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

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.

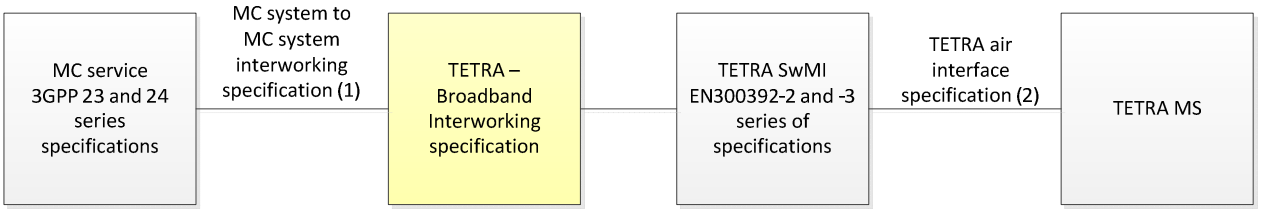

Figure 4.1-1: Concept of the interworking function

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.

6.2 User authentication

Each system carries out its own authentication locally. The TETRA system authenticates the MSs, the MC system authenticates the user. PIN entry can provide some additional level of user authentication to the device. Each system will have to trust that the connected system has correctly authenticated any user or the device as appropriate that makes a call request that is carried by the interworking function.

6.3 System authentication

6.3.1 Interface authentication

The authenticity of the interworking function will have to be verified by each system independently.

Users making calls across the interworking function will have to trust that their local system has verified the authenticity of that interface.

6.3.2 System authentication by IWF

The IWF will need to verify that the connected system(s) is valid and authentic, by explicit or implicit means.

6.4 Signalling protection

Each system may require signalling, including addressing of users and groups, to be kept confidential from unauthorised parties. These include eavesdroppers at the air interface. In the case of an MC system, confidentiality will generally also be required from the PLMN operator providing the underlying LTE service.

Each system has separate mechanisms to protect signalling from eavesdropping, and also to protect integrity of signalling. TETRA uses air interface encryption; MCPTT and MCData use a mixture of encryption of information within SIP bodies (XMLenc) and HTTPS for its signalling plane protection, and SRTCP for floor control. The connection between SIP core and SIP client in the device may also be encrypted, but this mechanism may not be in the trust domain of the MC service.

As these mechanisms are different, any interface carrying signalling between either system and the interworking function (as shown on figure 4.1-1) cannot be encrypted. Therefore, where any interconnecting network between a system and the interworking function is not trusted, additional measures should be taken to secure links between the relevant inter-system interface(s) and the interworking function. The interworking function itself will need to be protected by appropriate measures (e.g. physical, procedural) to prevent it from becoming a point of attack.

Both systems should implement their signalling protection mechanisms, to prevent one system operating without signalling confidentiality from providing a point of attack into communications on the other system.

6.5 Traffic protection

Traffic confidentiality can be provided within each system for speech.

For speech protection, MCPTT uses SRTP between clients using a secret group key for group communications that is provided in advance of the communications, and session keys negotiated at the start of calls for private calls, and offers end to end encryption. Identity based encryption is used for key management. The AES GCM algorithm implementation is used for traffic encryption. There is additional air interface encryption provided by the LTE network between the device and the eNodeB (but managed by the PLMN operator). 3GPP mission critical security is specified in 3GPP TS 33.180 [i.5].

MCData uses the same identity based key management principles as MCPTT. The user data can be carried over either signalling plane or media plane within the MC system in a TLV format, and encrypted with AES GCM. An identity based signature mechanism also allows the encrypted data to be signed.

TETRA uses air interface encryption as specified in ETSI EN 300 392-7 [i.3] for protection between MS and BS, with keys provided as part of the air interface authentication and OTAR functions. Additional end to end encryption can be overlaid, using a variety of algorithms. However, keys are provided in advance of communications by TETRA key management processes and not negotiated at the start of calls; and implementations compliant to TCCA SFPG Recommendations do not use GCM for synchronization.

For basic security, MCPTT media encryption could be applied as far as the interworking function, and TETRA air interface encryption applied inside the TETRA network. The same is also the case for MCData. The path between either system and the interworking function should be protected; and the interworking function itself will need to be protected by appropriate measures (e.g. physical, procedural) to prevent it from becoming a point of attack.

End to end encryption is possible separately inside each system, terminated at the interworking function. By terminating at the interworking function, a transcoding function is also possible to allow the native vocoders to be used on each system.

NOTE: There may be quality loss associated with transcoding.

