SLOVENSKI STANDARD
PSIST ETR 086-3:1999

01-julij-1999

Vseevropski sistem snopovnega radia (TETRA) - Specifikacija tehniļ nih zahtev - 3. del: Varnostni vidiki

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

Ta slovenski standard je istoveten z: ETR 086-3 Edition 1

ICS:

33.070.10	Prizemni snopovni radio (TETRA)	Terrestrial Trunked Radio (TETRA)

PSIST ETR 086-3:1999 en

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