SLOVENSKI STANDARD
SIST EN 301 040 V2.0.0:2003

01-december-2003

Prizemni snopovni radio (TETRA) – Varnost – Vmesnik za zakonito prestrezanje (LI)

Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface

Ta slovenski standard je istoveten z: **EN 301 040 Version 2.0.0**

ICS:

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

SIST EN 301 040 V2.0.0:2003 **en**

EN 301 040 V2.0.0 (1999-06)

European Standard (Telecommunications series)

Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface

Reference
DEN/TETRA-06027-1 (9mo01000.PDF)

Keywords
TETRA, security, voice, data

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Project Terrestrial Trunked Radio (TETRA).

National transposition dates	
Date of adoption of this EN:	25 June 1999
Date of latest announcement of this EN (doa):	30 September 1999
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 March 2000
Date of withdrawal of any conflicting National Standard (dow):	31 March 2000

1 Scope

The present document describes the implementation of a Lawful Interception interface in a TETRA system. It provides the requirements and specification of the interface within a TETRA system for the purpose of providing data to Law Enforcement Agencies (LEAs) in the area of Lawful Interception (LI) of communications.

The provision of a Lawful Interception interface for TETRA is a national option, however where it is provided it shall be provided as described in the present document.

The structure of lawful interception in telecommunications is in two parts: The internal interface of a network that is built using a particular technology; and, the external interface (known as the Handover Interface) that links the LEA to the network. Between these two parts may lie a mediation function to cater for national variances and delivery of the result of interception.

The Handover Interface may be the subject of national regulation and therefore the mediation function may be a matter of national regulation.

The subject of the present document is the internal LI interface that lies between the TETRA infrastructure and the mediation function.

The present document describes the data content of information flows from the TETRA system to the mediation function. It does not describe a communications protocol stack but assumes the use of one with entry made at layer 7 (application layer). The present document has been written with ROSE as a target layer 7 protocol and with the ASN.1 Basic Encoding Rules (BER) as the target layer 6 (presentation) protocol. To facilitate this the data definitions are made with ASN.1. This method allows configuration of either local or remote mediation functions. The EN does not specify how ROSE and BER are used.

The present document is structured as follows:

- clause 4 outlines the essential requirements for the TETRA LI interface;
- clause 5 presents the structural and behavioural models of the LI interface;
- clause 6 presents the data model and allocation behaviour in the LI interface.

The present document applies to TETRA services where access to the communication of TETRA Subscriber Identities (TSIs) is available in a network (Switching and Management Infrastructure (SwMI) or Radio Packet Data Infrastructure (RPDI)). Whilst this does not prohibit lawful interception of TETRA Direct Mode Operation (DMO) it removes the liability of network operators and service providers to provide a result of interception when communication does not make use of their networks.

The present document describes the normal and exceptional operation in each of the three operational phases of T-LI:

1 Setup:

The actions taken within the TETRA network to establish the monitoring of a target and the communications paths to the mediation function.

2 Monitoring:

The monitoring of target activity and its delivery to the mediation function.

3 Cleardown:

The removal of a monitor facility against a target and the cleardown of the communications paths to the mediation function.

The present document does not describe the means of transporting data from the TETRA network to the LEA, but describes only the means of capturing and encoding the activities of a target within the TETRA network and delivering this data to the mediation function.

The present document does not define the operations or technical requirements of the Handover Interface that takes data from the mediation function to the LEMF.

The present document does not define the operations or technical requirements of the Law Enforcement Monitoring Facility (LEMF).

NOTE 1: The present document presupposes some familiarity with the operation of TETRA systems and of lawful interception.

NOTE 2: The present document suggests a barrier to external manipulation of the TETRA infrastructure by means of a mediation function.

NOTE 3: No testpoint is provided in the present document to ensure conformance. This is addressed national standards pending the completion of a common handover interface being developed by ETSI TC SEC-LI in ES 201 671 [8] and to which the present document is provided as input.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] Official Journal of the European Communities, 99/C329/01: "Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications".

[2] ETR 331: "Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".

[3] ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[4] ETS 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

[5] ETS 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[6] ISO/IEC 8348 (1996): "Information technology - Open Systems Interconnection - Network Service Definition".

[7] ISO/IEC 8878 (1992): "Information technology - Telecommunications and information exchange between systems - Use of X.25 to provide the OSI Connection-mode Network Service".

