ETSI TS 102 721-5 V1.1.1 (2011-12)

Satellite Earth Stations and Systems;
Air Interface for S-band Mobile Interactive Multimedia (S-MIM);
Part 5: Protocol Specifications, Link Layer

Reference
DTS/SES-00318-5

Keywords
MSS, satellite

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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 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 (http://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.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Satellite Earth Stations and Systems (SES).

The present document is part 5 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.11].

Introduction

The present document concerns the S-MIM (S-band Mobile Interactive Multimedia) system in which a standardised S-band satellite mobile broadcast system is complemented by the addition of a return channel.

The technology applied has been developed in the framework of the publicly co-funded project "S-MIM" (ESTEC / Contract Number 22439/09/NL/US).

The S-MIM system specified herein is designed to provide:

- Interactive mobile broadcast services.
- Messaging services for handhelds and vehicular terminals, capable of serving millions of terminals due to a novel optimised air-interface in the RTN link.
- Real-time emergency services such as voice and file transfer, mainly addressing institutional users on-the-move such as fire brigades, civil protection, etc.

Inside the S-band, the 2 GHz MSS band is of particular interest for interactive multimedia, since it allows two-way transmission. Typically, the DVB-SH standard [i.10] is applied for broadcast transmission; ESDR [i.5] is an alternative. Essential requirements under the R&TTE directive are covered by the harmonized standard EN 302 574 [i.7], [i.8] and [i.9].

1 Scope

The present document is part 5 of a multi-part deliverable and concerns aspects of the air interface for the S-band Mobile Interactive Multimedia (S-MIM) system, and in particular it specifies the Link Layer protocols.

The other parts are listed in the foreword of part 1 [i.11].

2 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 http://docbox.etsi.org/Reference.

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

2.1 Normative references

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

[1] ETSI EN 301 192: "Digital Video Broadcasting (DVB); DVB specification for data broadcasting".

[2] ETSI TS 102 721-3: "Satellite Earth Stations and Systems; Air Interface for S-band Mobile Interactive Multimedia (S-MIM); Part 3: Physical Layer Specification, Return Link Asynchronous Access".

[3] ETSI TS 102 721-4: "Satellite Earth Stations and Systems; Air Interface for S-band Mobile Interactive Multimedia (S-MIM); Part 4: Physical Layer Specification, Return Link Synchronous Access".

[4] ETSI TS 102 721-6: "Satellite Earth Stations and Systems; Air Interface for S-band Mobile Interactive Multimedia (S-MIM); Part 6: Protocol Specifications, System Signalling".

[5] ETSI TS 133 102 (V10.0.0): "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Security architecture [3GPP TS 33.102 V10.0.0]".

[6] ETSI TS 133 105 (V10.0.0): "Universal Mobile Telecommunications System (UMTS); LTE; Cryptographic algorithm requirements [3GPP TS 33.105 V10.0.0]".

[7] IETF RFC 2406: "IP Encapsulating Security Payload (ESP)".

[8] IETF RFC 2464: "Transmission of IPv6 Packets over Ethernet Networks".

[9] IETF RFC 3409: "Lower Layer Guidelines for Robust RTP/UDP/IP Header Compression".

[10] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

[11] IETF RFC 4815: "RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095".

[12] IEEE Std 802-2001 "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture".

[13] IETF Internet Draft 6LowPAN-hc-15: "Compression Format for IPv6 Datagrams in Low Power and Lossy Networks (6LowPAN)".

2.2 Informative references

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 TS 102 611-1: "Digital Video Broadcasting (DVB); IP Datacast: Implementation Guidelines for Mobility; Part 1: IP Datacast over DVB-H".

[i.2] ETSI TS 102 611-2: "Digital Video Broadcasting (DVB); IP Datacast: Implementation Guidelines for Mobility; Part 2: IP Datacast over DVB-SH".

[i.3] ETSI TS 102 470-1: "Digital Video Broadcasting (DVB); IP Datacast: Program Specific Information (PSI)/Service Information (SI); Part 1: IP Datacast over DVB-H".

[i.4] IANA: "Robust Header Compression (ROHC) Profile identifiers".

NOTE: Available at http://www.iana.org/assignments/rohc-pro-ids/.

[i.5] ETSI EN 302 550: "Satellite Earth Stations and Systems (SES); Satellite Digital Radio (SDR) Systems", all parts and sub-parts.

[i.6] ETSI EN 301 545-2: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 2: Lower Layers for Satellite standard".

[i.7] ETSI EN 302 574-1: "Satellite Earth Stations and Systems (SES); Harmonized standard for satellite earth stations for MSS operating in the 1 980 MHz to 2 010 MHz (earth-to-space) and 2 170 MHz to 2 200 MHz (space-to-earth) frequency bands; Part 1: Complementary Ground Component (CGC) for wideband systems: Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive".

[i.8] ETSI EN 302 574-2: "Satellite Earth Stations and Systems (SES); Harmonized standard for satellite earth stations for MSS operating in the 1 980 MHz to 2 010 MHz (earth-to-space) and 2 170 MHz to 2 200 MHz (space-to-earth) frequency bands; Part 2: User Equipment (UE) for wideband systems: Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive".

[i.9] ETSI EN 302 574-3: "Satellite Earth Stations and Systems (SES); Harmonized standard for satellite earth stations for MSS operating in the 1 980 MHz to 2 010 MHz (earth-to-space) and 2 170 MHz to 2 200 MHz (space-to-earth) frequency bands; Part 3: User Equipment (UE) for narrowband systems: Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive".

[i.10] ETSI TS 102 585: "Digital Video Broadcasting (DVB); System Specifications for Satellite services to Handheld devices (SH) below 3 GHz".

[i.11] ETSI TS 102 721-1: "Satellite Earth Stations and Systems; Air Interface for S-band Mobile Interactive Multimedia (S-MIM); Part 1: General System Architecture and Configurations.".

[i.12] IETF RFC 4193: "Unique Local IPv6 Unicast Addresses".

[i.13] IETF RFC 2462: "IPv6 Stateless Address Autoconfiguration".

[i.14] IETF RFC 3095: " RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed".

[i.15] IETF RFC 4944: "Transmission of IPv6 Packets over IEEE 802.15.4 Networks".

[i.16] DVB BlueBook A155-1 "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (RCS2); Part 1: Overview and System Level specification", March 2011.

NOTE: Available at www.dvb.org.

[i.17] DVB BlueBook A155-2 "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System; Part 2: Lower Layers for Satellite standard", March 2011.

NOTE: Available at www.dvb.org.

3 Definitions and abbreviations

3.1 Definitions

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

2 GHz MSS band: 1 980 to 2 010 MHz (earth-to-space) and 2 170 to 2 200 MHz (space-to-earth) frequency bands

NOTE: These paired bands are assigned to MSS.

architecture: abstract representation of a communications system

NOTE: Three complementary types of architecture are defined:

- Functional Architecture: the discrete functional elements of the system and the associated logical interfaces.
- Network Architecture: the discrete physical (network) elements of the system and the associated physical interfaces.
- Protocol Architecture: the protocol stacks involved in the operation of the system and the associated peering relationships.

collector: terrestrial components that "collect" return link transmissions from terminals and forward them towards the ground segment

control plane: plane that has a layered structure and performs the call control and connection control functions; it deals with the signalling necessary to set up, supervise and release calls and connections

flow (of IP packets): traffic associated with a given connection-oriented, or connectionless, packet sequence having the same 5-tuple of source address, destination address, Source Port, Destination Port, and Protocol type

management plane: plane that provides two types of functions, namely layer management and plane management functions:

- **Plane management functions:** performs management functions related to a system as a whole and provides co-ordination between all the planes. Plane management has no layered structure.
- **Layer Management functions:** performs management functions (e.g. meta-signalling) relating to resources and parameters residing in its protocol entities.

repeater: terrestrial components that (mainly) repeat the satellite signal in the forward link

S-band: equivalent to 2 GHz MSS band

user plane: plane that has a layered structure and provides user information transfer, along with associated controls (e.g. flow control, recovery from errors, etc.)

3.2 Abbreviations

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

3G	Third generation mobile services,
3GPP	Third Generation Partnership Project
ACK	Acknowledgement
ALPDU	Addressed Link Protocol Data Unit
ARQ	Automatic Repeat reQuest
AuC	Authentication Centre
BCC	Bidirectional Compressed Channel
CAC	Call Admission Control
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CD	Compact Disk

CDMA	Code Division Multiple Access
CGC	Complementary Ground Component
CID	Context Identifier
CoS	Class of Service
CRC	Cyclic Redundancy Check
DAMA	Dynamic Assignment Multiple Access
DCH	Dedicated Channel
DCI	Destination Context Identifier
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DVB-H	Digital Video Broadcasting, services to Handhelds
DVB-RCS2	DVB Return Channel for Satellite 2nd generation
DVB-SH	Digital Video Broadcasting, Satellites services to Handhelds
DVB-SHrt	DVB-SH with real time features
EC	Encrypted Channel
ESP	Encapsulated Security Payload
E-SSA	Enhanced Spread Spectrum Aloha
ETSI	European Telecommunication Standards Institute
FWD	Forward
GHz	Giga Hertz
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSE	Generic Stream Encapsulation
HLR	Home Location Register
HNO	Home Network Operator
IANA	Internet Assigned Numbers Authority
ID	Identifier
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	IP Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	Initialisation and Refresh state
IS	Interface Satellite
L2	Layer 2
LAI	Local Area Identifier
LC	Load Control
LLC/SNAP	Logical Link Control/Sub-Network Access Protocol
MAC	Medium Access Control
MCC	Mobile Country Code
MPE	Multiprotocol Encapsulation
MPEG	Moving Pictures Experts Group
MPEG-TS	MPEG Transport Stream
MPE-IFEC	MPE Inter-burst FEC
MSB	Most Significant Bit
MSS	Mobile Satellite Services
NCC	Network Control Centre
nCC	Non-Compressed Channel
NEC	Non-Encrypted Channel
NRT	Non-Real Time
NRTP	Non-Real Time Pipe
PCCH	Physical Control Channel
PCH	Physical Channel
PDCH	Physical Data Channel
PDU	Protocol Data Unit
PHY	Physical Layer
PID	Packet Identifier
PLR	Packet Loss Ratio
PPDU	Payload-adapted Protocol Data Unit
PSI/SI	Program Specific Information/Service Information

QS-CDMA	Quasi Synchronous CDMA
RACH	Random Access Channel
RFC	Request for Comment
RLE	Return Link Encapsulation
RM	Resource Management
ROHC	Robust Header Compression
RTN	Return (link)
RTP	Real Time Pipe
RTP	Real Time Protocol
SA	Security Association
SAT	SSA Access Table
SCI	Source Context Identifier
SDR	Satellite Digital Radio
SFN	Single Frequency Network
S-MIM	S-band Mobile Interactive Multimedia
SS	Subsystem
SS1	Service Segment 1
SS2	Service Segment 2
SS3	Service Segment 3
SSA	Spread Spectrum Aloha
TCP	Transmission Control Protocol
TMSI	Temporary Mobile Subscriber Identity
UACK	Unequivocally Acknowledged Mode
UCC	Unidirectional Compressed Channel
UDP	User Datagram Protocol
ULA	Unique Local addressing
UMTS	Universal Mobile Telecommunications System
UsCC	Unidirectional stateless Compressed Channel
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
VoIP	Voice over IP General Description

4 General Description

The S-MIM Link Layer provides a number of functionalities that will allow transport of IP traffic of different types (broadcast, messaging, bidirectional traffic) over the radio interfaces of the S-MIM system.

The Link Layer implements the following functions:

- Header Compression to reduce the overhead transmitted over the system
- Encapsulation to transport the higher layer packets over the air interfaces of the S-MIM system
- MAC Layer Addressing
- ARQ for reliable link layer transmission
- Load control
- Call Admission Control/DAMA
- Security mechanisms
- Mobility Management

The related protocols are specified in the present document.

4.1 Forward Link

The detailed protocol stack for the S-MIM link and physical layers for access to SS1, SS2 and SS3 in the Forward Link is depicted in Figure 4.1.

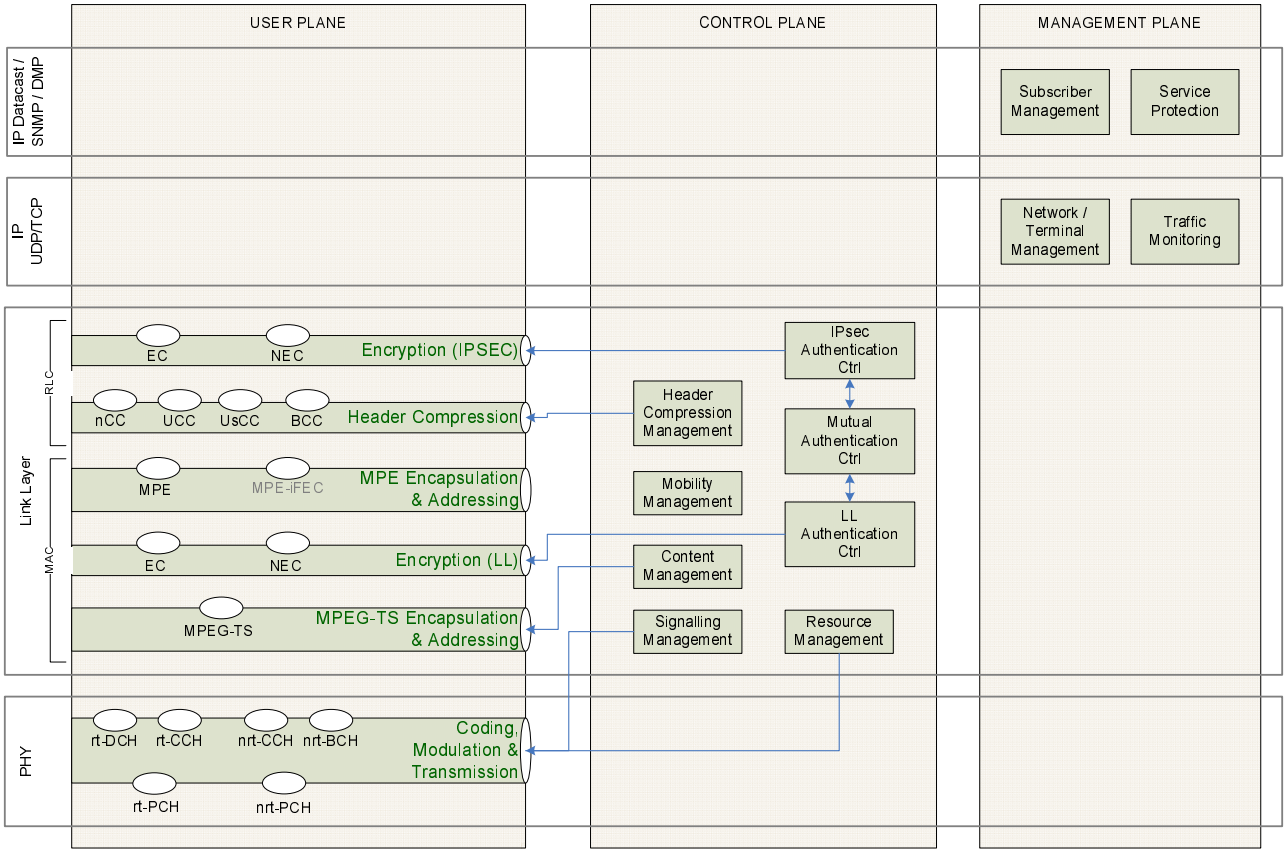

Figure 4.1: Detailed protocol stack for the Forward Link

4.1.1 Encryption Sub-layers

The encryption functions are split in two sublayers: at IP and at MAC layers to provide security in the access to the S-MIM communications system. In practice, hub and terminals will negotiate at which level encryption is applied (this will depend on the capabilities of the communication peers) and upon successful negotiation, encryption will be only applied at the agreed level by both peers according to the most restrictive capability. Both Encryption sub-layers, managed by the mutual authentication control function, provide two access services to the respective underlying sub-layer:

- Encrypted Channel (EC): upper layer packets mapped into this access service will be transmitted encrypted.
- Non-Encrypted Channel (NEC): upper layer packets mapped into this access service will be transmitted not encrypted.

4.1.2 Header Compression Sub-layer

The Header Compression sub-layer provides four access services (also called header compression channels) to the higher layer:

- Non-Compressed Channel (nCC): IP packets accessing through this service will be transmitted with uncompressed header. This header compression channel can be accessed by all applications and services in FWD and RTN links.
- Unidirectional Compressed Channel (UCC): IP packets accessing through this service will be transmitted with compressed header using the technique as specified in clause 5. This header compression channel can be accessed by SS1 broadcast/multicast applications (streaming, datacast) and services in the FWD link.
- Unidirectional stateless Compressed Channel (UsCC): IP packets accessing through this service will be transmitted with compressed header using the technique as specified in clause 5. This header compression channel can be accessed by short message application services in the FWD link.

- Bidirectional Compressed Channel (BCC): IP packets accessing through this service will be transmitted with compressed header using the technique as specified in clause 5. This header compression channel can be accessed by real-time bidirectional services in the FWD.

For the user plane, all four access services can be used. For the control plane, most of the data is system signalling that is generated below IP, and therefore header compression is not applicable. Signalling applied to support synchronisation of compression profiles in the Bidirectional Compressed Channel shall be transmitted with uncompressed header.

For the management plane, the higher layer signalling that deals with network and terminal management can access all four access services of the Header Compression sub-layer.

4.1.3 Encapsulation and Addressing sub-layers

Encapsulation and addressing is split in two sub-layers, one at MPE level and another one at MPEG-TS level. This splitting serves the possibility to insert MAC layer encryption in the Forward Link. These sub-layers shall provide the following encapsulation services in the FWD link:

- MPE Encapsulation:
  - MPE Encapsulation (mandatory)
  - MPE-iFEC Encapsulation (optional, only compatible with DVB-SH)
- MPEG Encapsulation.

NOTE: MPE-iFEC is only compatible with NRT broadcast. Unicast traffic needs a MAC address in the MPE header, which is incompatible with MPE-iFEC.

All planes (user, control and management) shall have access to the mandatory access services of this sub-layer.

In terms of addressing, broadcast, multicast and unicast addressing is supported in the S-MIM forward radio interface. Different descriptors can be used for addressing as defined in [1].

4.2 Return Link

The SSA and QS-CDMA options are described separately below.

4.2.1 Asynchronous Access

The detailed protocol stack for the S-MIM link any physical layers for access to SS1, SS2 in the Asynchronous Return Link is depicted in Figure 4.2.

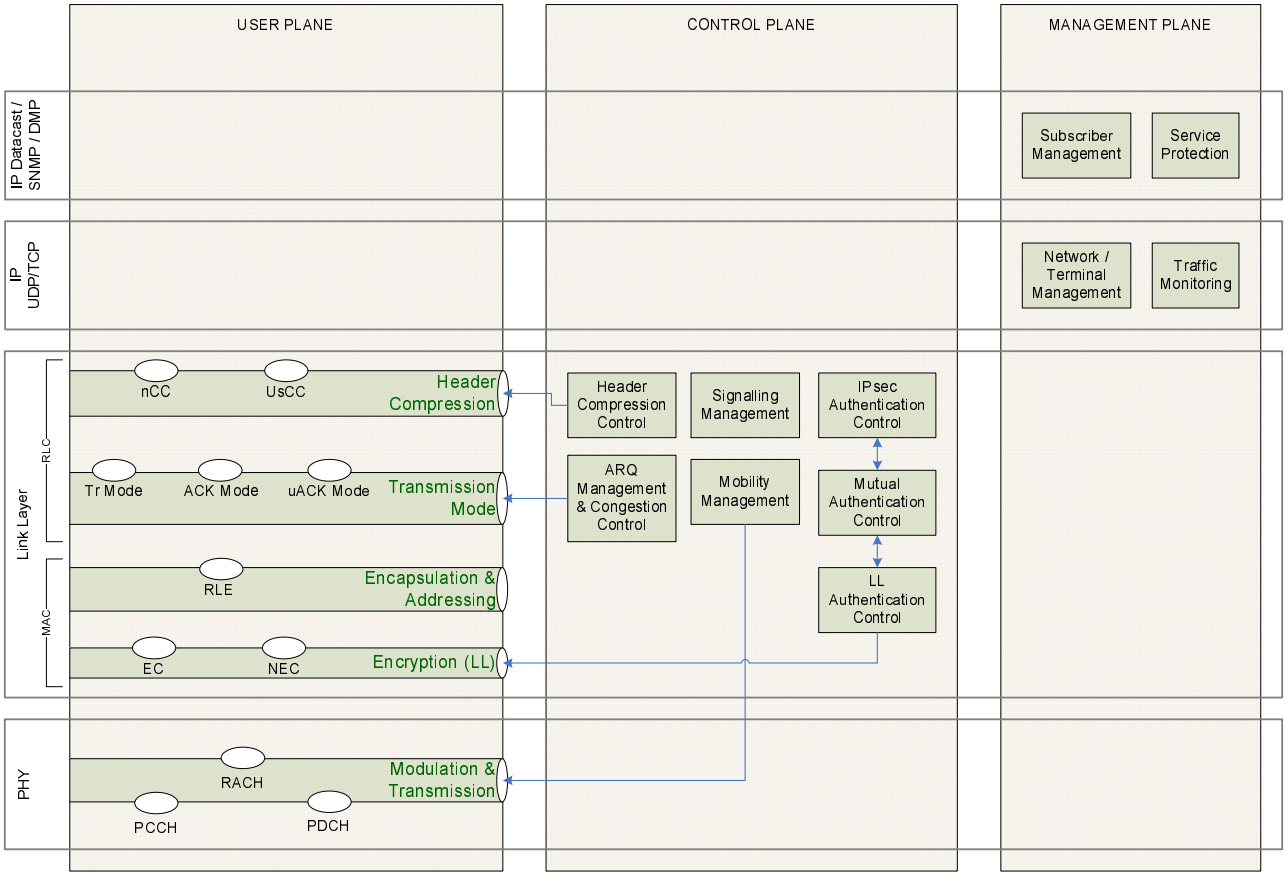

Figure 4.2: Detailed protocol stack for the Asynchronous Return Link

4.2.1.1 Header Compression Sub-layer

The Header Compression sub-layer provides two access services to the IP layer:

- Non-Compressed Channel (nCC).
- Unidirectional stateless Compressed Channel (UsCC).