For more comprehensive end to end security, without decrypting at the interworking function, end to end encryption can be applied on communications between MCPTT clients (and MCData clients) and TETRA devices. This would need to make use of TETRA protocols, vocoder and mechanisms in both the MCPTT system and the TETRA system, as the TETRA air interface would not be easily modified to carry another vocoder or other mechanisms, especially where these require a higher bandwidth.

If the TETRA vocoder and end to end encryption was to be used through to the MCPTT system, the extra bandwidth available on an LTE system could allow encryption synchronization to be carried without stealing speech frames. However, if this were possible, the source of encrypted speech on the MCPTT system would need to indicate candidate speech frames for stealing to the interworking function so that the normal stolen speech synchronization could be applied in the TETRA network; and in the reverse direction for speech originating in the TETRA, speech would be stolen for synchronization and so MCPTT clients would have to adapt to this.

6.6 Key management

6.6.1 TETRA air interface security

Air interface security will be within the domain of the TETRA system, and will not be extended to the interworking function, thus there are no key management considerations. Additional security between elements inside a TETRA SwMI and to any interworking function are outside the scope of the TETRA standards, and would depend on specific implementations.

6.6.2 MC service signalling security

If the interworking function acts as an MC service server within the MC system, depending on the standard developed following the relevant study [i.2], then server to server security needs to be extended to the interworking function. This would entail loading a Signalling Protection Key, a 128 bit AES key, into the interworking function.

6.6.3 Speech security

6.6.3.1 Encryption translation

End to end encryption is possible separately inside each system, terminated at the interworking function. To enable the interworking function to terminate end to end encryption within the MCPTT system, the interworking function would need to have an end point identity, and be provisioned with the appropriate public and private master keys to enable identity based key management to take place. Similarly, the interworking function would need to be provisioned with the necessary symmetric keys for use in the TETRA system, which would either mean an out of band key loading solution, or providing the interworking function with a TETRA ISSI such that OTAK can be used from a key management station.

6.6.3.2 Fully end to end

For fully end to end protection, the encryption mechanisms and key management would need to follow the TETRA key management practice of using pre-shared symmetric keys, as the identity based encryption used for key establishment in MCPTT would be difficult to establish in TETRA (due to the need to carry the MCPTT URI based identity and the public/private key material to TETRA users).

There would need to be a means to carry TETRA key management messages to the users on the MCPTT system, and to allow distribution by TETRA key management mechanisms may need an ISSI to be allocated to each MCPTT client.

Furthermore, if TETRA key management procedures are used, it will be necessary to associate a GSSI to each group within the MCPTT system to enable key associations to be made. Alternatively, an association process applicable to MCPTT group addresses will be needed.

6.7 Policy, auditing and reporting

A security policy will need to be in place which details which types of communication are permissible for interworking, and whether specific procedural measures are needed for these communications. Users need to be aware whether a call includes other users who are connected via an interworking interface.

Monitoring and filtering should be applied on links to the IWF to reduce its vulnerability to technical attack, and to record events on those links. An audit and reporting system should be in place to allow audit of normal and exceptional operating conditions, and the nature of exceptional events.

Traffic and signalling at the IWF may be logged for audit and analysis purposes, in addition to monitoring and logging of exceptional or threat events.

6.8 Solution implementation

Some threats, both general and specific to particular deployments. will need to be solved by implementation which is outside the scope of published standards.

7 Threat - Security Measure Analysis

7.1 Threat Summary

This section provides a summary of the threats (identified in clause 5), with identifiers by which they are referenced in the threat-security measure mapping table.

T5.2 Masquerade/impersonation:

- **T5.2.1** System impersonation
- **T5.2.2** IWF impersonation
- **T5.2.3** Client impersonation
- **T5.2.4** User impersonation

T5.3 Eavesdropping:

- **T5.3.1** Eavesdropping in other system
- **T5.3.2** Eavesdropping on external links between systems
- **T5.3.3** Eavesdropping IWF links within a system
- **T5.3.4** Eavesdropping within IWF

- **T5.3.5** Ambience listening invoked across IWF

T5.4 Traffic Analysis:

- **T5.4.1** Traffic analysis in other system
- **T5.4.2** Traffic analysis in intersystem link
- **T5.4.3** Traffic analysis within IWF

T5.5 Denial of Service:

- **T5.5.1** Excessive traffic in other system
- **T5.5.2** Improper use of high priority calls
- **T5.5.3** DoS of IWF
- **T5.5.4** DoS of key management

T5.6 Manipulation/Insertion:

- **T5.6.1** Traffic modification
- **T5.6.2** Signalling modification
- **T5.6.3** Signalling insertion
- **T5.6.4** Mapping modification
- **T5.6.5** Configuration modification
- **T5.6.6** False response

T5.7 Extraction:

- **T5.7.1** Keys extraction from IWF
- **T5.7.2** Keys extraction from TETRA terminals
- **T5.7.3** Keys extraction from high assurance MC terminals
- **T5.7.4** Key extraction from COTS MC terminals

T5.8 Replay:

- **T5.8.1** Traffic replay
- **T5.8.2** Signalling replay

T5.9 Repudiation:

- **T5.9.1** Repudiation

Threats to additional interfaces on an IWF, e.g. configuration and management interfaces, are a matter for implementation and are outside the scope of the present document.

