

May 2018

TCCA White Paper

Security considerations for interconnection of TETRA and Mission Critical broadband systems

Produced by TCCA's Security and Fraud Prevention Group (SFPG)

The Grainger Suite, Dobson House, Regent Centre,
Gosforth, Newcastle NE3 3PF, UK
T +44 (0) 191 231 4328 E admin@tcca.info

TCCA Limited is a company incorporated under the Companies Act in England and Wales, company number 04155039.
Registered office: The Grainger Suite, Dobson House, Regent Centre, Gosforth, Newcastle NE3 3PF, UK

Executive Summary

Broadband wireless standards, in particular 3GPP-specified 4G (and in future 5G), are being enhanced to support mission critical (MC) speech and data communications. This creates the need for secure interworking between users on MC broadband networks and those using ETSI specified TETRA for communications. In some cases, where TETRA provides the critical speech communications, interworking will be a permanent requirement. In other cases, where there is a long-term goal to support voice as well as data communications over MC broadband systems, interworking may be needed only for an interim period. However, this interim period may still extend for many years.

Security is only as good as the 'weakest link'. Therefore, there is a need to ensure that an appropriate level of security is established on both networks and in any intermediate gateways that connect the two types of system. A detailed threat, vulnerability and risk assessment should be carried out and appropriate security policies put in place to ensure a robust solution. Careful network configuration will be required in order to obtain the most secure outcome.

Index

Executive Summary **2**

Index **3**

Introduction **4**

User Requirements **4**

Interworking scenarios **4**

Interworking implementations **5**

Transcoding mode IWF 5

Transparent mode IWF 5

Dynamic/static IWF 6

Security considerations for interworking **6**

Introduction **6**

Authenticity **7**

Confidentiality **7**

Security considerations of the IWF 7

Physical security 8

End to end key management 8

MC broadband terminals **9**

Security policy, design and analysis **10**

Conclusions **11**

Glossary **11**

References **12**

Introduction

This paper is intended as information for the critical communications community who at present use TETRA systems, but also have needs to communicate using secure PTT systems over mission critical broadband and to communicate between TETRA and these broadband systems.

This paper provides an overview of how an MC broadband PTT system can be connected to a TETRA system for interworking without compromising the security of either system. The security aspects relating to authenticity, confidentiality, integrity and availability are considered, together with issues of having an interface between two different technologies.

Interworking with legacy LMR/PMR systems is a 3GPP standardisation item and is specified in 3GPP TS 23.283 [REF 1]. This paper considers the security implications of these functions.

User Requirements

Users will expect to communicate securely whilst using the MC broadband system or using the TETRA system and when interoperating between the two systems, which are providing the following services:

- Voice calls, including individual and group call will need to be supported, together with the possibilities of broadcast call and group patching/merging/regrouping.
- SDS data will also need to be supported.

A list of interworking requirements is given in ETSI TR 102 022-2 Section 4.6 [REF 2]. ETSI TR 103 565-1[REF 3]. The study into interworking and ETSI TR 103 565-2; Security of interworking between TETRA and MC broadband applications [REF 4].

Interworking scenarios

Some important interworking scenarios are that:

- In many cases, interworking will be needed for several years while MC broadband and TETRA systems operate in parallel. A shorter period of time may be needed if user organisations intend to transition completely from TETRA to MC broadband. The security solutions will differ according to the risk appetite of the user organisations. It is possible that if interworking only takes place for a short time, more risk may be acceptable in a solution.
- In some cases, the same user may need to make use of both MC broadband PTT systems and TETRA systems at different times (e.g. dependent on location, network coverage etc). However, as there is unlikely to be true 'roaming' between the two different types of systems, it is assumed that the user will have separate subscriptions on both systems (and will choose which system to use according to user needs), and any communications will effectively be the same as other interworking cases.

Interworking implementations

Some form of gateway, known as an interworking function (IWF) will be required to manage the connection between systems. This will incorporate the management of terminal numbering schemes and audio format translation. The interconnection options considered are:

- A dynamically created patch between groups on both systems by a dispatcher where they have access to both systems.
- A static mapping between groups on one system to equivalent groups on another system.

