



**SLOVENSKI STANDARD**  
**SIST EN 300 812-3 V2.2.1:2006**

01-april-2006

---

Df]nYa b]gbcj b]fUX]c`fH9HF5L!`Ja Ygb]`a YX`bUfc b]y`c`]XYbh]Z`UW]g`c`  
\_Uf]Wc`]b`a`cV]bc`cdfYa`c`fG`A!A9L!`"XY.`bHY[ f]fUbc`j`Yn`Y`f7L!`:]n] bYz`c[ ] bY  
]b`HG`A`Ud`]`UW]g`Y`\_UfU`hYf]gh`\_Y`

Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 3: Integrated Circuit (IC); Physical, logical and TSIM application characteristics

**ITeH STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN 300 812-3 V2.2.1:2006](https://standards.iteh.ai/catalog/standards/sist/6706ba22-b348-437e-9fa3-9da6a34a48d5/sist-en-300-812-3-v2-2-1-2006)

<https://standards.iteh.ai/catalog/standards/sist/6706ba22-b348-437e-9fa3-9da6a34a48d5/sist-en-300-812-3-v2-2-1-2006>

**Ta slovenski standard je istoveten z: EN 300 812-3 Version 2.2.1**

---

**ICS:**

33.070.10	Prizemni snopovni radio (TETRA)	Terrestrial Trunked Radio (TETRA)
-----------	---------------------------------	-----------------------------------

**SIST EN 300 812-3 V2.2.1:2006** en

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST EN 300 812-3 V2.2.1:2006

<https://standards.iteh.ai/catalog/standards/sist/6706ba22-b348-437e-9fa3-9da6a34a48d5/sist-en-300-812-3-v2-2-1-2006>

# ETSI EN 300 812-3 V2.2.1 (2004-02)

---

*European Standard (Telecommunications series)*

**Terrestrial Trunked Radio (TETRA);  
Subscriber Identity Module to  
Mobile Equipment (SIM-ME) interface;  
Part 3: Integrated Circuit (IC);  
Physical, logical and TSIM application characteristics**

---

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN 300 812-3 V2.2.1:2006](https://standards.iteh.ai/catalog/standards/sist/6706ba22-b348-437e-9fa3-9da6a34a48d5/sist-en-300-812-3-v2-2-1-2006)

<https://standards.iteh.ai/catalog/standards/sist/6706ba22-b348-437e-9fa3-9da6a34a48d5/sist-en-300-812-3-v2-2-1-2006>



## Reference

---

REN/TETRA-03102

## Keywords

---

card, security, SIM, TETRA**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

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST EN 300 812-3 V2.2.1:2006<https://standards.iteh.ai/catalog/standards/sist/6706ba22-b348-437e-9fa3-9da6a34a48d1/sist-en-300-812-3-v2-2-1-2006>  
**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](mailto: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 2004.  
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.

