in this document implies a MExE certificate. Other varieties of certificate will be explicitly qualified as a e.g. "Personal Certificate".

MExE device: UE (User Equipment) that supports MExE functionality in the ME (Mobile Equipment)

NOTE 11: The implementation of MExE shall be in the same physical device as the MT (Mobile Termination). Implementation of MExE functionality in the TE (Terminal Equipment) outside of the physical device containing the MT (Mobile Termination) is for further study.

MExE executable: is one or more applet, application, or content, which conforms to the MExE specification and may execute on any MExE device, conforming to the appropriate classmark

MExE Java VM: this is a standard Java virtual machine used to execute MExE Java applets and applications

MExE native library: this is a downloaded native library that can be accessed by MExE executables

MExE Server: node supporting MExE services in the MExE service environment

NOTE 12: The MExE server may be a web or WAP server providing services for users to download MExE executables. MExE server is not necessarily a special network element but may utilize the normal Internet service environment.

MExE-(U)SIM: (U)SIM that is capable of storing a security certificate that is accessible using standard mechanisms

MIDP application: MIDP application, or "MIDlet", is one that uses only the APIs defined by the MIDP and CLDC specifications.

MIDlet suite: collection of MIDP Applications, or MIDlets packaged together and share resources within the context of a single Java Virtual Machine

owner: owner of the MExE device

NOTE 13: An owner could be a user, operator (e.g. where the MExE device is obtained as part of a subscription and the cost of the MExE device is subsidised), service provider, or a third party (e.g. the MExE device is owned by the user's company and this company wishes to control how the MExE device is used)

power up event: abstract event that occurs when the MExE device is cold started (i.e. switched on)

QoS session: Lifetime of PDP context, the period between the opening and closing of a network connection whose characteristics are defined by a QoS profile

NOTE 14: Multiple QoS sessions may exist, each with a different QoS profile [28].

QoS profile: comprises of a number of QoS parameters

NOTE 15: A QoS profile is associated with each QoS session. The QoS profile defines the performance expectations placed on the bearer network [28].

requested QoS: QoS profile is requested at the beginning of a QoS session

NOTE 16: QoS modification requests are also possible during the lifetime of a QoS session [28] and [31].

sandbox: sandbox is a safe area to run Java code. Untrusted Java code executing in a sandbox has access to only certain resources [18].

service: service (which may consist of an application or applet, and its related content) is a set of functions offered to a user by an organisation, and may be performed on the MExE device and/or remotely

service name: identifier associated with a service, which could be a string, a fully qualified Java class name, a unique URI or other identifier

session: period between the launching of a MExE executable and its execution termination

NOTE 17: A WAP-session is established between the mobile and the WAP Gateway. The duration of a WAP-session can range from a second to years. The WAP-session can be associated with a particular subscription in the WAP Gateway.

signature: "Signing" is the process of encrypting a hash of the data using a private key

NOTE 18: If the signature can be decrypted using the public key, then the signature is valid.

signed JAR file: archives of Java classes or data that contain signatures that also include a way to identify the signer in the manifest [42] (the Manifest contains a file which has attributes defined in it)

subscribed QoS: network will not grant a QoS greater than that subscribed

NOTE 19: The QoS profile subscription parameters are held in the HLR. An end user may have several QoS subscriptions. For security and the prevention of damage to the network, the end user cannot directly modify the QoS subscription profile data [31].

user: user of the MExE device

valid (U)SIM application: identification by the MExE ME that a valid SIM card, or USIM application on the UICC, has been detected (e.g. through insertion of (U)SIM card, power up of MExE device etc.)

NOTE 20: Whenever this specification refers to valid (U)SIM, it implies a valid SIM card or USIM application on the UICC.

Further definitions specific to MExE are given in TS 22.057 [2].

3.2 Abbreviations

For the purposes of the present document the following abbreviations apply:

AA	Attribute Authority
API	Application Programming Interface
APDU	Application protocol data unit

ARPK	Administrator Root Public Key
CA	Certification Authority
CC/PP	Composite Capability/Preference Profiles
CGI	Common Gateway Interface
CCM	Certificate Configuration Message
CLDC	Connected Limited Device Configuration
CLI	Common Language Infrastructure
CP-Admin	Certificate Present (in the MExE (U)SIM) - Administrator
CP-TP	Certificate Present (in the MExE (U)SIM) - Third Party
CRL	Certificate Revocation List
Diff-serv	Differentiated Services
DTMF	Dual Tone Multiple Frequency
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transport Protocol Secure (https is http/1.1 over SSL, i.e. port 443)
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
JAD	Java Application Descriptor
J2ME	Java 2 Micro Edition
J2SE	Java 2 Standard Edition
JTAPI	Java Telephony Application Programming Interface
JAR file	Java Archive File
ME	Mobile Equipment
MIDP	Mobile Information Device Profile
MIDlet	MIDP Application
MMI	Man-Machine Interface
MRPK	Manufacturer Root Public Key
MSE	MExE Service Environment
MSISDN	Mobile Subscriber ISDN Number
MT	Mobile Termination
OCF	OpenCard Framework
OEM	Original Equipment Manufacturer
OCSP	Online Certificate Status Protocol
ORPK	Operator Root Public Key
QoS	Quality of Service
PDP	Packet Data Protocol
PKI	Public Key Infrastructure
RDF	Resource Description Format
RFC	Request For Comments
RPK	Root Public Key
SCVP	Simple Certificate Verification Protocol
SIM	Subscriber Identity Module
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TE	Terminal Equipment
TLS	Transport Layer Security
TP	Third Party
UDP	User Datagram Protocol
UE	User Equipment
UI	User Interface
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
USIM	Universal Subscriber Identity Module
USSD	Unstructured Supplementary Service Data
VM	Virtual Machine
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WBXML	WAP Binary XML

WDP	Wireless Datagram Protocol
WMLS	Wireless Markup Language Script
WSP	Wireless Session Protocol
WTA	Wireless Telephony Applications
WTAI	Wireless Telephony Applications Interface
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol
WWW	World Wide Web
XML	Extensible Markup Language

Further abbreviations are given in 3GPP TS 22.057 [2] and 3GPP TR 21.905 [44].

4 MExE basic principles

4.1 Generic MExE aspects

Support of at least one MExE classmark is mandatory. A MExE device may also include optional support for applications from any other MExE classmark (refer to clause 4.3 “Multiple Classmark support”).

This clause defines the common aspects of all MExE compliant devices, independent of MExE technology.

Considering the wide and diverse range of current and future technology and devices that (will) use wireless communication and provide services based thereon a one-size-fits-all approach is unrealistic. Instead the present document categorises devices by giving them different MExE classmarks. In this specification the following MExE classmarks are defined:

- MExE classmark 1 - based on WAP (Wireless Application Protocol) [6] - requires limited input and output facilities (e.g. as simple as a 3 lines by 15 characters display and a numeric keypad) on the client side, and is designed to provide quick and cheap information access even over narrow and slow data connections.

- MExE classmark 2 - based on PersonalJava [3] - provides and utilises a run-time system requiring more processing, storage, display and network resources, but supports more powerful applications and more flexible MMIs.

- MExE classmark 3 – based on J2ME CLDC and MIDP environment [34] and [35] – supports Java applications running on resource-constraineddevices.

- MExE classmark 4 – based on Common Language Infrastructure [50] Compact Profile – supports CLI based applications running on a broad range of connected devices.

Content negotiation allows for flexible choice of formats available from a server or adaptation of a service to the actual classmark of a specific client device.

Bi-directional capability negotiation between the MExE Service Environment and MExE device (including MExE classmark), supports the transfer of capabilities between the client and the server.

4.2 High level architecture

The following architectural model shows an example of how standardised transport mechanisms are used to transfer MExE services between the MExE device and the MExE service environment, or to support the interaction between two MExE devices executing a MExE service.

The MExE service environment could, as shown in figure 1 "Generic MExE architecture", consist of several service nodes each providing MExE services that can be transferred to the MExE device using mechanisms such as (but not limited to) fixed/mobile/cordless network protocols, Bluetooth, infrared, serial links, wireless optimised protocols, standard Internet protocols. These service nodes may exist in the circuit switched domain, packet switched domain, IP multimedia core network subsystem or in the internet space (e.g. SMS service centres, multimedia messaging servers, internet servers etc.). The MExE service environment may also include a proxy server to translate content defined in standard Internet protocols into their wireless optimised derivatives.

For the versatile support of MExE services, the wireless network shall provide the MExE device with access to a range of bearer services on the radio interface to support application control and transfer from the MExE service environment. As MExE also applies to fixed and cordless environments, MExE device may also access MExE services via non-wireless access mechanisms.

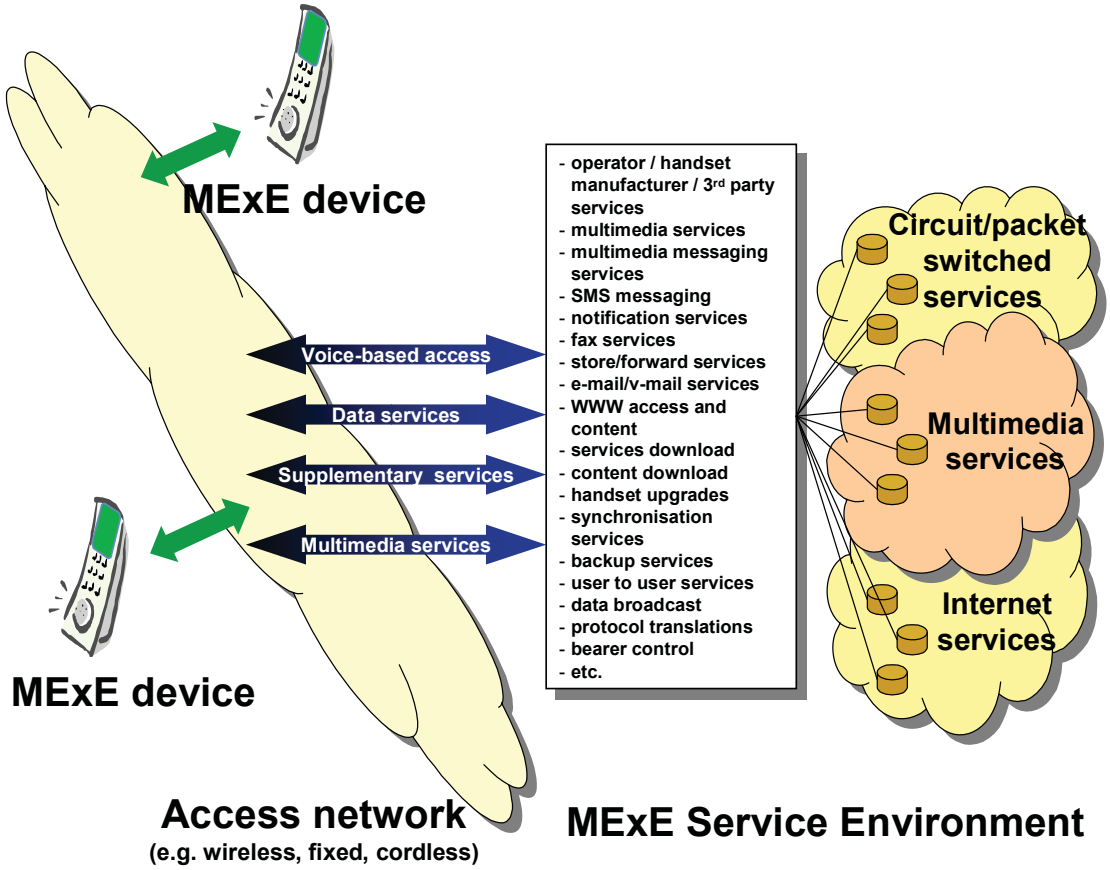


Figure 1: Generic MExE architecture

4.3 Multiple classmark support

Support of multiple MExE classmarks on a MExE device is optional.

A given MExE Classmark identifies support by a MExE device for a defined level of MExE functionality as defined by that classmark. Support of MExE classmarks by a MExE device shall enable flexible support of MExE functionality. A MExE device may support any multiple combinations of MExE classmarks.

The support of any other functionality by a MExE device is also possible, and is out of scope of this specification.

NOTE: Some implementation issues may arise from the multiple support of classmarks on a device, e.g.:

1) In conforming to all of the requirements, how are mandatory requirements in one classmark compatible with optional requirements for another?

2) With KJava and pJava on one device, MIDP can be on top of a JavaVM. Which of the classmarks will it be then? In conforming with both Classmark 2 and 3 requirements, are 2 VMs required in one device?

4.3.1 Classmark 1 service support in non-Classmark 1 MExE devices

Support of Classmark 1 executables in non-classmark 1 MExE devices is optional.

To allow access to services designed for MExE Classmark 1 devices, MExE devices other than Classmark 1 will need to support full or a subset of WAP protocol as identified below. Due to the fast evolution of new technologies, support of WAP in Classmarks other than Classmark 1 is not mandated by MExE specification. However WAP is a possibility for the integrity of service provisioning as well as quick access to information by feature rich devices (e.g. Java devices).

If Classmark 1 services are supported by non-Classmark 1 devices, Classmark 1 services shall execute in the same manner as they execute in a MExE Classmark 1 device. For that purpose, a MExE non-Classmark 1 device shall comply with data profile class (Class C) of WAP Class Conformance Requirement Specification [6].

NOTE: A more specific reference to the WAP Class Conformance Requirement Specification shall be supplied when available.

4.3.2 Classmark 2 service support in non-Classmark 2 MExE devices

Support of Classmark 2 executables in non-classmark 2 MExE devices is optional.

If Classmark 2 services are supported by non-Classmark 2 devices, Classmark 2 services shall execute in the same manner as they execute in a MExE Classmark 2 device.

4.3.3 Classmark 3 service support in non-Classmark 3 MExE devices

Support of Classmark 3 executables in non-classmark 3 MExE devices is optional.

If Classmark 3 services are supported by non-Classmark 3 devices, Classmark 3 services shall execute in the same manner as they execute in a MExE Classmark 3 device.

4.3.4 Classmark 4 service support in non-Classmark 4 MExE devices

Support of Classmark 4 executables in non-classmark 4 MExE devices is optional. If Classmark 4 services are supported by non-Classmark 4 devices, Classmark 4 services shall execute in the same manner as they execute in a MExE Classmark 4 device.

5 Generic MExE functions (excluding security)

5.1 User profile

Support of the user profile is optional.

NOTE: The user profile is not yet specified in an interoperable way. Support of the user profile will be defined when it has been fully specified in a fully interoperable way.

The user profile (which may consist of sub user profiles for a user) contains the characterisation of the MExE device as defined by the user and service provider. Further, it is also possible for multiple users of a MExE device to each have their own user profiles. The user profile is not unique to the MExE device, and this clause identifies the usage and content of the user profile from a MExE perspective only, and does not identify the generic support of user profiles in general. Refer to TS 22.101 [14] for further details on the user profile.

5.1.1 Location of, access to, and security of, the user profile

As multiple user profiles may be defined, the user is able to set up or receive calls/connections associated with different user profiles simultaneously by securely activating a user profile (with each user profile being associated with at least one unique identifier). Refer to table 5 "Security domains and actions" in the Security clause 6.3 "MExE executable permissions" for further details on user profile activation.

The user's characterisation of the MExE device in the user profile may be modified at any time by the user and the service provider, and changes affected at the earliest possible opportunity.

The security clause shall apply to all user profiles at all times, whether activated or not

The user profile shall be securely managed by the MExE device, and stored in a secure area of the MExE device (either (U)SIM or ME). The service provider may also retain the user profile in the network for service optimisation. User private data in the user profile may also be stored in the network, however only with the user permission.

The support of more than one user profile is not mandatory.

5.1.2 Support of the user profile

The user profile acts as a repository (which is always available in the MExE device) defining the MExE device behaviour.

MExE preferences and personalisation are supported in the user profile (e.g. UMTS portability and support of VHE defined in [12] and other 22-series specifications), which in turn is based on the Composite Capability/Preference Profile (CC/PP) specification from W3C [16].

MExE preferences and personalisation may not only be recorded directly in the user profile as supported by CC/PP (the direct referencing mechanism), but may also be retrieved from a URL (the indirect referencing mechanism) [22].

Generally, the user profile's CC/PP framework provides the mechanism for the standardised format of preferences, and its use of Resource Description Framework (RDF) permits the interoperable encoding of MExE preferences and personalisation. Future extensions will be supported by the W3C mechanism, allowing for evolution and development of MExE preferences and personalisation.

The set of preferences which are supported in the user profile consists of the following:

- user interface personalisation;
- the user's personalisation of the user interface;
- service personalisation and management;
- the user's generic service management information.

The coding and presentation of the above characteristics in the user profile is defined by the Composite Capability/Preference Profile (CC/PP) specification from W3C [16], and referenced by the MExE capability negotiation in clause 5.2 "Capability and content negotiation".

The following user preference information is supported by UAProf [17]. A MExE device shall support the following property in table 1 "Mandatory UAProf properties" of the UAProf schema for user preference information.

Table 1: Mandatory UAProf properties

Attribute	Description	Resolution Rule	Type	Sample Values
AcceptDownloadableSoftware	Indicates the user's preference on whether to accept downloadable software	Locked	Boolean	"Yes", "No"

It is recommended that a MExE device supports the following UAProf properties in table 2 "Recommended UAProf properties":

Table 2: Recommended UAProf properties

Attribute	Description	Resolution Rule	Type	Sample
CcppAccept-Language	User's preference for document language. Property value is a list of natural languages, where each item in the list is the name of a language as defined by RFC 1766 [46].	Append	Literal (Bag)	"zh-CN", "en fr"
PreferenceForFrames	User's preference for displaying frames	Locked	Boolean	"Yes", "No"
WapPushMsgPriority	User's settings for WAP Push message priorities	Locked	Literal	"critical", "low", "none"

Also, there is in UAProf [17] support for indicating MExE device's capabilities related to UI features, e.g. capability for displaying images or frames, as well as capability information about input and output methods.

5.1.3 User interface personalisation

Support of user interface personalisation as detailed in this clause is optional.

The MExE device interface consists of the buttons, menus, screens and MMI as designed and provided by the MExE device manufacturer; the nature of this MExE device interface is naturally evolving, MExE device specific and proprietary to the individual manufacturers of the industry. This interface is the one normally seen by the user in normal operation of his MExE device. This specification does not place any requirements or limitations on the individual manufacturers' MExE device interface.

The MExE MMI, in turn, is the interface available to the user to support MExE services and functionality on the MExE device. The nature of the MExE MMI interface, like the normal MExE device interface described above, is not standardised in any way, to allow for manufacturer innovation, cater for evolving market needs, and permit manufacturer differentiation. The MExE MMI, depending on different manufacturer implementations, may consist of the normal MExE device interface, the normal MExE device interface with modifications, a different interface to the normal MExE device interface, or some combinations thereof etc. MExE services operate within, and using the capabilities of, the MExE MMI.

User interface personalisation consists of two parts. The first part refers to the user's ability to request, and verify, the preferred changes to the user interface; thus the user's preferences, as supported by the specific MExE device, require to be recorded. The second part refers to the MExE device's support of the user's preferences for the interface, within the capabilities of an MExE device. By defining the user interface personalisation to consist of two stages, the preferences which have been recorded by the user may be transferred (as part of the user profile, e.g. CcppAccept-Language and/or PreferenceForFrames), and thereby provide portability of the user's preferences.

5.1.3.1 MExE user interface personalisation

Personalisation of the user interface offers the MExE Service Environment and or the user, the ability to inform the MExE device of the desired extent of personalisation. All support of the user interface personalisation is optional, not mandatory on any class of MExE device, and subject to the capabilities of the MExE device. Depending on the capability of the MExE device, the personalisation may be fully supported, partially supported, interpreted or ignored.

Personalisation of the user interface is not restricted to modifying the appearance of the MMI, but also the modification of MMI parameters (e.g. programming of the voicemail number). The user's personalisation of the interface is retained as part of the user profile.

5.1.3.2 Support of MExE user interface personalisation

MExE user interface personalisation is supported via the preferences in the user profile, which in turn is based on the Composite Capability/Preference Profile (CC/PP) specification from W3C [16].

User interface personalisation may not only be reported in the CC/PP request to the server (the direct referencing mechanism), but indeed the client may point to a URL (the indirect referencing mechanism) from where the user interface personalisation preferences may be retrieved.

Generally, the user profile's CC/PP framework provides the mechanism for the standardised format of preferences, and its use of Resource Description Framework (RDF) permits the interoperable encoding of user interface personalisation. Future extensions will be supported by the W3C mechanism, allowing for evolution and development of MExE user interface personalisation.

5.1.4 Virtual home environment

Virtual Home Environment (VHE) (see [11] and [12]) is defined as a concept for personalised service portability across network boundaries and between terminals. MExE is identified by VHE as one of the mechanisms which may be used to support VHE.

The characteristics of the VHE (to reflect any user or home environment modification of the user's VHE) shall be stored as part of the user profile.

5.2 Capability and content negotiation

Support of capability negotiation for all MExE devices is mandatory, while support of content negotiation is optional.

Interaction between the MExE device and the MSE for WWW/WAP browsing and service discovery shall be supported by the use of the hypertext transfer protocol HTTP/1.1 [9], or an HTTP/1.1 derived protocol (e.g. WSP as defined in Wireless Application Protocol [6]). Communication between the MExE device and the MSE supports:

- Capability negotiation

  The MExE device connects to the MSE by using HTTP/1.1 or an HTTP/1.1 derived protocol. Capability negotiation between the MExE device and the MSE only takes place for the first time after the MExE device has connected to the MSE, and the MSE is informed about the MExE device. Without this first initial contact from the MExE device, the MSE has no knowledge of the MExE device. After the first initial contact the MSE may connect to the MExE device by using HTTP/1.1 or an HTTP/1.1 derived protocol.

  Capability negotiation represents the mechanism by which the MExE device and the MSE interact to inform each other of the specific mechanisms, capabilities and support which each is able to provide or support within the scope of a MExE service interaction. The capability negotiation normally takes place prior to any content transfer between the two entities.

  Capability negotiation is used by the MExE device to inform the MSE of its capabilities. The MExE device may be informed by the MSE of its use of the MExE device's capabilities. The MExE device may also spontaneously inform the MSE of its capabilities (i.e. following a change in MExE support, such as removal of MExE device from a docking station with its keyboard, mouse and monitor). A subset of characteristics which may be transferred between the MExE device and the MSE during the capability negotiation are identified in clause 5.2.1 "Capability negotiation characteristics".

- Content negotiation

  Content negotiation represents the means by which the MExE device and the MSE inform each other of the requested and available form of content. If needed, the content negotiation may take place following capability negotiation between the two. The methods for content negotiation are the basic HTTP/1.1. or WSP methods explained in [9] and [6].

  Content negotiation is used to select the best representation of an entity when there are multiple representations of the entity available from the MSE. The entity (e.g. a service, an image, etc) is located behind a URI, and the application in the MExE device connects to the URI by using HTTP/1.1 or an HTTP/1.1 derived protocol. The best representation of an entity can be decided by the server (server-driven negotiation) or by the client application (agent-driven negotiation).

Both the capability and the content negotiation has the same purpose: to optimise the content according to client's capabilities. The term "content negotiation" has been used e.g. in the HTTP specification and the HTTP/1.1. and the WSP contain headers to perform the content negotiation. However, the capability negotiation in MExE aims at extending the basic HTTP and WSP methods for content negotiation by using CC/PP framework.

The content negotiation transferred between the MExE device and the MSE is identified in clause 5.2.3 "Client content capability report" onwards.

5.2.1 User profile and capability negotiation relationship

The user profile contains the user's preferences. Support of the user's preferences will depend on the capabilities of the MExE device. If the capabilities change, then the degree of support of the user's preferences may change too.

The capability negotiation between the MExE device and the MSE, as shown in figure 2 "Model of user profile and capability relationship", contains those user preferences which the MExE device is able to support.