These are as defined in clause 4.1.2.

4.2.1.2 Transmission Mode sub-layer

The Transmission Mode sub-layer, managed by the ARQ Management and Load control function, offers three access services to the Header Compression sub-layer:

- Transparent Mode (Tr Mode): PDUs mapped into this transmission mode will be transmitted without expecting any link layer acknowledgements in the forward link.
- Acknowledged Mode (ACK Mode): PDUs mapped into this transmission mode will require a link layer CRC-based acknowledgement in the forward link, as specified in clause 8.
- Unequivocally Acknowledged Mode (uACK Mode): PDUs mapped into this transmission mode will require a link layer dedicated and uniquely addressed ACK message in the forward link as specified in clause 8.

4.2.1.3 Encapsulation and Addressing sub-layer

The Encapsulation sub-layer offers one access service to the Transmission Mode sub-layer:

- RLE: Return Link Encapsulation.

Hence, RLE is used to encapsulate higher layer packets and to insert the system specific MAC layer addressing. The MAC layer addresses applied are specified in clause 7.

4.2.1.4 Encryption sub-layer

The encryption sub-layer, only in the link layer in the case of the return link, managed by the link layer authentication control, provide two access services to the Encapsulation and Addressing sub-layer:

- Encrypted Channel (EC): upper layer packets mapped into this access service will be transmitted encrypted, as specified in clause 11.
- Non-Encrypted Channel (NEC): upper layer packets mapped into this access service will be transmitted not encrypted.

4.2.2 Synchronous Access

The detailed protocol stack for the S-MIM link any physical layers for access to SS3, in the Synchronous Return Link is depicted in Figure 4.3.

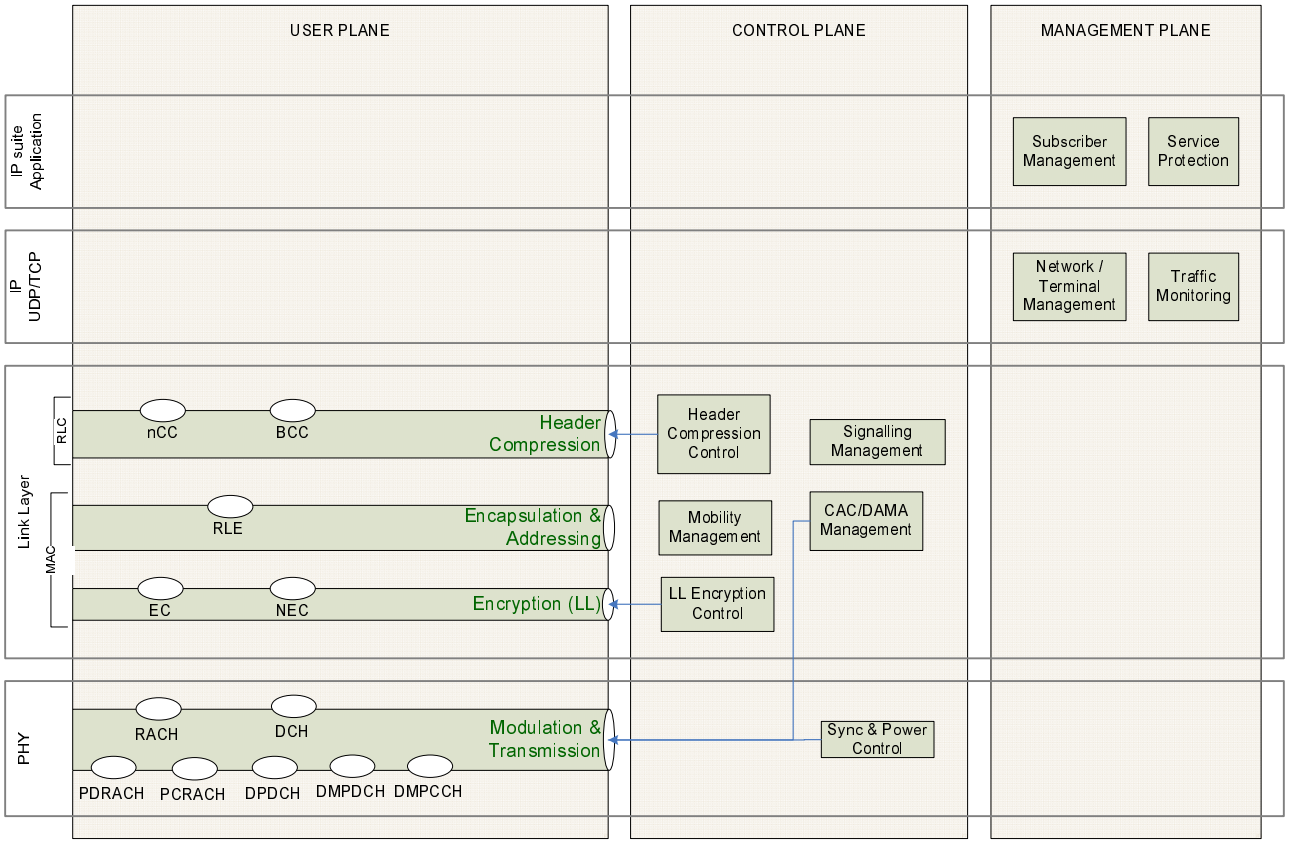

Figure 4.3: Detailed protocol stack for the Synchronous Return Link

4.2.2.1 Header Compression sub-layer

The Header Compression sub-layer provides two access services (also called header compression channel) to the IP layer:

- Non-Compressed Channel (nCC): IP packets accessing through this service will be transmitted with uncompressed header. This header compression channel can be accessed by all applications and services in FWD and RTN links.
- Bidirectional Compressed Channel (BCC): IP packets accessing through this service will be transmitted with compressed header using the technique as specified in clause 5. This header compression channel can be accessed by bidirectional services under SS3.

4.2.2.2 Encapsulation and Addressing sub-layer

The Encapsulation sub-layer offers one access service to the Transmission Mode sub-layer:

- RLE: Return Link Encapsulation.

Hence, RLE is used to encapsulate higher layer packets and to insert the system specific MAC layer addressing. The MAC layer addresses applied are specified in clause 7.

4.2.2.3 Encryption sub-layer

The encryption sub-layer, only in the link layer in the case of the return link, managed by the link layer authentication control, provide two access services to the Encapsulation and Addressing sub-layer:

- Encrypted Channel (EC): upper layer packets mapped into this access service will be transmitted encrypted, as specified in clause 11.
- Non-Encrypted Channel (NEC): upper layer packets mapped into this access service will be transmitted not encrypted.

5 Header Compression

The Header Compression sub-layer provides four access services (also called header compression channels in the present document) to the IP layer, as can be observed in Figure 5.1 and Figure 5.2:

- Non-Compressed Channel (nCC): IP packets accessing through this service will be transmitted with uncompressed header. This header compression channel can be accessed by all applications and services in FWD and RTN links. The traffic going through the path of the NCC can be mapped in all air interfaces of the FWD and RTN link of the S-MIM system.
- Unidirectional Compressed Channel (UCC): IP packets accessing through this service will be transmitted with compressed header using an adaptation of RoHC in unidirectional mode that will be specified in the following clauses. This header compression channel can be accessed by SS1 broadcast/multicast applications (streaming, datacast) and services in the FWD link. The traffic going through the path of the UCC can be mapped in the Non Real Time Pipe (NRTP) of the FWD air interface.
- Unidirectional stateless Compressed Channel (UsCC): IP packets accessing through this service will be transmitted with compressed header using an adaptation of the RFC 4944 [i.15] that will be specified in the following clauses. This header compression channel can be accessed by short message application services in the FWD and RTN links. The traffic going through the path of the UsCC can be mapped in the Real Time Pipe (RTP) or the Non Real Time Pipe (NRTP) of the FWD air interface and on the SSA air interface of the RTN link.
- Bidirectional Compressed Channel (BCC): IP packets accessing through this service will be transmitted with compressed header using an adaptation of RoHC in bidirectional mode. This header compression channel can be accessed by real-time bidirectional services in the FWD and RTN links. The traffic going through the path of the BCC can be mapped in the Real Time Pipe (RTP) of the FWD air interface and on the QS-CDMA air interface of the RTN link.

For the user plane, all four access services can be used. For the control plane, most of the data is system signalling that is generated below IP. However, some signalling to support the Bidirectional Compressed Channel shall be supported to synchronize compression profiles. It is therefore reasonable to state that this signalling will be transmitted with uncompressed header.

For the management plane, the higher layer signalling that deals with network and terminal management can access all four access services of the Header Compression Sub-layer.

The following clauses specify each of the protocols associated to each header compression channel.

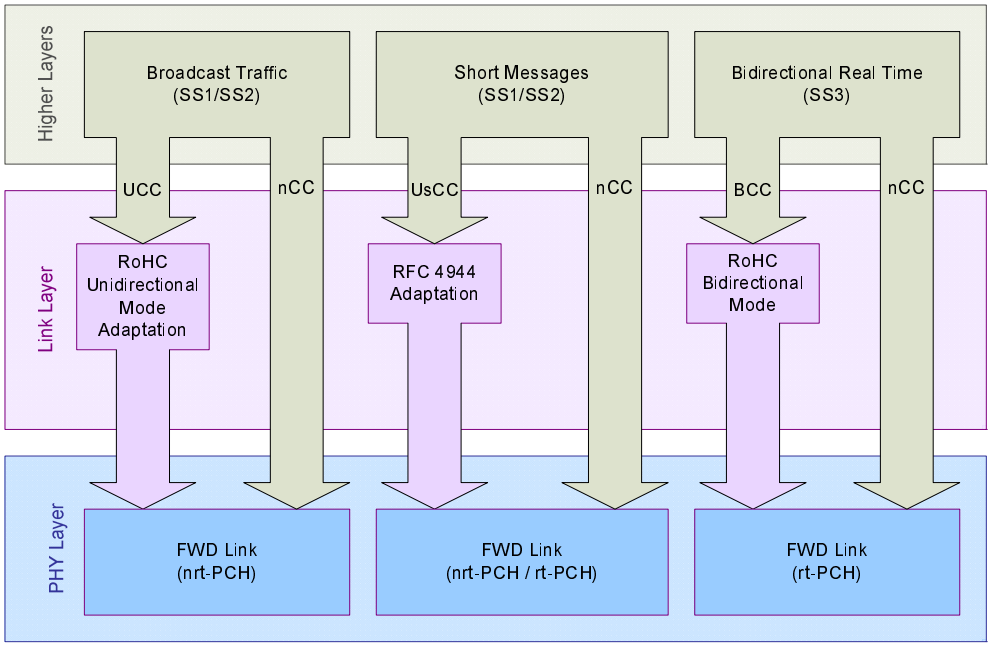

Figure 5.1: Header compression services in the FWD link

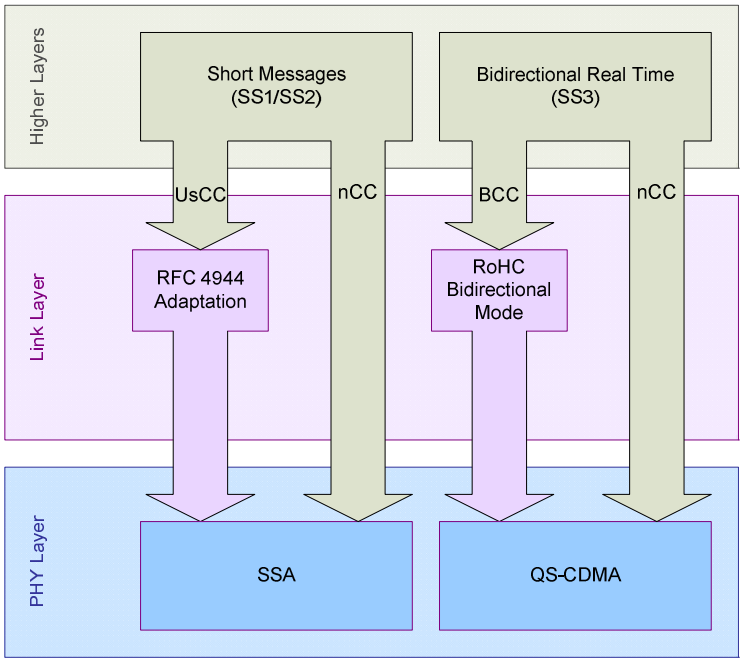

Figure 5.2: Header compression services in RTN link

5.1 Header Compression for Broadcast/Multicast Services

The use of header compression on broadcast/Multicast service is optional. If header compression is used, these services shall use a modified version of ROHC [11] as specified in this clause.

ROHC shall be used in the following configuration:

- Unidirectional mode.
- Multicast IP should not be discarded at the compressor, but be processed as normal unicast packets.

The state diagram of the compressor shall be the one defined in Figure 5.3.

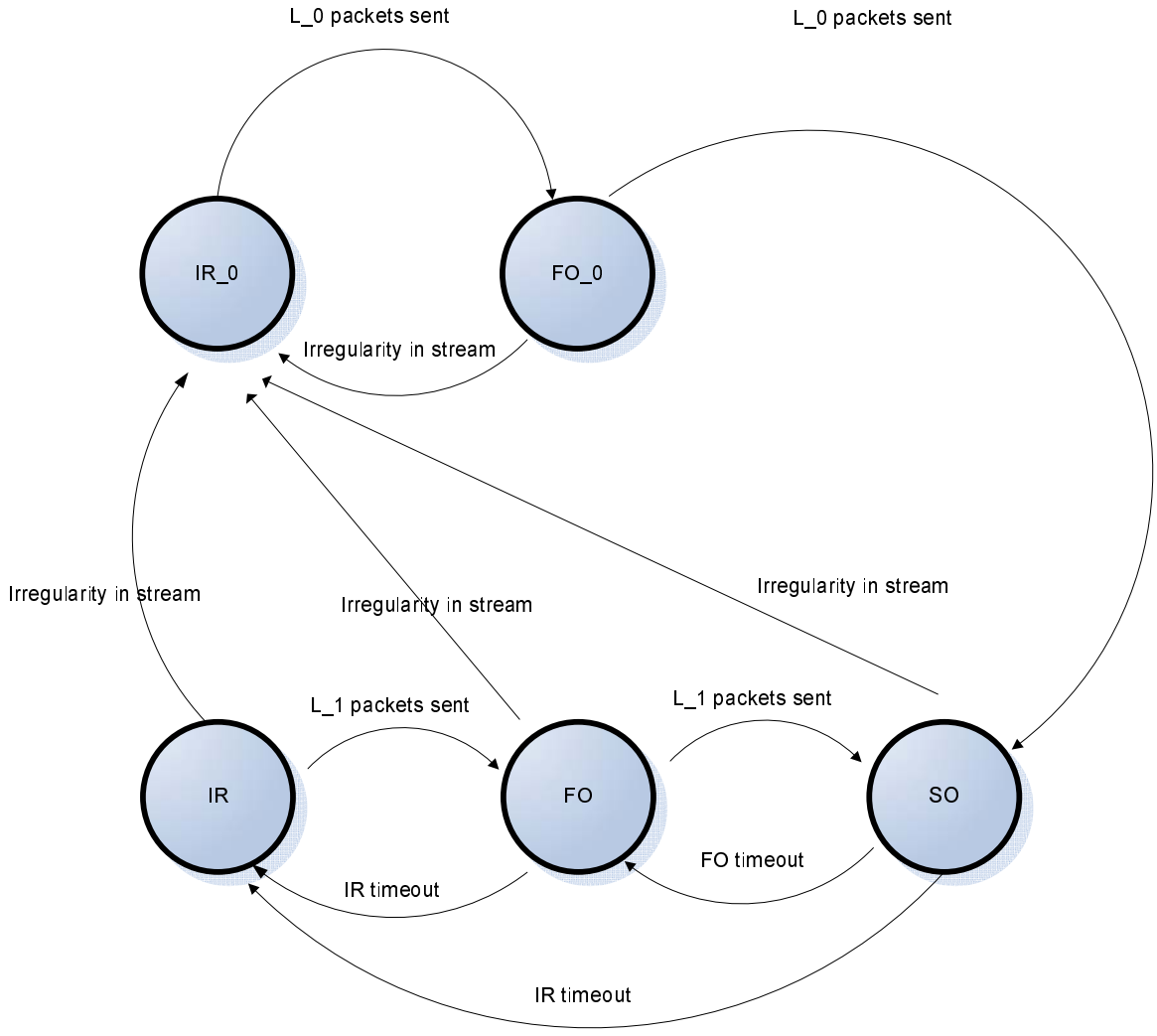

Figure 5.3: Modified ROHC compressor diagram

The behaviour in states IR_0 and IR is identical. The same applies for states FO_0 and FO.

The compressor starts in state IR_0. It only goes back to this state if some irregularity happens in the stream (unpredictable behaviour of some of the fields of the headers).

This compressor state diagram is introduced in order to minimize the mean size of the compressed header while providing a low zap time to the users.

In order to minimize zap time for users L_1 should be set to its minimum value, 1 packet. FO_timeout shall not be used (set to infinite). And IR_timeout shall be as low as possible, taking into account that the mean waiting time for a user to receive the context is IR_timeout/2 and the maximum waiting time for a user to get the context is IR_timeout. IR_timeout shall be in the order of a few seconds.

L_0 shall be sent to a value higher than 1 in order to avoid that an irregularity in the stream (unpredictable change) leads to loosing a burst of packets (the number of packets sent in IR_timeout).

5.2 Header Compression for Short Messages

These services are connectionless and will use UDP/IP. These services are static in the sense that the parameters used for the communication (IP addresses and port numbers) do not vary in a long period of time.

Header compression is optional for these services. Header compression can be applied separately in the FWD and RTN link (header compression may be used only in one of the links).

In case header compression is used, the header compression protocol defined in this clause shall be used for both FWD and RTN link. This header compression protocol is a modified version of RFC 4944 [i.15]. This mechanism allows compressing the IPv6 and UDP headers from 48 bytes down to 5 bytes (7 bytes if a CRC is used).

This mechanism allows applying header compression to 256 different services in the same return link. At the terminal side it allows to use header compression for up to 256 different UDP sockets.

This clause describes a modified version of the draft update of RFC 4944 [i.15] to tailor it to the needs of the S-MIM system. The modifications introduced are the following:

- Increase of the size of the CID extension.
- Different way of compressing UDP ports. Stateful compression of UDP ports is now supported allowing the 16 bits of source and destination port to be elided.

Figure 5.4 shows the base encoding; the meaning of each field is specified in [13].

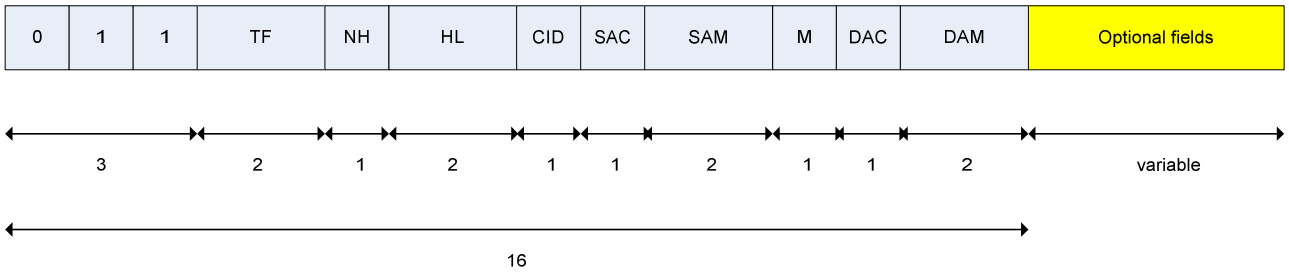

Figure 5.4: LOWPAN_HC base encoding

5.2.1 Context Identifier extension

Instead of defining 16 different contexts (4 bits) for source and destination addresses, the size of the context identifier extension has been increased so that now there are 256 contexts for source and destination (8 bits each). This allows the compression scheme to support up to 256 different service centres in the system, and at the terminal side it supports the use of up to 256 different UDP ports.