# Content

Intellectual Property Rights .....	8
Foreword.....	8
1 Scope .....	9
2 References .....	9
3 Definitions, symbols and abbreviations .....	11
3.1 Definitions .....	11
3.2 Symbols.....	13
3.3 Abbreviations .....	13
4 SIM characteristics .....	15
4.1 Format and layout.....	15
4.1.1 SIM .....	15
4.1.2 Plug-in SIM .....	15
4.2 Temperature range for card operation .....	15
4.3 Contacts.....	15
4.3.1 Provision of contacts.....	15
4.3.2 Activation and deactivation .....	16
4.3.3 Inactive contacts (contact conditions in the ME switched-off state).....	16
4.3.4 Contact pressure.....	16
4.4 Precedence (multiple SIM operation).....	16
4.5 Static protection.....	17
5 Electronic signals and transmission protocols.....	17
5.1 Supply voltage Vcc (contact C1).....	17
5.1.1 5 V technology SIM.....	17
5.1.2 3 V technology SIM.....	17
5.1.3 3 V technology SIM identification.....	17
5.1.4 3 V technology ME.....	17
5.1.5 3 V Only ME .....	18
5.1.6 Activation and deactivation of 3 V technology SIM .....	18
5.1.7 Supply voltage switching.....	18
5.1.8 Cross compatibility .....	18
5.1.9 Technology outlook .....	18
5.2 Reset (RST) (contact C2) .....	18
5.3 Programming voltage Vpp (contact C6).....	18
5.4 Clock CLK (contact C3).....	18
5.5 Input/Output (I/O) (contact C7).....	19
5.6 States .....	19
5.7 Baud rate .....	19
5.8 Answer To Reset (ATR).....	19
5.9 Bit/character duration and sampling time.....	19
5.10 Error handling .....	19
6 Logical model.....	20
6.1 General description.....	20
6.2 File identifier .....	20
6.3 Dedicated Files (DF) .....	21
6.4 Elementary Files (EF) .....	21
6.4.1 Transparent EF.....	21
6.4.2 Linear fixed EF .....	21
6.4.3 Key EF .....	22
6.4.4 Cyclic EF .....	23
6.5 Methods for selecting a file .....	23
6.6 Reservation of file IDs .....	24
7 Security features .....	25
7.1 Authentication and cipher key generation procedure .....	25

7.2	Support of Over The Air Re-keying (OTAR) distribution of cipher keys.....	26
7.3	Support of SIM-ME enhanced security .....	26
7.4	File access conditions .....	26
7.5	Storage of DCK.....	27
8	Description of the functions .....	27
8.1	SELECT .....	28
8.2	STATUS.....	28
8.3	READ BINARY.....	28
8.4	UPDATE BINARY .....	29
8.5	READ RECORD.....	29
8.6	READ KEY.....	30
8.7	UPDATE RECORD.....	30
8.8	SEEK.....	31
8.9	VERIFY CHV .....	31
8.10	CHANGE CHV.....	32
8.11	DISABLE CHV.....	32
8.12	ENABLE CHV .....	32
8.13	UNBLOCK CHV .....	33
8.14	INVALIDATE .....	33
8.15	REHABILITATE.....	33
8.16	TETRA authentication algorithms .....	33
8.16.1	GET RANDOM.....	34
8.16.2	TA11/TA12 ALGORITHM.....	34
8.16.3	TA21/TA22 ALGORITHM.....	34
8.16.4	TB4/TE ALGORITHM .....	34
8.17	OTAR algorithms.....	35
8.17.1	TA32 ALGORITHM.....	35
8.17.2	TA41/TA82 ALGORITHM.....	35
8.17.3	TA41/TA52 ALGORITHM.....	35
8.17.4	TA71/TE ALGORITHM .....	36
8.17.5	TB7/TA52 ALGORITHM.....	36
8.17.6	TA41/TA92 ALGORITHM.....	36
8.17.7	TB7/TA52 ALGORITHM.....	36
9	Description of the commands.....	37
9.1	Mapping principles.....	37
9.2	Coding of the commands.....	39
9.2.1	SELECT.....	40
9.2.2	STATUS.....	42
9.2.3	READ BINARY .....	42
9.2.4	UPDATE BINARY .....	42
9.2.5	READ RECORD .....	42
9.2.6	UPDATE RECORD .....	43
9.2.7	READ KEY .....	43
9.2.8	SEEK .....	43
9.2.9	VERIFY CHV .....	44
9.2.10	CHANGE CHV .....	44
9.2.11	DISABLE CHV .....	44
9.2.12	ENABLE CHV .....	44
9.2.13	UNBLOCK CHV.....	45
9.2.14	INVALIDATE.....	45
9.2.15	REHABILITATE .....	45
9.2.16	GET RANDOM.....	45
9.2.17	TA11/TA12 ALGORITHM.....	45
9.2.18	TA21/TA22 ALGORITHM.....	46
9.2.19	TB4/TE ALGORITHM .....	46
9.2.20	TA32 ALGORITHM.....	46
9.2.21	TA41/TA82 ALGORITHM.....	47
9.2.22	TA41/TA52 ALGORITHM.....	47
9.2.23	TA71/TE ALGORITHM .....	47
9.2.24	GET RESPONSE.....	47
9.2.25	TB7/TA52 ALGORITHM.....	48