In this way the MSE will serve a MExE device with the lowest common denominator of the users preferences, the MExE device capabilities and the provided service characteristics and support the user's preferences to the maximum degree.

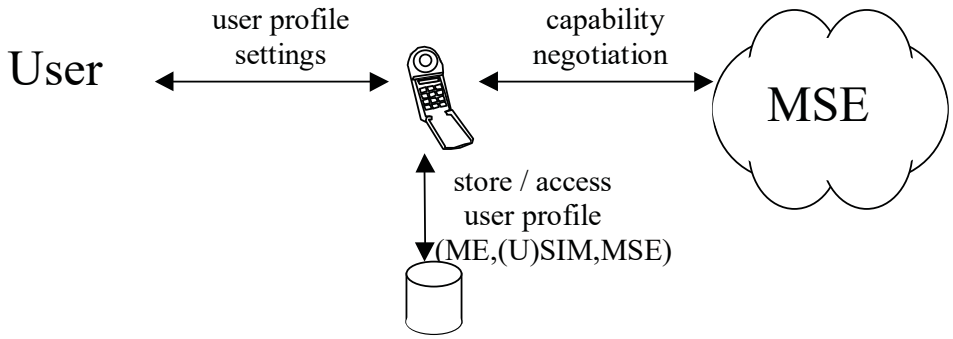


Figure 2: Model of user profile and capability relationship

5.2.2 Capability negotiation characteristics

The method for capability negotiation is based on the Composite Capability/ Preferences Profiles (CC/PP) specification made by W3C, [16]. The properties and the actual schema, table 3"UAProf properties supported by MExE", is based on the WAP UAProf specification [17]. The CC/PP framework is intended to provide an efficient mechanism for enabling enhanced content and service negotiation through a standardised format for user agent profiles. The use of Resource Description Framework (RDF) [37] in CC/PP allows for interoperable encoding of the profile metadata in XML[36] and supports multiple vocabularies to provide for future extensibility. The WAP UAProf is based on the CC/PP framework. The purpose of the UAProf outlined in this document is to specify:

- an RDF based schema and vocabulary for CC/PP in the context of the WAP UAProf that includes the class definitions and semantics of attributes described in a user agent profile, and
- guidelines for schema extensibility to support a composite profile that enables future additions to the vocabulary and schema.

Not all capabilities have to be reported in the request to the server but instead, the client may point to URL(s) where the server may fetch the properties. An MSE may, or may not, use the client capability information.

The generic set of capabilities which may be negotiated between the client and the server consists of the subsequently identified properties in the UAProf schema, [17].

A MExE device shall support the properties in the UAProf schema for capability negotiation defined in table 3 "UAProf properties supported by MExE" as "mandated properties".

It is recommended that MExE device supports the properties defined in the table 3"UAProf properties supported by MExE" as "recommended properties". It is not required that a MExE device shall send all the "recommended properties", when sending a request, however it should be possible for the MExE device to send one or more of the "recommended properties", with user permission.

The mandatory and recommended properties in table 3"UAProf properties supported by MExE" are specified in WAP UAProf [17].

Support of the properties of the UAProf schema in this specification shall not be limited to those listed in table 3 "UAProf properties supported by MExE". A MExE device may support any other properties from WAP UAProf specification [17].

Table 3: UAProf properties supported by MExE

Mandated Properties				
Attribute	Description		Type	Sample
MexeClassmarks	List of supported MExE classmarks (Note 1)		Literal (bag)	"1", "2", "3"
MexeSpec	The first two digits of the MExE Specification version that the MExE device conforms to		Literal	"3.3", "4.1"
MexeSecureDomains	Indicates whether the device supports the MExE security domains		Boolean	"Yes", "No"
Recommended Properties				
Vendor	MExE device vendor		Literal	"Lexus", "Ford"
Model	MExE device model number		Literal	"Mustang 90", "Q10"
SoftwareNumber	The number of the MExE device specific software.		Literal	"1.0", "2.7.0"
ScreenSize	The size of the MExE device's screen in units of pixels.		Dimension	"160x160", "640x480"
ScreenSizeChar	Size of the MExE device's screen in units of characters (based on the standard font).		Dimension	"12x4", "16x8"
ColorCapable	Whether the MExE device display supports colour		Boolean	"Yes", "No"
AudioInputEncoder	List of audio input encoders supported by the MExE device		Literal (bag)	"G.711"
VideoInputEncoder	List of video input encoders supported by the MExE device		Literal (bag)	"MPEG-1", "MPEG-2", "H.261"
PointingResolution	Type of resolution of the pointing accessory supported by the MExE device		Literal	"Character", "Line", "Pixel"
CcppAccept-Language	List of preferred document languages		Literal (bag)	"zh-CN" "en fr"
Keyboard	Type of keyboard supported by the MExE device as an indicator of ease of text entry.		Literal	"Disambiguating", "Qwerty", "PhoneKeypad"
SupportedBearers	List of bearers supported by the MExE device.		Literal (Bag)	"GPRS", "GUTS", "SMS", CSD", "USSD"
JavaPlatform	List of Java platforms and profiles installed on the device		Literal (Bag)	"Pjava/1.1.3-compatible", "MIDP1.0-compatible", "J2SE/1.0-compatible"
Proposed New Recommended Property				
CLIPlatform (Note 2)	List of CLI profiles installed on the device		Literal (Bag)	“CLI-Compact/1.0-compatible”, “CLI-Standard/1.0-compatible

NOTE 1: In pre-release 4.0.0 specifications the attribute MexeClassmark (as opposed to MexeClassmarks) which was a literal (as opposed to as Literal, Bag) indicating only one MExE classmark was notified.
NOTE 2: The property name “CLIPlatform” is proposed as a placeholder. Once a decision has been made the final property name will be proposed to UAProf for UAProf approval.

Generally, the combination of user profile and MExE device logic will determine the information sent in the capability negotiation from the MExE device to the MExE Service Environment. As an example, for the support of VideoInputEncoder information the user's profile controls if and when VideoInputEncoder information may be sent to the MExE Service Environment (e.g. never sent, always sent, only after user confirmation).

The capability negotiation process shall be used by the client to permit transfer of capabilities from the client to the server. By transferring its capabilities, the client will support efficient use of resources both over the radio interface as well as in the client or server. Capability negotiation shall be performed prior to transfer over the radio interface to verify as far as possible the ability of the client to support any services to be downloaded.

In order to transfer the capability information between the MExE device and the MSE, CC/PP method is used with the schema defined in the WAP UAProf working group.

5.2.3 Client content capability report

The client may perform content negotiation capabilities to the server by using appropriate HTTP/1.1 or WSP request headers. The following methods are available for content negotiation:

- Client software (product): `User-Agent` header;
- MIME media types: `Accept` header;
- Character set: `Accept-Charset` header;
- Content encoding: `Accept-Encoding` header;
- Language: `Accept-Language` header.

There is no need for MExE to specify any tokens for content negotiation, as these headers are already defined in HTTP and WSP. The formats for these headers are specified in [9] and [6].

5.2.4 Server role in capability negotiation

The server may request the capabilities of a client whenever required, and shall enquire of the client's capabilities prior to making each transaction resulting in a set of transfers to the client; the characteristics which may be reported in the client capability report are identified in the list above.

In server-driven negotiation the server signals to the client that the response entity was selected from a set of available representation.

5.2.5 Client-driven negotiation

If the server cannot specify an optimal version for the client basing on the CC/PP sent over to the server, the server may also indicate to client which type of versions are available and let the client make the decision. This method is already available in HTTP1.1. In client-driven negotiation the client selects the best representation after having received an initial response from the server.

5.3 Provisioning and management of services

Support of management of services as detailed in this clause is mandatory.

The MExE device shall be capable of supporting services in a standard (WAP or Java) execution environment independently of the MExE device manufacturer. Service provisioning provides a standardised method for a MExE device to discover and install services. It includes download and installation of the service's client application. Once discovered and delivered, services are managed by the user, under the principles stated in 3GPP TS 23.227 [48]. Management of services provides the user with the capability to:

- control the transfer of services;
- install and configure services;
- control the execution of services;
- terminate or suspend executing services;
- delete services;

on his MExE device.

5.3.1 Service discovery

A MExE user is able to request (or be informed about) the range of MExE services available from the MExE server to which it is connected. To be able to interactively discover the services via standard mechanisms such as WSP or HTTP, a MExE device should feature a browser which is a common tool for service discovery. The request, and transfer of information on MExE services from the MExE server is supported by the use of the capability negotiation mechanism.

All services available in the network continue to be available to the user, in addition to MExE services.

An example of an alternative means of receiving information on MExE services, is the use of an application on the MExE device which the user interrogates to provide services information (from various sources), and which in turn then obtains such information and presents it to the user. Such an example is not subject to standardisation.

5.3.2 Service transfer

The standardisation of the transferral of MExE services to a MExE device is outside the scope of this specification.

Examples of possible ways of supporting service transfer are from a MExE server or from another user MExE device (e.g. using wireless and standard protocols and mechanisms such as HTTP, FTP, proprietary protocols and mechanisms, via a serial link, infrared, Bluetooth data exchange, etc.).

The above examples are not exhaustive. Regardless of the means of transfer, all services are required to conform with the security requirements in clause 8 "Security".

5.3.3 Service installation and configuration

Installation of a service may result in changes to the MExE device user interface using icons, browsers or menus as applicable depending on the capability of the MExE device to support them. The name of the installed service may be contained in the package in which it was received (i.e. a JAR file or script), assigned by the user during configuration, or some other means. After installation, the service may be configured. Configuration of the service includes setting the user permissions that apply to the service (e.g. blanket permission for call origination). Configuration may be performed automatically based on the user profile.

The user controls whether a service transferred to the MExE device is automatically configured and installed in the MExE device. If automatic configuration and/or installation is enabled, the user is notified once it is completed. In the event that there is no authorisation for the automatic installation and/or configuration of a transferred service, the user is notified.

Subsequent user modification of a service's configuration (e.g. by modification of user profile settings) shall take effect at the earliest possible opportunity thereafter.

5.3.4 Service management

The MExE device shall support the ability to determine which services are transferred to, resident, installed or executing on the MExE device. The information relating to the services shall include the name as a minimum and the version number if available.

The user controls which services are permitted or denied to be transferred, resident, installed, configured or executing on the MExE device via the user profile, e.g. AcceptDownloadableSoftware. The user profile permits characteristics such as security level, identification of specific services etc. to manage services on the MExE device.

5.3.5 Service termination

A MExE device shall support the termination of services.

A service may terminate by itself, or be terminated by the provider of the service or by the user. The user is in charge of the service, except when the service provider may appropriately control the service as part of user support.

The mechanism for terminating a service is out of scope of standardisation and shall be provided on a service by service basis by the provider of the service.

5.3.6 Service deletion

A MExE device shall support the deletion of services.

A service may be deleted (i.e. removed) from the MExE device with the authorisation of the user. The deletion may be initiated by the authoriser of the service or by the user.

5.4 User control of application connections

Support of the user control of application connections is mandatory and shall follow the principles and requirements stated in 3GPP TS 23.227 [48].

This clause addresses the generic aspects of connection control supported by both WAP and Java classmark MExE devices.

In order to allow the user to maintain control over connections on his MExE device and the ability to initiate connections, the user shall be able to terminate or suspend any active connection associated with an application in the MExE environment of the MExE device. The user shall be able to obtain information about all connections associated with applications on the MExE device (e.g. requesting information, being informed by the MExE device etc.). Behaviour of the application following termination or suspension of its connection is undefined.

The specific support of connection control by WAP classmark MExE devices is identified in subsequent clause 7.3.1 "Call control", the security aspects of connection control are identified in clause 8 "Security", and the user control of connection authorisation is identified in clause 5.1 "User profile".

5.4.1 Journaling of network events

Support of the journaling of network events is mandatory.

To support the user in monitoring (potentially chargeable) network events initiated by services in the MExE environment, the MExE device shall maintain a record of network events initiated by MExE executables on the MExE device.

Network events for the purposes of journaling, are defined as events which result in the origination of connections by a service in the MExE environment of the MExE device. Examples of such events (any (potentially chargeable) network event initiated by services in the MExE environment) are:

- Sending an SMS message;
- Sending an USSD message;
- Initiating a circuit switched connection;
- Initiating a packet switched connection;
- Sending data over a packet switched connection.

The length, format and longevity of the journal is undefined and subject to manufacturers' discretion.

The journal shall be managed by the MExE device, and not be accessible by MExE executables.

5.4.2 User notification

Support of user notification is optional.

It is recommended that the MExE device should clearly display an indicator whenever network activity is in progress.

Ideally, this would be an icon on the phone's screen which is displayed whenever the MExE device is sending/receiving SMS, USSD, data call, voice call, or packets.

However, there are certain cases when this indicator need not be displayed, especially if it is obvious by some other means that the MExE device is performing network actions.

5.5 Quality of service

Support of Quality of Service is optional.

Quality of Service (QoS) [28] is seen by the end user as a measure of the amount of network resources given to an application by the underlying network. The network may employ a number of QoS mechanisms, but the end user /

MExE executable is not involved in these. The end user / MExE executable requires an interface into the network QoS through a visible set of standard parameters.

A QoS aware MExE executable may request a QoS from the network at the beginning of a QoS session. Changes in the level of QoS provided shall be notified to the end user / MExE executable. An end user may request a change in the QoS through the MExE device MMI. A MExE executable may have several QoS streams open simultaneously.

When the MExE execution environment supports QoS, the MExE executable shall be able to dynamically request a change in the level of QoS at connection setup request or subsequently during the connection. The end user / MExE executable may receive a rejection to a QoS modification request, upon which the end user / MExE executable must be notified.

The end user's service level QoS subscription parameters are stored in the network, they identify the maximum permissible QoS that a user may negotiate with the network. Several QoS subscriptions may be possible for one user. MExE is neither aware nor able to determine or modify the end user's service level QoS subscriptions.

Clause 9 "Quality of Service" defines the necessary functions for a MExE device to accommodate QoS management and provisioning. QoS management may be available directly to the MExE executables themselves, or to the MExE environment.

5.5.1 Introduction

Support of quality of service for MExE devices supporting bearers defined by QoS as defined in this clause is optional.

QoS aware MExE executables may be executing on the MExE device. To ensure correct operation with the QoS provisioning of the bearer network(s) the associated API's and the MExE QoS manager shall be supported by MExE device supporting bearers defined by QoS – see figure 3 "Logical MExE device QoS manager elements". Non QoS aware MExE executables shall operate with the defined QoS by the user or the network.

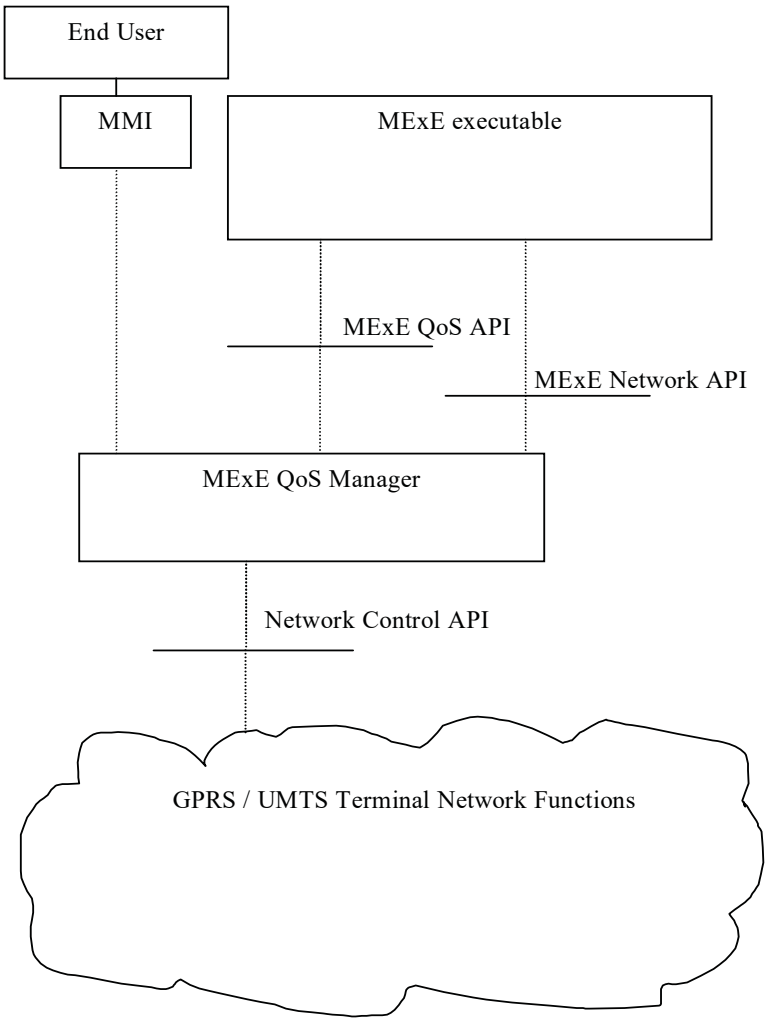


Figure 3: Logical MExE device QoS manager elements

5.5.2 MExE QoS support

In the logical architecture depicted in figure 3 "Logical MExE device QoS manager elements", a conceptual entity, a MExE QoS manager exists between the MExE executable and the Network Control API. A QoS API for MExE executables is provided and an API to the network is provided. The MExE QoS functions accommodate standard methods of end to end QoS provisioning.

For a MExE device supporting bearers defined by QoS, it is recommended that the MExE device shall support the following basic QoS operations:

- The end user should be able to manage the QoS directly via the MMI.

For MExE devices supporting bearers defined by QoS, the MExE device shall optionally support the following basic QoS operations:

- a mapping between the QoS requirements of the MExE executable and the network layer;
- MExE executables shall be able to indicate and interpret QoS values of the network via the MExE QoS Manager;
- MExE executables shall be able to modify the QoS dynamically;
- MExE executables shall be able to react to changes in the provided QoS;

MExE introduces two new elements to cater for QoS – the MExE QoS manager and the QoS API. The MExE QoS manager shall handle the fact that the network may not have QoS capabilities.

5.5.3 MExE QoS manager

As a conceptual entity, the MExE QoS manager is responsible for:

- Managing the QoS streams for MExE executables;
- Notification of the negotiated and delivered QoS to the end user / MExE executable.

The MExE QoS manager shall support the MExE QoS API according to the bearer supported by the MExE device, and provide functions such as:

- insert additional QoS signalling parameters;
- add the functionality of the MExE QoS API at best effort, if the network does not support it directly;
- translate between the QoS parameters from the MExE executable and those of the network;
- monitor the QoS delivered by the network and manage QoS requests between the MExE executable and the network;
- be informed by the MExE executable of the requested QoS traffic class;
- be informed by the MExE executable of the lowest QoS traffic class which can be accepted by the MExE executable;
- attempt to re-negotiate the QoS if it falls below the lowest QoS traffic class.

The MExE QoS manager may request information from the network regarding the QoS available.

The MExE QoS manager does not need to know the end user's subscribed QoS, this is held within the network and used to validate a requested QoS level.

The MExE QoS manager may also be accessed through the MExE device's MMI.

5.5.4 Network control API

The network control API shall provide the QoS manager with access to the network specific QoS control (e.g. as defined for GPRS/UMTS in [29] and [30]).

The MExE QoS manager may perform some QoS control, even if it is not provided in the network control.

5.5.5 MExE QoS API

The MExE QoS API provides the MExE executable with an interface to the QoS management. It does not require the MExE executable to have any knowledge of the underlying network, or how QoS is implemented in the network.

The QoS API shall provide the MExE executable with a standard set of parameters. Refer to [28] for details of these parameters (see note 1).

NOTE 1: The FLOWSPEC parameters, defined by the IETF Integrated Services Working Group, provide the QoS information required by QoS capable network elements.

Table 4 "Example parameters" shows the set of example parameters.

Table 4: Example parameters

Parameter	Units	Type
Token Bucket Rate	bytes /sec	32-bit IEEE floating point number
Token Bucket Size	bytes	32-bit IEEE floating point number
Peak Data Rate	bytes/sec	32-bit IEEE floating point number
Minimum Policed Unit	bytes	32-bit integer
Maximum Packet Size	bytes	32-bit integer
Latency	micro secs	32-bit integer
Delay Variation	micro secs	32-bit integer
Service Type		service type

As a minimum the following three parameters shall be supported by the MExE QoS manager:

- Token Bucket Rate;
- Token Bucket Size;
- Peak Data Rate.

NOTE 2: The discussion of UMTS bearer service parameters as well as radio access bearer parameters is still going on. Especially the bitrate parameters and reliability parameter are under discussion [28].

If the MExE executable does not provide a full set of QoS parameters, then the MExE QoS manager shall the provide QoS parameters based on information available to it (e.g. from the MMI settings), see clause 5.5.6 "Sources of Bearer Service Parameters".

5.5.6 Sources of bearer service parameters

A set of QoS parameters (QoS profile) specify the service provided to the user by the network. At bearer service establishment or modification different QoS profiles have to be taken into account. This is based on:

- The MExE device capabilities;
- The MExE device or the TE within the terminating network;
- A QoS profile in the QoS subscription (describes the upper limits);
- Default QoS profile (of the user or network);
- A Network specific QoS profile characterising for example the current resource availability or other network capabilities.

5.5.7 QoS streams

Several MExE executables may be executing in the MExE device, each with a different QoS requirement. Also, a MExE executable may operate several QoS streams, each with different parameter settings. The MExE QoS manager within the MExE device shall be able to deal with each stream independently.

5.5.8 QoS security

Only the end user, MExE executable or the network using a QoS stream should be able to modify the QoS of that stream.

5.6 Charging

Support of charging is outside the scope of MExE standardisation.

The following informative clauses provide a brief overview of the charging possibilities enabled by MExE.

5.6.1 Generic charging support

The standard GSM/UMTS charging records contain information sufficient to associate bearer usage and SMS/USSD messages with a subscriber.

Third party service providers and/or service providers may define charging regimes for MExE services (e.g. on a MExE or WAP server).

6 Generic MExE Security

6.1 Introduction

In order to manage the MExE and prevent attack from unfriendly sources or transferred applications unintentionally damaging the MExE device a security system is required. This clause defines the MExE security architecture.

The basis of MExE security is:

- a framework of permissions which defines the permissions transferred MExE executables have within the MExE device;
- the secure storage of these permissions (and permission type as defined in clause 6.5 "User permission types");
- conditions within the execution environment that ensure that MExE executables can only perform actions for which they have permission.

The MExE permissions framework is defined in 3GPP TS 22.057 [2] and is as follows (there is no implied hierarchy):

- MExE Security Operator Domain (MExE executables authorised by the HPLMN operator, as described in clause 6.3.1 "MExE executable permissions for operator, manufacturer and third party security domains");
- MExE Security Manufacturer Domain (MExE executables authorised by the ME manufacturer, as described in clause 6.3.1 "MExE executable permissions for operator, manufacturer and third party security domains");
- MExE Security Third Party Domain (trusted MExE executables authorised by trusted third parties, as described in clause 6.3.1 "MExE executable permissions for operator, manufacturer and third party security domains");
- MExE Untrusted Area. Untrusted MExE executables are not permitted to execute in a security domain (i.e. Operator domain, Manufacturer domain or Third Party domain) and execute in the Untrusted area, and have very reduced privileges as described in clause 6.3.2. "MExE executable permissions for untrusted MExE executables".

A MExE device shall support either all three security domains or no domains. If the security domains are not supported, then all applications shall be untrusted. The MExE device shall not support any subset of the three security domains. Support of the MExE Untrusted area is mandatory.

6.2 MExE executable integrity

If the 3 MExE security domains defined in clause 6.1 "Generic security" are not supported, then the pre-verification of MExE executables at launch time described in this clause is optional.

