

TETRA Security

1 The TETRA security functions

TETRA contains a wealth of security functions designed to protect users' information. This information can consist of the users' speech and data traffic and also other information that relates to the identities and operations of the users themselves. When describing these TETRA security functions it is important to make a distinction between the different categories of functions and their specific application. In TETRA the following categories can be identified.

1.1 Security mechanisms

These are independent self-contained functions that aim to achieve a specific security objective such as confidentiality of information or authentication of mobile terminals. Security mechanisms are the main building blocks for a security system.

1.2 Security management features

These are functions that are used to control, manage and operate the individual security mechanisms. They form the heart of the resulting security and should guarantee that the security features are integrated into a consistent security system. Furthermore they are used to realise interoperability of the security mechanisms over different networks. Key management is the most essential security management function.

1.3 Standard cryptographic algorithms

These are standardised system specific mathematical functions that are used, normally in combination with parameters called "cryptographic keys", to provide an adequate security level for the security mechanisms and the security management features. Standardised cryptographic algorithms are offered in TETRA to support interoperability between different TETRA systems.

1.4 Lawful interception mechanisms

These are functions that are used within some communication systems to provide the lawfully required access to information and communication, with the aim to fulfil national regulatory requirements. It is essential that such functions do not undermine the regular security of the system. Therefore these functions should be controlled through security management features.

1.5 Note on evaluating security mechanisms

It is very important to be aware of the different roles and objectives of these classes. In certain proprietary systems the first two classes are often confused. This results in a "knot" of security features, which is difficult to analyse and even harder to correctly implement and control in an operational environment. But also mechanisms and algorithms get confused. Sometimes one tends to assess security provided by a certain mechanism only by the strength of the algorithm used, ignoring the environment in which it is used.

2 Mutual authentication over the air interface

The TETRA standard supports the mutual authentication of a Mobile Station (MS) and the network, which is in TETRA normally referred to as the Switching and Management Infrastructure (SwMI). This makes it possible for a TETRA system to control the access to it and for an MS to check if a network can be trusted.

In TETRA, as in most other secure systems, the authentication process provides a firm basis for the overall security. It can be used for the following purposes:

- To ensure correct billing in Public Access systems;
- To control the access of the MS to the network and its services;
- To derive a unique session encryption key, the Derived Cipher Key (DCK) which is linked to the authentication, and which is then used to provide confidentiality of information transfer;
- To create a secure distribution channel for sensitive information such as other encryption keys;
- To control the disabling and enabling of an MS/SIM in a secure way; and
- To ensure that TETRA MSs are connected to a legitimate TETRA system.

This mutual authentication security mechanism is available for Voice and Data. In Direct Mode Operation (DMO) an explicit authentication mechanism is not available (MSs do not share their authentication keys with each other); in this case the use of Static Cipher Keys (SCKs) can however provide implicit mutual authentication.

There is a single standardised authentication algorithm set.

Mutual authentication is done on the basis of an authentication key K, which is unique for every MS or SIM if the latter is used. The K is both stored in the MS/SIM and in the network. Normally a specific network element is used to store the Authentication keys. This is called the Authentication Centre (AUC).

3 Encryption

The air interface is very vulnerable to eavesdropping and so modern mobile wireless communication systems need to have some form of air interface security. This air interface security is intended to secure the connection between MSs and the network. Air interface security is an effective means to provide security in a mobile network and some essential security functions can only be realised by air interface security. In most cases it is sufficient to rely on air interface security and take no further security measures. However, in TETRA systems needing a very high level of security, additional security may be required to protect information transmitted from one MS to another not only over the air interface but also within the network. In this case end-to-end security provides an efficient solution.

3.1 Air interface encryption

User traffic and signalling information can be encrypted over the air interface between the MS and the SwMI, both for individual and group communications. The Air interface encryption mechanism is available for Voice and Data in Trunked Mode Operation and in Direct Mode Operation. The use of several encryption algorithms, both standard and proprietary, is supported.

Traffic encryption protects user speech and data. Signalling encryption provides protection from traffic analysis, and prevents an eavesdropper from discovering who is operating in a particular area, or who is calling who.

3.2 End-to-end encryption

The TETRA end-to-end service can be realised in any number of ways. This means that a user may easily tailor an end-to-end encryption system to their particular requirements. This flexibility is essential for a standard like TETRA that will be implemented in many forms for different user groups.