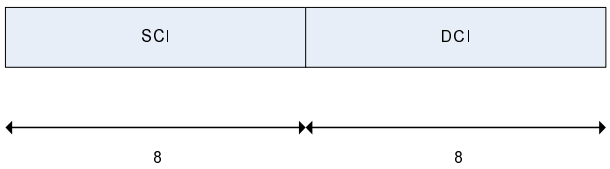

Figure 5.5: LOWPAN_IPHC Encoding of CID Extension

- SCI: Source Context Identifier: it identifies the prefix that is used when the IPv6 source address is statefully compressed.

- DCI: Destination Context Identifier: it identifies the prefix that is used when the IPv6 destination address is statefully compressed.

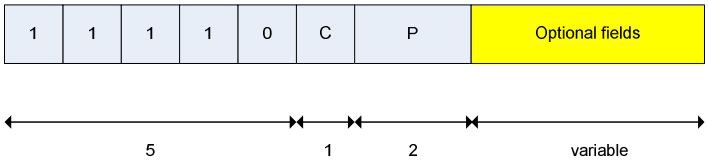

Figure 5.6: Updated RFC 4944 [i.15] LOWPAN_NHC header format

The header of the LOWPAN_NHC for UDP compression is shown in Figure 5.6. In comparison to the draft update of RFC 4944 [i.15] the port field (P) of LOWPAN_NHC has been changed:

- C, Checksum. This 1 bit field can take the following values:
  - 0: All 16 bits of Checksum are carried in-line. The Checksum MUST be included if there are no other end-to-end integrity checks that are stronger than what is provided by the UDP checksum. Such an integrity check MUST be end-to-end and cover the IPv6 pseudo-header, UDP header, and UDP payload.
  - 1: All 16 bits of Checksum are elided. The Checksum is recovered by recomputing it.
- P, Ports. This 2 bits long field can take the following values:
  - 00: All 16 bits for both Source Port and Destination Port are carried in-line.
  - 01: All 16 bits for Source Port are carried in-line. First 8 bits of Destination Port is 0xF0 and elided. The remaining 8 bits of Destination Port are carried in-line.
  - 10: First 8 bits of Source Port are 0xF0 and elided. The remaining 8 bits of Source Port are carried in-line. All 16 bits for Destination Port are carried in-line.
  - 11: All bits of both Source Port and Destination Port are elided. The ports can be derived using context information.

If updated RFC 4944 [i.15] is used to compress packets in the return link, the packet would look as shown in Figure 5.7. The following assumptions have been made:

- TF=11: Version, Traffic Class, and Flow Label field are not necessary (IP version is 6, and Traffic Class and Flow Label are always 0).
- NH=1: Transport layer protocol compressed.
- HL=11: Hop limit is 255.
- CID=1: Each service would use a different CID. We support up to 256 different services.
- SAC=0 and SAM=11: The source address can be derived from the MAC address.
- M=0: Destination Address is not multicast.
- DAC=1 and DAM= 11: The destination address is derived using context information.
- CID_Extension.
- C=0: No UDP checksum is sent. It might be necessary to send the CRC for some services.
- P=11: The source and destination UDP ports are elided; they can be derived from the context information.

Making all these suppositions the UDP/IPv6 header can be reduced to 40 bits (5 bytes).

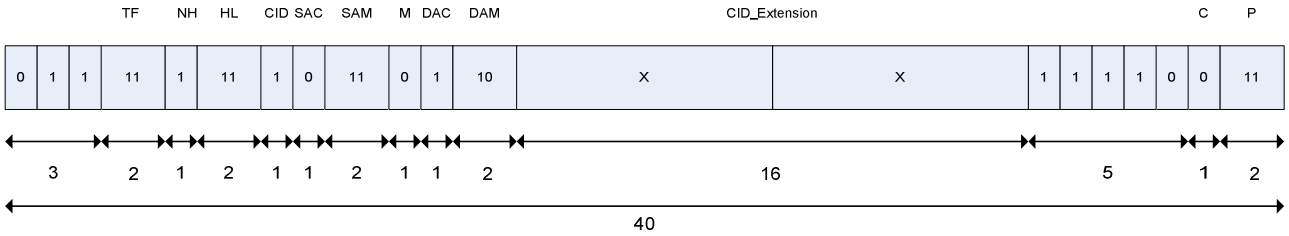

Figure 5.7: Example of compressed header using modified 6LOWPAN header compression

If updated RFC 4944 [i.15] is used to compress packets in the forward link, the packet would look as shown in Figure 5.7. The following assumptions have been made:

- TF=11: Version, Traffic Class, and Flow Label field are not necessary (IP version is 6, and Traffic Class and Flow Label are always 0).
- NH=1: Transport layer protocol compressed.
- HL=11: Hop limit is 255.
- CID=1: Each service would use a different CID. We support up to 256 different services (source address and port). There are also 256 different CID for the destination (256 different UDP ports can be addressed at each terminal).
- SAC=1 and SAM=11: The source address is elided. It can be completely derived from the context.
- M= 0: Destination Address is not multicast.
- DAC=1 and DAM= 11: The destination address and port are derived using context information.
- CID_Extension: The CID extension for source will correspond with the service and the CID extension for destination will be used to address different ports at the receiver.
- C=0: No UDP checksum is sent. It might be necessary to send the CRC for some services.
- P=11: The source and destination UDP ports are elided, they can be derived from the context information.

Making all these suppositions the UDP/IPv6 header can be reduced to 32 bits (4 bytes) whereas using standard 6LOWPAN header compression the size of the compressed header was 48 bits.

5.3 Header Compression for Bidirectional Services

The RoHC standard, [11] provides a good framework for header compression for large delay and error prone links and is proposed as the header compression schema for bidirectional services. Besides the unidirectional mode proposed for broadcast and multicast services in clause 5.3, the standard defines two additional modes of operation that may be used when a feedback channel is available:

- Bidirectional Optimistic Mode (O-mode): This mode aims to maximize the compression efficiency and sparse usage of the feedback channel.

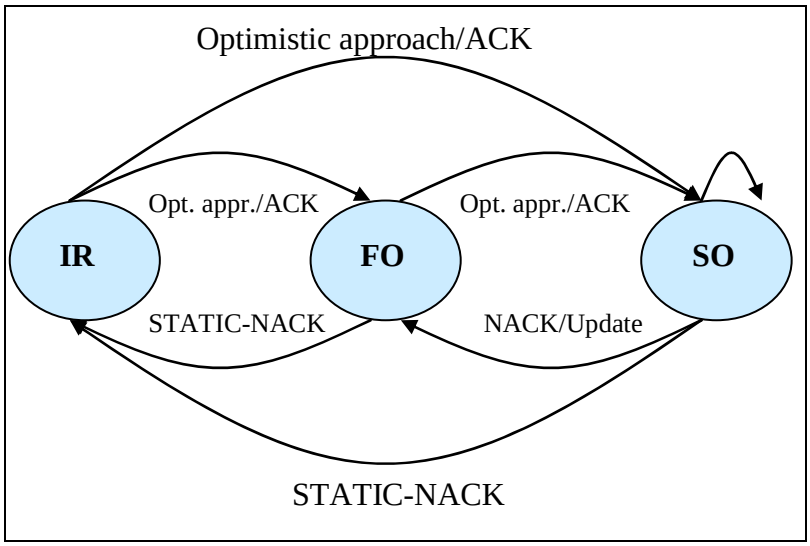

Figure 5.8: RoHC O-mode states diagram

- Bidirectional Reliable Mode (R-mode): This mode aims to maximize the robustness against loss propagation and damage propagation by an intensive usage of the feedback channel.

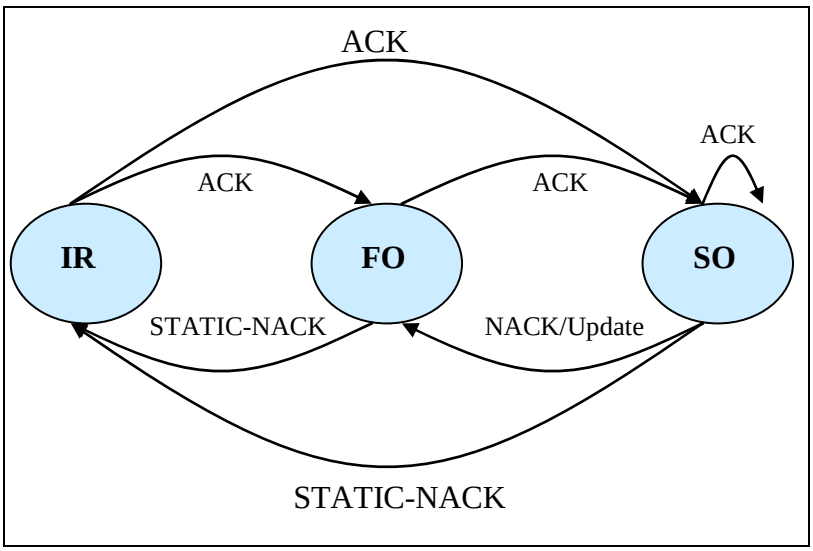

Figure 5.9: RoHC R-mode states diagram

5.3.1 Feedback Messages

For both O-mode and R-mode a feedback logical channel is required for the decompressor instance to send messages towards the associated compressor instance, this scenario is depicted by Figure 5.10.

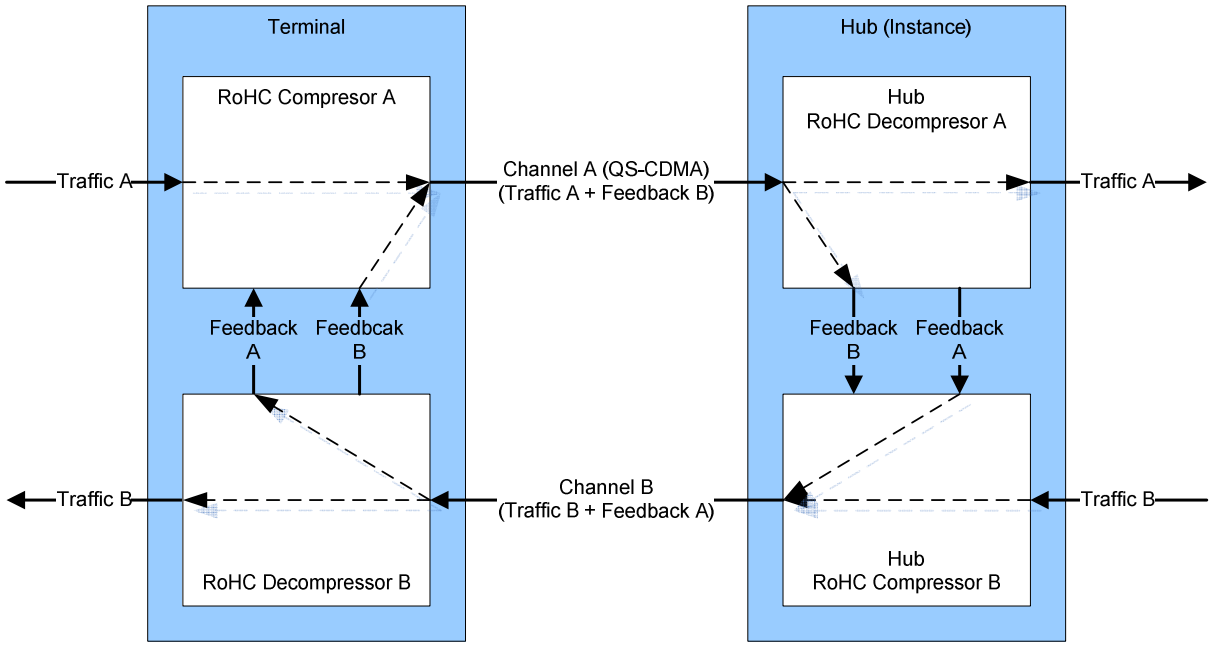

Figure 5.10: RoHC logical channels

Feedback messages consist of small RoHC packets without any application payload which can reach the compressor in three different ways:

- The interspersed feedback mode provides a mechanism to send the feedback messages as stand-alone packets among RoHC compressed packets in the same direction as the feedback channel.
- The piggybacked feedback mode provides a mechanism to send feedback messages encapsulated inside the headers of RoHC compressed packets in the same direction as the feedback channel.
- The dedicated feedback channel mode relies in the ability of the lower layers to provide a dedicated (logical) channel(s) to send the feedback messages.

5.3.1.1 Piggybacked or interspersed mode

The piggybacked mode method is preferable as it saves the large overhead introduced by the link layer encapsulation due to the very small size of the RoHC feedback packets.

The format of the feedback packet is shown in Figure 5.11.

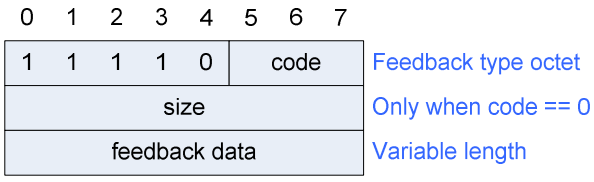

Figure 5.11: Piggybacked and interspersed RoHC feedback message format

The semantics of the feedback message are:

- *code*: When 0, indicates that a size field is present. Otherwise, a value in the range of 1 to 7 indicates the size of the feedback data field in bytes.
- *size*: When present, this field indicates the size of the feedback data field in bytes.
- *feedback data*: This is a profile specific feedback information which also includes the CID information. The semantics of this field are out of the scope of the present document and can be found in [11] and [1].

5.3.1.2 Dedicated channel mode

In case that the feedback message is sent through a dedicated feedback channel, its format shall be modified to that shown in Figure 5.12.

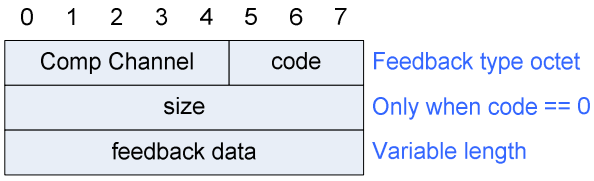

Figure 5.12: Dedicated channel RoHC feedback message format

The semantics of the feedback message are:

- *comp channel*: This field helps to identify to which compressor instance the feedback message shall be forwarded. This field shall be replaced by the 11110b sequence for the compressor to identify that the packet is a feedback message.
- *code*: as for standard semantics.
- *size*: as for standard semantics.
- *feedback data*: as for standard semantics.

The Hub shall create a compressor/decompressor pair of instances for each active channel against a terminal.

5.3.2 Encapsulation

Network datagrams, IPv4 and IPv6, are compressed with the RoHC technology and then passed through the layer 2 encapsulation which shall provide the functionalities below, from [9] and [11]:

- Error detection: Lower layers must detect errors in the reconstructed compressed datagram. It is recommended, though, that such invalid packets are passed up to the decompressor with an error mark.
- Packet length: RoHC is designed under the assumption that lower layers indicate the length of a compressed packet.
- Framing: The link layer must provide framing that makes it possible to distinguish frame boundaries and individual frames.
- Duplication and reordering: The channel between compressor and decompressor is required to not to duplicate and keep packet ordering.

Both RLE and MPE encapsulation methods used for the provision of Bidirectional services guarantee the assumptions above.

5.3.2.1 Encapsulation with MPE

The services provided through the forward link are based in MPE over MPEG2-TS. That is, all network datagrams shall be encapsulated with an MPE *datagram_section* as specified in [1].

- *LLC_SNAP_flag* shall be set to "1" and the payload type (IPv4/IPv6 ROHC Compressed) must be signalled through the LLC_SNAP structure.

In case feedback messages are not piggybacked but sent through a dedicated feedback channel, they shall be encapsulated in the QS-CDMA RoHC Feedback Message descriptor as it is defined in Part 8 [4].

5.3.2.2 Encapsulation with RLE

In the return link, the compressed network datagrams are encapsulated through the RLE protocol and identified with dedicated logical channels, as it is defined in clause 6.2.1, therefore the RLE *protocol_type* field can be omitted to reduce the overhead introduced by the encapsulator.

In case feedback messages are not piggybacked but generated as stand-alone packets, a specific logical channel shall be defined too, see clause 6.2.1.

5.3.3 RoHC parameters

The RoHC protocol is based on a number of parameters that form part of the negotiated channel state and per-context state.

- *rohc_large_cid*: This flag indicates whether short (0 or 1 byte) or large (1 or 2 bytes) CID identifiers are used.
- *rohc_max_cid*: This parameter constraints the maximum number of context identifiers (CIDs) to be used by the compressor.
- *rohc_profiles:* This parameter specifies the profiles supported by the decompressor. The compressor must not compress using a profile not supported by the decompressor. IANA standardizes RoHC profile identifiers [i.4], however in order to reduce the size of the negotiated descriptors the bit-mask of the Table 5.1 are used instead:

Table 5.1: *rohc_profiles* bit-masks

rohc_profiles	IANA / RFC5795	Description
0x0001	0x0000	Uncompressed
0x0002	0x0004	IP
0x0004	0x0002	IP/UDP
0x0008	0x0001	IP/UDP/RTP
0x0010	0x0006	IP/TCP
0x0020	0x0003	IP/ESP

- *rohc_feedback_for:* This parameter is used to identify the feedback channel.
- *rohc_mrru:* This parameter shall be set to 0 as both MPE and RLE provides segmentation facilities.

6 Encapsulation (Fragmentation & Reassembly)

The Encapsulation sub-layer provides two access services (also called encapsulation options) to the encryption sub-layer in the FWD link, see Figure 6.1:

- MPE/MPEG Encapsulation;
- MPE-iFEC/MPEG Encapsulation;

where the MPE/MPEG service is taken as baseline.

All planes (user, control and management) shall have access to all access services of this sub-layer. However, the use of one or the other access service shall not be on a per-packet basis, but shall be configured on a per-service type basis.

An upgrade of the S-MIM forward link sub-system shall be possible supporting GSE, provided that all related issues in DVB-SH are addressed in the future within the scope of DVB-SH standardisation.

In the RTN link, only one encapsulation service shall be provided: Return Link Encapsulation (RLE), see Figure 6.2.

NOTE: The present document takes into account the DVB-RCS2 draft version of March 2011 [i.16] and [i.17].

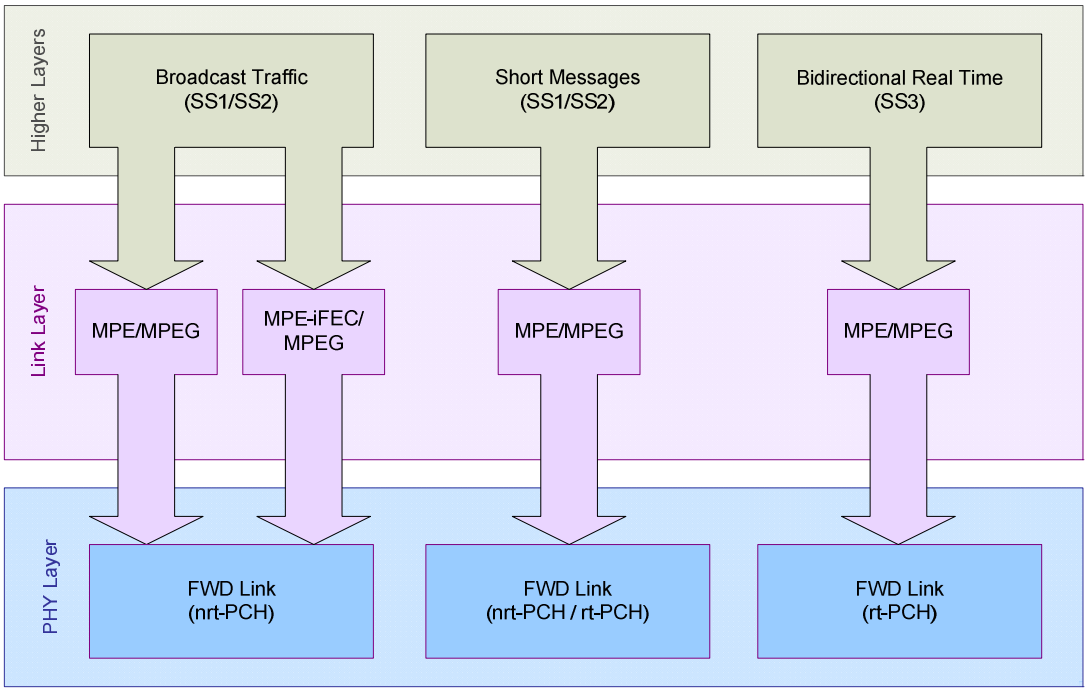

Figure 6.1: Encapsulation services in the FWD link

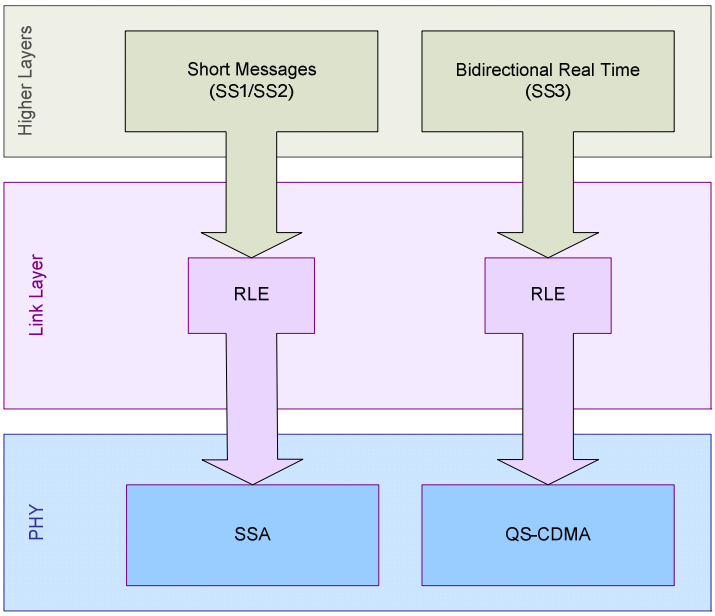

Figure 6.2: Encapsulation services in the RTN link

6.1 Forward Link Encapsulation

In the S-MIM system MPE will be used in similar way to DVB-H [i.3]:

- To encode an IP flow into a Transport Stream, Multiprotocol Encapsulation (MPE) shall be used. LLC_SNAP_flag = 0 shall be used when the MPE section encapsulates an (uncompressed) IPv6 packet. Stuffing bytes shall not be used. LLC_SNAP flag = 1 shall be used when the MPE section encapsulates a protocol different from IPv6 (ROHC, RFC 4944 [i.15]).