A potential threat is that MExE executables may be securely authenticated at the time of download, but tampered with or corrupted prior to being launched. Further a certificate may be compromised or expired. Authentication of a MExE executable at the time of download does not ensure that the MExE executable has not been modified when it is subsequently launched. Furthermore, authentication of a MExE executable at the time of launch does not ensure that the MExE executable is not modified during execution. Similarly, verification of the certificate at the time of download may not ensure that the certificate is valid at time of application launch, and verification of the certificate at the time of launch does not ensure that the certificate remains valid during execution.

Therefore, the MExE device shall ensure application integrity immediately prior to application execution.

Application integrity is defined as the state in which:-

- application code has not been modified since authentication; and
- the certificate containing the root public key is checked and known to be valid.

The mechanism by which the device preserves integrity is an implementation detail, dependant on the application storage mechanism and access. Examples of mechanisms that contribute to such application integrity could include :

- Storage of applications in a memory area that cannot be compromised on the device;
- Preventing launch of the application when the MExE device becomes aware that the certificate is invalidated;
- Full signature verification prior to each application invocation (see clause 6.2.1 “Full signature verification”);
- Optimised pre-launch signature verification (see clause 6.2.2 “Optimised pre-launch signature verification”);
- Periodic full signature verification by separate process during application execution.

The list of examples is not exhaustive and any other mechanisms ensuring application integrity may be equally considered.

A MExE device may furthermore ensure that the application code has not been modified during application execution.

6.2.1 Full signature verification

Full signature verification assumes that the procedure of validation for downloaded MExE executables and certificates is used. For more details see clause 6.7 “Certification and Authorization Architecture”.

6.2.2 Optimised pre-launch signature verification

This is an optional feature which is used to eliminate the potentially excessive overhead of checking a signature again after initial full certificate verification has already been performed.

To use this process the MExE device shall create a hash of the executable object (executable object fingerprint) as if checking the signature. This shall be stored in a protected verified application list, along with indication of the domain permissions for the application. The hash used shall be the same type as that used for signing the object. When launching an application or downloading an applet, the hash shall be performed as for when computing the signature. The verified application list shall then be checked; if the hash value is present and the entry has not expired then the application or applet may execute. If no list entry exists for this object, or the entry has expired, the process shall then proceed with the full signature verification. Note that the lists for applications and applets should be separate and that an implementation determines management policy for the lists (e.g., ageing policy, which entries to delete when trying to add a new entry to a full list etc.). One restriction imposed that shall be enforced is that the maximum number of uses for an entry before it is marked invalid is limited to some maximum value.

In the event that a new CCM is received by the MExE device, all verified application list entries shall be marked invalid unless some mechanism to determine the validity of an authorising certificate entry for each application is provided by the MExE device implementation.

6.3 MExE executable permissions

Support of MExE executable permissions as detailed in this clause is mandatory.

6.3.1 MExE executable permissions for operator, manufacturer and third party security domains

The following table 5 "Security domains and actions" specifies the permissions of operator, manufacturer and third party security domains in the order of restriction.

The actions listed in the security table 5 "Security domains and actions" are generic actions. These actions can only be performed by MExE executables via application programming interfaces (APIs) (which are intrinsically part of the MExE implementation) The security restrictions shall apply to MExE executables whether the API functionality is called directly or indirectly by the MExE executable. Explicit user permission is required for all actions by MExE executables in all domains. Types of user permission are defined in clause 6.5 "User permission types".

Untrusted MExE executables are not permitted access to any actions which access the phone functionality (phone functionality includes all the actions in table 5 "Security domains and actions") except for the exceptions identified in clause 6.3.2 "MExE executable permissions for untrusted MExE executables".

Actions available using interfaces giving access to the phone functionality (either in existence at the time of approval of this specification or not) that are not listed in the security table 5 "Security domains and actions" shall be categorised into one of the groups in the security table 5 "Security domains and actions" by comparing its action against the groups in order as they are listed in the table 5 "Security domains and actions". If an action can be categorised into a more restrictive group near the top of the table, then it shall not be again categorised into another, less restrictive, group further down in the table. For example, if a new action eventually results in forwarding a call, it shall be categorised into Network access. If the action is totally new, it shall be categorised into some of the groups by comparing its functionality to the group description below and by comparing with the list of actions listed in the table within the group.

1. Device core function access includes functions, which are an essential part of the phone functionality .
2. Support of core software download, which allows updating the ME radio, characteristics and properties by changing the core software in the ME (e.g. a new CODEC may be loaded into a ME, a new air interface, etc.)
3. (U)SIM smart card low level access includes functions, which allow communications at the transport service access point (send and receive application protocol data unit).
4. Network security access includes all functionalities which relate to CHV, CHV2, UNBLOCK CHV and UNBLOCK CHV2 (verification, management, reading or modifying), GSM authentication, GSM ciphering.
5. Network property access includes functions, which enable the management of operator-related data parameters and network settings.
6. Network services access includes all functionalities which result in or need interaction via the operator’s network.
7. User private data access includes all functionalities which relate to management, reading or modifying of data that the user has stored in the MExE device including user preferences.
8. MExE security functions access includes all functionalities which, through an API relate to certificate handling in the MExE device; end to end encryption, signed content, hashing, access to public, private, secret keys stored in the MExE device or in a smart card.
9. Application access includes the functionalities which relate to launch provisioned functionality, MExE executables, external executables ((U)SIM tool kit application,…) usage.
10. Lifecycle management includes the functionalities which are needed for installing or removing MExE executables in the MExE device.
11. Terminal data access includes the functions which relate to accessing terminal data, i.e. not user data.
12. Peripheral access includes the functionalities related to peripherals other than user interface peripherals usage through a high level software application interface.
13. Input output user interface access includes the functionalities related to the user interface and user notification means usage.

Table 5: Security domains and actions

	MExE Security Domains		
Actions	**Operator**	**Manufacturer**	**Third Party**
Device core function access Start/stop radio Turn on/off device Write time and/or date Activate a user profile Modify a user profile	No		
Support of Core Software Download e.g. Update ME software	No	Yes	No
(U)SIM smart card low level access[11] Send APDU Slot management (power on/off, reset, port lock…)	No		
[11] – Access to (U)SIM is provided using more high level API as phonebook, application launching			
Network Security access Run algorithm Verify CHV/2 or UNBLOCK CHV/2 Activate/deactivate CHV Modify CHV/2	No		
Network property access Get IMSI Get home network Select network	Yes	No	
Network services access Initiate a voice/data connection [3] Accept a voice/data connection [3] Call forward [4] Multiparty call [4] Call deflection [4] Explicit call transfer [4] Terminate an existing connection Hold an existing connection Resume an existing connection Send point-point message (e.g. SMS, USSD) [4] Query network status Get signal level Get call list QoS management	Yes		Yes [6]
[3] – A network connection may be via any supported bearer service [4] – Multiparty, deflection, and explicit call transfer shall be permitted only to numbers explicitly supplied by the user to the MExE Executable. Modification of call forward numbers stored in the network shall only be permitted to numbers explicitly supplied by the user to the operator. [6]– The Third Party domain's permission to access the networking action depends on the provisioning mechanism as described in clause 6.13.3 "Determining the administrator of the MExE device"			
User private data access [1] Read Write Get properties Delete Get Location Information Read stored SMS Delete stored SMS Modify user preferences	Yes[2] Yes[2] Yes[2] Yes[2] Yes[2] Yes[2] Yes[2] Yes[7]		
[1] – User private data includes user files, phonebook, MSISDN, etc located on the MExE device. [2] – The user shall be able to specify data access permissions within the capabilities of the MExE device. It is not applied to user preferences [7] – Trusted applications only have permission to modify user preferences, and not to activate or de-activate them. The user shall be able to specify for each domain, the preferences that applications in that domain can access. All other preferences shall not be accessible to that domain. The default shall be that there is no access. Single action user permission is the only type of user permission that shall be possible for changes to User Preferences.			

Actions	MExE Security Domains		
	Operator	Manufacturer	Third Party
MExE security functions access			
Install a certificate for a given domain	Yes [5]		
Uninstall a certificate for a given domain			
Replace a certificate for a given domain	Yes [5]		
Data encryption API			
Verify a signature API	Yes [5]		
Compute a digital signature API			
Hash a content API	Yes		
Non repudiation API	Yes		
	Yes		
	Yes		
	Yes		
[5] – Only the organisation whose public key is certified (or the organisation that certified the public key) can add, delete or replace a particular certificate.			
Application access			
Get application list	Yes[8]		
Launch an application	Yes[8]		
Get application status	Yes[8]		
Stop, suspend, resume an application	Yes[9]		
[8] – ME provisioned functionality access is limited to manufacturer domain. (U)SIM tool kit application access is limited to operator domain. MExE executable access is limited to MExE executable issued by the same issuer (identify by the certificate) of launched MExE executable [9] – Access is limited to MExE executable which launch the application. But the end user, shall have a way to stop the launched application, MExE environment may stop the launched application or launched application may stop itself.			
Lifecycle management	Yes		
Install a MExE Executable			
Uninstall a MExE executable			
Terminal data access			
Get manufacturer software version	Yes		
Read time and date	Yes		
Peripheral access	Yes		
Sound generation to speaker (e.g. via stream)			
Set speaker volume			
printer access			
Monitor the power state			
Change the power state			
Activate/ access Serial port (RS232, IrDA, Bluetooth, USB …) access			
Activate/access Parallel port			
Activate/access Smart card other than (U)SIM card (Send APDU, Slot management)			
Input output User interface access			
Input device (keyboard, mouse …)	Yes[10]		
Output device (display)	Yes[10]		
Output notification device(smart icon, sound, light, vibrator …)	Yes		
[10] – Access request requires no user permission.			

The lists in the groups in table 5 "Security domains and actions" are not exhaustive, and other actions which are of the same category shall be included in the group for the purposes of requesting user permission.

This clause identifies the permissions for MExE executables in the 3 security domains (operator, manufacturer and Third Party). The permissions do not apply to untrusted MExE executables which are not permitted to execute within the domains.

6.3.2 MExE executable permissions for untrusted MExE executables

When the Security Domains are not supported then all executables are untrusted and they execute in the untrusted area for which the executable permissions are defined as follow in table 6 "Executable permissions for untrusted MExE executables".

In order to facilitate untrusted MExE executables having some limited access to MExE device functionality beyond their very limited privileges, some of the access permissions in the previous table 5 "Security domains and actions" are extended to untrusted MExE executables and described in table 6 "Executable permissions for untrusted MExE executables" as well as in clause 6.11 "Separation of I/O streams".

The untrusted MExE executables permitted to use these facilities shall be MExE executables the user has downloaded him or herself, and not be MExE executables that have been pushed to the user. MExE executables on the MExE device due to the user having visited a particular Web site are considered to be MExE executables that the user had downloaded him or herself.

Untrusted MExE executables shall not be permitted access to any other functions.

Table 6: Executable permissions for untrusted MExE executables

<table>
<tr><th></th><th>Classmark 1</th><th>Classmark 2</th><th>Classmark 4</th><th>Classmark 3</th></tr>
<tr><td>User Interface</td><td colspan="3">An untrusted, uninstalled MExE executable (e.g. an applet) can access the user interface output and input without user permission, but the sending of user data to a server to which the MExE executables has a session connection (e.g. as part of a browser session) requires user permission.
An installed untrusted MExE executable shall only be able to access the user interface output and input with user permission (clearly, for the usability of untrusted MExE executables such as games, blanket user permission should be sought and given, and this is permissible).</td><td>Untrusted MExE executables can access the user interface output and input without the user permission.</td></tr>
<tr><td rowspan="2">File, Persistent Data</td><td colspan="4">File access is not permitted for untrusted MExE executables.</td></tr>
<tr><td colspan="3">But, untrusted MExE executables can access files only in the MExE executable's own directory.</td><td>But, persistent data may be stored via the MIDP record management system (stores are shared between MIDlets in the same MIDlet Suite).</td></tr>
<tr><td>Transmission over the Access Network</td><td colspan="4">Untrusted MExE executables shall be able to exchange data, voice, HTTP requests, etc. over the Access Network under the following conditions:
The recipient of a transmission (e.g. a phone number, a URL, a server name, etc.) shall be presented to the user for permission by a provisioned functionality of the MExE device itself, even if this recipient was already presented by the executable (this facility would support, for example, "click to dial" buttons/links in untrusted MExE executables).
It shall not be possible for an application to use a transmission channel that it did not initiate (except for MIDlets within the same MIDlet suite).</td></tr>
<tr><td>Generate DTMF</td><td colspan="4">Untrusted MExE executables shall be able to generate DTMF tones under the following conditions:
An untrusted MExE executable is only permitted to send DTMF tones in a currently active call. The request to generate DTMF tones in the currently active call, shall result in the characters which the tones represent being presented to the user for permission by a provisioned functionality of the MExE device.</td></tr>
<tr><td>Add Phonebook Entry</td><td colspan="4">Untrusted MExE executables shall be able to add a phonebook entry (i.e. name and number only) under the following conditions:
The name and the number to be added shall be displayed to the user for permission by a provisioned functionality of the MExE device and not by the MExE executable itself. The phonebook entry shall not be added without user permission. The function shall not be able to modify or delete any phonebook entry.</td></tr>
<tr><td>Executable Interaction</td><td colspan="4">Executable interaction is not permitted for untrusted MExE executables (except for MIDlets within the same MIDlet suite).</td></tr>
</table>

NOTE: The functionality of "Generate DTMF tones" and "Add Phonebook Entry" is not supported by the MIDP at the moment.

6.4 Handling of MExE executables when their valid root public key is not available

This clause considers the effect on MExE executables when the root public key of a secure domain (e.g. operator, manufacturer, third party) is no longer available (e.g. when the UICC is being physically removed, or the root public key is no longer valid).

6.4.1 Launching of MExE executables when their valid RPK is not available

It shall not be possible to launch a MExE executable to run in a security domain unless the root public key of that security domain is available and valid.

6.4.2 Currently executing secure MExE executables when their valid RPK is no longer available

On detection that the valid root public key of a secure domain is no longer present, the MExE device shall permit MExE executables currently executing in the secure domain controlled by that root public key to continue executing. Furthermore, if the same RPK is available again, the executable is allowed to keep on executing. However, if a different RPK is validated, the currently running MExE executables (under the old RPK) in that secure domain shall be terminated.

6.5 User permission types

Support of user permission types is mandatory.

The term "user permission" is defined to mean that the user can give permission for a specific action in one of the ways defined in table 7 "User Permissions". Support single action permission is mandatory, but support of blanket permission and session permission is optional.

Any request for user permission as described in table 7 "User Permissions" must display a user friendly name identifying the signer of the corresponding MExE executable, if available. The "subject" field of the certificate of the signer ("subject" here refers to the "subject" fields of WTLS and X.509 certificates and an equivalent field for any other format of certificate) shall be made available to the user upon request. If an application, for which user permission is being sought, is untrusted, the fact that the application is untrusted shall be at least visually indicated to the user, if the MExE device is capable of visual indication, whenever user permission is sought. Other means of indication are additionally permitted. If the MExE device is not capable of visual indication, or is not designed for use by a human user, other means of indication shall be used.

The MExE device shall allow user control of permissions relating to all action groups listed in the table 5 "Security domains and actions" that are required by the MExE executable and supported by the MExE device.

Multiple action group permissions may be controlled in a single user action on the MExE device regardless of the permission type as listed in table 7 "User Permissions". In such case, these action group permissions shall be made explicit to the user.

Note that blanket permission cannot be used for uninstalled MExE executables e.g. applets, WMLS.

Table 7: User Permissions

	User Permissions		
Permission Type	**Description**	**Invocation**	**Revocation**
blanket permission	The user gives blanket permission to the MExE executable for the specified action, and the MExE executable subsequently uses the user's original permission for the identified subsequent actions whenever the MExE executable is running.	Typically such permission would be given at MExE executable configuration or run time.	The blanket permission maybe revoked by the user at any time. The user permission no longer applies once the MExE executable has been removed.
session permission	The user gives permission to the MExE executable for the specified action during a specific run time session of an MExE executable, and the MExE executable subsequently uses the user's permission for the identified subsequent actions whilst the MExE executable session is still running.	Typically such permission would be given at MExE executable run time.	The session permission maybe revoked by the user at any time. The user permission no longer applies once the MExE executable run time session has terminated.
single action permission	The user gives a single permission to the MExE executable for the specified action; if the MExE executable subsequently wishes to repeat the action it must again request the user's permission for the identified subsequent action.	Typically such permission would be given at MExE executable run time.	The user permission no longer applies once the action has terminated.

6.6 Root Public keys

If the 3 MExE security domains defined in clause 6.1 "Generic security" are not supported, then the root public key management described in this clause is optional.

The definition of the secure mechanism in this clause to mark as valid a root public key certificate on the ME, is out of the scope of this specification.

6.6.1 Operator root public key

The ME may support secure storage for one or more certificates, each of which contains an operator root public key. The ME shall support the use and management of a certificate containing an operator root public key stored on the MExE-(U)SIM and in the ME. The ME shall behave according to clause 6.6.1.2 "ME actions on SIM insertion and/or power up". For support of public key management on the SIM and the USIM refer to 3GPP TS 51.011 [27] and 3GPP TS 31.102 [39] respectively. The certificate contains a root public key generated either by the operator, or by a CA trusted by the operator.

If the MExE device does not contain a valid operator root public key, then the certificate chain to MExE executable previously executing in the Operator Domain will be invalid, and the MExE executables will be excluded from the operator domain.

The user shall not be able to add or delete any type of operator public key (root or contained in a certificate).

Optionally, the operator may install a corresponding disaster-recovery root public key stored in the MExE device, enabling the operator to use a secure mechanism (involving the disaster-recovery key) to replace the certificate containing the standard operator root public key. It shall not be possible to use the disaster recovery operator root public key to replace the operator root public key unless both public keys are from the same operator.

There shall be no more than one valid operator root public key on the MExE device at any one time. A valid operator root public key on the (U)SIM shall always have precedence over any operator root public key on the ME. Any operator root public key(s) on the ME shall be marked invalid when a valid operator root public key is present on the (U)SIM.

An application signed by an operator shall not be able to execute in the Operator Domain unless the root public key of that operator is installed in the MExE device (either ME or MExE-(U)SIM) and is marked as trusted.

6.6.1.1 Caching of root public keys

The ME shall behave as if it reads the operator root public key from the secure area every time the ME needs the key to verify a signature. Examples of the secure area include an area on a (U)SIM or a secure, persistent area on the ME.

If the ME uses a mechanism for caching public keys, it shall do so in a way that maintains the integrity of the secure area and is consistent with the keys stored in the secure area. With the exception of improved performance, the operation of the device using cached public keys must be indistinguishable from that of a device that reads the key from the secure area every time it uses the key for verification.

No cached version of a key may exist beyond the expiration or termination of the key in the secure area. For example, if the ME caches a root public key held on the (U)SIM, the ME shall purge the cache when the (U)SIM application is stopped (or the SIM card is withdrawn).

6.6.1.2 MExE device actions on detection of valid (U)SIM application and/or power up

This clause defines the sequence of actions on identification by the MExE ME that a valid SIM card, or USIM application on the UICC, has been detected (e.g. through insertion of (U)SIM card, power up of MExE device etc.). More specifically, these actions relate to the enabling or disabling of the operator domain and the status of the operator applications on the ME.

The requirements in this clause ensure that the operator domain on the ME belongs to the same operator as the operator that issued the valid (U)SIM application (if detected) in the MExE device and, if there is an operator root public key (ORPK) on the MExE-(U)SIM, that trusted operator applications on the MExE device were verified using that ORPK.

The ME shall support the use and management of an Operator root public key (ORPK) on the MExE-(U)SIM.

On power up the MExE device shall behave as dictated by figure 4 "MExE device behaviour on power up" below.

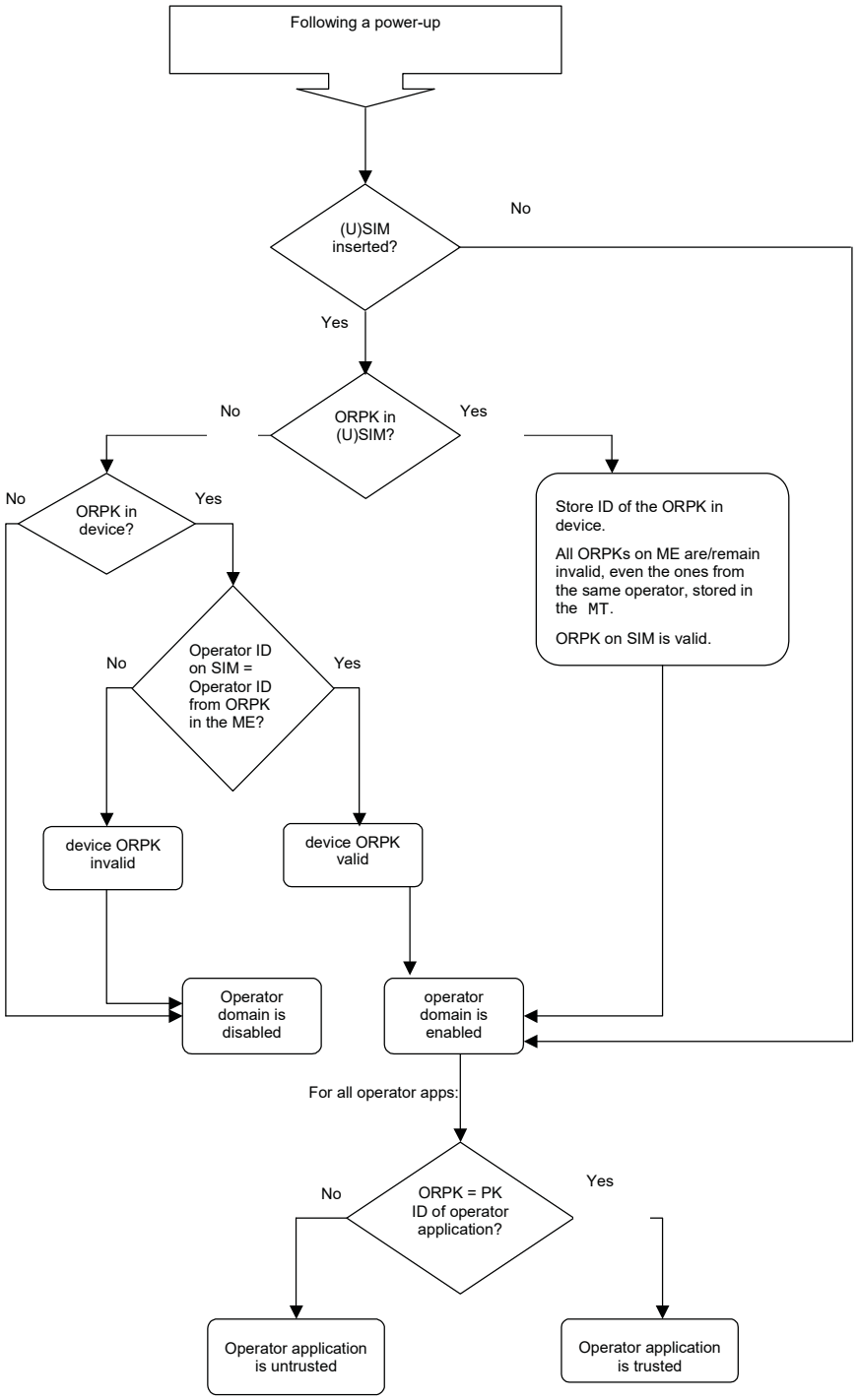


Figure 4: MExE device behaviour on power up

Note that the procedure in Figure 4 "MExE device behaviour on power up" checks for a match between the Operator ID on the (U)SIM and the Operator ID from the ORPK in the ME. Currently, one mechanism for defining the Operator ID on the (U)SIM is through use of the MCC+MNC. As an additional note, on DCS1900, the MCC+MNC is 6 digits, but elsewhere it is 5 digits. The MExE device needs to know how many digits to use. However, this is outside the scope of this specification. The implementations of MExE devices need to establish agreements on using the MCC+MNC as the Operator ID on the (U)SIM. Likewise, the implementations of MExE devices need to establish agreements on how to define the Operator ID belonging to the ORPK.

