ETSI EN 300 392-3-9 V1.2.1 (2020-04)

Terrestrial Trunked Radio (TETRA);
Voice plus Data (V+D);
Part 3: Interworking at the Inter-System Interface (ISI);
Sub-part 9: Transport layer independent, General design

Reference
REN/TCCE-03257

Keywords
management, mobility, TETRA

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - 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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

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 ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

The present document is part 3, sub-part 9 of a multi-part deliverable covering the Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D), as identified below:

Part 1: "General network design";

Part 2: "Air Interface (AI)";

Part 3: "Interworking at the Inter-System Interface (ISI)":

Sub-part 1: "General design";

Sub-part 2: "Additional Network Feature Individual Call (ANF-ISIIC)";

Sub-part 3: "Additional Network Feature Group Call (ANF-ISIGC)";

Sub-part 4: "Additional Network Feature Short Data Service (ANF-ISISDS)";

Sub-part 5: "Additional Network Feature for Mobility Management (ANF-ISIMM)";

Sub-part 6: "Speech format implementation for circuit mode transmission";

Sub-part 7: "Speech Format Implementation for Packet Mode Transmission";

Sub-part 8: "Generic Speech Format Implementation";

Sub-part 9: "Transport layer independent, General design";

Sub-part 10: "General design, PSS1 over E.1";

Sub-part 11: "General design, SIP/IP";

Sub-part 12: "Transport layer independent Additional Network Feature Individual Call (ANF-ISIIC)";

Sub-part 13: "Transport layer independent Additional Network Feature Group Call (ANF-ISIGC)";

Sub-part 14: "Transport layer independent Additional Network Feature Short Data Service (ANF-ISISDS)";

Sub-part 15: Transport layer independent Additional Network Feature, Mobility Management (ANF-ISIMM)";

Part 4: "Gateways basic operation";

Part 5: "Peripheral Equipment Interface (PEI)";

Part 7: "Security";

Part 9: "General requirements for supplementary services";

Part 10: "Supplementary services stage 1";

Part 11: "Supplementary services stage 2";

Part 12: "Supplementary services stage 3";

Part 13: "SDL model of the Air Interface (AI)";

Part 14: "Protocol Implementation Conformance Statement (PICS) proforma specification";

Part 15: "TETRA frequency bands, duplex spacings and channel numbering";

Part 16: "Network Performance Metrics";

Part 17: "TETRA V+D and DMO specifications";

Part 18: "Air interface optimized applications";

Part 19: "Interworking between TETRA and Broadband systems".

NOTE 1: Part 3, sub-parts 6 and 7 (Speech format implementation), part 4, sub-part 3 (Data networks gateway), part 10, sub-part 15 (Transfer of control), part 13 (SDL) and part 14 (PICS) of this multi-part deliverable are in status "historical" and are not maintained.

NOTE 2: Some parts are also published as Technical Specifications such as ETSI TS 100 392-2 and those may be the latest version of the document.

The present document is based on ETSI EN 300 392-3-1 "Interworking at the Inter-System Interface (ISI); General Design" [i.6]. The main differences are:

- Any transport protocol (PSS1) information is removed as several different transport protocols can be used.
- Any reference to ROSE ([i.4] and [i.5]) is removed and the necessary description of the PDU identification has been added.
- The ASN.1 specification of the PDUs has been re-designed taking into account that the reference to ROSE is removed.

For all subparts in the TETRA specification ETSI EN 300 392-3 "Interworking at the Inter-System Interface (ISI)" [3], [4], [5], [6], [7], [8] and [9] the terms ISI and TETRA ISI are equivalent.

National transposition dates	
Date of adoption of this EN:	13 November 2019
Date of latest announcement of this EN (doa):	31 July 2020
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 January 2021
Date of withdrawal of any conflicting National Standard (dow):	31 January 2021

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines the general aspects of interworking at the Inter-System Interface (ISI) for Terrestrial Trunked Radio (TETRA) system supporting Voice plus Data (V+D). Those specify the general concepts which are the basis of the ISI operation between TETRA systems. It introduces the Additional Network Features (ANFs) used at the ISI, and specifies:

- the general protocol mechanism upon which the definition of each ANF is based; and
- the security related functions over the ISI.

The specification of the general transport layer independent protocol mechanism applies to any TETRA Switching and Management Infrastructure (SwMI) which supports the ISI. The security requirements for the ISI only apply to SwMIs which support authentication or end-to-end encryption over the ISI.

Besides the ISI general design, the present sub-part, interworking at the Inter-System Interface comprises the following other sub-parts:

- General design, PSS1 over E.1 [3];
- General design, SIP/IP [4];
- Transport layer independent Additional Network Feature Individual Call (ANF-ISIIC) [5];
- Transport layer independent Additional Network Feature Group Call (ANF-ISIGC) [6];
- Transport layer independent Additional Network Feature Short Data Service (ANF-ISISDS) [7];
- Transport layer independent Additional Network Feature, Mobility Management (ANF-ISIMM) [8]; and
- Generic Speech Format Implementation [9].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE 1: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

NOTE 2: Note that for the TETRA standards, the reference is always to a European Standard (ETSI EN 300 xxx) if such has been published, but the latest version of that standard can be either an EN or a Technical Specification (ETSI TS 100 xxx), even if this is not visible in the reference list.

The following referenced documents are necessary for the application of the present document.

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

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

[3] ETSI EN 300 392-3-10: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 10: General design, PSS1 over E.1".

[4] ETSI EN 300 392-3-11: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 11: General design, SIP/IP".

[5] ETSI EN 300 392-3-12: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 12: Transport Layer Independent Additional Network Feature Individual Call (ANF-ISIIC)".

[6] ETSI EN 300 392-3-13: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 13: Transport layer independent Additional Network Feature Group Call (ANF-ISIGC)".

[7] ETSI EN 300 392-3-14: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 14: Transport Layer Independent Additional Network Feature Short Data Service (ANF-ISISDS)".

[8] ETSI EN 300 392-3-15: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 15: Transport layer independent Additional Network Feature, Mobility Management (ANF-ISIMM)".

[9] ETSI EN 300 392-3-8: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 8: Generic Speech Format Implementation".

[10] ETSI EN 302 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".

[11] ETSI EN 300 392-9: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 9: General requirements for supplementary services".

[12] Recommendation ITU-T X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

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

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE 1: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

NOTE 2: Note that for the TETRA standards, the reference is always to a European Standard (ETSI EN 300 xxx) if such has been published, but the latest version of that standard can be either an EN or a Technical Specification (ETSI TS 100 xxx), even if this is not visible in the reference list.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EN 300 395-1: "Terrestrial Trunked Radio (TETRA); Speech CODEC for full-rate traffic channel; Part 1: General description of speech functions".

[i.2] Recommendation ITU-T I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[i.3] Recommendation ITU-T Z.100: "Specification and description language (SDL)".

[i.4] Recommendation ITU-T X.219: "Remote Operations: Model, notation and service definition".

[i.5] Recommendation ITU-T X.229: "Remote Operations: Protocol specification".

[i.6] ETSI EN 300 392-3-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 1: General design".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

call independent: property of information which is conveyed between SwMI on a signalling connection which is not related to an audio call

call independent signalling connection: signalling connection established between ANF-ISI entities located in different Switching and Management Infrastructures that is not related to audio calls

destination SwMI: Switching and Management Infrastructure where the receiving ANF-ISI entity is located (in the context of a single one-way exchange of information between two ANF-ISI entities located in different Switching and Management Infrastructures)

Group TETRA Subscriber Identity (GTSI): TETRA Subscriber Identity assigned to a group

home SwMI: home of the MS's ITSI, i.e. the SwMI where the network code (MNC) is equal to that of the individual subscriber (ITSI)

invocation: action taken by the user or by the service provider to execute a specific service function within real time

ISI mediation function: entity which provides to different ANF-ISI entities the services that are not supported by the transport layer protocol

Location Area (LA): area within radio coverage of a base station or group of base stations within which a Mobile Station (MS) is allowed to operate

Mobile Network Identity (MNI): identity that identify the SwMI

NOTE: It consists of the Mobile Country Code (MCC) and the Mobile Network Code (MNC).

Mobile Station (MS): physical grouping that contains all of the mobile equipment that is used to obtain TETRA services

NOTE: By definition, a mobile station contains at least one Mobile Radio Stack (MRS).

originating SwMI: in the context of a TETRA call, Switching and Management Infrastructure where the calling user is registered (which implies that this user is located in that SwMI) or Switching and Management Infrastructure which originates a Call independent signalling connection

segmentation: act of generating two or more transport layer PDUs derived from one initial ISI PSU

service user: abstract representation of the totality of those entities in a single system that makes use of a service through a single access point

Short Subscriber Identity (SSI): network specific portion of a TSI

NOTE: A SSI is only unique within one TETRA sub-domain (one TETRA network).

source SwMI: switching and management infrastructure where the sending ANF-ISI entity is located (in the context of a single one-way exchange of information between two ANF-ISI entities located in different Switching and Management Infrastructures)

subscriber: user of a telecommunication service, based on a contract with the provider of the service

NOTE 1: The subscriber may be an individual or a group: in the first case it is identified by an ITSI, in the second, by a GTSI.

NOTE 2: The individual subscriber is able to access an SwMI either through a MS or Line Station.

supplementary service: service which modifies or supplements a basic bearer service or a basic teleservice

NOTE: 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

terminating SwMI: in the context of a TETRA call, Switching and Management Infrastructure where the called user is registered (which implies that this user is located in that SwMI) or Switching and Management Infrastructure which terminates a Call independent signalling connection

TETRA Subscriber Identity (TSI): global TETRA network address that is to identify an individual or a group subscriber within the domain of all TETRA networks

user: entity using the services of a telecommunications network via an externally accessible service access point

NOTE: An individual user may be a person or an application process.

visited SwMI: TETRA network which MNI is not equal to the user's MNI

3.2 Symbols

Void.

