3GPP TS 24.302 V12.3.0 (2013-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network and Terminals;
Access to the 3GPP Evolved Packet Core (EPC)
via non-3GPP access networks;
Stage 3
(Release 12)

Keywords
access, packet mode, UMTS, LTE

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the discovery and network selection procedures for access to 3GPP Evolved Packet Core (EPC) via non-3GPP access networks and includes Authentication and Access Authorization using Authentication, Authorization and Accounting (AAA) procedures used for the interworking of the 3GPP EPC and the non-3GPP access networks.

The present document also specifies the Tunnel management procedures used for establishing an end-to-end tunnel from the UE to the ePDG to the point of obtaining IP connectivity and includes the selection of the IP mobility mode.

The non-3GPP access networks considered in this present document are cdma2000® HRPD and Worldwide Interoperability for Microwave Access (WiMAX), and any access technologies covered in 3GPP TS 23.402 [6]. The present document also specifies UE access to PLMN IP-based services via restrictive non-3GPP access networks covered in 3GPP TS 33.402 [15]. These non-3GPP access networks can be trusted or untrusted access networks.

The present document is applicable to the UE and the network. In this technical specification the network is the 3GPP EPC.

NOTE: cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA).

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] Void.

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[5] Void.

[5A] 3GPP TS 23.203: "Policy and Charging Control Architecture".

[6] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[7] Void.

[8] Void.

[9] 3GPP TS 24.234: "3GPP System to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols".

[10] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)".

[11] 3GPP TS 24.303: "Mobility management based on Dual-Stack Mobile IPv6".

[12] 3GPP TS 24.304: "Mobility management based on Mobile IPv4; User Equipment (UE) - Foreign Agent interface".

[13] 3GPP TS 24.312: "Access Network Discovery and Selection Function (ANDSF) Management Object (MO)".

[14] 3GPP TS 25.304: "User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode".

[15] 3GPP TS 33.402: "3GPP System Architecture Evolution: Security aspects of non-3GPP accesses".

[16] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[16a] 3GPP TS 45.008: "Radio Access Network; Radio subsystem link control".

[17] 3GPP TS 29.273: "Evolved Packet System; 3GPP EPS AAA Interfaces".

[18] 3GPP TS 29.275: "Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols".

[19] 3GPP TS 29.276: "Optimized Handover Procedures and Protocols between EUTRAN Access and cdma2000 HRPD Access".

[20] 3GPP2 X.S0057-B v1.0: "E-UTRAN - HRPD Connectivity and Interworking: Core Network Aspects".

Editors note: The –B version of the above specification is still in preparation. –A version is available, but contains only the requirements for the prior release of this specification.

[21] 3GPP2 C.S0087-B v1.0: "E-UTRAN – HRPD and CDMA2000 1x Connectivity and Interworking: Air Interface Aspects".

Editors note: The –B version of the above specification is still in preparation. –A version is available, but contains only the requirements for the prior release of this specification.

[22] Void.

[23] 3GPP2 C.S0024-B v3.0: "cdma2000® High Rate Packet Data Air Interface Specification".

[23a] 3GPP2 C.S0016-D v1.0: "Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards".

[24] WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 2: "Architecture Tenets, Reference Model and Reference Points", November 2007.

[25] WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3: "Detailed Protocols and Procedures", November 2007.

[26] WiMAX Forum Mobile System Profile Release 1.0 Approved Specification Revision 1.4.0, April 2007.

[27] IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005: "IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendments 2 and Corrigendum 1", February 2006.

[28] IETF RFC 5996 (September 2010): "Internet Key Exchange Protocol Version 2 (IKEv2)".

[29] IETF RFC 3748 (June 2004): "Extensible Authentication Protocol (EAP)".

[30] IETF RFC 4301 (December 2005): "Security Architecture for the Internet Protocol".

[31] IETF RFC 4555 (June 2006): "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[32] IETF RFC 4303 (December 2005): "IP Encapsulating Security Payload (ESP)".

[33] IETF RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)"

[34] IETF RFC 3629 (November 2003): "UTF-8, a transformation format of ISO 10646".

[35] IETF RFC 1035 (November 1987): "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION".

[36] Void.

[37] IETF RFC 6153 (February 2011): "DHCPv4 and DHCPv6 Options for Access Network Discovery and Selection Function (ANDSF) Discovery".

[38] IETF RFC 5448 (May 2009): "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[39] OMA-ERELD-DM-V1_2: "Enabler Release Definition for OMA Device Management".