The ME shall only read the ORPK from the MExE-(U)SIM when required and shall not store a ORPK from the MExE-(U)SIM on the ME in a manner inconsistent with that detailed in clause 6.6.1.1 "Caching of root public keys".

When an operator root public key stored on the ME is marked as invalid, all operator applications verified using that root public key or by certificates verified by a chain that terminates with that root public key, shall cease operation as soon as possible and shall be marked as untrusted.

Removal of the (U)SIM shall not cause the status (i.e. valid or invalid) of any operator root public key on the MExE device to change.

6.6.2 Manufacturer root public key

The ME shall support secure storage for a certificate containing a manufacturer root public key. The certificate contains a root public key generated by the manufacturer of the MExE device, or by a CA trusted by the manufacturer of the MExE device.

If the ME does not contain a valid manufacturer root public key, then the certificate chain to MExE executable previously executing in the Manufacturer Domain will be invalid, and the MExE executables will be excluded from the manufacturer domain and marked as untrusted.

The user shall not be able to add or delete any type of manufacturer public key (root or contained in a certificate).

The Manufacturer shall put a root public key and optionally its corresponding disaster-recovery key in the ME at the time of manufacture, and use a proprietary secure mechanism (e.g. using the disaster-recovery key) to replace the certificate containing the manufacturer root public key. It shall not be possible to use the disaster recovery manufacturer root public key to replace the standard manufacturer root public key unless both public keys are from the same manufacturer.

An application signed by a manufacturer shall not be able to run in the Manufacturer Domain unless the root public key of that manufacturer is installed in the ME and is marked as trusted.

The manufacturer, and only the manufacturer, may use a secure mechanism to mark as valid/invalid a certificate containing the manufacturer root public key on the ME. It shall only be possible to use this mechanism to mark a certificate containing a new manufacturer root public key on the ME as valid, when all manufacturer root public keys are marked as invalid.

There shall be no more than one valid manufacturer root public key on the ME at any one time. Any other manufacturer root public key(s) on the ME device shall be marked invalid when a different manufacturer root public key is marked as valid on the ME.

6.6.3 Third party root public key

The ME shall support secure storage for at least one certificate containing a third party root public key. The ME shall support the use and management of certificates containing Third Party root public keys stored on the MExE-(U)SIM and in ME. For support of public key management on the SIM and the USIM refer to 3GPP TS 51.011 [27] and 3GPP TS 31.102 [39] respectively. The MExE device may contain root public key (s) generated by CA(s) implicitly trusted by the user. The user will be able to securely install (using a secure transport) or remove Third Party root public keys at any time using a system administrative tool.

The Manufacturer, Operator and Administrator may at their discretion, securely install certificates containing Third Party root public key(s) on behalf of the user, e.g. at the time of manufacture by the Manufacturer. See clause 6.10 "Certificate management" for details of Administrator control of Third Party certificate download.

If a Third Party public key is deleted or becomes invalid, then the certificate chain to MExE executables previously executing in the Third Party Domain certified by that public key will become "untrusted".

There may be any number of Third Party root public keys on the MExE device.

The third party domain administrator, i.e. the Administrator (user or other body) shall be able to enable and disable Third Party root public keys by using CCM, see clause 6.10.1 "Certificate configuration message (CCM)". The process of adding/removing public keys and enabling/disabling public key are independent.

All third party certificates shall be subject to restrictions imposed by valid certificate configuration messages.

See clause 6.10 "Certificate management" for the management of Third Party root public keys.

6.7 Certification and authorisation architecture

If the 3 MExE security domains defined in clause 6.1 "Generic security" are not supported, then the certificate and authorisation architecture described in this clause is optional.

In order to enforce the MExE security framework a MExE device is required to operate an authentication mechanism for verifying downloaded MExE executables. A successful authentication will result in the MExE executable being trusted; and able to be executed in a security domain (as determined by the root public key of its certification tree).

As the MExE device may want to authenticate content from many sources, a public key based solution is mandatory. Before trusting MExE executables, the MExE device will therefore check that the MExE executable was signed with a private key, for which the MExE device has the corresponding public key. The corresponding public key held in the MExE device must either be a root public key (securely installed in the MExE device, e.g. at manufacture) or a signed public key provided in a certificate. The MExE device must be able to verify certificates, i.e. have the public key (as a root key or in a certificate) corresponding to the private key used to sign the certificate. Support of certificate chains is therefore mandatory.

The requirements on authorisation and certification are given in clause 6.7.1 "Certification requirements". An example authorisation and certification process is described in clause 6.7.3 "Example certification process".

6.7.1 Certification requirements

A MExE device cannot verify certified MExE executables of a particular domain unless it has a root public key for that particular domain.

Root public keys shall be securely installed in the MExE device, say, at the time of manufacture.

It is recommended that a "disaster recovery" root public key be securely installed on the MExE device, to be used to install new root public keys when all other root public keys on the MExE device are invalid.

Third Party Domain root public keys will typically be installed along with and integrated into the MExE device browser, as is done for PC-based browsers.

A MExE executable can only be verified if the MExE device contains a valid root or certified public keys corresponding to the private key used to sign the MExE executable.

A MExE device shall support at least one level of certificate under operator, manufacturer or Third Party root public keys. The MExE device shall support at least one level of certificate chain analysis in a signed content package, as shown in figure 5 "Trust hierarchy".

A certificate (other than one containing a root public key) shall only be considered valid if the signature on the certificate is verified by a valid public key (root or contained in a certificate) already present on the MExE device and if the certificate being verified has not expired.

Public keys shall not be shared between domains.

6.7.1.1 MExE terminal requirements for certificate processing

A MExE device shall support the processing of X509 certificates profiled in the “WAP Certificate and CRL Profile” [47] together with additional requirements defined in the MExE specification, see clause 6.9.1.1 “X509 version 3”. The certificate chain depth is still mandated to be one level only, as mentioned in clause 6.7.1 “Certificate requirements” and indicated in figure 5 "Trust hierarchy".

A MExE device shall support the SHA1WithRSA signature algorithm. The object identifier value can be found in [49]. A MExE device may also support other signature algorithms.

MExE devices may also support the processing of other certificate formats.

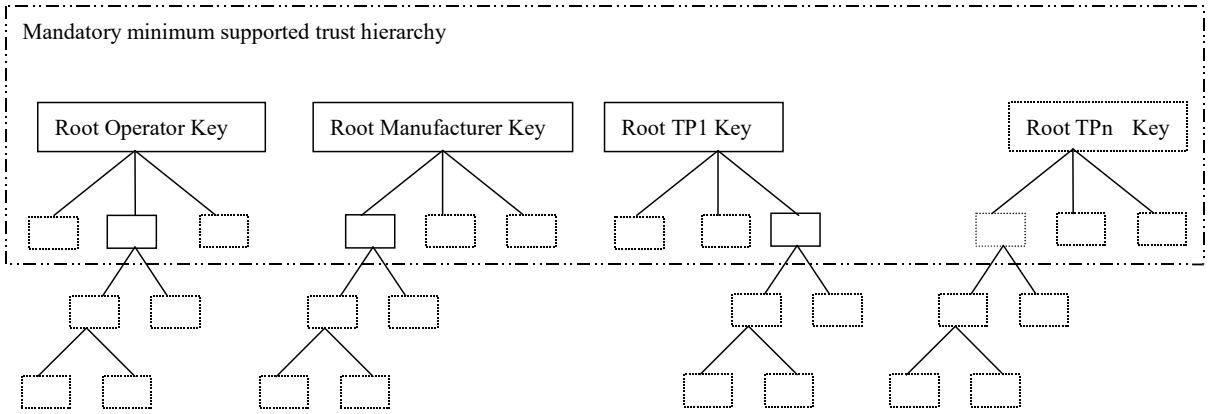


Figure 5: Trust hierarchy

The boxes below the root keys represent individual public key certificates. The solid boxes represent the minimum MExE, and the dotted boxes represent possible further support for public key certificates (either at the first or subsequent levels).

6.7.2 Certification administration requirements

For control of third party certificates, the MExE device supports storage of a certificate containing an administrator root public key as detailed in clause 6.13.1 “Administrator root public key”.

This certificate is managed separately from the hierarchy of Figure 5 “Trust Hierarchy” discussed in clause 6.7.1 “Certification requirements”. The administrator root public key in this certificate is primarily used for designating an administrator of the third party certificates. Note, the administrator root public key does not implicitly define a security domain, and is used in complement with the root public keys of the operator, manufacturer, and third party domains.

The relationship of the administrator certificate (and root public key) to the management of third party certificates is detailed in part of clause 6.10 “Certificate management”.

The relationship of the administrator certificate to the mechanism for determining if a third party certificate is trusted is detailed in part of clause 6.10.1 “Certificate configuration message (CCM)”.

Mechanisms for designating an administrator are detailed in clause 6.13.2 “Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device”.

6.7.3 Example certification process

The following processes might be followed in order to securely download a Third Party application to a MExE device.

Root public keys for a number of Certification Authorities (CAs) are installed in the MExE device, along with the MExE device browser, at manufacture. These root public keys can be used to verify certificates for Third Party MExE executables.

1. A third party software developer generates a private and public key pair (or obtains such a pair from a CA).
2. The third party software developer obtains a certificate for the public key from a CA. The certificate contains the developer public key, signed with the private key of the CA.
3. The 3rd party software developer adds all the certificates required in the key chain in the JAR.
4. The MExE device downloads a MExE executable of the third party software developer.

5. The MExE device verifies the certificate using the root public key, contained in the browser, of the relevant CA, and extracts the third party software developer public key and may store it in the certificate store for future use.

6. The MExE device verifies that the MExE executable was signed using the private key corresponding to the third party software developer public key and installs or rejects the MExE executable accordingly.

All downloaded applications shall follow the procedure described in clause 6.7.4 "Certificate Chain Verification" in order to verify the application signature and the certificate chain. If the 3 security domains are not supported, the procedure described in the next clause is optional.

6.7.4 Certificate Chain Verification

This clause presents the procedure of validation of any downloaded MExE executable. It checks for the presence of the signature used to sign the application as well as the presence and integrity of all the certificates needed to successfully verify the signature. As a result, the application under scrutiny is deemed trusted or untrusted, i.e. will be allowed execution in one of the secure domains or in untrusted area, or otherwise the application will not be allowed to be executed and will be deleted. In any outcome of the verification, the user is notified about the result. The user also may wish to see certificate details if the application is allowed to be executed on the MExE device.

The MExE device shall follow "certificate verification" procedure as described below. The procedure shall contain at least the following logical phases (not necessarily in the order stated below):

Signature and Certificate Verification Supported: Checks whether signature and certificate verification procedure is supported on the MExE ME.

Executable with Signature and End Entity Certificate (note): Checks whether the executable contains a signature together with the corresponding end entity certificate.

Valid Application Signature (note): This phase comprises the following checks:

- Check if the signature and the end entity certificate formats are supported by the device. If this check fails, the application is classified as untrusted.

- Check if the signature algorithm is supported/known by the device. If this check fails, the application is classified as untrusted.

- Check if the signature can be cryptographically verified by using the accompanying end entity certificate . If this check fails, the application is not allowed execution and is deleted.

Complete set of Intermediate Certificates Available (note): Checks if all the necessary intermediate certificates (certificates between the RPK and the end entity certificate) are available.

Valid RPK on (U)SIM/ME: Checks if a valid RPK (not expired) exists on the (U)SIM or on the ME that could verify a certificate chain originating from the end entity certificate accompanying the application.

NOTE: These steps could include validation (e.g. expiration, revocation, etc.) checking by means of e.g. OCSP, SCVP, CRL-Consultation, and etc. The use of certificate revocation checking is recommended but is not mandated or defined in this specification.

Certificate Chain Cryptographically Verified: Checks if all the certificates from the end entity certificate to the RPK can be verified cryptographically. Certificate verification shall be performed according to the functional requirements given in clause 6.1 "Basic Path Validation" of RFC 2459 [43] excluding revocation checking.

Secure Domains Supported: Checks whether MExE ME supports secure domains.

Only if all the above checks are successful, the downloaded application is deemed trusted and is allowed to be executed in the designated trusted domain (operator, manufacturer, trusted third party). Otherwise, the application is either untrusted (execution in the untrusted area only is allowed) or deleted (execution is not allowed at all) as per the figure 6 “Certificate Chain Verification Diagram” and as explained above. The executable shall only be designated into one of the trusted domains, and it shall be possible to verify the certificate chain unambiguously to one and only one root public key.

The MExE ME shall allow for a "user notification" procedure as described below.

It shall be possible to display certificate details to the user if requested, however, since the terminal might not have a display or might not be meant for a human user the methods presented in "user notification" section are not discussed any further in this specification. Figure 6 “Certificate Chain Verification Diagram” shows an example of the certificate chain verification procedure.

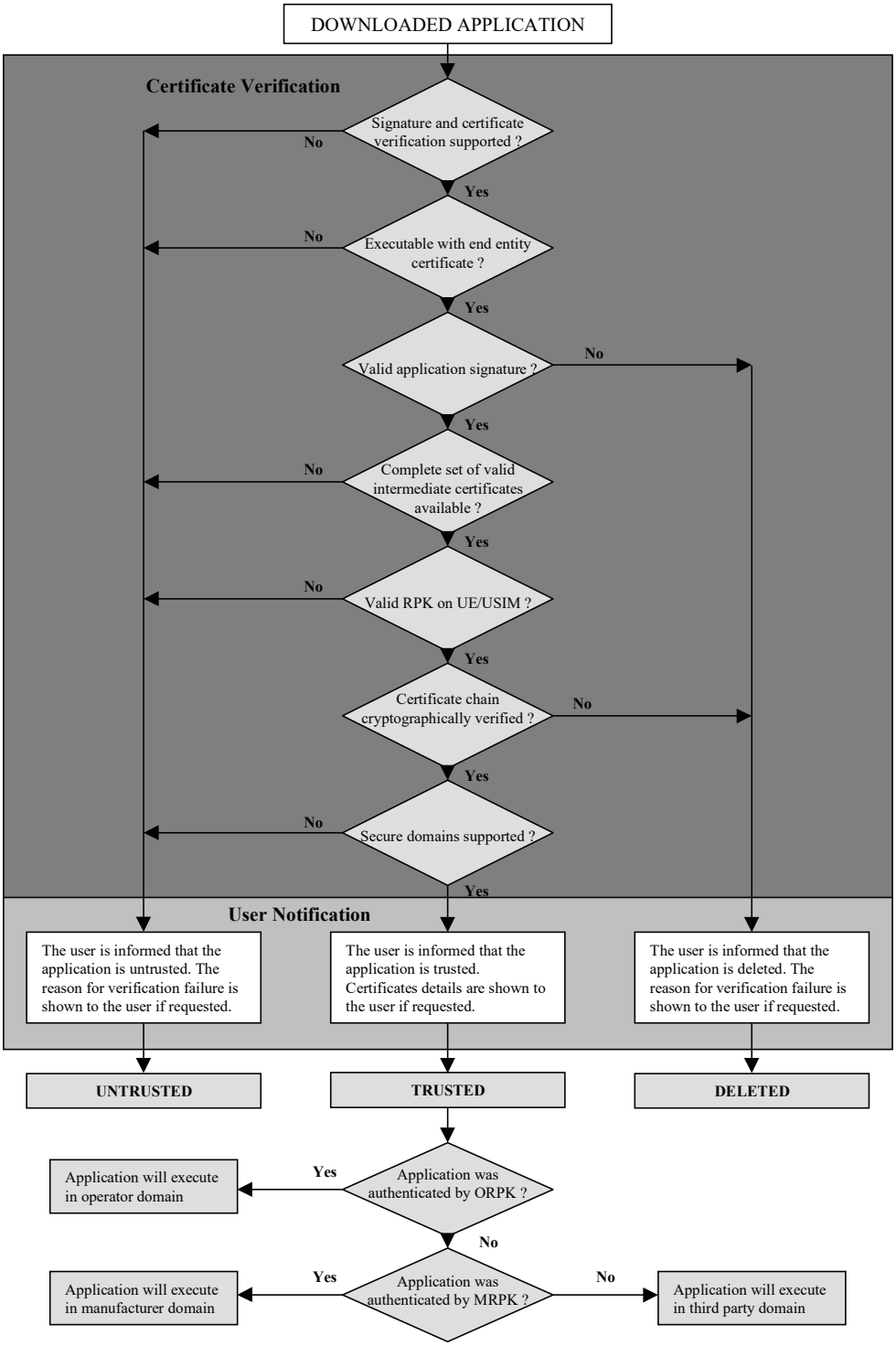


Figure 6: Certificate Chain Verification Diagram

6.8 Usage of Signed Content

6.8.1 Signed packages used for installation

If the 3 MExE security domains defined in clause 6.1 "Generic security" are not supported, then the signed packages used for installation, described in this clause, are optional.

The Java Archive (JAR) file format shall be supported on classmark 2 and 3 MExE devices for securely packaging objects that are to be downloaded and installed on the ME. The method for securely packaging objects for MExE classmark 1 devices may be referenced from the WAP specifications in a future release of this specification. A MExE device may support other proprietary means of downloading and installing objects.

The JAR file shall contain a manifest file that has at least the following attribute:

`MExE-Implementation-Type`

The information contained within the manifest file is represented as so-called "name: value" pairs, where "name" is represented by `MExE-Implementation-Type`. Groups of name-value pairs are known as a "section", where sections are separated from other sections by empty lines.

The `MExE-Implementation-Type` value shall be one of the following:-

- "**`MExENativeLibrary`**"

  in the case of a MExE Native Library (as described in 8.3.2 "Installing MExE native libraries");

- "**`TTPCertificate`**"

  in the case of a certificate containing a 3rd party root public key (as described in 6.8.2 "Installation of root certificates in a signed data package");

- "**`ManufacturerCertificate`**"

  in the case of a certificate containing a manufacturer root public key (as described in 6.8.2 "Installation of root certificates in a signed data package");

- "**`OperatorCertificate`**"

  in the case of a certificate containing an operator root public key (as described in clause 6.8.2 "Installation of root certificates in a signed data package");

- "**`AdminCertificate`**"

  in the case of an administrator certificate, which shall consist of a section containing both the administrator certificate and a CCM (as described in clause 6.8.2 "Installation of root certificates in a signed data package"); or

- **"OrdinaryTTPCertificate"**

  in the case of a certificate or certificate list containing 3rd party public key(s). An example of a certificate list syntax can be found in [52]

- **"OrdinaryManufacturerCertificate"**

  in the case of a certificate or certificate list containing manufacturer public key(s). An example of a certificate list syntax can be found in [52]

- **"OrdinaryOperatorCertificate"**

  in the case of a certificate or certificate list containing operator public key(s). An example of a certificate list syntax can be found in [52]

- "**`CCM`**"

  in the case of a CCM (as described in clause 6.8.2 "Installation of root certificates in a signed data package"); or

- *-free-format-value-*

  in the case of proprietary binaries or Java classes such as native DSP code, provisioned functionality upgrades and patches (as described in clause 6.8.3 "Installation of other signed data").

Refer to [42] for full details of how to encode the "name: value" pairs and "section" in a JAR manifest file.

See figure 7 "Signed packages". When a download of a JAR file is completed, the system installer shall read the manifest to determine what types of files are contained in the JAR, and install them appropriately.

Note that a signed package containing a library which does not have a manifest attribute "MExE-`Implementation-Type: MExENativeLibrary`" shall be considered to be some type of upgrade to libraries that are intrinsically part of the MExE device implementation rather than a "MExE native library". E.g.

```
MExE-Implementation-Type: ManufacturerUpgrade (something.dll)
```

(Recommended behaviour for the server is that it uses the capability information supplied from the MExE device to determine how to offer appropriate upgrades.)

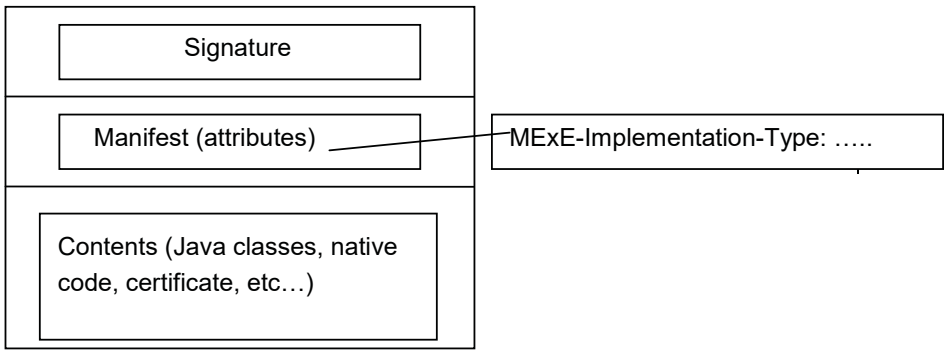


Figure 7: Signed packages

6.8.2 Installation of root certificates in a signed data package

Root certificates in a signed package (whose signature verifies as described in clause 6.6 "Root Public keys" to the Manufacturer root, Operator root, or the Administrator root), may be installed to the root public key store on the MExE device. Note that the certificate thus packaged does not necessarily belong to the manufacturer domain. The types of certificate that can be present and installed by packages are given in table 8 "Allowed certificate types in signed packages". The MExE device shall store the root public key as indicated by the certificate type.

When a certificate containing an Administrator root public key is thus contained in a signed package, the signed package (e.g. a JAR file in the case of Java based MExE classmarks) shall contain two files: the Administrator root public key and the CCM.

Table 8: Allowed certificate types in signed packages

Signature on Package	Allowed Certificate types in package
Administrator	Third Party
Manufacturer	Administrator, Manufacturer, Operator, Third Party
Operator	Administrator, Operator, Third Party

6.8.3 Installation of other signed data

A signed package of proprietary binaries or Java classes such as native DSP code, provisioned functionality upgrades and patches, whose signature verifies as described in clause 6.6.2 "Manufacturer root public key" as belonging to the Manufacturer Domain may be installed. The use of such binaries is outside the scope of MExE, but the manufacturer shall be responsible for ensuring that the integrity of MExE is not compromised.

Support of this feature is optional.

6.9 Certificate Format

6.9.1 Certificate extension for removal of network access

MExE defines the certificate extension (attribute) " access-Restriction". If the access-Restriction extension is present in a certificate used to verify the signature on a trusted application or in any certificate in the certificate chain used to verify that signature, then the application shall not be permitted the capabilities listed under "network service access" in the security table, (table 5 "Security domains and actions"). This restriction applies irrespective of any user permission for network service access that may or may not be requested by the application and/or given by the user.

The extension prevents the trusted applications of developers who do not need network service access from writing applications that can perform network service access.

The support of this extension in the operator domain is mandatory. The support of this extension in the manufacturer and third party domains is optional.

The extension is defined for X.509 version 3 only. Support for WTLS, X9.68 certificate formats is for further study.

6.9.1.1 X.509 version 3

The MExE certificate format as specified in clause 6.7.1.1 “MExE terminal requirements for certificate processing” shall support the X.509 version 3 access-Restriction extension.

X509 version 3 provides a mechanism to define extensions. An Object identifier (OID) is defined for each private extension as defined in X509 [26]. The extension is defined to be within the ETSI Object Identifier (OID) name space.

This extension shall apply irrespective of the presence or otherwise of any other X.509 key usage or extended key usage field.

Normal use of the "critical" flag for extensions apply. That is, if this extension is marked as critical in the certificate used to verify the signature on the application or in any certificate in the chain used to verify the signature and this extension cannot be processed in the MExE device then the certificate shall be considered invalid.

The syntax of the extension is defined in annex C “Access restriction certificate extension”.