3.3 Abbreviations

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

(V)ASSI	Visiting Alias Short Subscriber Identity
(V)GSSI	Visiting Group Short Subscriber Identity
AC	Authentication Centre
AI	Air Interface
ANF	Additional Network Feature
ANF-ISI	all Additional Network Features of the Inter-System Interface
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
ASSI	Alias Short Subscriber Identity
BER	Basic Encoding Rules
BS	Base Station
C	Conditional
CAD	Call Authorized by Dispatcher
CCK	Common Cipher Key
C-LDB	Controlling Linking DataBase
CLIR	Calling Line Identification Restriction
DCK	Derived Cipher Key
DMO	Direct Mode Operation
GCK	Group Cipher Key
GFP	Generic Functional Protocol
G-HDB	Group Home DataBase
GSSI	Group Short Subscriber Identity
GTSI	Group TETRA Subscriber Identity
G-VDB	Group Visited DataBase
HAC	Home Authentication Centre
HDB	Home DataBase
I-HDB	Individual Home DataBase
IP	Internet Protocol
ISI	Inter-System Interface
ISIGC	Inter-System Interface Group Call
ISIIC	Inter-System Interface Individual Call

ISIMM	Inter-System Interface Mobility Management
ISISDS	Inter-System Interface Short Data Service
ISISS	Inter-System Interface Supplementary Services
ITSI	Individual TETRA Subscriber Identity
ITU-T	International Telecommunication Union - sector Telecommunication
I-VDB	Individual Visited DataBase
K	authentication Key
KS	Key Seed
LA	Location Area
LDB	Linking DataBase
LS	Line Station
M	Mandatory
MCC	Mobile Country Code
MM	Mobility Management
MNC	Mobile Network Code
MNI	Mobile Network Identity
MRS	Mobile Radio Stack
MS	Mobile Station
O	Optional
OTAR	Over The Air Re-keying
PDU	Protocol Data Unit
PEI	Peripheral Equipment Interface
PICS	Protocol Implementation Conformance Statement
P-LDB	Participating Linking DataBase
ROSE	Remote Operation Service Element
RS	Random Seed
SAP	Service Access Point
SCK	Static Cipher Key
SDL	Specification and Description Language
SDS	Short Data Service
SIP	Session Initiation Protocol
SS	Supplementary Service
SSI	Short Subscriber Identity
SwMI	TETRA Switching and Management Infrastructure
TETRA	TErrestrial Trunked RAdio
TSI	TETRA Subscriber Identity
V+D	Voice plus Data
VAC	Visitor Authentication Centre
VDB	Visitor DataBase

4 ISI standardization methodology

4.1 3 stage methodology

The ISI Additional Network Features (ANFs), listed in clause 7, are standardized using the modelling method defined in Recommendation ITU-T I.130 [i.2].

4.2 Stage Descriptions

4.2.1 Stage 1 description

Stage 1 description defines the services which the standardized ANF entity provides to the concerned service users, e.g. SwMI entities in the case of TETRA. The services are visible at the Service Access Points (SAPs). The stage 1 description is intended to allow an understanding of the services independently from the implementation.

For normal point to point services the service model is shown in figure 4.1.

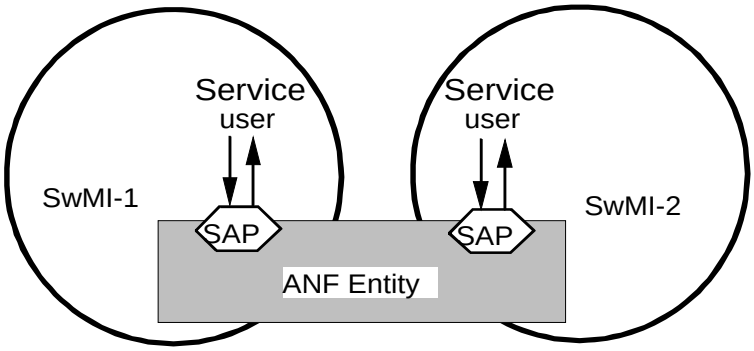


Figure 4.1: Service model for point to point services

Point to point services may span several SwMIs in a raw with each their Service user.

For point to multipoint services the service model is shown in figure 4.2.

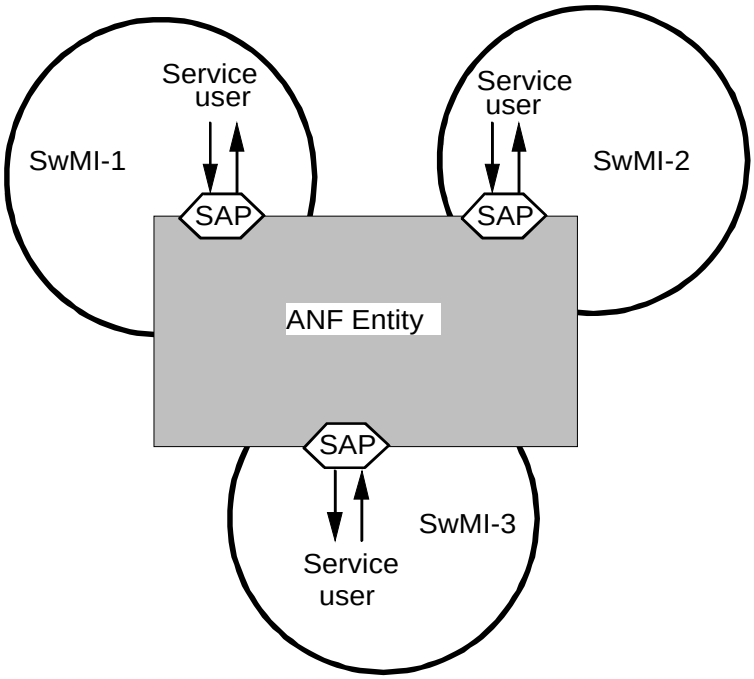


Figure 4.2: Service model for point to multipoint services

Point to multipoint services may span 2 or more SwMIs where one of the SwMIs is communicating with all the other SwMIs and the other SwMIs are not aware of each other, e.g. in a group call the controlling SwMI communicates with all participating SwMIs but the participating SwMIs are only communicate with the controlling SwMI.

4.2.2 Stage 2 description

Stage 2 description identifies the functional capabilities and the information flows needed to support the service as described in stage 1.

4.2.3 Stage 3 description

Stage 3 description gives a precise specification of the signalling protocols for the ANF services, i.e. the encoding rules for the information flows and the corresponding procedures.

4.3 Usage of Specification and Description Language (SDL)

SDL defined in Recommendation ITU-T Z.100 [i.3] is used to identify and represent the behaviour of the concerned ANF in providing services.

5 TETRA SwMI roles using ISI

5.1 Management configurations

5.1.1 Migration and group attachment configurations

5.1.1.1 SwMI roles for migration and group attachment

In order to support the Mobility Management (MM) functionality in different SwMIs for a given subscriber (whether individual subscriber or group), the following SwMI roles are defined:

- individual subscriber home SwMI: The Mobile Network Identity (MNI) of the individual subscriber home SwMI shall be equal to the extended part of the TSI of the subscriber;
- individual subscriber visited SwMI: The Mobile Network Identity (MNI) of the individual subscriber visited SwMI is different from the extended part of the TSI of that subscriber (since this SwMI is different from the individual subscriber home SwMI;
- group home SwMI: The Mobile Network Identity (MNI) of the group home SwMI shall be equal to the extended part of the TSI of the group;
- group visited SwMI: The Mobile Network Identity (MNI) of the group visited SwMI shall be different from the extended part of the TSI of the group.

5.1.1.2 SwMI databases

In order to support the individual subscriber and group MM functionality in the SwMIs, the following databases are defined:

- the HDB comprises information about the individual and/or group subscribers. It is located in the subscriber's home SwMI. The HDB is divided into Individual HDB (I-HDB) and Group HDB (G-HDB):
  - I-HDB contains the location tracking amongst SwMIs, i.e. in which SwMI is an individual subscriber currently located. In addition, the I-HDB is able to provide the basic and optionally the supplementary service migration profiles of the individual subscriber at migration;
  - G-HDB contains the group attachment tracking amongst SwMIs, i.e. which SwMIs are group attached. In addition, the G-HDB is able to provide the basic and optionally the supplementary service migration profiles of the group (subscriber) at group attachment;
- the VDB comprises temporary information about individual and/or group subscribers. For a given individual subscriber member of one or more groups, it is located in the SwMI where that subscriber is registered (be it his home SwMI or a visited SwMI). The VDB is divided into Individual VDB (I-VDB) and Group VDB (G-VDB):
  - I-VDB contains the Individual TETRA Subscriber Identity (ITSI) and Visiting Short Subscriber Alias Identity ((V)ASSI) association (if the individual subscriber is located in a visited SwMI) and the location tracking for the individual subscriber within the SwMI. In addition, the I-VDB is able to provide the basic and optionally the supplementary service profiles of the individual subscriber;
  - G-VDB contains the Group TETRA Subscriber Identity (GTSI) and Visiting Short Subscriber Group Identity ((V)GSSI) association(if located in a group visited SwMI) and the identities of the individual subscribers attached to the group in the SwMI. In addition, the G-VDB is able to provide the basic and optionally the supplementary service migration profiles of the attached group;

- the Authentication Centre (AC) in the home SwMI, i.e. Home Authentication Centre (HAC), may provide the authentication and Over The Air Re-keying (OTAR) parameters for the migrating individual subscriber. Similarly, the AC in the visited SwMI, i.e. the Visitor Authentication Centre (VAC), may contain the authentication and OTAR parameters provided by the home SwMI MM for the migrating individual subscriber. The HAC and the VAC are used in conjunction with the security services as described in clause 8.

NOTE: For ISI mobility configuration, the ACs (HAC and VAC) are considered as databases.

5.1.1.3 Migration scenarios

The migration is the act for an individual subscriber of moving from a Location Area (LA) in the network where that subscriber is currently registered (i.e. does have an I-VDB record) to a new LA in another network (either with different Mobile Network Code (MNC) and/or Mobile Country Code (MCC)) - where that subscriber is not registered.

Such migration from the ANF-ISI point of view shall take place:

- when an individual subscriber moves from one SwMI to another, i.e. from the SwMI where it was previously registered to a new one (be it his home SwMI or a visited SwMI);
- at power on, when the individual subscriber requests registration (migration) in a SwMI different from his home SwMI; or
- at power on, when the individual subscriber requests registration in the home SwMI and was registered at power off in another SwMI.

NOTE: From the mobile station point of view a registration is always required at power on; therefore the mobile station need not remember where it was registered at power off.

Figure 5.1 illustrates the ISI configuration when an individual subscriber migrates from a previous visited SwMI to new one.

