TETRA Security – An overview

1. Introduction and Background

During the last decade several standards for Mobile telecommunications have been developed. The best known is without any doubt the Global Standard for Mobile Communications (GSM) which is operational in many countries, both within and outside Europe. It is now the most successful standard for mobile communications. Also the Digital Enhanced Cordless Telecommunications (DECT) was successfully implemented in different environments for cordless telephony (Home, PABX).
A standard that has just left the standardisation phase and is now entering the implementation phase is the Terrestrial Trunked Radio (TETRA) standard. It is typically designed for the Professional Mobile Radio market and includes Private Mobile Radio (PMR) systems, typically for Military and Public Safety organisations, as well as Public Access Mobile Radio Systems for public services.
Finally, in 1999, the 3rd Generation Partnership Projects (3GPP) started the drafting of the Universal Mobile Telecommunication System (UMTS).

In all of these systems security has proved to be an essential aspect. This is exemplified in GSM where the inclusion of authentication of the mobile terminal by the network stopped the massive fraud that was occurring in the previous generation of analogue mobile systems. GSM also provided a very reasonable confidentiality over the radio path using an encryption that even today can not easily be broken in practice.
The DECT security was based upon the GSM security and added things to this like an enhanced key management support and also the possibility of the mobile terminal to authenticate the network. In its turn TETRA has built on the DECT security and added features which are relevant for Professional Mobile Radio users, such as end-to-end encryption, encryption for closed user groups and secure enabling and disabling of mobile terminals.
The security of UMTS is now getting its form. It is clear that it builds upon the security of the existing standards, but that it will also add further security functions.

Though there is a difference in the specific security in all these standards, they have common properties that make them superior compared to most non-standardised proprietary products. The security of the standards was specified by an open expert group using an open and structured approach and basing its work on well-established methods. The security specifications of all the systems, with the exception of the cryptographic algorithms used[1], are published and thus open to public scrutiny.

In this paper we will focus on TETRA security and describe in detail the TETRA security functions.

[1] A detailed description on standardised Cryptographic algorithms in Telecommunications Systems and issues relating to this can be found in [8]

This paper is largely based on a document [1] that was published before.

2. The TETRA security functions

When describing the 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.

- ***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.
- ***Security management features***. These are functions that are used to control, manage and operate the individual security mechanisms. They form the heart of the 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.
- ***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.
- ***Lawful interception mechanisms***. These are functions that are used within 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 the security management.

Figure 1 depicts the basic relations between the different security functions.