- An S-MIM receiver shall support decoding of IP-on-MPE.

- Each MPE section (datagram_section) shall contain exactly one IP datagram. The IP datagram shall be complete and unbroken, with appropriate source and destination addresses. In any Elementary Stream, an IP stream shall be carried in a single MPE section stream (i.e. only one MAC address used per IP stream).
- On different Elementary Streams or different Transport Streams, different MAC addresses for a particular IP flow may be used.
- An S-MIM Receiver may ignore MAC address when filtering IP streams.
- An Elementary Stream may carry multiple IP streams.
- On a particular Elementary Stream, a single MAC address may be associated with multiple IP streams (an MPE section stream may carry multiple IP streams).

For each Elementary Stream carrying IP stream(s), the SDT_actual should contain exactly one data_broadcast_descriptor with the data_broadcast_id set to 0x05 and the selector_length set to 2, indicating that Multiprotocol Encapsulation Info structure is included. The descriptor shall be associated with the Elementary Stream by means of service_id and component_tag. Within a Multiprotocol Encapsulation Info Structure, the alignment_indicator shall be set to 0, indicating that an alignment of 8 bits is used. Also, the max_sections_per_datagram shall be set to 1, indicating that each IP datagram is carried within a single MPE section.

On each MPE section, the MAC address should not be scrambled. If the MAC_IP_mapping_flag in the Multiprotocol Encapsulation Info Structure in the data_broadcast_descriptor is set to 1, an IP to MAC mapping shall be as described in RFC 2464 [8] for IPv6 multicast addresses.

The same IP to MAC mapping shall be used for other (non-multicast) addresses, too. This is convenient in that the same rule is used for all IP destination addresses, without making difference between unicast, multicast or any other kind of address. This is specified in clause 7.

The present document does not cover how the MAC address is formed if MAC_IP_mapping_flag is set to 0. Note that the MAC_address_range in Multiprotocol Encapsulation Info Structure limits the number of bytes used to carry the MAC address in the MPE section header.

An S-MIM Receiver may ignore the MAC address, and use the IP source and/or destination addresses carried in the IP datagram delivered in the payload of an MPE section instead. By processing a stream in this way a receiver would only be able to receive uncompressed IPv6 streams (LLC_SNAP_flag=0).

If link layer encryption is used in the forward link, payload_scrambling_control shall be set to 01. When link layer encryption is applied only the Payload of MPE shall be encrypted (including the LLC_SNAP header if present).

6.2 Return Link Encapsulation

The encapsulation protocol return link will be Return-link Encapsulation (RLE) as defined in the DVB-RCS2 standard [i.16] and [i.17]. The RLE provides mechanisms to encapsulate and fragment generic PDU, whether IP based or not, into physical frames. In addition the standard provides a native capability to create new facilities and to customize the use of header fields.

The following RLE configuration shall be applied for the specific case of the S-MIM radio interfaces:

- The Protocol_Type field shall be used in its compressed mode (1 byte) to identify the protocol of the encapsulated PDU. In particular, the default protocol shall be IPv6. In this case, the Protocol_Type field shall be omitted by setting the Protocol_Type_Suppressed flag set to 1. Otherwise, the following configuration of the Compressed_Protocol_Type field shall be used:

Table 6.1: Compressed protocol type values and supported protocols

Compressed protocol type value	Protocol
0x00-0x2F	Reserved
0x30	IPv4
0x31	Internal QS-CDMA signalling
0x32	Authentication signalling for SSA (LLC-SNAP)
0x33	Initial Authentication signalling
0x33-0x41	Reserved
0x42	ROHC bidirectional for QS-CDMA
0x43	ROCH feedback signalling for QS-CDMA
0x44	Modified RFC4944 [i.15]
0x45-0x7F	Reserved
0x80-0xFE	User Defined
0xFF	Reserved

- The alpdu_label_type field, present in the START PPDU and the FULL PPDU, shall be interpreted as follows:

Table 6.2: alpdu_label_type values

Alpdu_label_type value	ALPDU label size (bytes)
0	8 bytes
1	6 bytes
2	1 bytes
3	0 bytes

- use_alpdu_crc field shall be set to 1; therefore, the Integrity Protection of a Fragmented ALPDU shall be the ALPDU CRC method.
- The PPDU_Label_Byte shall be set to 0 (PPDU_Label remains unused).
- The fragment_id field is applied to identify fragments of the same packet. When a PPDU is not a FULL PPDU, all fragments corresponding to the same packet are assigned the same fragment_id. For the sake of avoiding ambiguities, the decapsulator must not assign the same fragment_id to PPDUs corresponding to different packets at the same time. This requirement might limit the transmitter throughput, see clause 6.2.3.

6.2.1 Encapsulation for SSA Radio Interface

Four different protocols shall be encapsulated in RLE to access SSA:

- IPv6
- IPv4
- RFC4944 [i.15] (header-compressed IP)
- LLC-SNAP (for authentication signalling)

Additionally, SSA requires the reservation of 1 byte for ARQ management, the reservation of 6B to carry the MAC address of the source and CoS differentiation (1 byte). Therefore, the following configuration shall be applied:

- Alpdu_label_type = 0 → (8 bytes long alpdu_label).
- Protocol_Type_Suppressed flag = 1 if the PDU to be encapsulated is IPv6.

- Protocol_Type_Suppressed flag = 0 if the PDU to be encapsulated is other than IPv6.
    - In this case, the Compressed_Protocol_Type field is present and shall be set according to table Table 6.1, depending on the encapsulated protocol.

The alpdu_label shall be applied to provide the following information:

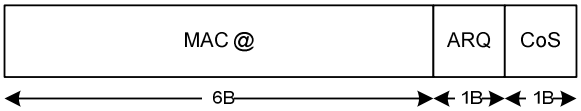

Figure 6.3: alpdu_label configuration for alpdu_label_type = 0 (use for SSA access)

- MAC address: as specified in clause 7.
- ARQ: information format as specified in clause 8.
- CoS: this field shall be interpreted as follows: 0x01 corresponds to the highest priority. The level of priority decreases as the CoS field value increases, 0xFF corresponds to the lowest priority and 0x00 remains reserved.

Additionally, the following shall be fulfilled at the physical layer burst:

- It shall set the use_explicit_payload_header_map to 1 in order to be capable of signalling the length of the burst payload.
- It shall use the payload_crc as specified in [2].

6.2.2 Encapsulation for QS-CDMA radio interface

Four different protocols shall be encapsulated in RLE to access QS-CDMA:

- IPv6
- IPv4
- ROHC - bidirectional mode (header-compressed IP)
- Internal MAC signalling

Additionally, QS-CDMA requires the reservation of 6B to carry the MAC address in the of the source RACH channel and CoS differentiation (1 byte). QS-CDMA has two types of transport channels, namely DCH and RACH. Different RLE configurations will be applied to access each transport channel.

6.2.2.1 DCH transport channel

- Alpdu_label_type = 2 → (3 bytes long alpdu_label)
- Protocol_Type_Suppressed flag = 1 if the PDU to be encapsulated is IPv6
- Protocol_Type_Suppressed flag = 0 if the PDU to be encapsulated is other than IPv6
    - In this case, the Compressed_Protocol_Type field is present and shall be set according to Table 6.1, depending on the encapsulated protocol.

The alpdu_label shall be applied to provide the following information:

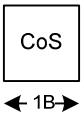

Figure 6.4: alpdu_label configuration for alpdu_label_type = 2 (used for QS-CDMA DCH access)

Additionally, the following shall be fulfilled at the physical layer burst:

- It must set the use_explicit_payload_header_map to 0 (since the physical layer header provides means to signal the payload length).
- It shall use the payload_crc (16 bit), as specified in [3].

6.2.2.2 RACH transport channel

- Alpdu_label_type = 1 → (8 bytes long alpdu_label).
- Protocol_Type_Suppressed flag = 0, since the RACH channel is used only for signalling.
- Compressed_Protocol_Type = 0x31.

The alpdu_label shall be applied to provide the following information:

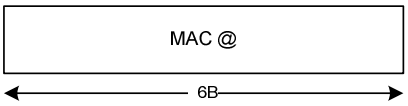

Figure 6.5: alpdu_label configuration for alpdu_label_type = 1 (used for QS-CDMA RACH access)

- MAC address as specified in clause 7.

Additionally, the following shall be fulfilled at the physical layer burst:

- It must set the use_explicit_payload_header_map to 0 (since the physical layer header provides means to signal the payload length).
- It shall use the payload_crc (16 bit), as specified in [3].

6.2.3 RLE Ambiguities in S-MIM

The RLE specification in [i.6] assumes that RLE packets carrying fragments of a single packet are guaranteed to be received in the same order they were sent. In the DVB-RCS2 specification [i.16] and [i.17], this assumption applies, but it does not hold necessarily in the SSA return link of the S-MIM radio interface. In particular, if interference cancellation is applied to enhance the demodulation performance, the time to demodulate one burst will depend on the number of interferers affecting that burst. This varies for each burst and therefore the demodulation time is different for different bursts.

With the RLE encapsulation protocol, the order of fragments of the same packet is only uniquely specified if the number of fragments is below 4. If the number of fragments is equal or higher than 4, the continuation PPDUs cannot be sorted with the information contained in the RLE fields. Therefore, if interference cancellation is applied at the SSA demodulator and packets may be fragmented in more than 3 fragments, an additional mechanism is required at the receiver (the hub) to allow unequivocal fragment sorting.

The following amendment shall be done to the RLE encapsulator at the terminal:

- The RLE encapsulator shall limit its output packet rate to N Network layer packets every Δ seconds, where N=7 is the number of fragment_id values available for encapsulating data and Δ is the difference between the maximum and minimum processing delay at the SSA demodulator.

Finally, in case frequency reuse is applied in the SSA return link, especially for frequency re-use 1, a mechanism has to be present to handle reception of duplicated packets through different demodulators (corresponding to beams or cells using the same frequency slot).

7 MAC Layer Addressing

Completing the encapsulation protocol, the definition of the system specific MAC layer addressing is provided in this clause. In particular, the authentication process will provide the necessary information to addressing terminals in the system.

7.1 Forward Link

The Addressing for the different services shall be performed based on IP/MAC notification tables as specified in [1]. Note that descriptors based on IP addresses or IP address ranges can only be used when the services are transported using uncompressed IP. If the services are carried using compressed IP or other protocol different from IP, the descriptor must be based on MAC addresses or MAC address ranges.

7.2 MPE MAC Address format

When the MAC address field of MPE is used the format specified in [12] shall be used. According to the specification of MPE in [1], the MAC address field in MPE is 48 bit long. The MAC address is fragmented in 6 fields of 8-bits, labelled MAC_address_1 to MAC_address_6. The order of the bits in the bytes is not reversed, so the Most Significant Bit (MSB) of each byte is transmitted first. The structure of the MPE MAC layer address is given in Table 7.1.

Table 7.1: Structure for the MPE MAC address

Syntax	Number of bits
MAC_address_1 () {	
Unicast/Multicast bit	1
Address validity.	1
S-MIM_address [1]	6
}	
MAC_address_2 () {	
S-MIM_address [2]	8
}	
MAC_address_3 () {	
S-MIM_address [3]	8
}	
MAC_address_4 () {	
S-MIM_address [4]	8
}	
MAC_address_5 () {	
S-MIM_address [5]	8
}	
MAC_address_6 () {	
S-MIM_address [6]	8
}	

The semantics of the MAC_addres_1 field are as follows:

Unicast/Multicast bit: If this bit is set to 0 the address is a Unicast address. If the bit is set to 1 the address is a Multicast address.

Address Validity: If this bit is set to 0 the address is an International Mobile Subscriber Identifier (IMSI) which is a globally unique address. If the bit is set to 1 the address is a Temporary Mobile Subscriber Identifier (TMSI), which is a locally administered address.

S-MIM_address [1]…[6]: This fields form the S-MIM system address (TMSI, IMSI or Multicast address). S-MIM_address[1] contains the 6 most significant of the S-MIM system MAC address. S-MIM_address[2]…[6] contain the remaining 5 bytes of the S-MIM system MAC address, being S-MIM_address[6] the less significant byte. The order of the bits inside the bytes is not reversed, so that the MSB of every byte is transmitted first.

The S-MIM System MAC address is therefore 46 bits long. This allows defining more than 7E13 (70 billion) different addresses.

7.3 Return Link

7.3.1 QS-CDMA return link

For the SS3 return link subsystem the format of the MAC address will be the same as the one specified for the forward link in clause 7.2.

7.3.1.1 MAC Layer addressing for RACH

For this carrier the MAC address of the source is required for the Hub to identify the originator terminal. This information cannot be derived from other means as all terminals share the same random access resource.

It is not required to use the MAC address of the destination, namely the Hub, because the each Hub should allocate different random access resources for co-located return link beams/spots.

7.3.1.2 MAC Layer addressing for QS-CDMA

Neither source nor destination MAC address is required as the dedicated resources are enough to identify both the terminal and the Hub.

7.3.2 SSA return link

In the SSA return link, no MAC destination addresses shall be used, since all the packets target the hub which controls the return link over which the packet was sent.

The MAC layer source address shall be used in the SSA return link. The format of the address will be the same as in the forward link, see Table 7.1.

NOTE: The terminal specifies if it is using its IMSI or TMSI as MAC address with the value of the address_validity field, see clause 7.2.

8 Link Layer ARQ

The Link Layer provides three Transmission Modes for services being mapped into the SSA air interface:

- ACK Mode: acknowledged mode. Upper sub-layer packets mapped into this transmission mode will require link layer acknowledgements in the form of a CRC in the forward link and a re-transmission buffer. All transmitted packets will be stored in the re-transmission buffer until they expire or the related ACK has been received by the terminal. The ACK mechanism to be applied will be specified in following clauses.
- uACK Mode: unequivocally acknowledged mode. Upper sub-layer packets mapped into this transmission mode will require link layer acknowledgements in the form of a dedicated unicast addressed ACK message for the terminal in the forward link and a re-transmission buffer. All transmitted packets will be stored in the re-transmission buffer until they expire or the related ACK has been received by the terminal. The ACK mechanism to be applied will be specified in following clauses.
- Tr-Mode: transparent mode. Upper sub-layer packets mapped into this transmission mode will be transmitted without expecting any link layer acknowledgements in the forward link. No re-transmission buffer is required for such transmissions.

In the SSA RTN link of the S-MIM system an ARQ mechanism shall be applied on network layer PDUs.

The alpdu_label of the RLE packet shall be used to signal the required information to perform ARQ. In particular, for the access to SSA, the alpdu_label format as specified in Figure 6.3 contains an ARQ byte. The format of the ARQ byte is shown in Figure 8.1 and Table 8.1. The Message_ID field shall be used as a counter.

Table 8.1: Structure for the ARQ byte

Syntax	Number of bits
ARQ_byte {	
ACK_Type	2
Message_ID	6
}	

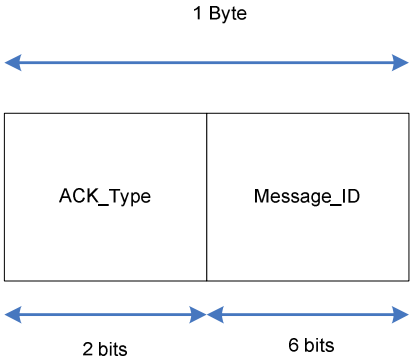

Figure 8.1: Packet format for the ARQ sub-protocol

The ACK_Type field is contained in the two first bits of the ARQ_byte. The value of this field determines the type of ACK to be applied to this message. The different values and their meaning are shown in Table 8.2.

Table 8.2: ACK Type field

Value	Meaning
00	No Link-layer layer ARQ needed (Tr-Mode)
01	CRC based Link layer ARQ (ACK Mode)
10	Unicast unequivocal link layer ARQ (uACK Mode)
11	Reserved for future use

A more detailed description of the transmission modes follows:

- Tr-Mode is used when no Link-layer layer ARQ is needed, for example because the reliability is provided at some other layer (on top of UDP, for example).
- ACK Mode applies a CRC-based ACK to each set of correctly received link layer packets that build the same higher layer (IP) packet. A dedicated channel on the FWD link will transport these acknowledgements. This channel shall be defined by reserving one PID. Terminals shall be notified over the FWD link which PID is associated with CRC based ACK. These ACKs will be a hash value of the correctly reassembled ALPDU after receiving correctly all link layer fragments (RLE packets) required to reassemble the ALPDU. This link layer ARQ mechanism provides reliability although some equivocation probability exists that depends on the length in bits of the CRC; this is so because it is possible that two terminals generate messages which result in the same hash value at the same time. In this case one terminal may wrongly interpret as own ACK an ACK which was actually meant for the other terminal. On the other hand, the use of a CRC-based link layer ARQ has the advantage that it requires very reduced resources in the FWD link, compared to unicast unequivocal link layer acknowledgments, that require a full link layer packet to acknowledge each reassembled ALPDU at the hub. However, if the CRC is sufficiently long, the probability of equivocation can be kept sufficiently low. The algorithm used for ACK CRC computation shall never yield an all zeros CRC.
- uACK Mode: A dedicated channel on the FWD link will transport these acknowledgements. This channel shall be defined by reserving one PID. Terminals shall be notified over the FWD link which PID is associated with unequivocal ACK. These ACKs are longer than the CRC ACKs, as each ACK requires a full link layer packet (MPEG-TS).

The other 6 bits are the Message_ID. This 6 bit long field shall be incremented by one at the transmitter whenever a packet is sent (used as a counter). When the value of the field reaches 63 the next Message_ID value shall be 0.

The ARQ mechanism will be applied on correctly assembled ALPDU, which is the link layer addressed PDU in RLE and corresponds to one IP packet. This means that one ACK will be generated at the hub for each correctly reassembled ALPDU during RLE decapsulation.

Since RLE decapsulation is only implemented in the hub and not in the CGCs, the link-layer ACK will be generated by the hub exclusively. If one message is received over the satellite RTN link, the hub will then transmit this link layer ACK over the satellite FWD link. If the messages arrive through a collector, the hub will transmit the ACK over the SFN cluster of the co-located repeater. The length of the CRC based ACK shall be signalled over the FWD link. In CRC based ARQ mode, the CRC shall use the well known CCITT polynomial 0x104c11db7 with an initial value of 0xffffffff and a final negation of the result. All zeros is not a valid CRC; if a CRC of all zeros is obtained by using these algorithms; it shall be changed to all ones.

The bit ordering for CRC calculation is as follows: bytes are taken most significant first. Within each byte, bits are taken least significant first. The resulting CRC is sent with the most significant byte first and the highest order bit of the reminder in the most significant bit of the byte. This is usually called a reflected CRC.

The calculated CRC with this method is 32-bit long. If the length of the CRC based ACK is less than 32 bit, the less significant bits of the CRC are taken (the ACK will always be shorter than 32 bit). In case the desired length of the CRC based ACK is longer than 32 bits, unequivocal ACKs shall be used instead.

The unequivocal ACK will be build by concatenating the MAC address of the terminal with the Message _ID field of the ACK header (contained in the packet label of RLE). The MAC layer shall be put in the most significant bytes. The unequivocal ACK will then be 51 bits long.

Table 8.3: Unequivocal ACK syntax

Syntax	Number of bits	Mnemonic
Unequivocal_ACK {		
MAC_Address	48	
Message_ID	6	
}		

8.1 ARQ Mechanism at Terminal: Stop and Wait Cumulative ARQ

The ARQ mechanism defined here is a Pre-emptive Stop and Wait Cumulative ARQ, applicable to all transmission modes (ACK mode, uACK mode and Tr-Mode).

There shall be one ARQ mechanism instance per available S-MIM return link, i.e. one for the satellite return link and one for the Collector link. Through the power control mechanism defined in Part 3, the terminal will decide which link to use. This means when a packet has to be scheduled, the terminal will check the available information on signal quality of each link and decide as follows:

1) it will select the satellite link if there is no collector link with sufficiently good signal and there is a satellite link with sufficiently good signal.

2) it will select the collector link if there is a collector link with sufficiently good signal, independently of the state of any available satellite return link.

Once the terminal decides on the link to be used, each L2 PDU is scheduled and inserted into the ARQ instance of the selected link. Even if the channel state changes during the processing of a PDU in the ARQ mechanism, this processing continues without taking into account the change.

