



**SLOVENSKI STANDARD**  
**SIST ETS 300 812 E1:2003**

**01-december-2003**

---

Df]nYa b]gbc dc j b]fUX]c`fH9HF5Ł!`J Ufbcgfb]j ]X]\_]'!`Ja Ygb]\_`a YX`bUfc b]ý\_c  
]XYbh]Z\_ U]g\_c`\_Uf]Vt`]b`a cV]bc`cdfYa c`fG-A!A9Ł

Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to  
Mobile Equipment (SIM - ME) interface

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

Ta slovenski standard je istoveten z: **ETS 300 812 Edition 1**  
<https://standards.iteh.ai/catalog/standards/sist/601a7169-c019-450f-891a-7d400027e0c0/sist-ets-300-812-e1-2003>

**ICS:**

|           |                                    |                                      |
|-----------|------------------------------------|--------------------------------------|
| 33.070.10 | Prizemni snopovni radio<br>(TETRA) | Terrestrial Trunked Radio<br>(TETRA) |
|-----------|------------------------------------|--------------------------------------|

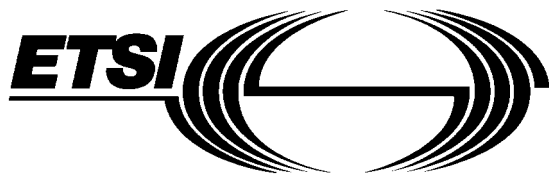
**SIST ETS 300 812 E1:2003**

**en**

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

SIST ETS 300 812 E1:2003

<https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003>



**E**UROPEAN  
**T**ELECOMMUNICATION  
**S**TANDARD

**ETS 300 812**

November 1998

Source: TETRA

Reference: DE/TETRA-07017

ICS: 33.020

**Key words:** Card, security, TETRA

**Terrestrial Trunked Radio (TETRA);  
Security aspects;**

**Subscriber Identity Module to Mobile Equipment (SIM - ME)  
interface**

<https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-1998>

**ETSI**

European Telecommunications Standards Institute

**ETSI Secretariat**

**Postal address:** F-06921 Sophia Antipolis CEDEX - FRANCE

**Office address:** 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE

**Internet:** secretariat@etsi.fr - <http://www.etsi.org>

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

**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 1998. All rights reserved.

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

[SIST ETS 300 812 E1:2003](https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003)