6.10 Certificate management

If the 3 MExE security domains defined in clause 6.1 "Generic security" are not supported, then the certificate management described in this clause is optional. The manufacturer may load initial third party certificates on the ME. Downloaded certificates shall be verified by an existing trusted certificate and placed in the domain defined by the root public key at the top of the verification chain for the downloaded certificate.

The administrator root certificate shall be provided on the (U)SIM if support for certificate storage on the (U)SIM exists (e.g. MExE-(U)SIM) or in the MExE device. For (U)SIMs not having certificate storage the administrator root may be downloaded using the root download procedure described in clause 6.13.4 "Administrator root certificate download mechanism".

The actions that may be performed for a given certificate are:

- addition;
- deletion;
- mark un-trusted (un-trusted certificates cannot be used to verify applications or other certificates. This process may be preferred to certificate deletion as there is a chance that the certificate may become trusted again in the near future);
- mark trusted (marking as trusted is the process of allowing an untrusted certificate to come into use again);
- modify fine grain access permissions (proposed as a future enhancement).

The ability to perform these actions depend on the certificate type being modified as well as the access level of the entity performing the operation.

Users may add a third party certificate as long as it is certified by an existing trusted certificate. Using a provisioned functionality, users may delete Third Party certificates.

The Administrator may mark trusted/untrusted Third-Party certificates using Certificate Configuration Messages (see clause 6.10.1 “Certificate configuration message (CCM)”.

Users cannot add or delete any Operator or Manufacturer certificate containing a root public key.

An example of public key infrastructure certificate management protocols can be found in [33].

6.10.1 Certificate configuration message (CCM)

If the 3 MExE security domains defined in clause 6.1 "Generic security" are not supported, then the certificate configuration message described in this clause is optional.

The MExE device shall use the CCM to determine the third party certificates (and only the Third Party certificates) that are trusted for use on the MExE device. The CCM shall only be used to enable or disable third party certificates and can not be used to delete certificates. The CCM may be periodically fetched or downloaded to a MExE device by the Administrator to dynamically configure the third party list using the mechanisms defined in clause 6.10.1.4 "Authorised CCM download mechanisms".

The Certificate Configuration Message shall be as shown in figure 8 "Format of a CCM". This message is essentially a simplified version of a certificate revocation list to satisfy a particular use case. More complex usage requires a full certificate revocation list.

The MExE device may additionally support other means of enabling/disabling root certificates.

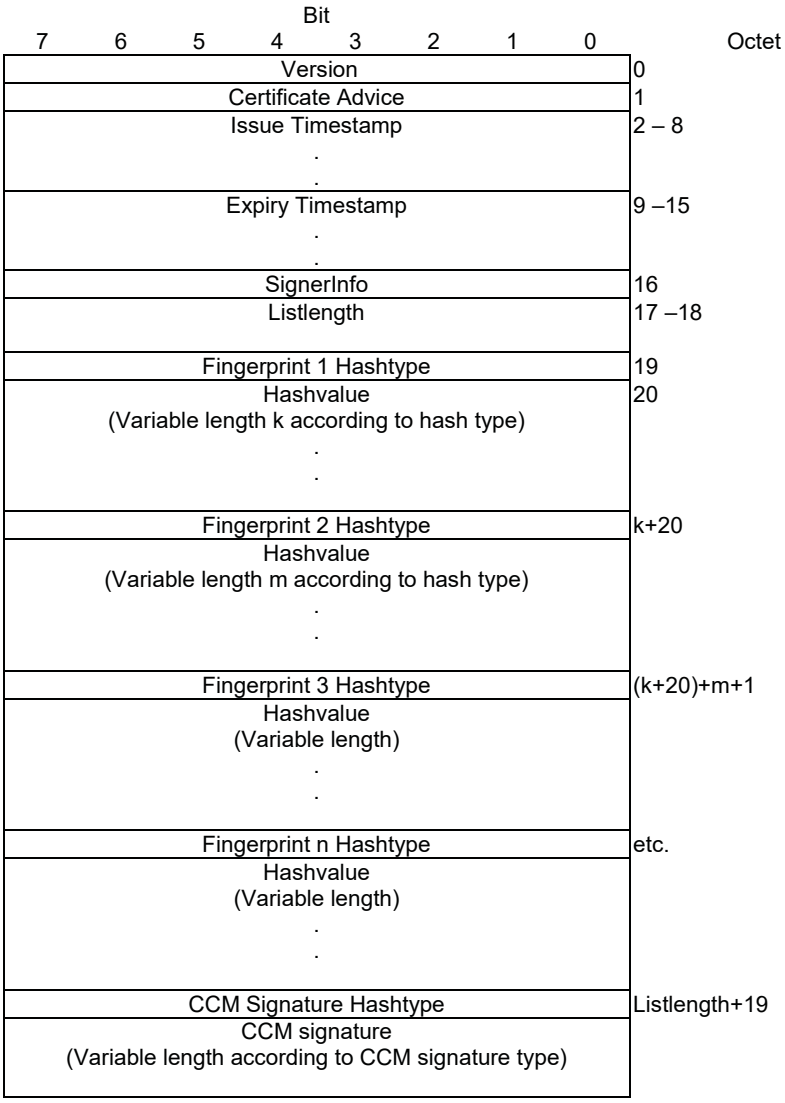


Figure 8: Format of a CCM

Version = The CCM format version is 0. All other values are reserved for future use.

Certificate Advice = enumerated { enable all present and future Third Party certificates (0), disable all present and future Third Party certificates (1), enable present list only (2),enable CCM list (3), disable CCM list (4) }. All other values are reserved for future use.

Issue and Expiry Timestamps = Fields used to identify the issue and expiry date of the CCM. The issue timestamp indicates a time before the current time of day (GMT) when a CCM message must be considered invalid. The expiry timestamp (GMT) identifies the time when a CCM is to be deemed no longer valid. The receiver shall use these parameters to detect a replay attack. A MExE device maintains information on the last valid CCM message received. A replay attack is an attacker replaying a previous valid CCM message to a MExE device in order to change the security settings. This is particularly dangerous for CCM messages used to enable certificates. Administrators should try and set the expiration time to be no longer than the next expected system update time of CCM information. CCM messages used to enable-all (rather than disable-all) certificates should be very short lived as the danger of these being used in a replay attack should be considered serious.

The encoding of time (GMT) shall be coded as an OCTET SEQUENCE of seven octets in length as follows:

Octet 0	1	2	3	4	5	Octet 6
Year		Month	Day	Hour	Minute	Second

Element	Size (bits)	Range
Year	16	$(0 – 65535)_{10}$
Month	8	$(1 – 12)_{10}$
Day	8	$(1 - 31)_{10}$
Hour	8	$(0- 23)_{10}$
Minute	8	$(0 – 59)_{10}$
Second (see note)	8	$(0 – 60)_{10}$
NOTE: The second field range includes the value 60 in order to accommodate leap seconds.		

For example, 1st January, 2001 00:00:30 would be encoded as: 07 d1 01 01 00 00 1E.

SignerInfo = one octet indicating the type of signer information for this CCM. The only currently defined value is device-admin = 0. In this case, no further signer information follows as it is implicit. All other values are reserved for future use.

Listlength = The total length of the fingerprint list not including the final CCM signature. Shall be zero when certificateAdvice = enable-all, disable-all or enable present list.

Hashtype = enumerated { signature (0), MD5 (1), SHA-1 (2) } All other values are reserved for future use.

The length of the Hashvalue field, number of octets output by the selected hash type, is 16 for MD5 [23] or 20 for SHA-1 [24].

The list entries shall contain certificate *fingerprints* in the form of hashes of the encoded signed certificates. The full hash output for the specified algorithm shall be used to generate the fingerprint. A list generator shall check to insure that no two list entries match when creating a list. For an X509v3 [26] or X9.68 (currently being drafted) certificate the fingerprint hash shall be computed over the ASN.1 encoded signed certificate object, first octet to last octet. For WTLS certificates the hash shall be computed over the signed WTLS certificate in network transmission format, first octet to last octet.

The signature type and length shall be indicated by the administrator certificate, which shall be present on the MExE device. If no administrator certificate is on the MExE device or if the signature is not verified, the message shall be rejected.

Upon receipt of a valid certificate configuration message the MExE device shall go through the third party certificate list, computing fingerprints if they are not stored with the certificate and enabling or disabling each certificate according to the following conditions:

- certificateAdvice is enable-all — all Third Party certificates shall be enabled;
- certificateAdvice is disable-all — all Third Party certificates shall be disabled;
- certificateAdvice is enable present list only — enable all Third Party certificates currently on MExE device, do not enable any future certificates (this option allows the list to be frozen at time of manufacture) until Administrator changes;
- certificateAdvice is enable-list — if its fingerprint occurs in the CCM, it shall be enabled, otherwise it shall be disabled;
- certificateAdvice is disable-list — if its fingerprint occurs in the CCM, it shall be disabled, otherwise it shall be enabled.

For future releases, the setting of fine grained permissions for each certificate is expected to be supported.

An implementation shall keep track of the domain that authorised a given executable. If a CCM message is received while MExE executables are currently executing, the implementation shall check to ensure that any executables no longer in the Third Party domain, have their permissions re-configured appropriately and actions that are no longer permissible are terminated.

6.10.1.1 CCM numbering convention

Bits are grouped into octets. The bits of an octet are shown horizontally and are numbered from 0 to 7. Multiple octets are shown vertically and are numbered from 0 to n.

6.10.1.2 CCM order of transmission

Frames are transferred in units of octets, in ascending numerical octet order (i.e., octet 0, 1, …, n-1, n). The order of bit transmission is specific to the underlying protocols used to transport the CCM.

6.10.1.3 CCM field mapping convention

When a field is contained within a single octet, the lowest bit number of the field represents the lowest-order value. When a field spans more than one octet, the order of bit values within each octet progressively decreases as the octet number increases. In that part of the field contained in a given octet the lowest bit number represents the lowest-order value.

For example, a 16 bit number can be represented as shown in figure 9 "Field mapping convention".

Bit								
7	6	5	4	3	2	1	0	
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	1st Octet of field
2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}	2nd Octet of field

Figure 9: Field mapping convention

6.10.1.4 Authorised CCM download mechanisms

The download of third party certificate lists by a remote administrator shall be performed by using a secure mechanism as defined below. The download mechanisms shall use HTTP over IP and/or the WAP Protocol. The URL from which the CCM is downloaded shall be in the administrator certificate if the CCM was not downloaded with the Administrator certificate. The format for storing the URL information with the certificate shall be as shown in figure 10 "CCM Message URL storage format":

Urltype	**CharacterSet**	**UrlLength**	**URL**

Figure 10: CCM Message URL storage format

Urltype= one byte, enumerated {WAP (0), HTTP (1)}. All other values are reserved for future use.

CharacterSet = one byte, Internet Assigned Numbers Authority assigned character set.

UrlLength = one byte unsigned integer, length of the URL in octets.

URL = a field where the format for storing the URL information in the certificate shall be defined as part of the enhanced administrator mechanism.

When the administrator is changed, then the CCM shall also be changed. If there is URL information with the certificate as described in figure 10 "CCM Message URL storage format", then the new CCM shall be obtained using the URL. If the Administrator certificate was downloaded in a JAR file, the CCM shall be obtained from the same JAR file.

6.11 Separation of I/O streams

Support of the separation of I/O streams is mandatory.

Except for the MExE Classmark 3 executables (MIDlets) from the same MIDlet Suite, there shall be strict separation of the user interface input and output streams between different MExE executables, i.e. it shall not be possible for one MExE executable to access the user interface input or output of another MExE executable. In particular, it shall not be possible for an untrusted MExE executable to access the user interface input and output destined for or proceeding from a trusted MExE executable. (This requirement is to prevent a long lived malicious MExE executable from eavesdropping upon on interfering with the user to MExE executables communications, for instance PINs, of a trusted MExE executable).

6.12 Core software download

Support of core software download is optional.

Core software download enables the MExE device radio, characteristics and properties to be updated by changing the software in the MExE device. E.g. a new CODEC may be loaded into a MExE device, a new air interface, etc. This process could include the transfer of executable code and software patches over the air.

This updating of core software (e.g. the Software Defined Radio (SDR) concept) can in principle be generically supported within the MExE framework by a MExE service that executes in the manufacturer security domain, and uses handset manufacturer proprietary APIs. Possible scenarios for the support of this functionality include:

- A MExE service that can be transferred to, and executed in, the manufacturer domain. The service would use manufacturer APIs to perform the software update, radio re-configuration, etc.

- A core software download application that executes in the manufacturers' domain that acts like a user agent in conjunction with a server to transfer software as needed or requested by the user. The core software download application uses manufacturer APIs to perform the software update, radio re-configuration, etc.

Similar functionality may be supported by a downloaded MExE service using manufacturer's OEM classes. All such OEM classes shall comply with the MExE security requirements in table 5 "Security domains and actions" and table 6 "Executable permissions for untrusted MExE executables".

The support of core software download functionality in a MExE device shall only be under the control of the MExE device manufacturer.

6.13 Administrator Concept

6.13.1 Administrator root public key

To help with the control of Third-Party certificates, the ME shall support secure storage for a certificate containing an administrator root public key. The ME shall support the use and management of a certificate containing an Administrator root public key stored on the MExE-(U)SIM and in the ME. The ME shall behave according to clause 6.13.3 “Determining the administrator of the MExE MS”. For support of public key management on the SIM and the USIM refer to 3GPP TS 51.011 [27] and 3GPP TS 31.102 [39] respectively.

A secure mechanism may be used to mark as valid/invalid a certificate containing the administrator root public key on the MExE device. It shall only be possible to use this mechanism to mark a certificate containing a new administrator root public key on the ME as valid, when all administrator root public keys are marked as invalid.

There shall be no more than one valid administrator root public key on the MExE device at any one time. A valid administrator root public key on the (U)SIM shall always have precedence over any administrator root public key on the ME. Any administrator root public key(s) on the ME shall be marked invalid when a valid administrator root public key is present on the (U)SIM.

The MExE device shall support the administrator designation mechanism explained in clause 6.13.2 "Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device" and the secure downloading of CCMs explained in clause 6.10.1.4 “Authorised CCM download mechanisms”.

The user shall not be able to delete an administrator root public key or certificate.

The system shall support a mechanism (as part of a provisioned functionality and/or inherently part of the MExE implementation) allowing the owner of the MExE device to manage the administrator root public key (including the

download of a new administrator root public key) as defined in clause 6.13.3.2.1 "Administrator of the MExE device is the user". This mechanism shall be secure so that only the owner can use this functionality.

The administrator root public key can be downloaded to the MExE device as described in clause 6.13.4 "Administrator root certificate download mechanism".

If the Administrator root public key is stored in the (U)SIM, the ME shall only read the Administrator root public key from the MExE-(U)SIM when required and shall not store the Administrator root public key from the MExE-(U)SIM on the ME in a manner inconsistent with that detailed in clause 6.6.1.1 "Caching of root public keys".

See clause 6.10 "Certificate management" for the management of Administrator root public keys.

The same root public key may be used for both the Administrator role and the operator or manufacturer domain. This facility does not imply any increased right of the manufacturer or operator to take the Administrator role.

If the same root public key is used for the operator domain and Administrator role and this root public key is stored on the MExE-(U)SIM (see [27] and [39]), there shall be separate entries relating to each use of the root public key in the operator and administrator trusted certificate directory files. These entries in the operator and Administrator trusted certificate directory files may point to the same root public key in the certificate data file.

If the root public key to be shared is not stored on the (U)SIM, then procedures relating to this are out of the scope of this specification.

6.13.2 Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device

If the 3 MExE security domains defined in clause 6.1 "Generic security" are not supported, then the administrator concept described in this clause is optional.

All applications in the Third-Party security domain are to be signed by a key which shall be verified back to a Third Party root public key on the MExE device. The Third Party root public keys shall be managed (e.g. addition/mark trusted/mark untrusted) by an administrator that is designated by the owner of the MExE device using the MExE administrator provisioning mechanism. A mechanism is required to be provided to enable the owner of the MExE device to dynamically assign an administrator. The mechanism shall support the following cases:

- the user is the owner;
- the owner is at a remote location. In this case the owner could be the operator, a service provider or a third party;
- the owner of the MExE-(U)SIM wants to be a temporary administrator.

6.13.3 MExE administrator determination mechanism

The administrator of the MExE device shall be determined by a two part logical process with the first part shown in the flowchart in figure 11 "MExE administrator determination mechanism". The second part of the logical process is in figure 12 "MExE administrator determination mechanism, for MExE-(U)SIM supporting third party certificates".

During power-up or MExE-(U)SIM insertion event, the provisioned mechanism shall look for an administrator root public key that is stored on the MExE-(U)SIM.

6.13.3.1 Determining the administrator of the MExE device

If an administrator root public key cannot be found on the MExE-(U)SIM, the provisioned mechanism shall look for one on the MExE device. This leads to the following two cases:

- administrator root public key is absent

  if the administrator root public key is absent, then the user shall automatically become the administrator of the MExE device.

- administrator root public key is present

if an administrator root public key is present, this root public key shall be used for all remote administration authentication, implying that the owner of the administrator root public key is the administrator. Note that the owner of the administrator root public key could be the user.

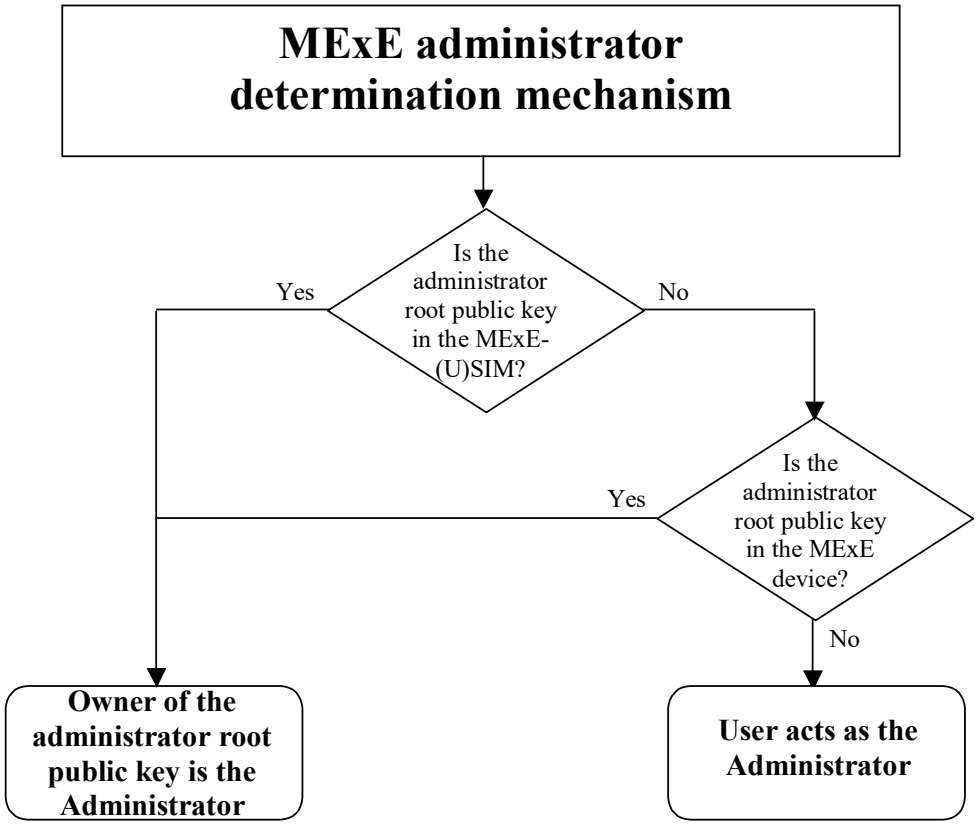


Figure 11: MExE administrator determination mechanism

6.13.3.2 Determining the administrator of the MExE device, for MExE-(U)SIM supporting third party certificates

The second part of the administrator determination mechanism is subsequently defined (see figure 12 "MExE administrator mechanism, for MExE-(U)SIM supporting third party certificates "), and shall be initiated after a power-up or MExE-(U)SIM insertion event is processed.

The following clauses 6.13.3.2.1 "Administrator of the MExE device is the user" and 6.13.3.2.2 "Administrator of the MExE device is not the user" assume that Third Party certificates can be added using the MExE-(U)SIM, however Third Party certificates may be added using a non-(U)SIM approach (e.g. inserted at the time of manufacture, signed package download etc.).

6.13.3.2.1 Administrator of the MExE device is the user

If the administrator is the user, then a check shall be made to determine whether there is a MExE-(U)SIM. If a MExE-(U)SIM is present, then a check shall then be made to determine whether there is a Third Party or an Administrator certificate containing a root public key in the MExE-(U)SIM. The second part of the administrator determination mechanism shall allow the MExE device to determine (via a format) what type of certificate is present:

- certificate present - third party (CP-TP)

  If a Third Party certificate containing a root public key is present in the MExE-(U)SIM then this certificate shall be considered by the MExE device as a Third Party certificate, whilst that valid MExE-(U)SIM application is present in the MExE device. The user shall be queried to allow or disallow the certificate as a Third Party.

- certificate present - administrator (CP-Admin)

If a temporary Administrator certificate containing a root public key is present in the MExE-(U)SIM, the user shall be queried whether to allow the certificate on the MExE-(U)SIM to take temporary control of the third party domain. By temporary control, it is meant that once the card is removed the administrator reverts back to the user administrator settings (i.e. the Administrator becomes the User). The above mechanism implies that the previous configuration settings for the administrator shall be saved, so that they may be restored. If the user disallows the MExE-(U)SIM certificate, the Third Party Domain shall not be able to use any of the network capabilities in the third party domain as identified in the network access section of the security table 5 "Security domains and actions".

If an administrator certificate is not present on the MExE-(U)SIM and the administrator is the user, the user shall continue to be the administrator and may make use of all functionality.

6.13.3.2.2 Administrator of the MExE device is not the user

If the administrator is not the user, then a check is made to determine if there is a MExE-(U)SIM. If a MExE-(U)SIM is present, then a check is made to see if there is a Third Party or an Administrator certificate containing a root public key in the MExE-(U)SIM.

If an Administrator certificate containing a root public key is present in the MExE-(U)SIM, then a comparison is made of this certificate's root public key with the Administrator root public key on the MExE device for the following cases:

- Case (a): they are the same;
- Case (b): they are not the same, but the MExE device certificate is cross-certified with the MExE-(U)SIM certificate (a cross-certificate exists on the MExE device);
- Case (c): they are not the same, but the MExE device certificate has a line of trust back to the MExE-(U)SIM certificate domain;
- Case (d): they are not the same.

If the owner of the public key in the certificate on the MExE-(U)SIM is to be a temporary administrator (CP-Admin), then in cases (a), (b) and (c), the temporary administrator shall be the owner of the CP-Admin root public key. In case (d), the Third Party domain shall not use any of the network capabilities in the third party domain as identified in the network access section of the security table 5 "Security domains and actions".

If the certificate is to be a Third Party certificate containing a root public key, then the certificate (CP-TP) shall be verified with the CCM and based on the content and permissions of the CCM, the certificate shall be added to the Third Party list or rejected.