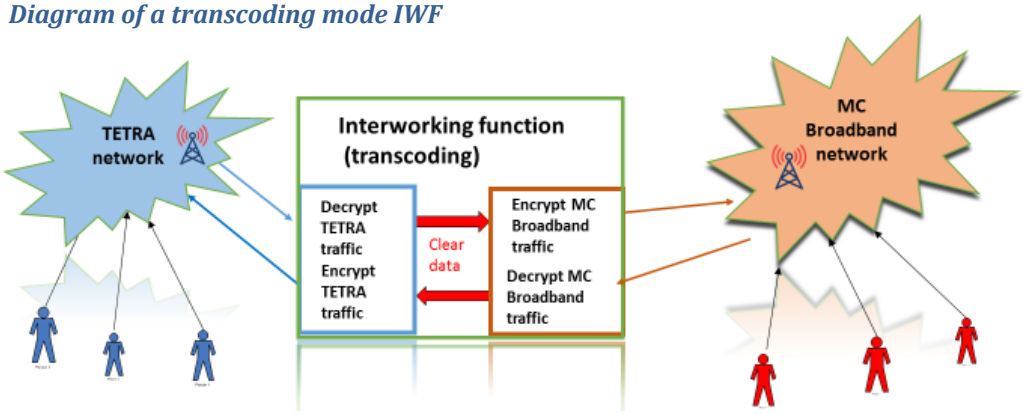
In both cases the audio could either be connected as unencoded clear audio or alternatively in a transparent mode where encrypted audio is passed unchanged between the systems.

The IWF may also support individual calls between the two systems, although it may require an address book to achieve this as it is likely that the formats of the addresses in each system will be different.

Transcoding mode IWF

A transcoding IWF decrypts the traffic from one side of the gateway and re-encrypts in the native form of the other side of the gateway.

Diagram of a transcoding mode IWF



On the TETRA side of the IWF, the audio is encoded with the TETRA ACELP codec and on the MC broadband side audio is encoded into the AMR-WB codec.

Transcoding mode has the advantage that neither side has to manage the codec and encryption mechanisms but there could be security issues because the data has to be unencrypted giving a potential security issue as eavesdropping at the point of interconnection could be a threat to confidentiality in the centre of the IWF. There may also be some performance issues due to the transcoding process.

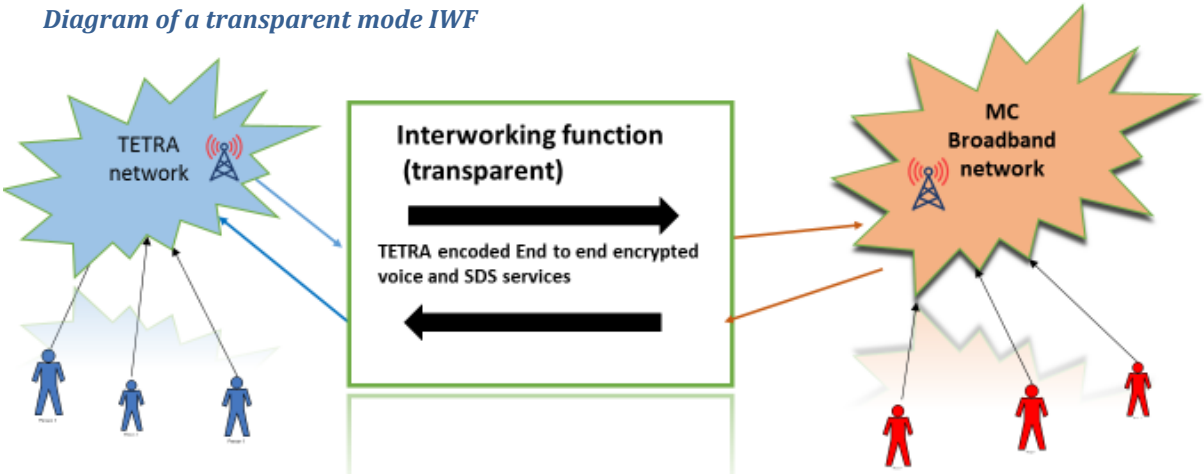
Transparent mode IWF

A transparent mode IWF carries speech and SDS data from one system unmodified to the other system.

If the speech was end to end encrypted, the encryption could therefore remain in place. This would require that terminals and dispatch positions support the same codec and encryption systems and

utilise the same encryption keys. It is unlikely that a TETRA terminal would support a codec other than ACELP. Therefore, the terminals in the MC broadband PTT system would need to support both the TETRA ACELP codec and the TETRA end to end encryption system, allowing a user organisation to distribute keys from a single key management solution.