Public Safety organisations will have specific (high) national security requirements for their implementation of end-to-end encryption, which will be different from the requirements of Military user groups, which have even greater security requirements. All such organisations need to be able to specify an end-to-end encryption system according to their own requirements. It can also be expected that commercial user groups will have a need for secure end-to-end encryption systems.

3.3 The TETRA Association End-to-End Encryption framework

Whereas the TETRA standard leaves the implementation of End to End encryption relatively open, it is important to realise that there are benefits in having standardised solutions. A standardised solution means that end users, even those who have particular requirements over the cryptography used, do not need to specify the rest of the end-to-end system (including the Key Management). This has led to the production of TETRA Association Security and Fraud Prevention Group (SFPG) Recommendation 02. This Recommendation fully specifies all that is required for an end-to-end service other than the detail of the cryptographic algorithms. These are treated as black-box functions.

In order to provide a complete solution for the general user, the Recommendation concludes with Appendices showing how these cryptographic functions can be realised by using sample implementations of publicly available algorithms. The first sample implementation used the International Data Encryption Algorithm (IDEA), which was a very well respected algorithm at the time, and an agreement was set up to allow reasonable use of the IPR. However more recently due to TETRA market demand a second sample implementation has been made using the Advanced Encryption Standard (AES), which is becoming widely adopted by many government users in Europe and elsewhere. AES has the advantages of being a newer design and of being IPR free.

Although these algorithms are described as sample solutions, in practice the choice of well respected public domain algorithms that have stood the test of publicly available cryptanalysis means that these solutions are completely acceptable for the majority of potential users of TETRA End to End encryption. The advantage of their adoption is the availability of MSs and key management solutions from multiple manufacturers.

The framework has been designed to be adaptable to a range of Security Policies, with the flexibility being achieved through a number of simple operational choices.

Copies of TETRA Association SFPG Recommendations may be obtained from the SFPG Secretariat.

3.4 Anonymity

The TETRA standard incorporates a mechanism for encrypting users' individual and group identities before transmitting these across the air interface. It is possible to make this encryption dynamic in the sense that an identity is encrypted in a different way on different occasions. This provides anonymity for the end users, and protection from traffic analysis. Again, this mechanism is available for Voice and Data in Trunked Mode Operation and in Direct Mode Operation.

3.5 Secure enabling and disabling of terminals

TETRA supports different options for a direct secure disabling or enabling of either:

- the MS equipment, based on the Terminal Equipment Identity (TEI);
- the MS subscription, based on the Individual TETRA Subscriber Identity (ITSI); or
- both the MS equipment and the MS subscription.

The purpose of providing separate mechanisms for equipment and subscription allows a practical means of disabling an MS even if the implementation places the ITSI on a separate SIM card, which is inserted into a Mobile Equipment to make a complete MS. The mechanisms allow the system operator to choose either the ITSI or the equipment, or both together.

If the TEI is disabled the MS's equipment cannot be used any more, even if another ITSI is inserted into the MS. If the ITSI is disabled an MS's equipment can still be used in combination with another (enabled) ITSI, whereas the ITSI cannot be used in any MS anymore. In addition the disabling can be either temporary (which leaves the possibility to enable again over the air) or permanent (which is irreversible).

In systems demanding a high security, disabling and enabling should only take place after mutual authentication has been performed. If this is not the case the feature (especially disabling) can obviously be used to attack the system.

4 Security management features

The mere fact that security functions are integrated in a system does not automatically imply that a system is fully secure. However, what is normally achieved is that the security risks are “condensed”, that is they are concentrated to specific elements in the system, which can be adequately controlled.

This control is one of the tasks of the security management. Another task of security management is to guarantee that the security mechanisms are used in the proper way and that the different mechanisms are integrated in an appropriate way to achieve an overall secure system. Security management is also responsible for realising the secure interoperability between different (TETRA) systems.

The form into which the security is condensed is normally that of “keys”. A key is a piece of secret information that is used, often in combination with cryptographic algorithms, to provide the actual security for a security mechanism. Often the keys form the interface between security management and the security features. Security management is responsible for dealing with the keys in a secure way. Though security management is partly an issue for the implementation, in communication systems like TETRA it is possible to specify certain management features, which support the security management. In addition the TETRA Association SFPG has produced Recommendations intended to support the management of security (especially key management).

Adequate security management is just as important as the actual security mechanisms. In TETRA key management, functionality and flexibility are key words. A large number of features have been integrated to support the key management.

