ETSI
TECHNICAL
REPORT

ETR 086-3

January 1994

Source: ETSI TC-RES

Reference: DTR/RES-06001

ICS: 33.060

Key words: TETRA, security

Trans European Trunked Radio (TETRA) system;
Technical requirements specification
Part 3: Security aspects

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

New presentation - see History box

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Blank page

Foreword

This ETSI Technical Report (ETR) has been prepared by the Radio Equipment and Systems (RES) Technical Committee of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status.

An ETR may be used to publish material which is either of an informative nature, relating to the use or application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or I-ETS.

This part of the ETR contains the specification of the Security aspects of the Trans European Trunked Radio (TETRA) system.

This ETR will be subject to revision and therefore future editions.

This ETR is divided into three parts:

Part 1: Voice plus Data (V+D) systems;

Part 2: Packet Data Optimized (PDO) systems;

Part 3: Security aspects.

Blank page

1 Scope

This ETSI Technical Report (ETR) defines the TETRA Security aspects, analyses the possible threats, defines the security objectives and requirements, and describes the security services.

2 References

For the purposes of this ETR the following references apply.

[1] ITU-T Recommendation X.25 (1993): "Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

[2] ETR 086-1 (1994): "Trans European Trunked Radio (TETRA) system; Technical requirements specifications; Part 1: Voice plus Data (V+D) systems".

[3] ISO 7498-2 (1989): "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

3 Definitions and abbreviations (TETRA 01.04)

3.1 Definitions

For the purposes of this ETR the following definitions apply:

Access control: the prevention of unauthorized use of resources, including the use of a resource in an unauthorized manner.

Authentication: the act of positively verifying that the true identity of an entity (network, user) is the same as the claimed identity.

Base Radio Stack (BRS): a logical grouping that includes all of the air interface protocol element in one base station (the fixed side of the air interface).

Base Station (BS): a physical grouping of equipment which provides the fixed portion of the air interface. One base station transmits and receives radio signals to and from a single location area (a single region of geographical coverage). A BS contains at least one Base Radio Stack (BRS).

Base Station Radio Part (BSRP): one physical sub-group of a base station which contains all the radio end points (one or more) that are connected to a single antenna system.

Bearer service: a type of telecommunication service that provides the capability for the transmission of signals between user-network interfaces.

Bi-directional channel: a channel that can carry information in both directions.

Broadcast call: a multipoint call in which the same information is transmitted simultaneously by the calling terminal to all available terminals.

Call: a complete information exchange between two or more parties.

NOTE 1: See also call transaction.

Call re-establishment (slow handover): the action of switching a call in progress from one cell to another or between radio channels in the same cell.

NOTE 2: Call re-establishment is used to allow established calls to continue when mobile stations move from one cell to another cell, or as a method to escape from co-channel interference.

Call transaction: all events associated with one continuous transmission of information during a call (including control signalling). A call consists of one or more call transactions.

NOTE 3: In a half-duplex call, the call consists of a sequence of unidirectional transactions.

Carrier (Radio Frequency (RF) carrier): the centre frequency of one radio transmission. A modulated carrier is used either for one uplink or one downlink.

Carrier pair: two different carriers which are allocated together to provide one uplink and one downlink. Normally the two carriers are allocated at a fixed frequency spacing (the duplex separation).

NOTE 4: Carrier pairs only refer to allocation of carriers, not to their use. For example, a bi-directional logical channel may be assigned to an uplink from one carrier pair plus a downlink from a different carrier pair.

Cell: the smallest geographical area where TETRA services may be obtained, using a certain set of radio frequencies.

NOTE 5: Each adjacent cell (touching or overlapping) should use a different set of radio frequencies to avoid co-channel interference.

Challenge-Response pair (C/R): a pair of 32 bit binary numbers linked by a security algorithm.

NOTE 6: When a user pays a subscription a key is distributed by the operator. This key is also stored in the subscriber information database.

Circuit switched connection: a connection that is established on request between two or more terminals and provides the exclusive use of the connection for information transfer until it is released.

Circuit switched data service: a data service that uses a circuit-switched connection to transfer data between data terminal equipment.

Circuit switched speech service: a service that uses a circuit-switched connection to transfer speech information between voice terminal equipment.

Closed user group: a (logical) group of users who are not allowed to communicate outside their group.

NOTE 7: Gateways to other networks and to particular subscribers may be accessible as a supplementary service.

Confidentiality (1): rendering information into the form of ciphertext, such that the information is only intelligible by entities that possess the reverse algorithm (i.e. the ability to recover the plaintext from the ciphertext).

Confidentiality (2): the property that information may not be available or disclosed to unauthorized individuals, entities or processes.

Connectionless packet data service: a service which transfers a single packet of data from one source node to one or more destination nodes in a single phase (i.e. without establishing a logical connection or virtual circuit).

Connection oriented packet data service: a service that transfers data from one source node to one destination node using a multi-phase protocol that establishes (and releases) logical connections or virtual circuits between end users that are then used to transferring packet data.

Data compression: a reversible process that reduces the quantity of data, without any loss of information.

Data integrity: the property that data has not been altered or destroyed in an unauthorized manner.

Data origin authentication: the corroboration that the origin of the source of data received is as claimed.

Direct mode: a mode of simplex operation where mobile subscriber radio units may communicate using radio frequencies which are outside the control of the network and without intervention of any base station.

Downlink: a unidirectional radio pathway for the transmission of signals from one Base Station (BS) to one or more Mobile Stations (MSs).

Duplex (full duplex): a mode of operation by which information can be transferred in both directions and where the two directions are independent. See also half duplex.

NOTE 8: In a packet switching environment (PDO or V+D signalling) protocols can be duplex at one layer and half duplex at another layer.

Encryption: the conversion of plaintext to ciphertext.

End to end: is within the TETRA boundaries:

- from TETRA terminal to TETRA terminal (LS or MS);
- from TETRA terminal to gateways;
- including inter system interface.

External user: an application which does recognize TETRA messages and cannot therefore directly invoke TETRA services.

NOTE 9: An external user may be involved in communications which also involve TETRA equipment, but the external user has no direct control over the TETRA facilities.

Facility: the means to assist the performance of an action.

Gateway: a device which will enable the interconnecting of two networks which inherently use different and incompatible protocols.

Half duplex (semi duplex): a mode of operation by which information can be transferred in both directions but the transfers are mutually dependent (i.e. uplink and downlink transfers share some resources). See also duplex.

NOTE 10: In a packet switching environment (PDO or V+D signalling) protocols can be duplex at one layer and half duplex at another layer.

Home Data Base (HDB): the data base in the MS's home TETRA network. In the HDB all necessary information about the MS is collected and stored permanently. Also information about how to find a migrating MS is stored in the HDB. There is logically only one data base in a TETRA network.

Identity exchange: a procedure in which the individual MS identity (i.e. ITSI, ISSI or ASSI) is exchanged for an alias identity (i.e. ISSI or ASSI).

NOTE 11: This is carried out for one of two purposes, either for security purposes where the real ISSI is not sent over the air interface or for exchanging a migrating MS's long ITSI identity to an unambiguous short ISSI or ASSI identity.

Implicit registration: is when the location of the MS is noticed through messages other then location updating messages, e.g. CC messages.

Incoming call: a terminating call which, from the viewpoint of an individual party, is a call that was initiated by another party.

NOTE 12: See also outgoing call.

Inter-operability: an attribute that describes the ability of a given subscriber terminal to obtain service from a given infrastructure, using the appropriate standard TETRA interface protocols.

NOTE 13: See also level of inter-operability and profile.

Inter-system inter-working capability: the ability of a particular TETRA infrastructure to exchange meaningful information with other TETRA infrastructures, using the standard TETRA inter-system inter-working protocols.

NOTE 14: An infrastructure can be characterized by the combination of its inter-system inter-working capability and its air interface profile. See also the definition of profile, and level of inter-working.

Key: a sequence of symbols that controls the operations of encipherment and decipherment.

Key management: the generation, selection, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

Level of inter-operability: the maximum level of service that can be obtained from a particular pair of equipment (one subscriber terminal and one infrastructure).

NOTE 15: See also interoperability and profile.

Level of inter-working: the maximum level of inter-system inter-working information transfer that is possible between a particular pair of equipment's (i.e. between two particular TETRAs).

NOTE 16: See also inter-system inter-working capability.

Local Line Connected Terminal (LLCT): a type of subscriber terminal which allows a TETRA user to communicate via a cable which is linked directly (i.e. not via a transit network) to the TETRA Switching and Management Infrastructure (SwMI).

Location Area (LA): an area within a TETRA network that may comprise one, several or all cells. An MS may move freely without re-registering within a location area. An MS has continuity of service within a location area. A location area is geographically static.

Logical channel: a logical communications pathway between two or more parties. A logical channel may be unidirectional or bidirectional.

Message trunking: a method of traffic channel organization where each traffic channel is permanently allocated for the complete duration of the call, which may included several separate call transactions (several pressel activations by separate terminals). The channel is only de-allocated if the call is (explicitly) released or if a timeout expires.

NOTE 17: See also transmission trunking, quasi-transmission trunking, statistical multiplexing and quasi-statistical multiplexing.

Migration: the change of location area, each belonging to different TETRA network.

Mobility: the act of a subscriber terminal changing its physical location.

Multicast: the transmission of the same information from one source node to a defined set of destination nodes.

Multiple registration: when a mobile is allowed to simultaneously be registered in more than one location area.

Mobile Radio Stack (MRS): a logical grouping that includes all of the air interface protocol element in one MS (the mobile side of the air interface).

Mobile Station (MS): a physical grouping that contains all of the mobile equipment that is used to obtain TETRA services. By definition, a mobile station contains at least one Mobile Radio Stack (MRS).

Network: a collection of subscriber terminals interconnected through telecommunications devices.

Network management entity: an entity that has access to all parts of the network.

Node: a point at which a packet is manipulated (e.g. sourced, sunk, routed or switched).

Open channel: a dedicated traffic channel that is reserved for the exclusive use of a closed user group.

NOTE 18: See also pseudo open channel.

Outgoing call: a call which, from the viewpoint of an individual participant in the call, is initiated by that participant.

NOTE 19: See also incoming call.

Phase: one discrete part of a procedure, where the start and end of the part can be clearly identified (e.g. by the dispatch of a primitive).

Plaintext: information (including data) which is intelligible to all entities.

Primitive: a distinct data elements that is exchanged between adjacent protocol layers.

NOTE 20: A primitive may be defined in either an abstract or concrete format.

NOTE 21: A service primitive contains one Service Data Unit (SDU).

Private system: a TETRA system established by a private organization so that a group of subscriber terminals that are part of the system can establish calls between one another using the facilities of the private TETRA system.

Process: the exact mechanism whereby a given service is performed.

NOTE 22: If a service conforms to a standard process, it should be performed according to the process defined in the standard.

Profile: the capability of a particular equipment. This is defined separately for individual subscriber terminals and individual infrastructures.

NOTE 23: See also inter-operability and level of inter-operability.

Provision: the act of supplying a given service.

NOTE 24: A Switching and Management Infrastructure (SwMI) may be capable of supporting a service. However, it may not supply the service to certain subscriber terminals for which the service is not subscribed.

Pseudo open channel: a method of assigning traffic channels to a closed user group such that the group appear to have exclusive use of a dedicated traffic channel.

NOTE 25: See also open channel.

Public system: a TETRA network which is established and operated by an organization for the purpose of providing services to subscribing members of the public and third party organizations.

Quasi-statistical multiplexing (quasi-statistical trunking): a multiplexing method which assigns one or more traffic channels to packets from several sources on an "as-needed" basis. Each packet is assigned to one channel, but several packets may be served by a given channel at the same time (the channel capacity being shared amongst them).

NOTE 26: See also transmission trunking, message trunking, quasi-transmission trunking and statistical multiplexing.

Quasi-transmission trunking: a method of traffic channel organization where each traffic channel is allocated for the each call transaction (while the pressel is activated) and in addition the channel de-allocation is delayed for a short period at the end of the transaction (after the pressel release). During this "channel hold-time" the channel allocation may be re-used for a new call transaction that is part of the same call. A delayed channel de-allocation procedure will apply at the end of each transaction.

NOTE 27: See also transmission trunking, message trunking, statistical multiplexing, and quasi-statistical multiplexing.

Radio End Point (REP): the location of the radio function of transmitting or receiving on one carrier.

NOTE 28: A base station will contain several radio endpoints, typically half will be transmitters and half will be receivers.

Radio Packet Data Infrastructure (RPDI): all of the TETRA equipment for a Packet Data Optimized (PDO) network except for subscriber terminals. The RPDI enables subscriber terminals to communicate with each other via the RPDI.

NOTE 29: The RPDI may also make it possible for subscriber equipment to communicate via other transit networks to external applications. MSs can access the RPDI using the air interface.

Registered Area (RA): the total area for which a MS is currently registered. The RA is defined by the list of location areas contained in the latest successful registration.

NOTE 30: The registered area may be non-contiguous.

Registration: a function which allows an MS to tell the TETRA network that it has changed location area (roaming or migration), TETRA subscriber identity or mode of operation. This function enables the network to keep track of the MS.

Roaming: the change of location area within the same TETRA network.

Remote Line Connected Terminal (RLCT): a type of subscriber terminal which allows a TETRA user to communicate via a pathway which includes a transit network and the TETRA Switching and Management Infrastructure (SwMI).

Repudiation: denial by one of the entities involved in a communication of having participated in all or part of a communication.

Search Area (SA): an area comprising all location areas where a MS may search for service.

Security service: a service provided by a layer of communicating open systems which ensures adequate security of the systems or of data transfers.

Signalling: the exchange of information specifically concerned with the establishment and control of connections, and with management, in a telecommunication network.

Statistical multiplexing: a multiplexing method which assigns one or more traffic channels to packets from several sources on an "as-needed" basis. Each packet is assigned to one channel, and each channel serves the packets sequentially (each packet is completed before a new packet is started).

NOTE 31: See also transmission trunking, message trunking, quasi-transmission trunking and quasi-statistical multiplexing.