<https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003>

## Content

|  |    |
|--|----|
| Foreword.....  | 9  |
| 1 Scope .....  | 11 |
| 2 Normative references .....   | 11 |
| 3 Definitions, abbreviations and symbols .....                                 | 13 |
| 3.1 Definitions.....   | 13 |
| 3.2 Abbreviations.....   | 15 |
| 3.3 Symbols.....   | 16 |
| 4 SIM characteristics.....   | 16 |
| 4.1 Format and layout .....  | 16 |
| 4.1.1 SIM.....   | 17 |
| 4.1.2 Plug-in SIM.....   | 17 |
| 4.1.3 Virtual SIM.....   | 17 |
| 4.2 Temperature range for card operation .....                                 | 17 |
| 4.3 Contacts.....  | 17 |
| 4.3.1 Provision of contacts .....  | 17 |
| 4.3.2 Activation and deactivation .....  | 17 |
| 4.3.3 Inactive contacts (contact conditions in the ME switched-off state)..... | 18 |
| 4.3.4 Contact pressure.....  | 18 |
| 4.4 Precedence (multiple SIM operation) .....                                  | 18 |
| 4.5 Static protection.....   | 18 |
| 5 Electronic signals and transmission protocols .....                          | 18 |
| 5.1 Supply voltage $V_{cc}$ (contact C1).....                                  | 19 |
| 5.1.1 5 V technology SIM.....  | 19 |
| 5.1.2 3 V technology SIM.....  | 19 |
| 5.1.3 3 V technology SIM identification.....                                   | 19 |
| 5.1.4 3 V technology ME.....   | 19 |
| 5.1.5 3 V Only ME.....   | 19 |
| 5.1.6 Activation and deactivation of 3 V technology SIM.....                   | 19 |
| 5.1.7 Supply voltage switching.....  | 20 |
| 5.1.8 Cross compatibility .....  | 20 |
| 5.1.9 Technology outlook.....  | 20 |
| 5.2 Reset (RST) (contact C2).....  | 20 |
| 5.3 Programming voltage $V_{pp}$ (contact C6).....                             | 20 |
| 5.4 Clock CLK (contact C3).....  | 20 |
| 5.5 Input/Output (I/O) (contact C7) .....                                      | 20 |
| 5.6 States .....   | 21 |
| 5.7 Baud rate .....  | 21 |
| 5.8 Answer To Reset (ATR) .....  | 21 |
| 5.9 Bit/character duration and sampling time.....                              | 21 |
| 5.10 Error handling .....  | 21 |
| 6 Logical model.....   | 21 |
| 6.1 General description .....  | 21 |
| 6.2 File identifier .....  | 22 |
| 6.3 Dedicated Files (DF) .....   | 22 |
| 6.4 Elementary Files (EF).....   | 23 |
| 6.4.1 Transparent EF.....  | 23 |
| 6.4.2 Linear fixed EF.....   | 23 |
| 6.4.3 Key EF.....  | 24 |
| 6.4.4 Cyclic EF.....   | 24 |
| 6.5 Methods for selecting a file .....   | 25 |
| 6.6 Reservation of file IDs .....  | 26 |

|        |  |    |
|--------|--|----|
| 7      | Security features .....  | 26 |
| 7.1    | Authentication and cipher key generation procedure .....                   | 27 |
| 7.2    | Support of Over The Air Re-keying (OTAR) distribution of cipher keys ..... | 27 |
| 7.3    | Support of SIM-ME enhanced security .....                                  | 27 |
| 7.4    | File access conditions .....   | 27 |
| 7.5    | Storage of CHV information .....   | 29 |
| 7.6    | Storage of DCK .....   | 29 |
| 8      | Description of the functions .....   | 29 |
| 8.1    | SELECT .....   | 29 |
| 8.2    | STATUS .....   | 30 |
| 8.3    | READ BINARY .....  | 30 |
| 8.4    | UPDATE BINARY .....  | 30 |
| 8.5    | READ RECORD .....  | 30 |
| 8.6    | READ KEY .....   | 31 |
| 8.7    | UPDATE RECORD .....  | 31 |
| 8.8    | SEEK .....   | 32 |
| 8.9    | VERIFY CHV .....   | 33 |
| 8.10   | CHANGE CHV .....   | 33 |
| 8.11   | DISABLE CHV .....  | 34 |
| 8.12   | ENABLE CHV .....   | 34 |
| 8.13   | UNBLOCK CHV .....  | 34 |
| 8.14   | INVALIDATE .....   | 35 |
| 8.15   | REHABILITATE .....   | 35 |
| 8.16   | TETRA authentication algorithms .....                                      | 35 |
| 8.16.1 | GET RANDOM .....   | 35 |
| 8.16.2 | TA11/12 ALGORITHM .....  | 36 |
| 8.16.3 | TA21/22 ALGORITHM .....  | 36 |
| 8.16.4 | TB4/TE ALGORITHM .....   | 36 |
| 8.17   | OTAR algorithms .....  | 36 |
| 8.17.1 | TA32 ALGORITHM .....   | 37 |
| 8.17.2 | TA82 ALGORITHM .....   | 37 |
| 8.17.3 | TA41/52 ALGORITHM .....  | 37 |
| 8.17.4 | TA71 ALGORITHM .....   | 37 |
| 9      | Description of the commands .....  | 38 |
| 9.1    | Mapping principles .....   | 38 |
| 9.2    | Coding of the commands .....   | 39 |
| 9.2.1  | SELECT .....   | 41 |
| 9.2.2  | STATUS .....   | 43 |
| 9.2.3  | READ BINARY .....  | 43 |
| 9.2.4  | UPDATE BINARY .....  | 43 |
| 9.2.5  | READ RECORD .....  | 43 |
| 9.2.6  | UPDATE RECORD .....  | 44 |
| 9.2.7  | READ KEY .....   | 44 |
| 9.2.8  | SEEK .....   | 44 |
| 9.2.9  | VERIFY CHV .....   | 45 |
| 9.2.10 | CHANGE CHV .....   | 45 |
| 9.2.11 | DISABLE CHV .....  | 45 |
| 9.2.12 | ENABLE CHV .....   | 45 |
| 9.2.13 | UNBLOCK CHV .....  | 46 |
| 9.2.14 | INVALIDATE .....   | 46 |
| 9.2.15 | REHABILITATE .....   | 46 |
| 9.2.16 | GET RANDOM .....   | 46 |
| 9.2.17 | TA11/12 ALGORITHM .....  | 46 |
| 9.2.18 | TA21/22 ALGORITHM .....  | 47 |
| 9.2.19 | TB4/TE ALGORITHM .....   | 47 |
| 9.2.20 | TA32 ALGORITHM .....   | 47 |
| 9.2.21 | TA82 ALGORITHM .....   | 48 |
| 9.2.22 | TA41/52 ALGORITHM .....  | 48 |