4.1 Authentication Key

The authentication key K is used for mutual authentication between an MS and the SwMI. The TETRA standard describes three possible methods for generating this key, which can be a function of a fixed User Authentication Key, an Authentication Code entered by the user, or a combination of the two. Most systems require the MS to store the UAK or K itself rather than making use of user input due to the management issues associated with remembering long codes.

4.2 Keys for air interface encryption

There are several sorts of encryption keys. Some keys may be derived or transferred as part of the authentication procedure, some keys can be sent to MSs using Over The Air Re-keying (OTAR) or some may be preloaded in the MSs. There are keys with long term and short term key lifetimes. Special mechanisms are included to protect the keys with a long lifetime.

- The **Derived Cipher Key (DCK)** is derived during the authentication procedure. It can be used to encrypt the link between the network and the MS on an individual basis. Thus it can also provide an extended implicit authentication during the call,

and can be used for encryption of uplink communications (i.e. the communication from the MS to the network) as well as downlink communications from network to an individual MS.

- The **Common Cipher Key (CCK)** is generated by the SwMI and distributed, encrypted with the DCK, to each MS. It is efficient to use this key for encryption of messages that are directed to groups of MSs spread across one or more Location Areas (LAs). When the CCK is distributed to an MS over the air interface using OTAR it is encrypted with the DCK of this MS.

- The **Group Cipher Key (GCK)** is linked to a specific closed user group. It is generated by the SwMI and distributed to the MSs of a group (e.g. by pre-provisioning of the MS, on a Smart card, or by using OTAR (see below)). Within a Location Area the GCK is always used in a modified form. It is combined with the CCK in a specific algorithm to obtain the Modified Group Cipher Key (MGCK). The MGCK is used to encrypt the closed user group messages for groups of MSs. When the GCK is distributed to an MS over the air interface using OTAR it is encrypted with a session encryption key derived from the Authentication Key for this MS, or with a Group Session Key.

- The **Static Cipher Key (SCK)**, finally, is a predetermined key, which can be used without prior authentication. It is "static" in the sense that it is a fixed key that is not changed by another security function (e.g. by an authentication exchange) until it is replaced. TETRA supports the use of up to thirty-two (32) SCKs in an MS, per network. They can be distributed similarly to the GCKs. Their use is largely implementation dependent but they can be used for encryption in Direct Mode Operation (where they may also provide explicit authentication) and in certain TETRA systems also for encryption for group and individual communications. The SCK may also be used in a system that normally uses DCKs and CCKs as an alternative to those keys in fallback conditions. When an SCK is distributed to an MS over the air interface using OTAR it is encrypted with a session encryption key derived from the Authentication Key for this MS.

When used in DMO, SCKs may be grouped in a way that allows several SCKs to be associated with the same talkgroup(s). This allows an MS to have a current SCK defined for transmission, but to allow reception on one of the others. This allows a practical key management mechanism to be constructed, where one MS may be commanded to start using a new SCK for transmission before the changeover message has reached another MS.

5 Over The Air Re-keying (OTAR)

As indicated above there is a possibility to distribute or update CCKs, GCKs and SCKs using a Over The Air Re-keying (OTAR) mechanism. This mechanism makes it possible to send air interface encryption keys in a secure way from the SwMI over the air directly to an MS and can be applied provided that an authentication key K is available for the MS. The OTAR messages for an individual MS are encrypted using session encryption keys that are derived from the authentication key for that MS. Alternatively, a Group Session Key for OTAR may be used to distribute keys to groups of MSs at the same time.

A similar OTAR mechanism is also available for the management of end-to-end encryption keys. This is usually referred to as Over The Air Keying (OTAK) to distinguish it from the air interface service.

6 Transfer of authentication information between networks

If a TETRA MS roams to a TETRA network other than its “home” network, this “visited” TETRA network will need to obtain authentication information from the “home” network of this MS in order to be able to perform mutual authentication and generate and/or distribute encryption keys. The transfer of authentication information between networks is in principle supported in three ways. The most straightforward method is to simply transfer the authentication key K to the visited network. For security reasons this is however not advisable. A second option is to transfer certain information that can be used for one single authentication procedure. This is basically the same method as is applied in GSM and can be implemented in a very secure way. However this is only practical where the MS cannot mutually authenticate the SwMI – otherwise the visited SwMI would have to interrogate the home SwMI for a response each time the MS invoked this mutual authentication. A third alternative is therefore supported. This allows a home network to transfer a set of session authentication keys for an MS, which can be used for repeated authentications, to a visited network without revealing the original authentication key of the MS. This option combines security and efficiency and permits mutual authentication to take place at a realistic pace.