7.2 Security Measure Summary

This section provides a summary of the security measures (identified in clause 6), with identifiers by which they are referenced in the threat-security measure mapping table.

M6.1 Service authorization:

- **M6.1.1** User interworking authorization

- **M6.1.2** Group interworking authorization

M6.2 User authentication:

- **M6.2.1** User authentication

M6.3 Interface authentication:

- **M6.3.1** Authentication of IWF by system
- **M6.3.2** Authentication of system by IWF

M6.4 Signalling protection:

- **M6.4.1** Signalling confidentiality within MC system
- **M6.4.2** Signalling confidentiality within TETRA system, including use of AIE
- **M6.4.3** System signalling integrity within MC system
- **M6.4.4** System signalling integrity within TETRA system
- **M6.4.5** IWF links protection
- **M6.4.6** IWF protection

M6.5 Traffic confidentiality:

- **M6.5.1** Traffic confidentiality within MC System
- **M6.5.2** Traffic confidentiality within TETRA System, including use of AIE
- **M6.5.3** E2EE where IWF is the endpoint

NOTE: Applies to E2EE from both MC and TETRA side of IWF.

- **M6.5.4** E2EE through IWF

M6.6 Key management:

- **M6.6.1** TETRA AI key management
- **M6.6.2** MC key management
- **M6.6.3** E2EE key management

M6.7 Policing, auditing and reporting:

- M6.7.1 Traffic policing and filtering on link to IWF
- M6.7.2 Audit and reporting of events and exceptions on IWF
- M6.7.3 Logging of signalling and traffic at IWF

M6.8 Solution implementation:

- M6.8 Solve by implementation

7.3 Cross Reference Table

This clause provides a mapping of the security measures to which threats they protect against. Table 1 indicates where a countermeasure may partially or totally mitigate a threat by use of a '✓'. No assessment is made whether the set of countermeasures indicated fully or partially mitigate each threat.

Table 1: Threats and Security Measures

	M6.1.1 User interworking authorization	M6.1.2 Group interworking authorization	M6.2.1 User authentication	M6.3.1 Authentication of IWF by system	M6.3.2 Authentication of system by IWF	M6.4.1 Signalling confidentiality within MC system	M6.4.2 Signalling confidentiality within TETRA system	M6.4.3 System signalling integrity within MC system	M6.4.4 System signalling Integrity within TETRA system	M6.4.5 IWF links protection	M6.4.6 IWF protection	M6.5.1 Traffic confidentiality within MC system	M6.5.2 Traffic confidentiality within TETRA system	M6.5.3 E2EE where IWF is the endpoint	M6.5.4 E2EE through IWF	M6.6.1 TETRA AI key management	M6.6.2 MC key management	M6.6.3 E2EE key management	M6.7.1 Traffic policing and filtering on link to IWF	M6.7.2 Audit and reporting of events and exceptions on IWF	M6.7.3 Logging of signalling and traffic at IWF	M6.8 Solve by implementation
T5.2.1 System impersonation					✓																	
T5.2.2 IWF impersonation				✓																		
T5.2.3 Client impersonation			✓																			
T5.2.4 User impersonation			✓																			
T5.3.1 Eavesdropping in other system		✓				✓	✓					✓	✓	✓								
T5.3.2 Eavesdropping on external links between systems										✓				✓	✓							
T5.3.3 Eavesdropping IWF links within a system										✓					✓							
T5.3.4 Eavesdropping within IWF											✓				✓							
T5.3.5 Ambience listening invoked across IWF	✓							✓	✓										✓			
T5.4.1 Traffic analysis in other system														✓								
T5.4.2 Traffic analysis in intersystem link															✓							
T5.4.3 Traffic analysis within IWF															✓							
T5.5.1 Excessive traffic in other system																			✓	✓	✓	✓
T5.5.2 Improper use of high priority calls	✓							✓	✓										✓	✓	✓	