9.2.26	TA41/TA92 ALGORITHM.....	48
9.2.27	TB7/TA82 ALGORITHM.....	48
9.3	Definitions and coding .....	48
9.4	Status conditions returned by the card.....	50
9.4.1	Responses to commands which are correctly executed .....	50
9.4.2	Memory management .....	50
9.4.3	Referencing management .....	50
9.4.4	Security management.....	50
9.4.5	Application independent errors.....	51
9.4.6	Commands versus possible status responses .....	51
10	Contents of the EFs .....	52
10.1	General requirements .....	52
10.2	Contents of the EFs at the MF level .....	52
10.2.1	EF <sub>ICCID</sub> (Card Identification).....	52
10.2.2	EF <sub>DIR</sub> (Application directory) .....	53
10.2.3	EF <sub>LP</sub> (Language Preference) .....	54
10.3	Contents of the EFs at the TETRA application level .....	54
10.3.1	EF <sub>SST</sub> (SIM Service Table) .....	54
10.3.2	EF <sub>ITSI</sub> (Individual Tetra Subscriber Identity) .....	57
10.3.3	EF <sub>ITSIDIS</sub> (ITSI Disabled).....	59
10.3.4	EF <sub>UNAME</sub> (Username) .....	60
10.3.5	EF <sub>SCT</sub> (Subscriber Class Table).....	60
10.3.6	EF <sub>PHASE</sub> (Phase identification) .....	62
10.3.7	EF <sub>CCK</sub> (Common Cipher Key) .....	62
10.3.8	EF <sub>CCKLOC</sub> (CCK location areas) .....	64
10.3.9	EF <sub>SCK</sub> (Static Cipher Keys).....	68
10.3.10	EF <sub>GSSIS</sub> (Static GSSIs) .....	70
10.3.11	EF <sub>GRDS</sub> (Group related data for static GSSIs) .....	71
10.3.12	EF <sub>GSSID</sub> (Dynamic GSSIs).....	73
10.3.13	EF <sub>GRDD</sub> (Group related data for dynamic GSSIs).....	73
10.3.14	EF <sub>GCK</sub> (Group Cipher Keys) .....	74
10.3.15	Void .....	76
10.3.16	EF <sub>GINFO</sub> (User's group information) .....	76
10.3.17	EF <sub>SEC</sub> (Security settings) .....	78
10.3.18	EF <sub>FORBID</sub> (Forbidden networks).....	79
10.3.19	EF <sub>PREF</sub> (Preferred networks) .....	80
10.3.20	EF <sub>SPN</sub> (Service Provider Name) .....	82
10.3.21	Void .....	83
10.3.22	EF <sub>DNWRK</sub> (Broadcast network information).....	83
10.3.23	EF <sub>NWT</sub> (Network table) .....	84
10.3.24	EF <sub>GWT</sub> (Gateway table) .....	85
10.3.25	EF <sub>CMT</sub> (Call Modifier Table).....	87
10.3.26	EF <sub>ADNGWT</sub> (Abbreviated Dialling Number with Gateways) .....	90
10.3.27	EF <sub>GWTEXT1</sub> (Gateway Extension1).....	92
10.3.28	EF <sub>ADNTETRA</sub> (Abbreviated dialling numbers for TETRA network) .....	92
10.3.29	EF <sub>EXTA</sub> (Extension A) .....	94
10.3.30	EF <sub>FDNGWT</sub> (Fixed dialling numbers with Gateways) .....	94
10.3.31	EF <sub>GWTEXT2</sub> (Gateway Extension2).....	95
10.3.32	EF <sub>FDNTETRA</sub> (Fixed dialling numbers for TETRA network) .....	96
10.3.33	EF <sub>EXTB</sub> (Extension B).....	96
10.3.34	EF <sub>LNDGWT</sub> (Last number dialled with Gateways) .....	97
10.3.35	EF <sub>LNDTETRA</sub> (Last numbers dialled for TETRA network).....	97
10.3.36	EF <sub>SDNGWT</sub> (Service Dialling Numbers with gateway) .....	98
10.3.37	EF <sub>GWTEXT3</sub> (Gateway Extension3).....	98
10.3.38	EF <sub>SDNTETRA</sub> (Service Dialling Numbers for TETRA network) .....	99
10.3.39	EF <sub>STXT</sub> (Status message texts).....	99
10.3.40	EF <sub>MSGTXT</sub> (SDS-1 message texts).....	100
10.3.41	EF <sub>SDS123</sub> (Status and SDS type 1, 2 and 3 message storage) .....	101
10.3.42	EF <sub>SDS4</sub> (SDS type 4 message storage).....	103
10.3.43	EF <sub>MSGEXT</sub> (Message Extension).....	110
10.3.44	EF <sub>EADDR</sub> (Emergency addresses).....	110