Subscriber terminals: an equipment which an internal user can use to communicate with another user. Mobile Stations (MS), Local Line Connected Terminals (LLCT) and Remote Line Connected Terminals (RLCT) are the only types of subscriber terminal.

Supplementary service: a supplementary service modifies or supplements a bearer service or a teleservice. A supplementary service cannot be offered to a customer as a stand alone service. It should be offered in combination with a bearer service or a teleservice.

Switching and Management Infrastructure (SwMI): all of the TETRA equipment for a Voice plus Data (V+D) network except for subscriber terminals. The SwMI enables subscriber terminals to communicate with each other via the SwMI.

NOTE 32: The SwMI may also make it possible for subscriber equipment to communicate via other transit networks to external applications. Mobile Stations (MS) can access the SwMI using the air interface.

Teleservice: a type of telecommunications service that provides the complete capability, including terminal equipment functions, for communication between users according to agreed protocols.

Tetra Equipment Identity (TEI): an electronic serial number which is permanently connected to the TETRA equipment. When it is transmitted over the air interface, it is protected by an algorithm.

Threat: a potential violation of security.

Transaction (packet transaction): all the processes and procedures associated with the transmission of one packet of information between peer network layer protocol entities on opposite sides of the air interface.

Transaction (voice transaction): all of the processes and procedures associated with the unidirectional transmission of one packet of (user) information between network layer service boundaries that lie on opposite sides of the air interface.

Transmission trunking: a method of traffic channel organization where each traffic channel is individually allocated for each call transaction (for each activation of the pressel). The channel is immediately de-allocated at the end of the call transaction (subject to unavoidable protocol delays).

NOTE 33: See also message trunking, quasi-transmission trunking, statistical multiplexing and quasi-statistical multiplexing.

Two-frequency simplex: a physical layer mode of operation, where a radio end point is either receiving on one RF carrier or transmitting on another (different) RF carrier. The transmit and receive operations are dependent; transmission implies no reception, and reception implies no transmission.

Two-frequency simultaneous duplex (two frequency duplex) (two frequency full duplex): a physical layer mode of operation where a radio end point is receiving on one RF carrier and transmitting on another (different) RF carrier at the same time (the periods of transmission and reception are not separated in time). The transmit and receive operations are independent.

NOTE 34: The word duplex always implies the existence of independent transmit and receive operations. A duplex radio requires extra processing compared to a simplex radio.

Two frequency time division duplex (two frequency semi-duplex) (two frequency half-duplex): a physical layer mode of operation where a radio end point is receiving on one RF carrier and also transmitting on another (different) RF carrier, but the periods of transmission and reception are displaced (interleaved) in time. The transmit and receive operations are independent.

Unidirectional channel: a channel that can only carry information in one direction.

Uplink: a unidirectional radio communication pathway for the transmission of signals from one or more MSs to one BS.

Visited Data Base (VDB): is the data base in a visited TETRA network. When an MS has migrated to a TETRA network and exchanged its ITSI to an ISSI or an ASSI belonging to the VDB, subsequent roaming will take place in the visited network without contact with the HDB. There is logically only one VDB per TETRA system.

3.2 General abbreviations

For the purposes of this ETR the following general abbreviations apply:

ASSI	Alias Short Subscriber Identity
ATSI	Alias TETRA Subscriber Identity
BS	Base Station
C/R	Challenge-Response pair
CL (C/L)	Connectionless
CLNP	Connectionless Network Protocol
CLNS	Connectionless Network Service
CMCE	Circuit Mode Control Entity
CO (C/O)	Connection Oriented
CONP	Connection-Oriented Network Protocol
CONS	Connection-Oriented Network Service
DCE	Data Circuit-terminating Equipment
DGNA	Dynamic Group Number Assignment
DLC	Data Link Control
DM	Direct Mode
DTE	Data Terminating Equipment
ETSI	European Telecommunications Standards Institute
GSSI	Group Short Subscriber Identity
GTSI	Group TETRA Subscriber Identity
HDB	Home Data Base
ISDN	Integrated Services Digital Network
ISI	Inter System Interface
ISO	International Organisation for Standardisation
ISSI	Individual Short Subscriber Identity
ITSI	Individual TETRA Subscriber Identity
LA	Location Area
LLC	Logical Link Control
LS	Line Station
MAC	Medium Access Control
MCC	Mobile Country Code (Identity), part of ITSI
MLE	Mobile Link Entity
MM	Mobility Management
MNC	Mobile Network Code (Identity), part of ITSI
MS	Mobile Station
MSI	Mobile Subscriber Identity
MT	Mobile Termination
MTU	Mobile Terminating Unit
NT	Network Termination
NWK	Network
OSI	Open Systems Interconnection
PAD	Packet Assembler/ Disassembler
PD	Protocol Discriminator
PDN	Public Data Network
PDO	Packet Data Optimized
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PSTN	Public Switched Telephone Network
PTN	Private Telephone Network
PTNX	Private Telephone Network eXchange
PVC	Permanent Virtual Circuit
RES-6	ETSI Sub-Technical Committee RES-6 (Radio Equipment and Systems - 6)
RA	Registered Area
RPDI	Radio Packet Data Infrastructure
RPDN	Radio Packet Data Network
S-CLNP	Specific Connectionless Network Protocol
S-CLNS	Specific Connectionless Network Service
SA	Search Area
SAP	Service Access Point
SDL	(Functional) Specification and Description Language

SDU	Service Data Unit
SNAcP	Sub-Network Access Protocol
SNDCP	Sub-Network Dependent Convergence Protocol
SNICP	Sub-Network Independent Convergence Protocol
SS	Supplementary Service

NOTE: The abbreviation SS is only used when refering to a specific Supplementary Service.

SwMI	Switching and Management Infrastructure
TBD	To Be Determined
TDC	Transient Data Channel
TE	Terminal Equipment
TEI	TETRA Equipment Identity
TETRA	Trans European Trunked RAdio
TMI	TETRA Management Identity
USSI	Unexchanged Short Subscriber Identity
V+D	Voice Plus Data
VC	Virtual Call
VDB	Visited Data Base
VPA	Virtual Point of Attachment
X.25 PLP	X.25 Packet Layer Protocol (Layer 3 of ITU-T Recommendation X.25 [1])

3.3 Supplementary service abbreviations

AL	Ambience Listening
AoC	Advice of Charge
AP	Access Priority
AS	Area Selection
BIC	Barring of Incoming Calls
BOC	Barring of Outgoing Calls
CAD	Call Authorized by Dispatcher
CCBS	Call Completion to Busy Subscriber
CCNR	Call Completion on No Reply
CFB	Call Forwarding on Busy
CFNRy	Call Forwarding on No Reply
CFNRc	Call Forwarding on Mobile Subscriber Not Reachable
CFU	Call Forwarding Unconditional
CLIP	Calling Line Identification Presentation
CLIR	Calling/Connected Line Identification Restriction
COLP	Connected Line Identification Presentation
CR	Call Report
CRT	Call Retention
CW	Call Waiting
DGNA	Dynamic Group Number Assignment
DL	Discreet Listening
HOLD	Call Hold
IC	Include Call
LE	Late Entry
LSC	List Search Call
PC	Priority Call
PPC	Pre-emptive Priority Call
SNA	Short Number Addressing
TC	Transfer of Control of Call
TPI	Talking Party Identification

4 Security aspects (TETRA 02.20)

4.1 General

This clause defines the TETRA security policy, the field of application and gives the standardization boundaries. The methodology followed for TETRA is also described, the definition of the TETRA players is given as well as the principles of security profiles.

4.1.1 Introduction

Individual users, subscribers and network operators should, if they wish, be protected against the undesirable intrusion of third parties.

The general principles on which TETRA system security will be based is outlined in the basic Reference Model for OSI: ISO 7498-2 [3] which gives the general description of security services and mechanisms, the relationship of services, mechanisms and layers, and their placement.

This Clause defines the services which are optionally available in a TETRA system. Only those features which enhance the security in a TETRA network are considered.

4.1.2 Applicability of the security services

The TETRA protocol will be defined to support all of the listed features but implementation of these security services in a particular network is an operator option. Security mechanisms will be defined in TETRA, where the organization can choose the security level in private networks and where for public networks there will be a standard security mechanism corresponding to the security functionality.

An Mobile Station (MS)/Line Station (LS) should be able to operate with the security services demanded by the network. Each security service is considered to be totally independent of the others. The security standard should offer a modular security system out of which operators can choose. Thus a network operator may support any single security services or any combination of security services depending on the application.

Each security mechanism uses a different algorithm which are not defined in this ETR.

Quality of service should not decrease significantly and interoperability should also be ensured.

The TETRA standard is concerned only with information flowing within the TETRA system at the standardized boundaries and is aimed primarily at protecting access to information at the radio interface. The TETRA infrastructure is not standardized within TETRA, however if no physical security restrictions are placed on access to the system equipment itself then these measures will be in vain.

System/subscriber database protection methods are considered to be outside the scope of this ETR.

4.2 Security policy

The TETRA security policy is provided as a guideline and a set of rules:

- in order to protect the TETRA network operator's information;
- for the implementation of the TETRA security mechanisms;
- in order to protect the user information and interests;

and covers all players as defined in subclause 4.7.

The TETRA security policy provides a set of security services to allow the players to build their own security policy based on the security services.

The TETRA security policy will determine those elements of the system security that are always applied or in force and those that the user may choose to use as he sees fit. The policy can be divided into two separate components based on the nature of the authorization involved, as either ruled based policy or identity based policy.

The goal of the TETRA identity based security policy is to filter access to data or resources. The users access to TETRA should be controlled, also the supplementary services they use, and their priorities which is related to resources.

The ruled based security policy rests on data and resources marked with security labels. For example the TETRA user identity may be included with data.

Table 1 lists who has access to which information.

Table 1: Information access

	Information	Access
1	Accounting information	Network operator
2	Authentication information	Network operator
3	Availability information	Dispatcher
4	Configuration information	Organization manager - network operator
5	Fault information	Network operator - organization manager
6	ISI individual service information	Network operator
7	Info about user	Included in 2 above
8	ISI user information	Network operator - organization manager
9	ISI system information	Network operator
10	Performance information	Network operator - organization manager
11	Registration information	Network operator - organization manager - dispatcher
12	Security information	TBD
13	Service provision information	Network operator - organization manager
14	Subscriber information	Network operator
15	System broadcast information	Network operator
16	Telecoms service control	Network operator
17	V+D data exchange control	Network operator
18	V+D user data	Network operator - user
19	Voice call control data	Network operator
20	Voice messages	Dispatcher - user
21	Algorithm management	SAGE
22	Key management information	TBD
23	Security mechanism information	STAG - manufacturer

4.3 The field of application

The security requirements will apply to the following four TETRA standards:

- Voice plus Data (V+D);

- Packet Data Optimized (PDO);

- Direct Mode (DM);

- the TETRA CODEC.

The requirements may be different for each of the standards; this part of the ETR describes the Voice plus Data (V+D) security, specifics related to the Packet Data Optimized and Direct Mode, when they exist, and are described in specific subclauses.

TETRA security provides a description of services and related mechanisms and defines the position in the architecture and the layers where the services and mechanisms may be provided. Additional security measures may be needed in end systems, installations and organizations; this is outside the scope of this ETR except when they impact security services visible in OSI (the TETRA standards will follow the OSI model).

This part of this ETR is concerned only with those aspects of security which affect interoperability.

4.4 General architecture

The general architecture is described in figures 1 and 2. These figures show the standardized interfaces within TETRA:

a) V+D and PDO:

  - I1 radio air interface (MS to BS);

- I2 fixed terminal interface, local or remote (LS to BS);

- I3 Inter System Interface (ISI);

- I4 Terminal Equipment interface (TE to MT);

- I5 Gateways (PSTN, ISDN, PDN, PTN);

- I6 Network Management Unit interface (NMU);

b) DM:

(to be determined).

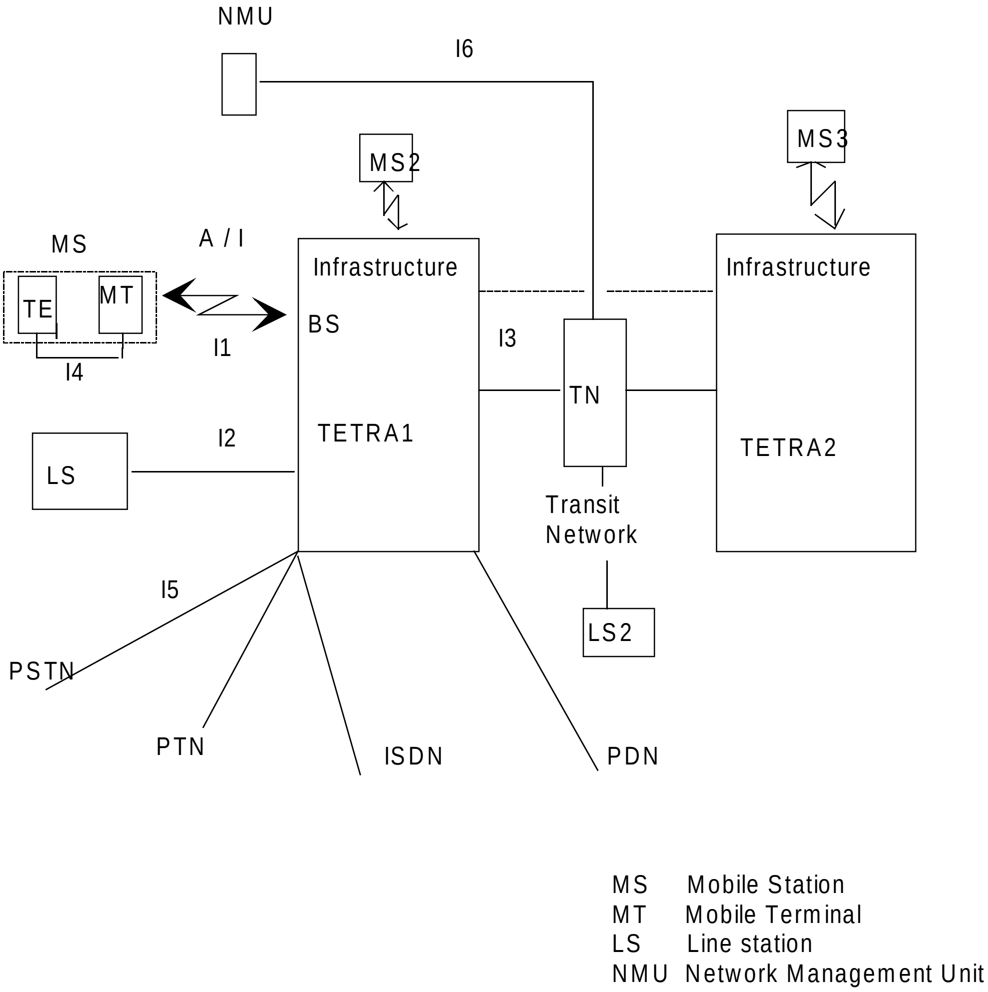


Figure 1: TETRA voice plus data

The TETRA bearer services are described in ETR 086-1 [2], Clause 5.