	M6.1.1 User interworking authorization	M6.1.2 Group interworking authorization	M6.2.1 User authentication	M6.3.1 Authentication of IWF by system	M6.3.2 Authentication of system by IWF	M6.4.1 Signalling confidentiality within MC system	M6.4.2 Signalling confidentiality within TETRA system	M6.4.3 System signalling integrity within MC system	M6.4.4 System signalling Integrity within TETRA system	M6.4.5 IWF links protection	M6.4.6 IWF protection	M6.5.1 Traffic confidentiality within MC system	M6.5.2 Traffic confidentiality within TETRA system	M6.5.3 E2EE where IWF is the endpoint	M6.5.4 E2EE through IWF	M6.6.1 TETRA AI key management	M6.6.2 MC key management	M6.6.3 E2EE key management	M6.7.1 Traffic policing and filtering on link to IWF	M6.7.2 Audit and reporting of events and exceptions on IWF	M6.7.3 Logging of signalling and traffic at IWF	M6.8 Solve by implementation
T5.5.3 DoS of IWF											✓								✓	✓	✓	✓
T5.5.4 DoS of key management						✓	✓	✓	✓			✓	✓									
T5.6.1 Traffic modification												✓	✓	✓	✓				✓	✓	✓	
T5.6.2 Signalling modification						✓	✓												✓	✓	✓	
T5.6.3 Signalling insertion						✓	✓												✓	✓	✓	
T5.6.4 Mapping modification										✓					✓			✓				
T5.6.5 Configuration modification						✓		✓														
T5.6.6 False response						✓	✓	✓	✓	✓	✓								✓	✓	✓	
T5.7.1 Keys extraction from IWF										✓												
T5.7.2 Keys extraction from TETRA terminals																	✓	✓				✓
T5.7.3 Keys extraction from high assurance MC terminals																	✓	✓				✓
T5.7.4 Key extraction from COTS MC terminals																	✓	✓				✓
T5.8.1 Traffic replay See notes 1 and 3												✓	✓								✓	✓
T5.8.2 Signalling replay See notes 2 and 3								✓	✓												✓	✓
T5.9.1 Repudiation	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓										✓	✓

NOTE 1: TETRA E2EE may provide replay protection if the Real Time Clock is enabled.
NOTE 2: Signalling replay may be partially solved by signalling protection mechanisms within MC system.
NOTE 3: TETRA Air interface encryption also provides protection against signalling received on the TETRA air interface.

8 Candidate solutions for standardization

8.1 General

This clause lists the security measures which may require additional TETRA standardization work in order to produce a satisfactory technical solution. The following measures are not listed as they can be satisfied by other means:

- Measures which can already be fulfilled by TETRA standards.
- Measures which can be fulfilled by implementations, and do not require standard changes to achieve.
- Measures which require 3GPP standardization.

8.2 Candidate measures for standardization

8.2.1 M6.1 Service authorization

Authorization for a user or group for interworking communications is a matter of system implementation and outside the scope of standards.

The mechanisms and formats for address mapping in the IWF may be candidates for standardization and allow an implementation to allow inclusion in an address book at the IWF as an authorization mechanism.

8.2.2 M6.2 User authentication

User authentication mechanisms are already specified by TETRA and 3GPP standards.

8.2.3 M6.3 Interface authentication

Authentication of the IWF is outside the scope of TETRA and 3GPP standards, and will be dependent on implementations.

8.2.4 M6.4 Signalling protection

Signalling confidentiality and integrity protection in TETRA is provided by the air interface encryption mechanism at the air interface, and is dependent on implementations within the TETRA SwMI. Security of the links to the IWF will be implementation dependent.

Signalling protection in 3GPP systems are specified by 3GPP standards.

8.2.5 M6.5 Traffic confidentiality.

Traffic confidentiality is provided by end to end encryption mechanisms specified in TETRA and 3GPP standards. Where AIE only is in use, traffic confidentiality with a TETRA system is dependent on the implementation.

8.2.6 M6.6 Key management

TETRA and 3GPP provide standardized solutions for key management within their respective systems.

If TETRA end to end encryption key management is to be extended to permit end to end communications between users in both systems, there may need to be standards describing how these mechanisms operate in a 3GPP environment. However as detailed TETRA end to end encryption is outside the scope of ETSI EN 300 392-7 [i.3] and ETSI EN 302 109 [i.4], such work would be outside the scope of TETRA standards.

8.2.7 M6.7 Policy, auditing and reporting

Policy, auditing and reporting functions are implementation dependent and outside the scope of the TETRA standards.

8.2.8 M6.8 Solution implementation

Solution implementation is inherently outside the scope of published standards.

9 Conclusions

The present document has assessed the security threats and applicable countermeasures to interworking between TETRA and 3GPP MC systems.

Of the applicable countermeasures, the mapping function between TETRA and 3GPP addressing is a candidate for standardization. The remainder are either within scope of existing standards, or need to be solved in implementation.

Implementers may wish to take note of the threats and countermeasures in designing a solution.

History

Document history		
V1.1.1	May 2018	Publication