[40] Void

[41] "Unicode 5.1.0, Unicode Standard Annex #15; Unicode Normalization Forms", March 2008. http://www.unicode.org.

[42] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[43] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol".

[44] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[45] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[46] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[47] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".

[48] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[49] IETF RFC 4739: "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".

[50] 3GPP TS 29.274: "Tunnelling Protocol for Control plane (GTPv2-C)".

[51] 3GPP TS 24.139: "3GPP System-Fixed Broadband Access Network Interworking; Stage 3".

[52] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[53] IETF RFC 2817 (May 2000): "Upgrading to TLS Within HTTP/1.1".

[54] IETF RFC 5246 (August 2008): "The Transport Layer Security (TLS) Protocol Version 1.2".

[55] IETF RFC 6066 (January 2011): "Transport Layer Security (TLS) Extensions: Extension Definitions".

[56] 3GPP TS 24.244: "Wireless LAN control plane protocol for trusted WLAN access to EPC".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

Access Network Discovery and Selection Function: In this specification, Access Network Discovery and Selection Function (ANDSF) is a network element specified in 3GPP TS 23.402 [6]. Unless otherwise specified, the term ANDSF is used to refer to both Home and Visited ANDSF.

Emergency session: In this specification, an emergency session is an emergency PDN connection established in E-UTRAN and handed over to a S2a based cdma2000® HRPD access network.

Home ANDSF: In this specification, the Home ANDSF (H-ANDSF) is an ANDSF element located in the home PLMN of a UE.

Set of Access network discovery information: In this specification, a set of Access network discovery information is the access network discovery information from a single ANDSF**.**

Set of Inter-system mobility policy: In this specification, a set of Inter-system mobility policy is the inter-system policy information received from a single ANDSF**.**

Visited ANDSF: In this specification, the Visited ANDSF (V-ANDSF) is an ANDSF element located in the visited PLMN of a UE.

Restrictive non-3GPP access network type I: a non-3GPP access network forwarding IP packets of TCP connections initiated by a served UE, with destination port 443, and with destination address outside of the non-3GPP access network, and discarding IP packets of some or all other TCP connections initiated by the served UE, with destination address outside of the non-3GPP access network.

Restrictive non-3GPP access network type II: a non-3GPP access network discarding IP packets of TCP connections initiated by a served UE, with destination address outside of the non-3GPP access network, where the non-3GPP access network contains HTTP proxy supporting HTTP CONNECT method for URIs with port 443 and with host outside of the non-3GPP access network.

Restrictive non-3GPP access network: restrictive non-3GPP access network type I or restrictive non-3GPP access network type II.

Firewall traversal tunnel (FTT): a TCP connection with TLS connection enabling passing of messages between UE in restrictive non-3GPP access network and ePDG.

Firewall traversal tunnel keep-alive time (FTT KAT): a maximum time between two subsequent messages sent by UE in the firewall traversal tunnel.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.122 [4] apply:

EHPLMN
Home PLMN
RPLMN
Visited PLMN

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.402 [6] apply:

IFOM capable UE
Inter-APN routing capable UE
Local Operating Environment Information
MAPCON capable UE
S2a
S2b
S2c
Non-seamless WLAN offload capable UE
Single-connection mode (SCM)
Transparent single-connection mode (TSCM)
Multi-connection mode (MCM)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 29.273 [17] apply:

STa

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.301 [10] apply:

Evolved packet core network
Evolved packet system

For the purposes of the present document, the following terms and definitions given in WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] apply:

Network Access Provider
Network Service Provider

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.402 [15] apply:

External AAA server

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AKA	Authentication and Key Agreement
ANDSF	Access Network Discovery and Selection Function
ANDSF-SN	Access Network Discovery and Selection Function Server Name
ANID	Access Network Identity
APN	Access Point Name
DHCP	Dynamic Host Configuration Protocol
DM	Device Management
DNS	Domain Name System
DSMIPv6	Dual-Stack MIPv6
eAN/PCF	Evolved Access Network Packet Control Function
EAP	Extensible Authentication Protocol
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HA	Home Agent
H-ANDSF	Home-ANDSF
HRPD	High Rate Packet Data
HSGW	HRPD Serving Gateway
IEEE	Institute of Electrical and Electronics Engineers
IFOM	IP Flow Mobility
IKEv2	Internet Key Exchange version 2
IARP	Inter-APN Routing Policy
IPMS	IP Mobility Mode Selection
ISMP	Inter-system Mobility Policy
ISRP	Inter-system Routing Policy
IANA	Internet Assigned Numbers Authority
I-WLAN	Interworking – WLAN
MAPCON	Multi Access PDN Connectivity
MCM	Multi-connection mode
MO	Management Object
NAI	Network Access Identifier
NAP	Network Access Provider
NBM	Network based mobility management
NSP	Network Service Provider
NSWO	Non-Seamless WLAN Offload
OMA	Open Mobile Alliance