The following transmission operational procedure is based on the premise that the fragments (link layer packets) belonging to only one IP packet shall be waiting for ACK at the same time in the retransmission buffer.

The terminal shall behave as follows:

1) When there is an IP packet available, the terminal schedules it for transmission. If there are several packets backlogged in the scheduling queue, the terminal schedules the packet with highest priority CoS = j, such that the CoS value of each packet is denoted by 'i' belonging to the set [1,J], where J is the lowest priority, and 'j' is the highest present value of 'i' in the scheduling buffer.

2) During fragmentation/encapsulation of the scheduled IP packet, the terminal assigned a Message_ID (*n*) to the fragments of the IP packet for transmission; therefore, the Message_ID value *n* is marked as "blocked".

3) The terminal executes the procedure '*Wait for next transmission opportunity*'. When this procedure is closed, the terminal goes to step (4).

4) The first link layer packet with Message_ID value *n* is transmitted.

5) The tx_time_out timer is set to the value 'back_off_time' applicable to the CoS j of the currently scheduled packet, which is indicated by the Hub in the SAT signalling table in the FWD link:

   a) If the packet requires ACK:

      i) The link layer packet is stored in the retransmission buffer;

      ii) The NRtx counter(*n*) is set to the value 'max_retransmissions' applicable to the CoS of the currently scheduled packet, which is indicated by the Hub in the SAT signalling table in the FWD link;

      iii) For each remaining link layer packet with Message_ID *n*:

         1) From the previous transmission, the terminal waits until the tx_time_out timer expires and upon expiry, it transmits the next link layer packet with Message_ID *n;*

         2) the transmitted link layer packet is stored in the retransmission buffer;

         3) The tx_time_out timer is set to the value 'back_off_time' applicable to the CoS of the currently scheduled packet.

      iv) The terminal sets the Rtx_Timer to the value 'ack_time_out' applicable to the CoS of the currently scheduled packet, which is indicated by the Hub in the SAT signalling table in the FWD link, and waits until this timer expires or an ACK is received.

      v) If the Rtx_Timer(*n*) expires (reaches the value 0) and no ACK was received for the link layer packets with Message_ID value *n*:

         1) If the counter NRtx_counter(n) is still higher than 0:

            a) NRtx_counter(n) is decreased by one (set to NRtx_counter(n)-1);

            b) for each link layer packet with Message_ID value *n:* the terminal waits until the tx_time_out timer expires and transmits the next link layer packet in the retransmission buffer;

            c) the terminal goes back to 3).a).iv).

         2) If the counter NRtx_counter(n) is equal to 0:

            a) The link layer packets with Message_ID *n* were unsuccessfully delivered and the terminal goes to the procedure *'Clear Message_ID = n'*.

            b) After completion of the procedure *'Clear Message_ID = n'*, the terminal goes back to step (2).

      vi) If an ACK was received for the packets with Message_ID value *n* before the Rtx_Timer(*n*) expires:

         1) The link layer packets with Message_ID = n are successfully delivered the terminal goes to the procedure *'Clear Message_ID = n'*.

         2) After completion of the procedure *'Clear Message_ID = n'*, the terminal goes back to step (2).

Procedure 'Clear Message_ID = n'

1) The terminal deletes the remaining link layer packets in the retransmission buffer with Message_ID = n;

2) The terminal clears the retransmission timer and counter (Rtx_timer(n) and NRtx_counter(n)) associated to Message_ID = n;

3) The terminal marks the Message_ID = n as free.

4) The terminal waits until the tx_time_out expires.

Procedure '*Wait for next transmission opportunity*'

The terminal calculates a random variable X a in the range [0,1] and compare it with the value 'persistence_index' that is indicated by the Hub in the SAT signalling table in the FWD link:

1) if X < 'persistence_index', the terminal will start managing the transmission of the next set of link layer packets with the same Message_ID;

2) otherwise, the terminal will wait a period of time equal to the value 'back_off_time' and will go back to step (1) of the procedure '*Wait for next transmission opportunity*'.

With the procedures described above, the transmission of the fragments belonging to a specific IP packet can only be triggered after successful transmission of all fragments of the previous IP packet or after expiration of the IP packet. Accordingly, only link layer packets with the same Message_ID (belonging to the same IP packet) can be at the same time in the retransmission buffer.

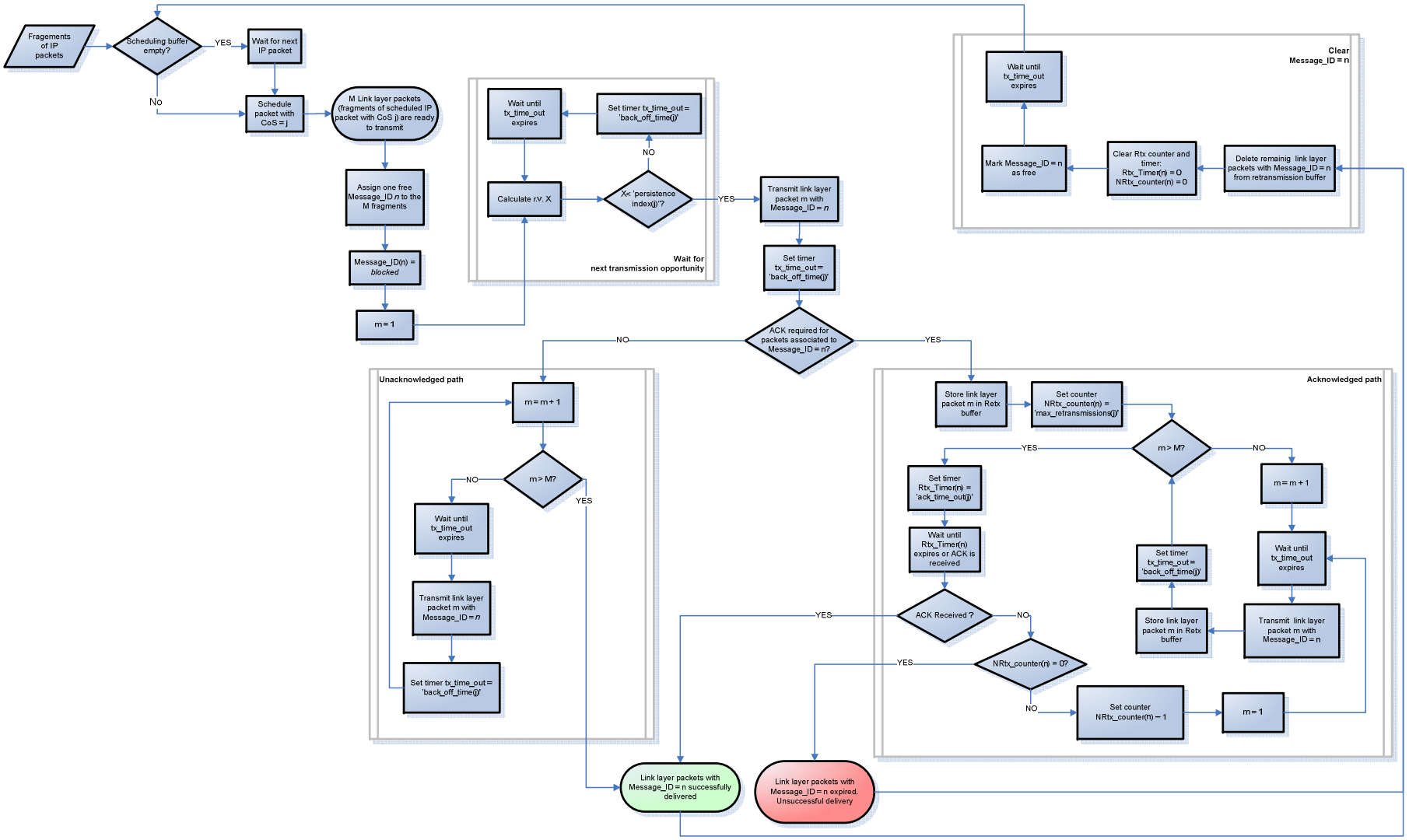

Figure 8.2: Flow chart of the Pre-emptive Stop and Wait Cumulative ARQ with CoS support

9 Load control (LC)

The LC for the RTN link only is specified (the FWD link is internal to the hub and is not specified). LC is implemented by (i) monitoring the load in the RTN link and (ii) signalling to the terminals the parameters to be used by the ARQ mechanism to limit the overall load. This signalling is implemented in the SAT and SDT tables in TS 102 721-6 [4].

In this way the LC "tunes" the ARQ through signalling to control the SSA RTN load.

The RTN load control manager function is devoted to monitor the system load in the return link and to actively reduce the traffic load when congestion is detected to keep the packet loss ratio below a selected threshold. Two functional subelements that contribute to the purpose of RTN load control can be identified:

- **RTN load monitoring function**: this function monitors the return link load, through a given output parameter from the SSA demodulator and the information received by the CAC/DAMA manager in the RM Module SS3 regarding the active SS3 real time sessions. If a certain load threshold (set by the NCC) is exceeded, the return load control function detects congestion in the return link.
- **Congestion resolution function**: this function is devoted to react upon congestion detection by the RTN load control function to reduce the packet loss ratio below a threshold established by the NCC. This function will also determine which actions must be carried out to remain below the threshold PLR.

9.1.1 Internal Interfaces

Both subfunctions of the RTN Load Control Manager are interconnected, as the RTN load monitoring function will trigger the load control resolution function whenever it detects congestion.

Additionally, the RTN load monitoring function will interface the NCC policies related to SS1/SS2, as among these policies the congestion detection threshold(s) will be defined and stored.

Furthermore, the congestion resolution function also interfaces the NCC policies in order to apply the right parameters for congestion resolution in the load control signalling in the FWD link.

9.1.2 External Interfaces

The RTN link resources are shared between the SSA and QS-CDMA interfaces. Therefore, an interface between the CAC/DAMA functions (corresponding to the QS-CDMA interface) and the RTN load control manager is necessary to better balance the resource share. Through this interface both functions can exchange channel load estimations. It is recommended to implement this interface at IP level to allow separable Hubs for SS1/SS2 services and SS3 services.

Finally, the load control resolution function will interface the signalling manager in order to update the load control information in the system signalling for the upcoming signalling transmission.

10 Call Admission Control/DAMA

In the next clauses some flow charts depicts the protocols involved in the CAC/DAMA for the SS3 which involves both the FWD and RTN links. A more detailed description of the contents of the messages interchanged can be found in TS 102 721-6 [4].

10.1 Capacity Allocation Initiated by the Terminal

The procedure shown in Figure 10.1 is used by SS3 terminals to request dedicated resources. It is assumed that the terminal is in LOGGED_ON state as defined in [6].

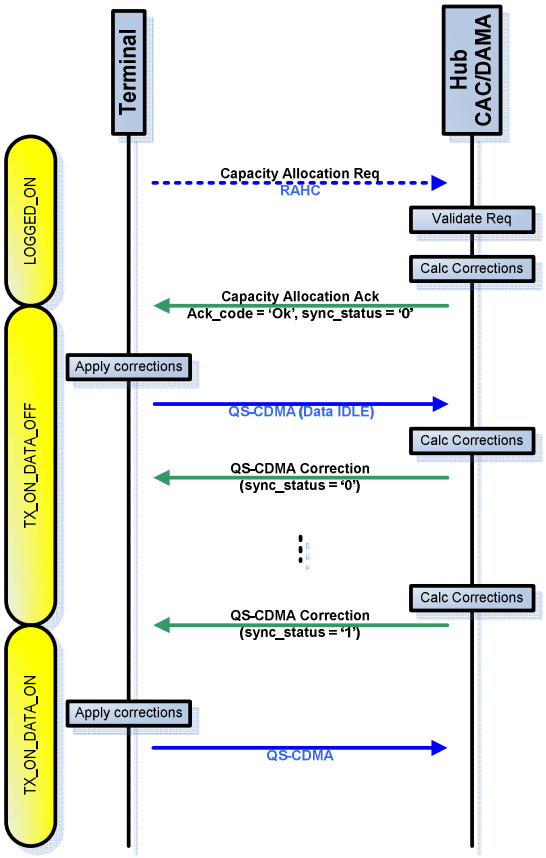

Figure 10.1: Capacity Allocation initiated by the Terminal

10.2 Capacity Allocation Initiated by the Hub

The procedure shown in Figure 10.2 is used by the Hub to announce a SS3 terminal to request dedicated resources. It is assumed that the terminal is in LOGGED_ON state as defined in [6].

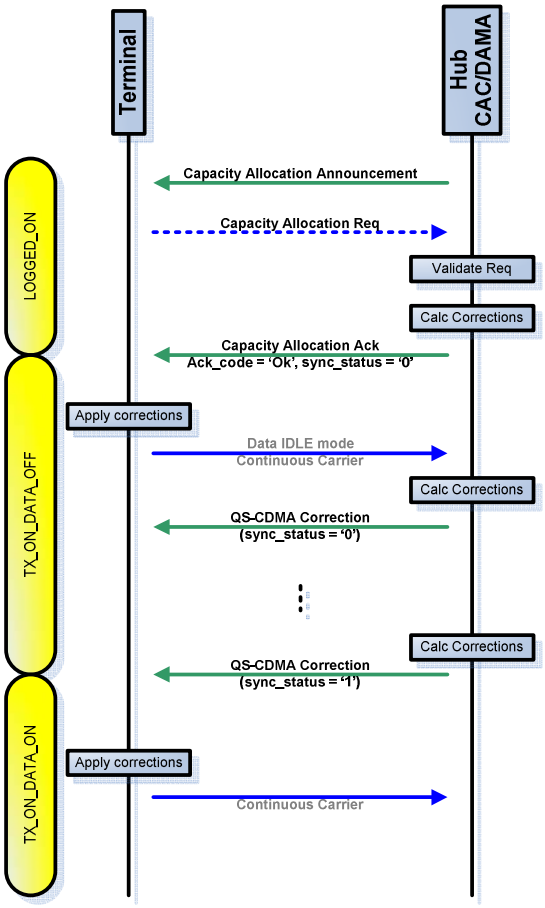

Figure 10.2: Capacity Allocation initiated by the Hub

10.3 Capacity Release Initiated by the Terminal

The procedure shown in Figure 10.3 is used by SS3 terminals to request the release of previously allocated resources. It is assumed that the terminal is in TX_ON_DATA_ON state as defined in [6].

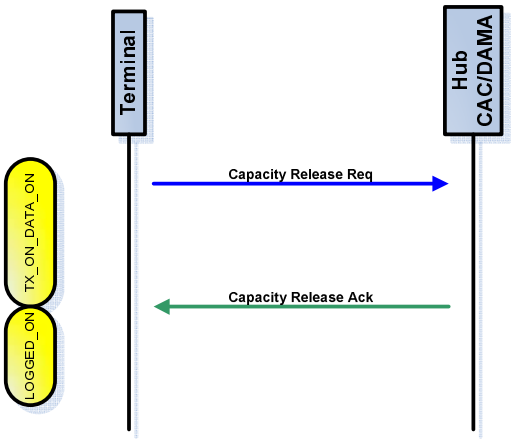

Figure 10.3: Capacity Release initiated by the Terminal

10.4 Capacity Release Initiated by the Hub

The procedure shown in Figure 10.4 is used by the Hub to indicate to a SS3 terminal to release its allocated resources.

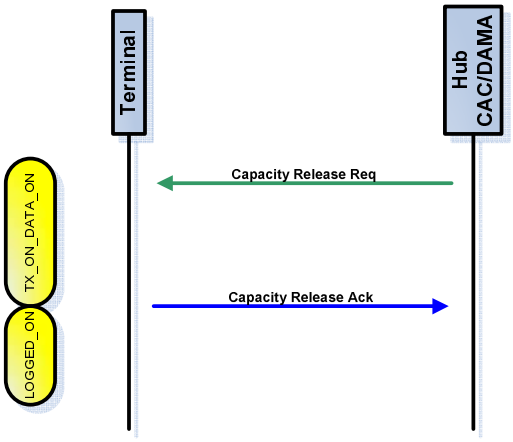

Figure 10.4: Capacity Release initiated by the Hub

11 Security Mechanisms

Security mechanisms refer to mutual authentication and encryption. Mutual authentication is carried out at link layer, while encryption may be applied either at the link or at the network layer. Encryption at the link layer is preferred, but it is in general not compatible with existing broadcast standards. Therefore, S-MIM provides the flexibility to allow network layer encryption (IPSEC) in the forward link, independently of the return link, in order to be backward compatible with existing broadcast systems that could be applied as FWD air interface in the S-MIM system.

Terminal and hub will negotiate their encryption capabilities in order to establish a common encryption strategy for communications with that terminal. This flexibility allows backward compatibility with broadcast systems that could be applied as FWD radio interface in the S-MIM system and do not support link layer encryption.

In the S-MIM System the security functions for system level security are implemented only in the hub and the terminals. Complementary Ground Components (CGC) can be considered transparent to security functions, since demodulated SSA bursts are forwarded to the hub without decrypting them and the CGCs do not own VLRs.

UMTS mechanisms for authentication, key exchange and the TMSI renewal, according to the 3GPP standards [5] and [6], are reused in the S-MIM system.

In the forward link encryption can be applied either at link layer, again reusing UMTS mechanisms, or at IP layer. In case encryption at IP layer is used IPsec is applied. Concretely the Internet Key Exchange protocol version 2 (IKEv2) [11] is used for the negotiation of security associations (SA) and Encapsulated Security Protocol (ESP) [7] is used in transport mode to provide privacy and integrity.

Since the way how security is applied can be negotiated, an instance is needed to carry out this negotiation. This entity is the signalling manager, which resides in the link layer.

Within the PSI/SI, the hub broadcasts periodically a descriptor that identifies service areas controlled by different hubs: the 'original_network_id' parameter uniquely identifies the controlling hub of the service area, whereas the 'network_id' uniquely identifies the linguistic beam within the hub. This distinction is necessary since one hub may control one or more linguistic beams. It is assumed that one HLR/VLR is present in each hub. Each terminal has stored in its USIM the identifier of its "home network" (its home hub), i.e. the 'original_network_id' and will this way be capable of recognising its home hub. When a security association has been established with one VLR (the home one or a foreign one) and due to mobility the terminal starts receiving PSI/SI with a different 'original_network_id', it will assume that its security associations are no longer valid and will start the authentication process.

For the sake of simplicity, and analogy with UMTS, the 'original_network_id' will be also referred to as Local Area Identifier (LAI) in the following.

The flow diagram in Figure 11.1 shows the different security procedures performed after terminal power up and the order in which they are carried out. The steps are the following:

- After power up, the terminal searches for a FWD link.
- If a FWD link is present the terminal waits until the hub broadcasts the LAI.
- When the terminal receives the LAI, it compares it to the previously stored LAI.
  - If the LAI is the same the terminal does not need to renew its authentication. The link is then secured.
  - If the LAI has changed the security association has to be re-established, a mutual authentication procedure must be performed.
- The terminal performs the mutual authentication procedure. At the end of this procedure the return link is secured by means of Link layer security.
- The terminal notifies the Hub its security capabilities.
- If the hub supports link layer security over the FWD link and the terminal also does, link layer security shall be used for the FWD link. To do this, after receiving the security capabilities of the terminal, the hub informs the terminal that link layer security will be used in the FWD link (see clause 11.1.3).
- If either the hub or the terminal does not support link layer security, the hub initiates an IPsec negotiation procedure.