|     |         |  |    |
|-----|---------|--|----|
|     | 9.2.23  | TA71 ALGORITHM .....   | 48 |
|     | 9.2.24  | GET RESPONSE .....   | 48 |
| 9.3 |         | Definitions and coding .....                                       | 49 |
| 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 .....  | 51 |
|     | 9.4.5   | Application independent errors .....                               | 51 |
|     | 9.4.6   | Commands versus possible status responses .....                    | 52 |
| 10  |         | Contents of the EFs .....  | 52 |
|     | 10.1    | Contents of EFs located either at application level or above ..... | 53 |
|     | 10.1.1  | EFCHV .....  | 53 |
|     | 10.2    | Contents of the EFs at the MF level .....                          | 54 |
|     | 10.2.1  | EFICCD (Card Identification) .....                                 | 54 |
|     | 10.2.2  | EFDIR (Application directory) .....                                | 55 |
|     | 10.2.3  | EFLP (Language Preference) .....                                   | 56 |
|     | 10.3    | Contents of the EFs at the TETRA application level .....           | 56 |
|     | 10.3.1  | EF SST (SIM Service Table) .....                                   | 56 |
|     | 10.3.2  | EFITSI (Individual Tetra Subscriber Identity) .....                | 59 |
|     | 10.3.3  | EFITSIDIS (ITSI Disabled) .....                                    | 60 |
|     | 10.3.4  | EFUNAME (Username) .....   | 61 |
|     | 10.3.5  | EF SCT (Subscriber Class Table) .....                              | 61 |
|     | 10.3.6  | EF PHASE (Phase identification) .....                              | 62 |
|     | 10.3.7  | EF CCK (Common Cipher Key) .....                                   | 63 |
|     | 10.3.8  | EF CCKLOC (CCK location areas) .....                               | 64 |
|     | 10.3.9  | EF SCK (Static Cipher Keys) .....                                  | 65 |
|     | 10.3.10 | EF GSSIS (Static GSSIs) .....                                      | 67 |
|     | 10.3.11 | EF GRDS (Group related data for static GSSIs) .....                | 68 |
|     | 10.3.12 | EF GSSID (Dynamic GSSIs) .....                                     | 70 |
|     | 10.3.13 | EF GRDD (Group related data for dynamic GSSIs) .....               | 70 |
|     | 10.3.14 | EF GCK (Group Cipher Keys) .....                                   | 71 |
|     | 10.3.15 | EF MGCK (Modified Group Cipher Keys) .....                         | 72 |
|     | 10.3.16 | EF GINFO (User's group information) .....                          | 73 |
|     | 10.3.17 | EF SEC (Security settings) .....                                   | 75 |
|     | 10.3.18 | EF FORBID (Forbidden networks) .....                               | 75 |
|     | 10.3.19 | EF PREF (Preferred networks) .....                                 | 77 |
|     | 10.3.20 | EF SPN (Service Provider Name) .....                               | 78 |
|     | 10.3.21 | EF LOCI (Location information) .....                               | 78 |
|     | 10.3.22 | EF DNWRK (Broadcast network information) .....                     | 79 |
|     | 10.3.23 | EF NWT (Network table) .....                                       | 81 |
|     | 10.3.24 | EF GWT (Gateway table) .....                                       | 82 |
|     | 10.3.25 | EF CMT (Call Modifier Table) .....                                 | 83 |
|     | 10.3.26 | EF ADN (Abbreviated Dialling Number) .....                         | 85 |
|     | 10.3.27 | EF EXT1 (Extension1) .....   | 87 |
|     | 10.3.28 | EF ADNTETRA (Abbreviated dialling numbers for TETRA network) ..... | 88 |
|     | 10.3.29 | EF EXTA (Extension A) .....  | 89 |
|     | 10.3.30 | EF FDN (Fixed dialling numbers) .....                              | 90 |
|     | 10.3.31 | EF EXT2 (Extension2) .....   | 91 |
|     | 10.3.32 | EF FDNTETRA (Fixed dialling numbers for TETRA network) .....       | 91 |
|     | 10.3.33 | EF EXTB (Extension B) .....  | 92 |
|     | 10.3.34 | EF LND (Last number dialled) .....                                 | 92 |
|     | 10.3.35 | EF LNDTETRA (Last numbers dialled for TETRA network) .....         | 93 |
|     | 10.3.36 | EF SDN (Service Dialling Numbers) .....                            | 93 |
|     | 10.3.37 | EF EXT3 (Extension3) .....   | 94 |
|     | 10.3.38 | EF SDNTETRA (Service Dialling Numbers for TETRA network) .....     | 94 |
|     | 10.3.39 | EF STXT (Status message texts) .....                               | 95 |
|     | 10.3.40 | EF MSGTXT (SDS-1 message texts) .....                              | 96 |
|     | 10.3.41 | EF SDS123 (Status and SDS type 1, 2 and 3 message storage) .....   | 97 |

