ETSI TR 102 021-6 V1.2.1 (2011-08)

Terrestrial Trunked Radio (TETRA);
User Requirement Specification TETRA Release 2.1;
Part 6: Smart Card (SC) and Subscriber Identity Module (SIM)

Reference
RTR/TETRA-01195

Keywords
SC, SIM, Smart Card, TETRA, UR, user

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

Contents

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://ipr.etsi.org).

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

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Terrestrial Trunked Radio (TETRA).

The present document is part 6 of a multi-part deliverable covering the User Requirement Specification for TETRA Release 2 and Release 2.1, as identified below:

Part 1: "General overview" (Release 2.1);

Part 2: "High Speed Data" (Release 2.1);

Part 3: "Codec" (Release 2);

Part 4: "Air Interface Enhancements" (Release 2.1);

Part 5: "Interworking and Roaming" (Release 2.1);

Part 6: "Smart Card and Subscriber Identity Module" (Release 2.1);

Part 7: "Security" (Release 2.1);

Part 8: "Air - Ground - Air services" (Release 2);

Part 9: "Peripheral Equipment Interface" (Release 2.1);

Part 10: "Local Mode Broadband" (Release 2.1);

Part 11: "Over The Air Management" (Release 2.1);

Part 12: "Direct Mode Operation" (Release 2.1).

Introduction

The Terms of Reference for TC TETRA approved at ETSI Board meeting #69, November 2008 is to produce ETSI deliverables (and maintenance thereafter) in accordance with the following requirements.

The Terms of Reference for TC TETRA are to produce ETSI deliverables (and maintenance thereafter) in accordance with the following requirements:

a) The provision of user driven services, facilities and functionality as required by traditional Professional Mobile Radio (PMR) user organisations such as the Emergency Services, Government, Military, Transportation, Utility and Industrial organisations as well as Public Access Mobile Radio (PAMR) operators.

b) The evolution and enhancement of TETRA as required by the market with the provision of new services, facilities and functionality made possible by new technology innovations and standards.

c) Further enhancements of the TETRA standard in order to provide increased benefits and optimisation in terms of spectrum efficiency, network capacity, system performance, quality of service, security and other relevant parameters.

d) The backward compatibility and integration of the new services, facilities and functionality with existing TETRA standards in order to future-proof the existing and future investments of TETRA users.

Technical Objective:

TETRA is one of a number of digital wireless communication technologies standardised by ETSI.

ETSI TC TETRA produces standards and/or adapts existing standards for efficient digital PMR and PAMR voice and data services, including broadband evolution. The approved programme for TETRA Release 2.1 covers work areas, namely:

- high speed data;
- air interface enhancements;
- interworking and roaming;
- smart card and subscriber identity module;
- security;
- air-ground-air services;
- peripheral equipment interface enhancements;
- local mode broadband;
- over-the-air management;
- direct mode operation.

The User Requirement Specification for each of these work areas is covered by its own document.

The present document provides the User Requirement Specification for the TETRA Smart Card and Subscriber Identity Module required by TC TETRA for TETRA Release 2.1.

1 Scope

The present document defines the user requirements for Smart Card (SC) and Subscriber Identity Module (SIM) and is applicable to the specification of TETRA Release 2.1 equipment.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI ES 200 812-1: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (TSIM-ME) interface; Part 1: Universal Integrated Circuit Card (UICC); Physical and logical characteristics".

[i.2] ETSI TR 102 021-4: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2.1; Part 4: Air Interface Enhancements".

[i.3] ETSI TR 102 021-7: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2.1; Part 7: Security".

[i.4] ETSI TR 102 021-9: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2.1; Part 9: Peripheral Equipment Interface".

[i.5] ETSI TR 102 021-11: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2.1; Part 11: Over-The-Air Management".

[i.6] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[i.7] ETSI EN 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) ".

[i.8] ETSI TS 100 392-18-3: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D) and Direct Mode Operation (DMO); Part 18: Air interface optimized applications; Sub-part 3: Direct mode Over The Air Management protocol (DOTAM)".

[i.9] 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".

[i.10] TETRA MOU Association Security and Fraud Prevention Group Recommendation 02 and 07.

NOTE: Available at http://www.tetramou.com/members/page.