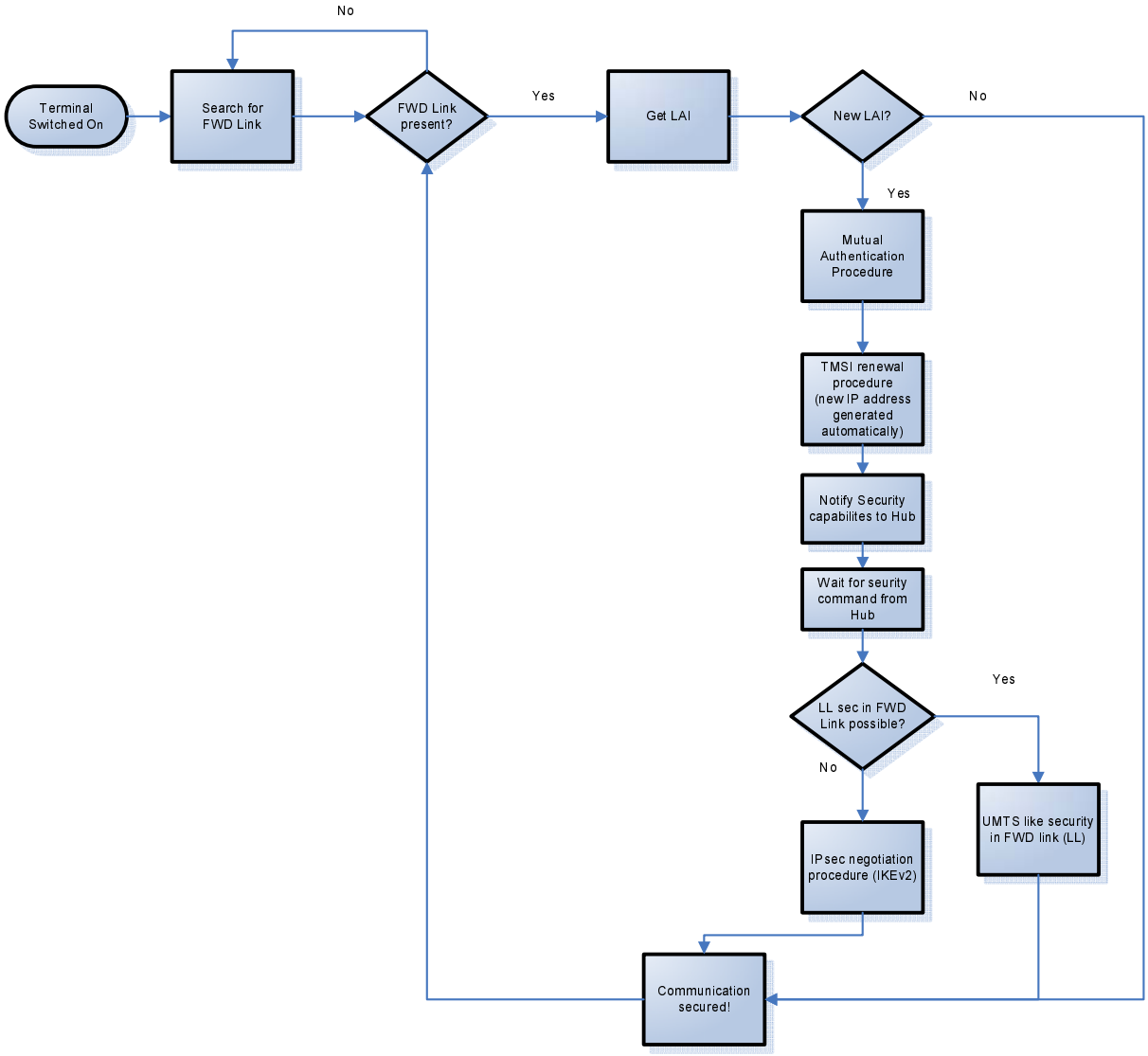

Figure 11.1: Mutual authentication procedures used in the S-MIM system after terminal power up

11.1 Security procedures

11.1.1 Mutual authentication procedure

This procedure is used to authenticate the terminal in the network. Furthermore it allows terminals to authenticate the network. This procedure is identical to the UMTS mutual authentication procedure and shall be performed as specified in [5].

After this procedure the terminal and the hub have a valid encryption key (CK) and a valid integrity check key (IK) for the communication session. These keys are applied when link layer security is used. The same key is applied in the forward and return link.

The parameters involved in this procedure are the following:

- CK: encryption key.
- IK: integrity Key.
- RAND: random number generated by the HLR.
- XRES: expected response from the terminal.

- RES: response from the terminal to the challenge (RAND) from the network.
- AUTN: parameters generated by the HLR which is used at the terminal to authenticate the network.
- IMSI: International Mobile Subscriber Identifier.
- TMSI: Temporary Mobile Subscriber Identifier.
- HLR: Home Location Register.
- VLR: Visitor Location Register.
- AuC: Authentication Center.

11.1.1.1 Mutual Authentication procedure using IMSI over Satellite

This procedure is used for the first entry into the S-MIM network, or when the LAI received over the air interface is different from the previously received LAI stored in the terminal.

This procedure is used when terminal does not have valid TMSI and CK and IK. The authentication procedure provides CK and IK and is followed by a TMSI renewal.

Since there is no valid CK and IK, the messages involved in this procedure are sent unencrypted and without integrity check.

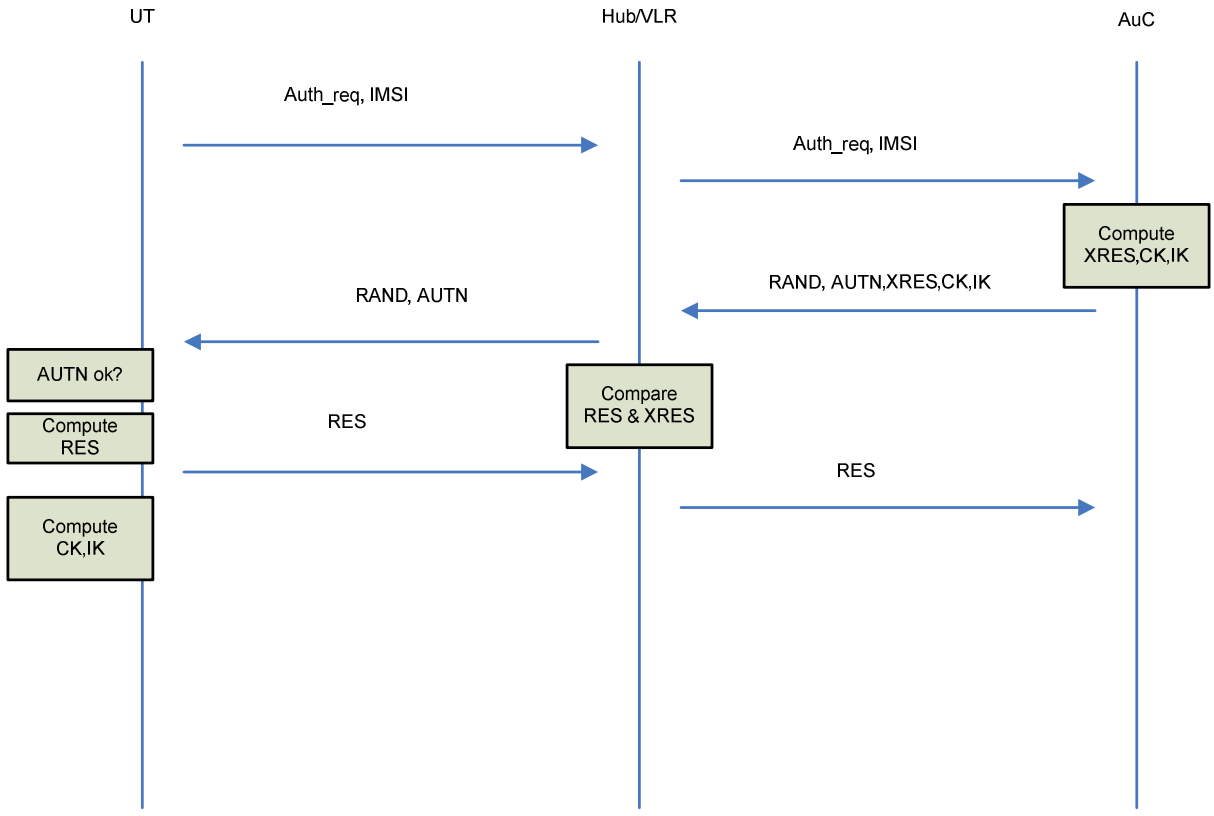

Figure 11.2: UMTS authentication procedure over satellite using IMSI

11.1.1.2 Mutual Authentication procedure using IMSI over CGC

This procedure is essentially the same as the equivalent procedure over satellite. The only difference is that the CGC is used to relay packets, however the functionality regarding security resides in the terminal and the hub, being the CGC transparent to security.

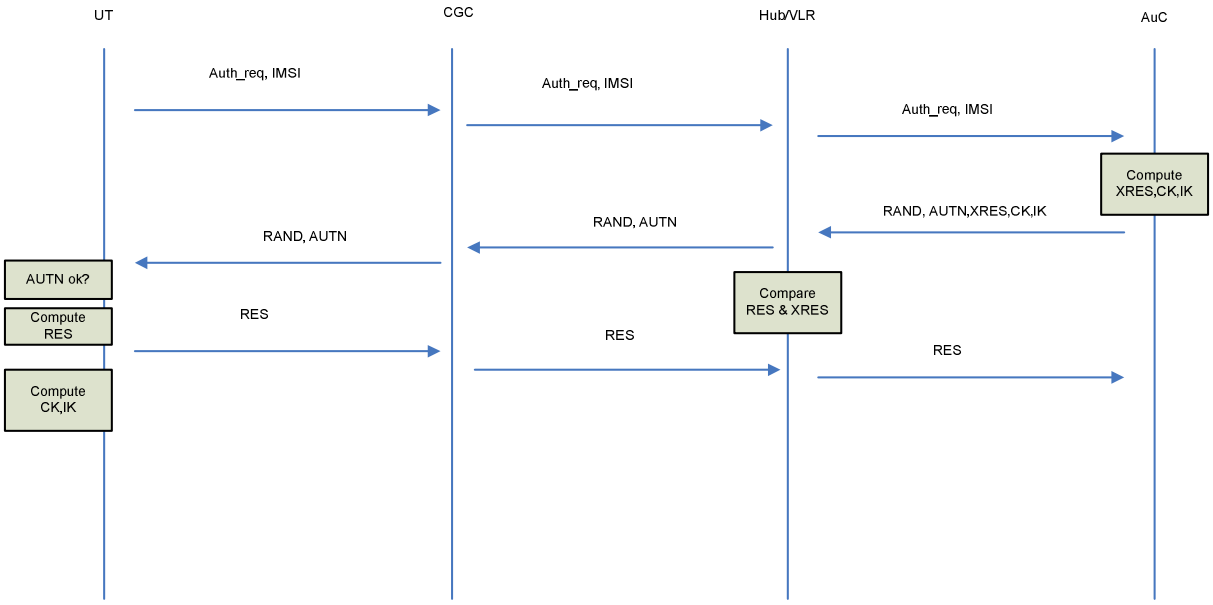

Figure 11.3: UMTS authentication procedure over CGC using IMSI

11.1.1.3 Mutual Authentication procedure using TMSI over Satellite

This procedure is used by the terminals to renew the authentication in the network provided that they have been authenticated in the network before. This implies the terminal has already a valid CK and IK and TMSI.

In contrast to the authentication procedure using IMSI, in this case all messages are sent encrypted. Moreover the authentication procedure does not have to be followed by a TMSI renewal.

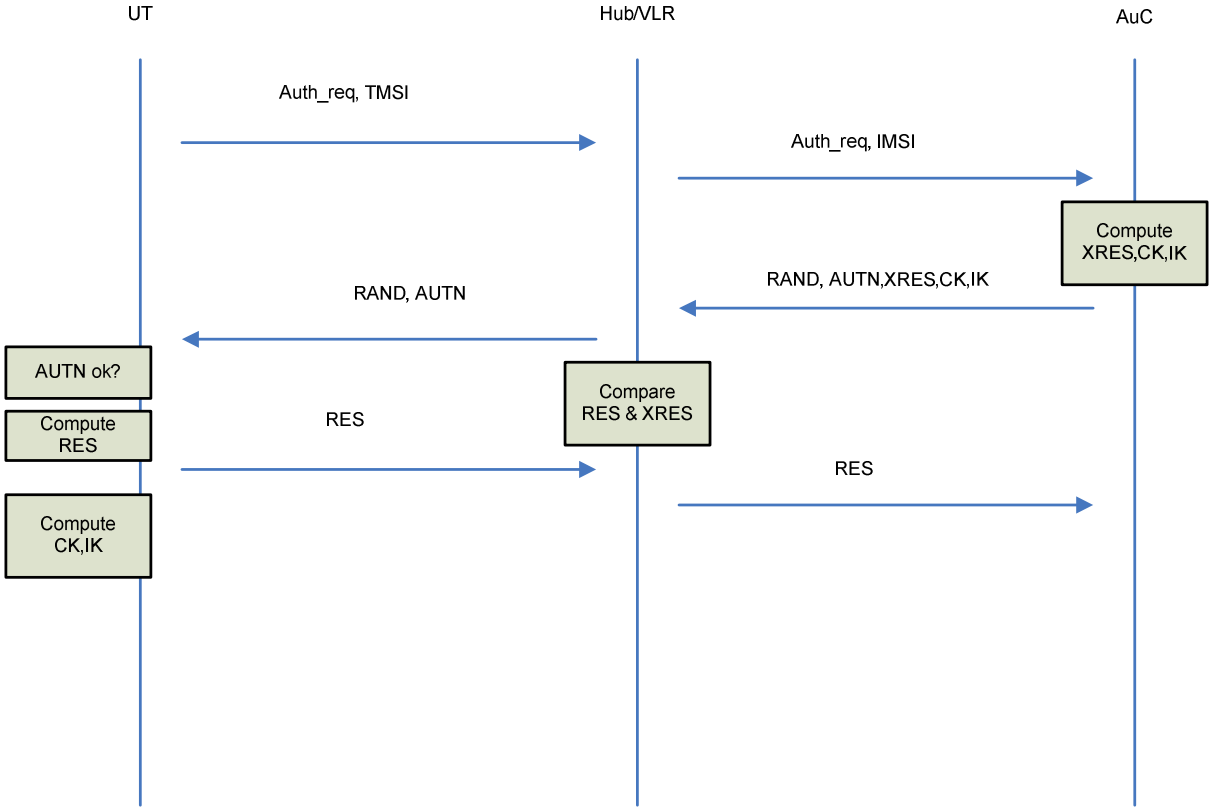

Figure 11.4: UMTS authentication using TMSI

11.1.1.4 Mutual Authentication procedure using TMSI over CGC

This procedure is essentially the same as the equivalent for satellite. The only difference is that the CGC is acting as a relay forwarding the messages from the terminal to the hub and vice versa.

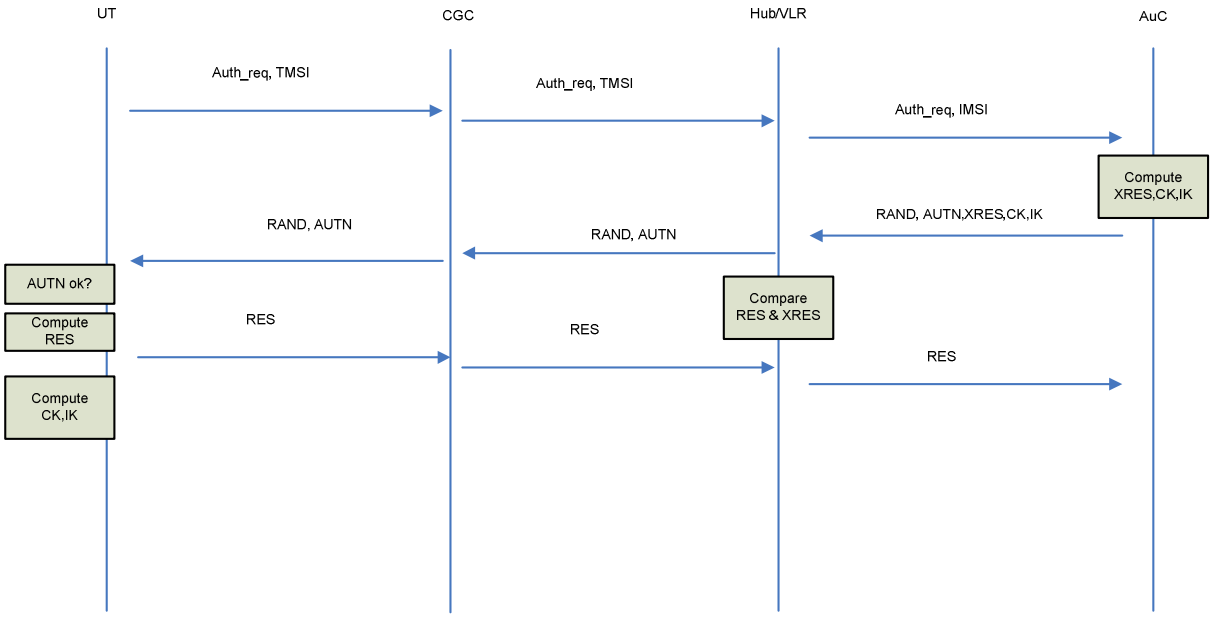

Figure 11.5: UMTS authentication using TMSI over CGC

11.1.2 TMSI renewal procedure

The procedure to renew the TMSI over satellite shall be performed as specified in [5]. This procedure assigns a new temporary MAC address to a terminal. The use of temporary MAC addresses increases the security of the system.

The validity of a TMSI is monitored by the hub. When a TMSI has been used to secure a certain amount of data (or the exchange of data during a limited period of time) the TMSI shall be renewed. This amount of data (or period of time) will depend on the implementation.

The first message of this procedure in which the hub notifies TMSI_new to the terminal can be sent either in clear text (no encryption) or encrypted depending on the state of the security over the FWD link. The second message of the procedure is always sent encrypted using link layer security.

NOTE: The TMSI renewal procedure only concerns the VLR where the terminal is located. The HLR of the terminal is not notified about the new address.

A number of requirements shall be fulfilled in the management of TMSIs as follows:

It shall be noted that a TMSI association is between a terminal and a serving hub limited in time or in volume of data. The same TMSI shall not be valid at the same time for other associations. Consequently, for every new association, a free TMSI shall be allocated. To avoid ambiguities, the TMSI must be local to a location area. In particular, a set of TMSIs shall be allocated to each serving hub. With such allocation, there is no ambiguity when resolving the validity of the current association of a terminal with a specific serving hub. In the case that the same hub manages more than one linguistic beam, the hub must be capable of keeping track of the TMSIs allocated to each beam managed by the hub.

11.1.2.1 TMSI renewal procedure over Sat

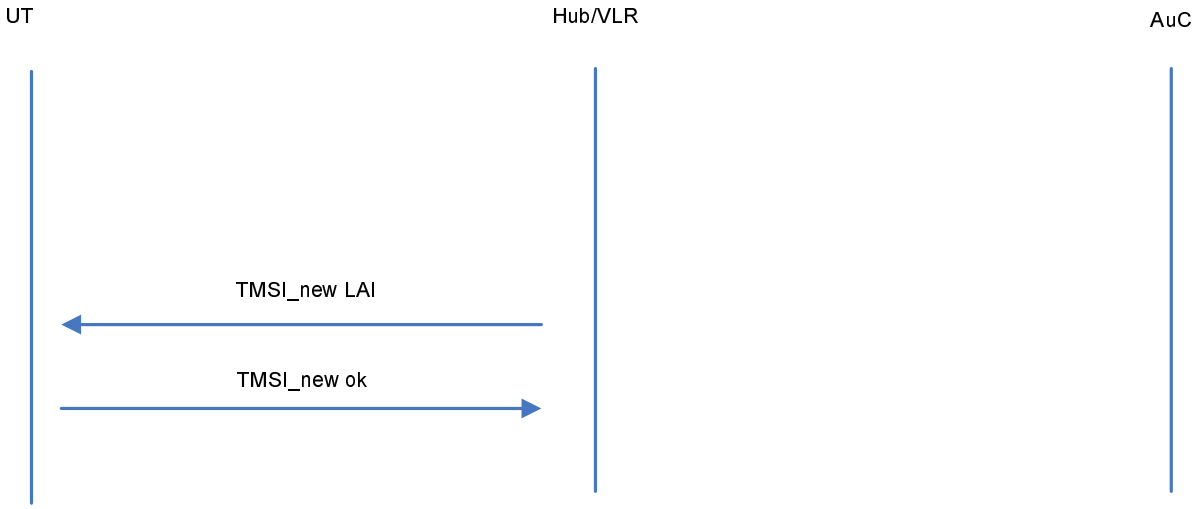

Figure 11.6: TMSI renewal over sat

11.1.2.2 TMSI renewal procedure over CGC

The TMSI renewal procedure over is the same as the equivalent over satellite, with the only difference that the CGC acts as a relay between the terminal and the hub.

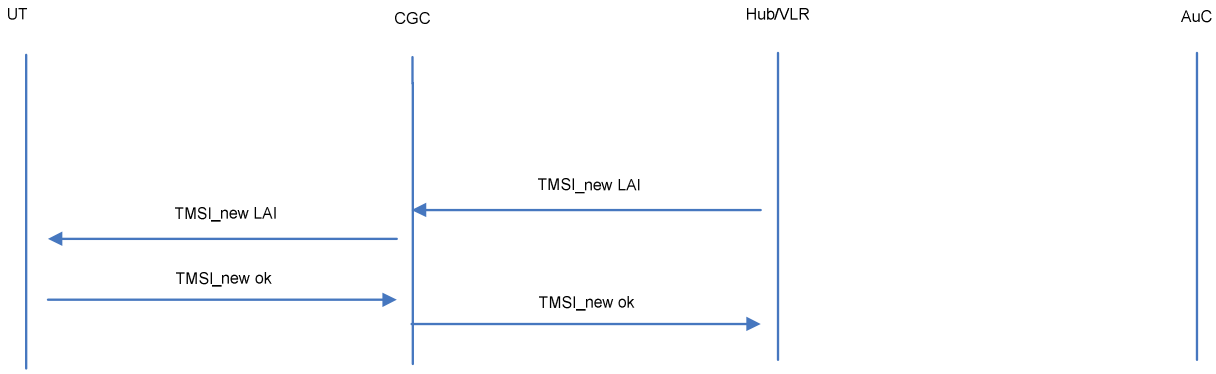

Figure 11.7: TMSI renewal over CGC

11.1.3 Forward link security negotiation procedure

After the mutual authentication procedure and the TMSI renewal procedure, terminals must perform the forward link security negotiation procedure. The purpose of this procedure is to establish a secure connection over the forward link.

This procedure is initiated by the user terminal with a *Security_Capabilities* notification message. This message is sent in the uplink using the protocol type Initial Authentication signalling (see Table 6.1). The syntax of this message is the given in Table 11.1.