[8] ES 201 671: "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

call: any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunication system where at least one of the parties to the call(for the purposes of the present document) is a user of a TETRA system.

content of communication: information exchanged between two or more users of a telecommunications service where at least one of the users is accessing the service in a TETRA network whilst a call is established, excluding intercept related information. This includes information which may, as part of some TETRA service, be stored by one user for subsequent retrieval by another.

NOTE 1: The user in the above definition may be any addressable entity in the TETRA domain using either a TSI [3] or some other valid network address (undefined).

Coordinated Universal Time (UTC): time scale maintained by the Bureau International de l'Heure (International Time Bureau) that forms the basis of a coordinated dissemination of standard frequencies and time signals.

NOTE 2: The source of this definition is Recommendation 460-2 of the Consultative Committee on International Radio (CCIR). CCIR has also defined the acronym for Coordinated Universal Time as UTC.

co-target: correspondent of the target (i.e. the individual or group address with whom the target is communicating).

identity: technical label which may represent the origin or destination of any TETRA traffic, as a rule clearly identified by a physical communication identity number (such as a telephone number) or the logical or virtual communication identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis.

intercept related information: collection of information or data associated with TETRA services involving the target, specifically call associated information or data, service associated information or data (e.g. service profile management by subscriber) and location information.

Interception (OR Lawful Interception): action (based on the law), performed by a network operator/service provider, of making available certain information and providing that information to an LEMF.

NOTE 3: In the present document the term interception is not used to describe the action of observing communications by an LEA.

interception interface: physical and logical locations within the network operator's/service provider's TETRA facilities where access to the content of communication and intercept related information is provided. The interception interface is not necessarily a single, fixed point.

interception measure: technical measure which facilitates the interception of TETRA traffic pursuant to the relevant national laws and regulations.

interception subject: person or persons, specified in a lawful authorization, whose communications are to be intercepted.

Law Enforcement Agency (LEA): organization authorized by a lawful authorization based on a national law to receive the results of communication interceptions.

Law Enforcement Monitoring Facility (LEMF): law enforcement facility designated as the transmission destination for the results of interception relating to a particular interception subject.

lawful authorization: permission granted to an LEA under certain conditions to intercept specified communication and requiring co-operation from a network operator/service provider. Typically this refers to a warrant or order issued by a lawfully authorized body.

LI interface: physical and logical interface across which the results of interception are delivered from a network operator/service provider to a LEMF.

NOTE 4: In ETR 331 [2] this interface is termed the handover interface. The term handover is used in TETRA systems to describe the maintenance of a call when the mobile party moves between cells.

location information: information relating to the geographic, physical or logical location of an identity relating to an interception subject.

mediation function: function that lies between the LEA and the TETRA SwMI that translates data from the SwMI for use by the collection function of the LEA. The mediation function may be resident in the TETRA SwMI and is specified by the protocols and data on the interface to the TETRA SwMI (as defined in the present document) and to the collection function (as defined by the LEA).

multi-user gateway: reserved address given to a gateway port that is used only for intermediate call support, e.g. ISDN gateway.

Private Mobile Radio (PMR): radio system designed for a closed user group.

Public Access Mobile Radio (PAMR): radio system available to members of the general public generally by subscription. The owner and operator are unlikely to be the same as the user.

Public Network Operator (PNO): operator of a public infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means.

Quality of Service (QoS): quality specification of a TETRA channel, system, virtual channel, computer-TETRA session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

reliability: probability that a system or service will perform in a satisfactory manner for a given period of time when used under specific operating conditions.

result of interception: information relating to a target service, including the content of communication and intercept related information, which is passed by a network operator or service provider to an LEA. Intercept related information may be provided whether or not call activity is taking place.

served user: user receiving the intercepted traffic.

service provider: natural or legal person providing one or more public communication services whose provision consists wholly or partly in the transmission and routing of signals on a network. A service provider need not necessarily run his own network.

NOTE 5: To avoid confusion the term TETRA service provider may be used to distinguish the operator of a TETRA system from the service provider in traditional public networks.

target: identity associated with a target service (see below) used by the interception subject.

Target Group TETRA Subscriber Identity (GTSI): identity associated with a target service (see below) used by the interception subject where the interception subject is a group.

target service: communication service associated with an interception subject and usually specified in a lawful authorization for interception.

NOTE 6: There may be more than one target service associated with a single interception subject.