PCO	Protocol Configuration Options
P-GW	PDN Gateway
PDU	Protocol Data Unit
SCM	Single-connection mode
S-GW	Serving Gateway
SPI	Security Parameters Index
TSCM	Transparent single-connection mode
UE	User Equipment
UICC	Universal Integrated Circuit Card
V-ANDSF	Visited-ANDSF
W-APN	WLAN APN
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WLCP	WLAN Control Protocol
WMF	WiMAX Forum

4 General

4.1 Trusted and untrusted accesses

The HPLMN operator of the EPC selects whether a connected non-3GPP IP access network is a trusted or untrusted IP access network.

For a trusted non-3GPP IP access network the communication between the UE and the EPC is secure. For an untrusted non-3GPP IP access network the communication between the UE and the EPC is not trusted to be secure.

For a trusted non-3GPP IP access network, all communication between the access network and the EPC is transferred over pre-established secure links.For an untrusted non-3GPP IP access network, to secure communication between the UE and the EPC:

- A single IPSec tunnel needs to be established to the ePDG for all PDN connections when S2c interface is used; or
- An IPSec tunnel needs to be established with the same ePDG for each PDN connection when S2b interface is used.

4.2 cdma2000® HRPD Access System

The cdma2000® HRPD system is a wireless mobile system developed under the auspices of 3GPP2. The cdma2000® HRPD system and its access network subsystem is compliant with 3GPP2 X.S0057 [20] and 3GPP2 C.S0087 [21], which define the core network and air interface aspects, respectively.

4.3 WiMAX Access System

The WiMAX system is a wireless mobile broadband system developed under the auspices of the WMF and the IEEE. The WiMAX system and its access network subsystem are compliant with WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 2 [24]. The protocol architecture and signalling of the WiMAX system is specified in WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] which supports the air interface defined in WiMAX Forum Mobile System Profile Release 1.0 Approved Specification Revision 1.4.0 [26] specifying selected profiles of IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005 [27] that are to be supported. The WiMAX access system correspond to the WiMAX Access Service Network (ASN) and to relevant interfaces, as defined in WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25].

4.4 Identities

4.4.1 User identities

The user identification shall be either the root NAI, or the decorated NAI as defined in 3GPP TS 23.003 [3], when the UE accesses the EPC via non-3GPP access networks, and gets authentication, authorization and accounting services from the EPC. For handover of an emergency session from E-UTRAN to a S2a based cdma2000® HRPD access network, if IMSI is not available (i.e. a UE without USIM) or IMSI is unauthenticated, the IMEI shall be used for the identification, as part of the emergency NAI as defined in 3GPP TS 23.003 [3].

User identification in non-3GPP accesses may require additional identities that are out of the scope of 3GPP.

IETF RFC 4187 [33] and 3GPP TS 23.003 [3] provide definitions for UE and user identities although they use slightly different terms. Similar terms are also used in 3GPP TS 33.402 [15]. The following list provides term equivalencies and describes the relation between various user identities.

- The Root-NAI as specified in 3GPP TS 23.003 [3] is to be used as the permanent identity as specified in 3GPP TS 33.402 [15].
- The Fast-Reauthentication NAI as specified in 3GPP TS 23.003 [3] is to be used as the Fast-Reauthentication Identity or the re-authentication ID as specified in 3GPP TS 33.402 [15].
- The Pseudonym Identity as specified in 3GPP TS 23.003 [3] is to be used as the Pseudonym as specified in 3GPP TS 33.402 [15].

4.4.2 Identification of IP Services/PDN connections

For access to EPC the Access Point Name (APN) is used for identifying IP services/PDN connections. The detailed definition of APN as used for access to EPC is specified in 3GPP TS 23.003 [3]. APN is conveyed in the IKEv2 signaling during tunnel establishment when S2b interface is used for UE to access EPC. When UE accesses to EPC via S2a using trusted WLAN access network, APN is conveyed in EAP-AKA' signaling for single-connection mode (SCM) or in WLAN Control Protocol (WLCP) signaling (see 3GPP TS 24.244 [56]) for multi-connection mode (MCM)

4.4.3 FQDN for ePDG Selection

An ePDG Fully Qualified Domain Name (ePDG FQDN) is constructed by UE and used as input to the DNS mechanism for ePDG selection.