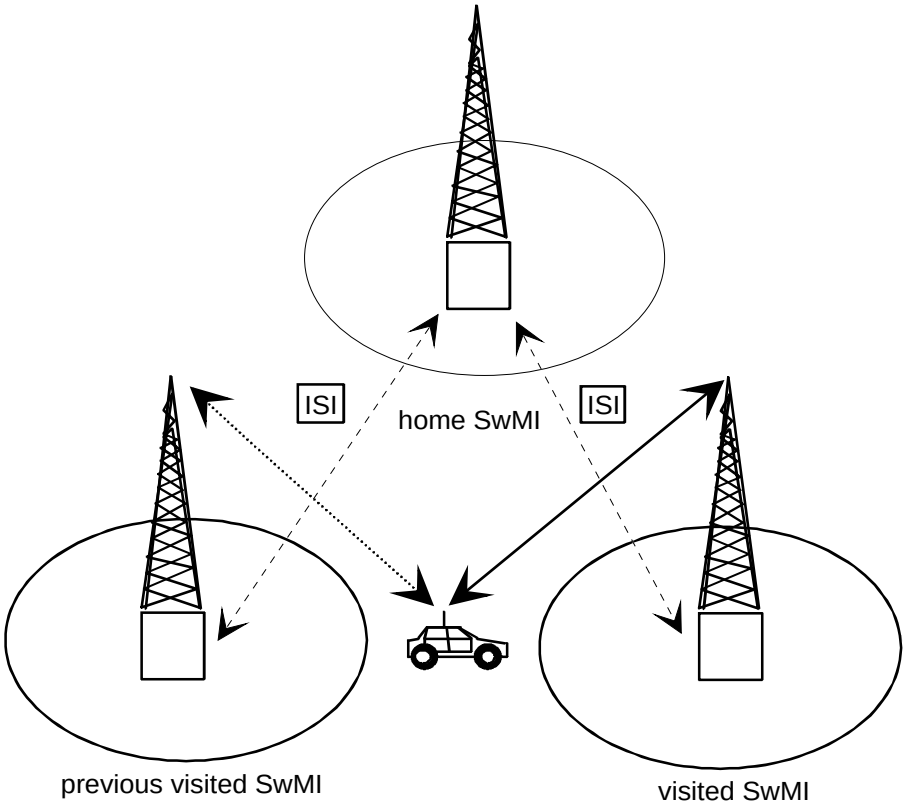


Figure 5.1: Migration scenario between SwMIs

At migration, the home SwMI shall update the individual subscriber's location information in the I-HDB.

The SwMI in which the migrating user has just registered (whether that SwMI is a visited SwMI or his home SwMI - in the latter case this means that the user has just migrated back into his home SwMI) shall create an I-VDB record to be used for the subscriber's location tracking within this SwMI. In addition, if that SwMI is different from the user home SwMI (i.e. it is the user visited SwMI), it shall fetch the subscriber's migration profiles (sent through ANF-ISIMM else defined by default) and save them in the I-VDB.

The migration profiles shall indicate the subscriber's service authorizations during the migration in the visited SwMI. The visited SwMI shall also allocate the (V)ASSI for the individual subscriber as defined in clause 7.2.2 of ETSI EN 300 392-1 [1].

As part of the migration procedure (after the individual subscriber has been successfully registered in the SwMI into which it has just migrated), the SwMI where it was previously registered shall remove the subscriber's information from its I-VDB.

A MS/LS may contain more than one TETRA Subscriber Identity (TSI) family and the migration procedure shall have to be completed for each of them independently.

5.1.1.4 Group attachment scenarios

The group attachment procedure enables individual subscribers registered in another SwMI than the home SwMI of a group of which they are member to participate in calls to that group.

NOTE: An individual subscriber member of a group may be registered in another SwMI than the home SwMI of that group because either:

- his home SwMI is the same as that of the group and he has migrated; or
- his home SwMI is different and either he is registered in his home SwMI or he has migrated into another SwMI than the group home SwMI.

As result of the group attachment, the home SwMI shall know to which SwMIs the group call will be extended and those SwMIs will themselves handle group call set-ups.

Figure 5.2 illustrates the ISI configuration for the attachment to a group of which an individual user is a member, of the visited SwMI where that subscriber has migrated when the group and that subscriber have the same home SwMI.

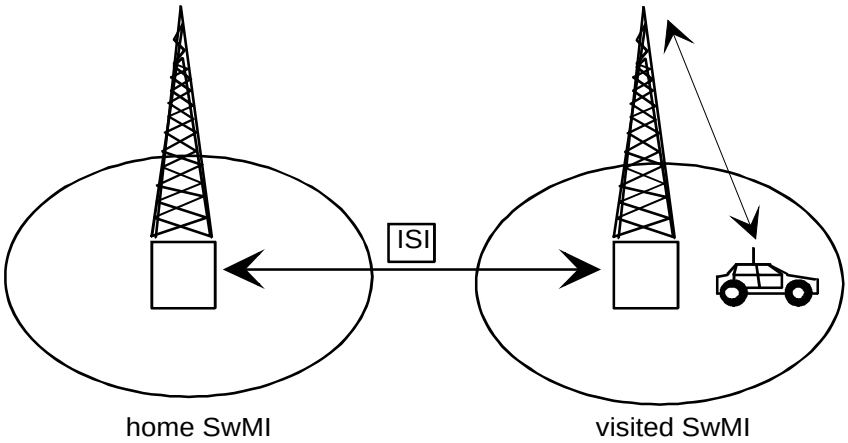


Figure 5.2: Group attachment scenario

When a new SwMI is attached to a group:

- the group home SwMI shall update the G-HDB with that new attachment; and

- that new SwMI shall record in the G-VDB the identity of the individual subscriber member of the group to be used for the subscribers' group attachment tracking within that SwMI and the group attachment tracking for that SwMI, i.e. which individual subscribers are attached to the group in that SwMI. In addition, that SwMI shall fetch the migration profiles for the group (sent through ANF-ISIMM else defined by default) and save them in the G-VDB. The migration profiles shall indicate the service authorizations for the group in that SwMI. That SwMI shall also allocate the (V)GSSI for the group as defined in clause 7.2.2 of ETSI EN 300 392-1 [1].

An individual subscriber may attach to one or more groups and each of those shall be attached independently.

5.1.2 Group linking configurations

The group linking shall enable the combining of groups with different home SwMIs (over the ISI). The call made to a group linked to another one shall result in a combined group call set-up to the members of the groups. The combined group call is described in the document defining ANF-ISIGC.

In order to support the group linking functionality in different SwMIs, the following roles are defined for SwMIs for group linking establishment:

- linking controlling SwMI: The group linking controlling SwMI controls the making of the linking for the group, i.e. group linking. In addition, the linking controlling SwMI can create the group linking service profile to be used for the group linking. The group linking controlling SwMI is the home SwMI of one of the linked groups;

- linking participating SwMI: The group linking participating SwMI participates the group linking in linking (joining) one or more groups to the group linking. The group linking participating SwMI is the home SwMI of the linked group.

In order to support the group linking functionality in different SwMIs, the following roles are defined for SwMIs for call establishment and maintenance:

- (linking) originating SwMI: The group linking originating SwMI initiates the call to group formed by linking. The group linking originating SwMI is either the group linking controlling SwMI or the group linking participating SwMI;

NOTE: This definition assumes that only attached members of the linked groups can originate calls to the combined group formed by linking.

- linking controlling SwMI: The group linking controlling SwMI sets up the call and incorporates linking participating SwMIs to the call;

- (linking) participating SwMI: The SwMIs other than linking controlling SwMI participating the linked groups call.

In addition, the following database functionalities are defined for the SwMIs supporting group linking:

- Controlling Linking DataBase (C-LDB): The C-LDB contains the linking tracking for the linked groups, i.e. the information which groups are part of the group linking. In addition, the C-LDB contains the linking service profile for the group linking. The C-LDB is located in the linking controlling SwMI.

- Participating Linking DataBase (P-LDB): The P-LDB contains the linking tracking for one of the linked groups, i.e. the information whether the group is linked or not. The P-LDB is located in the home SwMI of the group.

From two to several groups may be linked together using group linking. Figure 5.3 illustrates the ISI configuration for group linking when three groups are linked together.

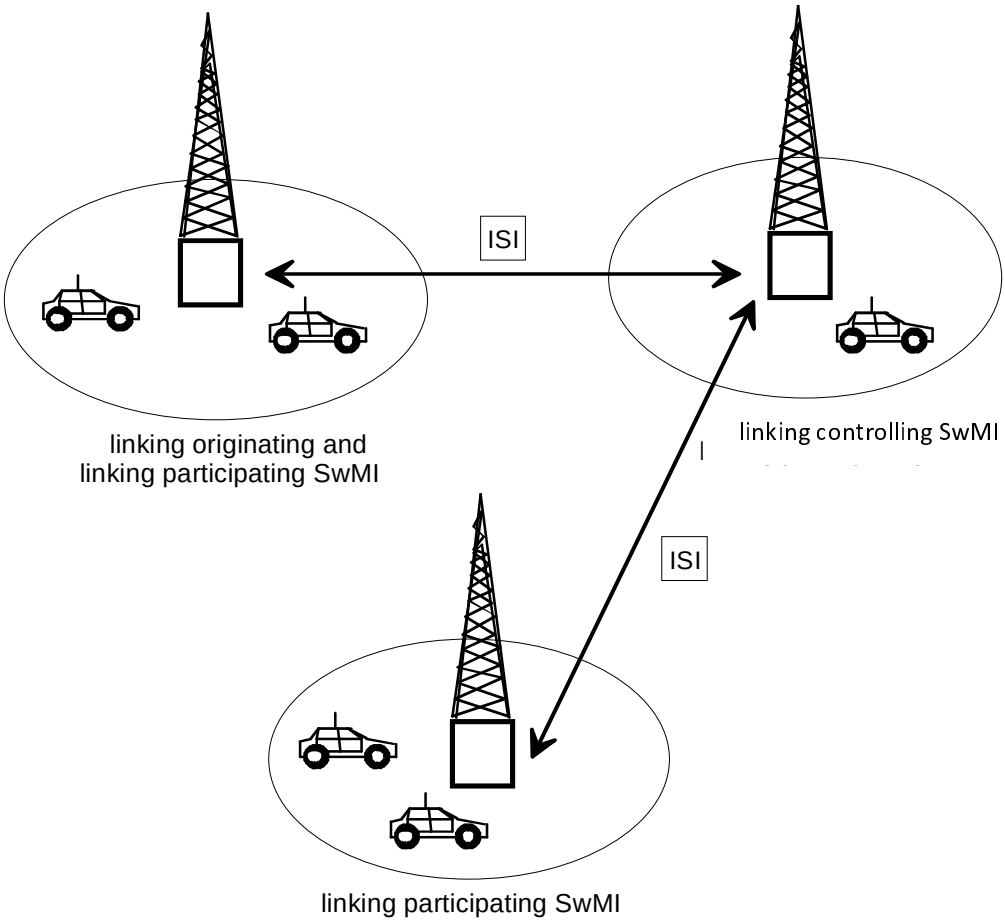


Figure 5.3: Group linking scenario

At group linking, the linking controlling SwMI shall co-ordinate and keep track of the group linking amongst the linking participating SwMIs. In addition, the linking controlling SwMI shall create the linking service profile for the group linking and save it to the C-LDB.