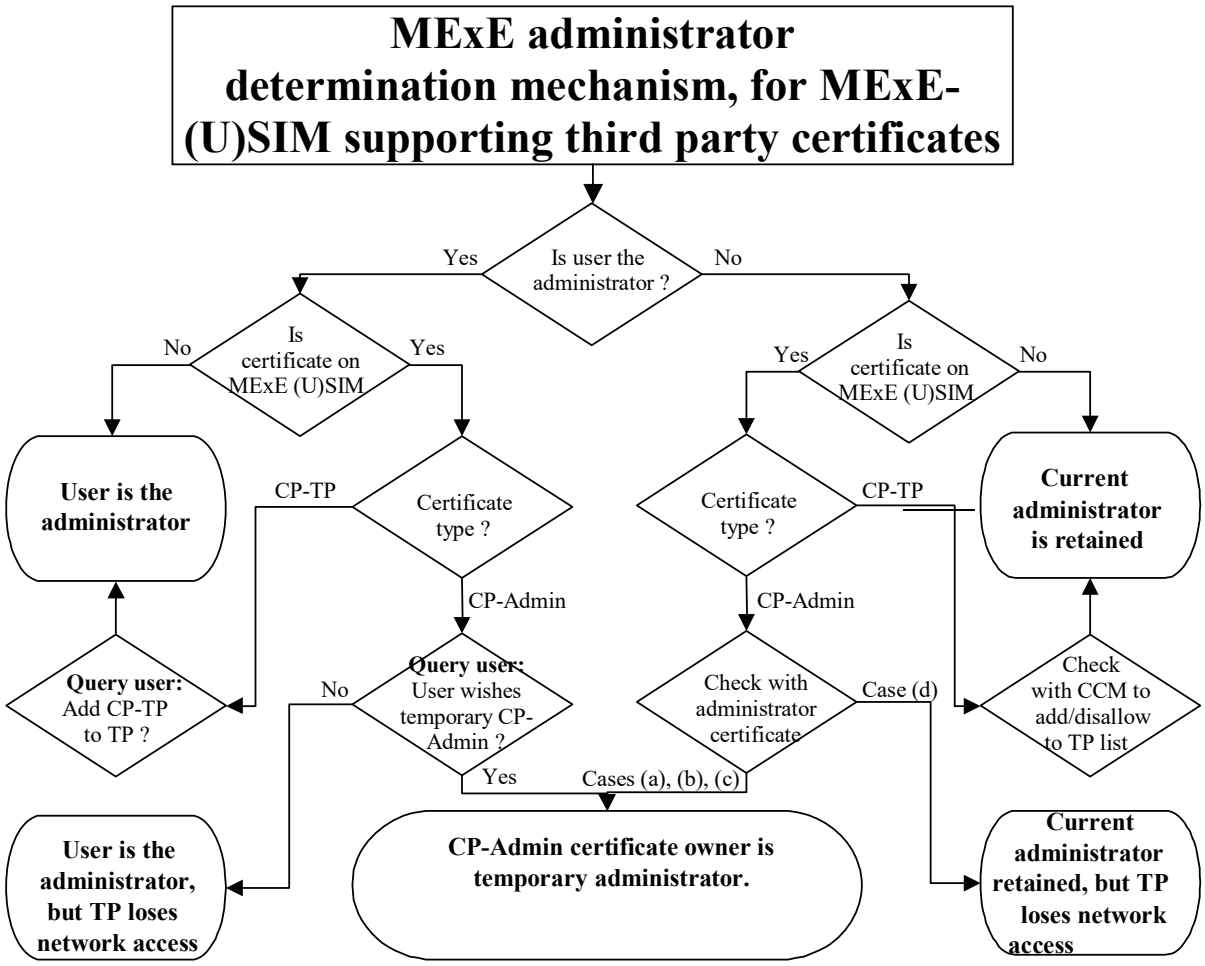


Figure 12: MExE administrator determination mechanism, for MExE-(U)SIM supporting third party certificates

6.13.4 Administrator root certificate download mechanism

MExE devices supporting (U)SIMs without certificates shall at least support the following procedure to download the administrator root certificate.

1. Upon sign-up with an administrator the user and administrator will make contact.
2. The administrator service centre will obtain any required information from the user and inform the user by SMS or other means of the location of the administrator root certificate.
3. The user will initiate the download of the Administrator root certificate using a signed package.
4. Once the procedure is complete the MExE device shall compute the hash of the received Administrator certificate containing root public key.
5. The user will contact the administrator and enters on the MExE device at least the first 8 bytes using decimal value of the hash of the Administrator root public key information provided by the administrator . The MExE device compares the beginning of computed hash value and the abbreviated hash value entered by the user If these two values are the same ,the provisioning process will be complete. If the two values are different this shall be indicated to the user who should inform the administrator of this.

Alternative methods to download an administrator root certificate may be used where appropriate but must insure that the certificate is received by the MExE device unaltered.

7 MExE Classmark 1 (WAP environment)

7.1 Introduction

Classmark 1 MExE devices are based on Wireless Application protocol (WAP).

The Wireless Application Protocol is a standard to present and deliver wireless information and telephony services on mobile phones as well as other wireless terminals. Supporting mandatory features of WAP, WAP enabled devices provide access to the World Wide Web based content for small mobile devices.

7.1.1 WAP MExE devices

Support of WAP in a MExE classmark 1 device as detailed in this clause is mandatory.

WAP MExE devices shall be based on the WAP specifications [6]. In addition to the base specifications in [6], further developments made in the WAP specifications shall form part of this MExE specification.

WAP MExE devices shall implement the WAP version as specified in reference [6], or a later version, under the condition that the version of WAP is backward compatible with the version specified in reference [6].

The existing WAP specification covers security, creation and transfer of WAP executables and content, access, and execution.

7.1.2 High level architecture

The WAP architecture provides a scaleable and extensible environment for application development for mobile communication devices. This is achieved through a layered design of the entire protocol stack.

The key features of WAP include:

- Markup language (WML) and a script language (WMLScript) designed to create applications on the small displays of handheld devices. WML does not assume that a QWERTY keyboard or a mouse is available for user input. Unlike the flat structure of HTML documents, WML documents are divided into a set of well defined units of user interactions. One unit of interaction is called a card, and services are created by letting the user navigate back and forth between cards from one or several WML documents. WML has a smaller set of markup tags that makes it more appropriate to implement in handheld devices, than, say, HTML.

- Light-weight protocol stack to minimise the required bandwidth and to guarantee that a maximum number of wireless network types can run WAP applications. For example, GSM SMS/USSD, circuit switched data (CSD), and GPRS.

- A framework for Wireless Telephony Applications (WTA) allows access to telephony functionality such as call control, phone book and messaging from within WMLScript scripts. This allows operators to develop telephony applications integrated into WML/WMLScript services.

Since WAP is based on a scalable layered architecture, each layer can develop independently of the others. This makes it possible to switch onto new bearers, to use new transport protocols, without major changes in the other layers.

7.2 Non Security

7.2.1 WAP components

Mandatory and optional components of WAP are specified in the WAP specifications. Services and applications shall be able to determine the presence of optional parts of the functionality.

7.2.2 Services

WAP is a general purpose application based on World Wide Web (WWW) technologies and philosophies. Many services can be provided to both WAP clients and traditional WWW clients, from the same server. Services are created based on the same information space. The major difference is the user interface. The user interface of WAP services is realised by the Wireless Markup Language, WML [6], and has a menu tree oriented structure, instead of the traditional flat structure of HTML pages.

Typical WAP services provided to mobile phones may include (this list is not exhaustive):

- News
- Weather information
- Package Tracking
- Stocks
- Telephony Services
- Time Tables
- Access to corporate databases
- Sports

7.2.2.1 User interface

The user interface of WAP services is realised by the Wireless Markup Language, WML [6]. WML does not define the user interface itself, the implementation of the browser defines how the WML data is presented to the user (e.g. hyperlinks are blue and underlined). The script language, WMLScript [6], may be used to enhance the standard browsing and presentation facilities of WML with behavioural capabilities, and to access the device and its peripheral functionality.

7.2.2.2 Access points

Services may be hosted on standard HTTP servers and can be created with proven technologies; CGI, Java Servlets. URLs are used to address services.

The WAP network topology is shown in figure 13 "WAP network topology".

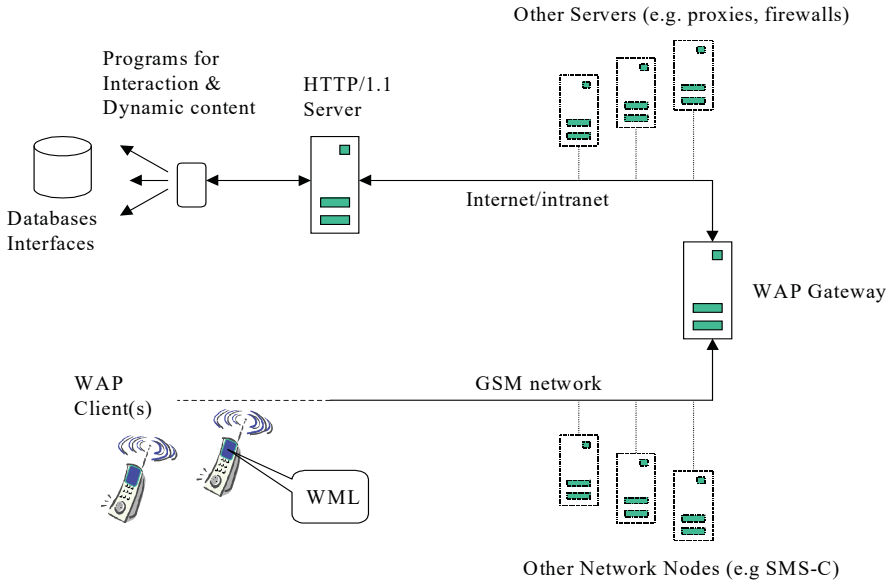


Figure 13: WAP network topology

Mobile phones access services by sending a request with a URI to the WAP gateway. The URI is used to identify the origin server on which the service is available. The request is sent from the mobile phone by the WAP protocols over one of the available bearer networks. The WAP Gateway is a WAP to HTTP/1.1 proxy that translates the WAP request into an HTTP/1.1 request (from binary form to text). The HTTP/1.1 request is passed on to the server identified by the URI.

The HTTP server may have multiple access points to various databases and other services available in the infrastructure network. Once the request has been serviced a response is sent back to the WAP Gateway, which in turn translates it into a WAP response (from text to binary form) and sends it down to the mobile phone.

Note that WAP does not specify anything "behind" the WAP Gateway. However it is assumed that the origin server is an HTTP/1.1 server, and that the WAP Gateway has access to the TCP/IP network on which the origin server is hosted.

7.2.2.3 Transferring

The core of WSP [6] is a binary version of the Hypertext Transfer Protocol - HTTP/1.1 [9]. The core function of WSP is the same as for HTTP/1.1. A client sends a request to the server using an appropriate request method with a URI and information about the client. The server responds with a status code and possibly (if success) the requested content.

There is a differentiation between an origin server and a WSP server. The origin server is where the content is stored, and the WSP server is where the WSP session terminates. The WSP server is also typically the WAP gateway.

In addition to the basic HTTP/1.1 function, WSP has some functions that can not be found in HTTP/1.1, they are:

- Session Establishment and Management
  Before a request is sent, the WSP client can establish a session with the server. During session establishment the client and server exchange static headers. The header are cached for the duration of the session, thus they need to be sent in every single request within the session. Static headers may be: `Accept` headers, `User-agent` header, etc. In addition, capabilities such as supported optional protocol functions, the maximum service data unit the protocol can handle, the maximum number of simultaneously outstanding requests, supported header code pages, etc. can also be exchanged during session establishment.

- Header encoding
  WSP is using a compact binary header encoding to minimise the number of bytes sent over the air.

- Asynchronous transactions
  WSP allows for multiple asynchronous transactions, that is, unordered transactions.

- Transaction Abort
  WSP support abortion of an outstanding transaction.

- Datagram transport
  WSP together with the helper protocol Wireless Transaction Protocol, WTP [9], can run over a datagram transport such as SMS or UDP. The WDP can also be used for non-IP bearers.

- Push
  WSP supports the push of data from server to client. This can be done within and outside of a session. It can be done with and without acknowledgement from the client. Push of indications down to mobile phones is an essential function many wireless applications.

7.2.2.3.1 WSP and HTTP/1.1 Proxy Function

The WAP Architecture is a client-proxy-server architecture. The client is typically a mobile phone, the data gateway is the WAP Gateway and the server is the origin server (a standard HTTP server). The WAP Gateway translates the binary WSP header into text formatted HTTP/1.1 headers and passes them on to the origin server. In the opposite direction the WAP Gateway translates the text formatted HTTP/1.1 header into binary WSP headers. If the WAP Gateway receives a header it does not recognise it simply passes it on as an unknown header. Unknown headers that are not part of the WSP Header Code page or Extended code pages (negotiated at session establishment) are sent in plain text for the client to interpret as best it can.

7.2.3 WAP charging support

The WAP protocol suite in [6], with upgrades as identified in this specification, does not specify mechanisms for charging (e.g. charging records) or subscription management. WAP is bearer independent and is running as an application on top of the bearer network. However the WAP architecture suggests that appropriate charging information can be collected in the WAP Gateway; the point of convergence for all WAP traffic.

The WAP security protocol can be used for authentication of the subscriber.

7.2.4 CC/PP over WSP (Classmark 1)

In Classmark 1, according to the WAP User Agent Profile Specification [17], the CC/PP description is encoded with WBXML [45] after which it is carried over by WSP, [17].

7.3 Security

7.3.1 Call control

WAP telephony services are written in WML and WMLScript. The WAP Telephony API (WTAI) exposes telephony functions to service authors as a set of libraries. The WTAI function libraries can be accessed from WML as URIs, and from WMLScript as script functions. The following libraries have been specified:

- Public library
  This includes functions that are available in all networks, and can be provided by any third party service provider; and not only the network operator. The user must acknowledge the function before it is carried out. Functions have been specified, which can be used e.g. to initiate a mobile originated call, send DTMF tones and add phonebook entry.

- Network Common library
  This includes functions that are available in all networks, and can be provided only by the network operator. E.g. functions for advanced call control, accessing the phonebook, and sending and reading network text (SMS) have been specified.

- Network Specific library
  Functions that are only available in certain types of networks, and can be provided only by the network operator. For GSM, e.g. functions for call reject, call hold, call transfer, multiparty, getting location information and sending USSD have been specified.

The WML and WMLScript author uses the WTAI libraries to create web services for mobile phones with telephony capabilities.

Call control shall be performed using WTA.

7.3.2 Local phonebook

WAP Telephony API (WTAI) is used to access the information stored in the phonebook on the MExE device or the (U)SIM. Phonebook entries consist of name, number and identity. Phonebook entries can be read, written, deleted, and searched for.

8 MExE Classmark 2 (PersonalJava environment)

8.1 Introduction

Classmark 2 specifies Personal Java enabled devices with the addition of the JavaPhone API.

The Personal Java[3] application environment is the standard Java environment optimised for consumer electronic devices designed to support World Wide Web content including Java applets. The Personal Java API is a feature level

subset of J2SE with some Java packages optional and some API modifications necessary for the needs of small portable devices (for example an optimised version of the Abstract Windowing Toolkit targeted to small displays).

JavaPhone[4] is a vertical extension to the Personal Java platform that defines APIs for telephony control, messaging, address book and calendar information, etc.

8.1.1 Classmark 2 MExE devices

Support of PersonalJava in a MExE classmark 2 device as detailed in this clause is mandatory.

MExE Classmark 2 devices shall be based on the API for Personal Java, which defines the required and optional components of Personal Java /JavaPhone APIs that shall be used to realise a Classmark 2 compliant MExE device.

The APIs primarily define the functions available to a Personal Java based MExE device such that services (specified in the form of Java classes and interfaces) can control such a MExE device in a standardised way.

Many aspects of the MExE Classmark 2 API specification are optional. Services and applications shall be able to determine the presence of optional parts of the functionality. When optional parts of the functionality are implemented, the API shall be supported.

8.1.2 High level architecture

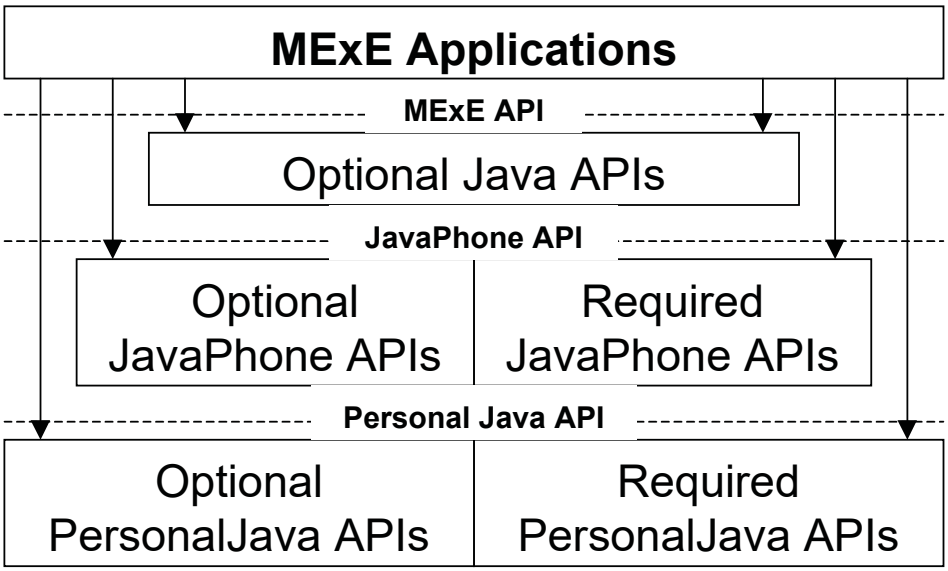


Figure 14: Basic functional architecture of a PersonalJava MExE device

The functional architecture of a Java MExE classmark 2 device is shown in figure 14 "Basic functional architecture of a PersonalJava MExE device". Java applets, applications, and services access functionality via the MExE PersonalJava API. The MExE PersonalJava API is based on a combination of optional Java APIs and the Wireless Profile of the JavaPhone API [4]. The JavaPhone API is based on the PersonalJava API [3].

8.2 Non Security

8.2.1 High level functions

8.2.1.1 Optional Java packages

The use of Java encourages development of modular interfaces and minimal required functionality. Additional functionality is provided by optional APIs specified in terms of the Java language. Java packages are containers for the highest level of functionality in the Java language. In some cases, optional Java packages are specified in terms of Java classes and interfaces. Classes and interfaces are elements contained inside packages.

The following table 9 "Optional Java packages of the Wireless Profile of the JavaPhone APIs" specifies the defined optional Java packages of the Wireless Profile of the JavaPhone APIs [4]. Within some of the packages, certain classes and methods may be individually specified as optional by the JavaPhone API specification.

Where a mandatory package is identified, it is implicit that any packages called by that mandatory package are also mandatory.

Table 9: Optional Java packages of the Wireless Profile of the JavaPhone APIs

JavaPhone API	Java package	Optional/Mandatory
Addressbook	Javax.pim.addressbook	Mandatory
User Profile	Javax.pim.userprofile	Mandatory
Calendar	Javax.pim.calendar	Mandatory
Network	Java.net	Mandatory
Datagram	Javax.net.datagram	Mandatory
Power Monitor	Javax.power.monitor	Mandatory
Power Management	Javax.power.management	Optional
Install	Javax.install	Optional
Communications	Java.comm	Optional
SSL	Javax.net.ssl	Optional
JTAPI Core Package	Javax.telephony	Mandatory
JTAPI Core Capabilities Package	Javax.telephony.capabilities	Mandatory
JTAPI Core Events Package	Javax.telephony.events	Mandatory
JTAPI Call Control Package	Javax.telephony.callcontrol	Optional
JTAPI Call Control Capabilities Package	Javax.telephony.callcontrol.capabilities	Optional
JTAPI Call Control Events Package	Javax.telephony.callcontrol.events	Optional
JTAPI Phone Package	Javax.telephony.phone	Optional
JTAPI Phone Capabilities Package	Javax.telephony.phone.capabilities	Optional
JTAPI Phone Events Package	Javax.telephony.phone.events	Optional
JTAPI Mobile Package	Javax.telephony.mobile	Mandatory
	Java.math	Optional
	Java.rmi	Optional
	Java.rmi.dgc	Optional
	Java.rmi.registry	Optional
	Java.rmi.server	Optional
	Java.security	Optional
	Java.security.interfaces	Optional
	Java.sql	Optional
	Java.io	Optional

8.2.1.2 Required and optional PersonalJava APIs

MExE classmark 2 devices shall support the PersonalJava specification [3]. The PersonalJava APIs provide a standardised and readily implementable execution environment as a means for applications, applets, and content:

- to access and personalise the user interface via the java.awt packages;
- to utilise both Internet and Intranet connections via the java.net package.

8.2.1.3 Required and optional JavaPhone APIs

The JavaPhone APIs extend the PersonalJava APIs to provide functionality unique to telephony devices. MExE classmark 2 devices shall support the Wireless Profile of the JavaPhone API specification [4]. MExE classmark 2 devices shall support all APIs specified as required by the Wireless Profile in the JavaPhone API specification. All APIs that are optional in the Wireless Profile shall be optional in MExE classmark 2 devices.

8.2.1.3.1 Application installation

MExE classmark 2 devices shall support the following JAR file manifest entries (as described in the JavaPhone specification) as described below:

- Implementation-Title

  the Implementation-Title shall be used in any textual description of the application which is displayed in the UI element used to launch the application. E.g. the text displayed with an icon.

- Main-Icon

  the use of icons to launch applications is optional, however if icons are used as elements to launch the application, then the icon file within the JAR file named by the Main-Icon attribute shall be displayed, and may be scaled if desired.

- Main-Class and Class-Path

  when the application is launched, the MExE Java VM shall be supplied with the classpath and shall call the main() method in the class named by the Main-Class attribute.

8.2.1.3.2 Power

MExE classmark 2 devices shall support the Power Monitor package (javax.power.monitor) as specified by the JavaPhone API to access the power level of the MExE device and receive notifications concerning changes in power states.

Note that the Power Monitor package does not specify the minimum required events that should be generated under certain circumstances. MExE classmark 2 device shall at least implement the following event generation:

- BatteryCritical

shall be generated when the battery is at a critically low level.

- BatteryNormal

shall be generated when the battery is no longer low.

All the other event generation should be supported by the implementation.

8.2.1.3.3 Datagram recipient addressing

The syntax described in Concrete Addressing [4] specifies the format to be used for raw text-only GSM SMS messages, UDP datagram via IP, and WAP datagram via GSM SMS message(s).

As a minimum, the formats above shall be supported if the MExE device supports the relevant bearer/transport combination.

NOTE: For the purposes of this clause, "GSM SMS" means SMS as defined by the 3GPP specifications including 3GPP TS 23.040.

8.2.1.4 Required and optional MExE PersonalJava APIs

MExE classmark 2 devices shall not be required to support any other Java APIs.

MExE classmark 2 devices may optionally support any other Java APIs which comply with the MExE security requirements in table 5 "Security domains and actions", such as:

- OCF SmartCard API OpenCard, available from [21]. If the MExE device supports smartcards other than the (U)SIM, and the smartcard is open to 3rd party applications, then the opencard.core.terminal section of the OpenCard API may be used to access the card.

8.2.1.5 Mandated services and applications

8.2.1.5.1 Network protocol support

Support for network protocols in MExE classmark 2 devices is specified in the following table 10 "Support for network protocols":

Table 10: Support for network protocols

Protocol	Optional/Mandatory
HTTP/1.1 [9]	Mandatory
HTTPS	Mandatory
Gopher	Optional
ftp	Optional
mailto [25]	Mandatory
File	Optional

8.2.2 CC/PP over HTTP (Classmark 2)

In Classmark 2 the CC/PP is carried over by using CC/PP over HTTP, [15] and optionally CC/PP over WSP, [17].

8.2.3 Java charging support

MExE Java devices do not require any additional specific charging (e.g. charging records) or subscription management. Java usage of network resources is bearer independent and runs as applications on top of the bearer network.

8.3 Security

If the 3 MExE security domains defined in clause 6.1 "Generic security" are not supported, then the Java security described in this clause is optional.

8.3.1 PersonalJava security

There are two types of Java security [20]: sandbox, and fine grain.

The sandbox model [18] has just one domain; there is no concept of a *partly trusted* domain. The sandbox meaning of "trusted" means it is totally unrestricted to access all system resources.