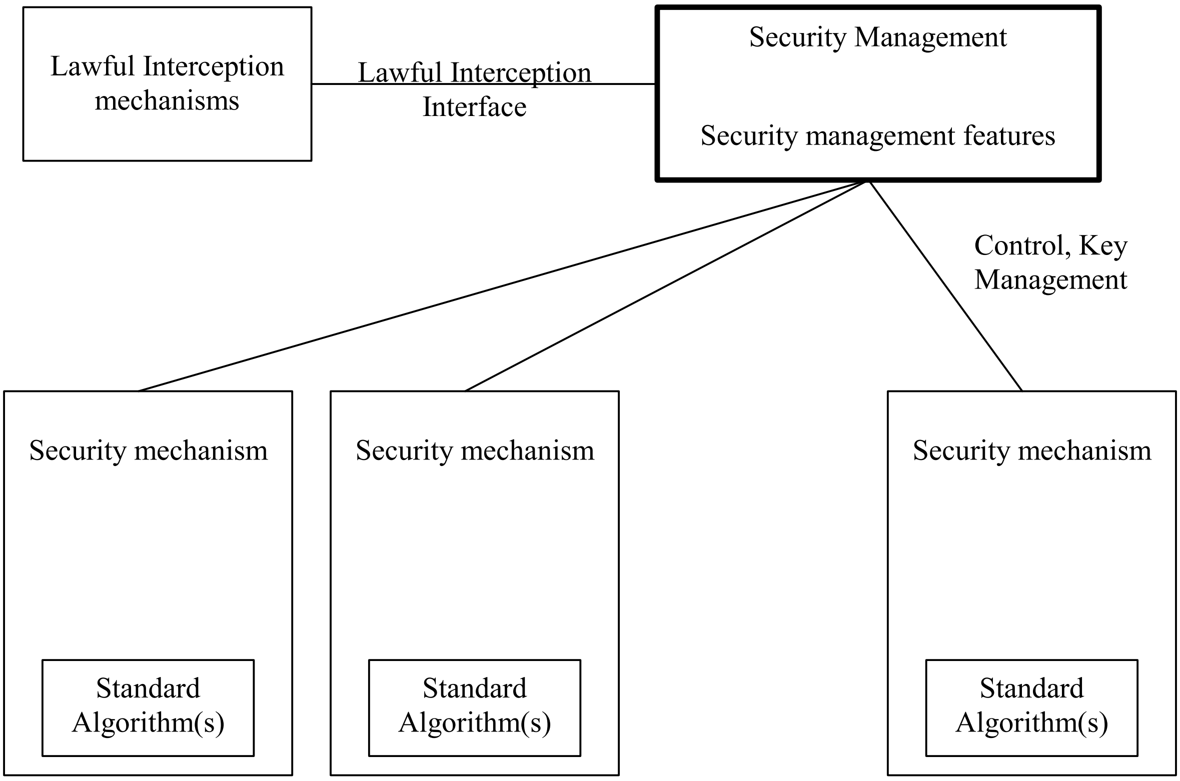


Figure 1 – Relations between security

It is very important to be aware of the different roles and objectives of these classes. In certain proprietary systems especially 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. (This has occurred for the GSM encryption and the A5/1 encryption algorithm).

2.1 Security mechanisms

The security mechanisms integrated in the TETRA standard are described in this section. A full description can be found in the formal ETSI standards [2] and [3] that can be obtained via http://www.etsi.org .

2.1.1 Mutual authentication over the air interface

The TETRA standard supports the mutual authentication of a Mobile Station (MS) on the one hand and the network, which is in TETRA normally referred to as the Switching and Management Infrastructure (SwMI), on the other. 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 is a firm basis for the overall security. It can be used for the following purposes.

1. Ensure a correct billing in public assess systems;
2. Control the access of the MS to the network and its services;
3. Derive a unique session encryption key, the Derived Cipher Key (DCK)[2] which is linked to the authentication, and establish other security parameters
4. Create a secure distribution channel for sensitive information such as other encryption keys;
5. Control the disabling and enabling of an MS/SIM[3] is a secure way; and
6. Ensure that TETRA MS's are connected to the legitimate TETRA system.

The mutual authentication security mechanism is available for Voice and Data and Packet Data Optimised mode. In Direct Mode Operation (DMO)[4] an explicit authentication mechanism is not available; in this case the use of Static Cipher Keys (SCK)[5] can however provide implicit mutual authentication.

The use of several authentication algorithms, both standard and proprietary, is supported (see section 2.3.2).

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).

Mutual authentication using an Authentication Centre is illustrated in the figure below.

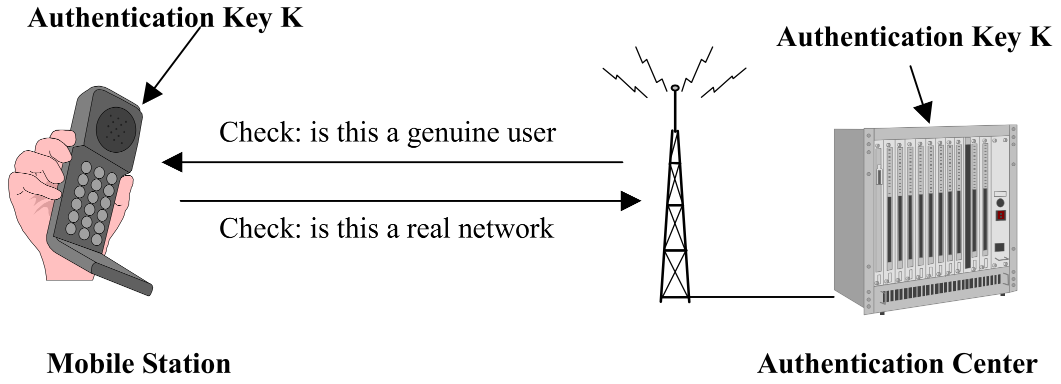


Figure 2 – Mutual authentication

[2] The Derived Cipher Key (DCK) is a unique encryption key used to encrypt information which is exchanged on the link between the network and the MS, see also section 2.2.2.

[3] The Subscriber Identity Module (SIM) is a piece of hardware (often a Smart Card) that contains the essential subscriber information including the authentication key and that can be placed in an MS to "personalise" it.