Each of the linking participating SwMIs shall link a group to the group linking and create a P-LDB record to be used for the group during the group linking.

A group can be part of only one group linking at a given time.

5.2 Call processing

5.2.1 Group call processing

In order to support group call processing in different SwMIs, the following SwMI roles are defined:

- Originating SwMI: The SwMI where the calling user is located; it may or may not coincide with the home SwMI of that user. The originating SwMI may or may not coincide with the controlling SwMI in which case the SwMI is in general called the controlling SwMI. If the originating SwMI does not coincide with the controlling SwMI, the SwMI will act as a participating SwMI after the call setup has been concluded.

NOTE 1: In the present document, the term "coincide" means "to have the same MNI".

- Controlling SwMI: The controlling SwMI shall be in charge to set up and maintain a call extending over two or more SwMIs involving more than one SwMI.

- Participating SwMI: A SwMI which is different from the controlling SwMI and where the group call is established (see note 2).

NOTE 2: To extend the group call to the participating SwMI, either the group linking is used (see clause 5.1.2) or the controlling SwMI will have to know that at least one member of the controlling group is registered there and attached to the group: this means that the participating SwMI will have to be attached to the group (see clause 5.1.1.4).

NOTE 3: Once the call has been established, the role of the originating SwMI will cease. Unless it coincides with the controlling SwMI, it will become a participating SwMI.

Point-to-multipoint call set-up between SwMIs shall be set-up as a logical star configuration where the controlling SwMI shall be the centre of the star.

After a user has sent his set-up request for a group call, the originating SwMI if different from the controlling SwMI shall invoke an ANF-ISIGC to pass that request to the controlling SwMI, which shall take over the establishment of the call. This shall hold regardless of whether the calling user is located or not in his home SwMI. Some called users may be located in the controlling SwMI.

Figure 5.4 illustrates the ISI connection when a group call is initiated between two SwMIs, the originating SwMI being the home SwMI of the group. The originating SwMI is then also the controlling SwMI.

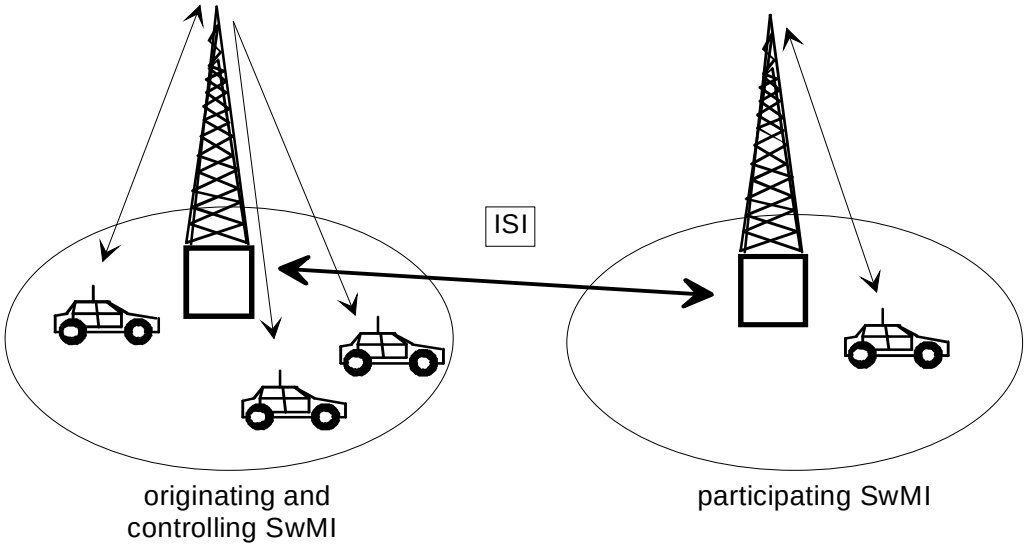


Figure 5.4: Group call configuration

Figure 5.5 illustrates the ISI connection when the originating SwMI of a group call is not the group home SwMI. The originating SwMI becomes then a participating SwMI after the call setup has been completed.

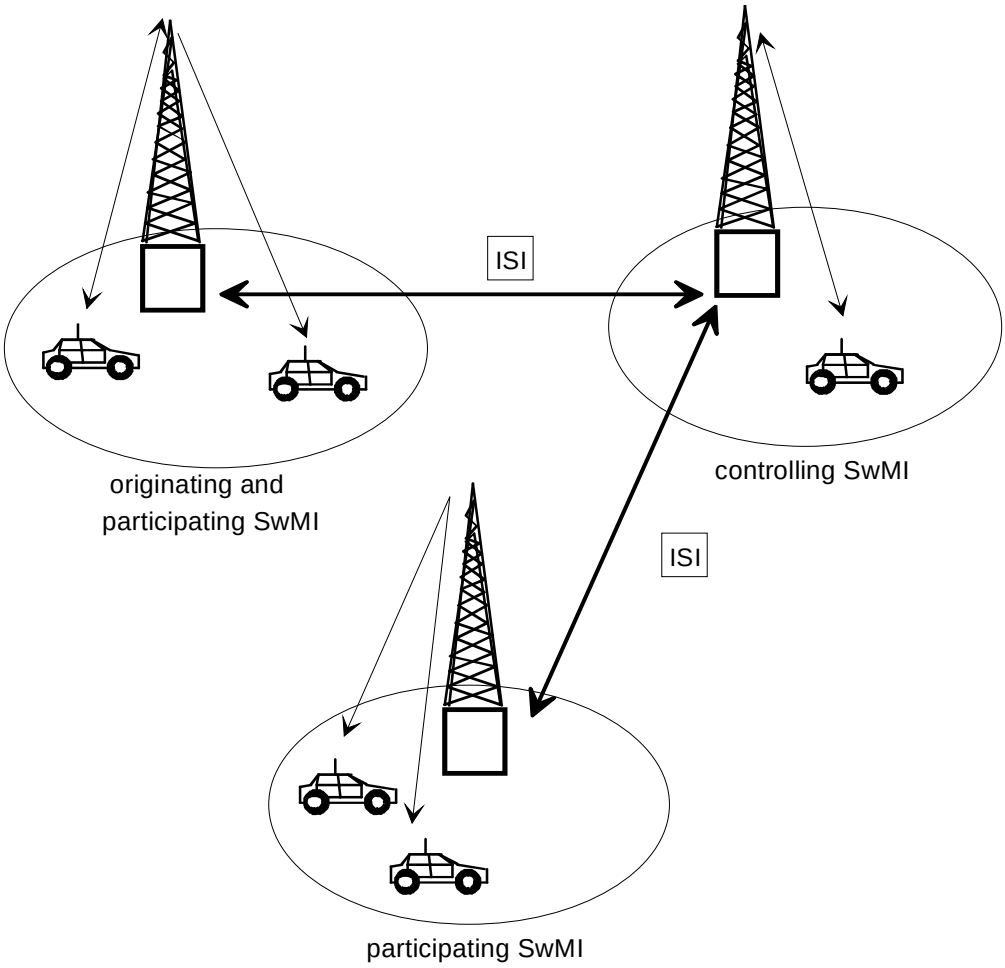


Figure 5.5: Group call processing

5.2.2 Individual call processing

When an SwMI sets up an individual call an ANF-ISIIC shall be invoked to extend this call over the ISI. Figure 5.6 illustrates the ISI configuration when an individual call is initiated between two SwMIs.

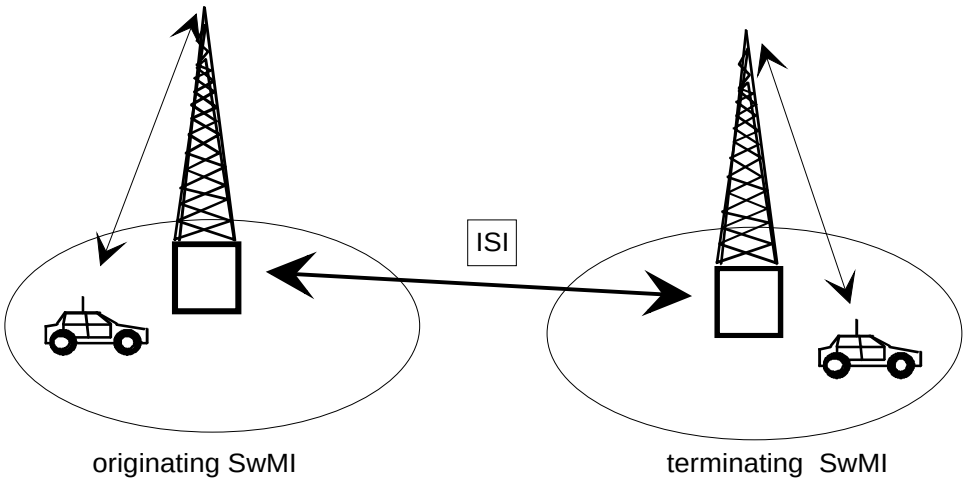


Figure 5.6: Individual call processing

The SwMI where the calling user is located is called the originating SwMI. It may or may not coincide with the home SwMI of that user.

NOTE 1: In the present document, the term "coincide" means "to have the same MNI".

When a user is called, the invoked ANF-ISIIC will first route the call request to the called SwMI, this routeing being independent of whether or not the originating SwMI is the home SwMI of the calling user. The invoked ANF-ISIIC will then ensure the adequate routeing of the call to the terminating SwMI in the called SwMI. Three possible cases arise for this routeing:

- the called SwMI is the called user home SwMI and this user has not migrated; or
- the called SwMI is the called user home SwMI and this user has migrated; or
- the called SwMI is not the home SwMI of the called user and this user has migrated (i.e. the home SwMI of this user is the originating SwMI).

The originating SwMI shall control transmission granting for half duplex operation.

NOTE 2: The allocation of transmission control to the originating SwMI was somewhat arbitrary; however it is more logical than to the terminating SwMI.