10.3.45	EF <sub>EINFO</sub> (Emergency call information).....	112
10.3.46	EF <sub>DMOch</sub> (DMO radio channel information) .....	113
10.3.47	EF <sub>MSch</sub> (MS allocation of DMO channels) .....	114
10.3.48	EF <sub>KH</sub> (List of Key Holders).....	115
10.3.49	EF <sub>REPGATE</sub> (DMO repeater and gateway list) .....	116
10.3.50	EF <sub>AD</sub> (Administrative data).....	117
10.3.51	EF <sub>PREF_LA</sub> (Preferred location areas) .....	117
10.3.52	EF <sub>LNDComp</sub> (Composite LND file).....	118
10.3.53	EF <sub>DFLTSTSGT</sub> (Status Default Target).....	119
10.3.54	EF <sub>SDSMEM_STATUS</sub> (SDS Memory Status) .....	122
10.3.55	EF <sub>WELCOME</sub> (Welcome Message).....	124
10.3.56	EF <sub>SDSR</sub> (SDS delivery report).....	124
10.3.57	EF <sub>SDSP</sub> (SDS parameters) .....	125
10.3.58	EF <sub>DIALSC</sub> (Dialling schemes for TETRA network).....	126
10.3.59	EF <sub>APN</sub> (APN table) .....	127
10.3.60	Void .....	128
10.3.61	EF <sub>PNI</sub> (Private Number Information).....	128
10.3.62	EF <sub>SCAN</sub> (Scan list files).....	129
10.3.63	EF <sub>SCAND</sub> (Scan list data) .....	130
10.3.64	EF <sub>DMO_GSSIS</sub> (DMO pre-programmed group numbers).....	131
10.3.65	EF <sub>DMO_GRDS</sub> (Group related data for DMO static GSSIs).....	131
10.3.66	EF <sub>GTMO_GDMO</sub> (TMO - DMO selected group association) .....	132
10.3.67	EF <sub>GDMO_GTMO</sub> (DMO - TMO selected group association).....	133
10.3.68	EF <sub>DMO_DEP</sub> (Default encryption parameters) .....	133
10.3.69	EF <sub>GSKO</sub> ( Group Session Key) .....	135
10.4	Contents of the EFs at the Telecom level .....	136
10.4.1	EF <sub>ADN</sub> (Abbreviated dialling numbers) .....	136
10.4.2	EF <sub>FDN</sub> (Fixed dialling numbers) .....	140
10.4.3	EF <sub>MSISDN</sub> (MSISDN) .....	140
10.4.4	EF <sub>LND</sub> (Last number dialled).....	141
10.4.5	EF <sub>SDN</sub> (Service Dialling Numbers) .....	141
10.4.6	EF <sub>EXT1</sub> (Extension1).....	142
10.4.7	EF <sub>EXT2</sub> (Extension2).....	143
10.4.8	EF <sub>EXT3</sub> (Extension3).....	144
10.5	Files of TETRA .....	144
11	Application protocol.....	146
11.1	General procedures .....	147
11.1.1	Reading an EF.....	147
11.1.2	Updating an EF .....	147
11.1.3	Invalidating an EF.....	148
11.2	SIM management procedures .....	148
11.2.1	SIM initialization .....	148
11.2.2	TETRA session initialization.....	148
11.2.3	TETRA session termination.....	149
11.2.4	Language preference request .....	149
11.2.5	Administrative information request .....	149
11.2.6	SIM service table request.....	149
11.2.7	SIM phase request.....	149
11.2.8	SIM presence detection.....	149
11.2.9	SIM card number request.....	149
11.2.10	Common Cipher Key request.....	149
11.3	CHV related procedures .....	150
11.3.1	CHV verification .....	150
11.3.2	CHV value substitution.....	150
11.3.3	CHV disabling .....	150
11.3.4	CHV enabling .....	151
11.3.5	CHV unblocking.....	151
11.4	TETRA security related procedures .....	151
11.4.1	Authentication procedures and generation of DCK .....	152
11.4.1.1	Mutual authentication requirement request .....	152
11.4.1.2	SIM authentication .....	152