Target Terminal Equipment Identity (TEI): identity associated with a target service (see above) used by the interception subject where the interception target is an equipment.

telecommunication: any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASSI	Assigned Short Subscriber Identity
BER	Basic Encoding Rules
CCIR	Consultative Committee on International Radio
CGI	Cell Global Identification
CONS	Connection Oriented Network Service
DMO	Direct Mode Operation
DSS1	Digital Subscriber Signalling System No. one
GTSI	Group TETRA Subscriber Identity
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITSI	Individual TETRA Subscriber Identity
LA	Location Area
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LII	Lawful Interception Interface
MF	Mediation Function
MNI	Mobile Network Identity
MS	Mobile Station
PAMR	Public Access Mobile Radio
PISN	Public Integrated Services Network
PMR	Private Mobile Radio
PNO	Public Network Operator
PSS1	Private Signalling System number one
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RPDI	Radio Packet Data Infrastructure
SCLNS	Specific ConnectionLess Network Service
SDL	Service and Description Language
SDS	Short Data Service
SS	Supplementary Service
SSI	Short Subscriber Identity
SwMI	Switching and Management Infrastructure
TEI	TETRA Equipment Identity
TSI	TETRA Subscriber Identity
TETRA	Terrestrial Trunked Radio
UTC	Coordinated Universal Time
VC	Virtual Circuit

4 User (LEA) requirements - the administrative interface

This clause presents the user requirements derived from [1] and specifically related to the lawful interception of TETRA with the LEA being the user.

The network operator/service provider shall use best endeavours at all times to comply with the requirements of the LEA. The specific information to be made available shall be made clear by the LEA.

The present document describes the internal LI interface of a TETRA network, and does not specify the means by which data is delivered to the LEA or to its designated Law Enforcement Monitoring Facility (LEMF). However the internal LI interface is defined in such a way that data may be carried transparently on most networks.

NOTE: In this context "internal" means within the boundary of the TETRA infrastructure. The boundary may extend in such a manner that the TETRA LI function is remote from other components of the SwMI, or it may be co-located with other SwMI components.

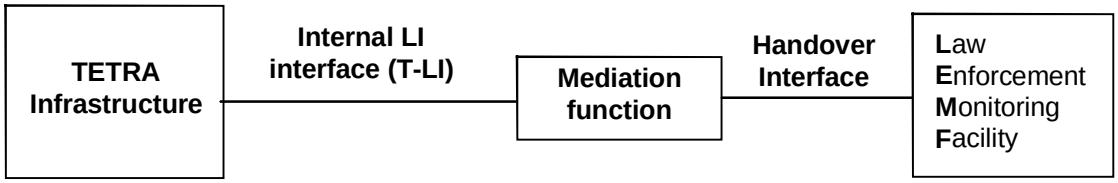

Figure 1: General reference model of lawful interception from user perspective

The general reference model of figure 1 shows that the overall LI interface lies between the LEMF and the TETRA infrastructure. The subject of the present document is the internal LI interface that lies between the TETRA infrastructure and the mediation function.

4.1 Non-disclosure

The network operator/service provider and the LEA should jointly agree confidentiality on the manner in which interception measures are implemented in a given TETRA installation with the manufacturers of the technical installations for the implementation of interception measures.

Information relating to target identities and target services to which interception is being applied at any time in the life of the TETRA installation and as defined thereafter by the LEA should not be made available to unauthorized persons.

4.2 Identification of the identity to be intercepted

The target may be any valid TETRA Subscriber Address (TSI). If the TSI is used for group communication it shall be referred to as a Group TSI (GTSI), if used for an individual it shall be referred to as an Individual TSI (ITSI). The address space of TETRA is "flat" so there is no reserved address space for either GTSIs or ITSIs. A multi-user gateway should not be allowed to be a target.

If the target is an individual (ITSI) it is possible that the target may belong to one or more groups. Groups of which the target is a member shall be identified as those groups to which the target's ITSI has made a group attachment. The attachment that identifies these groups may be requested by the MS with the target's ITSI, enforced by the SwMI or a permanent attachment; and provision shall be made for interception of communications within groups to which the target's ITSI is attached by any of these means. The group communications should cease being intercepted after such time that the SwMI deems the MS to no longer be attached to the group, e.g. by specific detachment, de-registration etc.

In some instances network addresses (TSIs) may be provided in blocks to user groups (e.g. to fleet operators). The network operator/service provider shall make every effort to identify an unique target identity based upon data present in the original warrant. If the network operator/service provider is unable to map an unique address to the characteristics of the target defined in the interception warrant the LI interface shall not be invoked.