5.2.3 Transit

Additionally any SwMI may have a transit capability for the following cases:

- forward switching in the case of individual call where the SwMI is the called user home SwMI and where the called user has migrated;
- call restoration;
- the group linking participating SwMI expanding the call to SwMIs where the members of the participating linked group are located;
- specific supplementary operation (e.g. call diversion).

6 Introduction to ISI ANFs

6.1 ISI ANF Overview

The following functional ANFs will be defined for the ISI:

- Transport layer Independent Additional Network Feature - Inter-System Interface Mobility Management (ANF-ISIMM).
- Transport layer Independent Additional Network Feature - Inter-System Interface Individual Call (ANF-ISIIC).
- Transport layer Independent Additional Network Feature - Inter-System Interface Group Call (ANF-ISIGC).
- Transport layer Independent Additional Network Feature - Inter-System Interface Short Data service (ANF-ISISDS).
- Transport layer Independent Additional Network Feature - Inter-System Interface Supplementary Services (ANF-ISISS).

6.2 ANF-ISIMM

ANF-ISIMM enables the TETRA mobility management, authentication and OTAR services to inter-operate in different SwMIs linked through one or more ISIs. In doing so, ANF-ISIMM allows the individual subscribers e.g. to migrate, to be authenticated, to attach to groups and, thus, to participate in individual and group calls.

NOTE: The TETRA air interface MM services are defined in clause 15 of ETSI EN 300 392-2 [2], and the TETRA security authentication and the OTAR key management services in clause 4 of ETSI EN 300 392-7 [13]. However, ANF-ISIMM does not support the forward registration nor the assignment of Group Cipher key (GCK) as defined in clause 15 of ETSI EN 300 392-2 [2], and in clause 4 of ETSI EN 300 392-7 [13], respectively.

In addition, ANF-ISIMM offers database fault recovery services for SwMIs, in order to recover the databases after faulty situations, and group linking and unlinking services, in order to enable the dynamic combining of groups to support combined group calls between SwMIs.

6.3 ANF-ISIIC

ANF-ISIIC enables calls to be set-up from a TETRA user registered in one SwMI to another TETRA user registered in another SwMI, operating at the ISI of both SwMIs. It also supports call restoration when a user has migrated to another TETRA SwMI during an established call. Additionally, ANF-ISIIC allows TETRA signalling information to be passed from a TETRA SwMI to another TETRA SwMI supporting the TETRA individual call procedures as defined in clauses 11 and 14 of ETSI EN 300 392-3-12 [5].

6.4 ANF-ISIGC

ANF-ISIGC enables point-to-multipoint calls to be set-up between TETRA users located in more than one TETRA SwMI, operating at the ISI of all these SwMIs. Additionally, the ANF-ISIGC shall handle transmission control signalling from all SwMIs involved in the given group call supporting the point to multipoint TETRA call procedures defined in clauses 11 and 14 of ETSI EN 300 392-3-13 [6].

6.5 ANF-ISISDS

ANF-ISISDS enables point-to-point or point-to-multipoint short data messages to be passed between TETRA users located in more than one TETRA SwMI. SDS messages are transported using call independent signalling, refer to ETSI EN 300 392-3-14 [7].

6.6 ANF-ISISS

ANF-ISISS is a transport mechanism to allow signalling information exchange between two SwMIs for the control of TETRA supplementary services. It operates over the ISIs of both SwMIs - see clause 10 of ETSI EN 300 392-9 [11].

It is used e.g. for the exchange of signalling information between peer Circuit Mode Control Entities (CMCEs), as defined in clause 14 of ETSI EN 300 392-2 [2], in the specifications of a number of protocols for the operation of supplementary services.

7 ISI Generic Functional Protocol (ISI GFP)

7.1 Protocol model

The ISI Generic Functional Protocol (ISI GFP) model consists of three layers; the ANF ISI entities, ISI Mediation Function and Transport Protocol Control. The ANF ISI entities manage and control the sending of the ANF-ISI PDUs. Signalling needs for TETRA ISI operation which are not directly supported by the transport protocol control are provided by ISI Mediation Function.

The ISI Mediation Function does not by itself control any ANF-ISI PDUs but rather provides a means to convey them.

The ANF-ISI Entities are independent on the used transport protocol.

Figure 7.1 shows the conceptual model of the ISI GFP.

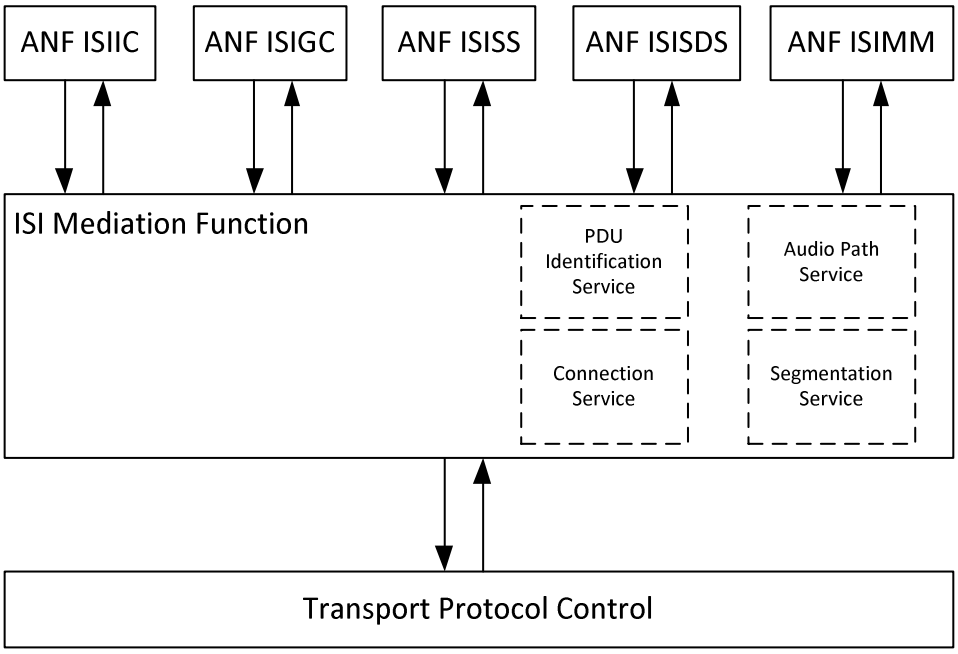


Figure 7.1: Conceptual Model of the ISI Generic Functional Protocol

The ISI Mediation Function coordinates the identification of message flows and controls the conveying of the message flows across the transport protocol. The ISI Mediation Function contains a number of services which are closely related to the transport protocol.

The Transport Protocol Control function determines which message to use for the transport of the ISI messages. The Transport Protocol Control function is transport protocol dependent. The transport protocol can be any protocol which can route the ISI PDUs between TETRA networks.

7.2 Services provided by the conceptual protocol model entities

ANF entities (i.e. ANF-ISIIC, ANF-ISIGC, ANF-ISISDS, ANF-ISISS and ANF-ISIMM entities) use the services of the ISI Mediation Function to convey ANF-ISI PDUs via a transport protocol between SwMIs.

The ISI Mediation Function may include a number of services dependent on the transport protocol. The services can be:

- PDU Identification Service.
  Each PDU containing an ISI APDU is identified by a ISI header. The PDU identification service is mandatory and transport protocol independent.

- Audio Path Service.
  The Audio Path Service might comprise channel selection, media negotiations etc. The Audio Path Service is mandatory but is transport protocol dependent.

- Connection Service.
  The Connection Service is optional and is transport protocol dependent. It may control the Transport Protocol Call Control signalling.

- Segmentation Service.
  The Segmentation Service is used if the transport protocol has a maximum message length. The Segmentation Service is optional and is transport protocol dependent.

7.3 Addressing and transport

Addressing and transport issues are transport layer dependent and are described in the related transport protocol general design documents.

7.4 ISI GFP requirements and operation definition

7.4.1 General

Each ANF-ISI PDU shall be encoded as an OCTET STRING in the argument of the operation tetraIsiMessage specified in table 7.7.1 using Abstract Syntax Notation One (ASN.1, 2000 version).

NOTE: This operation is common to all ANF-ISI protocols.