Diagram of a transparent mode IWF



Dynamic/static IWF

An IWF can connect groups between systems either dynamically or via a static connection. These options include:

- A static interconnection implies that permanently configured specific groups are linked whenever interworking is invoked. Therefore, only intentional patching can occur but there would be a lack of flexibility.
- In a dynamic interconnection, a dispatcher may be able to select which group on one system is patched to a specific group on the other system and can dynamically change which user groups are patched together. In some case this could have security risks through inadvertent connections between groups.

Security considerations for interworking

Introduction

Communications security is much more comprehensive than just encryption of voice and data communications. It encompasses all measures to provide protection against the many different threats to a telecommunications system. These threats may be divided into those affecting confidentiality, integrity and availability.

A systems security policy should be developed at a very early stage in the introduction of an interworking programme which must take into account an analysis of threats, vulnerabilities and risk after which appropriate countermeasures should be implemented.

Below, we highlight some of the major security elements which will probably need to be considered.

It should be noted that TCCA SFPG is producing Recommendation 14, a detailed technical recommendation on security of interworking between TETRA and MC broadband systems [REF 5].

Authenticity

Ensuring the authenticity of users, terminals and infrastructure is essential in secure communications systems and this will ensure that only authorised users are able to gain access. There are major differences in how proof of authenticity is obtained in MC broadband systems and TETRA systems. The principal difference being that TETRA provides strong authentication of the terminal and network, whereas MC broadband systems focus on authentication of the user.

Therefore, security policy must ensure that there are no gaps left that would compromise security when interworking between MC broadband systems and TETRA systems.

Confidentiality

Confidentiality protection ensures that users' messages are protected against the threat of eavesdropping. However, as shown below, both systems' encryption methods are incompatible because:

- TETRA provides an air interface encryption service using session keys derived from the authentication process for individual calls and uplink transmissions from the terminals and also common and group keys for group transmissions from the infrastructure to the terminals. An end to end encrypted service may also be provided as described in [REF 6].
- MC broadband systems offer air interface encryption as well as identity-based end to end encryption for key management which provides a session key for individual calls and shared key for group calls.

To overcome this incompatibility and maintain confidentiality, the IWF must either provide encryption translation (transcoding) or provide a transparent connection, which in practice would require the MC terminals to support TETRA end to end encryption.

Security considerations of the IWF

There will be a choice between IWFs that decrypt and re-encrypt messages through them (transcoding) or those that allow encrypted transmissions through unchanged (transparent). Some considerations for IWF design are listed below:

- A dispatcher may be able to listen to and take part in all calls, including those that are intended to be protected by end to end encryption.
- The dynamic patching of groups may be problematic when using a transcoding IWF if an incorrect patch could result in information being passed to the wrong target user group. This in turn could have consequences for confidentiality of information as well as the loss of communications in the correct groups.
- On the other hand, dynamic patching gives increased flexibility by allowing communications groups to be patched together dynamically, according to the user need at the time.
- A transparent connection of end to end encrypted communications provides protection against accidental incorrect patching by a dispatcher, as long as talkgroups are separated by using different encryption keys.
- An interconnection between TETRA and MC broadband systems should only be in place for the time it is required.

Physical Security

Access to a dispatcher position that could control an IWF may give an adversary the opportunity to incorrectly patch groups between systems. The sensitivity of group communications in both systems (which may differ) should be taken into account when formulating security policy in respect of access controls.

The IWF must be considered a sensitive point in the interconnection system and along with its links to both systems will need to be protected to avoid compromise.

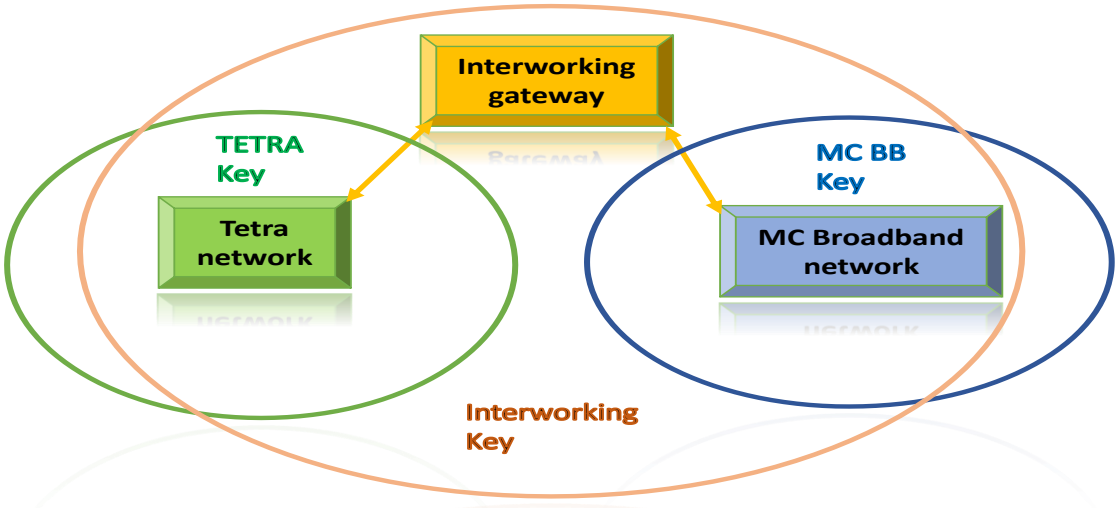
If an address book is used to achieve address translation between the systems it needs to be implemented in a secure manner to avoid exposure of the user identities.