3 Definitions and abbreviations

3.1 Definitions

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

Cryptographic Module (CM): functional entity of a Smart Card (SC) which encapsulates the following security functions:

1) cryptographic algorithms for authentication between Smart Card (SC) and Mobile Equipment (ME);
2) cryptographic algorithms for End-to-End Encryption of traffic data;
3) over-the-air key management functions for End-to-End Encryption cipher key material (OTAK);
4) tamper-proof data management of End-to-End Encryption cipher key material.

Cryptographic Smart Card (CSC): Smart Card (SC) incorporating a Cryptographic Module (CM)

Mobile Equipment (ME): physical part of a Mobile Station (MS) which is used to obtain TETRA services in V+D and DMO and which interfaces to and is parameterized either by a Smart Card (SC) or Subscriber Identity Module (SIM)

Mobile Station (MS): physical entity consisting of two parts, Mobile Equipment (ME) and Smart Card (SC)

Operational-Tactical Address (OPTA): subscriber identity which provides additional information about a subscriber's operational role or user organisation and which is not used for air interface addressing, e.g. for call setup

Personalized Smart Card (PSC): Smart Card (SC) incorporating a Cryptographic Module (CM) and a Subscriber Identity Module (SIM)

Smart Card (SC): physical part of a Mobile Station (MS) incorporating a Cryptographic Module (CM) and an optional Subscriber Identity Module (SIM)

Subscriber Identity Module (SIM): optional functional entity of a Smart Card (SC) which encapsulates the following personalisation function: tamper-proof data management of user data

TETRA Release 2: Work Programme with new terms of reference within ETSI Project TETRA to enhance the services and facilities of TETRA in order to meet new user requirements, utilize new technology and increase the longevity of TETRA within the traditional market domains of PMR and PAMR

TETRA Release 2.1: Work Programme within TC TETRA to enhance the services and facilities of TETRA in order to meet new user requirements, utilise new technology and increase the longevity of TETRA within the traditional market domains of PMR and PAMR

3.2 Abbreviations

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

API	Application Programming Interface
APN	Access Point Name
CM	Cryptographic Module
CSC	Cryptographic Smart Card
DGNA	Dynamic Group Number Assignment
DM-MS	Direct Mode – Mobile Station
DMO	Direct Mode Operation
DOTAM	Direct Mode Over-The-Air Management
E2EE	End-to-End Encryption

ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
ITSI	Individual TETRA Subscriber Identity
K	Authentication Key
LTE	Long Term Evolution
ME	Mobile Equipment
MMI	Man-Machine Interface
MNI	Mobile Network Identity
MS	Mobile Station
MSISDN	Mobile Station Integrated Services Digital network Number
OPTA	Operational-Tactical Address
OTAK	Over-The-Air Key management
PABX	Private Access Branch Exchange
PAMR	Public Access Mobile Radio
PEI	Peripheral Equipment Interface
PIN	Personal Identification Number
PMR	Private Mobile Radio
PPDR	Public Protection and Disaster Relief
PSC	Personalized Smart Card
PSTN	Public Switched Telephone Network
PUK	Personal Unblocking Key
REF	Reference number
SC	Smart Card
SCK	Static Cipher Key
SCTK	Smart Card Application Toolkit
SDS	Short Data Service
SDS-TL	Short Data Service Transport
SIM	Subscriber Identity Module
STK	SIM Application Toolkit
SwMI	Switching and Management Infrastructure
TC	Technical Committee
TEI	TETRA Equipment Identity
TETRA	Terrestrial Trunked Radio
TM-MS	Trunked Mode – Mobile Station
TR	Technical Report
TSIM	TETRA Subscriber Identity Module
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
URS	User Requirement Specification
V+D	Voice plus Data

4 User Requirement Specification

4.1 Introduction

In some PMR networks for PPDR users, user management and network management are handled separately. The operator performs the task of network management, i.e. monitoring, alarming, and administration of network elements. User organisations require to manage their users, e.g. to commission new subscribers, locally by themselves and not centrally by an operator. Furthermore, they do not want to disclose the operational-tactical use of the network to anyone else including the operator. Thus, the linkage between a real user name and a user air interface address (ITSI) should be unknown to the operator. In addition to this, the operator should not have access to the cryptographic algorithms and associated cipher key material employed for End-to-End Encryption and should only be able to decrypt end-to-end encrypted messages under well defined exceptional conditions ("lawful interception").

