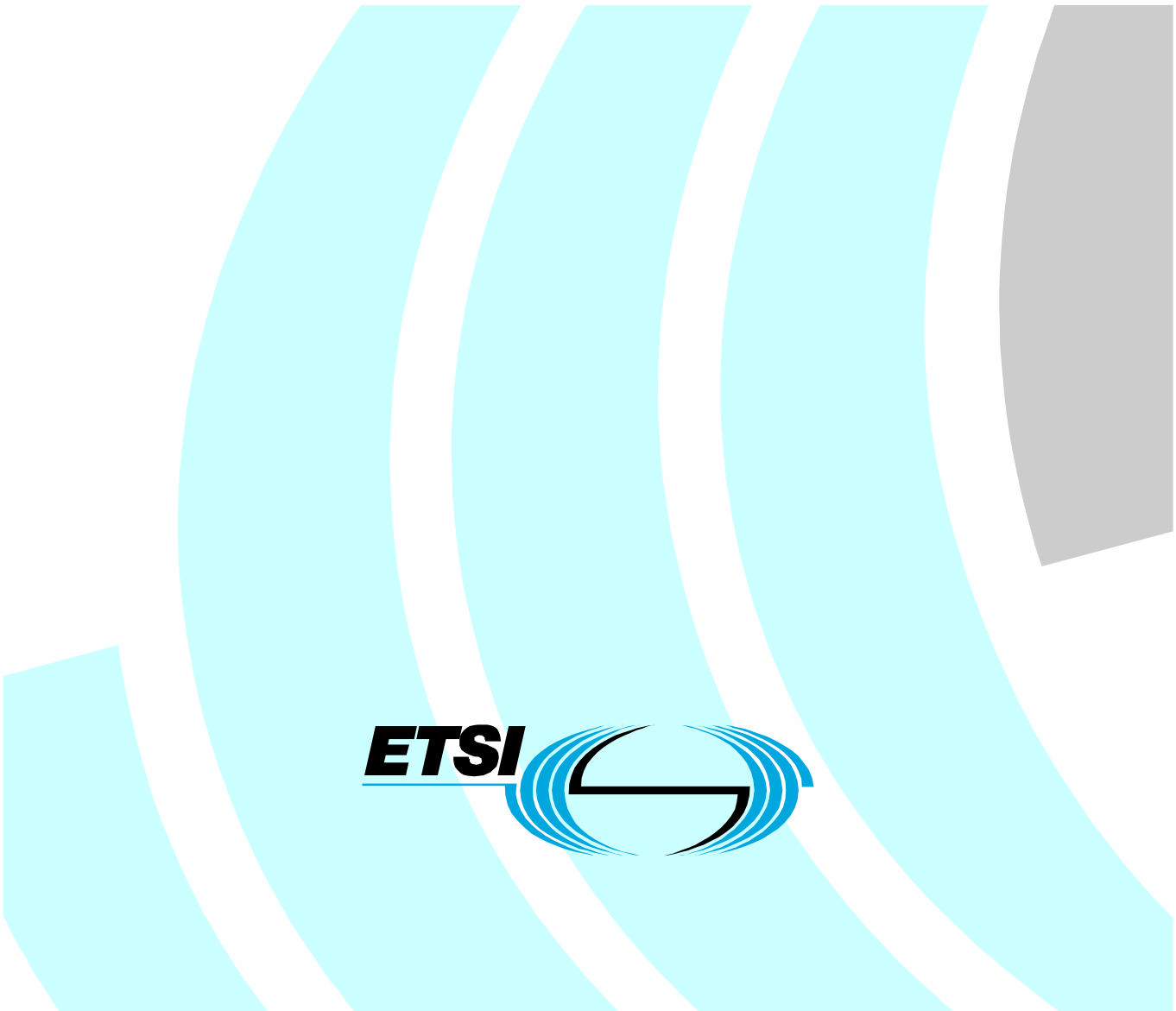
ETSI TR 102 021-7 V1.2.1 (2002-10)

Technical Report

Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 7: Security



Reference
RTR/TETRA-01077

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

Important notice

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

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

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

Copyright Notification

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 Project 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, as identified below:

Part 1: "General Overview";

Part 2: "High Speed Data";

Part 3: "Codec";

Part 4: "Air Interface Enhancements";

Part 5: "Interworking and Roaming";

Part 6: "Subscriber Identity Module (SIM)";

Part 7: "Security".

Introduction

The TETRA Release 2 suite of standards was mandated in the new Terms of Reference (ToR) for ETSI Project TETRA approved at ETSI Board meeting number 28 (Board 28) on 6th September 2000 [1], [2]. Its aim was to enhance the services and facilities of TETRA in order to meet the emerging user requirements, utilize new technologies and, by maintaining the competitiveness with other wireless technologies, increase the future proofness of TETRA as the standard for PMR and PAMR world-wide.