The teleservices are described in ETR 086-1 [2], Clause 5.

Voice and data supplementary services, and packet data optimized facilities are described in ETR 086-1 [2], Clause 5.

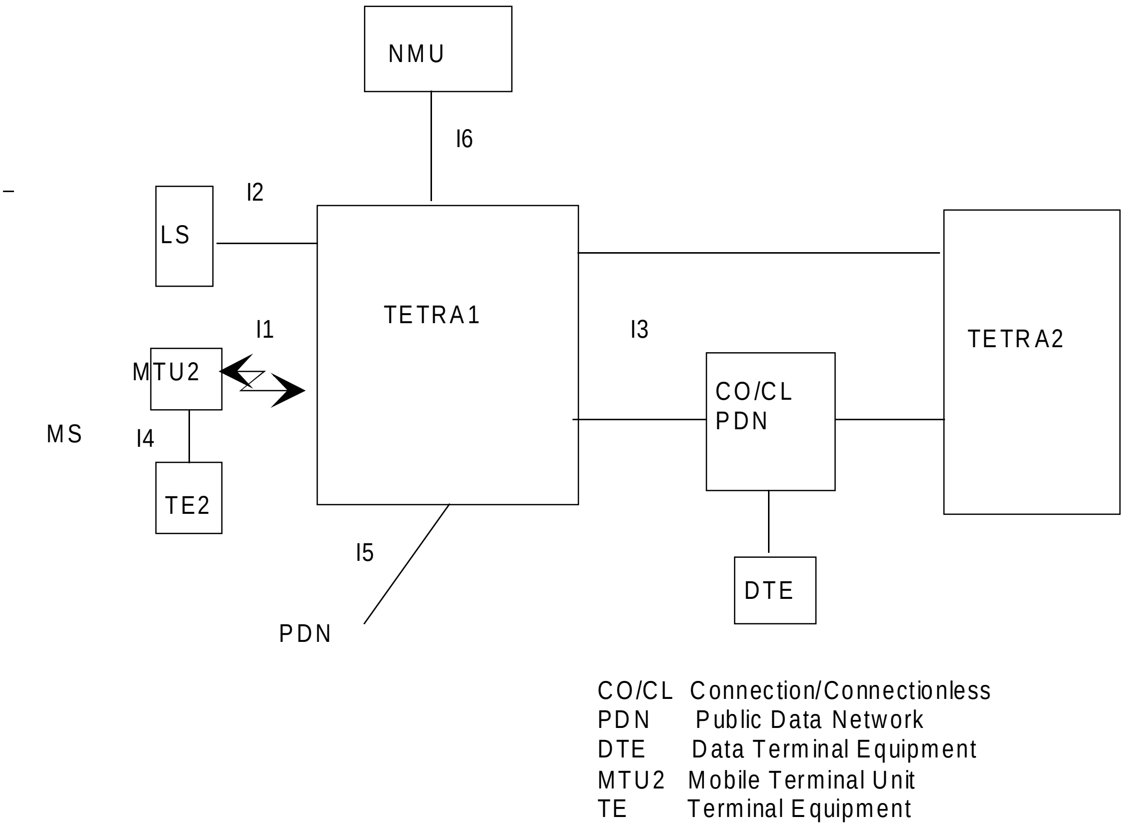


Figure 2: TETRA packet data optimized

The TETRA protocols at the standardized interfaces follow the ISO layering (up to layer 3). Security services are included in the OSI security architecture and also mechanisms which implement those services (see ISO 7498-2 [3]).

Priority is given to the security related to the I1 and I3 interfaces.

4.5 The standardization boundaries

The general architecture gives the interfaces which are standardized within TETRA. Security is not standardized at the application level.

Different levels of security standardization are possible in TETRA:

- protocol plus mechanisms;

- only the protocol;

- a protocol and a mechanism.

It is assumed that protocol plus one mechanism is the level of standardization chosen but the option taken is to have a generic protocol permitting several mechanisms on the air interface. This allows the implementation of different mechanisms.

It is also assumed that key distribution is covered in this standardization procedure, but key management is covered in network management/security management.

Security algorithms are not part of this standard description, they are developed by other entities such as SAGE.

The standardization boundaries are set according to priorities defined within the following areas for TETRA standardization, refer to Clause 7.

4.6 Methodology and outputs

The TETRA security design follows the following steps:

- first the threat analysis is described in Clause 5;
- once the players are identified security objectives and requirements are described in Clause 6;
- from this, the selection and specification of security services/features are described in Clause 7 according to priorities defined;
- the specification of the associated security mechanisms will be described in the future TETRA standards;
- the components of the security mechanisms will be described in the future TETRA standards;
- the definition of the security management (key management, key distribution) will be described in the future TETRA standards;
- the physical allocation will be described in future TETRA standards;
- the specification of requirements for cryptographic algorithms is not part of this ETR;
- performances related to security will be part of the performance objectives in a future TETRA standard, and for simulation, in the TETRA designer's guide.

4.7 Definition of TETRA players

In order to define security objectives and requirements within TETRA, different types of players have been identified, with links between them and a hierarchy. Figure 3 shows the types:

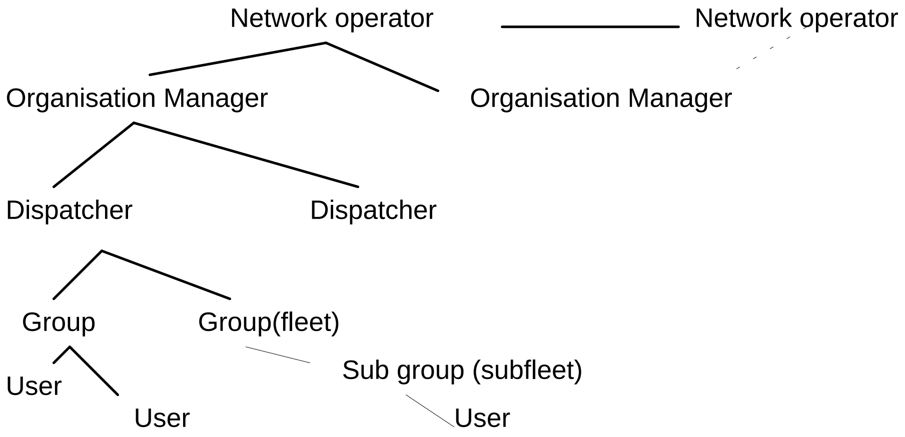


Figure 3: TETRA players

These different levels of players can eventually be merged or not exist depending of the application. They may share different resources of the network (infrastructure, mobiles).

As an example, a TETRA infrastructure managed by one network operator may be shared by different independent organizations which do not have necessarily the same security requirements. A TETRA network can be connected to a second TETRA network with not the same level of security, while mobiles can move to this second network. Figure 4 shows possible configurations.

Two types of networks can be defined, Public Access Mobile Radio (PAMR) networks and Private Mobile Radio (PMR) networks with different types of users and their own security requirements.

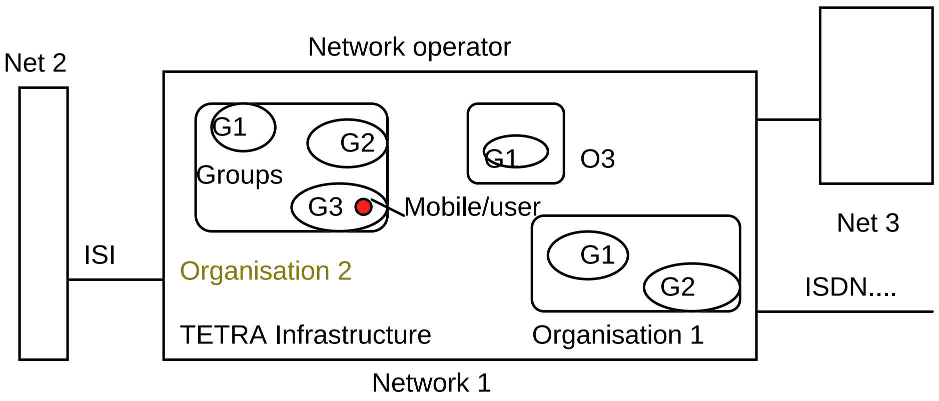


Figure 4: Players in TETRA

The following definitions of the TETRA players are given.

Network operator: the person or company who builds and runs the TETRA network **(**PAMR) and who has people or companies as customers. Different levels can exist within the network operators like a super network manager who controls more than one TETRA Network. These levels may not exist in the case of a PMR.

Organization manager: the person who runs the organization of his users within his organization. The organization manager can be the same as the network operator in the case of a PMR.

Operational dispatcher: the person who manages the groups and users. There can be different levels within the operational dispatchers like a supervisor who manages several dispatchers.

Subscriber: this is the organization or person identified in the TETRA network by his subscription. Billing if applied will relate to the subscriber.

User: the user is the person who belongs to the organization and who uses a mobile or line connected terminal for his calls or data transfers. The user can be the same as the subscriber. The user identity will be defined in the future TETRA standard.

An Advice of Charge (AoC) can be given to the user corresponding to his use of the resources within the organization.

Mobile owner: a mobile can be used by different users within the organization or belonging to different organizations. The terminal can belong to a different person from the user or subscriber. The terminal owner can be the same as the user or subscriber. The mobile can be split into two, and eventually three, separate parts like TE, MTU, SIM. Each part can correspond to different owners.

Manufacturer: this is the mobile manufacturer or the infrastructure manufacturer.

Maintenance personnel: these are the personnel which maintain either the mobiles or the infrastructure.

4.8 Principles of security profiles

A security profile is a combination of security services having a certain level, the level being the strength of a mechanism within a service. There can be several security levels for the same security service.

These profiles concern public networks where different profiles are offered, the use of the same profile then allows interoperability.

The proposed profiles are:

- minimum security profile with protection of billing only;

- medium security profile for user privacy on the air interface;

- high security profile.

They are detailed in Clause 7.

5 Threat analysis (TETRA 02.21)

5.1 Introduction

In this clause the TETRA system is analysed for possible threats. The base for this analysis is the TETRA system as far as it has been developed until now, without the incorporation of possible security measures.

The analysis is made for both, private and public systems. The impacts of an optional connection of the TETRA system to public or private fixed networks are included in the analysis as well. Also, the special features and procedures of TETRA have been analysed.

Also in this clause, the weaknesses of the system are analysed for each of the threats, i.e. it is discussed which attacks are possible or likely to realise a specific threat. However, the relationship between threats and the underlying attacks is not one-to-one; a threat to the system can be realised by different attacks and the same basic attack can have different effects depending on the intention of the attacker. These inter-dependencies between the threats and the attacks are handled by cross references in order not to annoy the reader with too much repetition.

In subclause 5.2, the threats to a communication system are classified and assessment criteria for the threats are given. Subclauses 5.3 to 5.5 describe the different classes of threats and their impact on the TETRA system. Finally, in subclause 5.6 the complete clause is summarised and an outlook is given.

5.2 Classification of threats

Threats to a communication system can be grouped in three classes:

- message related threats:

  to this class belong those threats that are directed at individual messages that are transmitted in the system, e.g. between two (or more) users of the system, between network operators, between a user and a service provider;

- user related threats:

  to this class belong those threats that are directed at the general behaviour of the users of a system, i.e. finding out what they are doing when and where;

- system related threats:

  to this class belong those threats that are directed at the integrity of the system as a whole or at parts of it to get access to (parts of) the system or to impair the system functionality.

A description of the threats or of the underlying attacks should address the following items to allow an assessment of the threats and attacks:

- the kind of attacks that are possible to realise the threat;

- possible penetration points for the attacks, e.g.:

  - the radio interface between mobile stations and base stations;
  - wired interfaces to terminals;
  - links within the TETRA infrastructure;
  - interfaces to other networks;
  - network management and maintenance interfaces;
  - other elements in the TETRA infrastructure, like databases and network nodes.

  NOTE: A survey of TETRA interfaces is given in Annex B.

- persons that might be interested in mounting an attack, e.g.:
    - legitimate users;
    - maintenance personnel;
    - outsiders.

- motives and conceivable profits for the attackers, e.g.:
    - gaining unauthorized access to valuable information;
    - gaining access to services without proper authorization and/or payment;
    - spoofing of users;
    - impeding or disrupting services achieved by competitors.

- difficulty of the attack (what are the required expert knowledge and resources to carry out the attack), e.g.:

- can be done by everybody with publicly available knowledge of the system:
    - sophisticated insider knowledge is necessary;
    - commercially available equipment can be used;
    - the necessary equipment must be manufactured or largely modified.

- outlines of available mechanisms that can help to prevent the attacks:

    in the following, the classes of threats are refined and the underlying attacks are described according to the list above. Wherever necessary, we indicate the type of system (public or private) and the type of information (voice, user data, control data, management data) that is subject to the threat or attack described.