11.4.1.3	SwMI authentication .....	152
11.4.2	TETRA OTAR key computation (CCK, GCK, SCK) .....	152
11.4.2.1	CCK distribution .....	152
11.4.2.2	Void.....	152
11.4.2.3	GCK distribution.....	152
11.4.2.4	SCK distribution .....	153
11.4.3	ITSI request .....	153
11.4.4	ITSI disabling/re-enabling .....	153
11.5	Subscription related procedures .....	153
11.5.1	Username request.....	153
11.5.2	ITSI temporarily disabled enquiry .....	153
11.5.3	Subscriber class request .....	154
11.5.4	Void .....	154
11.5.5	Group identity information .....	154
11.5.5.1	Static Group identity information .....	154
11.5.5.2	Dynamic Group identity information .....	154
11.5.6	Group related data.....	154
11.5.7	User's group information .....	154
11.5.8	Call modifiers .....	155
11.5.9	Service Provider Name .....	155
11.5.10	DMO channel procedures .....	155
11.5.11	Emergency addresses .....	155
11.5.12	Interrupted emergency call request .....	155
11.6	Network related procedures.....	155
11.6.1	Forbidden networks .....	156
11.6.2	Preferred networks.....	156
11.7	Dialling number related procedures .....	156
11.7.1	Dialling numbers under DF <sub>TETRA</sub> .....	156
11.7.2	Dialling numbers under DF <sub>TELECOM</sub> .....	157
11.7.3	FDNGWT specific procedures .....	158
11.7.3.1	FDNGWT capability request .....	159
11.7.3.2	FDNGWT disabling .....	159
11.7.3.3	FDNGWT enabling .....	159
11.8	Status and short data message procedures .....	159
11.8.1	Display of status message texts.....	159
11.8.2	Display of SDS1 message texts .....	160
11.8.3	Storage of status and SDS messages types 1, 2 and 3.....	160
11.8.4	Storage of SDS messages type 4.....	160
11.8.5	SDS delivery report .....	160
11.8.6	Default Status Target .....	161
<b>Annex A (normative): Plug-in SIM.....</b>		<b>162</b>
<b>Annex B (informative): FDN Procedures .....</b>		<b>163</b>
<b>Annex C (informative): Suggested contents of EFs at pre-personalization.....</b>		<b>164</b>
C.1	Contents of the EFs at the MF level .....	164
C.2	Contents of the EFs at the TETRA application level .....	164
C.3	Contents of the EFs at the Telecom Level.....	166
<b>Annex D (normative): Database structure for group IDs and phone books .....</b>		<b>167</b>
<b>Annex E (informative): Emergency call facilities and procedures.....</b>		<b>169</b>
<b>Annex F (informative): Composite List of Last Dialed Numbers. ....</b>		<b>171</b>
<b>Annex G (informative): Bibliography.....</b>		<b>173</b>
<b>Annex H (informative): Change requests.....</b>		<b>174</b>
History .....		175

