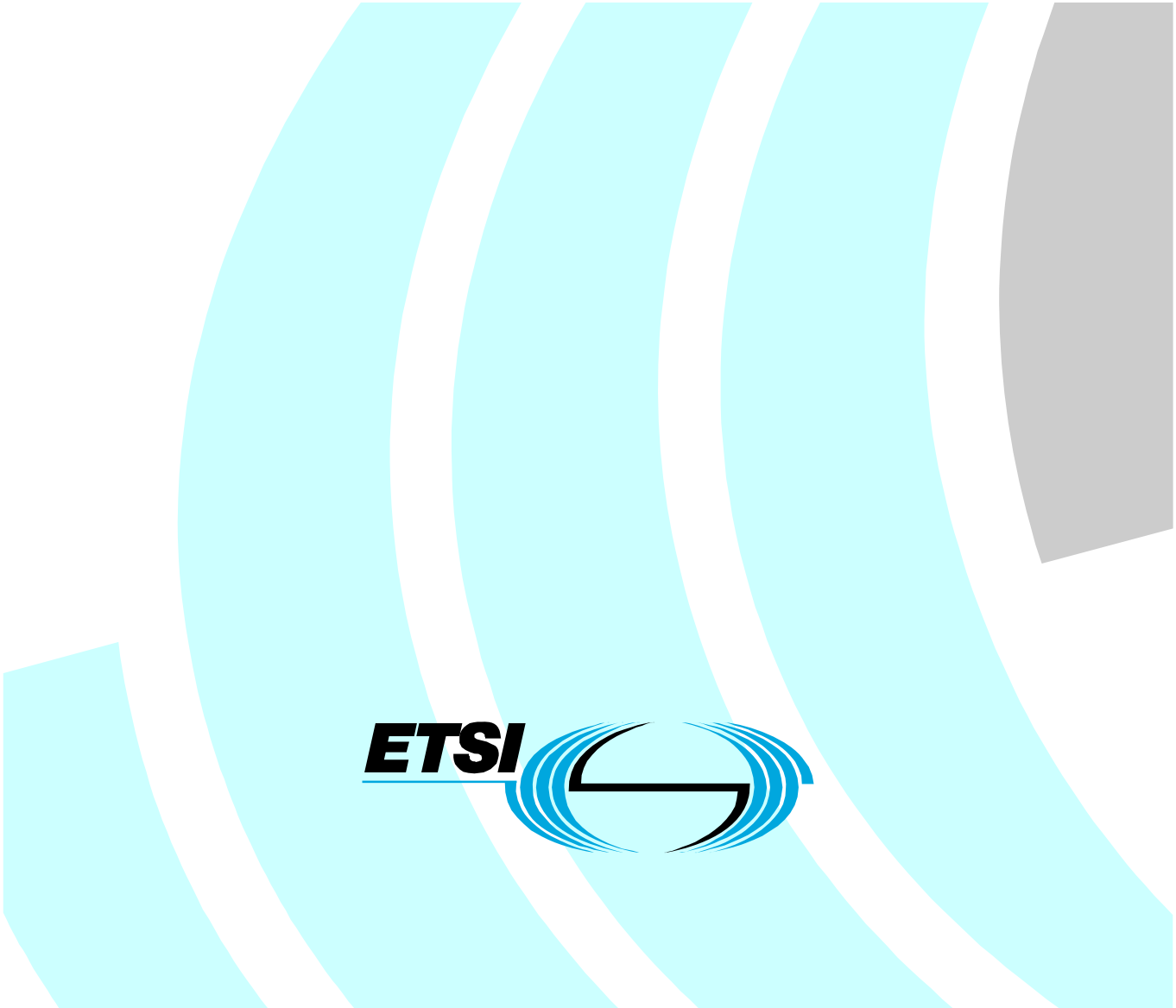
ETSI TR 102 021-7 V1.3.1 (2010-12)

Technical Report

Terrestrial Trunked Radio (TETRA);
User Requirement Specification TETRA Release 2.1;
Part 7: Security



Reference
RTR/TETRA-01196

Keywords
security, TETRA, 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://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 Report (TR) has been produced by ETSI Technical Committee Terrestrial Trunked Radio (TETRA).