Table 11.1: Security capabilities message syntax

Syntax	Number of bits	Mnemonic
Security_Capabilities {		
Link_Layer_Security	1	bslbf
IP_Layer_Security	1	bslbf
Reserved for future use	6	
}		

The meaning of the different fields in the message is the following:

- Link_Layer_Security: A value of 1 indicates that the terminal supports link layer security in the forward link. A value of 0 indicates that the terminal does not support link layer security in the forward link.
- IP_Layer_Security: A value of 1 indicates that the terminal supports IP layer security in the forward link. A value of 0 indicates that the terminal does not support IP layer security in the forward link.

It shall be noted that the access to services that require the use of the return link must be protected. As a minimum, IP layer security shall be supported by hub and terminals. Advanced hubs and terminals will support also link layer security. The case that neither link layer nor IP layer security features are supported must not happen. Additionally, the case that there is no common supported security feature by hub and terminal must not happen.

Upon reception of a security capabilities message, the hub shall decide at which layer to apply security in the forward Link. When both link layer security and IP layer security are possible, link layer security shall be preferred. In case the hub decides to apply link layer security on the forward link the hub shall reply with an encrypted dummy message, i.e. an IP packet with no payload. The reception of a packet using link layer encryption over the forward link shall be interpreted by the terminal as a confirmation that link layer security will be user over the forward link.

In case IP layer security is applied and not link layer security, the hub shall automatically start an IPsec security association with the terminal as defined in clause 11.2.

11.1.3.1 Forward link security negotiation procedure over Sat

The forward link security negotiation procedure over satellite is shown in Figure 11.8 for the case in which link layer security is used over the forward link . In case IP layer security is used the procedure is shown in clause 11.2.

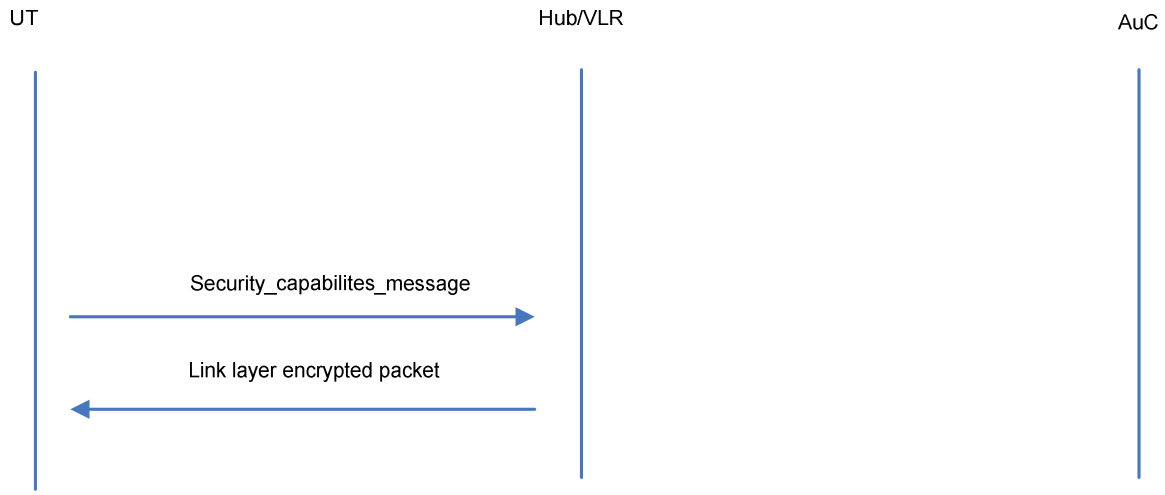

Figure 11.8: Forward link security negotiation procedure over Satellite. Link layer security

11.1.3.2 Forward link security negotiation procedure over CGC

The forward link security negotiation procedure over CGC is shown in Figure 11.8 for the case in which link layer security is used over the forward link. In case IP layer security is used the procedure is shown in clause 11.2.

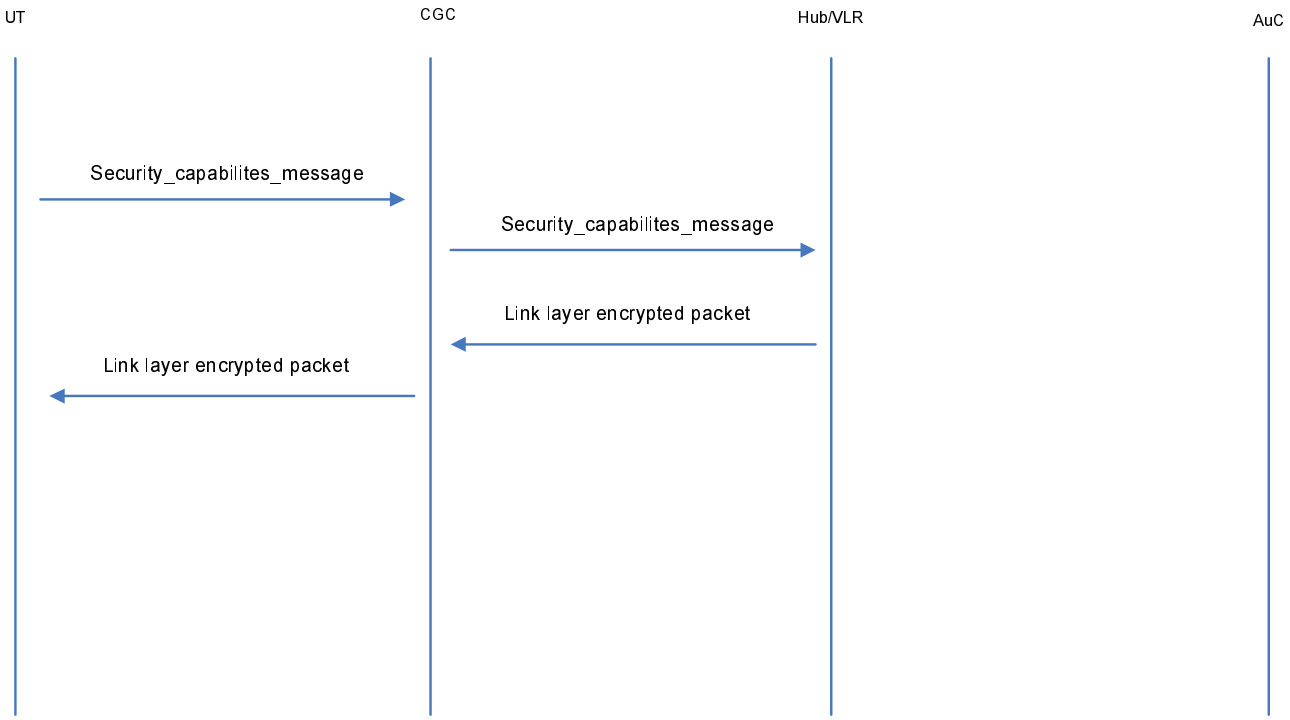

Figure 11.9: Forward link security negotiation procedure over CGC. Link layer security

11.2 IP Layer Security

Security at IP Layer will be provided by using the IPsec protocol suite. IP layer security will only be used in the forward link.

The IPsec negotiation shall be performed using IKEv2 as specified in [7].

In order provide privacy and integrity ESP shall be used in transport mode [9].

This protocol is based on the Diffie Hellman key exchange in order to establish a unidirectional Security Association (SA) for ESP. The unidirectional ESP-SA is established generally after 4 messages. Under a Denial of Service Attack (DoS) IKEv2 can also require 6 messages to establish the unidirectional ESP-SA.

ESP allows the use of different encryption algorithms. The encryption algorithm and its configuration parameters will depend on the implementation. Hub and terminal will agree on the encryption algorithm and its parameters during the IKEv2 negotiation.

The validity of the different IPsec SA shall be implementation dependent. However, due to the scarceness of the bandwidth, it is recommended to specify it based on volume and not time. This way a SA can be valid for a large period of time, avoiding frequent negotiation processes and the consequent overhead.

The dynamic IP-addressing is also a mean of providing security. Whenever the IP address of the terminal changes, a new IPsec negotiation shall be carried out.

The IKEv2 negotiation shall be preceded by a message from the terminal in which the terminal informs the hub of its security capabilities. In case either the hub or the terminal do not support link layer security in the FWD link, the hub will start an IPsec negotiation to secure the FWD link

Since IPsec is located at the network layer, the CGC will be completely transparent to IPsec. They will act as a relay from terminal to hub; therefore the IKE negotiation will not be affected.

To summarize, once the IPsec negotiation has taken place, the terminal and the hub will have two different security keys:

- K_IKE. IKE session encryption key. Used to secure the negotiation (to establish and refresh K_IKE and K_ESP).

- K_ESP. ESP encryption key, used to secure the transmission of data in the FWD link.

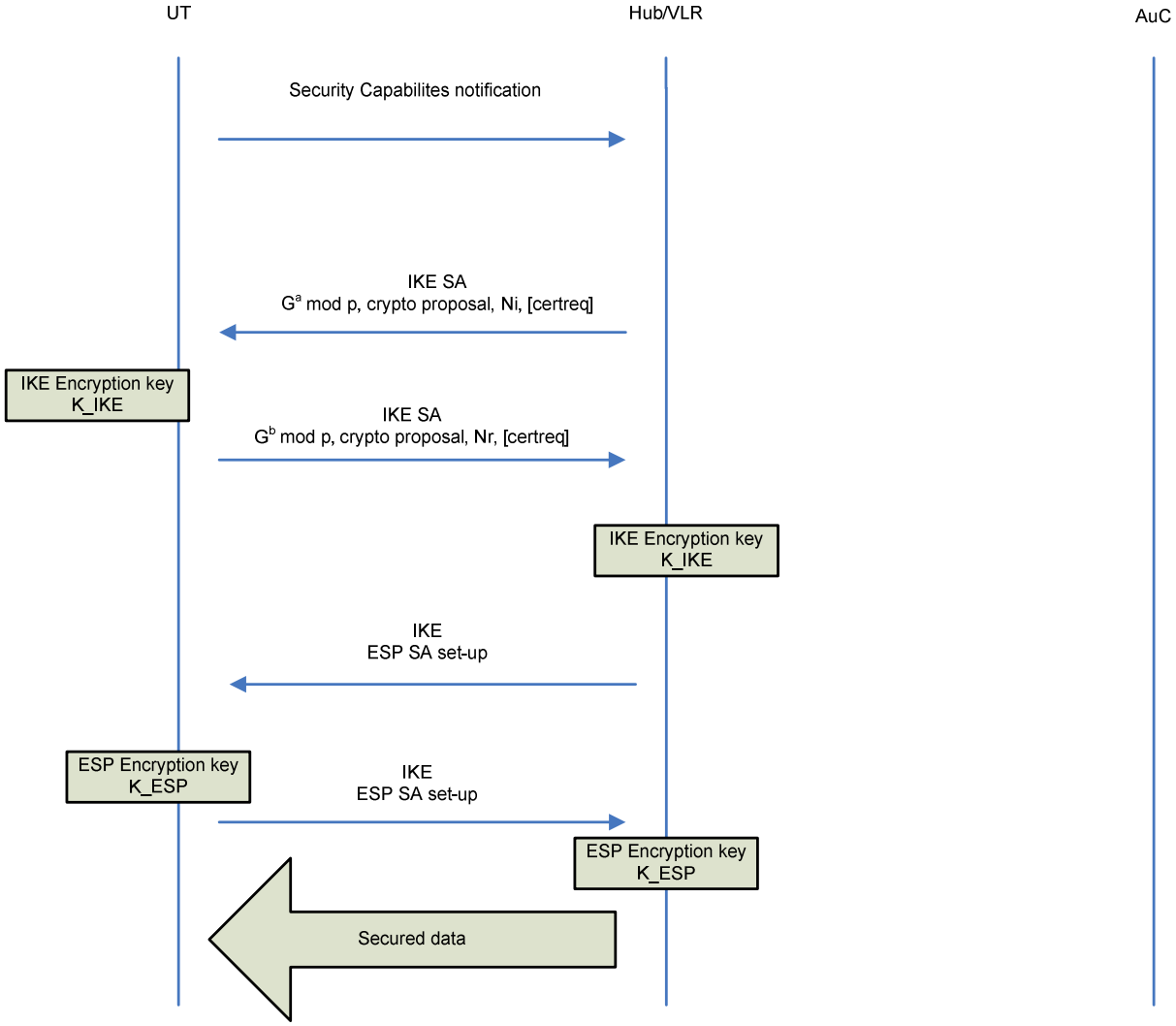

Figure 11.10: IKEv2 negotiation for FWD link

12 Mobility Management

12.1 Location Management Protocol

In mobile networks, location management refers to the network identifying the location area of a terminal to locate it whenever the terminal receives a call, message, paging signal, etc. With this definition, it is not the terminal the one "understanding" its location, but the network.

In the S-MIM system, the satellite shall reach the terminal in the coverage area of a linguistic beam. Therefore, this is the smallest area unit for locating the terminal that is relevant to the S-MIM system. Obviously, the terminal may be also reached through a CGC cluster if the terminal is under the coverage area of any CGC in the cluster. So eventually, it is also interesting for the system to know if a terminal is currently under the coverage area of a CGC in order to reach the terminal.

Given that in the S-MIM system the coverage area of FWD and RTN links may not be symmetric (as spotbeams may deployed in the satellite RTN link and not all Repeaters are associated to a Collector), solving the location area of the terminal does not determine uniquely through which return link the terminal will transmit at each moment of time, thus the location area at the FWD link will be independent of the location area of the same terminal in the RTN link. Nevertheless, the system can identify which resource was used by a terminal for each transmission, as each received packet through any interface (resource) identifies the source of the packet (the terminal). This information might be relevant for billing issues if the operator of the terrestrial infrastructure is not the same as the operator of the satellite infrastructure.

At the terminal side, it is relevant for operational aspects to understand its location area in the RTN link, since it will have to select a RTN link resource for transmission (cell selection procedure).

The different location area definitions, namely Satellite Service Area, FWD Cell, RTN Spot Area and RTN Cell are applicable to the remaining of this clause.

It is assumed that in general, each linguistic beam can be managed by a different service provider. The terminal shall be capable of identifying its home network, i.e. the beam or beams managed by its operator. Therefore, the terminal shall have stored the corresponding Network_Id and the Original_Network_Id belonging to its operator.

12.1.1 Terminal Location in the FWD Link

When a terminal switches on, it will scan the S-band frequency range in scope for the S-MIM system until it can decode a broadcast channel providing PSI/SI information tables about the configuration of the network.

These signalling tables contain the Network_Id and the Original_Network_Id parameters that describe the linguistic beam and the managing hub for that beam, respectively. If the received signal was from the satellite link, the terminal can uniquely resolve with this information its Satellite Service Area. If the signal was received from a Repeater, the following cases apply:

- The global content will repeat the PSI/SI information sent by the satellite; therefore, the terminal will be able to identify the Satellite Service Area.
- If the Repeater is broadcasting local content, a dedicated PSI/SI table shall be provided to let the terminal identify the local content that is available in its SFN cluster. In the local content, the Cell_Id descriptor identifies the SFN cluster within the linguistic beam. With this information, the terminal can uniquely identify the FWD Cell.

The Mobility Management Controller at the terminal will store the Network_Id, the Original_Network_Id and (if the signal received was from a Repeater) the Cell_Id.

The information broadcast in the signalling tables of the FWD link, see Part 8 [4], will provide all required information about the network configuration.

In the case that the terminal is able to receive correctly the signal from two or more broadcast channels at the same time (in overlapping areas), the following applies:

- In the case that two signals are received, one from the satellite and one from a CGC, the Satellite Service Area indicated by both signals is always identical. The terminal shall interpret that it is in the indicated Satellite Service Area and additionally, that it is also within the FWD Cell indicated by the Cell_ID in the PSI/SI tables of the local content.
- In the case that several satellite signals are received correctly in overlapping areas of several linguistic beams, the terminal shall select one of the received broadcast signals (similar to a cell selection in cellular networks). In fact, it is probable that each linguistic beam is managed by a different service provider, hence, selecting one or another beam might imply roaming in general. Therefore, the following guidelines shall be considered:
    - If one of the received signals corresponds to the home network of the terminal, the terminal shall select the Satellite Service Area corresponding to its home network and store the corresponding Network_Id and the Original_Network_Id.

- If several of the received signals correspond to the home network of the terminal, the terminal shall select the broadcast signal with higher reception quality by default and store the corresponding Network_Id and the Original_Network_Id. However, the terminal shall also be capable letting the user selecting manually the Satellite Service Area (for example to enjoy services not provided in all Satellite Service Areas).

- If none of the received signals correspond to the home network of the terminal, the terminal shall select by default the broadcast signal with higher reception quality and store the corresponding Network_Id and the Original_Network_Id. However, the terminal shall also be capable letting the user selecting manually the Satellite Service Area (for example to enjoy services not provided in all Satellite Service Areas).

If the terminal has return link capabilities and the FWD link signals the availability of one or more RTN links, the terminal will perform first the cell selection procedure, described in the following clause, and then mutual authentication with the hub, described in clause 11.1. Through the mutual authentication procedure, a security association will be created between the terminal and the hub. Thanks to this procedure, the hub can determine the current FWD and RTN location of the terminal and it will store this information in the VLR.

For security reasons, the temporary address given to the terminal after mutual authentication will be renewed after its expiry (typically linked to a maximum amount of transmitted data in the S-MIM system). Whenever the TMSI renewal mechanism is triggered, the location information of the terminal is updated at the hub VLR.

12.1.2 Terminal Location in the RTN Link: Cell Selection Procedure

Due to the capability of the S-MIM system to manage asymmetrical coverage in FWD and RTN links, several RTN links can be present for the FWD link that broadcasts the RTN links configuration information. This level of uncertainty can be solved in different ways, depending on the capabilities of the terminal. Solutions are proposed for the following cases:

- Terminals equipped with a "positioning" device (e.g. GPS, GNSS)

- Terminals not equipped with a "positioning" device.

Terminals equipped with a "positioning" device download (offline, for example through a web site or with a CD) or have already stored in memory the RTN coverage maps of the system. The terminal can derive from this information what the available RTN links in its location area and select the most suitable one.

It shall be noted that the RTN Cell Selection shall be only triggered after the FWD link location has been fixed by the terminal (a Satellite Service Area has been stored at the Mobility Management controller at the terminal). The reason is that the FWD link provides information about configuration information of the return links managed within that Satellite Service Area.

The criterion for selection of one or another RTN link shall be configurable. However, some relevant criteria are mentioned below:

- In the presence of a Collector, the terminal shall always select the Collector RTN link, regardless of the presence of a satellite RTN link. The reason is that Collectors are mainly deployed to relax the capacity at the satellite in dense areas.

- Among RTN links of the same type (satellite or terrestrial), the terminal may select the less congested RTN link (the load level is signalled in the FWD link - see TS 102 721-6 [4]).

The following shall be noted:

- Terminals accessing SS1 and SS2 may or may not be equipped with a positioning device.

- Terminals accessing SS3 must be equipped with a positioning device.

- Terminals accessing SS3 will trigger a Call Admission Control (CAC) mechanism to request for resources before starting transmitting data corresponding to a session flow.

Terminals accessing SS3 will use the positioning device to resolve their global position and will use the CAC request message also to indicate their position to the hub. In general, terminals need the coverage maps of the S-MIM system to perform Cell Selection. However, the storing capacity requirements at the SS3 terminals to store the coverage maps of the S-MIM system can be relaxed, since the hub can inform the terminal through a CAC accept/reject message about the most suited spotbeam for transmissions in the return link.

12.1.2.1 Positioning Device-Disabled Terminals

The procedure described below shall be applied to terminals without positioning device and/or terminals with positioning device with outdated coverage maps.

Terminals not equipped with a "positioning" device (this is applicable to low cost terminals for SS1/S2) cannot solve the uncertainty about the suitable return links as straight forward as the "positioning" device-enabled terminals. They receive through the FWD link the configuration information of one or more RTN links and can only differentiate between satellite and terrestrial RTN links, but not among the ones of the same type. In the case of spotbeam coverage in the RTN link, the terminal is not even able to understand which of the satellite RTN links (that seem to be available through the FWD link signalling) provides coverage in the area where the terminal is. Hence, a protocol is required for the terminal to find out which are the suitable RTN links for it. For this purpose, a trial an error protocol is proposed in the following.

If the FWD location didn't change (the terminal is still in the same Satellite Service Area as in the last transmission) the terminal shall assume that the RTN link applied in the previous transmission is still valid and will use it for the next transmission.

If after a few retransmissions (according to the tuning of the ARQ mechanism for) no ACK was received, the terminal will interpret that this RTN link is not valid anymore and will try any of the others announced by the FWD link (randomly). The terminal will repeat this procedure until it succeeds.

If the FWD location changed from the last RTN link transmission, the terminal will select randomly any of the RTN links signalled in the new FWD location and apply the trial and error strategy until it succeeds.

If frequency reuse 1 is applied in the system, the terminal will succeed at the first try. Otherwise, it is expected that a number of tries in the order of 3 will be required as maximum, as a scenario with 6 linguistic beams and about 44 spotbeams gives a less than 8 spotbeams per linguistic beam in average and assuming a frequency reuse of 3, three tries shall be sufficient to succeed.