|          |  |     |
|----------|--|-----|
| 10.3.42  | EF <sub>SDS4</sub> (SDS type 4 message storage).....       | 104 |
| 10.3.43  | EF <sub>MSGEXT</sub> (Message Extension).....              | 107 |
| 10.3.44  | EF <sub>EADDR</sub> (Emergency addresses).....             | 107 |
| 10.3.45  | EF <sub>EINFO</sub> (Emergency call information).....      | 109 |
| 10.3.46  | EF <sub>DMOCh</sub> (DMO channel information).....         | 110 |
| 10.3.47  | EF <sub>MSCh</sub> (MS allocation of DMO channels).....    | 110 |
| 10.3.48  | EF <sub>KH</sub> (List of Key Holders).....                | 111 |
| 10.3.49  | EF <sub>REPGATE</sub> (DMO repeater and gateway list)..... | 112 |
| 10.3.50  | EF <sub>AD</sub> (Administrative data).....                | 113 |
| 11       | Application protocol.....                                  | 115 |
| 11.1     | General procedures.....                                    | 117 |
| 11.1.1   | Reading an EF.....   | 117 |
| 11.1.2   | Updating an EF.....  | 117 |
| 11.1.3   | Invalidating an EF.....                                    | 117 |
| 11.2     | SIM management procedures.....                             | 117 |
| 11.2.1   | SIM initialization.....                                    | 117 |
| 11.2.2   | TETRA session initialization.....                          | 117 |
| 11.2.3   | TETRA session termination.....                             | 118 |
| 11.2.4   | Language preference request.....                           | 118 |
| 11.2.5   | Administrative information request.....                    | 119 |
| 11.2.6   | SIM service table request.....                             | 119 |
| 11.2.7   | SIM phase request.....                                     | 119 |
| 11.2.8   | SIM presence detection.....                                | 119 |
| 11.2.9   | SIM card number request.....                               | 119 |
| 11.2.10  | Common Cipher Key request.....                             | 119 |
| 11.3     | CHV related procedures.....                                | 119 |
| 11.3.1   | CHV verification.....                                      | 119 |
| 11.3.2   | CHV value substitution.....                                | 120 |
| 11.3.3   | CHV disabling.....   | 120 |
| 11.3.4   | CHV enabling.....  | 120 |
| 11.3.5   | CHV unblocking.....  | 120 |
| 11.4     | TETRA security related procedures.....                     | 121 |
| 11.4.1   | Authentication procedures and generation of DCK.....       | 121 |
| 11.4.1.1 | Mutual authentication requirement request.....             | 121 |
| 11.4.1.2 | SIM authentication.....                                    | 121 |
| 11.4.1.3 | SwMI authentication.....                                   | 121 |
| 11.4.2   | TETRA OTAR key computation (CCK, GCK, SCK).....            | 121 |
| 11.4.2.1 | CCK distribution.....                                      | 121 |
| 11.4.2.2 | CCK changeover.....  | 121 |
| 11.4.2.3 | GCK distribution.....                                      | 122 |
| 11.4.2.4 | SCK distribution.....                                      | 122 |
| 11.4.3   | ITSI request.....  | 122 |
| 11.4.4   | ITSI disabling/re-enabling.....                            | 122 |
| 11.5     | Subscription related procedures.....                       | 123 |
| 11.5.1   | Username request.....                                      | 123 |
| 11.5.2   | ITSI temporarily disabled enquiry.....                     | 123 |
| 11.5.3   | Subscriber class request.....                              | 123 |
| 11.5.4   | Location information.....                                  | 123 |
| 11.5.5   | Group identity information.....                            | 123 |
| 11.5.6   | Group related data.....                                    | 123 |
| 11.5.7   | User's group information.....                              | 124 |
| 11.5.8   | Call modifiers.....  | 124 |
| 11.5.9   | Service Provider Name.....                                 | 124 |
| 11.5.10  | DMO channel procedures.....                                | 124 |
| 11.5.11  | Emergency addresses.....                                   | 124 |
| 11.5.12  | Interrupted emergency call request.....                    | 124 |
| 11.6     | Network related procedures.....                            | 125 |
| 11.6.1   | Forbidden networks.....                                    | 125 |
| 11.6.2   | Preferred networks.....                                    | 125 |