## 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 European Standard (Telecommunications series) has been produced by ETSI Project Terrestrial Trunked Radio (TETRA).

It was originally published as EN 300 812 (V2.1.1) and then converted into a sub-part EN 300 812-3 to support technology defined in the present document. The other parts of this series are currently published in TS and ES formats:

The present document is part 3 of a multi-part deliverable covering the Subscriber Identity Module to Mobile Equipment (SIM-ME) interface, as identified below:

ES 200 812-1: "Universal Integrated Circuit Card (UICC); Physical and logical characteristics";

ES 200 812-2: "Universal Integrated Circuit Card (UICC); Characteristics of the TSIM application";

**EN 200 812-3: "Integrated Circuit (IC); Physical, logical and TSIM application characteristics".**

NOTE: Part 3 was originally published as EN 300 812 and defines different technology than part 1 and part 2.

<https://standards.iteh.ai/catalog/standards/sist/6706ba22-b348-437e-9fa5-9da6a34a48d5/sist-en-300-812-3-v2-2-1-2006>

### National transposition dates

Date of adoption of this EN:	20 February 2004
Date of latest announcement of this EN (doa):	31 May 2004
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 November 2004
Date of withdrawal of any conflicting National Standard (dow):	30 November 2004

---

# 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 TETRA 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 a ME independently of the respective manufacturers and operators. The concept of a split of the MS into these elements as well as the distinction between the TETRA network operation phase, which is also called TETRA operations, and the administrative management phase is described in the User Requirement Specification ETR 295 [6].

The present document defines:

- the requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;
- the model which shall be used as a basis for the design of the logical structure of the SIM;
- the security features; This edition of the standard covers the security mechanisms for ITSI based services including authentication and OTAR for keys addressed to an ITSI;
- the interface functions;
- the commands;
- the contents of the files required for the TETRA application;
- the application protocol.

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

The physical SIM described in the present document is a removable Integrated Circuit (IC) card. The SIM is an optional device within TETRA MSs. The present document does not preclude the implementation of fully functional MSs without a SIM. All references to mobile equipment in the present document are to be taken to mean mobile equipment which have been designed to operate with a SIM.

The present document deals with all aspects of trunked mode MS operation. For direct mode MS operation key user operation is supported by the SIM but not key holder or key generator operation. Furthermore, storage of information for direct mode MS operation in repeater and gateway mode are supported, but any extra storage required in the direct mode repeater or direct mode gateway terminals themselves is not supported.

---

# 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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

- [1] ETSI EN 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".
- [2] ETSI EN 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