The detailed format of this ePDG FQDN is specified in 3GPP TS 23.003 [3].

4.4.4 Access Network Identity

For access to EPC through a trusted non-3GPP access network via S2a the UE has to use the Access Network Identity (ANID) in the key derivation (see 3GPP TS 33.402 [15]). The handling of the Access Network Identity is described in subclause 6.4.2.4 and the generic format and specific values for the Access Network Identity are defined in subclause 8.1.1.

4.4.5 ANDSF Server Name

The ANDSF Server Name (ANDSF-SN) is used for ANDSF discovery. The detailed rules are defined in subclause 6.8.2.2.1 and the format of the ANDSF-SN is specified in 3GPP TS 23.003 [3].

4.4.6 Home Agent address(es)

If DSMIPv6 is used, the Home Agent IPv6 address (and optionally an IPv4 address) are needed. Within this specification, Home Agent address(es) signalling via IKEv2 between the UE and the ePDG is defined in subclause 7.4.1.

4.4.7 Security Parameters Index

The Security Parameters Index (SPI, see IETF RFC 4301 [30]) identifies uniquely a security association between the UE and the ePDG. For the case of NBM using S2b a one to one mapping between SPI and PDN connection applies.

4.5 Fixed Broadband Access System

The Fixed Broadband Access system is a type of high-speed Internet access for multi-service broadband packet networking. The Fixed Broadband Access system is specified by the Broadband Forum, including addressing interoperability, architecture and management.

For support of Fixed Access Broadband access interworking, the EPC network procedures and the UE procedures are specified in 3GPP TS 24.139 [51].

For support of Fixed Broadband access convergence, the architecture is specified in 3GPP TS 23.203 [5A] and the UE procedures are the same as the UE procedures for support of Fixed Broadband access interworking.

4.6 Restrictive non-3GPP access networks

An untrusted non-3GPP access network can be a restrictive non-3GPP access network. When the UE is served by a restrictive non-3GPP access network, the UE and the ePDG follow the additional procedures described in the annex F.

5 Network Discovery and Selection

5.1 Access network discovery and selection procedures

5.1.1 General

If PLMN selection specified in 3GPP TS 23.122 [4] and in 3GPP TS 24.234 [9] is applicable (e.g., at switch on, recovery from lack of coverage, or user selection of applicable access technology), the PLMN selection to select the highest priority PLMN according to these specifications is performed before any access network discovery and selection procedures based on ANDSF rules are performed in the selected PLMN.

In the access network discovery procedure the UE may get from the ANDSF information on available access networks in its vicinity. The UE may obtain this information by querying the ANDSF, and may use this information when determining the presence of operator preferred access networks. Determination of the presence of access networks requires using radio access specific procedures, which are not further described here.

The UE can first select an access network and then determine the presence of this access network, or first determine the presence of several access networks and then select between them. If a higher priority access network has been found connected to the same PLMN or a higher priority PLMN, the UE will then attempt to attach via that network.

5.1.2 Access network discovery procedure

5.1.2.1 Triggering the discovery of operator preferred access networks with the ANDSF

The UE may initiate communications with the ANDSF for operator preferred access network discovery:

- When conditions set up within the policies available in the UE are met; or
- When a user requests for manual selection.

NOTE 1: The minimum allowed time interval between two consecutive UE initiated requests towards the ANDSF can be set by operator policies.

NOTE 2: The UE changing of access networks can override the minimum allowed time interval setting.

5.1.2.2 Discovering availability of access networks

The UE may apply the techniques specific to the non-3GPP access technologies to discover available non-3GPP access networks. Such techniques will not be further described here.

In addition, the UE may signal to the ANDSF to obtain information on operator preferred access networks. The discovery of the ANDSF by the UE, the connection to the ANDSF by the UE and the signalling between the UE and the ANDSF are given in sub clause 6.8.

5.1.3 Access network selection procedure

5.1.3.1 General

The access network selection may be classified as inter-technology or intra-technology.

The UE can use information received from ANDSF for inter-technology access network selection; other mechanisms for inter-technology access network selection are out of scope of this specification.

5.1.3.2 Specific intra-technology access network selection

In this release of the specification the use of the following specific intra-technology access network selection procedures is specified.

5.1.3.2.1 cdma2000® HRPD access network selection

The access network selection process for cdma2000® HRPD access networks shall follow 3GPP2 X.S0057 [20].

5.1.3.2.2 WiMAX NAP selection

The access network selection process for WiMAX which encompasses the NAP discovery and access, shall follow the WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25].