7 The standard TETRA cryptographic algorithms

The TETRA standard offers a number of standard cryptographic algorithms which all have their own specific purpose. This section explains this purpose and the use of these standard algorithms.

7.1 Air interface encryption algorithms

A number of air interface encryption algorithms have been specified as part of the TETRA standard, which allows easy interoperability in multi vendor systems. Alternative algorithms can also be supported provided that they can meet the requirements imposed by the coupling to the TETRA protocols, and provided that the user accepts the potential loss of multi vendor supply. Several requirements have been taken into account when specifying the standard algorithms. The most important of these are the need for diversity and export control regulations.

7.2 Need for diversity

It has already been explained that there will be a wide range of TETRA networks and applications. Not all users want to 'share' their standard encryption algorithms with all other TETRA users. For example, the European Public Safety Organisations (associated with the European Schengen organisation) require their own standard air interface encryption algorithm.

7.3 Export control regulation

Equipment that includes encryption algorithms is likely to be subject to specific export controls in addition to any other functional controls. The encryption related controls are slowly being relaxed. Such controls are country specific, but 33 major industrial countries derive their national controls from a commonly agreed policy. This policy is published under the banner of the Wassenaar Arrangement (see <http://www.wassenaar.org>). Controls on cryptography fall under Category 5 part 2. Four standard encryption algorithms are currently available for use in TETRA systems. These have been developed by ETSI's Security Algorithm Group of Experts (SAGE) to satisfy two different criteria. These are explained below.

7.4 TEA2 and TEA3: Restricted Export Algorithms

These algorithms are controlled items under the 1998 Wassenaar Arrangement rules. The algorithms have been primarily designed for use by Public Safety Organisations. The former algorithm (TEA2) has been assigned for use by Public Safety Organisations in Schengen and related countries.

7.5 TEA1 and TEA4: More Readily Exportable Algorithms

TEA1 (as the numbering implies) was the first algorithm available. TEA4 reflects the more relaxed controls of the 1998 Wassenaar Arrangement.

The standard TETRA Encryption Algorithms are available to TETRA users and manufacturers. They are distributed by a custodian. In case of the TEA1, TEA3 and TEA4 the custodian is ETSI (see <http://www.etsi.org>, section algorithms and codes). TEA2 is distributed by the Dutch Police IT organisation.

Export control regulations also have implications for MSs that are fitted with End to End encryption, or that are capable of End to End encryption even if that encryption process is not provided. For example, any MS incorporating a smart card interface that is capable of end-to-end encryption is considered subject to export control even if the radio does not have a smart card inserted. Such detailed specification of the smart card to radio interface is potentially considered subject to export control under the Wassenaar Arrangement. The TETRA Association therefore encourages manufacturers to consult their national export control authorities in advance and apply for export licences as appropriate.

8 Air interface authentication and key management algorithms

There is also a set of standard air interface authentication and key management algorithms, designed to allow easy interoperability in multi-vendor systems, which have been specified as part of the TETRA standard.

The requirements on diversity and export control regulations do not exist in the case of authentication and key management algorithms. Therefore, only a single set of standard air interface authentication and key management algorithms has been specified. This algorithm set is called the TAA1. Its specification is distributed by its custodian, which is also ETSI.

9 End-to-end encryption algorithms

SFPG Recommendation 02, which describes a standard End to End encryption implementation is written around four black-box cryptographic functions designated E1 to E4. Those users with the necessary expertise may define how these are realised using algorithm(s) of their own choice. The only constraint is that the algorithm(s) have to fit within the broad parameters of functions E1 to E4.

For those users who are content to follow a public standard, the recommendation includes Appendices which shows how these cryptographic functions can be realised using the IDEA or AES algorithm. So, the body of the recommendation together with the appendix forms the complete specification for a standard TETRA end-to-end encrypted voice service. The IPR for IDEA is owned by MediaCrypt AG, who should be approached for licensing information. AES has the advantages of being a newer design and of being IPR free and is becoming widely adopted by many government users in Europe and elsewhere.

10 Lawful interception mechanisms

In most European countries there is an obligation on operators of public (and sometimes private) telecommunication networks to provide lawful interception facilities to the responsible national authorities. Since a standardised solution is much more cost efficient than proprietary implementations on a case by case basis, it was decided to provide support for lawful interception within the TETRA standard. A subgroup of the TETRA security group has specified the requirements for a Lawful Interception Interface to support the mechanisms for lawful interception. The detailed implementation of this interface might differ on a country to country basis.