- [3] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [4] ETSI ETS 300 392-12-22: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 12: Supplementary services stage 3; Sub-part 22: Dynamic Group Number Assignment (DGNA)".
- [5] ETSI ETS 300 394-2 (all parts): "Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 2: Protocol testing specification for Voice plus Data (V+D)".
- [6] ETSI ETR 295: "Terrestrial Trunked Radio (TETRA); User requirements for Subscriber Identity Module (SIM)".
- [7] ETSI EN 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".
- [8] Void.
- [9] ETSI TS 100 977: "Digital cellular telecommunications system (Phase 2+) (GSM); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11)".
- [10] ETSI TS 100 900: "Digital cellular telecommunications system (Phase 2+) (GSM); Alphabets and language-specific information (GSM 03.38 version 7.2.0 Release 1998)".
- [11] ETSI TS 100 906: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Stations (MS) features (GSM 02.07 version 7.1.0 Release 1998)".
- [12] ETSI TS 100 907: "Digital cellular telecommunications system (Phase 2+); Man-machine Interface (MMI) of the Mobile Station (MS) (3GPP TS 02.30 version 7.1.1 Release 1998)".
- [13] ETSI TS 100 927: "Digital cellular telecommunications system (Phase 2+); Numbering, Addressing and Identification (3GPP TS 03.03 version 7.7.0 Release 1998)".
- [14] GTS GSM 04.08: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile radio; Layer 3 specification (GSM 04.08)".  
<https://standards.ietf.org/catalog/standards/sist/6706ba22-b348-437e-9fa3-9da6a34a48d5/sist-en-300-812-3-v2-2-1-2006>
- [15] ETSI ETS 300 641: "Digital cellular telecommunications system (Phase 2) (GSM); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.12)".
- [16] ISO/IEC 7810: "Identification cards - Physical characteristics".
- [17] ISO/IEC 7811-1: "Identification cards - Recording technique - Part 1: Embossing".
- [18] Void.
- [19] ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".
- [20] ISO/IEC 7816-2 (1999): "Information technology - Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and location of the contacts".
- [21] ISO/IEC 7816-3 (1997): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".
- [22] ISO/IEC 7816-5: "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers".
- [23] ISO 639 (all parts): "Code for the representation of names of languages".
- [24] ISO/IEC 8859-1 (1998): "Information technology - 8 bit-single byte coded graphic character sets - Part 1: Latin alphabet No. 1".
- [25] CEN EN 1375: "Identification card system - Intersector integrated circuit(s) card additional formats - ID-000 card size and physical characteristics".

- [26] 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".
- [27] ITU-T Recommendation E.118: "The international telecommunication charge card".
- [28] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".
- [29] ETSI ES 200 812-2: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (TSIM-ME) interface; Part 2: Universal Integrated Circuit Card (UICC); Characteristics of the TSIM application".

## 3 Definitions, symbols and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in EN 300 392-1 [1] and the following apply:

**access conditions:** set of security attributes associated with access to an Elementary File (EF):

- ADM (administrative):  
indicates an access condition defined by the card issuer. Before issue of the card ADM serves as a placeholder for an access condition to be defined by the card issuer. Any access condition may be assigned. The assigned access condition is used during the usage phase of the SIM;
- AUTI (authorized immediate):  
defines access conditions to an EF under which access shall be only possible immediately following successful authentication of the Switching and Management Infrastructure (SwMI);
- CHVn (card holder verification):  
defines the access condition to an EF which requires verification of the user identity (n = 1 or n = 2);
- NEV (never):  
access to the EF is never allowed across the SIM-ME interface.

**administrative phase:** part of the card life between the manufacturing phase and the usage phase

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

**application protocol:** set of procedures required by the application which are located and used in the Integrated Circuit (IC) card and outside the IC card (external application)

**card holder verification:** authentication of the user to the SIM card

**card session:** link between the card and the external world starting with the Answer To Reset (ATR) and ending with a subsequent reset or a deactivation of the card

**current directory:** latest Master File (MF) or Dedicated File (DF) selected

**current Elementary File (EF):** latest EF selected

**current file:** latest MF, DF, or EF selected

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

**key generator:** secure system entity authorized to generate Static Cipher Keys (SCKs) for Direct Mode Operation (DMO)

**key holder:** secure system entity authorized to distribute SCKs for DMO

**key user:** standard Direct Mode (DM) terminal which uses SCKs provided by an authorized key holder

**ID-1 SIM:** SIM having the format of an ID-1 card (see ISO/IEC 7816-1 [19])

**input:** signifies data input to the SIM functions (defined in clause 8):

Input from SIM input from the SIM internal memory;

Input from EF internal input from an EF on the SIM;

Input from ME data contained in a command APDU passed across the SIM-ME interface.