[4] Direct Mode Operation (DMO) is the direct communication between Mobile Stations without the use of a network

[5] The Static Cipher Key (SCK) is a fixed pre-stored encryption key used to encrypt information which is exchanged on the link between the network and the MS/SIM, see also section 2.2.2.

2.1.2 Encryption

As the air interface is very vulnerable to eavesdropping modern mobile and wireless communications systems all have some form of air interface security. This air interface security is intended to secure the connection between MS's 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.

The difference between the scope of air interface security and end-to-end security is illustrated in figure 3 below

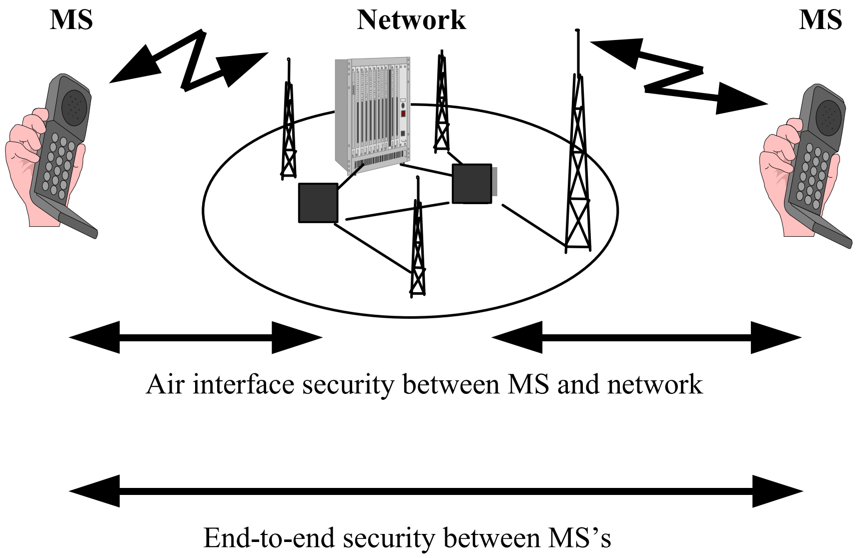

MS
Network
MS
Air interface security between MS and network
End-to-end security between MS's

Figure 3 – Air interface security versus end–to-end security

2.1.2.1 Air interface encryption

Using a variety of keys (see section 2.2.2), user 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 and Direct Mode Operation. The use of several encryption algorithms, both standard and proprietary, is supported (see section 2.3.1).

2.1.2.2 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 his own 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.

The TETRA MoU End-to-End Encryption framework

Recognition of the fact that many users, whilst having particular requirements over the cryptography used, may have no wish to specify the rest of the end-to-end system (including the Key Management) has led to the production of TETRA MoU SFPG recommendation 2 [5]. 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. However, in order to provide a complete solution for the general user, the Recommendation concludes with an appendix showing how these cryptographic functions can be realised using the well known IDEA algorithm.

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 MoU SFPG Recommendations may be obtained from the SFPG Secretariat (Mrs. Marjan Bolle - m.bolle@kpn.com).

2.1.3 Anonymity

Anonymity can be achieved by the SwIM assigning temporary individual or group identities and then encrypting these identities over 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. Again, this mechanism is available for Voice and Data and Direct Mode Operation.

