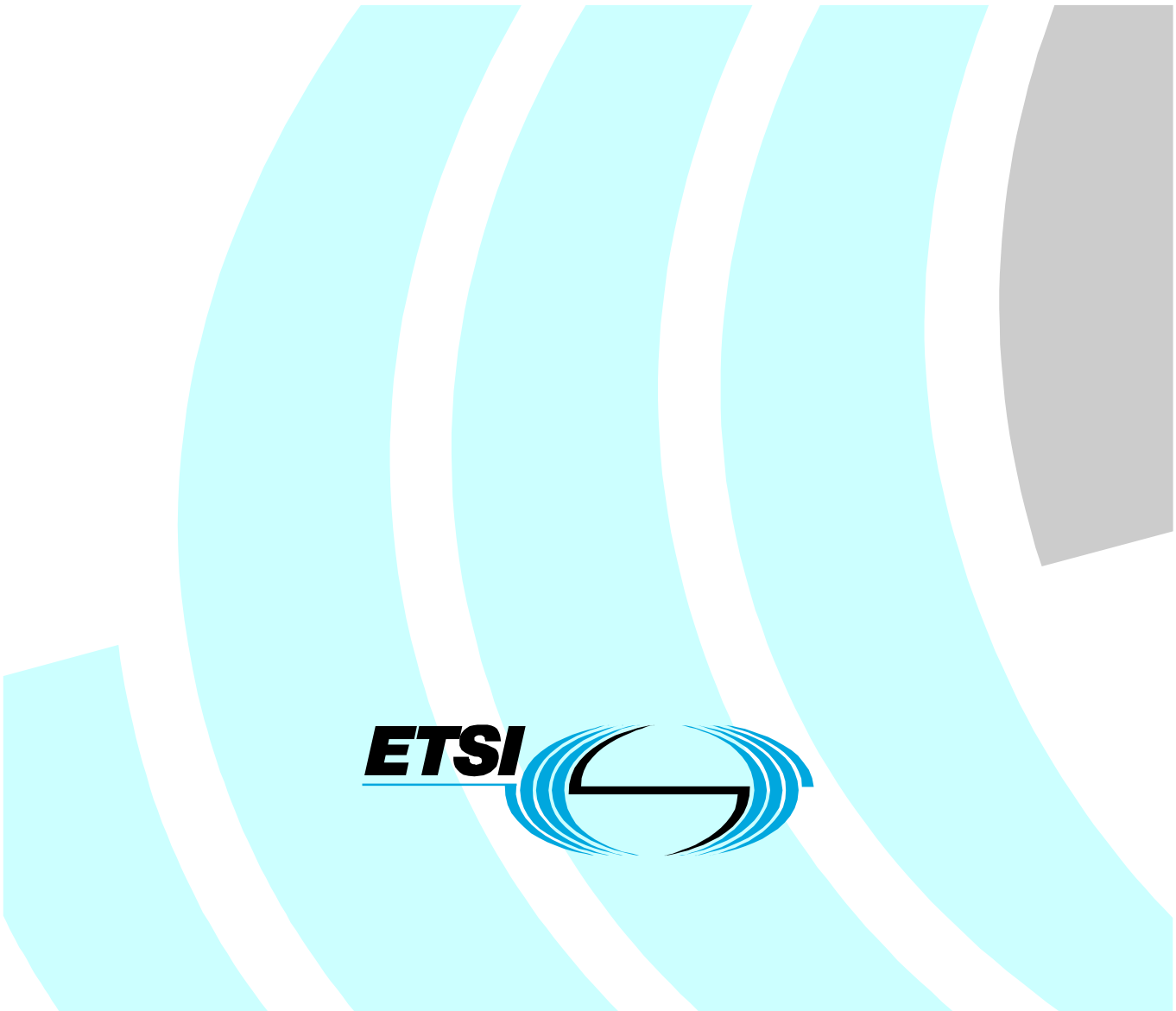
ETSI TR 102 021-7 V1.1.1 (2001-12)

Technical Report

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



Reference
DTR/TETRA-01077

Keywords
TETRA, user, security

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 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 [7][8]. 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 futureproofness 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 outlines core requirements, required work and timescales for security standardization of TETRA Release 2.

The present document is applicable to the specification of TETRA Release 2 equipment.

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.

2 References

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

[1] ETSI TR 102 021-1: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 1: General Overview".

[2] ETSI TR 102 021-2: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 2: High Speed Data".

[3] ETSI TR 102 021-3: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 3: Codec".

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

[5] ETSI TR 102 021-5: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 5: Interworking and Roaming".

[6] ETSI TR 102 021-6: "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2; Part 6: Subscriber Identity Module (SIM)".

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

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

[9] TETRA MoU Recommendation 02: "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

3.2 Abbreviations

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

EPT	ETSI Project TETRA
ETSI	European Telecommunications Standards Institute
HSD	High Speed Data
MoU	Memorandum of Understanding
OTAR	Over The Air Re-keying

PAMR	Public Access Mobile Radio
PMR	Private Mobile Radio
SIM	Subscriber Identity Module
TAPS	TETRA Advanced Packet Service
TETRA	TErrestrial Trunked RAdio
TR	Technical Report
URS	User Requirement Specification
WG	EPT Working Group
WG6	EPT Security working group

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.

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.

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:

- the system should be able to provide authentication of the terminal, the infrastructure and the end user;
- the system should be able to provide confidentiality protection for user plane information over the air interface;
- the system should be able to provide confidentiality and integrity protection of control plane information over the air interface;
- the system 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 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;
- the authentication and OTAR mechanisms used in TETRA Release 2 shall be the same as the TETRA Release 1 authentication and OTAR mechanisms;
- the remote enable and disable functions of TETRA Release 1 shall apply to TETRA Release 2 systems and mobile stations;

- 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 TETRA MoU Recommendation 02 [9]. 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 TETRA MoU Recommendation 02 [9];

- the system should be able to support a secure mechanism whereby information held on the SIM is protected from unauthorized access;

- the security aspects of a SIM specified for a TETRA Release 2 mobile station must be able to support all TETRA Release 1 SIM security features in the same mobile station.

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 be subject to any increased threat.

Annex A: Bibliography

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