Using the sandbox system, each MExE security domain shall be implemented as running in a sandbox, configured with different privileges corresponding to those of the domain. If the security domains are not supported then the Java sandbox security model shall be supported and it shall be configured for untrusted MExE executables support only, as defined in clause 6.3 “MExE executable permissions”.Using the fine grain Java security system [19], each MExE security domain will be a set of constraints within which a Java fine grain security domain can be configured.

8.3.1.1 Java applet certification in PersonalJava

Support for trusted applets is optional. Although a Java application shall be executed in a trusted domain if its certification can be validated, a Java Applet will not necessarily be executed in a trusted domain even if it does have a valid signature. It will be up to the implementers to decide if "trusted" Applets will be supported. (In certain implementations, all Applets may be always executed as "untrusted".)

8.3.1.2 Java application signature verification in PersonalJava

The verification of the certification of the application or applet shall be performed as described in clause 6.6 ”Root Public keys” and clause 6.13.2 “Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE MS”.

8.3.1.3 Java loading native libraries in PersonalJava

The MExE Java VM may be able to load native libraries that are intrinsically part of the MExE device implementation and MExE native libraries. The MExE Java VM shall not load other native libraries.

8.3.2 Installing MExE native libraries

A signed native library whose signature verifies as describe in clause 6.6.2 "Manufacturer root public key" as belonging to the Manufacturer Domain may be installed as a "MExE native library".

A MExE native library may be called by a MExE executable, and shall not compromise the MExE security system.

Support of MExE native library signed package installation is optional.

9 MExE Classmark 3 (J2ME CLDC environment)

9.1 Introduction

Classmark 3 MExE devices are based on the Connected Limited Device Configuration (CLDC) with the Mobile Information Device Profile (MIDP).

Java 2 Micro Edition (J2ME) is a version of the Java 2 platform targeted at consumer electronics and embedded devices. CLDC consists of a virtual machine and a set of APIs suitable for providing tailored runtime environments. The J2ME CLDC is targeted at resource constrained connected devices (e.g. memory size, processor speed etc.).

9.1.1 Classmark 3 MExE devices

Support of CLDC/MIDP in a MExE classmark 3 device as detailed in this clause is mandatory.

MExE Classmark 3 devices are based on the J2ME Connected Limited Device Configuration (CLDC) with the Mobile Information Device Profile (MIDP).

All APIs defined by CLDC and MIDP shall be supported by a MExE classmark 3 device.

9.1.2 High level architecture

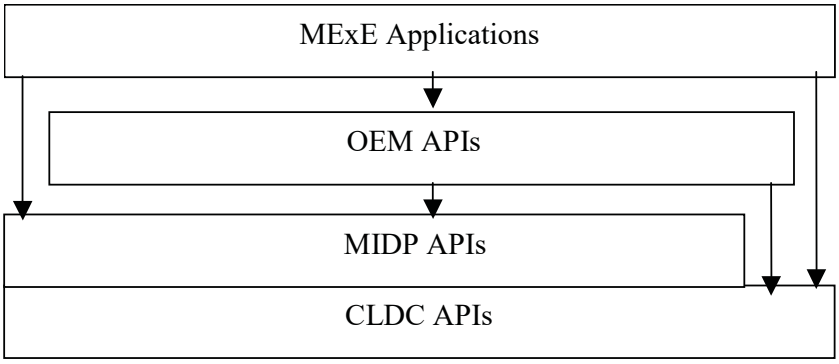


Figure 15: Functional architecture of a Classmark 3 MExE device

The functional architecture of a Classmark 3 MExE device is shown in figure 15 "Functional architecture of a Classmark 3 MExE device". The MExE API is based on the combination of CLDC APIs and MIDP APIs. OEM specific APIs are outside the scope of MExE specification. CLDC and MIDP APIs are defined in J2ME [34] and [35].

9.1.3 High level functionality

J2ME CLDC and MIDP addresses a large market of resource-constrained devices and is aimed to provide complete end-to-end solution for creating dynamically extensible networked products and applications. It allows the use of Java programming language as the standard platform for secure delivery of dynamic content for the extensible next-generation devices.

In order to fit into various types of the devices and support extensibility, J2ME defines in *Configuration* a minimum platform with a virtual machine features and minimum libraries which are available on all devices of similar class. In a *Profile* J2ME addresses the specific demand of a certain category of the devices allowing additional APIs. Profile is implemented on top of configuration (see figure 15 "Functional architecture of a Classmark 3 MExE device"). Classmark 3 MExE device shall be based on the following types of configuration and profile: Connected Limited Device Configuration (CLDC) and Mobile Information Device Profile (MIDP).

9.2 Non Security

9.2.1 Connected Limited Device Configuration (CLDC)

Classmark 3 devices shall support CLDC specification [34].

CLDC provides only high level libraries without focus on any specific device categories. Defining "the lowest common denominator" of Java technology all features included in CLDC must be generally applicable to a wide variety of the devices. CLDC does not address to a certain device category. Such features are specified in a profile. CLDC does not define any optional features.

The classes provided by CLDC are either subset of J2SE (Standard Edition) classes or CLDC specific classes which can be mapped onto J2SE. Classes belonging to the packages: Java.io, Java.lang, Java.util are a subset of corresponding Java2SE libraries, while classes specified in Javax.microedition.io are specific CLDC classes, which, however, can be mapped onto Java2SE.

Javax.microedition.io provides generic connection framework for supporting input/output and networking in a generalized and extensible manner. The framework is a functional subset of Java2SE classes which can be mapped to common low-level hardware or to any Java2SE implementation. It does not provide a set of different kinds of abstractions for different forms of communications, but rather a set of related abstractions are used at the application programming level.

The framework uses a hierarchy of Connection interfaces that group together classes of protocols with the same semantics. The actual supported protocols or implementation of the specific protocols is outside the scope of CLDC Generic Connection Framework and is maintained at the profile level.

The basic set of available Connection interfaces is the following:

- Connection;
- ContentConnection;
- Datagram;
- DatagramConnection;
- InputConnection;
- OutputConnection;
- StreamConnection;
- StreamConnectionNotifier

9.2.2 Mobile Information Device Profile (MIDP)

MExE classmark 3 devices shall support MIDP specification [35]. MIDP is based on CLDC. Some of the features of CLDC are modified or extended by MIDP [35].

9.2.2.1 Networking

While CLDC specifies only a generic Connector used for all types of connections, MIDP extends connectivity support by providing support of the subset of the HTTP protocol. HttpConnection API provides the additional functionality to set request header, parse response headers and perform HTTP specific functions. The API must support RFC 2396 [40] and RFC 2616 [41].

The MIDP does not provide support for datagrams. If a Datagram API is to be implemented, the DatagramConnection interface defined in CLDC shall be used.

9.2.2.2 MID Applications (MIDlet)

A MIDP application (or MIDlet) uses the APIs defined by the MIDP and CLDC specifications. One or more MIDlets may be packed in one JAR file. Sharing of data between MIDlets is controlled by the individual APIs (e.g. Record Management System API).

Application Management Software provides an environment in which a MIDlet is installed, started, stopped and uninstalled. Each JAR file can be accompanied by an Application Descriptor (a text file consisting of name/value pairs), which is used to manage MIDlet and is used by MIDlet for configuration specific attributes. With the help of descriptor file, verification prior to software download is done to ensure that the MIDlet is suited to the device: Java Application Manager checks if the application already exists on the device, verifies the version number (whether an update is needed or not) and reading the JAR-file-size information ensures that there is sufficient amount of memory on the device to save the file. The minimum attributes which the Application Descriptor must contain are the following:

- MIDlet-Name;
- MIDlet-Version;
- MIDlet-Vendor;
- MIDlet-Jar-URL;
- MIDlet-Jar-Size.

Mandatory and optional attributes are defined in [35]. If the mandatory attributes are not identical in the descriptor file and in the manifest file, the JAR file shall not be installed.

9.2.2.3 MIDlet Suites

MIDlets may be packaged together in a single JAR file, forming a MIDlet suite. MIDlets in a MIDlet suite share the classes in the JAR file and the persistent storage is the MIDP Record Management System.

MIDlets in a MIDlet suite may be discovered, transferred, installed and deleted together as a packaged set of MIDlets. The deletion of a MIDlet in a MIDlet suite may result in the deletion of the entire MIDlet suite, in which case the user shall be notified of the deletion of the MIDlet suite.

9.2.2.4 Record Storage

The MIDP provides a mechanism for MIDlets to persistently store data and later retrieve it. The persistent storage mechanism is called Record Management System. Record stores are created in platform-dependent locations and are not exposed to MIDlets. The record store maintains a version number, which is incremented each time the content of the record store is modified. A record store is shared between all MIDlets in a MIDlet suite.

9.2.3 Required and optional MExE APIs

Support of any other Java APIs besides CLDC and MIDP is not mandated in a Classmark 3 MExE device. A Classmark 3 MExE device may optionally support any other Java APIs which comply with the MExE security requirements.

9.2.4 Service discovery and management

A browser installed on a MExE device should support MIME type text/vnd.sun.j2me.app-descriptor. This support allows the user to browse and discover a Java application which can then be downloaded. Capability negotiation

information in the request header can determine which application to present. MIDlets and MIDlet suites should be indicated to the user, and if the MExE device has a display, may be presented as an icon and a tag or as a textual tag only.

A JAD file can be downloaded and used to determine if the MIDlet is deemed suitable for download and installation. If it is suitable, the JAR file can be downloaded and installed. If not, the MExE device should be able to prompt the user so that the user might choose to take such actions such as deletion of some existing applications if there is not enough space to install the new application. If the application chosen to be installed already exists on the device, the user should be notified so that he could take further actions either to download the chosen version or to retain the existing one.

The user should be able either to launch the MIDlet immediately or later.

9.2.5 Transfer of capability negotiation information in Classmark 3

In Classmark 3 the CC/PP is carried over by using CC/PP over HTTP, [15] and optionally CC/PP over WSP, [17].

Also MIDP itself provides a simple mechanism for applications to indicate the capabilities they require. The Java Application Descriptor File (JAD), which is a file that can be stored and downloaded separately to the application itself, contains information such as application name, version number, JAR file size, data storage requirements etc. The Application Descriptor can accompany the JAR file and can be used to ensure prior to the actual application download that the application suits the MExE device. The JAD file is described in more details in the clause 9.2.2.2 " MID Applications (MIDlet)".

9.3 Security

If the 3 MExE security domains defined in clause 6.1 "Generic security" are not supported, then the Java security described in this clause is optional.

9.3.1 CLDC security

A Java execution environment running on a Classmark 3 MExE device shall comply with the security requirements defined in the CLDC specification [34]. That is, it shall comply with both the low-level virtual machine security requirements and the application-level security requirements.

The application-level CLDC security requirements define a sandbox security model where Java classfiles are verified. Java APIs available to the application are limited to those APIs which have been defined by the configuration and profiles supported by the MExE device. Downloading and management of the Java applications on the MExE device takes place at the native level, no user-definable Java class loaders are provided and the set of APIs available to a MIDlet is closed.

The low-level CLDC virtual machine security requirements define a Java classfile pre-verification mechanism which takes place off- MExE device (e.g. on the server prior to downloading) and inserts a special attribute called a "stack map" into class files to facilitate runtime verification of the same classfiles.

10 MExE classmark 4 (CLI Compact environment)

10.1 Introduction

Classmark 4 specifies CLI Compact Profile enabled devices.

The CLI [50] environment is a programming language neutral, OS and CPU portable environment. The CLI can support applications and services written in a wide range of programming languages, for example Visual Basic, ECMAScript and C#. The CLI Compact Profile specifies a minimal set of class libraries, supporting common runtime library features as well as web services infrastructure, including HTTP[9], TCP/IP, XML[36] & SOAP[51]. Such devices not only may have limited memory and CPU capability, but also limited (or no) display.

10.1.1 High level architecture

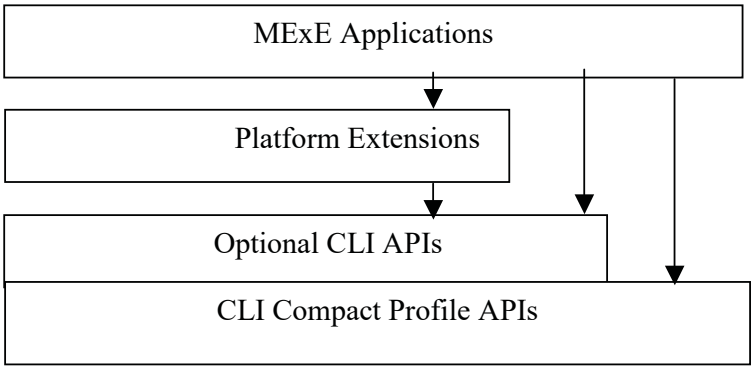


Figure 16: Basic functional architecture of a CLI MExE device

The functional architecture of a CLI MExE classmark 4 device is shown in Figure 16 "Basic functional architecture of a CLI MExE device". CLI based applications and services access functionality via the MExE CLI Compact Profile API. Additional CLI APIs and OEM specific APIs are outside the scope of the MExE specification. The CLI Compact Profile APIs are defined in CLI specified by ECMA [50].

10.2 Non security

Support of CLI Compact Profile in a MExE classmark 4 UE as detailed in this subclause is mandatory.

MExE Classmark 4 devices shall be based CLI Compact Profile specifications [50]. The specifications define the runtime environment and APIs available to a CLI based MExE device such that services (specified in the form of language independent classes and interfaces) can control such a device in a standardised way.

All mandatory components of the CLI compact profile shall be included. Additional CLI APIs or OEM APIs may be available. It shall be possible for services and applications to determine the presence of additional parts of the functionality. When an additional optional CLI component is implemented, the component shall be fully implemented.

10.2.1 High level functionality

CLI provides a language-neutral, CPU and OS portable, secure infrastructure for executing applications and services that interoperate seamlessly with highly available web services. The CLI Compact Profile provides a mobile client-focussed subset of these services on a broad market of connected devices. Using multiple programming languages for application and service creation allows adoption of a large pool of programming talent, as well as interoperability between existing service components.

Functionality is exposed to applications and services in the form of classes and interfaces. Classes can be written in any supported language. APIs can be exposed to the developer using the language syntax of choice. Classes and interfaces are collected into namespaces, which aim to represent a coherent, mutually-dependant set of functionality.

The following Table 11 "CLI Compact Profile Namespaces" specifies the defined mandatory namespaces, i.e. the namespaces defined in the CLI Compact Profile containing classes which are required for CLI Compact Profile conformance.

Table 11: CLI Compact Profile Namespaces

CLI Compact Profile Namespaces
System
System.Collections
System.Globalization
System.IO
System.Text
System.Threading
System.Runtime.CompilerServices
System.Reflection
System.Net
System.XML

The namespaces outlined in Table 11 define the core of the CLI programming model. The System namespace defines data types, including simple data types such as integers, collections such as arrays, and string data types with methods for textual manipulation. System.Globalization enables applications to adapt at runtime to user and cultural UI preferences by modifying list sorting order, currency symbol selection, date and calendar formats, input methods, and language presentation within text strings. The programming model supports threads, with thread manipulation primitives defined in System.Threading. System.Reflection enables progammatic inspection of application metadata such as class structure, properties, and data types on method parameters. System.Net includes support for transport-independent sockets, HTTP connections, and infrastructure for consuming web services. System.XML enables simple parsing and construction of XML objects.

10.2.2 Network protocol support

Support for network protocols in MExE classmark 4 devices is specified in the following Table 12 "Support for network protocols in Classmark 4 devices":

Table 12: Support for network protocols in Classmark 4 devices

Protocol	Optionality
HTTP/1.1 [9]	Mandatory
HTTPS	Mandatory
SOAP [51]	Mandatory
Gopher	Optional
ftp	Optional
mailto [25]	Optional
File	Optional

10.2.3 Power Management

MExE Classmark 4 devices have no application or service accessible APIs to detect the power level of the device. Classmark 4 applications or services may be paused by the MExE device if power passes below a certain threshold. Such an activity is implementation dependant.

10.2.4 CLI charging support

MExE CLI devices do not require any additional specific charging (e.g. charging records) or subscription management. Use of network resources from a CLI application or service is bearer independent and runs as applications on top of the bearer network.

10.2.5 CC/PP over HTTP or WSP (Classmark 4)

In Classmark 4 the CC/PP is carried over by using CC/PP over HTTP [15] and optionally CC/PP over WSP, [17].

10.3 Security

10.3.1 CLI Security

Support of CLI security in a MExE classmark 4 device, as detailed in this clause, is mandatory.

The CLI specification includes a detailed algorithm to verify the safety and integrity of CLI application code, known as "application verification" [50]. An application is either verified as "safe" or "unsafe". The result of the application verification process is presented to the rest of the CLI runtime environment before program execution. This is distinct from the certificate and signature verification that MExE performs before executing an application inside the MExE environment.

Applications that are verified as unsafe may contain code that could potentially access the environment in an unauthorized manner. For example, code that uses pointer arithmetic or accesses arrays using out-of-bounds indices would be deemed unsafe. An unsafe application shall not be permitted to execute in the MExE environment. Once an application is verified as safe, this information is passed on to the rest of the CLI runtime environment, which will then apply the MExE security policy, as specified under clause 6.1, "Generic Security".

The CLI runtime environment may be able to load libraries that are intrinsically part of the MExE device implementation. Such intrinsic libraries may contain unsafe code, however other libraries containing unsafe code are prohibited.

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

A.1 PKCS#15 certificate object attributes presentation

Details from PKCS#15[32] in this Annex A.1 "PKCS#15 certificate object attributes presentation" are for information only.

A.1.1 Object common attributes

Label	human readable label to describe the certificate
Flags	indicates whether the object is private (e.g. CHV authentication request), whether the object is read only.
Authentication object identifier	a cross-reference back to the authentication object, which describes the properties of a CHV, used to protect this object.

A.1.2 Certificate common attributes

identifier	the identifier is used for correlation between the public key contained in the certificate and the associated private key.
Authority	indicates whether the certificate is for an authority (i.e. CA or AA) or not.
Request identifier	used to search a certificate : Issuer and serial number SHA-1 hash, or issuer public key SHA-1hash, or public key subject SHA-1 hash.
Thumbprint	used as secure way to verify that no one has tampered with a certificate: hash on to be signed certificate (internet). MExE uses the thumbprint to enable or disable a certificate through the certificate configuration message (CCM).

A.1.3 Certificate attributes

Type of certificate indicates the type of certificate: WTLS, X509, SPKI, PGP, X9.68.

Value direct value or indirect file path or URL.

MExE only supports storage of WTLS, X509, X9.68 certificates.

A.1.4 Specific X.509 certificate attributes

For information see PKCS#15 [32].

A.2 MExE profile of PKCS#15

`PKCS15CommonObjectAttributes.label` must be present. The value content is unspecified.

`PKCS15CommonObjectAttributes.Flag` must be present. The value shall be private, not modifiable by MExE device.

`PKCS15CommonObjectAttributes.Authentication` must be present. The value shall be "CHV1". The certificates files are protected by CHV1, because MExE need also IMSI to manage domains availability.

PKCS15CommonCertificateAttributes.Id must be present. The value content is unspecified.

PKCS15CommonCertificateAttributes.Authority must be present if and only if certificate is a CA certificate. The value is true.

PKCS15CommonCertificateAttributes.RequestId must be at least present if certificate is an operator or third party root certificate. The value shall be the same as the ones used in the issuer/authority key identifier field of the certificates, provided by this issuer (as in RFC2459 document [43]). The aim of this attribute is to give a easy way to search a key issuer of a received certificate without reading all certificates content.

PKCS15CommonCertificateAttributes.Thumbprint must be at least present if certificate is a third party root certificate. The value shall be the same as the ones used in CCM. The aim of this attribute is to give a easy way to search a certificate with reference included in CCM message.

Domain attribute presence and value shall be added as soon as it will be available in PKCS#15 v1.1.

PKCS15(type)CertificateAttributes.value must be present Value is a indirect file path (path, index, offset). Index and offset default value is 0.

Specific X509 attributes are not supported:

PKCS15X509CertificateAttributes.subject must not be present.

PKCS15X509CertificateAttributes.issuer must not be present.

PKCS15X509CertificateAttributes.serialNumber must not be present.

The MExE device shall recognise all optional present fields above. The MExE device shall accept and ignore all unused fields or new field extensions.

A.3 Coding and storage in MExE-(U)SIM

See detail of file hierarchy and file properties in (U)SIM document [27] and [39].

Since the domain attribute is not available in PKCS#15 v1.0, MExE creates one directory file for each trusted domain. If the domain attribute is available in the next PKCS#15 versions, for future new domains, MExE may create a common directory file. See abstract syntax definition and coding detail in PKCS#15 document [32].

The address of the certificate descriptor Elementary File is fixed.

According to PKCS#15 [32] clause 6.6 "Certificates" , the contents of a certificate descriptor Elementary File must be the *value* of the DER encoding of a **SEQUENCE OF PKCS15Certificate** (i.e. excluding the outermost tag and length bytes).

The address of the certificate data Elementary File is unspecified.

According to PKCS#15 [32] clause 6.6 "Certificates", the certificate data value is coded according to the related certificate type (e.g. DER for X5.09, base64 for SPKI and PGP, WTLS network format for WTLS, DER or PER for X9.68).

Annex B (informative): PKCS#15 certificate objects ASN1 expanded syntax extract

```
{  -- sequence of certificate

x509Certificate,[0] x509AttributeCertificate,[1] spkiCertificate, [2] pgpCertificate,
[3] wtlsCertificate,[4] x9-68Certificate : {

        commonObjectAttributes {

            label  "" UTF8 string OPTIONAL,

            flags  {private (0), modificable (1)} bit string OPTIONAL, --

            authId  octet string OPTIONAL, --

        },

     CommonCertificateAttributes {

            iD      octet string,

            authority boolean default not an authority,

            requestId {

       idtype integer

       IdValueoctet string

                        pkcs15IssuerAndSerialNumber PKCS15KEY-IDENTIFIER::=

                                {SYNTAX PKCS15-OPAQUE.&Type IDENTIFIED BY 1}

                                -- As defined in RFC [CMS]

                        pkcs15SubjectKeyIdentifier PKCS15KEY-IDENTIFIER ::=

                                {SYNTAX OCTET STRING IDENTIFIED BY 2}

                                -- From x509v3 certificate extension

                        pkcs15IssuerAndSerialNumberHash PKCS15KEY-IDENTIFIER ::=

                                {SYNTAX OCTET STRING IDENTIFIED BY 3}

                                -- Assumes SHA-1 hash of DER encoding of IssuerAndSerialNumber

                        pkcs15SubjectKeyHash PKCS15KEY-IDENTIFIER ::=

                                {SYNTAX OCTET STRING IDENTIFIED BY 4}

                                -- Hash method defined in Section 7.

                        pkcs15IssuerKeyHash PKCS15KEY-IDENTIFIER ::=

                                {SYNTAX OCTET STRING IDENTIFIED BY 5}

                                -- Hash method defined in Section 7.

     } OPTIONAL,

     thumbprint   [0] OOBCertHash OPTIONAL, -- hash on to be signed certificate, used for
secure certificate identification as CCM using

        },

        [1] typeAttributes {
```

```
 value indirect : path : {
                path      octet string, -- '4331'H Reference by file identifier
          index    integer OPTIONAL, -- ‘XXXX’H offset in file
          [0] length  integer OPTIONAL, -- ‘XXXX’H length in file
            }
      -- other optional attributes are defined for X509 certificate
        }
    },
}
```

Annex C (normative): Access restriction certificate extension

access-Restriction extension

id-ETSI OBJECT IDENTIFIER ::= {ITU identified-organization (3) ETSI } ::= {ETSI}

id-mexe OBJECT IDENTIFIER ::= {ETSI MExE}

Id-mexe-accessRestriction ::= {id-mexe 1}

AccessRestriction ::= BIT STRING {

network_service_access (0),}

Annex D (informative): MExE executable life cycle

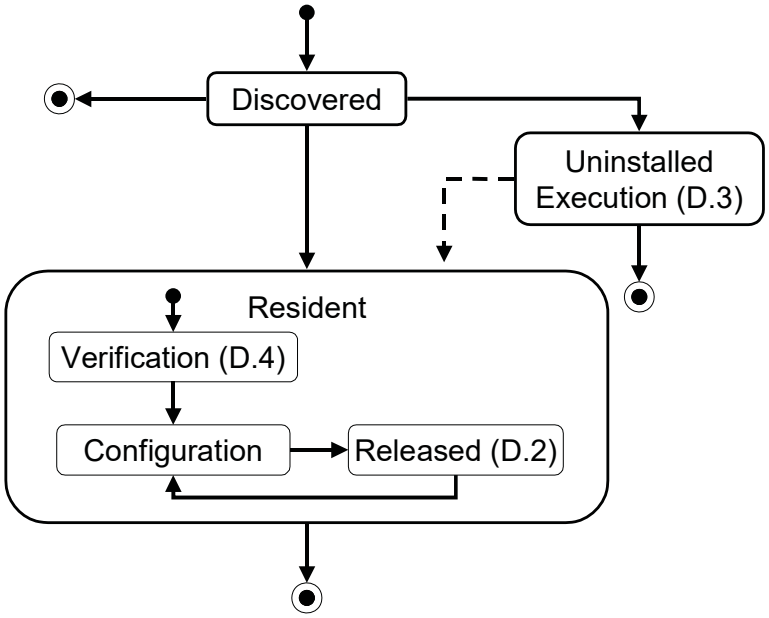
This is a conceptual description of the life cycle of a MExE executable. There may be small deviations in a specific classmark.