With regard to Mobile Stations (MS), separating user and network management requires to split up an MS into Mobile Equipment (ME) to be commissioned by the network management and a Smart Card (SC) to be commissioned by the user management.

Furthermore, PMR and PAMR networks require a considerable quantity of personalisation data to be entered into an MS before the MS can be used in service. In general, the programming APIs for the MSs differ between manufacturers. The use of SCs simplifies the logistics process of operators and user organisations supporting the use of MSs from several different manufacturers because only one physical interface and API is necessary.

By including all personalisation data in an SC, an alternative ME may be personalised to the end-users' requirements simply by the insertion of the end-users existing SC. This simplifies and improves the service that can be offered by network operators and user organisations to the customer and end-user. A Smart Card (SC) incorporates a Cryptographic Module (CM) and/or a Subscriber Identity Module (SIM).

The CM encapsulates end-to-end security functions:

1) cryptographic algorithms for authentication of the SC to the ME;
2) cryptographic algorithms for End-to-End Encryption of traffic data;
3) over-the-air key management functions for End-to-End Encryption cipher key material (OTAK);
4) confidentiality of End-to-End Encryption key material when passed over the SC-ME interface;
5) tamper-proof data management of SC-ME authentication key material;
6) tamper-proof data management of End-to-End Encryption cipher key material;

The SIM encapsulates air interface security and personalisation functions:

1) cryptographic algorithms for authentication of the MS to the SwMI;
2) confidentiality of air interface encryption key material and user data when passed over the SC-ME interface;
3) tamper-proof data management of MS-SwMI authentication key material;
4) tamper-proof data management of air interface encryption key material;
5) tamper-proof data management of user data;
6) cryptographic algorithms for authentication of the SC to the ME in case the CM is not incorporated;
7) tamper-proof data management of SC-ME authentication key material in case the CM is not incorporated.

Smart Cards will be used in the following configurations:

- Personalized Smart Card (PSC)

  In this configuration, the SC contains a CM and a SIM.

- Cryptographic Smart Card (CSC)

  In this configuration, the SC contains a CM, but no SIM. Due to not using a SIM, user data is not stored on the Smart Card in this configuration.

- SIM only

  This configuration contains SIM, but no CM.

NOTE: The Universal Integrated Circuit Card physical and logical characteristics are defined in ES 200 812-1 [i.1].

With the addition of applications supporting access to other radio technologies to the SC, the SC should support inter-standard roaming when placed in an appropriate ME. A sub-set of the features and functions should support TETRA Release 2.1 only.

In addition, the SC should permit the development and implementation of additional services in a timely manner, probably through SC application toolkit functionality, suitably adopted for TETRA networks.

The evolving SC standard should consider, in conjunction with Working Groups studying the ME and the MMI, at least two other operational scenarios:

- a standardised method of sharing one ME with several end-users. This means that the ability to change or update the appropriate personalization data by simple exchange of the SC or by other means as appropriate is of importance;
- the use of dual- and multi-standard terminals using different radio technologies. Some of these technologies (e.g. GSM, UMTS or LTE) involve the mandatory use of a SIM.

Furthermore, a Smart Card Application Toolkit (SCTK) or SIM Application Toolkit (STK) should provide an interface to external applications for accessing the SC security and personalisation functions. It should be possible to address SCTK and STK via PEI, see also TR 102 021-9 [i.4].

There should be appropriate mechanisms in place to ensure that any export licence requirements regarding controlling the encryption supported by the MS can be complied with.

User Requirement Specifications for security are presented in TR 102 021-7 [i.3].

4.2 Security functions

4.2.1 Authentication

The PSC should store the authentication key K and does not pass the authentication key to the ME. This is why, the PSC should contain the necessary MS-SwMI authentication algorithms.

The PSC should support both, mutual SC-ME authentication after powering on and mutual MS-SwMI authentication during initial and periodic registration. The CSC should support mutual SC-ME authentication. An MS should be able to authenticate to a SwMI when the SC is temporarily or permanently disabled, see also clause 4.2.4.