The present document is part 7 of a multi-part deliverable covering the User Requirement Specifications (URSs) 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: "Subscriber Identity Module (SIM)" (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 are to produce ETSI deliverables (and maintenance thereafter) in accordance with the following requirements:

- The provision of user driven services, facilities and functionality as required by traditional Professional Mobile Radio (PMR) user organizations such as the Emergency Services, Government, Military, Transportation, Utility and Industrial organizations as well as Public Access Mobile Radio (PAMR) Operators.
- 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.
- Further enhancements of the TETRA standard in order to provide increased benefits and optimization in terms of spectrum efficiency, network capacity, system performance, quality of service, security and other relevant parameters.

- 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 standardized 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 present document provides the User Requirement Specifications for Security.

The URS is required by TC TETRA to guide the enhancement of the current TETRA standard, mainly the evolution of the HSD standard part towards broadband.

1 Scope

The present document contains the User Requirements Specifications (URS) which are described in non-technical terms.

Although high level requirements are proposed by the present document, it is considered restrictive to mandate particular security implementations at this point, until a revised threat analysis has been undertaken.

The present document 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 202 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".

3 Definitions and abbreviations

3.1 Definitions

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

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, utilize 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:

GCK-N	Group Cipher Key Number
GCK-VN	Group Cipher Key Version Number
HSD	High Speed Data
ITSI	Individual TETRA Subscriber Identity
K	authentication Key
ME	Mobile Equipment
OTAK	Over The Air Keying
OTAR	Over The Air Re-keying
PAMR	Public Access Mobile Radio
PMR	Private Mobile Radio
SIM	Subscriber Identity Module
TEAx	TETRA Encryption Algorithm x
TEDS	TETRA Enhanced Data Service
URS	User Requirement Specification

4 User Requirement Specification

4.1 User Requirements from questionnaire

Due to the specialist nature of security requirements and also due in some part to the sensitivity of users to discuss in open forum threats to any current standard, it was not considered appropriate to collect security requirements as part of the wider TETRA Release 2 user questionnaire sent out in 2001.

4.2 User Requirements derived from work on TETRA Release 1

TETRA Release 1, TETRA Release 2, and TETRA Release 2.1 should be maintained at an equal level of security. If further enhancements to the security of TETRA Release 2.1 are required, they should be applicable to all TETRA Releases up to Release 2.1. This is considered fundamental to Public Safety users as current and future systems are required to be implemented such that security accreditation can be achieved. This also applies to possible "stand-alone" developments such as HSD through direct access TEDS. High speed data solutions including evolution towards broadband require further consideration of security aspects.

It should be noted that security requirements apply to the standard as a whole, and individual requirements may not need satisfying with explicit security requirements, e.g. integrity can be checked with non-cryptographic integrity checking error correction schemes when used in conjunction with encryption schemes which may in themselves not provide integrity checks.

NOTE: TETRA is not required to support security protocols derived from other domains (e.g. GSM).

4.3 Core requirements

Although system requirements should be derived from the new threat analysis, it is considered probable that as a minimum the following core requirements will need to be supported by TETRA Release 2.1:

1) The TETRA Release 2.1 security standard should be able to provide authentication of the terminal and the infrastructure or the Smart Card and the infrastructure and should use, as far as possible, the mechanisms used in TETRA Release 1. In addition the standard should provide for authentication of the end user using, as far as possible, mechanisms provided in TETRA Release 1.

NOTE 1: An application level user authentication method is outside the scope of the air interface security standards.

2) The TETRA Release 2.1 security standard should be able to provide confidentiality protection for user plane information over the air interface.

3) The TETRA Release 2.1 security standard should be able to provide confidentiality and integrity protection of control plane information over the air interface. The integrity mechanism should not use strong cryptographic methods but should rely upon the mechanisms inherent in the use of a stream cipher and non-cryptographic checksums (e.g. LLC and L2-CRC) as per TETRA Release 1.

4) The TETRA Release 2.1 security standard should be able to provide confidentiality and integrity protection of all over-the-air management messages over the air interface.

5) The TETRA Release 2.1 security standard should be able to provide replay protection for both user plane and control plane information over the air interface for a sufficient period to meet international Public Safety and commercial markets. The keystream repeat length of the algorithms should remain unchanged at 23 days (approx) to avoid needing different key management principles for TETRA Release 2.1. Any change to the timeslot frequency, or to the use of fixed timeslots, may require fundamental redesign to the TEAx series of algorithms. Therefore in order to maintain the use of the TEAx series with as much backward compatibility as possible the same timeslot frequency should be maintained.