5.3 Message related threats

This class of threats comprises those threats that are directed at individual messages. The following threats can be distinguished:

- interception;
- manipulation; and
- repudiation.

They are described in the following subclauses.

5.3.1 Interception

This threat means, that an unauthorized party may learn information transferred or stored in a TETRA system. It applies to public and private systems and to all kinds of information. According to the penetration points the following threats can be distinguished.

5.3.1.1 Interception at the radio interface

Attacks that lead to this threat can be relatively simple due to the radio characteristics of the TETRA system. Possible attacks to get access to sensitive data are monitoring the data "in the air" and masquerading as one of the entities at both sides of the radio interface.

Voice plus data "in the air" can be monitored in the following ways (the original communication is not disturbed):

- as with analogue radio interfaces, scanners to intercept digital radio interfaces will be for sale eventually and could easily be used by anybody. Even if that is not the case, scanners can be built by people with sufficient knowledge of radio technology and the TETRA specifications;

- besides this, a user of the system could use his (possibly modified) mobile station to listen to the communications of any channels he/she wants to. Probably, only little knowledge is necessary. This attack can also be done by anybody who has access to a stolen mobile station.

For masquerading the following possibilities exist:

- anybody might actively [1] masquerade as another user (or terminal) to receive the information intended for this user. This attack can be realised in different ways, e.g. with the help of replay of data (see chapter on manipulation);

- another attack might be an entity masquerading as a base station to attract calls from mobiles. This attack is very expensive (concerning costs and the necessary knowledge), so this attack is only done, if a very big profit is expected. Attackers will probably only be criminal organizations (e.g. terrorist organizations).

The profit for the attacker depends on the kind of information he/she is intercepting:

- Voice, user data:
  - confidential information may be intercepted. Depending on the nature of the information, this might be very useful for the attacker and very harmful to the victim.

- Control data:
  - the attacker may get information, e.g. about the identity or group identity of the sender and/or receiver of some information, about his/her location and/or priority, about the identity or location of the terminal used, about the service requested. The attacker can observe a user, trying to find out his/her habits (see also chapter on user related threats). The information gained may also be used later for other attacks, e.g. to masquerade as another user or to manipulate some data.

- Management data:
  - the attacker might intercept management information, e.g. information concerning network operation, information concerning connections to other networks, charging information. If security measures are applied, then much information related to these measures is interesting to an attacker, e.g. keys used for encryption or keys used for authentication. This information can then be used to support other attacks, e.g. to masquerade as another user.

Monitoring of data "in the air" can never be detected or prevented by security mechanisms [2]. By enciphering it is possible to make sure that the intercepted information is not intelligible to others but the intended receiver. Masquerading can be prevented with the help of authentication mechanisms.

5.3.1.2 Interception in the fixed parts of the network

To intercept information in the fixed parts of the network [3], the same kinds of attacks can be carried out as for interception at the radio interface. The only difference is, that physical access to the entities or wires of the TETRA system or a connected network, e.g. PSTN, is necessary.

- Information can be monitored in the following ways (the original communication is not disturbed):
  - an attacker can tap a wire of any system interface (see Annex B) and use a commercially available (and possibly modified) protocol analyser to understand the information sent. For this attack, only little knowledge is necessary;
  - an attacker can intercept all information processed or stored within an entity of the system. This attacker needs physical access to a network node, e.g. a base station, and good

[1] As opposed to the passive listening, described above.

[2] By the use of Quantum mechanics data can be exchanged in such a way that interception of the data can be detected (not prevented) with arbitrary high possibility. This system is under development, at the moment it is not applicable for mobile systems, therefore it is assumed that Quantum mechanics will not be realised for the TETRA system.

[3] The term "fixed parts" is used to describe all nodes and links of the network but the mobile station and its interface to the base station. However, not only wired lines can be used in the "fixed part" of a TETRA system, also radio links may be possible. For radio links analogues threats as for the radio interface between mobile station and base station have to be considered.

knowledge of the internal working of the system. He/she is likely to be an insider, such as maintenance or operating personnel.

- For masquerading the following possibilities exist:

  - somebody might masquerade as a fixed entity of the system at any of its interfaces (see Annex B). However, this seems to be more complicated as masquerading as a base station at the radio interface. Besides, these attacks have the disadvantage, that it is necessary to cut existing connections, which might be noticed;

  - a special case of the above is the masquerade as a system entity over an interface that is not permanently connected, such as the inter system interface (labelled I5 in Annex B) between two TETRA systems that are connected through a transit network.

The same considerations concerning the profit for the attacker hold as for interception at the radio interface: the profit depends a lot on the kind of data that is intercepted. The only difference is, that more management data can be intercepted and misused, since the majority of the management data is transmitted inside the wired part of the network. An example for these interesting management data in the case of security measures are the challenge-response pairs for authentication of a mobile station, which might be exchanged between different systems.

Possible countermeasures are essentially the same as in the case of interception at the radio interface, i.e. encryption and authentication mechanisms.

5.3.2 Manipulation

This threat means, that an unauthorized party may be able to change information in the system. It applies to public and private systems and to all kinds of information. Different sorts of manipulations have to be considered:

- simple changes (e.g. inversion of bits);

- deletion or insertion of parts of the message or file;

- deletion of the whole message or file;

- insertion of new data or voice signals, deliberately chosen by the attacker;

- re-ordering of messages;

- replay of pre-recorded data or voice signals.

The first five items are combined to the term "modification". According to the penetration points the following threats can be distinguished.

5.3.2.1 Manipulation at the radio interface

Some attacks that lead to this threat [4] can be relatively simple due to the radio characteristics of the TETRA system. Possible attacks are modification of the data sent "in the air" and masquerading as another entity.

- Concerning modification of data "in the air" the following holds: a transmitter sending on the same channel as a mobile station, but with more transmitting power, will always drown out this mobile.

  - This can be done accidentally, as the following scenario shows: mobile station MS1 is sending to base station BS1 and MS2 is sending to BS2 on the same frequency and time slot. MS1 falls into a radio gap, so MS2 is received by BS1. If there is no possibility to distinguish the mobile stations at a very low level, BS1 will handle the data from MS2 as if it were from MS1.

[4] Unless explicitly indicated otherwise, the term "radio interface" is used for the interface between a mobile station and a base station of a TETRA network, i.e. interface I1 in the diagrams of the annex.

  - Of course, this can be done intentionally, too. Depending on the knowledge of the attacker, even very accurate modifications are possible.

  However, not all kinds of modifications mentioned in the list above can be made "on the fly" at the radio interface. The messages cannot be reordered. Data or voice signals can only be deleted indirectly: it should be modified in such a way that the receiver (e.g. voice coder) discards the data because of too many errors. Insertions can only be made in transmitting intervals.

- In order to insert new or pre-recorded data and voice signals, masquerading as a user or base station is possible in the same way as in the case of interception. Due to the radio characteristics replay attacks are particularly easy. It is not even necessary, that the attacker can understand the (possibly enciphered) messages, he/she simply replays them. Even if some authentication mechanisms are applied, it might be possible to thwart the authentication procedure by replaying data (e.g. identifiers and passwords).

  In the case of voice calls where the communicating parties know each other, the only sensible attack seems to be recording of some calls, and then (perhaps after some reordering) replaying of the voice. For calls where the communicating parties do not know each other or if the recognition of the voice cannot be guaranteed, insertion of the own voice of the attacker is possible.

The profit for the attacker depends on the kind of data he/she is manipulating. Random modifications to annoy the users in general are possible (e.g. isolation of a specific user, paralysing of the whole system, see also chapter on the threat "denial of service"), but more specific manipulations usually carry greater advantages:

- Voice, user data:

  the profit for the attacker depends on the significance of the information and can potentially be very high.
- Control data:

  an attacker could change, e.g. the identity of a sender and/or receiver, his/her location, the identity or location of a terminal used, the priority, the header of some data. These changes can be used to misroute some information or to masquerade as another user.

- Management data:

  the attacker might change management data, e.g. to impair the service (e.g. isolation of a node, see subclause 5.5.1). Also, charging information may be manipulated to save money. If security measures are applied, another example is manipulation of authentication data to isolate a user or to masquerade.

These manipulation attacks cannot be prevented by (algorithmic) security mechanisms. All that can be done, is to apply mechanisms that allow the receiver of the signal to detect manipulations with high probability.

5.3.2.2 Manipulation in the fixed parts of the network

In contrast to the radio interface, in the fixed parts of the network [5)] all kinds of manipulation are possible: deletion, reordering and insertion of data is possible without restriction. The underlying attacks can be in principle at least the same as for manipulation at the radio interface, with the following attacks added:

- Manipulations can be done in the following ways:

  - an attacker can use some equipment infiltrated into any interface of the system (see Annex B) to manipulate the data and voice signals being transferred there;

[5)] The term "fixed parts" is used to describe all nodes and links of the network but the mobile station and its interface to the base station. However, not only wired lines can be used in the "fixed part" of a TETRA system, also radio links may be possible. For radio links analogues threats as for the radio interface between mobile station and base station have to be considered.

  - deletion can be carried out, e.g. by physical action like wire-cutting, but also by rerouting of the data (e.g. by manipulation of the data header);

  - an attacker, who has access to an entity in the system, e.g. a base station, can manipulate the data or voice signals being processed or stored, as well;

  - this attacker needs physical access to a network node, e.g. a base station, and good knowledge of the internal working of the system. He/she is likely to be an insider, such as maintenance or operating personnel.

- For masquerading the following holds:

  - somebody might masquerade as a fixed entity of the system at any of its interfaces (see Annex B) to manipulate the through-going data. However, this seems to be more complicated as masquerading as a base station at the radio interface. Besides, these attacks have the disadvantage, that it is necessary to cut existing connections, which might be noticed. Masquerading is possible, e.g. with the help of replay of messages (see subclause 5.3.2.1). The attacker can in principle masquerade as any entity of the system;

  - a special case of the above is the masquerade as a system entity over an interface that is not permanently connected, such as the inter system interface (labelled I5 in Annex B) between two TETRA systems that are connected through a transit network.

The profit for the attacker is in principle the same as for manipulation at the radio interface. However, in the fixed part of the network more data are available to the attacker for manipulations, e.g. some management data not being transmitted over the radio interface.

5.3.3 Repudiation

This threat means, that one of the parties involved in a communication denies (parts of) it. Two kinds of repudiation threats can be distinguished: repudiation of delivery or repudiation of origin. Potential attackers are the normal users of the system, either the sender or the receiver of some message. Therefore, this threat mainly applies to public and private networks where mutual trust between the users cannot always be assumed.

5.3.3.1 Repudiation of delivery

This threat arises in the following situation: one person has sent some message to another person. The message is received by this second person. However, afterwards the receiving person denies the receipt of the message.

EXAMPLE: An attack where the receiver gets some orders (which he/she perhaps does not like) and denies afterwards the receipt of them. From the outside, this can not be distinguished from the case, where an attacker falsely pretends having sent the message.

This attack can be prevented with cryptographic security measures. The sending person gets an undeniable proof, that the intended receiver must have received the data. This proof can be used to convince a third person. A non-cryptographic measure that is usually sufficient in most situations is comprehensive recording of all traffic by a trustworthy centre (in combination with reliable authentication of users).

5.3.3.2 Repudiation of origin

This threat arises in the following situation: one person has sent some message to another person. The message is received by this second person. However, afterwards the sending person denies having sent the message.

- An example is an attack, where a receiver gets some message, e.g. some orders, which the sender afterwards denies having sent. From the outside, this is not distinguishable from the case, where an attacker falsely pretends having received the message.

This attack can be prevented with similar cryptographic security measures as the attack concerning repudiation of delivery. In this case, the receiving person gets an undeniable proof, that the intended person has sent the data. This proof can be used to convince a third person. Comprehensive recording of all traffic by a trustworthy centre (in combination with reliable authentication of users) is an equally applicable measure, as well.

5.4 User related threats

This class of threats comprises those threats that are directed at the users of the system, rather than against individual messages. The following threats can be distinguished: traffic analysis and observability.

5.4.1 Traffic analysis

This threat means, that (part of) the traffic within a network can be analysed. Possible interesting information can be, e.g. the rate of messages, the length of the messages, the sender or receiver identities. It may even be interesting for the attacker to recognize, if some messages are sent at all at a certain time and at a specific interface. Methods to carry out this attack are in general the same as for interception. For this attack, the attacker is typically an outsider of the system.

Of course, encryption of the message content and as much as possible of the control data is a prerequisite for the prevention of traffic analysis. However, even if the traffic is encrypted at a low level (link-to-link), some patterns may be found and used for statistical analysis. Encryption should, therefore, be complemented by other measures like padding of messages and insertion of dummy messages.

5.4.2 Observability

This threat means, that the behaviour of a specific (not necessarily known) user might be observed. The attacker will learn, e.g. when this user makes which calls from what location, to which groups he/she belongs to, which priority he/she has. Analysis of the charging information is possible, too. For an outside attacker, this threat is simply a special case of traffic analysis. However, observability also covers cases where users or operators of the system try to gather information about other users, which they are not supposed to have access to.

The major countermeasure against observability is the use of pseudonyms for anonymous sending, receiving and charging. But even if a pseudonym is used for the identification of the user to the system, the different calls of this user can be interconnected as long as the pseudonym doesn't change. If the attacker then manages to link one of these calls to a specific user (e.g. by calling him/her) he/she can link all these calls to that user.

5.5 System related threats

This class comprises threats that are directed at the system as a whole or at parts of it, rather than against specific users or single messages. The following threats can be distinguished: denial of service and unauthorized use of resources. They are described in the following.

5.5.1 Denial of service

This threat means, that a service is intentionally impaired or made unavailable by an unauthorized attacker from inside or outside the system. Examples for possible attacks are:

- an attacker erases all messages passing through a specific interface. The methods can be the same as for manipulation;

- an attacker delays messages going in one or both directions. The methods can be the same as for manipulation;

- an attacker overflows the system with messages generated by him/herself. This could be done by any normal user of the system;

- an attacker disconnects a node from the system either by manipulating the system configuration or by physical manipulation (e.g. wire cutting);

- an attacker jams on the radio path;

- an attacker can abuse supplementary services.