|                        |  |     |
|------------------------|--|-----|
| 11.7                   | Phonebook related procedures.....                        | 125 |
| 11.7.1                 | Dialling numbers.....                                    | 125 |
| 11.7.2                 | FDN specific procedures.....                             | 127 |
| 11.7.2.1               | FDN capability request.....                              | 127 |
| 11.7.2.2               | FDN disabling.....                                       | 127 |
| 11.7.2.3               | FDN enabling.....  | 127 |
| 11.8                   | Status and short data message procedures .....           | 127 |
| 11.8.1                 | Display of status message texts .....                    | 127 |
| 11.8.2                 | Display of SDS1 message texts .....                      | 128 |
| 11.8.3                 | Storage of status and SDS messages types 1, 2 and 3..... | 128 |
| 11.8.4                 | Storage of SDS messages type 4 .....                     | 128 |
| Annex A (normative):   | Plug-in SIM.....   | 129 |
| Annex B (informative): | FDN Procedures .....                                     | 130 |
| Annex C (informative): | Suggested contents of EFs at pre-personalization .....   | 131 |
| Annex D (normative):   | Database structure for group IDs and phone books .....   | 132 |
| Annex E (informative): | Emergency call facilities and procedures.....            | 134 |
| Annex F (informative): | Bibliography.....  | 136 |
| History .....          |  | 137 |