4.2.2 End-to-End Encryption

The CM contains the necessary End-to-End Encryption algorithms and supports End-to-End Encryption of traffic data for the following services:

- half duplex individual direct call in V+D and DMO;
- half duplex individual hook call in V+D;
- full duplex individual hook call in V+D;
- group call in V+D and DMO;
- SDS-TL in V+D and DMO;
- full duplex circuit mode data in V+D;
- half duplex circuit mode data in V+D and DMO;
- packet data in V+D.

When an MS initiates an emergency individual or group call to a control room residing in the SwMI, then the control room might not be aware of or have access to the End-to-End Encryption cipher key material necessary to communicate with the MS. This is why, emergency calls should not be End-to-End Encrypted.

Status, SDS type 1, 2, and 3 are not used in conjunction with End-to-End Encryption, because an End-to-End Encryption algorithm would add too much overhead to such short messages.

A DM-GATE or DM-REP/GATE should support End-to-End Encryption of traffic data between DM-MSs and TM-MSs for the following services:

- half duplex individual direct call;
- group call;
- SDS-TL;
- half duplex circuit mode data.

The CM supports over-the-air key management (OTAK) of dynamic End-to-End Encryption cipher key material. Furthermore, the CM supports the use of pre-shared static End-to-End Encryption cipher key material.

For CM, there may be a secure link between ME and SC in order to protect storing of End-to-End Encryption cipher key material.

4.2.3 Operational-Tactical Address

Requirements for using the operational-tactical address can be found in TR 102 021-4 [i.2].

4.2.4 Enable and disable

Three different mechanisms are supported for enabling and disabling subscribers. The first two only apply to Personalized Smart Cards. The third applies to both PSC and CSC as it is a function of the CM and not the SIM.

1) Physical temporary and permanent enabling and disabling of an ME are based on TEI. When an ME is disabled, the SC inserted in the ME is not affected and may be re-used in another ME.

2) Physical temporary and permanent enabling and disabling of an SC are based on ITSI. When an SC is disabled, the ME the SC is inserted in is not affected and may be re-used with another SC.

3) Cryptographic temporary and permanent enabling and disabling of an SC are based on key management of end-to-end cipher key material. When an SC is cryptographically disabled, then the SC is no longer able to use the end-to-end cipher key material which is associated with the ITSI or one or several GTSIs stored on the SC. Furthermore, the ME the SC is inserted in is not affected and may be re-used with another SC.

Additionally for the CSC, when subscription is disabled there should be scope for the ME to instruct the CSC to perform E2E material erase.

4.3 Personalisation functions

A SIM is a tamper-proof container of personalised user parameters. In some PMR networks with large numbers of subscribers, it is vital to operators that user management is able to maintain personalised user parameters over-the-air, see also TR 102 021-11 [i.5]. Otherwise, users and operators will not be able to handle the logistics process associated with maintaining personalised user parameters.

User parameters can be categorised into parameters directly belonging to a subscriber identity, parameters not depending on subscriber identity, and parameters depending on subscriber identity.

In addition to the parameters mentioned in the following clauses, operators and users need to be able:

- to define user parameters by themselves which are specific to their network or even user organisation;
- to securely manage network or user organisation specific parameters on the SC or SIM;
- to maintain network or user organisation specific parameters over-the-air.

4.3.1 Subscriber identity

The SIM supports tamper-proof data management of the following user parameters which directly belong to a subscriber identity:

- Individual TETRA Subscriber Identity (ITSI);
- TETRA authentication Key (K);
- AIE keys (optionally);
- Personal Identification Number (PIN);
- Personal Unblocking Key (PUK);
- Operational-Tactical Address (OPTA) as an option.

For SIM, there should be a secure link between ME and SC in order to protect transfer of subscriber identities.

4.3.2 Parameters not depending on subscriber identity

The SIM should support tamper-proof data management of the following user parameters which do not depend on subscriber identity and should be available in all networks MS is registered to:

- phonebook with ITSI and MSISDN entries;
- history of last called ITSI and MSISDN;
- archive of SDS messages (sent, received, draft, etc.);
- white list of valid TETRA networks (list of MNIs);
- white list of valid non-TETRA networks.