It is very difficult to protect a system against the numerous possible attacks that lead to denial of service (the above list being far from complete). The most effective ways to protect the system against the effects of intentional impairment are the same that are used to ensure its general availability in the face of accidental failure, i.e. redundancy and flexibility. In addition to this, comprehensive auditing can be an effective deterrent against potential attackers.

5.5.2 Un-authorized use of resources

Two kinds of threats can be distinguished: use of prohibited resources and use of resources beyond the authorized limits. Resources are, e.g. radio channels, equipment, service or system databases.

5.5.2.1 Use of prohibited resources

The user is not allowed to use the resource at all. Possible attacks can be:

- an attacker can masquerade as another user and execute the access rights of this user in order to get access to prohibited resources, e.g. access to the system as a whole, or access to specific services;

- an attacker can use stolen or non-type approved equipment;

- an attacker with sufficient knowledge of the internal working of the system may be able to acquire additional access rights or circumvent access control mechanisms.

The most important countermeasures against this threat are reliable authentication of users and operators and a sound design and implementation of the mechanisms for administration of access rights and enforcement of access control decisions.

5.5.2.2 Use of resources beyond the authorized limits

The user is allowed to use the resource, but goes beyond his/her access rights. Possible attacks can be:

- an attacker might misuse some information he/she got for other purposes, e.g. the network operator or service provider can misuse some personal data of users;

- an attacker who has borrowed some equipment, e.g. a mobile station, and who is allowed to use this equipment only to a certain extent can nevertheless try to excess the limits;

- attacks can be directed against the objective of fair access to the system for all users. This can be done, e.g. by the misuse of priorities or by manipulating a mobile station in such a way, that it always has the first access after a collision with another mobile station on the RACH. In this way, the other users of the system have no equal chance to use the resources.

Protection against this threat requires, in addition to authentication and access control mechanisms, comprehensive auditing of critical activities in the system.

5.6 Summary

In subclauses 5.2 to 5.5 the threats and attacks that might be directed against the TETRA system have been analysed. Due to the existence of a radio interface, some attacks will be easy to perform, if no countermeasures are taken. Examples for such easy attacks are interception of data and masquerading as another user. But the other threats and attacks have to be considered carefully as well, as they may lead to a great damage for the victims.

It is the purpose of the elaboration on security objectives and requirements to decide, for which threats and attacks countermeasures have to be provided. This work will be based on this threat analysis and will take into account the specific requirements of the specific customers. Then, based on the requirements identified, the security architecture can be developed.

6 Security objectives and requirements (TETRA 02.22)

6.1 Introduction

This clause gives the security objectives and requirements for TETRA.

The following players have been identified and are defined in subclause 4.7:

- network operator;
- organization manager;
- dispatcher;
- subscriber;
- user;
- owner of a mobile;
- manufacturer;
- maintenance personnel.

In this clause their security objectives and requirements are analysed. A comprehensive list of objectives and requirements is given for the above players (however, there were no objectives identified for the last two players in the list). To improve readability, listing is done separately for the following classes of security issues:

- correct charging;
- authenticity;
- confidentiality of communication;
- integrity of communication;
- privacy;
- traffic flow confidentiality;
- monitoring;
- protection of resources;
- security management;
- non-repudiation.

A survey of the security objectives is given and the players attached to them. A table that indicates the relative priorities of the security requirements for various types of TETRA networks is also included.

6.2 Description of objectives and requirements

Each of the following subclauses contains a list of security objectives and requirements that apply to the respective security issue. The objectives are ordered according to the players that they are attached to. Objectives are marked with an _ and numbered O-x.y. After each objective, we list the requirements that can be derived from them. Requirements are marked with -> and numbered R-x.y.z.

When reading the lists of objectives and requirements, please keep the following points in mind:

1) objectives and requirements concerning incontestable charging are not considered;
2) Direct Mode (DM) is not covered in this ETR;
3) the objectives and requirements of the dispatcher, when involved in a communication, are the same as those of a user;
4) in many cases the same requirements are held by various players, however, they are not always repeated.

6.2.1 Correct charging

To ensure correct charging is an important security objective, mainly for public systems. The term is meant to comprise the possibly conflicting requirements of the charging entity on one hand and the entities being charged on the other hand.

Network operator:	_	**wants to secure charges towards subscribers:**	O-1.1
	→	Registration of the subscribers	R-1.1.1
	→	Authentication of the subscribers	R-1.1.2
	→	Correct measurement of type and duration of the calls (traffic logs)	R-1.1.3
	→	Protection against masquerading of (part of) the network	R-1.1.4
	_	**wants to secure charges towards other network operators:**	O-1.2
	→	Authentication of other network operators via ISI interface	R-1.2.1
	→	Authentication of subscribers via ISI	R-1.2.2
	→	Integrity (and confidentiality) of charging information	R-1.2.3
	_	**wants to check charging by other network operators:**	O-1.3
	→	Secure information concerning type and duration of the calls (traffic logs, statistics)	R-1.3.1
	→	Check quality of the authentication procedure by the other network operators	R-1.3.2
Organization manager:	_	**wants to check charging concerning his organization:**	O-1.4
	→	Secure information concerning type and duration of the calls (traffic logs, statistics)	R-1.4.1
	→	Check quality of the authentication procedure by network operator	R-1.4.2
Subscriber:	_	**wants to check charging concerning his users:**	O-1.5
	→	Correct measurement of type and duration of the call	R-1.5.1
	→	Registration and authentication	R-1.5.2
User:	_	**wants to check charging concerning his calls:**	O-1.6
	→	Secure advice of charge	R-1.6.1

6.2.2 Authenticity

Authentication of an entity means that a proof of the true identity of that entity is received. To ensure the authenticity of the communicating entities is one of the most basic security objectives in any communication system. There are many different objectives and requirements by each of the various players.

Network operator:	_	**wants to authenticate the organization manager:**	O-2.1
	→	Authentication of organization manager	R-2.1.1
	_	**wants to authenticate other network operators:**	O-2.2
	→	Mutual authentication of network operators	R-2.2.1
Organization manager:	_	**wants to authenticate the users:**	O-2.3
	→	Authentication of users	R-2.3.1
Dispatcher:	_	**wants to authenticate the users:**	O-2.4
	→	Check quality of authentication mechanism from the network operator	R-2.4.1
	→	Receive reports on authentication failures of users	R-2.4.2
	_	**wants to authenticate group membership:**	O-2.5
	→	Registration of group members, incl. late entry	R-2.5.1
	→	Group management tools	R-2.5.2
	→	Secure dynamic group number reassignment	R-2.5.3
	→	Security of remote change of parameters in the mobile	R-2.5.4
	_	**wants to authenticate external connections:**	O-2.6
	→	Authentication of communication partners for outgoing calls	R-2.6.1
	→	Authentication of communication partners for incoming calls	R-2.6.2

Subscriber:	_	**wants to authenticate users of his subscription:**	O-2.7
	→	Authentication of the users of his subscription (local, e.g. by a smart card with a PIN)	R-2.7.1
User:	_	**wants to authenticate the network:**	O-2.8
	→	Terminal should authenticate network entities (e.g. to prevent an illegal base station to disable legal mobiles)	R-2.8.1
	_	**wants to authenticate communication partners:**	O-2.9
	→	Mutual end-to-end authentication of the communication partner)	R-2.9.1
Owner of a mobile:	_	**wants the network to authenticate the mobile (e.g. to prevent misuse):**	O-2.10
	→	Authentication of mobiles by the network	R-2.10.1
	_	**wants the mobile to authenticate the user:**	O-2.11
	→	Authentication of user by the mobile	R-2.11.1

6.2.3 Confidentiality of communication

Confidentiality of communication is provided if the messages transmitted over the system cannot be read by anybody but the intended receivers. A reasonable level of confidentiality is required in any modern radio communication system. High level confidentiality is particularly needed in private systems used by public safety organizations.

Network operator:	_	**wants to ensure the confidentiality of control and management information:**	O-3.1
	→	Encryption of the control channel at the air-interface	R-3.1.1
	→	Encryption of the control and management information within the fixed network	R-3.1.2
Organization manager:	_	**wants to ensure the confidentiality of communication in his organization:**	O-3.2
	→	Encryption of the user channel at the air-interface	R-3.2.1
	→	End-to-end encryption of voice and data	R-3.2.2
Dispatcher:	_	**wants to ensure the confidentiality of communication in his group:**	O-3.3
	→	Prevention of users' bypassing the security functionality	R-3.3.1
User:	_	**wants to ensure the confidentiality of his communication:**	O-3.4
	→	Encryption of the user channel at the air-interface	R-3.4.1
	→	End-to-end encryption of voice and data	R-3.4.2

6.2.4 Integrity of communication

Integrity of communication is provided if the messages transmitted over a system cannot be (accidentally or intentionally) be modified without the receiver's notice. A reasonable level of integrity is required in any modern radio communication system. High level integrity is particularly needed in private systems used by public safety organizations. As there are more possibilities for the manipulation of data than of voice signals, integrity requirements are more important for data communications.

Network operator:	_	**wants to ensure the integrity of control and management information:**	O-4.1
	→	Integrity check of the control channel at the air-interface	R-4.1.1
	→	Integrity check of the control and management information within the fixed network	R-4.1.2
Organization manager:	_	**wants to ensure the integrity of communication in his organization:**	O-4.2
	→	Integrity check of the user channel at the air-interface	R-4.2.1
	→	End-to-end integrity check of data	R-4.2.2
Dispatcher:	_	**wants to ensure the integrity of communication in his group:**	O-4.3
	→	Prevention of users' bypassing the security functionality	R-4.3.1
User:	_	**wants to ensure the integrity of his communication:**	O-4.4
	→	Integrity check of the user channel at the air-interface	R-4.4.1
	→	End-to-end integrity check of data	R-4.4.2
	→	Prevention of replay for voice	R-4.4.3

6.2.5 Privacy

Any communication system has to ensure the privacy of the persons using or operating it, i.e. to prevent misuse of data concerning persons. Due to legal demands, this set of requirements is particularly important in public systems.

Network operator:	_	**has to protect information related to persons according to legal demands:**	O-5.1
	→	Access control to data bases containing personal information	R-5.1.1
	→	Confidentiality of personal information when transmitted	R-5.1.2
	→	Monitoring of forwarding and processing of personal information	R-5.1.3
Organization manager:	_	**has to protect information related to persons within his organization:**	O-5.2
	→	Access control to organization data bases	R-5.2.1
	→	Confidentiality of personal information when transmitted	R-5.2.2
	→	Monitoring of forwarding and processing of personal information	R-5.2.3
Subscriber:	_	**wants his personal information to be protected:**	O-5.3
	→	Access control to subscriber data base	R-5.3.1
	→	Confidentiality of subscriber information when transmitted	R-5.3.2
User:	_	**wants his personal information to be protected:**	O-5.4
	→	Access control to user data base (including SIM)	R-5.4.1
	→	Confidentiality of user information when transmitted	R-5.4.2
	_	**wants to protect his identity while using the system:**	O-5.5
	→	Non-exposure of identity at the air interface	R-5.5.1
	→	Possibility of anonymous call	R-5.5.2

	_	**wants to protect his location while using the system:**	O-5.6
	→	Non-exposure of location information to network provider	R-5.6.1
Owner of the mobile:	_	**wants his personal information to be protected:**	O-5.7
	→	Access control to mobile data base	R-5.7.1

6.2.6 Traffic flow confidentiality

Traffic flow confidentiality is aimed to prevent the disclosure of information that can be inferred from observing traffic patterns, even in the presence of encryption of the message contents. It is typically required in high level security systems, such as private mobile communication systems operated by public safety organizations.

Organization manager:	_	**wants to ensure traffic flow confidentiality within the organization**	O-6.1
	→	Provision and management of covert identities for users, user groups, and subscribers	R-6.1.1
	→	Confidentiality of control information	R-6.1.2
Dispatcher:	_	**wants to ensure traffic flow confidentiality within the group**	O-6.2
	→	Provision and management of covert identities for users and user groups	R-6.2.1
	→	Confidentiality of control information	R-6.2.2
User:	_	**wants to ensure traffic flow confidentiality of his own traffic**	O-6.3
	→	Confidentiality of control information	R-6.3.1
	→	Traffic padding	R-6.3.2
	→	Generation of dummy traffic	R-6.3.3

6.2.7 Monitoring

The ability to monitor the traffic and the communication in the network is a routine requirement for private mobile radio systems. To a more limited extent it applies to public systems, as well. Monitoring is partly in opposition to other security requirements, particularly confidentiality and privacy.

Organization manager:	_	**wants to monitor the traffic and the communication of his organization:**	O-7.1
	→	Authentication of organization manager for monitoring	R-7.1.1
	→	Provision for legal access to encrypted traffic	R-7.1.2
	→	Reports from the network operator on user traffic of his organization	R-7.1.3
Dispatcher:	_	**wants to monitor the traffic and the communication of his group(s):**	O-7.2
	→	Authentication of dispatcher for monitoring or logging of actions	R-7.2.1
	→	Provision for legal access to encrypted traffic	R-7.2.2
User:	_	**wants to monitor the traffic and the communication of his or other groups, when authorized:**	O-7.3
	→	Provision for legal access to encrypted traffic	R-7.3.1

6.2.8 Protection of resources

Protection of resources comprises a very large set of requirements, mainly connected to the field of system reliability rather than security. The following objectives and requirements are those, which are expected to have a potential impact on the design of the security architecture.