5.2 EPC network selection

5.2.1 General

The following EPC network selection procedures are defined:

1) WiMAX specific;

2) EPC network selection via cdma2000® HRPD access is given in 3GPP TS 23.122 [4] with any exceptions detailed in subclause 5.3.4.

3) EPC network selection via WLAN access shall follow the procedures defined for PLMN selection given in subclause 5.2 of 3GPP TS 24.234 [9] with the exception of the tunnel set up procedure. When the UE is connected to EPC through WLAN access, the tunnel is set-up with the ePDG (as described in clause 7 of this document) or with the HA (as described in 3GPP TS 24.303 [11]); and

4) Generic EPC network selection for other access technologies not listed above.

The UE can utilize information received from ANDSF to which EPCs an access network is connected as described in 3GPP TS 24.312 [13]. Additionally, any technology specific means can be employed to acquire such information, but these are out of scope of this specification.

NOTE: There are no specific EPC network selection procedures specified for emergency access in this version of the specification.

5.2.2 Generic EPC network selection procedure

5.2.2.1 Identification of the EPC

The identification of EPC shall be based on one of the following:

- PLMN-Id (i.e. pair of MCC+MNC), as specified in 3GPP TS 23.003 [3]; or
- Home/Visited Network Realm/Domain, as specified in 3GPP TS 23.003 [3].

5.2.2.2 Selection at switch-on or recovery from lack of coverage

5.2.2.2.1 UE selection modes

Two modes of EPC network selection are defined, manual and automatic.

At switch-on or following recovery from lack of coverage, the UE shall select the EPC network according to the selected operating mode.

5.2.2.2.2 Manual EPC network selection

The UE shall present the list of available EPC networks, to which connectivity is provided through the selected non-3GPP access network, to the user. If UE's HPLMN or PLMNs equivalent to it are in this list, they shall be shown in the highest ranking order. The ordering of the rest of entries in the list is implementation dependent. If available, the UE should display names and/or realms/domains.

If multiple equivalent HPLMNs are available, then the display order among them is UE implementation specific.

5.2.2.2.3 Automatic EPC network selection

The UE may use locally stored data for selecting between EPC networks available for connectivity via the currently selected non-3GPP access network.

The UE shall select a PLMN according to the PLMN selection procedures of the selected non-3GPP access network.

Additional criteria are out of scope of this specification and remain implementation specific.

5.2.3 Access technology specific EPC network selection procedures

5.2.3.1 EPC network selection procedures for WiMAX

5.2.3.1.1 Identification of the EPC by the WiMAX access network

With WiMAX as a non-3GPP access network, the WiMAX NSP is mapped onto the EPC network operator. The NSP indication can be provided to the UE in accordance to WiMAX Forum Network Architecture Release 1.0 version 1.2 [25]. The WiMAX access network should advertise the NSP identity of the EPC in the MCC, MNC format.

5.2.3.1.2 Selection at switch-on or recovery from lack of coverage

5.2.3.1.2.1 UE selection modes

There are two modes of network selection, namely, manual network selection and automatic network selection.

At switch-on or following recovery from lack of coverage, the UE shall follow one of the following two procedures depending on its operating mode.

5.2.3.1.2.2 Manual EPC network selection

The manual network selection for WiMAX access shall follow the WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] with the following exceptions and additions:

- When presenting the list of available networks for user selection, the UE shall provide the network name of the related MCC + MNC pair. If that is not possible, the UE shall provide the MCC + MNC pair; and
- If the UE is unable to register to the user selected NSP, further UE action is implementation dependent.

5.2.3.1.2.3 Automatic EPC network selection)

The automatic network selection for WiMAX access shall follow the WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] without any exceptions or additions.

5.3 Access Network reselection

5.3.1 General

The network reselection procedure shall be executed based on the user's request or the operator's policy. Such operator policy for supporting network reselection can be provided by the ANDSF or can be pre-provisioned in the UE.

5.3.2 UE procedures

The UE may retrieve information from ANDSF, which includes available access network and operator's policy as specified in subclause 6.8.2.

The information which is retrieved from the ANDSF shall not impact the PLMN selection and reselection procedures specified in 3GPP TS 23.122 [4] and in 3GPP TS 24.234 [9].

The network reselection procedure can be in automatic mode or manual mode dependent on UE configuration settings. For WiMAX access, the manual mode reselection shall follow the behaviour described in subclause 5.2.3.1.2.2 and the automatic mode reselection shall follow the behaviour described in subclause 5.2.3.1.2.3.

5.3.3 EPC procedures

The ANDSF shall send available access network(s) and operator's policy to the UE in response to the UE’s request or based on the network triggers as specified in subclause 6.8.2.