In some instances the target may be a particular equipment identified by its Terminal Equipment Identity (TEI). The network operator/service provider shall use best endeavours to identify a target TSI. This may require the network operator/service provider to invoke the Mobility Management (MM) service and to use the TEI PROVIDE protocol exchange to identify the ITSI using the target equipment. The present document does not impose a mandate for the support in TETRA systems of this protocol. The use of such a service should not break the rules of service transparency given in subclause 4.6.

4.3 Result of interception

4.3.1 Network validity of result of interception

A network operator/service provider shall only provide a result of interception for targets operating in their network irrespective of the target belonging to that network. If an interception target migrates to a second TETRA network there shall be no requirement for the home network operator/service provider to provide a result of interception from the visited network.

4.3.2 Identification of result of interception

The result of interception provided at the LEMF side of the LI interface shall be given a unique identification that shall allow identification of the LEA, the target, network operator/service provider and the warrant reference.

The internal interface shall in addition provide a unique identification to correlate the data to be submitted to the LEMF with the internal interception provision.

4.3.3 Format of result of interception

The network operator/service provider shall, prior to delivery of the result of interception:

1) remove any air interface encryption, scrambling and channel coding;

2) provide the LEA with decrypted material for applications where relevant keys and algorithms are available.

The content of real time communication shall be provided as a verbatim bit stream. In particular no speech transcoding shall be applied (in the TETRA SwMI), and where appropriate TETRA encoded speech shall be provided to the MF.

4.3.4 Content of result of interception

The result of interception shall contain:

- the content of all calls originated by the target;
- the content of all calls addressed to the target;
- the content of multi-party calls in which to the best knowledge of the network operator/service provider the target is participating;
- the content of broadcast calls to a user population of which to the best knowledge of the network operator/service provider the target is a member.

In addition the result of interception shall contain:

1) the identities that have attempted communication with the target, successful or not;

2) the identities that the target has attempted communication with, successful or not;

3) identities used by or associated with the target;

4) details of services used and their associated parameters;

5) those signals emitted by the target invoking additional or modified services;

6) time-stamps for identifying the beginning, end and duration of the connection;

7) actual destination and intermediate directory numbers if call has been diverted;

8) location information;

9) advice of charge for provision of result of interception.

The result of interception shall apply to all call types if, and as long as, to the best knowledge of the network operator/service provider, the target is a participant.

For group calls, the GTSI shall be identified as being used by the ITSI where to the best knowledge of the network operator/service provider the target is a participant in the group. This may be achieved by recording the ATTACH/DETACH GROUP IDENTITY messages that dynamically associate an ITSI to a GTSI, or by defining an ITSI as always attached to a group. If a group requires dynamic attachment and the target has not explicitly attached then there is no association of ITSI to GTSI for that group.

NOTE: For further explanation of this topic see ETS 300 392-2 [4], subclauses 14.5.2 and 16.8.

4.3.5 Auditing of result of interception

In order to prevent, and to trace, misuse of the technical functions integrated in the TETRA installation enabling interception, any activation or application of these functions in relation to a given identity shall be fully recorded, including any activation or application caused by faulty or unauthorized input. The records should cover some or all of the following items:

1) the identity of target;
2) the target service(s) concerned;
3) the LEMF to which the result of interception is routed;
4) an authenticator suitable to identify the operating personnel (including date and time of input);
5) a reference to the lawful authorization.

The network operator/service provider should ensure that the records are tamper-proof and only accessible by authorized individuals in accordance with local laws relating to data privacy.

4.4 Location information

A network operator shall provide to the best of their knowledge any location information that may be requested by the LEA and addressed within the initiating warrant. Such data should be within the normal operating parameters of the TETRA network and may take one or more of the following forms:

1) the current location area (or base station if available) at which the target is registered;
2) the current line identity associated with a registered target;
3) the line or service identity to which the target is currently registered and to which calls are redirected.

The location information should be delivered at one or more of the following times:

1) with registration;
2) with result of interception;
3) as specified by the LEMF.

4.5 Time constraints

The result of interception shall be made available during the period specified by the interception warrant, at the LEMF side of the LI interface.

A network operator shall provide data for new calls from the time commencing no earlier than the time at which the interception request is received.

The instance of the LI interface and communication shall be established to the LEMF as quickly as possible after issue of an interception warrant. Thereafter the result of interception shall be delivered to the LI interface on a real-time or near real-time basis.