Network operator:	_	**wants to protect the infrastructure of the system:**	O-8.1
	→	Protection against unauthorized use of services	R-8.1.1
	→	Protection against unauthorized use of radio resources (e.g. misuse of priorities)	R-8.1.2
	→	Access control to databases	R-8.1.3
	→	Knowledge of the state of every part of the infrastructure	R-8.1.4
	→	Access control for configuration/network management	R-8.1.5
	→	Protection of radio channels (particularly control channels) against jamming	R-8.1.6
	→	Fall-back mode of security in case of network degradation	R-8.1.7
	→	Disabling of terminals	R-8.1.8
Organization manager:	_	**wants to be able to control the use of services**	O-8.2
	→	Management of authorization	R-8.2.1
	→	Enforcement of authorization	R-8.2.2
Dispatcher:	_	**wants to be able to control the use of services**	O-8.3
	→	Real-time control and enforcement	R-8.3.1
	→	Barring of incoming and outgoing external calls	R-8.3.2
	→	Authorization of calls by dispatcher	R-8.3.3
	→	Disabling of terminals	R-8.3.4
Subscriber:	_	**wants to protect the use of his account**	O-8.4
	→	Use of personalized devices (SIM-cards)	R-8.4.1

Owner of the mobile:	_	**wants to protect his mobile**	O-8.5
	→	Protection against misuse of stolen or lost mobiles	R-8.5.1
	→	Blacklist management	R-8.5.2

6.2.9 Security management

The complex security functions within the network call for sophisticated control and management. The management functions are security critical themselves and, therefore, subject to security requirements.

Network operator:	_	**wants to be informed about status of security within the network:**	O-9.1
	→	Recording of security relevant information	R-9.1.1
	→	Alarm functions for security relevant events	R-9.1.2
	→	Intrusion detection	R-9.1.3
	→	Jamming detection	R-9.1.4
	_	**wants to be able to control the security functions within the network:**	O-9.2
	→	Customisation of security functions to users' needs	R-9.2.1
	→	Adaptation of security functions to current situation	R-9.2.2
Organization manager:	_	**wants to be informed about status of security within the network, in particular end-to-end security:**	O-9.3
	→	Recording of security relevant information	R-9.3.1
	_	**wants to be able to control end-to-end security:**	O-9.4
	→	Adaptation of security functions to current situation	R-9.4.1

Dispatcher:	_	**wants to be informed about status of security within the network, in particular end-to-end security:**	O-9.5
	→	Recording of security relevant information	R-9.5.1
	→	Alarm functions for security relevant events	R-9.5.2
	_	**wants to be able to control end-to-end security:**	O-9.6
	→	Adaptation of security functions to current situation	R-9.6.1
User:	_	**wants to be informed about status of security within the network, in particular end-to-end security:**	O-9.7
	→	Indication of security level and state	R-9.7.1
	_	**wants to be able to control end-to-end security:**	O-9.8
	→	Selection and adaptation of security functions to current situation	R-9.8.1

6.2.10 Non-repudiation

The requirements for non-repudiation in most private systems (i.e. with a common point of trust) are covered by subclause 6.2.7. Non-repudiation for public systems is for further study.

6.3 Survey of objectives

The following table 2 gives a survey of all the objectives described in the previous section ordered according to the players that are attached to each objective.

Table 2

wants to	N	O	D	S	U	Ow	SO
secure charges towards subscribers	X						
secure charges towards other network operators	X						
check charging by other network operators	X						
check charging concerning his organization		X					
check charging concerning his users				X			
check charging concerning his calls					X		
authenticate the organization manager	X						
authenticate other network operators	X						
authenticate the users		X	X				
authenticate group membership			X				
authenticate external connections			X				
authenticate users of his subscription				X			
authenticate the network					X		
authenticate communication partners					X		
the network to authenticate the mobile						X	
the mobile to authenticate the user						X	
ensure the confidentiality of control and management information	X						
ensure the confidentiality of communication in his organization		X					
ensure the confidentiality of communication in his group			X				
ensure the confidentiality of his communication					X		
ensure the integrity of control and management information	X						
ensure the integrity of communication in his organization		X					
ensure the integrity of communication in his group			X				
ensure the integrity of his communication					X		
protect information related to persons according to legal demands	X						
protect information related to persons within his organization		X					
his personal information to be protected				X	X		
protect his identity while using the system					X		
protect his location while using the system					X		
his personal information to be protected						X	
ensure traffic flow confidentiality within the organization		X					
ensure traffic flow confidentiality within the group			X				
ensure traffic flow confidentiality of his own traffic					X		

(continued)

Table 2 (concluded)

wants to	N	O	D	S	U	Ow	SO
monitor the traffic and the communication of his organization	X						
monitor the traffic and the communication of his group(s)			X				
monitor the traffic and the communication of his or other groups					X		
protect the infrastructure of the system	X						
be able to control the use of services		X	X				
protect the use of his account				X			
protect his mobile					X		
be informed about status of security within the network	X						
be able to control the security functions within the network	X						
be informed about status of security within the network, in particular end-to-end security		X					
be able to control end-to-end security		X	X	X			
be informed about status of security within the network, in particular end-to-end security			X	X			
Non-Repudiation	?	?	?	?	?	?	?

N	Network operator	X	player has objective
O	Organization manager	?	to be defined
D	Dispatcher		
S	Subscriber		
U	User		
Ow	Owner of mobile		

6.4 Rating of security requirements

The following table indicates the relative priorities of the security requirements listed in subclauses 6.1 to 6.3. Separate priorities are assigned for the cases of public networks, private networks for commercial organizations (e.g. transport company), and private networks for public safety organizations (e.g. police). For networks that are shared between two or more organizations, the priorities can usually be derived by forming the maximum of the priorities for the types of organizations involved and the priorities for public networks.

There are cases where identical or very similar requirements are derived from several objectives. These requirements have received different numbers and are listed separately in the following tables. A cross reference between identical or almost identical requirements is given by the leftmost column. Whenever there is an entry to this column, it points to set of identical or almost identical requirements. The sets are listed in subclause 6.4.10.

NOTE: The priorities given to any of the requirements apply to the requirement in pursuit of the objective it was originally drawn from.

6.4.1 Correct charging

		Public networks			Private networks for commercial organizations			Private networks for public safety		
Requirement		Low	Medium	High	Low	Medium	High	Low	Medium	High
	R-1.1.1			X	X			X		
	R-1.1.2			X	X			X		
a	R-1.1.3			X	X			X		
	R-1.1.4	X			X			X		
b	R-1.2.1		X		X			X		
	R-1.2.2			X	X			X		
	R-1.2.3			X	X			X		
	R-1.3.1		X		X			X		
c	R-1.3.2			X	X			X		
	R-1.4.1		X		X			X		
c	R-1.4.2			X	X			X		
a	R-1.5.1			X	X			X		
	R-1.5.2			X	X			X		
	R-1.6.1		X		X			X		

6.4.2 Authenticity

		Public networks			Private networks for commercial organizations			Private networks for public safety		
Requirement		Low	Medium	High	Low	Medium	High	Low	Medium	High
	R-2.1.1			X			X			X
b	R-2.2.1		X			X				X
	R-2.3.1		X			X				X
c	R-2.4.1		X		X			X		
	R-2.4.2		X			X				X
	R-2.5.1		X			X				X
	R-2.5.2		X			X				X
	R-2.5.3		X			X				X
	R-2.5.4			X		X				X
	R-2.6.1	X			X					X
	R-2.6.2		X			X				X
	R-2.7.1			X		X				X
	R-2.8.1	X			X					X
	R-2.9.1		X			X				X
	R-2.10.1		X		X					X
	R-2.11.1		X		X					X

6.4.3 Confidentiality of communication

		Public networks			Private networks for commercial organizations			Private networks for public safety		
Requirement		**Low**	**Medium**	**High**	**Low**	**Medium**	**High**	**Low**	**Medium**	High
	R-3.1.1		X			X				X
	R-3.1.2	X			X				X	
d	R-3.2.1			X			X			X
e	R-3.2.2	X			X					X
	R-3.3.1		X			X				X
d	R-3.4.1			X			X			X
e	R-3.4.2	X			X					X

6.4.4 Integrity of communication

		Public networks			Private networks for commercial organizations			Private networks for public safety		
Requirement		**Low**	**Medium**	**High**	**Low**	**Medium**	**High**	**Low**	**Medium.**	**High**
	R-4.1.1			X			X			X
	R-4.1.2			X			X			X
f	R-4.2.1	X			X			X		
g	R-4.2.2	X				X				X
	R-4.3.1		X			X				X
f	R-4.4.1	X			X			X		
g	R-4.4.2		X			X				X
	R-4.4.3		X			X				X

6.4.5 Privacy

		Public networks			Private networks for commercial organizations			Private networks for public safety		
Requirement		**Low**	**Medium**	**High**	**Low**	**Medium**	**High**	**Low**	**Medium**	**High**
h	R-5.1.1			X			X			X
j	R-5.1.2			X			X			X
k	R-5.1.3			X			X			X
h	R-5.2.1			X			X			X
j	R-5.2.2			X			X			X
k	R-5.2.3			X			X			X
h	R-5.3.1			X		X				X
j	R-5.3.2			X		X				X
h	R-5.4.1		X		X					X
j	R-5.4.2		X		X					X
	R-5.5.1		X		X					X
	R-5.5.2		X		X			X		
	R-5.6.1		X		X			X		
h	R-5.7.1		X		X			X		

6.4.6 Traffic flow confidentiality

		Public networks			Private networks for commercial organizations			Private networks for public safety		
Requirement		Low	Medium	High	Low	Medium	High	Low	Medium	High
l	R-6.1.1		X			X				X
m	R-6.1.2		X			X				X
l	R-6.2.1		X			X				X
m	R-6.2.2		X			X				X
m	R-6.3.1		X			X				X
	R-6.3.2	X			X				X	
	R-6.3.3	X			X				X	

6.4.7 Monitoring

		Public networks			Private networks for commercial organizations			Private networks for public safety		
Requirement		Low	Medium	High	Low	Medium	High	Low	Medium	High
	R-7.1.1	X				X				X
n	R-7.1.2	X			X					X
	R-7.1.3		X		X			X		
	R-7.2.1	X				X				X
n	R-7.2.2	X			X				X	
n	R-7.3.1	X			X				X	

6.4.8 Protection of resources

		Public networks			Private networks for commercial organization			Private networks for public safety		
Requirement		Low	Medium	High	Low	Medium	High	Low	Medium	High
	R-8.1.1			X		X			X	
	R-8.1.2			X		X				X
	R-8.1.3			X		X				X
	R-8.1.4			X		X				X
	R-8.1.5			X		X				X
	R-8.1.6		X		X					X
	R-8.1.7		X		X					X
	R-8.1.8		X			X				X
	R-8.2.1			X	X				X	
	R-8.2.2			X	X				X	
	R-8.3.1	X			X				X	
	R-8.3.2		X			X			X	
	R-8.3.3		X			X			X	
	R-8.3.4		X			X				X
	R-8.4.1			X	X				X	
	R-8.5.1		X		X					X
	R-8.5.2		X			X				X

6.4.9 Security management

		Public networks			Private networks for commercial organization			Private networks for public safety		
Requirement		Low	Medium	High	Low	Medium	High	Low	Medium	High
p	R-9.1.1			X		X				X
	R-9.1.2		X		X					X
	R-9.1.3		X		X				X	
	R-9.1.4		X		X				X	
	R-9.2.1	X			X				X	
q	R-9.2.2		X			X			X	
p	R-9.3.1		X			X				X
q	R-9.4.1	X			X				X	
p	R-9.5.1		X			X				X
	R-9.5.2	X			X					X
q	R-9.6.1		X			X				X
	R-9.7.1	X			X					X
	R-9.8.1	X			X				X	

6.4.10 Classes of identical or almost identical requirements

a) R-1.1.3, R-1.5.1;

b) R-1.2.1, R-2.2.1;

c) R-1.3.2, R.1.4.2, R-2.4.1;

d) R-3.2.1, R-3.4.1;

e) R-3.2.2, R-3.4.2;

f) R-4.2.1, R-4.4.1;

g) R-4.2.2, R-4.4.2;

h) R-5.1.1, R-5.2.1, R-5.3.1, R-5.4.1, R-5.7.1;

j) R-5.1.2, R-5.2.2, R-5.3.2, R-5.4.2;

k) R-5.1.3, R-5.2.3;

l) R-6.1.1, R-6.2.1;

m) R-6.1.2, R-6.2.2, R-6.3.1;

n) R-7.1.2, R-7.2.2, R-7.3.1;

p) R-9.1.1, R-9.3.1, R-9.5.1;

q) R-9.2.2, R-9.4.1, R-9.6.1.

7 Security services (TETRA 02.23)

7.1 Introduction

The purpose of this clause is to define the standardized security services of a TETRA system. A security service represents a well-defined part of the abstract functionality provided by the system to enhance its overall security quality. Considerations about protocols and algorithms that have to be employed to provide these services are not covered by this ETR.

The clause is structured as follows. Subclause 7.2 gives a survey of all possible areas of security that possibly could be relevant to TETRA systems. Of course, not all of them will be covered by this ETR. The security services that have been selected for standardization are listed under the heading of the area where they belong to. The detailed description of those services is given in subclause 7.2. For this purpose the services are grouped into sections according to their functional relations. Annex A contains tables that show the relevance of the security requirements identified in Clause 6 to the various areas.