2.1.4 Secure enabling and disabling of terminals

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

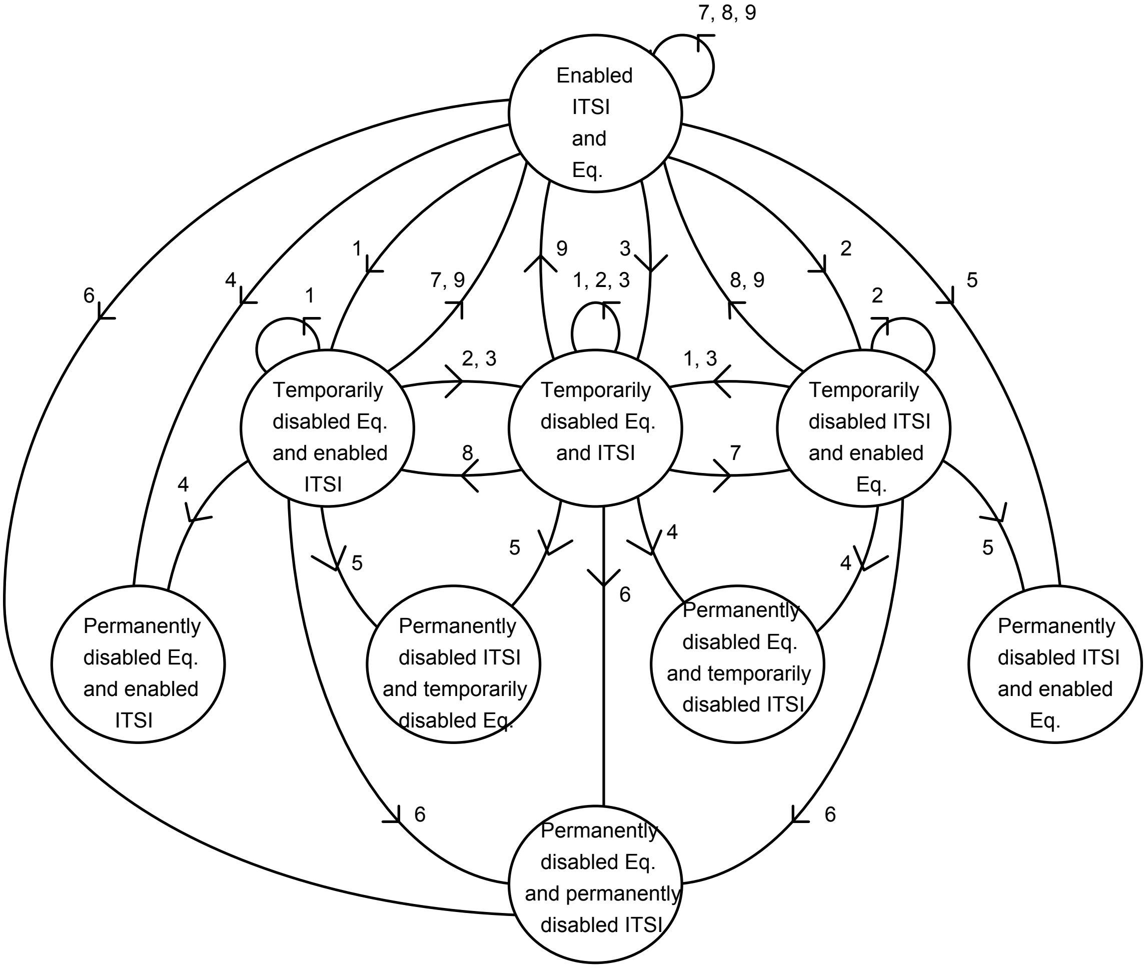
- the MS equipment, based on the Terminal Equipment Identity (TEI);
- the MS subscription, based on the Individual TETRA Subscriber Identity (ITSI); or
- both the MS equipment and the MS subscription.

If the TEI is disabled the MS can not be used anymore, even if another ITSI (which can be stored in a detachable module such as a SIM) is inserted in the MS. If the ITSI is disabled an MS can still be used in combination with another (enabled) ITSI. The ITSI can not be used in any MS anymore.

In addition the disabling can be either temporary (which leaves the possibility to enable again) or permanent (which is irreversible). This results in the following nine states:

TEI	ITSI
Enabled	Enabled
Enabled	Temp disabled
Enabled	Perm disabled
Temp disabled	Enabled
Temp disabled	Temp disabled
Temp disabled	Perm disabled
Perm disabled	Enabled
Perm disabled	Temp disabled
Perm disabled	Perm disabled

The state diagram below, copied from the TETRA security standard [2], describes functions and states.


7, 8, 9
Enabled ITSI and Eq.
1
9
3
2
6
4
1
7, 9
1, 2, 3
8, 9
2
5
2, 3
1, 3
Temporarily disabled Eq. and enabled ITSI
Temporarily disabled Eq. and ITSI
Temporarily disabled ITSI and enabled Eq.
8
7
4
5
5
4
4
5
6
Permanently disabled Eq. and enabled ITSI
Permanently disabled ITSI and temporarily disabled Eq.
Permanently disabled Eq. and temporarily disabled ITSI
Permanently disabled ITSI and enabled Eq.
6
6
Permanently disabled Eq. and permanently disabled ITSI

KEY:

1) temporary disabling of equipment;
2) temporary disabling of ITSI;
3) temporary disabling of equipment and ITSI;
4) permanent disabling of equipment;
5) permanent disabling of ITSI;
6) permanent disabling of equipment and ITSI;
7) enabling of equipment;
8) enabling of ITSI;
9) enabling of equipment and ITSI.