5.3.4 Periodic EPC network reselection attempts

In automatic mode, when UE is not in its HPLMN or one of its equivalent HPLMNs, the UE shall make a periodic attempt to return to its HPLMN or one of its equivalent HPLMNs. For this purpose the timer value given in the EF_{HPPLMN} as defined in 3GPP TS 31.102 [45] shall be used with the following exceptions:-

- For UE accessing the EPC via cdma2000® HRPD access networks, the UE's search for a more preferred system shall abide by the parameters and procedures defined in 3GPP2 C.S0016 [23a].
- For UE accessing the EPC via WiMAX access networks, the time period between periodic network searches is implementation specific.
- For UE accessing the EPC via any other non-3GPP access networks, unless the UE has availability to EF_{HPPLMN}, the time period between periodic network searches is implementation specific but shall not be less than 30 minutes.

5.4 Data traffic routing of IP flows

5.4.1 General

In regards to the routing of IP flows, 3GPP TS 23.402 [6] defines the following UE capabilities: IFOM capability, inter-APN routing capability, NSWO capability and MAPCON capability. Any of these capabilities can be enabled and disabled via UE configuration means outside of the scope of this document. A capability that exists and has not been disabled is considered as supported. A capability that does not exist or the existing capability that has been disabled is considered as not supported.

A UE can have several sets of information about access technologies or access networks or both to assist in determining the data traffic routing of IP flows. These sets of information are:

- the Inter-APN Routing policies. For an IFOM capable UE or a non-seamless WLAN offload capable UE, or a MAPCON capable UE or any combination of these capabilities, the IARP can be statically provided within that UE. Additionally, the IARP can be provided by the H-ANDSF. The UE shall ignore the IARP received from the V-ANDSF;

- the Inter-System Routing policies. The ISRP can be statically provisioned in the UE or it can be provided over the S14 interface by the H-ANDSF or the V-ANDSF or both;

- the Local Operating Environment Information. The Local Operating Environment Information can be optionally generated by the UE locally and the contents of Local Operating Environment Information is implementation dependant; and

- user preference settings.

This clause describes the relationship amongst these information sets and how they are used in order to route data traffic of IP flows. The Local Operating Environment Information does not apply to MAPCON rules in this version of the specification.

5.4.2 Access technology or access network selection

When selecting the access technologies or access networks or both to route the data traffic of IP flows, a UE supporting IFOM or non-seamless WLAN offload and provided with user preferences and having IARP rule for NSWO, ISRP or Local Operating Environment Information or any combination of them may perform the following:

- when selecting the access technology or access network or both for routing data traffic of a specific IP flow the user preference settings take precedence over IARP rule for NSWO (if present), ISRP (if present) and Local Operating Environment Information (if present).

When selecting the access technologies or access networks or both to route the data traffic of IP flows, a UE supporting IFOM or non-seamless WLAN offload and having IARP rule for NSWO, ISRP and Local Operating Environment Information and no user preference settings may perform the following:

- if based on the content of Local Operating Environment the UE supporting IFOM or non-seamless WLAN offload decides that an access technology or access network or both do not meet implementation specific criteria for routing data traffic of a specific IP flow, the UE may exclude that access technology or access network or both when deciding on the routing of the data traffic for those IP flows.

When selecting the access technologies or access networks or both to route the data traffic of IP flows, a UE supporting IFOM or non-seamless WLAN offload having Local Operating Environment Information and none of available ISRP, IARP rule for NSWO and user preference settings may perform the following:

- the UE supporting IFOM or non-seamless WLAN offload selects the access technology or access network or both for routing data traffic of a specific IP flow by evaluating the available access technologies or access networks against the Local Operating Environment Information.

When a UE supporting MAPCON selects the access technologies or access networks or both, to route the data traffic of a specific APN, the user preference settings shall take precedence over ISRP (if present).

The user preference settings shall take precedence over IARP (if present). If no valid IARP present, then Inter-APN routing policy configuration is UE implementation dependent.

6 UE – EPC Network protocols

6.1 General

6.2 Trusted and Untrusted Accesses

6.2.1 General

For a UE, the trust relationship of a non-3GPP IP access network is determined by the home PLMN operator. That trust relationship is indicated to the UE via the following methods:

- Pre-configured policies in the UE by the home PLMN operator.
- Dynamic indication during 3GPP-based access authentication.

For a trusted non-3GPP IP access network, the UE shall follow the access methods given in subclause 6.4. For an untrusted non-3GPP IP access network, the UE shall follow the access methods given in subclause 6.5.