7.2 Survey of possible areas for the standardization of security

In this subclause a list of possible areas for the standardization of security within TETRA is given. For each area the security services and functions that will be described in this subclause is given.

a) **End-to-end security:** this area comprises security services for user channels between terminals. The following service will be standardized:

A.1: Information confidentiality for voice (end-to-end).

b) **Air-interface security:** this area comprises security services for user channels on the air-interface between mobile terminals and the TETRA infrastructure. The following service will be standardized:

B.1: Information confidentiality for voice (air-interface).

c) **Signalling security:** this area comprises security services for signalling channels between terminals and the TETRA infrastructure. The following services will be standardized:

C.1: User identity confidentiality;
C.2: Group identity confidentiality;
C.3: Signalling information confidentiality;
C.4: Data integrity and data origin authentication for signalling data.

d) **End-to-end key management:** this area comprises security services for key management for end-to-end security services between terminals.

e) **Air-interface key management:** this area comprises security services for key management for security functions on the air-interface between mobile terminals and the TETRA infrastructure. The following service will be standardized:

E.1: Air-interface key management service.

f) **Local key management:** this area comprises security services for key management for security functions between user and terminal.

g) **End-to-end authentication:** this area comprises security services for authentication between communication partners (users).

h) **Air-interface authentication:** this area comprises security services for authentication on the air-interface between users/terminals and the TETRA infrastructure. The following services will be standardized:

H.1: Authentication of user (air-interface);
H.2: Authentication of TETRA infrastructure (air-interface).

j) **Local authentication:** this area comprises security services for authentication between user and terminal.

k) **Access control to services:** this area comprises security services for access to services.

l) **Non-repudiation:** this area comprises security services for non-repudiation. This area is for further study.

m) **Inter-system security:** this area comprises security services to protect the interworking of different TETRA systems.

n) **Jamming countermeasures:** this area comprises security services to protect against the effects of jamming. This area is still under study.

p) **Correct charging:** this area comprises security services to guarantee correct charging. This area is still under study.

q) **System management:** this area comprises security services to protect the security of system management.

r) **Organizational procedures:** this area comprises organizational security procedures that will, however, not be standardized.

7.3 Description of security services

7.3.1 Confidentiality services

7.3.1.1 General aspects

The general purpose of confidentiality services for TETRA is to protect sensitive data, either stored or transmitted from deliberate or accidental disclosure to an individual, entity or process not authorized to have knowledge of that data.

Looking at the way confidentiality is provided from an abstract point of view shows that it relies on two transformations:

- the hide transformation that protects data from deliberate or accidental disclosure; and

- the reveal transformation that allows to undo the hiding transformation.

For many instances, the hide/reveal transformation will be just an encrypt/decrypt. However, the concept is more general since confidentiality can also be provided, e.g. by access control mechanisms for stored data or procedures for hiding traffic patterns.

To become applicable, the hide/reveal transformations require in general some supplementary data (e.g. cipher keys). The properties of the supplementary data are influenced among others by the characteristics of the data to be protected, the related hide/reveal transformation, etc. The supplementary data itself, its generation, distribution, storage and deletion will often need to be protected against disclosure.

7.3.1.2 Relations to other security services

Authentication: confidentiality, in particular the establishment of a confidential channel, is tightly related to the authentication. In general, the latter provides for the supplementary data (e.g. as a result of a challenge-response procedure or provided by a Certification Authority) being subsequently used by the authenticated parties for a confidentiality-protected communication.

Data integrity and data origin authentication: basically, integrity and confidentiality of data are independent features. It may well be that while the integrity of some information is mandatory, its secrecy is optional or unnecessary and vice versa. However, it is well known that by properly adding redundancy to messages, confidentiality may provide for their integrity.

Access control: access control in conjunction with authentication may provide for confidentiality of stored data. Often this protection is considered sufficient.

7.3.1.3 Information confidentiality for voice (End-to-End) - A.1

What does the service provide?

Confidentiality of voice signals between two or more terminals.

On what information is the service applied?

This applies to voice signals after encoding in the terminal and before forward error correction (on the sending side).

Instance of invocation: individually per call.

Origin of invocation: this service is invoked by one of the communicating parties.

Effect of invocation in case of success: establishment of an uninterrupted confidential channel between two users or a group of users.

Effect of invocation in case of failure: it is mandatory to inform the user about the failure. Any other actions depend on the security policy in force.

Threats covered: this service can prevent the unauthorized interception of voice signals in any part of the system (see subclauses 5.3.1.1 and 5.3.1.2).

Requirements concerned: R-3.2.2, R-3.4.2 End-to-end encryption of voice and data.

Relations to other services: the establishment of a confidential channel requires a previous authenticated key exchange or distribution (end-to-end) between the terminals.

Additional information: none.

7.3.1.4 Information confidentiality for voice (air-interface) - B.1

What does the service provide?

Confidentiality of voice signals between a mobile terminal and the TETRA infrastructure.

On what information is the service applied?

This applies to voice signals after encoding and before forward error correction (on the sending side).

Instance of invocation: this service is mandatory invoked for each call.

Origin of invocation: this service is invoked by the TETRA infrastructure.

Effect of invocation in case of success: establishment of a confidential channel between a mobile terminal and the TETRA infrastructure.

Effect of invocation in case of failure: it is mandatory to inform the user about the failure. Any other actions depend on the security policy in force.

Threats covered: this service can prevent the unauthorized interception of voice signals at the air-interface (see subclauses 5.3.1.1).

Requirements concerned: R-3.2.1, R-3.4.2 Encryption of the user channel at the air interface.

Relations to other services: the establishment of a confidential channel requires a previous authenticated key exchange or distribution between the mobile terminal and the base station.

Additional information: none.

7.3.1.5 User identity confidentiality - C.1

The individual user identity has the special role to provide a unique identification of the user. The user identity is transferable and can be removed from the equipment by the user.

What does the service provide?

The user identity confidentiality is the property that the Individual TETRA Subscriber Identity (ITSI) or Individual Short Subscriber Identity (ISSI) is not made available or disclosed to unauthorized individuals, entities or processes.

This feature provides privacy of the identities of the users who are using TETRA network resources (e.g. traffic channel or any signalling means).

On what information is the service applied?

This service applies to the ITSI or ISSI.

Instance of invocation: individually per call.

Origin of invocation: this service is invoked during the mobility management procedures in MS: registration with or without authorization and with identity exchange at roaming and migration. If registration is granted a new identity is sent to the MS which will be used in subsequent communications.

This applies for all signalling sequences on the radio path.

Effect of invocation in case of success: the ITSI is transmitted at registration, with identity exchange, it is then being replaced by the Alias TETRA Subscriber Identity (ATSI) assuming registration (and eventually authentication) are granted. The ISSI is replaced by the Alias Short Subscriber Identity (ASSI). The ATSI/ASSI is translated by the infrastructure to the correct ITSI/ASSI to gain access to the correct entry of the user data base.

An ATSI cannot be derived from the knowledge of the ITSI and the user is known to other users by his ITSI. If a valid ATSI/ASSI is available it should be used in place of the ITSI/ISSI.

In case of migration an ATSI (but not the ITSI) can be given by the visited network.

Effect of invocation in case of failure: in case of failure where no ASSI is available, then open identification is available using the ITSI during registration. The ITSI is encrypted.

Threats covered: this service protects against reuse of ITSI/ISSI, reduces the possibility of tracing the location of a mobile user by listening to the signalling exchanges on the radio path and also protects against unauthorized access to the user data base (see subclauses 5.4.1 and 5.5.2.1).

Requirements concerned: R-5.1.2, R-5.2.2, R-5.3.2, R-5.4.2 Confidentiality of personal information when transmitted.

R-5.5.1 Non-exposure of identity at the air-interface.

Relations to other services: it allows for improvement of user data confidentiality.

Additional information: none.

7.3.1.6 Group identity confidentiality - C.2

One or more Group TETRA Subscriber Identities (GTSI) or Group Short Subscriber Identities (GSSI) may be allocated in addition to the ITSI. The GTSI may be pre-allocated (like ITSIs) or allocated dynamically by the network using the supplementary service Dynamic Group Number Assignment (DGNA). There is no equivalent of the ATSI with the GTSI.

All the TSIs should be held in non-volatile memory but the TSIs are non-permanent and can be changed by the user.

The same GTSI may be allocated to several ITSIs.

Group and individual identities have the same structure and are allocated from the same subdomain. GTSIs are allocated by the network.

There is no confidentiality of the GTSI itself which is transmitted as it is on the air-interface but the GTSI cannot be derived from the ITSI and reverse, and a given group user should only be known by the other users by his GTSI.

A supplementary service Dynamic Group Number Assignment (DGNA) allows to modify through the air-interface the GTSI (under design).

As a conclusion there is no explicit service related to group identity confidentiality except possible use of DGNA.

Group identity can be protected by part of the signalling information confidentiality.

Threats covered: the threat relates to the availability or possible disclosure of the GTSI and GTSI content.

Requirements concerned: R-5.1.2, R-5.2.2, R-5.3.2, R-5.4.2 Confidentiality of personal information when transmitted.

R-5.5.1 Non-exposure of identity at the air-interface.

Relations to other services: authentication.

Additional information: Other TETRA identities:

TMI: TETRA Management Identity. This identity is allocated to a terminal before it can be used. It cannot be exchanged dynamically or transferred. The TMI should only be used as an address by the internal network management functions.

Secure networks may restrict the use of TMI.

TEI: TETRA Equipment Identity. It identifies one piece of TETRA equipment and is allocated by the equipment manufacturer. A management entity can ask the TEI which is unique.

TEI interrogation should be carried out with protection of the signalling. The removal of the device or access to the TEI should disable the equipment or its use.

7.3.1.7 Signalling information confidentiality - C.3

What does the service provide?

Confidentiality of all logical signalling channels at the air-interface of a TETRA network.

On what information is the service applied?

This applies to all control information at the air-interface of a TETRA network.

Instance of invocation: invocation after registration of a mobile station.

Origin of invocation: this service is invoked by the TETRA infrastructure.

Effect of invocation in case of success: establishment of an uninterrupted confidential control channel between the TETRA infrastructure and mobile station.

Effect of invocation in case of failure: actions depend on the security policy in force, e.g.:

Information to the user in case of failure: in case of failure where no confidential control channel is available to the mobile station, a new registration is necessary.

Threats covered: interception of control signals at the air-interface (see subclauses 6.1.1, 5.4.1 and 7.1).

Requirements concerned: R-3.1.1 Encryption of the control channel at the air-interface.

R-5.1.2, R-5.2.2, R-5.3.2, R-5.4.2	Confidentiality of personal information when transmitted.
R-5.5.1	Non-exposure of identity at the air-interface.
R-6.1.2, R-6.2.2, R-6.3.1	Confidentiality of control information.

Relations to other services: the establishment of a confidential channel requires a previous authenticated key exchange or distribution between the mobile station and the TETRA infrastructure (during registration?).

Additional information: none.

7.3.2 Authentication [6] and key management services

7.3.2.1 General aspects

Authentication of an entity means that a proof of the true identity of that entity is received. Authentication can be mutual, from the transmitter to the receiver and vice versa, or just unilateral, depending on what is required. Authentication takes place at the beginning of the call and is, depending on the used mechanism, valid only for that instance or during the entire call. In the first case it can be desirable to regularly repeat the authentication procedure in order to be sure that the communication still takes place between the same entities.

Key management is the generation, distribution, selection, deletion and administration of cryptographic keys used for authentication and encryption of the information on all communication channels. Secure distribution of keys cannot take place without mutual authentication of the entities that transmit and receive the keys. Key management and authentication are therefore closely related. Described are the key management functions that are used by various security services.

7.3.2.2 Relations to other security services

Confidentiality: confidentiality services can generally be provided only after a successful authentication of the parties involved and the provision of the security parameters and the required keys.

Data Integrity and Data Origin Authentication: data integrity and data origin authentication services can generally be provided only after a successful authentication of the parties involved and the provision of the security parameters and the required keys.

Access Control: in most cases access control decisions are based of the identity of the entity claiming access to a resource. Thus, authentication is a necessary prerequisite for the enforcement of these decisions.

7.3.2.3 Authentication of user (air-interface) - H1

What does the service provide?

Authentication of the user identity to the TETRA infrastructure.

On what information is the service applied?

This applies to the user identity or the group identity.

Instance of invocation: at registration and repeatedly after that, depending on the security policy.

Origin of invocation: this service is invoked by the TETRA infrastructure.

Effect of invocation in case of success: the user is admitted to the TETRA infrastructure when authorized.

[6] The term "authentication here is used in the sense of "authentication of an entity" as opposed to "data origin authentication".

Effect of invocation in case of failure: the user is not admitted to the TETRA infrastructure.

Threats covered: this service protects against the threats that can be carried out by masquerading as another user: i.e. unauthorized interception and manipulation of information at the radio interface, as well as unauthorized use of resources (see subclauses 5.3.1.1, 5.3.2.1 and 5.5.2).

Requirements concerned: R-1.1.2, R-1.5.2, R-2.3.1 Authentication of users and subscribers.

There are many more requirements that indirectly affect this service through other security services that rely on authentication (cf. following paragraph).

Relations to other services: air-interface security services, signalling security services and access control can only be invoked after a successful authentication on the air-interface.

Additional information: none.

7.3.2.4 Authentication of TETRA infrastructure (air-interface) - H2

What does the service provide?

Authentication of the TETRA infrastructure to the user.

On what information is the service applied?

This applies to the TETRA infrastructure identity.

Instance of invocation: at registration and repeatedly after that, depending on the security policy.

Origin of invocation: this service is invoked by the mobile terminal.

Effect of invocation in case of success: the user is sure about the TETRA infrastructure identity and will access the TETRA infrastructure.

Effect of invocation in case of failure: the user is not sure about the TETRA infrastructure identity and will not access the TETRA infrastructure.

Threats covered: this service protects against the threats that can be carried out by masquerading as another TETRA infrastructure: i.e. unauthorized interception and manipulation of information at the radio interface, as well as unauthorized use of resources (see subclauses 5.3.1.1, 5.3.2.1 and 5.5.2).

Requirements concerned: R-1.1.4, R-2.8.1 Authentication of network entities.

There are many more requirements that indirectly affect this service through other security services that rely on authentication (cf. following paragraph).

Relations to other services: air-interface security services, signalling security services and access control can only be invoked after a successful authentication on the air-interface.

Additional information: none.

7.3.2.5 Air-interface key management service - E1

The air-interface key management service is divided into functions that are used by the air-interface authentication services and functions that are used by air interface confidentiality and integrity services.

7.3.2.5.1 Key management functions for air-interface authentication

What do the functions provide?

Distribution and deletion of the keys to be used for air-interface authentication.

On what information are the functions applied?

Control channel information.

Instance of invocation: at registration and repeatedly after that, depending on the security policy.

Origin of invocation: these functions are invoked by the TETRA infrastructure (authentication of user) or the mobile terminal (authentication of TETRA infrastructure).