6) The structure of TETRA Release 2.1 keys should be identical to TETRA Release 1 keys. (By "structure" we mean the length of the key, the length of the key number (e.g. GCK-N) and the length of the key version number (e.g. GCK-VN).) TETRA Release 2.1 should use the same encryption algorithms as TETRA Release 1.

7) The authentication and OTAR mechanisms used in TETRA Release 2.1 should be the same as the TETRA Release 1 authentication and OTAR mechanisms. Where TEDS carriers are a part of a TETRA Release 1 network, registration and authentication will be based on an ITSI/K pair which are known on the Release 1 network, and authentication will take place according to TETRA Release 1 standards on the TETRA Release 1 network before TEDS services can be used. In networks where HSD carriers are not part of a TETRA Release 1 network, registration and authentication should be based on a similar ITSI/K pair known to the TETRA Release 2.1 network using same or similar authentication mechanisms as in TETRA Release 1 network.

NOTE 2: The authentication and OTAR protocols will operate on both TETRA Release 1 and TETRA Release 2.1 carriers.

8) The remote enable and disable functions of TETRA Release 1 should apply to TETRA Release 2.1 systems and mobile stations.

9) Where TETRA Release 2.1 systems and mobile stations support TETRA Release 1 circuit-mode calls, it should be possible to provide additional protection for user plane information by means of end-to-end encryption according to ES 202 109 [i.1]. If circuit-mode calls are to be supported in TETRA Release 2.1, it should be possible to provide them with end-to-end encryption according to ES 202 109 [i.1]. If a TETRA Release 2.1 codec is required to operate in a TETRA Release 1 air interface environment, then either the bit rate should be less than the TETRA Release 1 codec air interface and bits allocated for end to end encryption synchronization, or frame stealing should be supported to allow the TETRA Release 1 encryption synchronization mechanisms to be maintained. Where frame stealing is the supported synchronization method the codec should be able to sustain a frame stealing rate compatible with TETRA Release 1 standards requiring a stealing rate of between 1 and 4 stolen frames per second.

10) The system should be able to support a mechanism whereby information held on a removable personalization module (e.g. Smart Card) is protected from unauthorized access. A Smart Card may contain the ITSI/K pair and the authentication algorithms.

11) Any requirement to personalize the TETRA SIM or Smart Card over the air, or to use the SIM or the Smart Card for other security critical applications (e.g. financial transactions) will require an extra application level of security applied in addition to the air interface and the SIM/Smard Card-ME encryption. This is outside the scope of the TETRA standards.

12) The TETRA Release 2.1 security standard should be able to provide end-to-end confidentiality protection of Short Data Services concurrently with TEDS.

13) Any terminal should be authenticated with security parameters established before location services are made operational.

14) All TETRA Release 2.1 elements should be designed with the export license limitations in mind to avoid intentional or unintentional breaking of these rules, e.g. by plugging in an end-to-end encrypting Smart Card into a terminal that is not allowed to work with one.

15) In cases where the authentication function of an ITSI and the related end-to-end encryption OTAK functionality exist in separate but connected physical elements, e.g. some Smart Card implementations, the connecting interface should support (mutual) authentication.

It should be recognized that these requirements may exceed those needed by some commercial operators. In these cases it may be appropriate to allow implementations that provide a lower level of protection as with the different classes that are supported within TETRA Release 1.

4.4 Work required

It is considered appropriate that a revised threat analysis is produced to encompass any new services and facilities that become available through TETRA Release 2.1. WG6 should also work with other WGs to ensure that the security requirements are passed through to any new standards that are produced.

4.5 Testing requirements

The new security requirements should be traceable to a new threat analysis.

4.6 Timescales

Security standardization should be completed in line with other developments such as Air Interface Enhancements, HSD, Smart Card/SIM, Local Mode Broadband, and Over The Air Management. This should ensure that any users wishing to migrate their systems from TETRA 1 to Release 2.1 are not being subject to any increased threat.

History

Document history		
V1.1.1	December 2001	Publication (Historical)
V1.2.1	October 2002	Publication
V1.3.1	December 2010	Publication