12.2 Handover Protocols for SS1/SS2

12.2.1 FWD link handover

The management of mobility for DVB-H and DVB-SH systems is defined in ETSI specifications [i.1] and [i.2]. These documents identify a set of use cases for a FWD link handover. If DVB-SH is applied as forward link radio interface in the S-MIM system, forward link mobility shall be compliant to the ETSI specifications [i.1] and [i.2].

For SS1 content delivery purposes over the FWD link, the primary interest is to guarantee seamless reception of a certain IP flow when a user is changing the communication channel or, more in general, when some parameters change: this is called ***handover***. Note that the case of roaming does not correspond to a seamless handover during service operation, but to the case that the terminal detects a Satellite Service Area which is not it's home one and is not managed by the same hub and the terminal selects that Satellite Service Area. Only if roaming agreements are in place between the operator of the home Satellite Service Area of the terminal and the Satellite Service Area that the terminal is visiting, the mutual authentication procedure will be possible.

12.2.2 RTN Link Handover

The Cell Selection procedure defined in clause 12.1.2 applies.

12.3 Handover Protocols for SS3

This clause remains for further study.

12.4 Roaming

12.4.1 Scope of roaming in the S-MIM system

The architecture of the S-MIM system allows that a satellite hub manages one or more linguistic beams, and the corresponding return links (spotbeams). Each hub could be managed by a different service operator, and different services shall be provided in different linguistic beams (and their corresponding return links). As soon as different managing elements appear in the network (satellite hubs), the support of roaming functions becomes necessary if full mobility shall be provided in the system.

Similarly to terrestrial wireless systems, concretely UMTS, the user will subscribe to a S-MIM operator that provides S-MIM services in its geographical area. This subscription will allow the user to access the contracted services through the satellite beam/s and CGCs managed by this operator in the geographical area where this operator provides the services. If roaming agreements are in place between different S-MIM operators, a S-MIM user shall be also capable of accessing services through the satellite beam/s and CGCs of other operators, as far as the operator provides the contracted services package by the user. In practice, roaming agreements together with roaming procedures will allow a user to access services in the visited network without prior subscription to the visited operator.

This implies the security challenge of enabling a S-MIM terminal and the visited S-MIM network to authenticate each other, negotiating security mechanisms, and establishing cryptographic keys to secure the network access without any prior direct trust relationship, as well as using the same credentials on authentication across different hubs. For this purpose, the managing hubs of different S-MIM operators and S-MIM networks must interface each order to verify the existence of roaming authorisation for any requesting visiting terminal, as shown in Figure 12.1.

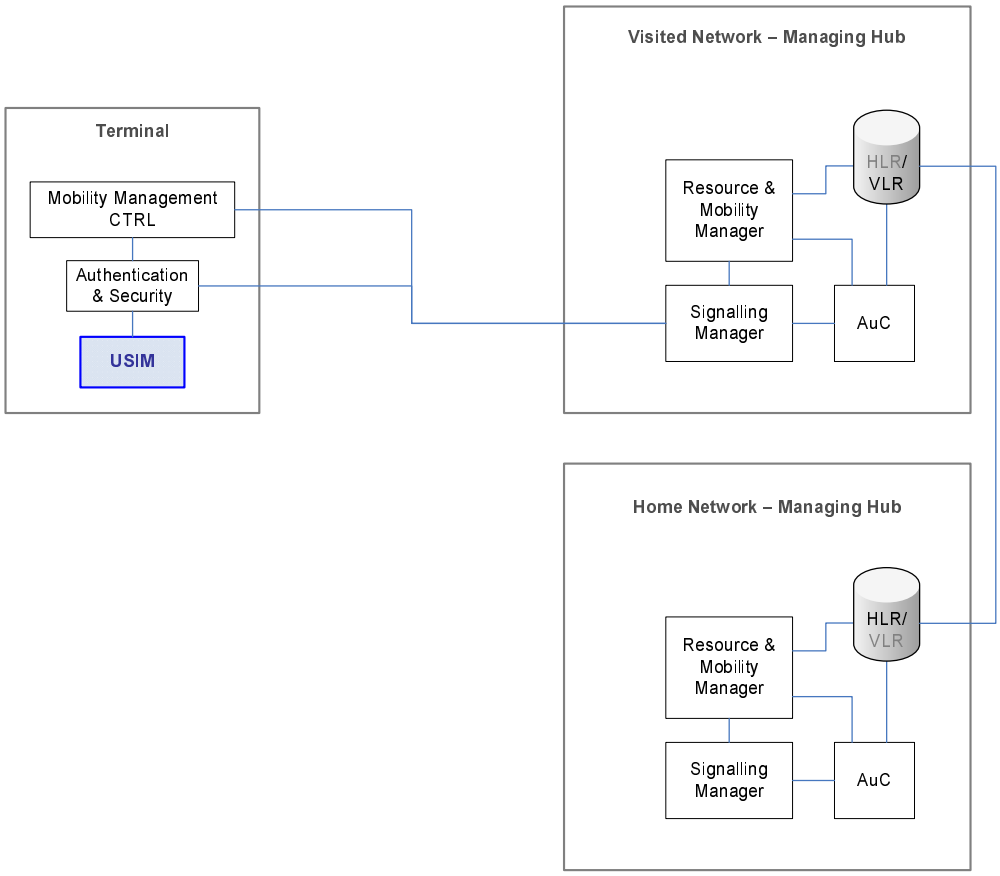

Figure 12.1: Illustration of roaming interfaces

In the context of the S-MIM system, the mechanisms that are required to allow roaming across different S-MIM networks will be specified. In this context, a S-MIM network is composed by one or several linguistic beams (and the corresponding return links) distributing the same set of services, the managing hub, and the CGCs managed by the hub. Roaming functions are executed when a terminal moves into a geographical area where the managing hub is a different one.

A S-MIM user (or subscriber), at the time of contracting the S-MIM service, "registers" to its home network operator. In practice, this means that the home network operator (HNO), defined by the home-hub and the home-beam to that terminal, will allocate an IMSI and a long-term secret key IK for that subscriber. These information are stored in the USIM on the terminal side, and at the AuC on the network (hub) side.

In the UMTS specifications, the IMSI, is in practice composed of 3 elements, namely the mobile country code (MCC), the mobile network code (MNC) and the MSN (the mobile subscriber number). In the S-MIM network the MNC will be applied to identify the S-MIM satellite/terrestrial system worldwide, while the MCC will be applied to identify the linguistic beam (and serving hub). Therefore, the home network of the terminal can be unequivocally identified by the IMSI.

12.4.2 The roaming procedure

When a terminal enters in the coverage area of a linguistic beam managed by a different hub than its home hub (home network), it will start receiving also the broadcast signalling of the visited network, which indicates the identity of the managing hub (through the original_network_id). The terminal will compare the hub identity with the stored one and if it is not the same, it will start the mutual authentication procedure using IMSI (see clause 11.1.1.1), as the previous security association that allowed this terminal identify itself using the TMSI is not valid in the new network.

Upon reception of the authentication request (using IMSI), the AuC of the hub will identify that the provided IMSI does not correspond to any user of this beam, and will identify, through the MCC component of the IMSI, which is the 'home network' (beam and hub) of this user. The VLR at the 'visited network' (beam and hub) will send an *'auntentication_data_request'* to the HLR at the home network of the visiting user. If there is a roaming agreement in place, the HLR of the home network will reply with an authentication vector which contains the RAND, AUTN, IK, CK and RES for the visiting user. The VLR of the visited network will forward the RAND and AUTN to the user and keep the rest of parameters to proceed with the mutual authentication procedure, as specified in clause 11.1.1.1. This process is illustrated in Figure 12.2. This roaming procedure is based on the mutual authentication procedure specified in [5] for the case that the authentication is done with a foreign network; the major difference is that the process is initiated by the terminal when it detects that it is receiving the broadcast signalling of a foreign network.

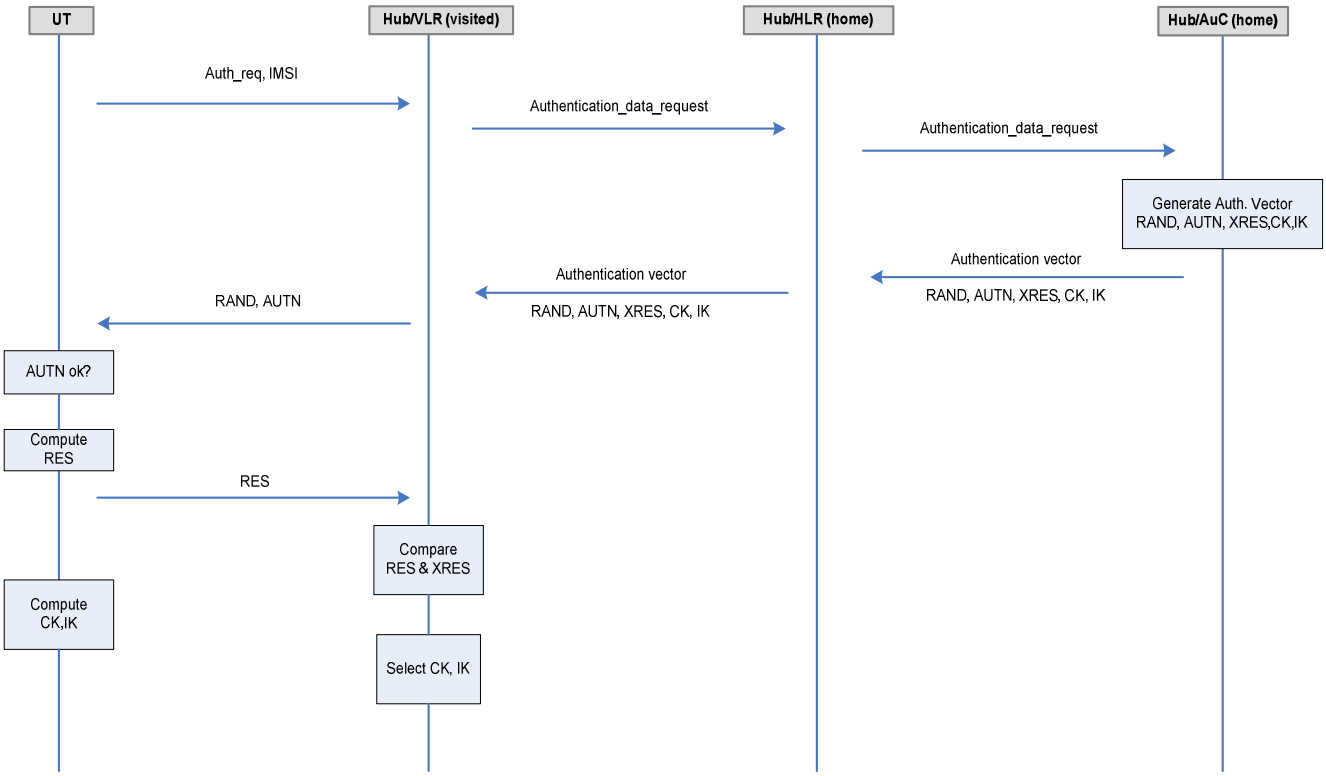

Figure 12.2: Mutual authentication procedure with roaming

Annex A (informative): Recommendations for use of higher layer protocols

A.1 IP Addressing

A.1.1 Unique Local IPv6 address

For access to services in SS1 and SS2, where the communication takes place between users and Service Providers, Ipv6 Link Local addressing is recommended.

Unique Local addressing (ULA), (RFC 4193 [i.12]) is the equivalent to private addressing in IPv4. Conversely to link-local addresses, they are routable within a site but not at Internet as they are not considered global.

The format of this kind of addressing is shown in Table A.1:

Table A.1: Unique local IPv6 address

7 bits	1	40 bits	16 bits	64 bits
Prefix	L	Global ID	Subnet ID	Interface ID

The semantics of a unique local IPv6 address are:

- *Prefix***:** it is fixed to FC00::/7 prefix to identify Local IPv6 unicast addresses.
- *L***:** Set to 1 if the prefix is locally assigned.
- *Global ID***:** 40-bit global identifier used to create a globally unique prefix.
- *Subnet ID***:** 16-bit Subnet ID is an identifier of a subnet within the site.
- *Interface ID***:** 64-bit Interface ID.

This kind of IP addressing allows stateless auto-configuration which is well explained in the RFC 2462 [i.13]. However this mechanism implies that there is a router directly connected to the node that sends router advertisements publishing the Global ID plus Subnet ID. This information should be provided by the HUB adding overhead to the traffic at the satellite link.

Thus the main option is to statically configure the IPv6 address, not manually but automatically:

- *Global ID and Subnet ID*: these parameters should be provided by S-MIM network administrator as both values should be fixed for all the network. So this information should be stored at the terminal.
- *Interface ID*: should derive this value from the locally administered MAC address (IMSI). The process can be illustrated with the following example:

Example assuming that a terminal the MAC address: 34-56-78-9A-BC-DE:

First an interface identifier is built by inserting FF-FE as the third and fourth octet. The interface identifier would be 34-56-FF-FE-78-9A-BC-DE.

Then the IPv6 link local address of the terminal is built by appending the interface identifier to the prefix FE80::/64. The resulting IPv6 address would be: FE80::34-56-FF-FE-78-9A-BC-DE.

Provided that the locally administered MAC addresses are unique, the resulting local unique unicast IPv6 address would be also unique.

This kind of IPv6 address should be used mainly by B3/C class terminals, whose IP sessions (VoIP for eCall) are ended at SIP and RTP proxies at SSM3. However, global IPv6 addressing could also be contemplated but due to the kind of services running within them and the high amount of potential users local unique IPv6 addressing is preferred because of global address saving.

As this IPv6 address is auto-assigned by each terminal just using its MAC address, the elements located at the HUB that communicate with B3/C class terminals can make the same calculation as the HUB knows about MAC addressing in each B3/C class terminal as well.

A.1.2 Global IPv6 address

The use of Global IPv6 addresses become necessary when the terminal connect to other data networks different from the S-MIM network, for example to send an SMS to a UMTS terminal or to establish a telephone call with a PSTN terminal.

The amount of potential D class terminals is much lower than B3/C class ones and they should use global IPv6 addresses to communicate with external networks. The global IPv6 address obtained either by means of DHCP6 during the logon procedure or by static configuration.

Nevertheless, in SS3 IPv6 unique local addresses should be used for B3 terminals as well as D terminals (only Satellite interface). This implementation reduces the overhead introduced by the DHCPv6 protocol in the satellite network.

As a first option, D terminals should have an IPv6 unique local address at its satellite interface. However, the addressing behind this satellite modem should be IPv6 global and the corresponding IP routing configuration should be configured at the HUB routers.

The particular case of use of D terminals makes us contemplate the possibility of having IPv4 addressing behind a third element beyond the satellite modem at LAN interface.

Taking into account that IPv6-tunneling between SEL (OSM3) and SEP (SSM3) is contemplated as the implementation in S-MIM for two-way IP connectivity the range of these IPv4 addresses should be private so that this range is not replicated within S-MIM. In the future, when IPv4 to IPv6 protocol translation standards are more consolidated a full NAT translation at SEL and/or SEP should be considered as a further option and IPv4 private range will be able to replicate regardless of the class D terminal.

Therefore, as S-MIM satellite segment addressing will probably be IPv6, some elements should perform IPv4 to IPv6 translation at D terminal's SEL (see Figure A.1) such as SIP and RTP proxies. However, for the other SS3 service, 2 way IP connectivity, IPv6 tunnelling should be used for the moment instead of protocol translation. The IPv6 address employed to perform this tunnelling should be the global one.

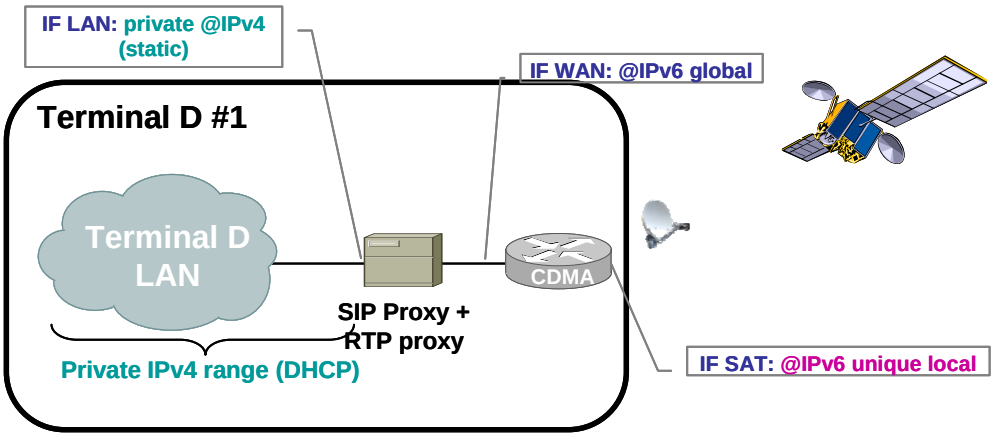

Figure A.1: Terminal D IPv4 to IPv6

Annex B (informative): Recommendations for SS3 handover

In the scope of the SS3 subsystem, a handover involves both the forward and return links. As the provision of SS3 services is based in (i) a connection-oriented basis at network (IP) level and in (ii) a continuous carrier in the return link rather that in random burst basis as the SSA does, some special remarks should be observed.

B.1 Forward Link Handover

For the FWD link, the SS3 services are built over the same air interface, namely DVB-SHrt, as SS1/2 services so the same considerations observed for the FWD link handover do apply, see clause 12.2.

B.2 Return Link Handover

The handover in the scope of the RTN link affects at two different levels: spot selection and spot handover.

B.2.1 Spot Selection Procedure

The same observations made for SS1/SS2 spot selection also applicable to SS3 at LogOn and Capacity Request phase. That is, whenever the terminal has no dedicated resources already allocated in the QS-CDMA domain. At this phase the terminal should resolve the appropriate RTN spot beam to transmit to.

It is assumed that all SS3 enabled terminals has all the necessary information to resolve at any time the correct return link spot beam. This assumption is based in the following primitives:

- Terminals D and E are static at runtime so no handover may happen; this terminals are only concerned about spot selection. It is assumed that these terminals are statically configured with all the required information (i.e. its geographical position) during the deployment phase, for terminals D, or the installation, terminals of class E.
- Terminals B3 and C are mobile terminals so both handover and spot selection concerns them. Both classes of terminals aims at providing eCall service, so it is assumed that they are "positioning" device enabled so their geographical position is self-known by the terminal which, therefore, may be used, in combination with stored coverage maps, to select the appropriate return link spot.

In the scope of the spot selection procedure, both terminals B3 and C, might use the "positioning" device disabled procedure introduced in clause 12.1.2.1. However, this mechanism, as it will be stated in clause 12.3, is not enough for handover, so all SS3 terminals should be equipped with coverage maps and a "positioning" device SS.

B.2.2 Handover

Unlike spot selection, handover is the process that the terminal should execute to switch from one return spot beam to another in the case the terminal has dedicated resources allocated. Notice that the RTN spot handover may or may not involve a FWD link handover.

The handover procedure should be initiated by the terminal which is the element aware of the geographical location and can predict (detect) the need for a RTN link spot switch. Notice that the Hub cannot detect this requirement as it has not information enough to differentiate between fadings and lack of coverage due to a RTN link spot transition.

Once a terminal detects that a RTN link handover is required it sends handover request to the Hub which includes the precise location of the terminal. The Hub, upon reception of the handover request, resolves the RTN link spot to which perform the handover and checks the availability of resources. If resources are available, the Hub generates a positive Ack indicating the new RTN spot and the new resources.

The terminal, upon reception of the positive ACK, should start transmitting using the new resources.

B.3 Network Layer (IP) Handover

In addition to physical handover consideration, and due to the fact that SS3 services are also connection-oriented at network layer (IP) level, there should be some mechanism that allows seamless handover at IP level within an active session.

At IP level, the proposed seamless horizontal handover mechanism relies on the Internal Transport Network that connects all Hubs and the SEP/SSM3 in a meshed way. In order to guarantee IP session continuity dynamic IP routing, that should be updated every time a handover request is accepted, should be configured throughout this network.

This approach assumes the following points to work:

- Fixed IPv6 address assignation: a particular S-MIM terminal should have and maintain the same IP address regardless of the Hub to which is attached at a certain moment.
- Internal Transport Network with few routers: in order to reduce as much as possible the number of routers involved in dynamic routing (i.e. OSPF) should be as low as possible.

B.4 Link Layer Handover

There are also some handover considerations regarding the link layer. In particular and in the scope of SS3, the RoHC protocol defines a set of rules to follow in case of handover. Those are stated in RFC 3409 [9].

The handover in the scope of the RoHC should be handled in two different ways:

- Defining internal mechanism, intra or inter Hub depending on whether the RTN spots are managed by the same Hub or not, for transferring the header compression context between nodes at or before handover. Hub are connected in a meshed way with high capacity IP networks, [$I\_hc\_ip_1$] that can be used to support handover.
- In case this internal mechanism is not available, the context may be resynchronized by the header compression scheme itself by means of a context refresh. For this mechanism to work, control layer should inform the compressor when a handover has occurred, so that it knows when to refresh the context. In RFC 3095 [i.14], clause 6.3.1, some implementation parameters at the compressor side are present, in particular the CONTEXT_REINITIALIZATION signal might be used to support the handover approach at hand.

History

Document history		
V1.1.1	December 2011	Publication