ETSI TR 103 565-2 V1.1.1 (2018-05)

TETRA and Critical Communications Evolution (TCCE);
Interworking between TETRA and
3GPP mission critical services;
Part 2: Security of interworking between
TETRA and Broadband applications

Reference

DTR/TCCE-06192

Keywords

broadband, radio, TETRA

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

TETRA users are adopting broadband technologies based on 3GPP LTE for critical communications to add new services and capabilities to their operations. TETRA systems are required to work alongside and together with such broadband critical communications systems to enable the users to benefit from the strengths of both technologies.

Interworking is necessary with both the developing suite of 3GPP Mission Critical applications including MCPTT and MCData applications, and also with more general use of broadband networks for enhanced bandwidth and higher speed general data applications. The present document describes the security related aspects of such interworking between technologies. It contains use cases for secure interworking, security related issues and potential security solutions.

1 Scope

The present document contains use cases, threats and security solutions for interworking between TETRA and 3GPP standardized mission critical broadband systems. The security solutions generated within the present document are assessed for applicability to further standardization work. The security solutions also highlights areas which need to be solved by implementation.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative 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 referenced document (including any amendments) applies.

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

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 TR 103 565: "TETRA and Critical Communications Evolution (TCCE); Terrestrial Trunked Radio (TETRA); Study into interworking between TETRA and 3GPP mission critical services".

[i.2] 3GPP TR 23.782: "Study on mission critical communication interworking between LTE and non-LTE systems".

[i.3] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[i.4] ETSI EN 302 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".

[i.5] 3GPP TS 33.180: "Security of the mission critical service".

3 Definitions and abbreviations

3.1 Definitions

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

air interface encryption: encryption which protects a radio link only

end-to-end encryption: encryption within or at the source end system, with the corresponding decryption occurring only within or at the destination end system

3.2 Abbreviations

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

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
AI	Air Interface
AIE	Air Interface Encryption
BS	Base Station
COTS	Commercial Off The Shelf
DoS	Denial of Service
E2EE	End to End Encryption
eNodeB	enhanced Node B
GCM	Galois Counter Mode
GSSI	Group Short Subscriber Identity
HTTPS	Secure Hyper Text Transfer Protocol
ID	IDentity
ISSI	Individual Short Subscriber Identity
IWF	InterWorking Function
LMR	Land Mobile Radio
LTE	Long Term Evolution
MC	Mission Critical
MCData	Mission Critical Data
MCPTT	Mission Critical Push To Talk
MS	Mobile Station
OTAK	Over The Air Key management
OTAR	Over The Air Rekeying
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
SFPG	Security and Fraud Prevention Group
SIP	Session Initiation Protocol
SRTCP	Secure Real Time Protocol
SRTP	Secure Real-time Transport Protocol
SwMI	Switching and Management Infrastructure
TCCA	The Critical Communications Association
TETRA	TErrestrial Trunked RAdio
TLV	Type Length Value
TR	Technical Report
URI	Uniform Resource Identifier
XMLenc	eXtensible Markup Language encryption

4 Interworking overview

4.1 Interworking realization

The interworking function is realized according to ETSI TR 103 565 [i.1] as an adaptation between a TETRA SwMI and the 3GPP MC system LMR interworking interface, to be specified within 3GPP Release 15, and has been studied in 3GPP TR 23.782 [i.2]. This is shown in figure 4.1-1.

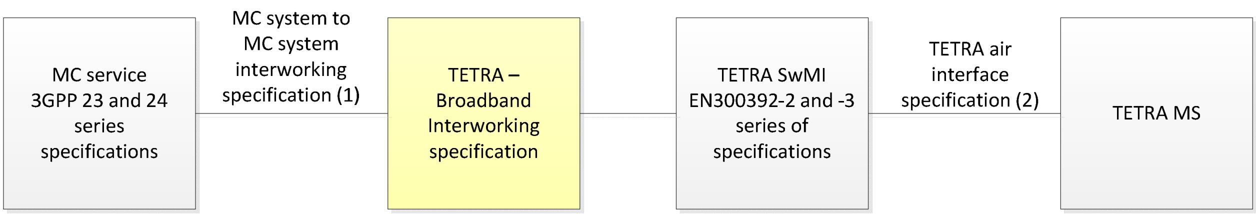

Figure 4.1-1: Concept of the interworking function

The interworking function provides a single logical interface between each pair of one MC service and one TETRA SwMI. Any realization of multiple interfaces between a pair of systems e.g. for resilience is outside the scope of the present document.

Note that the interworking function in ETSI TR 103 565 [i.1] specifies behaviour, and is not necessarily intended to be a specification for a physical interface device. Thus either or both of the interfaces to an interworking function may not be exposed and may be internal to the implementation of a solution. This should be taken into account when assessing the security issues.