Users may not be aware that an interconnection is in place and this may determine the sensitivity of communications that can be exchanged. A robust warning system could be put in place.

End to end key management

Considerations for end to end key management are different depending on whether a transparent or transcoding IWF is employed:

- If a transcoding mode interconnection is used, key management can take place independently on each system. The IWF must be configured with any necessary identities to be a recipient of key management messages.
- On either system, the security manager must recognise that communications are passing through a clear interconnection system and are protected differently on the target system. The manager may consider that keys within the interconnection mechanism could have different vulnerabilities to those in terminals within either system. Because of this, it may be advisable that encryption keys used for interconnection to the other system are different from keys that are used solely within one system such that a compromise of the interconnection system does not compromise other communications.
- When using a transparent interconnection, the approach of using separate keys may also be considered. Networks may be connected some of the time and operate separately at other times. This is shown in the diagram and entails using different keys when an interconnection between two groups is in place.



The physical means of implementing encryption on a terminal is one of the factors in the security of the overall system. A terminal on one system using a hardware security module for encryption and key storage may be considered to be reasonably protected against a technical attack, for example one intended to recover the encryption keys. However, if the interconnected system uses a different approach in its terminals, for example a software application without specific hardware storage, the keys may be more vulnerable to extraction. Thus, the security manager would again be advised to use different keys for interconnected use from those only used within one system, in case of compromise of terminals on the other system.

MC Broadband Terminals

The following points need to be taken into consideration regarding MC broadband terminals:

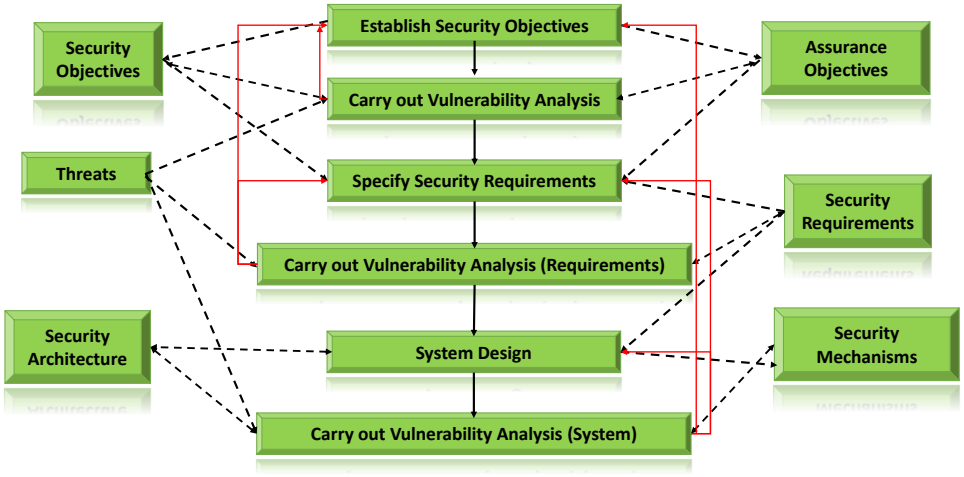
- If fully transparent end-to-end encryption is to be employed, it will be necessary for the MC broadband terminal to be capable of supporting the TETRA ACELP codec, the TETRA encryption and the key management mechanisms defined in SFPG Recommendation 02 [REF 6].
- Unlike TETRA terminals which tend to have a closed architecture, it is likely that MC broadband will be implemented on generic terminals with a generic operating system. This implies that the systems security manager will need to take care that only trusted applications have been installed on the terminal and that the terminal's authentication to the correct MC broadband network cannot be subverted. It will be important that unused services are disabled and locked down and that the user should be prevented from enabling functionality not required operationally.
- Key storage and encryption processes on a generic broadband terminal present a security risk because it is unlikely that protection given by dedicated encryption hardware and secure key storage will be present.
- The security limitations of MC broadband terminals may determine the limit of the maximum classification of information that can be carried by the service.