Table 7.1: Operation in support of TETRA encoding PDU

```
TetraIsiOperation {ccitt (0) identified-organization (4) etsi (0)
tetra(392) isi-encoding-operation(0)}

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

EXPORTS
  ISI;


OPERATION::=CLASS
{
           &operationCode     Code     UNIQUE OPTIONAL,
           &ArgumentType               OPTIONAL,
           &Errors            ERROR    OPTIONAL

}

WITH SYNTAX
{
            [CODE             &operationCode]
            [ARGUMENT         &ArgumentType ]
            [ERRORS           &Errors]
}

ERROR::=CLASS
{
           &ParameterType        OPTIONAL,
           &errorCode     Code   OPTIONAL
}
WITH SYNTAX
{
            [PARAMETER &ParameterType]
            [CODE &errorCode]
}

Code ::= CHOICE
{
            local              INTEGER,
            global             OBJECT IDENTIFIER
}


Invoke ::= SEQUENCE
{
     invokeId             INTEGER,
     operationValue       OPERATION.&operationCode ({tetraIsiMessage }),
     argument             OPERATION.&ArgumentType ({tetraIsiMessage})
}


Result::= SEQUENCE
{
     invokeId             INTEGER,
     operationValue       OPERATION.&operationCode ({tetraIsiMessage }),
```

```
     result               OPERATION.&ArgumentType ({tetraIsiMessage})
}


ReturnError::= SEQUENCE
{
     invokeId         INTEGER,
     errorValue       OPERATION.&Errors.&errorCode ({tetraIsiMessage}),
     errorParameter   OPERATION.&Errors.&ParameterType ({tetraIsiMessage})
}

Reject ::= SEQUENCE
{
     invokeId          INTEGER,
     problem           CHOICE
                       {
                                      general [0] GeneralProblem,
                                      invoke [1] InvokeProblem
                       }
}


ISI ::= CHOICE
{
         invoke           [1] Invoke,
         result           [2] Result,
         returnError      [3] ReturnError,
         reject           [4] Reject
}

GeneralProblem ::= INTEGER
{
               unrecognizedPDU (0),
               mistypedPDU (1),
               badlyStructuredPDU (2)
}

InvokeProblem ::= INTEGER
{
               duplicateInvocation (0),
               unrecognizedOperation (1),
               mistypedArgument (2),
               resourceLimitation (3),
               initiator-releasing(4),
}



tetraIsiMessage OPERATION ::= {
  CODE     global: {ccitt (0) identified-organization (4) etsi (0)tetra(392) isi-encoding-
operation(0)}
  ARGUMENT IsiArgument
  ERRORS { incompleteTetraPDU |
           requestNotSupported |
           invalidInfoElement |
           unspecified
         }
}
-- Definition of general used data types:
IsiArgument ::= SEQUENCE { sourceEntity [0] IMPLICIT AnfSubEntity,
                           destinationEntity [1] IMPLICIT AnfSubEntity,
                           tetraMessage [2] IMPLICIT OCTET STRING }


incompleteTetraPDU ERROR ::= {
       PARAMETER ErrorOctetString
       CODE local:1 }

requestNotSupported ERROR ::= {
       PARAMETER ErrorRequestNotSupported
       CODE local:4 }

invalidInfoElement ERROR ::= {
       PARAMETER ErrorInvalidInfo
       CODE local:5 }

unspecified ERROR ::= {
       CODE local:0 }
```

```
AnfSubEntity ::= ENUMERATED { anfIsiss (1),
                              anfIsimm (2),
                              anfIsiic (3),
                              anfIsigc (4),
                              anfIsisd (5),
                              callUnrelatedSignalling (6) }

ErrorOctetString
     ::= SEQUENCE { octetstring [0] IMPLICIT OCTET STRING }

ErrorRequestNotSupported
     ::= CHOICE { mmRequestNotSupported MMRequestNotSupported,
                  ssRequestNotSupported SSRequestNotSupported
}

MMRequestNotSupported ::= [0] OCTET STRING

SSRequestNotSupported
     ::= CHOICE {
                listSSNotSupported         [1] ListSSNotSupported,
                listSSActionNotSupported   [2] ListSSActionNotSupported,
                combinedSSListNotSupported [3] CombinedSSListNotSupported
}

ListSSNotSupported ::= OCTET STRING


SSActionNotSupported
      ::= SEQUENCE {
                  ssType [6] IMPLICIT OCTET STRING,
                  ssPduType [7] IMPLICIT OCTET STRING }

ListSSActionNotSupported
      ::= CHOICE {
                 ssAction [4] IMPLICIT SSActionNotSupported,
                 ssActionSeq [5] IMPLICIT SEQUENCE OF SSActionNotSupported }

CombinedSSListNotSupported
      ::= SEQUENCE {
                  listSSNotSupported [0] ListSSNotSupported,
                  listSSActionNotSupported [1] ListSSActionNotSupported }

ErrorInvalidInfo
      ::= CHOICE {
                 invalidInfo [0] IMPLICIT InvalidInfoType,
                 invalidInfoSeq [1] IMPLICIT SEQUENCE OF InvalidInfoType }

InvalidInfoType
      ::= SEQUENCE {
                  pduIndicator [2] IMPLICIT OCTET STRING,
                  elementType [3] IMPLICIT INTEGER (1..3),
                  elementPosition [4] IMPLICIT INTEGER }



END -- of TetraIsiOperation
```

TETRA ISI APDUs shall be encoded in accordance with the Basic Encoding Rules (BER) defined for ASN.1 in Recommendation ITU-T X.690 [12], with the following restrictions:

- when the definite form is used for length encoding, a data value of length less than 128 octets shall have the length encoded in the short form;
- when the long form is used for length encoding, the minimum number of octets shall be used to encode the length field; and
- values of the type OCTET STRING or BIT STRING shall be encoded in a primitive form.

Receiving entities shall be able to interpret all length forms of the basic encoding rules.

The following data elements shall be included in the argument of the tetraIsiMessage Invoke APDU:

- element destinationEntity, which defines the destination ANF in the receiving ISI;
- element sourceEntity, which defines the source ANF of the Invoke APDU;
- element tetraMessage, which contains the ANF-ISI PDU.

The Invoke ID is unique between two TETRA networks for each call or each sequence of call independent messages. The Invoke ID identifies the call or the sequence of call independent ISI messages.

7.4.2 Result

The tetraIsiMessage Result APDU enables the receiving SwMI to return a positive reply to an Invoke APDU. It may be used when an ANF-ISI PDU sent in the Invoke APDU needs a confirmed response. The argument of the tetraIsiMessage Result APDU shall be defined on a case by case basis (in the standard where the use of that APDU is specified).

7.4.3 ReturnError

The tetraIsiMessage ReturnError APDU enables the receiving SwMI to return a negative reply, if a tetraIsiMessage Invoke APDU while still being recognized as at least partially valid cannot be accepted because of one or more of the following errors:

- incompleteTetraPdu: the received ANF-ISI PDU was incomplete because of segmentation error (see ETSI EN 300 392-3-10 [3]);
- requestNotSupported: the destination entity does not support the service requested by the ANF-ISI PDU. The use of that error indication is specified in the protocol definitions of the relevant ANFs (e.g. see clause 6.3.3 of ETSI EN 300 392-3-12 [5] for ANF-ISIIC or clause 10.3 of ETSI EN 300 392-9 [11] for ANF-ISISS). The parameter of this error is dependent on the destination entity:
  - if the destination entity is the ANF-ISIIC, there shall be no parameter (since the request not supported is clearly identifiable without any need for additional information);
  - if the destination entity is the ANF-ISIMM, the parameter shall contain the value (or the list of values) of the information element ANF-ISIMM PDU type corresponding to the ANF-ISIMM PDU(s) not supported;
  - if the destination entity is the ANF-ISISS, the parameter shall contain one or both of the two following lists:
    - for the request(s) related to SS(s) not supported, the corresponding value (or the corresponding list of values) of the information element SS type (see table 5 of ETSI EN 300 392-9 [11]);
    - for the request(s) related to action(s) not supported for specific SS(s) (which is (are) supported), the corresponding values (or the corresponding list of values) of the information elements SS type and SS PDU type (see tables 5 and 6 of ETSI EN 300 392-9 [11]);
- invalidInfoElement: at least one element of the ANF-ISI PDU cannot be understood. For each such PDU the first invalid information element detected shall be indicated by the parameter of this error using the following three pieces of information:
  - the ANF-ISI PDU identification, i.e.:
    - for ANF-ISISS: the corresponding values (or the corresponding list of values) of the information elements SS type and SS PDU type (see tables 5 and 6 of ETSI EN 300 392-9 [11]);
    - for other ANF-ISI PDUs: the corresponding value (or the corresponding list of values) of the information element PDU type;
  - the type of the first element of this PDU which was not understood;

- the position of this element in the list of information elements of the same type present in the PDU (e.g. third type 1 element in some specific SS PDU received);
- the above three pieces of information shall be repeated in the parameter of the error invalidInfoElement for each ANF-ISI PDU in which one invalid information element has been detected by the receiving SwMI;

- unspecified.

If one error listed above has occurred, the ReturnError APDU shall be sent with the appropriate error value, and its possible associated parameter value. If more than one has occurred, the error value sent shall specify only one error, and the parameter value, the parameters possibly associated with this error. This single error shall be chosen according to their priority, this priority being defined by their rank in the above list, e.g. if the error incompleteTetraPDU has occurred (because of segmentation error), it shall be the error indicated, and if no error incompleteTetraPDU has occurred and if requestNotSupported has occurred, the latter shall be the error indicated.

The decision taken by the SwMI when its ISI Mediation Function entity receives a ReturnError APDU when the peer SwMI has not already cleared the signalling connection is an implementation matter (it may clear that connection; and may or may not attempt to establish it later).

7.4.4 Reject

The tetraIsiMessage Reject APDU enables the receiving SwMI to return a negative reply in Invoke Problem element of ISI Reject APDU, if an incoming Invoke APDU cannot be accepted because of the following problems:

- duplicateInvocation (0): The same Invoke ID identifier is used between the two SwMIs for two different calls or for two call independent ISI message sequences;
- unrecognizedOperation (1): The operation is not one of those agreed for the ISI APDUs or indicated ANF-ISI is not supported in the SwMI;
- mistypedArgument (2): The type of the operation argument is not one of those agreed for the ISI APDUs;
- resourceLimitation (3): The entity is not able to perform the invoked operation due to resource limitation;
- initiator-releasing (4): The initiator is not willing to perform the invoked operation because it is attempting to release the call or call independent connection.

The decision taken by the SwMI when its ISI Mediation Function entity receives a reject APDU and the peer SwMI has not already cleared the signalling connection is an implementation matter (in most cases it will clear that connection; and may or may not attempt to establish it later).

7.4.5 Procedures

ANF-ISI PDUs are sent from one ANF to its peer ANF. The ANF PDUs are conveyed in an ISI-Invoke APDU when transported from one ISI Mediation Function to the peer ISI Mediation Function.

If there are no errors in the ISI-APDUs then both peer ISI Mediation Functions shall send all ANF-ISI PDUs in ISI-Invoke APDUs.

For backward compatibility reasons the invoking ISI Mediation Function may receive a response in an ISI Result APDU from the destination ISI Mediation Function. The destination Mediation Function can only send one ISI- Result APDU per invoked ISIMM service and the ISI-Result APDU is sent as an immediate response to the first ISI Invoke APDU of the service, i.e. if a destination ISI Mediation Function sends an ANF-ISI PDU in an ISI-Result APDU, no other APDUs having the same Invoke Identifier are sent from the ISI Mediation Function in an ISI-Invoke APDU in between.

If the receiving ISI Mediation Function cannot read the ISI header or the indicated ANF-ISI is not supported, the ISI Mediation Function shall send an ISI-Reject APDU. The cases when ISI Reject should be sent are defined in clause 7.4.4.

If the receiving ANF-ISI cannot read the ANF-ISI PDU or the PDU contains parameters which are not supported the ANF-ISI shall initiate a return error to be sent to the sending ANF-ISI. The return error shall be sent as an ISI-Return Error APDU from the receiving to the sending ISI Mediation Function. The cases when ISI ReturnError should be sent are defined in clause 7.4.3.

The actions in the sending and the receiving ISI Mediation Function in relation the ISI-Reject and ISI-ReturnError is network dependent and is outside the scope of the present document.