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

[SIST ETS 300 812 E1:2003](https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003)

<https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003>

Blank page

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

[SIST ETS 300 812 E1:2003](https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003)

<https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003>

## Foreword

This European Telecommunication Standard (ETS) has been produced by the Terrestrial Trunked Radio (TETRA) Project of the European Telecommunications Standards Institute (ETSI).

| Transposition dates   |                  |
|---|------------------|
| Date of adoption of this ETS:   | 27 November 1998 |
| Date of latest announcement of this ETS (doa):  | 28 February 1999 |
| Date of latest publication of new National Standard or endorsement of this ETS (dop/e): | 31 August 1999   |
| Date of withdrawal of any conflicting National Standard (dow):                          | 31 August 1999   |

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

[SIST ETS 300 812 E1:2003](https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003)

<https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003>

Blank page

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

[SIST ETS 300 812 E1:2003](https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003)

<https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003>

## 1 Scope

This ETS 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 an 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 [9].

This ETS 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;
- the interface functions;
- the commands;
- the contents of the files required for the TETRA application;
- the application protocol.

This ETS 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. This ETS does not specify any of the security algorithms which may be used.

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

This ETS 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 Normative references

This ETS incorporates, by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to, or revisions of, any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references, the latest edition of the publication referred to applies.

- [1] ISO 7810 (1985): "Identification cards - Physical characteristics".
- [2] ISO 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing".
- [3] ISO 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".
- [4] ISO/IEC 7816-1 (1987): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".

- [5] ISO/ISO 7816-2 (1988): "Information technology - Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and location of the contacts".
- [6] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".
- [7] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange".
- [8] ENV 1375-1: "Identification card systems - Intersector integrated circuit(s) card additional formats - Part 1: ID-000 card size and physical characteristics".
- [9] ETR 295: "User requirements for Subscriber Identity Module (SIM)".
- [10] ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General Network Design".
- [11] ETS 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".
- [12] ETS 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [13] ETS 300 396-3: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 3: Mobile Station to Mobile Station (MS-MS) Air Interface (AI) protocol".
- [14] ETS 300 608 (1996): "Digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (GSM 11.11)".  
<https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7119902709c9/sist-ets-300-812-e1-2003>
- [15] ETS 300 641 (1996): "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (GSM 11.12)".
- [16] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".
- [17] ETS 300 628 (1994): "European digital cellular telecommunications system (Phase 2); Alphabets and language-specific information (GSM 3.38)".
- [18] CCITT Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) – Information technology – 7-bit coded character set for information interchange)".
- [19] ETS 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".
- [20] 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)".
- [21] CCITT Recommendation E.118: "The international telecommunication charge card".

- [22] ISO 8859-1 (1987): "Information processing 8 bit-single byte coded graphic character sets - Part 1: Latin alphabet No. 1".
- [23] ETS 300 394-2 (1997): "Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 2: Protocol testing specification for Voice plus Data (V+D)".

### 3 Definitions, abbreviations and symbols

#### 3.1 Definitions

For the purposes of this ETS, the following definitions apply. For further information and definitions refer to ETS 300 392-1 [10].

**access conditions:** A 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  $n = 2$ ).

<https://standards.iteh.ai/catalog/standards/sist/66fa7109-c6f9-430f-891a-7d400027e0c0/sist-ets-300-812-e1-2003>

NEV (never):

access to the EF is never allowed across the SIM-ME interface.

RAU (reserved for administrative use):

defines access conditions to an EF which is restricted to the administrative phase of the SIM.

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

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

**application protocol:** The 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:** A 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:** The latest Master File (MF) or Dedicated File (DF) selected.

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

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