Security policy, design and analysis

Whatever form the interworking function takes, it will join together elements of two secure systems employing different technologies with resulting complex security requirements. It is recommended that a security policy defining the interworking system and its connectivity is developed at an early stage.

Compliance to an international security standard should be considered. Two examples of standards are shown below. These give methodologies for setting security objectives, carrying out vulnerability analysis.

There is an ETSI technical specification (TS 102 165-1) Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA) [REF 7]. The specification lays out formal methodologies for developing security policies and designing systems incorporating the appropriate countermeasures. The diagram below shows the process.



Another very useful reference is ISO 27001; a specification for an information security management system (ISMS) [REF 8]. An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

Conclusions

Secure interoperability between TETRA and MC broadband PTT systems is possible. User organisations need to be aware of the differences in mechanisms between the two types of system so that these can be taken into account together with their own security needs in designing an actual solution.

A comprehensive risk assessment should be undertaken, which must consider:

- The solution adopted and the length of time over which this solution will be in use.
- The location, ownership, design and installation of the interconnection gateway.
- The implementations of security mechanisms on TETRA and the MC broadband network and terminals must also be reviewed, and the key management policy should include any restrictions needed when sharing keys between users across both systems.

The security classification of user speech and data should drive the decision on whether to use a transcoding IWF or whether to implement a transparent fully end to end encrypted solution, which requires the TETRA codec and encryption system to be installed on the MC broadband terminal.

Above all, the system operating procedures need to take these factors into account and ensure that legitimate use of the terminals on both systems and the classification of information that can be exchanged are well known to users.

Glossary

4G	4th Generation public mobile radio technology
5G	5th Generation public mobile radio technology
3GPP	3rd Generation Partnership Project – a collaboration of Standards Development Organisations which is responsible for the specification of 3G, 4G and 5G public mobile communications technologies.
AMR-WB	Adaptive Multi-Rate Wideband` Codec, used for 4G systems speech encoding
ACELP	Arithmetic Code Excited Linear Prediction – the type of speech codec used in TETRA
Codec	Coder/Decoder used to encode and decode speech and video
ETSI	European Telecommunications Standards Institute – responsible for the TETRA standard
ISMS	Information Security Management System
ISO	International Organization for Standardization
IWF	Interworking Function
MC	Mission Critical – applied to broadband systems
PTT	Push to Talk – structured communication between individuals and within groups where one party transmits at a time
PMR	Professional or Private mobile radio systems; known as LMR (Land Mobile radio) in US
SDS	TETRA Short Data Service
SFPG	Security and Fraud Prevention Group - a TCCA Working Group
TCCA	The Critical Communications Association (TCCA) - see www.tcca.info
TETRA	Terrestrial Trunked Radio - a digital trunked mobile radio technology
Transcoding	The process of data being decoded at the gateway and re-encoded in the other systems format. Maybe a security and performance consideration
Transparent gateway	In this context, a gateway that passes data without any intermediate transcoding

TVRA	Threat, Vulnerability and Risk Analysis

References

REF No.	Number	Title
1	3GPP TS 23.283	Mission Critical Communication interworking between Land Mobile Radio Systems
2	ETSI TR 102 022-2	User Requirements Specification; Mission Critical Broadband Communications; Part 2: Critical Communications Application
3	TR 103 565-1	Study into interworking between TETRA and 3GPP mission critical services; Part 1: General considerations for interworking.
4	TR 103 565-2	Study into interworking between TETRA and 3GPP mission critical services; Part 2: Security of interworking between TETRA and Broadband applications.
5	TCCA SFPG Recommendation 14	Security of interworking between TETRA and 3GPP MC systems. *Note 1*
6	TCCA SFPG Recommendation 02	TETRA End to End encryption. *Note 2*
7	ETSI TS 102 165-1	CYBER; Method and protocols; Part 1: method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)
8	ISO 27001-web page	Information technology Security technique: Information Security Management Systems Requirements

Note 1: Not yet available, in draft at time of writing and will be available as per note 2.

Note 2: This is a controlled document available to TCCA members on request from TETRA SFPG Secretariat; Marjan Bolle; email: SFPG@TCCA.info