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 the disabling) can obviously be used to attack the system. The TETRA standard leaves open the possibility to disable and enable without mutual authentication first taking place, but in practice this will only be done in systems with a low security level.

2.2 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 so to say “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 the 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. The security management is also responsible for realising the secure interoperability between different (TETRA) systems.

The form in 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 to a security mechanism. Often the keys form the interface between the security management and the security features. The security management is responsible for dealing with the keys in a secure way. Though the 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 MoU SFPG has produced Recommendations [6] and [7] to support the security management (especially the key management).

An 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. A summary of those is provided below.

2.2.1 Authentication Key

The authentication key K is used for mutual authentication between an MS and the SwMI. There are three possible methods for generating K which are outlined below.

Method 1 – Generation of K from an Authentication Code (AC)
In this case the user types in an Authentication code via the keyboard of the handset. The digits of the AC are represented as a string of bits. This bit string is translated using an algorithm to the key K.
The AC is normally not stored in the handset. In the Network (Authentication Centre) either the K or the AC is stored. In the latter case the K is derived form the AC every time this is needed. This method is used if it is needed to identify the user of a handset, but not the handset. It should be noted that the AC

would normally have much less then 128 information bits. Therefore this method for generation of K should only be used in exceptional cases, e.g. if there is a need for user authentication only or if a key needs to be generated immediately and there is no possibility to use a User Authentication Key (UAK - see below).

Method 2 - Generation of K from an User Authentication Key (UAK)
The User Authentication Key is an unpredictable (random) value of any desirable length (usually 128 bits). The K is derived from the UAK using an algorithm. The UAK or (normally) the K is stored in the handset (or SIM) and the network (Authentication Centre). If the UAK is stored then every time the K has to be derived from it. This method is used if it is needed to identify the handset. It will be the most common method of key generation in TETRA systems.

Method 3 - Generation of K from an Authentication Code (AC) and an User Authentication Key (UAK)
In this case the K is derived from an AC entered by the user via the keyboard of the handset and a UAK stored in the handset. The derivation of K from AC and UAK is done via an algorithm. In the network either only the resulting K is stored, or both the AC and UAK are stored. This method is used if it is necessary to identify both the user and the handset.

2.2.2 Keys for air interface encryption

There are several sorts of encryption keys. The key may be derived or transferred as part of the authentication procedure, the keys can be sent to MS's using Over The Air Re-keying (OTAR, see also section 2.2.3) or they may be preloaded in the MS's. There are keys with long term and short term key lifetimes. Special mechanisms are included to protect the keys with a long lifetime. For the interested reader a description of the keys for encryption within the TETRA system is provided below.

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 e.g. be used for encryption of uplink communications (i.e. the communication from the MS to the network).

The **Common Cipher Key** (CCK) is generated by the SwMI and distributed, encrypted with the DCK, to MS's. It is efficient to use this key for encryption of messages that are directed to a certain Location Area (LA)[6]. In practice the CCK can be used to set up a group call with all MS's that at the moment are in a certain area, independent of the specific closed user groups these MS's are part of.
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 MS's of a group (e.g. similarly to the CCK, on a Smart card, or using OTAR (see

[6] A Location Area is a geographical area where a network and a number of MS's are operational which have certain logical connections (e.g. Public Safety organisations of a city, a department, etc).

below)). Within a Location Area the GCK is always used in a modified form. It is encrypted by the CCK to obtain the **Modified Group Cipher Key** (MGCK). If an MS is in this Location Area the MGCK is used to encrypt the closed user group messages for this MS.
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.

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 (e.g. by an authentication exchange) until it is replaced. TETRA supports the use of up to thirty-two (32) SCK's. They can be distributed similarly to the GCK's. Their use is largely implementation dependent but they can be used for e.g. 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.
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.

2.2.3 OTAR

As indicated above there is a possibility to distribute or update CCK's, GCK's and SCK's using a Over The Air Re-keying (OTAR) mechanism. This mechanism makes it possible to send in a secure way air interface encryption keys from the SwMI over the air directly to an MS and can be applied as long as an authentication key K is available for the MS. The OTAR messages to an MS are encrypted using session encryption keys that are derived from the authentication key for this MS.
The OTAR mechanism can be used for both an individual MS and for groups of MS's.
A mechanism similar to OTAR is also available for the management of end-to-end encryption keys.