4.3.3 Parameters depending on subscriber identity

The SIM should support tamper-proof data management of the following user parameters which depend on subscriber identity and is specific for each network an MS is registered to:

- list of valid preferred location areas;
- list of valid subscriber classes;
- list of status texts and a mapping to pre-coded status values;
- mapping of pre-coded status values to speed dial keys;
- gateway addresses of connected non-TETRA networks (PSTN, PABX, APN);
- address of the SDS Service Centre;
- one SCK-set per MNI for DMO and fallback mode operation according to clause 4.2.4 "The SCK", refer to EN 300 392-7 [i.6];
- list of V+D groups according to clause 6.3.13 "Group assignment", refer to EN 300 392-12-22 [i.7];
- list of DMO groups according to clause 6.3.6 "DMO group definition", refer to TS 100 392-18-3 [i.8].

For SIM, there should be a secure link between ME and SC in order to protect transfer of air interface encryption cipher key material.

4.4 Smart Card reference implementation

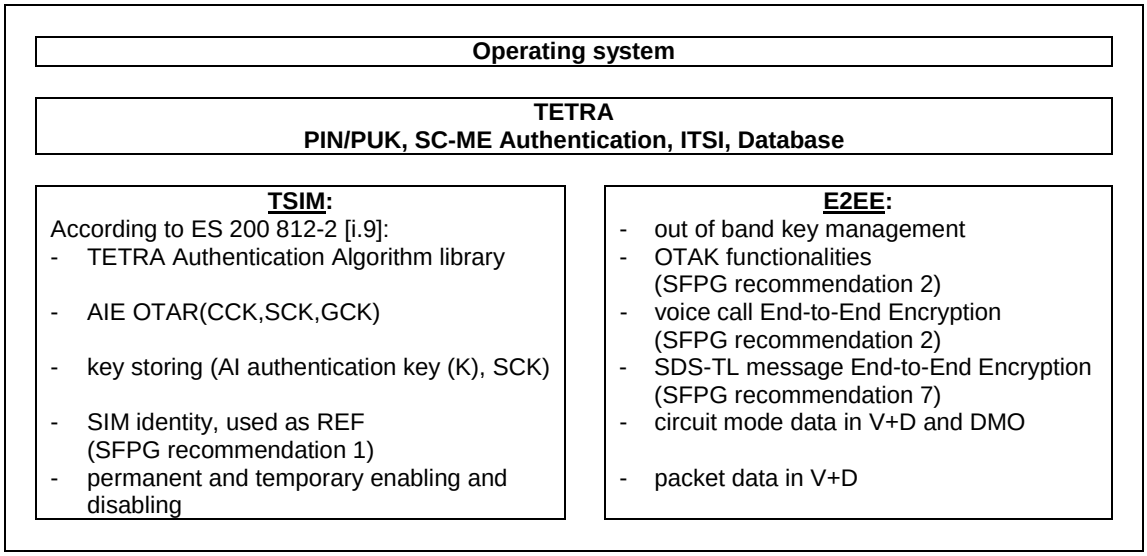
The following description of SC/Tetra SIM is included to give more information on how this might be realised:

A TETRA Smart Card can be divided into four blocks: Operating system, general TETRA application, TSIM application and E2EE application. The Smart Card contains an Operating system, which is dependent on the manufacturer of the Smart Card HW and one or several applications, which can be run by selecting them individually. The applications contain specific features and some of those may require PIN code verification before processing.

The general TETRA application has tasks like verification of PIN/PUK and the authentication between a terminal and a Smart Card. PIN and PUK codes are stored into a database of the TETRA application; they are not stored to elementary files. PIN and PUK codes will be programmed in the initialization function which initializes databases. The PIN code can be changed but the PUK code cannot be changed (except by a new initialization). The PIN code will be locked after 3 failed verifications. It can be unblocked using the PUK code. The PUK code is locked after 10 failed verifications. If the PUK code is locked a new initialization is required.

There also exist two officially specified applications, which are TSIM and E2EE. The TSIM features are specified in ES 200 812-2 [i.9] and E2EE features in the SFPG recommendation documents part 2 and part 7 [i.10]. The main features of each application are described in the block diagram in table 1.

Table 1: TETRA Smart Card contents



For a Personalised Smart Card it is expected that all the functional blocks in table 1 are present. For the Cryptographic Smart Card these would be the operating system, the common TETRA block and the E2EE block. For SIM only the blocks will be operating system; the common TETRA block and TSIM.

History

Document history		
V1.1.1	August 2002	Publication
V1.2.1	August 2011	Publication