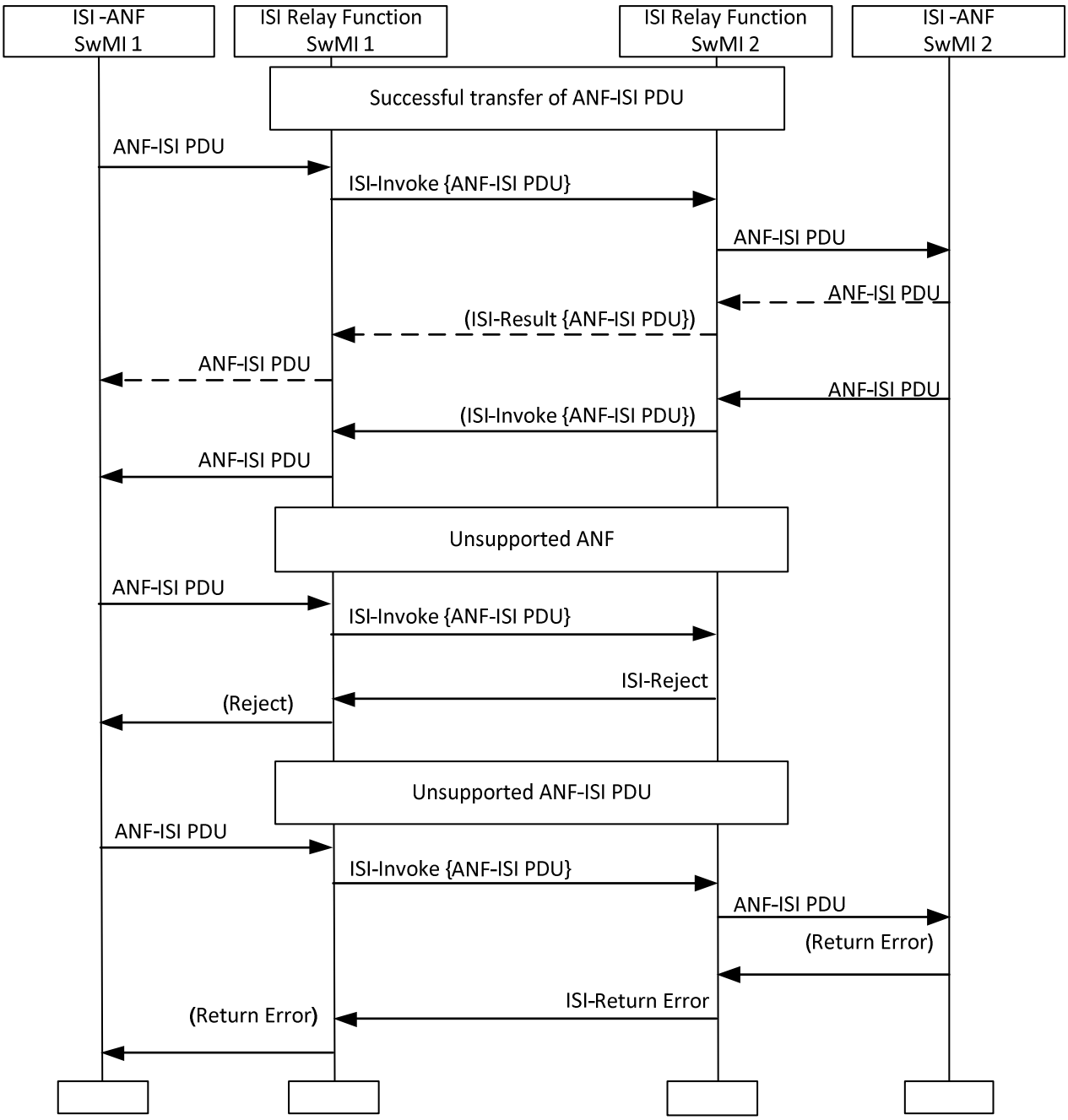


Figure 7.2: Generic Signalling Procedure

8 Security related functions the ISI

8.1 Security overview

Authentication and encryption of the connections used between SwMIs are outside the scope of TETRA standardization. However ITSI authentication, end-to-end encryption and end-to-end key management have impact on the ISI.

In addition, the specific requirements on ANF-ISIMM to support air interface encryption in a visited SwMI for an individual subscriber (i.e. when this SwMI is different from his home SwMI) are defined in annex A. This annex includes also a supporting explanation for the various possible types of cipher key which may be used at the air interface and their relationship with authentication.

8.2 ITSI authentication

When migrating, an individual subscriber may have to be authenticated by the visited SwMI, if this SwMI and the subscriber's home SwMI both support this option. To support it, upon request from the visited SwMI using ANF-ISIMM, the home SwMI shall send the authentication parameters over the ISI to the visited SwMI also using ANF-ISIMM. Those authentication parameters are a session key for each of MS and SwMI authentication (KS and KS') and a Random Seed (RS) used to seed the authentication algorithm.

The home network shall send those authentication parameters to a visited SwMI for an MS when requested by the visited SwMI. This visited SwMI may then use them for authentication, using the procedure defined in clauses 4.2 and 4.3 of ETSI EN 300 392-7 [13]. This procedure may be repeated within the time limits advised by the home SwMI.

NOTE 1: This method which does not reveal the original authentication key of the MS combines security and efficiency.

The same authentication parameters sent by the home SwMI allow an individual subscriber which has migrated to authenticate the infrastructure, using the procedure defined in clause 4.3 of ETSI EN 300 392-7 [13]. Formally, this procedure shall only authenticate the home SwMI. But by acting as an agent to the authentication process the visited SwMI is implicitly authenticated.

NOTE 2: In a symmetric key authentication process there is authentication only between the holders of the key (in this case the MS and the home SwMI of that MS). If an intermediary holds some of the data, or performs part of the process, then the home SwMI is in effect distributing its management function to that intermediary. In the ISI case the intermediary is the visited SwMI and is essentially part of a distributed home SwMI. It can therefore be trusted. In such an instance the visited SwMI is trusted in the same way that a BS within the home SwMI is trusted.

8.3 End-to-end encryption

There is no end-to-end encryption algorithm or method defined for TETRA. However a mechanism is described to support the synchronization of synchronous stream ciphers, with synchronization data sent interspersed with the encrypted voice or data traffic. The frequency at which such signalling can be sent is defined in clause 7 of ETSI EN 300 392-7 [13]. This synchronization data has to be correlated in a bit exact manner to the encrypted traffic. This is ensured at the air interface by using the frame stealing mechanism. To ensure it over the ISI, an in-band signalling method shall be used between the source and the destination SwMIs. This method shall be such that the destination SwMI of the call shall receive stolen frames from the source SwMI in such a sequence that it shall be able to correctly transmit these across the air interface, i.e. the exact relation between stolen frames and the first and second half slots of a timeslot shall be maintained.

This implies that frame and timeslot boundaries, and ordering, shall be retained across the ISI for end-to-end encrypted calls.

NOTE: A similar requirement exists for voice calls, between TETRA codecs (see ETSI EN 300 395-1 [i.1]).

8.4 End-to-end key management via ISI

Clause 4.6 of ETSI EN 302 109 [10] provides a means of transporting end-to-end key management material over the air interface by use of short data messages. The quantity of data transported is 2 047 bits minus a data type identifier, which corresponds to the maximum length of a type 4 short data message. To allow the extension of such messages over the ISI between SwMIs, ANF-ISISDS shall be supported.

Annex A (normative): Security - supporting encryption over ISI

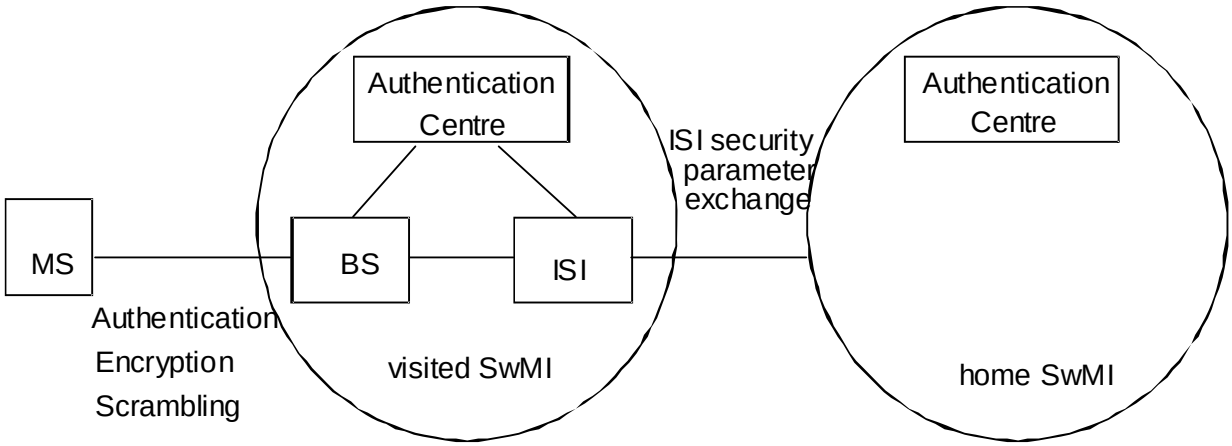
A.1 Overview

This annex describes the support of air interface encryption by transmission of security parameters over the ISI. The material presented here also describes the major differences between support of security functions over the ISI, and the support of the same functionality at the air interface.

Air interface encryption takes place in layer 2 of the air interface protocol stack. The layer 3 authentication service, embedded in MM, can provide a cipher key to layer 2 that is strongly bound to authentication (i.e. it allows implicit authentication of all messages sent that are encrypted using this key). In addition the layer 3 OTAR service, embedded in MM, can provide cipher keys to layer 2.

When migrating, an individual subscriber may have to be authenticated to the visited SwMI. This shall be achieved by the ISI supporting transport of authentication parameters from home SwMI to visited SwMI.

The air interface authentication mechanism uses a secret key schema that ensures that the authentication Key (K) is known only to the AC and the MS. In order to enable authentication of a migrated MS, the home SwMI and the visited SwMI shall support the ANF-ISIMM functionality allowing authentication of a (individual) subscriber in a visited SwMI. As described in clause A.2.2.2, at the same time, this will allow the visited SwMI to support the air interface encryption service using Derived Cipher Key (DCK) for a user having migrated. If, instead of this air interface encryption service, the visited SwMI supports the air interface encryption service using Static Cipher Key (SCK) (see clause A.2.2.4), in order to enable migrating users to use this service, the home SwMI and the visited SwMI shall support ANF-ISIMM functionality OTAR SCK for a subscriber in a visited SwMI.



NOTE: BS = Base Station.