**Master File (MF):** unique mandatory DF representing the root

**Mobile equipment (ME):** part of the MS which interfaces to the SIM card

**Mobile Station (MS):** entirety of the equipment needed to communicate with the infrastructure (in trunked mode of operation) or direct with another MS (in direct mode of operation)

**output:** signifies data output from the SIM functions (defined in clause 8):

Output to SIM data shall be stored on the SIM in non-permanent memory for the duration of the TETRA session;

Output to EF internal updating of an EF on the SIM;

Output to ME data contained in a response APDU passed across the SIM-ME interface.

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

**personalization:** addition of subscriber and end user data to the appropriate EFs in the SIM during the administrative phase of a card's life cycle

**pre-personalization:** assignment of EF values at the manufacturing phase of a card's life cycle

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

**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

**Subscriber Identity Module (SIM) or SIM card:** integrated circuit card containing network related subscriber information

**T = 0:** half-duplex asynchronous character based transmission protocol. As defined in ISO/IEC 7816-3 [21]

**T = 1:** half-duplex asynchronous block based transmission protocol. The protocol may be initiated after ATR. As defined in ISO/IEC 7816-3 [21]

**TETRA application:** set of security mechanisms, files, data and protocols required by TETRA

**TETRA session:** part of the card session dedicated to the TETRA operation

**TETRA SIM:** subscriber identity module used in a TETRA MS

**usage phase:** part of the card life, after the administrative phase, when the card is being used for operational purposes

**5 V technology SIM:** SIM operating at 5 V  $\pm$ 10 %

**3 V technology SIM:** SIM operating at 3 V  $\pm$ 10 % and 5 V  $\pm$ 10 %

**3 V technology ME:** ME operating the SIM - ME interface at 3 V  $\pm$ 10 % according to ETS 300 641 [15] and 5 V  $\pm$ 10 % according to TS 100 977 [9]

**3 V only ME:** ME only operating the SIM - ME interface at 3 V  $\pm$ 10 % according to ETS 300 641 [15]

## 3.2 Symbols

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

"0" to "9" and "A" to "F"	The sixteen hexadecimal digits
V <sub>cc</sub>	Supply voltage
V <sub>pp</sub>	Programming voltage

## 3.3 Abbreviations

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

ADM	ADMInistrative (see definitions)
ADN	Abbreviated Dialling Number
ALW	ALWays
APDU	Application Protocol Data Unit
APN	Access Point Name
ASSI	Alias Short Subscriber Identity
ATR	Answer To Reset
AUTI	AUTHorized Immediate (see definitions)
BCD	Binary Coded Decimal
CCK	Common Cipher Key
CCK-id	CCK identifier
CHV	Card Holder Verification (see definitions)
CLA	CLAss
CLK	CLoCK
DCK	Derived Cipher Key
DCK1	Part 1 of the DCK
DCK2	Part 2 of the DCK
DF	Dedicated File
DGNA	Dynamic Group Number Assignment
DM	Direct Mode
DMO	Direct Mode Operation
DTMF	Dual Tone Multiple Frequency
EF	Elementary File
FDN	Fixed Dialling Number
FSSN	Fleet Specific Short Number
GCK	Group Cipher Key
GCKN	Group Cipher Key Number
GCK-VN	GCK Version Number
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSSI	Group Short Subscriber Identity
GTSI	Group Tetra Subscriber Identity
I/O	Input/Output
IC	Integrated Circuit
ID	IDentifier
INS	INStruction code
IP	Internet Protocol
ISSI	Individual Short Subscriber Identity
ITSI	Individual TETRA Subscriber Identity
K	individual subscriber authentication Key
KE	Enhanced security Key
KSO	Session Key for Over the air re-keying