The approved programme for TETRA Release 2 covers five work areas, namely:

- High speed data
- Speech coding
- Air interface enhancements
- Interworking and roaming
- SIM

and the User Requirement Specification for each of these work areas is covered by its own document. In addition, though not listed as a separate area of activity in the approved work programme, any significant market requirement for enhancement to TETRA Security will also be taken on board and is covered by a separate URS.

The present document provides the User Requirement Specification for Security.

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 equipment.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] B28(00)12: "Extension of EPT Terms of Reference to Enable TETRA "Release 2".

[2] B28(00)24 Rev 2: "Summary minutes, decisions and actions from 28th ETSI Board Meeting", Sophia Antipolis, 5-6 September 2000.

[3] 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 (see bibliography) 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

3.2 Abbreviations

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

EPT	ETSI Project TETRA
HSD	High Speed Data
ITSI	Individual TETRA Subscriber Identity
K	authentication Key
ME	Mobile Equipment
OTAR	Over The Air Re-keying
PAMR	Public Access Mobile Radio
PMR	Private Mobile Radio
SIM	Subscriber Identity Module
TAPS	TETRA Advanced Packet Service
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 (see bibliography).

4.2 User Requirements derived from work on TETRA Release 1

TETRA Release 1 and TETRA Release 2 should be maintained at an equal level of security. If further enhancements to the security of TETRA Release 2 are required, they should be applicable to both TETRA Release 1 and Release 2. This is considered fundamental to Public Safety users as current and future systems must be implemented such that security accreditation can be achieved. This also applies to possible "stand-alone" developments such as HSD through TAPS. There are no further security considerations required for TAPS. TEDS requires 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) The TETRA Release 2 security standard should be able to provide authentication of the terminal 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 security standard should be able to provide confidentiality protection for user plane information over the air interface.

3) The TETRA Release 2 security standard should be able to provide confidentiality and integrity protection of control plane information over the air interface. The integrity mechanism shall not use strong cryptographic methods but shall 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 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. 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.

5) The structure of TETRA Release 2 keys shall 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 shall use the same encryption algorithms as TETRA Release 1.

6) The authentication and OTAR mechanisms used in TETRA Release 2 shall be the same as the TETRA Release 1 authentication and OTAR mechanisms. TEDS carriers will be part of a TETRA Release 1 network, and 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.

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

7) The remote enable and disable functions of TETRA Release 1 should apply to TETRA Release 2 systems and mobile stations.

8) Where TETRA Release 2 systems and mobile stations support TETRA Release 1 circuit-mode calls, it shall be possible to provide additional protection for user plane information by means of end-to-end encryption according to ES 202 109 [3]. If circuit-mode calls are to be supported in TETRA Release 2, it must be possible to provide them with end-to-end encryption according to ES 202 109 [3]. If a TETRA Release 2 codec is required to operate in a TETRA Release 1 air interface environment, then either the bit rate must be less than the TETRA Release 1 codec air interface and bits allocated for end to end encryption synchronization, or frame stealing must 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.

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

NOTE 3: There is no known method for providing an OTAR mechanism based on K in the current TETRA security standard that makes the use of SIM to store updateable keys viable, *because of the lack of an encryption mechanism over the SIM-ME interface. In addition post-personalization file storage structures do not lend themselves to secure storage of key material.* In cases where OTAR is essential the K/ITSI pair and algorithm set (TAA1) can be stored on the ME and the SIM used to store other (non-key related) personalization data.

10) Any requirement to personalize the TETRA SIM over the air, or to use the SIM 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-ME encryption. This is outside the scope of the TETRA standards.

11) The TETRA Release 2 security standard should be able to provide end-to-end confidentiality protection of Short Data Services concurrently with TEDS.

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

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. 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 and HSD. This should ensure that any users wishing to migrate their systems from TETRA 1 to Release 2 are not being subject to any increased threat.

Annex A: Bibliography

- ETSI TR 102 021-1: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 1: General Overview".
- ETSI TR 102 021-2: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 2: High Speed Data".
- ETSI TR 102 021-3: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 3: Codec".
- ETSI TR 102 021-4: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 4: Air Interface Enhancements".
- ETSI TR 102 021-5: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 5: Interworking and Roaming".
- ETSI TR 102 021-6: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 6: Subscriber Identity Module (SIM)".
- EPT13(00)17r1: "TETRA Release 2 Work Programme".
- EPT/WG1(01)046v9: "ETSI Project TETRA (EPT) TETRA Release 2 Questionnaire".

History

Document history		
V1.1.1	December 2001	Publication
V1.2.1	October 2002	Publication