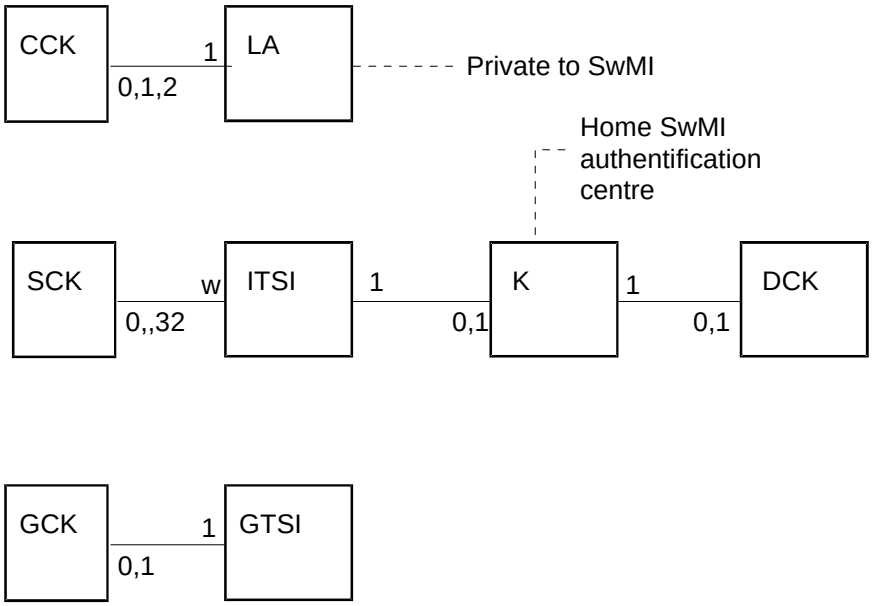
Figure A.1: Overview of ISI in place within TETRA

In figure A.1 the AC holds the ITSI/secret key K relationship and is a trusted part of the SwMI, see ETSI EN 300 392-7 [13]. By authenticating the individual subscriber to the network and then using the authentication process to derive an encryption key the air-interface is made secure and this individual subscriber becomes trusted. The present document does not provide any means for secure transport of call control signalling although it is allowed to carry authentication parameters and other security related signalling data.

A.2 Encryption

A.2.1 ISI relation to air interface and end-to-end encryption

The air interface encryption system in TETRA (see ETSI EN 300 392-7 [13]) operates on the radio link between individual subscriber and BSs of the SwMI. The cipher keys may be dynamically derived. Encryption synchronization will be derived from the frame numbering system. As this encryption applies at the air interface, information will be decrypted at the BSs of the SwMI, and therefore will be unencrypted at point of presentation to the ISI.



NOTE 1: The relation between the SCK and ITSI allows up to 32 keys to be associated with any ITSI but SCKs may not be shared among ITSIs.
NOTE 2: Only one Common Cipher Key (CCK) shall be in use at one time in an LA.
NOTE 3: The cardinality of each relation is shown by the figures attached to each link, e.g. an ITSI can have 1 or 0 keys K, and K can be associated with only one ITSI. An open relation is shown by a letter (e.g. "w" for SCK to ITSI).

Figure A.2: Mapping of cipher key and TETRA address relationships

In order to use encryption at the air interface, the serving BS and the individual subscriber shall have the same keys. figure A.2 shows the relation of cipher keys to destination addresses (ITSI/GTSI). For the ISI to be invoked for the transfer of a key, and for the air interface service OTAR to be invoked, the destination address (ITSI/GTSI) has to be allowed to use in the visited SwMI.

End-to-end encrypted traffic between individual subscribers shall remain encrypted across the ISI. End-to-end encryption does not encrypt the ISI signalling.

A.2.2 Air interface encryption key management via ISI

A.2.2.1 OTAR

In ETSI EN 300 392-7 [13] a mechanism of key management over the air interface is described i.e. OTAR. This mechanism allows the SwMI to distribute keys to individual subscribers. Each key is sealed prior to distribution: i.e. it is packaged in an encrypted form where the key to be used is derived from the secret key K.

The keys that are used for air interface encryption are described in relationship to the ISI in the following clauses.

NOTE: This description is given in more detail in the ETSI EN 300 392-3-15 [8] defining ANF-ISIMM.

A.2.2.2 Secret Key of individual subscriber (K)

K shall not be transferred over the ISI.

A.2.2.3 Derived Cipher Key (DCK)

Authentication is a prerequisite of DCK.

The DCK shall be generated within the SwMI where the individual subscriber has requested registration. It shall not be valid in a different SwMI, and shall be generated afresh by authentication in a SwMI. It shall not be transferred across the ISI.

In order to support the use of DCK in the visited SwMI ANF-ISIMM shall support the transfer of DCK generator parameters from the AC of the home SwMI of the migrating individual subscriber. These parameters shall consist of the session key for individual subscriber authentication, the session key for SwMI authentication and the random seed. These parameters are used in the authentication algorithms which as an output of successful authentication allow DCK to be generated. The terms authentication parameters and DCK generator parameters are equivalent and should be used to reflect the user intention.

A.2.2.4 Common Cipher Key (CCK)

Authentication is a prerequisite of CCK.

The CCK shall be generated within an SwMI and shall be valid within one or more LAs of that SwMI. It shall not be known within a different SwMI. If an individual subscriber migrates and request registration in a new SwMI, it shall be authenticated by this SwMI, and obtain the relevant CCK within that new SwMI. The CCK shall not be transported via the ISI.

A.2.2.5 Static Cipher Key (SCK)

The SCK may be valid in many SwMIs and may require to be modified from the home SwMI across the ISI. In addition the visited SwMI may require to distribute versions of SCK to all registered users of its SwMI.

The visited SwMI may generate SCK locally. In order to distribute this locally generated SCK, ANF-ISIMM shall support the transfer from the home SwMI to the visited SwMI of parameters to allow the SCK to be sealed. These parameters shall be:

- Session Key for OTAR; and
- RS for OTAR.

The home SwMI may wish to distribute a new SCK to a migrating subscriber. Such a key shall not be used by the visited SwMI, but only in the home SwMI. The home SwMI shall then request ANF-ISIMM to transfer the sealed key and the parameters to allow the migrating individual subscriber to unseal it. These parameters shall be:

- RS for OTAR;
- SCK number; and
- SCK version number.

A.2.2.6 Group Cipher Key (GCK)

Authentication is a prerequisite of GCK.

For secure group calls in an SwMI there shall be a key, GCK, associated with the group address (GTSI).

In a visited SwMI a GCK shall only be used if it is generated and assigned by the visited SwMI. This shall not invoke ANF-ISIMM.

Annex B (informative): Encoding Example

Table B.1 shows an example of encoding the ANF.ISIGC SETUP INITIATE PDU. The binary is - without changes - to be added in the appropriate field in the carrier protocol.

NOTE: The Invoke ID is dependent on the transport dependent General Design document. For PSS1 as transport protocol the length is 2 octets, for SIP as transport protocol the length is 5 octets and the Invoke ID contains the MNI (MCC and MNC) of the originating SwMI. The following example is made for SIP as transport protocol.

Table B.1: Example of encoding an ANF-ISIGC SETUP INITIATE PDU

	Context specific-constructed-invoke APDU	10100001_2
	Length = 50 octets	00100011_2
InvokeId	Universal-integer tag 2	00000010_2
	length = 5 octets	00000101_2
	arbitrary value = 260 279 1234	01000001_2
		00000001_2
		00010111_2
		00000100_2
		11010010_2
OperationValue	universal-object identifier tag 6	00000110_2
	length = 5 octets	00000101_2
	encoding of { 0 4 0 392 0}	00000100_2
		00000000_2
		10000011_2
		00001000_2
		00000000_2
ARGUMENT: tetraIsiMessage		
Sequence	Universal constructed sequence	00110000_2
	Length = 34 octets	00010111_2
SourceEntity	Context specific-primitive-tag 0	10000000_2
	length = 1 octet	00000001_2
	ANF-ISIGC	00000100_2
DestinationEntity	Context specific-primitive-tag 1	10000001_2
	length = 1 octet	00000001_2
	ANF-ISIGC	00000100_2
TetraMessage		
	Context specific-primitive-tag 2	10000010_2
	Length = 26 octets	00001111_2
PDU Type	SETUP INITIATE	100010_2
Selected area number	arbitrary value: 15	00001111_2
Controlling SwMI MNI	arbitrary value: 260 279	$010000010000000100010111_2$
Linking Group Identifier	Linking group GTSI not present	0_2
Originating SwMI MNI	arbitrary value: 260 279	$010000010000000100010111_2$
Call timeout	arbitrary value: 2	0010_2
Basic Service Information		

Circuit Mode Type	speech (0)	000_2
Encryption flag	Class 2 (1)	1_2
Communication type	Point-to-multipoint (1)	01_2
Speech Service	TETRA encoded speech(0)	00_2
Speech Service Chosen	CODEC	000_2
Security Level at Air Interface	Class 2	01_2
Call Priority	Priority not defined	0000_2
Call Ownership	Not a call owner	0_2
SS-COLR invoked for connected group	SS-COLR not invoked	0_2
Connected party SSI	arbitrary value: 11123420	$101010011011101011011100_2$
Connected Party Extension	arbitrary value: 260 279	$010000010000000100010111_2$
Number of external group member identified	arbitrary value: 0	0000_2
SS-CLIR invoked for calling party	SS CLIR not invoked	0_2
Calling party SSI	arbitrary value: 11123248	$101010011011101000110000_2$
Calling party extension	arbitrary value: 260 279	$010000010000000100010111_2$
External subscriber number length	arbitrary value: 0	00000_2
Temporary group member indication	The calling party is member of the group (0)	0_2
Dispatcher acceptance	SS-CAD not invoked (0)	0_2
Call amalgamation	Call is not amalgamated	0_2
Number of critical users	arbitrary value: 0	0000_2
Setup response time-out	2 seconds	0010_2
O-bit	No optional type 2 elements present	0_2
M-bit	No optional type 3/4 elements present	0_2

END of TetraMessage	
Extension	OMITTED

Annex C (informative): Change requests

The present document includes change requests as presented in table C.1.

Table C.1: Change requests

No	CR vers.	Standard Version	Clauses affected	Title	CR Status
001	01	1.1.2	2.1, 2.2, 6.3, 6.4, 6.5, 7.4.3, A.2.2.1	Correction to references	WG3 approved 190327

History

Document history		
V1.1.1	May 2018	Publication as ETSI TS 100 392-3-9
V1.2.0	August 2019	EN Approval Procedure AP 20191113: 2019-08-15 to 2019-11-13
V1.2.1	April 2020	Publication