If the dynamic trust relationship indication is received during 3GPP-based access authentication, the UE shall rely on the dynamic trust relationship indication. Otherwise the UE shall follow the pre-configured policies for a specific non-3GPP access network. If no dynamic indicator is received, and no pre-configured policy matches a specific non-3GPP access network where the UE attempts to access, the UE shall follow the procedure defined in subclause 6.2.4.

6.2.2 Pre-configured policies in the UE

The following types of policies can be pre-configured on the UE by the home PLMN operator:

- Pre-configured trust relationship policies for specific non-3GPP access technologies and/or PLMNs. For example, the UE may be configured to use the procedures for trusted access networks as described in subclause 6.4 as follows:
  - an access network of access technology X1 from PLMN Y1 is trusted; and/or
  - any access network of access technology X2 is trusted; and/or
  - any access network from PLMN Y2 is trusted; and/or
  - any access network is trusted.

The format of the pre-configured policies is not specified in this release of this specification.

6.2.3 Dynamic Indication

If the UE performs 3GPP-based access authentication, the 3GPP AAA server may send a trust relationship indicator of the non-3GPP access network to the UE during the EAP-AKA or EAP-AKA' based access authentication (i.e. EAP-AKA, EAP-AKA') as specified in 3GPP TS 33.402 [15]. If non-3GPP access network is trusted, the 3GPP AAA server shall send this trust relationship indicator as specified in 3GPP TS 29.273 [17]. The indicator is sent using a AT_TRUST_IND attribute, by extending the EAP-AKA (and EAP-AKA') protocol as specified in subclause 8.2 of IETF RFC 4187 [33]. This attribute is provided in EAP-Request/AKA-Challenge or EAP- Request/AKA'-Challenge message payload respectively. The detailed coding of this attribute is described in subclause 8.2.3.1.

6.2.4 No trust relationship information

If no dynamic indicator is received, and no pre-configured policies matches a specific non-3GPP access network where the UE attempts to access, the UE shall consider it as untrusted network and operate based on subclause 6.5.

6.3 IP Mobility Mode Selection

6.3.1 General

The IP mobility mechanisms supported between 3GPP and non-3GPP accesses within an operator and its roaming partner's network may be based on either:

a) Static Configuration; or

b) Dynamic Configuration.

The choice between a) and b) depends upon operators' preferences or roaming agreement or both.

6.3.2 Static configuration of inter-access mobility mechanism

For networks deploying a single IP mobility management mechanism, the statically configured mobility mechanism can be access type or roaming agreement specific or both. The information about the mechanism to be used in such scenario is expected to be provisioned into the terminal and the network.

In static configuration, if there is a mismatch between the IP mobility mode mechanism parameters pre-configured in the network and in the UE, the UE may not be able to access the EPC. If the UE is able to access the EPC even if there is a mismatch between the IP mobility mode mechanisms, the network may not be able to provide session continuity for the UE. More details of the possible cases of mismatch between the IP mobility mode mechanism are described in the informative annex D.

If the network is configured with a static mobility mechanism and the AAA server implements protocol extensions for a dynamic IP Mobility Mode Selection (IPMS) exchange, the AAA server shall send to the UE an AT_RESULT_IND attribute during the authentication procedure as it is described in subclause 6.3.3.1.2.

6.3.3 Dynamic configuration of inter-access mobility mechanism

6.3.3.0 General

Dynamic IP Mobility Mode Selection (IPMS) consists of:

- IP mobility management protocol selection between Network Based Mobility (NBM), DSMIPv6 or MIPv4; and
- Decision on IP address preservation if NBM is selected

Upon initial attachment to a non-3GPP access and upon handoff to non-3GPP accesses, the UE performs IPMS by providing an indication during network access authentication for EPC. For trusted access, the indication is provided before an IP address is allocated to the UE, while in untrusted access network, the indication is provided during IKEv2 signalling for IPSec tunnel establishment with the ePDG.

When the UE provides an explicit indication for IPMS, then the network shall provide the indication to the UE identifying the selected mobility management mechanism.

When the dynamic IP mobility mode selection is used if the UE does not receive any indication of a selected mobility protocol after the UE provided an explicit indication, it is considered as an abnormal case and the UE may not get connectivity to the EPC.

NOTE: The scenarios for mobility mode selection are described in subclause 4.1.3 of 3GPP TS 23.402 [6].