The Unified Modelling Language (UML) [38] is used in the description. (This is a brief description of the symbols. A rounded rectangle is a state. An arrow is a transition between states. A dot is an initial state indicating the starting state when the enclosing state is entered. A circle with a dot is a final state. When a final state is activated the enclosing state ends.)

Figures in parenthesis are references to clauses in the specification.

D.1 State of a MExE executable

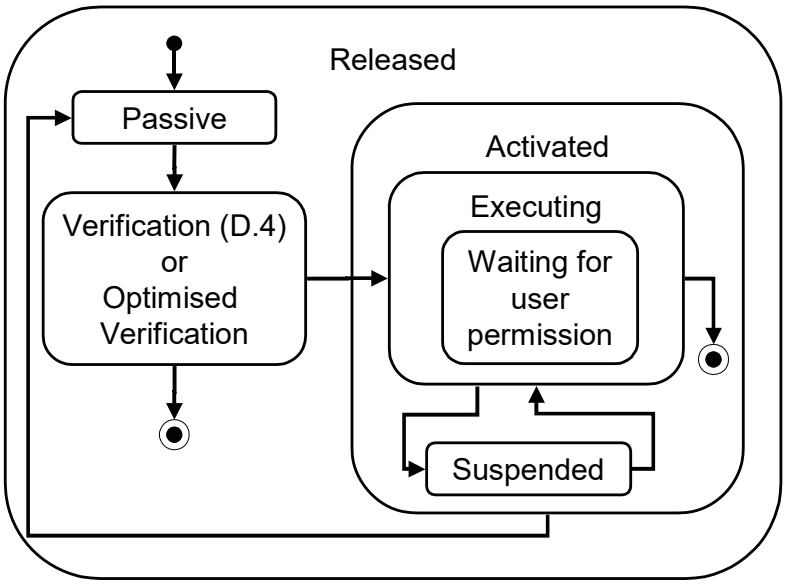
The life cycle of MExE executables (clause 5.3 "Provisioning and management of services") is described using a state machine. In a MExE device a MExE executable can have the following states and transitions between states.



State or Transition (=>)	Description
Initial => Discovered	The MExE executable is discovered (clause 5.3.1 "Service discovery").
Discovered	The MExE executable is discovered and can be installed or executed without installation. (Only executables useable on the MExE device should enter this state.)
Discovered => Resident	The discovered executable is selected to be installed and the executable is transferred (clause 5.3.2 "Service transfer") to the MExE device for installation.
Discovered => Uninstalled Execution	The discovered executable is selected to be executed without installation.
Discovered => final state	The executable is undiscovered.
Resident	The executable is stored in the MExE device. It has been transferred or is pre-loaded.
Verification	This is the initial sub-state of the Resident state. This is a composite state. There is a description of the Verification state in D.4.
Verification => Configuration	The result of the verification indicates that the executable can be installed in one of the Domains.
Configuration	This is a sub-state of the Resident state. The executable can be configured, manually or automatically (clause 5.3.3 "Service installation and configuration").
Configuration => Released	The service is released for execution.
Released	This is a sub-state of the Resident state. The executable is resident, configured and released for execution. This is a composite state and there is a description of it in D.2.
Released => Configuration	The executable is blocked for execution or an executable has changes security domain (The user shall have the possibility to review the configuration before the executable is released for execution with different privileges.).
Resident => final state	The Resident state is left when the service is deleted (clause 5.3.6 "Service deletion"). From the MExE device point of view the executable does not exist any more. (The Integrity and Certification Validation (clause 6.10 "Certificate management") can also force a deletion)
Uninstalled Execution	The executable is executed without installation. This is a composite state. There is a description of the Uninstalled Execution state in D.3.
Uninstalled Execution => final state	The Uninstalled Execution state is left when the executable terminates by itself or when the user terminates the executable (clause 5.3.5 “Service termination”). From the MExE device point of view the executable does not exist any more.
Uninstalled Execution => Resident	This is a possible but unusual transition. A MExE executable that has been used for uninstalled execution is installed without retransferring.

D.2 Released state

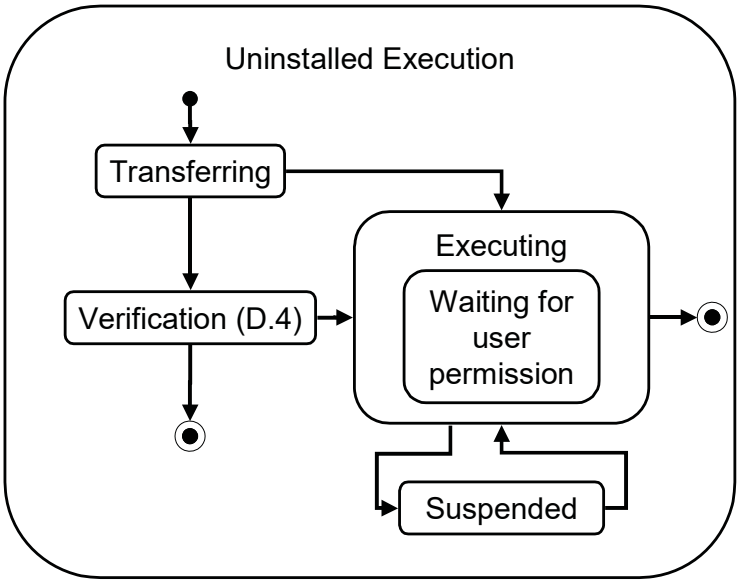
A MExE executable in the Released state is resident, configured and released for execution.



State or Transition (=>)	Description
Passive	This is the initial state. The executable can be invoked.
Passive => Verification	The MExE executable is invoked.
Verification (or Optimised Verification)	The verification can either be done according to the Verification state described in D.4 or as an Optimised Verification described in (clause 6.2.2 "Optimised application signature verification").
Verification => Executing	The result of the verification indicates that the executable may be executed. The Activated state and its sub-state Executing are entered.
Verification => final state	The MExE executable has changed its security state and it must not be executed.
Activated	The MExE executable is activated.
Executing	This is a sub-state of Activated. The executable executes (if it is not waiting for user permission).
Executing => final state	The Executing state is left when the executable terminates by itself. The Activated state is left and the Passive state is entered.
Waiting for user permission	This is a sub-state to Executing. (If there is support for multi-threaded applications, this state can be a state concurrent to the Executing state.) The MExE executable is waiting for permission to perform some action (clause 6.3.1 "MExE executable permissions for operator, manufacturer and third party security domains").
Suspended	This is a sub-state of Activated. The execution is suspended (clause 5.3 "Provisioning and management of services").
Activated => Passive	The Activated state is left when the executable terminates by itself or when the user terminates the executable (clause 5.3.5 "Service termination").

D.3 Uninstalled Execution state

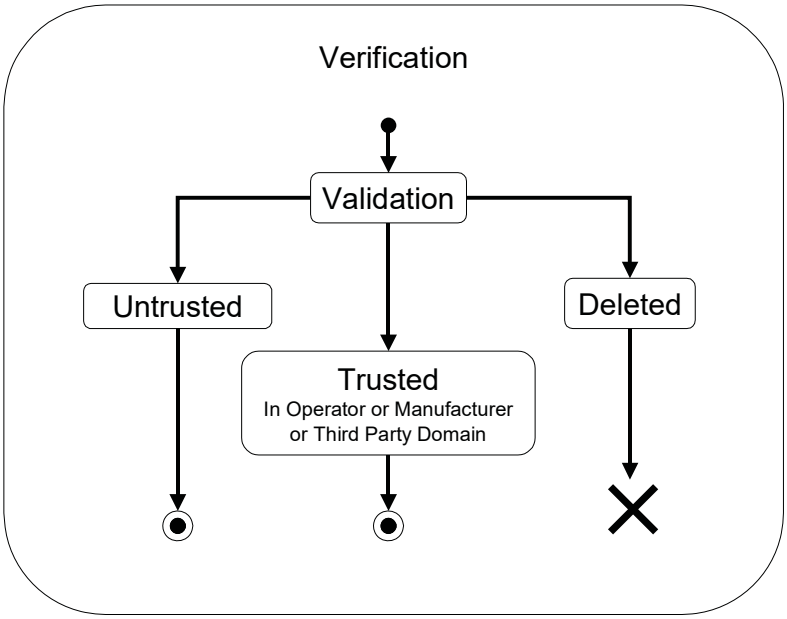
In the Uninstalled Execution state a MExE executable is executed without installation.



State or Transition (=>)	Description
Transferring	This is the initial state of Uninstalled Execution. The MExE executable is transferred to the MExE device.
Transferring => Verification	If the executable is signed the Verification state is entered after the transferring is finished.
Transferring => Executing	If the executable is not signed the Executing state is entered. (To allow streaming, this can be done before the transfer is finished.)
Verification	This is a composite state. There is a description of the Verification state in D.4.
Verification => Executing	The result of verification indicates that the executable may be executed.
Verification => final state	The result of verification indicates that the executable must not be executed and the Uninstalled Execution state is ended.
Executing	The MExE executable is executing.
Executing => final state	The Executing state is left when the execution terminates by itself (The Uninstalled Execution state is left.)
Waiting for user permission	This is a sub-state to Executing. (If there is support for multi-threaded applications, this state can be a state concurrent to the Executing state.) The MExE executable is waiting for permission to perform some action (clause 6.3.1 "MExE executable permissions for operator, manufacturer and third party security domains").
Suspended	The execution is suspended (clause 5.3 "Provisioning and management of services")

D.4 Verification

The integrity and certification validation (clause 6.10 "Certificate management") is done in the Verification state. The result of validation determines the change of state.



State	Description
Validation	This is the initial state. The integrity and certification validation (clause 6.10 "Certificate management") is done.
Untrusted	The executable is untrusted (clause 6.1 "Generic security")
Trusted in Operator Domain	The executable is verified to belong to the Operator Domain (clause 6.1 "Generic security").
Trusted in Manufacturer Domain	The executable is verified to belong to the Manufacturer Domain (clause 6.1 "Generic security").
Trusted in Third Party Domain	The executable is verified to belong to the Third Party Domain (clause 6.1 "Generic security").
Deleted	The executable is not permitted in any Domain and it is deleted.

Annex E (informative): MExE conformance requirements

The table of Conformance Requirements define the minimum set of features that a conformant MExE device must implement.

Legend:-

M - Mandatory feature/requirement

O - Optional feature

N/A - Feature is not applicable: the MExE specification does not prevent this feature from being implemented; however, support of this feature is not required for a MExE device to be regarded as being compliant with a specific MExE Classmark device. Therefore the specification does not indicate whether the feature is optional or mandatory.

M/O – Support as such is required. Mandatory and Optional features are gathered into a table

ID	Requirement	Reference	CM1	CM2	CM3
4-1	Support of at least one MExE classmark on a MExE device	4	M	M	M
4-2	Support of multiple combinations of MExE classmarks	10.1	O	O	O
4-3	Support of WAP	4.2.5	M	O	O
4-4	If Classmark 1 services are supported by non-Classmark 1 devices, Classmark 1 services shall execute in the same manner as they execute in a MExE Classmark 1 device	4.5.1	N/A	M	M
4-5	Support of PersonalJava	8.1, 8.1.1	O	M	O
4-6	If Classmark 2 services are supported by non-Classmark 2 devices, Classmark 2 services shall execute in the same manner as they execute in a MExE Classmark 2 device.	4.5.2	M	N/A	M
4-7	Support of CLDC and MIDP	9.1, 9.1.1	O	O	M
4-8	If Classmark 3 services are supported by non-Classmark 3 devices, Classmark 3 services shall execute in the same manner as they execute in a MExE Classmark 3 device.	4.5.3	M	M	N/A
4-9	Support of capability negotiation process	4.2	M	M	M
4-10	Support for interaction between the MExE device and the MSE by the use of HTTP/1.1or HTTP/1.1 derived protocol (e.g. WSP)	4.2	M	M	M
4-11	Support of the properties in the UAProf schema for capability negotiation	5.2.1	M/O	M/O	M/O
4-12	Support of content negotiation	4.2	O	O	O
4-13	Support of user profiles	5.2	O	O	O
4-14	Support of more than one user profile (if user profiles supported)	5.2.2	O	O	O
4-15	Ability to retain the user profile in the network (if user profiles supported)	5.2.2	O	O	O
4-16	User permission for retaining the user profile in the network (if user profiles supported)	5.2.2	M	M	M
4-17	Support of direct and indirect referencing mechanisms in retrieval of MExE preferences (if user profiles supported)	8.2.2	O	O	O
4-18	Support of the properties in the UAProf schema for user preference information (if user profiles supported)	8.2.2	M	M	M
4-19	Support of user interface personalisation	5.1	O	O	O
4-20	Support of direct and indirect referencing mechanisms in retrieval of user interface personalisation preferences	5.1.1	O	O	O
4-21	Ability to support VHE	9.2.5	O	O	O

ID	Requirement	Reference	CM1	CM2	CM3
4-22	Storage of the VHE characteristics as a part of the user profile (if VHE and user profile is supported)	9.2.5	M	M	M
4-23	Capability to discover new services	5.1.3.1	M	M	M
4-24	Support for a browser for service discovery	5.1.3.1	O	O	O
4-25	Ability to control service installation and configuration	4.10.3	N/A	M	M
4-26	Ability to determine which services are transferred to, resident, configured or executing on the MExE device (provide the name and, if available, version number)	4.10.4	M	M	M
4-27	Service termination capability	4.10.5	M	M	M
4-28	Capability to delete a service	4.10.6	M	M	M
4-29	User's ability to terminate or suspend any active connection associated with any MExE executable	5.3	M	M	M
4-30	User's ability to obtain information on all connections associated with any MExE executable on the MExE device	5.3	M	M	M
4-31	Support of journaling of network events by MExE executables	5.4	M	M	M
4-32	Management of the journal by the MExE device, with no access to it by MExE executables	5.4	M	M	M
4-33	Indicate whenever network activity is in progress	5.4.1	O	O	O
4-34	Support of QoS management by MExE	5.4.2, 9	O	O	O
4-35	Support of core software download functionality	5.5	O	O	O
4-36	Core software download (if supported) only under control of the MExE device manufacturer	5.5	M	M	M
5-1	Call control using WTA scripts	7.3.1	M	O	O
6-1	Support of the Wireless Profile of the JavaPhone API specification (Optional Java packages of Wireless Profile of the JavaPhone APIs as presented in Table 9 "Optional Java packages of the Wireless Profile of the JavaPhone APIs")	8.2.1.1, 8.2.1.3	O	M/O	O
6-2	Support of the JAR file manifest entries as per JavaPhone specification	8.2.1.3.1	O	M	O
6-3	The use of icons to launch applications	8.2.1.3.1	O	O	O
6-4	If icons are used as elements to launch the application, then the icon file within the JAR file named by the Main-Icon attribute shall be displayed	8.2.1.3.1	O	M	O
6-5	Implementation of "BatteryCritical", "BatteryNormal" event generation	8.2.1.3.2	O	M	O
6-6	Support for the following formats in Datagram recipient addressing: raw text-only GSM SMS message, UDP datagram via IP, and WAP datagram via GSM SMS message(s)	8.2.1.3.3	O	M	O
6-7	Support any other Java APIs which comply with the MExE security requirements in Table 5 "Security domains and actions"	8.2.1.4	O	O	O
6-8	Support for network protocols as per table 10 "Support for network protocols"	8.2.1.5.1	O	M/O	O
6-9	Support of MIDlet discovery and management via a browser using MIME type text/vnd.sun.j2me.app-descriptor	9.2.4	O	O	O
6-10	Indication of MIDlets and MIDlet suites to the user (with a tag or icon and tag)	9.2.4	O	O	O
7-1	Support of charging regimes of MExE services (charging mechanisms are outside the scope of MExE specification).	5.6.1	O	O	O
8-1	Support of the untrusted area	6.1	M	M	M
8-2	Support of all three security domains together (i.e. operator, manufacturer and third party), or no security domains at all	6.1	M	M	M
8-3	Security restrictions shall apply to MExE executables when API functionality is directly or indirectly called by MExE executables	6.3	M	M	M
8-4	Support for permissions of operator, manufacturer and third party security domains in the order of restriction (as defined in table 5 of MExE specification).	6.3.1	M	M	M
8-5	Access by MExE untrusted executables limited to the functionality specified in the table 6 of MExE specification	6.3.2	M	M	M
8-6	Separation of the user interface input and output streams between different MExE executables (except for the MIDlets in the same MIDlet suite)	6.11	M	M	M
8-7	Support of single action permission with a prompt for the user	6.5	M	M	M
8-8	Support of session permission and blanket permission with a prompt for the user	6.5	O	O	O
8-9	Indication to the user whenever user permission is sought by an untrusted MExE executable	6.5	M	M	M
8-10	Ability of the user to request to be informed of the "subject" field of the	6.5	M	M	M

ID	Requirement	Reference	CM1	CM2	CM3
	certificate of the signer (if secure domains supported)				
8-11	Support for public key based solution of content authentication (if secure domains supported)	6.7	M	M	M
8-12	Support of certificate chains (if secure domains supported)	6.7	M	M	M
8-13	Support at least one level of certificate under operator, manufacturer or Third Party root public keys (if secure domains supported)	6.7	M	M	M
8-14	Secure installation of root public keys in the MExE device (if secure domains supported)	6.7.1	M	M	M
8-15	Prohibition to share public keys between domains (if secure domains supported)	6.7.1	M	M	M
8-16	Support the use and management of an operator root public key on the (U)SIM (if secure domains supported)	6.6.1	M	M	M
8-17	Prohibition of the user to add or delete any type of operator public keys (if secure domains supported)	6.6.1	M	M	M
8-18	Support of operator and manufacturer disaster recovery root public keys (if secure domains supported)	8.5.	O	O	O
8-19	Support of the use and management of the operator root public key (if secure domains supported)	8.5.1.	M	M	M
8-20	Support of the use and management of the manufacturer root public key (if secure domains supported)	6.6.2	M	M	M
8-21	Support of the use and management of the third party root public keys (if secure domains supported)	6.6.3	M	M	M
8-22	Support of the use and management of the administrator root public key (if secure domains supported)	6.13.1	M	M	M
8-23	Support of the administrator designation mechanism (if secure domains supported)	6.13.1	M	M	M
8-24	Support of the certificate configuration management (if secure domains supported)	6.10	M	M	M
8-25	Use of the CCM by MExE device to determine the third party certificates that are trusted for the use on the MExE device (if secure domains supported)	6.10.1	M	M	M
8-26	Additional support of other means to enable/disable root certificates (if secure domains supported)	6.10.1	O	O	O
8-27	Support of authorised CCM download mechanisms (if secure domains supported)	8.7.	M	M	M
8-28	When the administrator is changed, then the CCM shall also be changed. (if secure domains supported)	8.7.	M	M	M
8-29	Support of provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device (if secure domains supported)	6.13.2	M	M	M
8-30	Support of the cases: the user is the owner, the user is at remote location, the owner of the MExE-(U)SIM wants to be a temporary administrator (if secure domains supported)	6.13.2	M	M	M
8-31	Support for determining the administrator of the MExE device (if secure domains supported)	6.13.3	M	M	M
8-32	Either sandbox or fine grain Java security shall be supported	8.3.1	N/A	M	N/A
8-33	Support for trusted applets (if secure domains supported)	8.3.1	N/A	O	O
8-34	Verification of the certification of the application or applet (if secure domains supported)	8.3.1.2	M	M	M
8-35	Java loading native libraries that are intrinsically part of the MExE device implementation, and MExE native libraries	8.3.1.3	O	O	O
8-36	No loading of other native libraries	8.3.1.3	N/A	M	N/A
8-37	Support of the JAR file format devices for securely packaging objects that are to be downloaded and installed on the MExE device	10.3.1	N/A	M	M
8-38	Support for other proprietary means of downloading and installing objects	10.3.1	O	O	O
8-39	Support of MExE native library signed package installation	8.3.2	N/A	O	O
8-40	Support for the case when a certificate containing an Administrator root public key is thus contained in a signed package, the signed package (JAR) shall contain two files: the Administrator root public key and the CCM (if secure domains supported).	6.8.2	N/A	M	M
8-41	Support of installation of other signed data (e.g. proprietary binaries or Java classes such as native DSP code, provisioned functionality upgrades and patches) (if secure domains supported).	6.8.3	O	O	O
8-42	Support for administrator root certificate mechanism (if secure domains supported).	6.13.4	M	M	M

ID	Requirement	Reference	CM1	CM2	CM3
8-43	Support of alternative methods to download an administrator root certificate (if secure domains supported).	6.13.4	O	O	O
8-44	Support of optimised signature verification of applications (if secure domains supported).	6.8.1	O	O	O
9-1	Support of QoS API by MExE device	9	O	O	O
9-2	Support of a basic QoS operations	5.5.2	O	O	O
9-3	Support of MExE QoS API by MExE QoS Manager	5.5.3	O	O	O
9-4	Provision of the MExE QoS Manager functions	5.5.3	O	O	O
9-5	Ability to manage QoS through the MExE device's MMI	5.5.3	O	O	O
9-6	QoS control by MExE QoS Manager, if it is not provided in the network control	5.5.4	O	O	O
9-7	Provision of a standard set of parameters by a QoS API to MExE executable	5.5.5	O	O	O
9-8	Ability of MExE QoS Manager to deal independently with each of the several simultaneous QoS streams	5.5.7	O	O	O

Annex F (informative): Change history

TSG	T-Tdoc	T2-Tdoc	CR	Rev	Rel	Subject	Cat	Version-Current	Version-New
T#16	TP-020102	T2-020393	118		Rel6	Restructuring of the MExE-specification	D	5.0.0	6.0.0
T#17	TP-020202	T2-020652	119		Rel6	CC/PP section cleanup	D	6.0.0	6.1.0
T#17	TP-020202	T2-020660	120		Rel6	Adding new attributes to the JAR manifest file	C	6.0.0	6.1.0
T#21	TP-030169	T2-030400	122		Rel6	Correcting figure and table numbering	D	6.1.0	6.2.0
-	-	-	-	-	Rel-7	Update to Rel-7 version (MCC)	-	6.2.0	7.0.0

History

Document history		
V7.0.0	June 2007	Publication