4.2 Use cases

The use cases for interworking between TETRA and 3GPP MCPTT and associated MCData services are as follow:

- Short term usage, where a user community is in transition from use of TETRA to use of MCPTT and MCData, and requires communications between users during this activity. 'Short term' may still require interworking for several years, especially where nationwide systems are deployed.
- Long term, where users use both TETRA and LTE for communications for the foreseeable future, without time limit. Use of one or the other technology may be dependent on user role, on user location or communications type (e.g. use of TETRA for voice, LTE for high speed data aspects).

There may be no difference in the solutions for security between a 'short term' and a 'long term' use of interworking; however a user organization may be prepared to accept some increased level of risk for a shorter term and take an increased level of risk into account as part of a cost-benefit decision when deciding which measures to implement.

Either use case may require security to be maintained fully end to end.

4.3 Security aspects of interworking

Each system will be responsible for managing its own security aspects, such as authorization, authentication of user or device and protection of signalling and traffic information. End to end encrypted material should be able to pass between users on both systems.

There are two goals associated with security:

- The solution should not affect security for any users of either system that are not involved in interworking with the other system.
- The solution should maintain as high a level of security as possible for users that are involved in interworking communications with users in the other system.

5 Threats

5.1 General

This clause details some of the threats to interworking between TETRA and MC systems.

5.2 Masquerade and impersonation

The following threats are possible relating to masquerade and impersonation:

- Systems: one system may be impersonated at the interworking function to the other system.
- Interworking function: a fake interworking function impersonates an interworking function and associated system.
- Clients: a client on one system may enable impersonation of another client of the same system to gain access to inter-system communications.

- Users: a user on one system may impersonate another of the same system to gain access to inter-system communications.

5.3 Eavesdropping

Eavesdropping could apply to speech or data traffic, as well as to control functions.

Eavesdropping may take place on an exposed interface in one system between clients and servers (or between clients and peripheral devices) which compromises communications on the other system during interworking communications, this could include an air interface.

Eavesdropping may take place on external links to the interworking function, or in a device introduced into a link as a 'man in the middle' device with the intention of eavesdropping on that link.

Eavesdropping may take place on links to the interworking function that are internal to one system.

Eavesdropping may take place within the interworking function, for example if the interworking function needs to decrypt information received from one system prior to re-encrypting it for transmission into the other system.

NOTE: The interworking function may be internal to one system, or even to both systems if a single physical infrastructure provides both TETRA and MC services.

Ambience listening invoked across the interworking function (if supported) provides an additional possibility for eavesdropping on a user, without the user being aware.

5.4 Traffic analysis

Access to one system discovers information concerning traffic on the other system.

Access to the interworking function or to links either side of the interworking function allows traffic analysis to be carried out with respect to users or groups on either system.

- Direct access to call flow information through access to the interworking function.
- Access to address books or group linking tables allows information discovered on one system to be aligned with information on the other system.
- Information concerning group member affiliation.
- Access to accounting and management tools on one system or on the interworking function provides information about call statistics applying to interworking calls.

Eavesdropping on links to the interworking function provides direct access to traffic flow information.

5.5 Denial of service

Generate excessive traffic on a group on one system to deny service to the interconnected (linked) group on the other system.

Placing a call with high priority on one system may affect the available resources on the interconnected system.

Upset operation of the interworking function; e.g. erase an address book, interrupt a link, physical attack.

Interrupt key management services.

A successful attack on the interworking function resulting in its unavailability will cause loss of inter system communications.

5.6 Manipulation/insertion

Modification of frame formats to confuse encrypted speech with synchronization stolen frames or signalling frames. May also be a denial of service attack by modifying control information.

Insertion or modification of signalling information.

Modification of mapping of groups between systems.

Attack on configuration management interfaces to modify addresses, mapping and other configuration data.

Modification of traffic passed between systems.

Insertion of acknowledgements (positive or negative) to falsify delivery responses.

Adding unauthorised users to a group, or unauthorised linking of groups on one system may misdirect traffic to users who are unknown to the interconnected system.

It may not be apparent to a user that the group in which he is communicating is interconnected to a group on the other system.

5.7 Extraction of security information

Extraction of encryption keys or other security parameters that are stored in the interworking function or other network elements for the purpose of enabling secure interworking; security parameters can then be used to mount an attack at the interface or within one of the interconnected systems.

Extraction of encryption keys or other security parameters from terminals, especially from Commercial Off The Shelf (COTS) terminals and applications.

5.8 Replay

Replay of signalling or traffic information at the interworking interface.

Replay on one system may not be obvious from the perspective of the interconnected system.

5.9 Repudiation

It may be difficult to prove the origin of communications from the interconnected system.

6 Security measures

6.1 Service authorization

Users will be expected to be authorized to interwork across the interworking function with users in the other type of system. Groups are expected to also be authorized for interworking communications.

If group call affiliations are managed locally, then each system can be responsible for authorizing its users to join groups which are connected to groups in the other system, without involvement of the interworking function.

If identity translation is needed by an address book in order to interwork with individual services, then being present in this address book can provide additional authorization for interworking, in addition to any authorization within the local system. If the MC system uses different addresses for different services (e.g. MCPTT-ID, MCData ID) then the presence of a service specific address will also provide some degree of service level authorization.