2.2.4 Transfer of authentication information between networks

If a TETRA MS roams to another TETRA network 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 in 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 in TETRA systems it might cause too much overhead to transfer this information on a regular basis. A third alternative is therefore supported. This allows a home network to transfer only once a session authentication key 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.

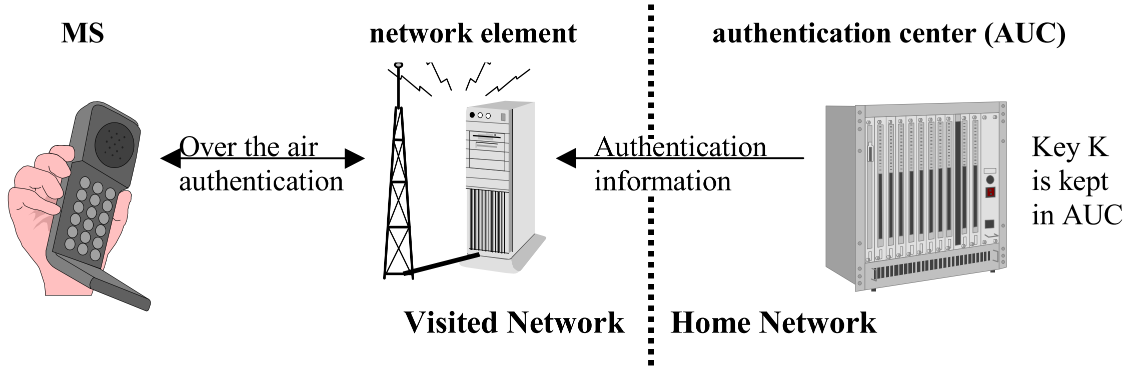

MS
network element
authentication center (AUC)
Over the air authentication
Authentication information
Key K is kept in AUC
Visited Network
Home Network

Figure 4 – Authentication in a visited network without disclosing the authentication key

2.3 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.

2.3.1 Air interface encryption algorithms

TETRA users can specify their own air interface encryption algorithm. However, for reasons of easy interoperability in multi vendor systems, a number of air interface encryption algorithms have been specified as part of the TETRA standard. Several requirements have been taken into account when specifying these standard algorithms. The most important of these are the need for diversity and export control regulations.

Need for diversity

In this paper 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.

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 two different criteria. These are explained below.

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.

TEA1 and TEA4: Readily Exportable Algorithms

TEA1 (as the numbering implies) was an early design. 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). The TEA2 is distributed by the Dutch Police IT organisation.

2.3.2 Air interface authentication and key management algorithms

TETRA users can specify their own air interface authentication and key management algorithm. Again for easy interoperability in multivendor systems, also a set of standard air interface authentication and key management algorithms has 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 also is ETSI.

2.3.3 End-to-end encryption algorithms

The end-to-end standard 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 an appendix which shows how these cryptographic functions can be realised using the IDEA 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. On this basis the TETRA MoU has established a licence agreement with ASCOM (the owners of IDEA) covering the use of IDEA in this context.

Details of the licensing agreement and how to make an application are available from the SFPG secretariat (Mrs. Marjan Bolle - m.bolle@kpn.com).

2.4 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 standardised a Lawful Interception Interface [4] to support the mechanisms for lawful interception. The detailed implementation of this interface might differ on a country to country basis.

References

[1] G. Roelofsen, TETRA Security – Information Security Technical Report, Vol 5, No. 3 (2000), pp 44-54

[2] ETS 300 392-7, Terrestrial Trunked Radio (TETRA), Voice plus Data (V+D), Part 7: Security Version 2.1.1

[3] ETS 300 396-6, Terrestrial Trunked Radio (TETRA), Direct Mode Operation (DMO), Part 6: Security (1998)

[4] EN 301 040 , Terrestrial Trunked Radio (TETRA), Security, Lawful Interception (LI) Interface, V2.0.0 (1998)

[5] TETRA MoU SFPG Recommendation 02 - End-to-End Encryption

[6] TETRA MoU SFPG Recommendation 01 - Key Distribution (KD)

[7] TETRA MoU SFPG Recommendation 06 - Management of Static Cipher Keys in DMO (under construction)

[8] G. Roelofsen, Cryptographic Algorithms in Telecommunications Systems – Information Security Technical Report, Vol 4, No. 1 (1999), pp 29-37