Effect of invocation in case of success: authentication can take place.

Effect of invocation in case of failure: no authentication can take place so the user is not admitted to the TETRA infrastructure or the user is not sure about the identity of the TETRA infrastructure and will not access the TETRA infrastructure.

Threats covered: key management does not directly prevent any threats. Indirectly the same threats are covered as indicated in the sections on air-interface authentication

Requirements concerned: there are no requirements that directly affect key management. It is indirectly affected by the same requirements as air-interface authentication services.

Relations to other services: these functions are used by all air-interface authentication services that require keys.

Additional information: none.

7.3.2.5.2 Key management functions for air-interface confidentiality and integrity services

What do the functions provide?

Distribution, selection and deletion of the keys to be used for air-interface confidentiality and/or integrity on the user channel and/or the control channel.

On what information is the service applied?

User channel and/or control channel information.

Instance of invocation: at registration and repeatedly after that, depending on the security policy.

Origin of invocation: these functions are invoked by the TETRA infrastructure.

Effect of invocation in case of success: establishment of a confidential user channel and/or control channel.

Effect of invocation in case of failure: the user channel and/or control channel will use the previous key (this is notified to the dispatcher) or else will be in clear mode (this is notified to the user and the dispatcher). Depending on the security policy, the functions are invoked repeatedly after that until successful.

Threats covered: key management does not directly prevent any threats. Indirectly the same threats are covered as indicated in the sections on air-interface confidentiality and integrity.

Requirements concerned: there are no requirements that directly affect key management. It is indirectly affected by the same requirements as air-interface confidentiality and integrity services.

Relations to other services: these functions are used by all air-interface confidentiality and integrity services that require keys.

Additional information: none.

7.3.3 Integrity services

7.3.3.1 General aspects

Data integrity is defined as the assurance that source data is maintained identically at the receiver, including protection against malicious interference with data.

Data origin authentication is the process of verifying the true identity of the data source and its eligibility to originate specific classes of information.

7.3.3.2 Relations to other security services

Authentication: data integrity and data origin authentication services are useful only if the communicating parties are authenticated. The authentication procedure can be used to provide security parameters and the required keys.

Confidentiality: in some cases (i.e. if the data contain enough redundancy), a confidentiality service can provide for data integrity and data origin authentication, also.

7.3.3.3 Data integrity and data origin authentication for signalling data - C4

What does the service provide?

This service allows assurance and checking of the integrity of control information between terminals and the TETRA infrastructure and provides the means for assuring the origin of such information.

Control information includes relevant management information.

On what information is the service applied?

This applies to all control information between terminals and the TETRA infrastructure.

Instance of invocation: at registration and per call.

Origin of invocation: this is invoked at all exchanges of control information.

Effect of invocation in case of success: establishment of requested services.

Effect of invocation in case of failure: actions depend on the security policy in force.

Threats covered: all kinds of manipulation of control information at the air interface including spoofing by replaying of historical data. This kind of action can lead to, e.g. to impersonation of authorized users by unauthorized users, deception of charging functions or by-passing of security functionality (see subclauses 5.3.2.1 and 5.5.2).

Requirements concerned: R-4.1.1 Integrity check of the control channel at the air-interface.

Relations to other services: the successful completion of this service is essential to allow any other services to be invoked.

Additional information: none.

Annex A (informative): Tables of requirements

The following tables indicate which of the security requirements identified in Clause 6 influence the services of each of the standardization areas that were discussed in this ETR. Refer to Clause 6 for decoding the numbered requirements.

A.1 Correct charging

Requirement	Service areas															
	a	b	c	d	e	f	g	h	j	k	l	m	n	p	q	r
R-1.1.1					•									•		
R-1.1.2					•			•								
R-1.1.3														•		
R-1.1.4					•			•								
R-1.2.1												•				
R-1.2.2												•				
R-1.2.3												•				
R-1.3.1														•		
R-1.3.2																•
R-1.4.1														•		
R-1.4.2																•
R-1.5.1														•		
R-1.5.2					•			•						•		
R-1.6.1														•		

A.2 Authenticity

Requirement	Service areas															
	a	b	c	d	e	f	g	h	j	k	l	m	n	p	q	r
R-2.1.1															•	
R-2.2.1												•				
R-2.3.1				•	•		•	•								
R-2.4.1																•
R-2.4.2															•	
R-2.5.1				•											•	
R-2.5.2															•	
R-2.5.3				•			•								•	
R-2.5.4					•			•							•	
R-2.6.1				•			•								•	
R-2.6.2				•			•								•	
R-2.7.1						•			•							
R-2.8.1					•			•								
R-2.9.1				•			•									
R-2.10.1					•			•								
R-2.11.1						•			•							

A.3 Confidentiality of communication

Requirement	Service areas															
	a	b	c	d	e	f	g	h	j	k	l	m	n	p	q	r
R-3.1.1			•		•			•								
R-3.1.2														•		
R-3.2.1		•			•			•								
R-3.2.2	•			•			•									
R-3.3.1														•		
R-3.4.1		•			•			•								
R-3.4.2	•			•			•									

A.4 Integrity of communication

Requirement	Service areas															
	a	b	c	d	e	f	g	h	j	k	l	m	n	p	q	r
R-4.1.1			•		•			•								
R-4.1.2														•		
R-4.2.1		•			•			•								
R-4.2.2	•			•			•									
R-4.3.1														•		
R-4.4.1		•			•			•								
R-4.4.2	•			•			•									
R-4.4.3	•			•			•									

A.5 Privacy

Requirement	Service areas															
	a	b	c	d	e	f	g	h	j	k	l	m	n	p	q	r
R-5.1.1															•	
R-5.1.2			•		•			•							•	
R-5.1.3															•	•
R-5.2.1															•	
R-5.2.2			•		•			•							•	
R-5.2.3															•	•
R-5.3.1															•	
R-5.3.2			•		•			•							•	
R-5.4.1															•	
R-5.4.2			•		•			•							•	
R-5.5.1			•		•			•								
R-5.5.2														•	•	
R-5.6.1															•	
R-5.7.1															•	

A.6 Traffic flow confidentiality

Requirement	Service areas															
	a	b	c	d	e	f	g	h	j	k	l	m	n	p	q	r
R-6.1.1															•	
R-6.1.2	•		•	•	•		•	•								
R-6.2.1															•	
R-6.2.2	•		•	•	•		•	•								
R-6.3.1	•		•	•	•		•	•								
R-6.3.2	•	•	•	•	•		•	•								
R-6.3.3	•	•	•	•	•		•	•								

A.7 Monitoring

Requirement	Service areas															
	a	b	c	d	e	f	g	h	j	k	l	m	n	p	q	r
R-7.1.1															•	
R-7.1.2				•											•	
R-7.1.3															•	
R-7.2.1															•	
R-7.2.2				•											•	
R-7.3.1				•											•	

A.8 Protection of resources

Requirement	Service areas															
	a	b	c	d	e	f	g	h	j	k	l	m	n	p	q	r
R-8.1.1					•			•		•						
R-8.1.2					•			•								
R-8.1.3															•	
R-8.1.4															•	•
R-8.1.5															•	
R-8.1.6													•			
R-8.1.7															•	
R-8.1.8			•		•			•								
R-8.2.1															•	
R-8.2.2															•	
R-8.3.1				•			•			•						
R-8.3.2				•			•			•						
R-8.3.3				•			•			•						
R-8.3.4															•	
R-8.4.1						•			•							
R-8.5.1						•			•						•	
R-8.5.2															•	

A.9 Security management

Requirement	Service areas															
	a	b	c	d	e	f	g	h	j	k	l	m	n	p	q	r
R-9.1.1															•	
R-9.1.2															•	
R-9.1.3															•	
R-9.1.4													•			
R-9.2.1															•	
R-9.2.2															•	
R-9.3.1															•	
R-9.4.1															•	
R-9.5.1															•	
R-9.5.2															•	
R-9.6.1															•	
R-9.7.1															•	
R-9.8.1															•	

A.10 Non-repudiation

Requirements concerning non-repudiation have been left for further study.

Annex B (informative): TETRA V+D and PDO interfaces

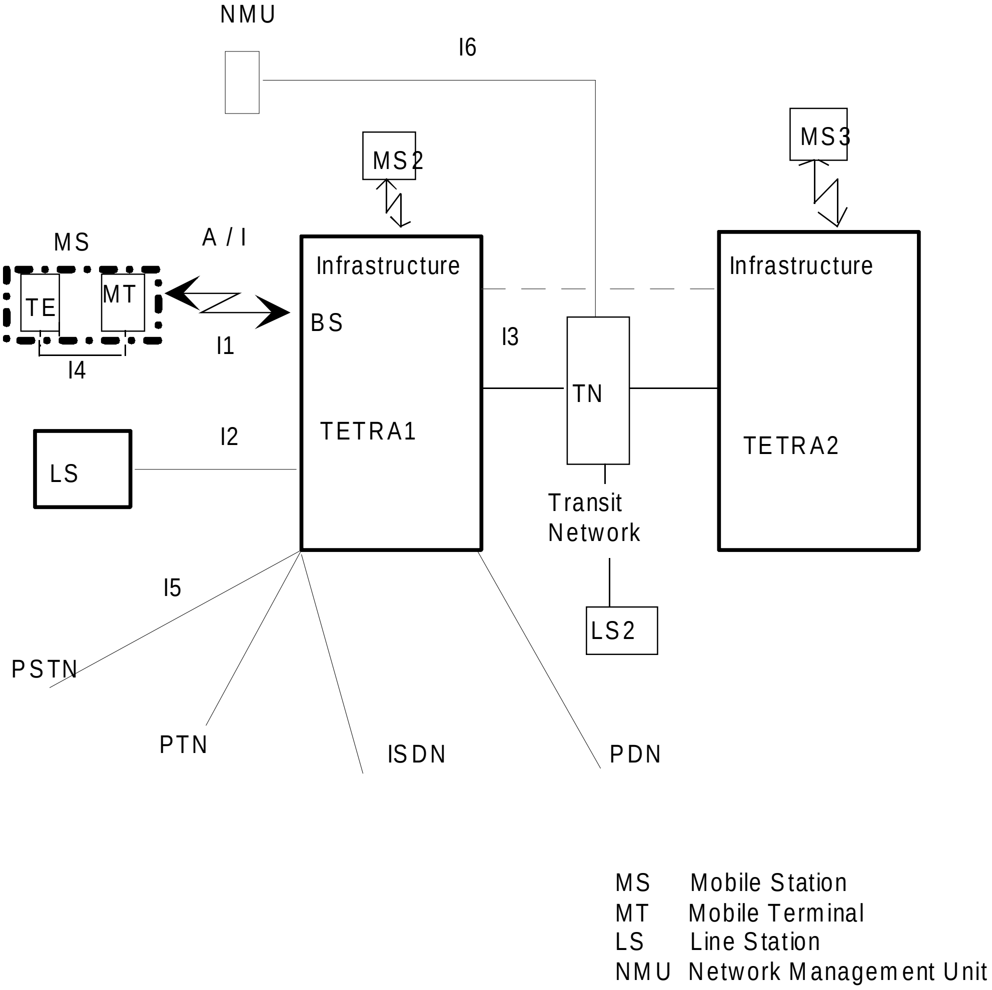
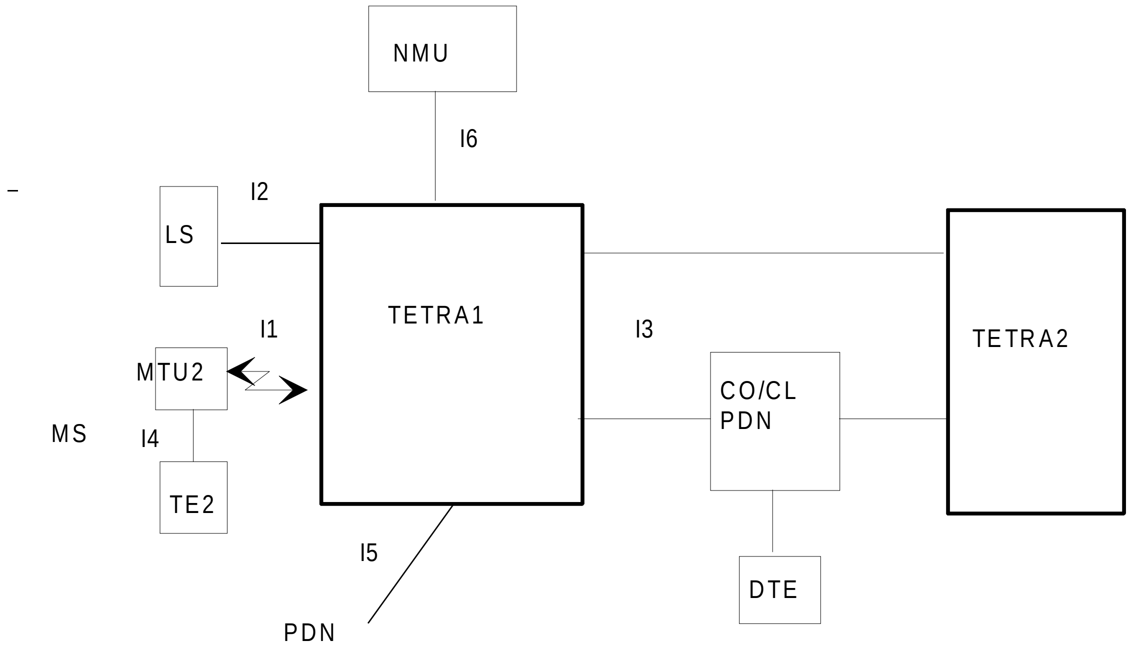


Figure B.1: TETRA V+D interfaces



CO/CL	Connection/Connectionless
PDN	Public Data Network
DTE	Data Terminal Equipment
MTU2	Mobile Terminal Unit
TE	Terminal Equipment

Figure B.2: TETRA PDO interfaces

History

Document history	
January 1994	First Edition
October 1995	Converted into Adobe Acrobat Portable Document Format (PDF)