6.3.3.1 IPMS indication

6.3.3.1.1 IPMS indication from UE to 3GPP AAA server

During network access authentication, UE may provide an explicit indication to the 3GPP AAA server about the supported mobility protocol by using an attribute in the EAP-AKA and EAP-AKA' protocols, to extend these protocols as specified in subclause 8.2 of IETF RFC 4187 [33]. This attribute is provided in EAP-Response/AKA-Challenge and corresponding EAP-AKA' message payload.

The UE may provide the indication for IPMS using AT_IPMS_IND attribute in EAP-AKA or EAP-AKA' if the UE receives the AT_RESULT_IND attribute within the EAP-Request/AKA-Challenge message, or the EAP-Request/AKA'-Challenge message (when EAP-AKA' is used). If the UE provides the AT_IPMS_IND attribute within the EAP-Response/AKA-Challenge message payload or within the EAP-Response/AKA'-Challenge message payload (when EAP-AKA' is used), the UE shall also provide the AT_RESULT_IND attribute within the message.

If the UE supports IPMS indication, it shall indicate support for one or more mobility protocols in AT_IPMS_IND attribute as follows:

- the UE shall indicate support for DSMIPv6 if the UE supports DSMIPv6; and
- the UE shall indicate support for MIPv4 if the UE supports MIPv4; and
- during initial attach, the UE should indicate support for NBM if the UE supports address preservation based on NBM between the access it is attaching to and all other accesses that the UE supports.; or
- upon handover, the UE shall indicate support for NBM if the UE supports address preservation based on NBM while moving from source access network to target non-3GPP access network that the UE is attaching to.

NOTE: The UE can be configured not to use IPMS indication, e.g. the UE is DSMIP capable only.

If the UE does not support any mobility protocol then the UE shall not send the AT_IPMS_IND attribute to the 3GPP AAA server.

The preference of protocol may be indicated based on the policies configured on the UE. The detailed coding of this attribute is described in subclause 8.2.1.1.

6.3.3.1.2 IPMS indication from 3GPP AAA server to UE

A 3GPP AAA server supporting IPMS shall include the AT_RESULT_IND attribute within the EAP-Request/AKA-Challenge and corresponding EAP-AKA' message payload.

If the UE provided an explicit indication as described in subclause 6.3.3, the 3GPP AAA server shall inform the UE of its decision on the mobility protocol and IP preservation mode by invoking an EAP-Request/AKA-Notification dialogue when EAP-AKA is used or an EAP-Request/AKA'-Notification dialogue when EAP-AKA' is used.

On selecting the mobility protocol based on UE indication, access network capabilities and network policies, the 3GPP AAA server shall indicate the selected protocol to the UE by using the AT_IPMS_RES attribute. If the 3GPP AAA server does not receive any indication from the UE but knows the UE's policies allow the usage of NBM and knows the home and access network supports NBM, the network shall use NBM shall be used for providing connectivity to the UE.

If the AT_IPMS_RES attribute indicates DSMIPv6 then the UE shall follow the procedures defined in 3GPP TS 24.303 [11].

If the AT_IPMS_RES attribute indicates MIPv4 support, then the UE shall follow the procedures defined in 3GPP TS 24.304 [12].

The detailed coding of this attribute is described in subclause 8.2.1.2.

6.4 Authentication and authorization for accessing EPC via a trusted non-3GPP access network

6.4.1 General

For access to the EPC via a trusted non-3GPP access network, a connection shall be established between the UE and the trusted non-3GPP access network using signalling procedures specific to the trusted non-3GPP access network, which are out of scope of this present document.

Access authentication signalling for access to the EPC shall be executed between the UE and 3GPP AAA server to ensure mutual authentication of the user and the EPC, with the exception of UEs without IMSI (see subclauses 4.4.1 and 6.6.3.2). Such authentication is based on IETF protocols as specified in 3GPP TS 33.402 [15].

EAP-AKA' is used for access authentication in the trusted access network, according to 3GPP TS 33.402 [15], subclause 6.2. According to 3GPP TS 33.402 [15], subclause 6.1, EAP-AKA' can be skipped if conditions listed in subclause 9.2.2.1 of 3GPP TS 33.402 [15] are met.

If the access network does not support EAP-AKA or EAP-AKA' and the UE considers the access network as trusted, the UE shall access to the EPC only via S2c and any authentication method (EAP-based or otherwise) can be used for access authentication as long as the criteria set in 3GPP TS 33.402 [15], subclause 9.2.2.1 are met.

During S2c bootstrapping EAP-AKA authentication is performed between the UE and the PDN-GW as specified in 3GPP TS 24.303 [11] and 3GPP TS 33.402 [15].

6.4.1A TWAN connection modes

As part of EAP-AKA' authentication via TWAN, the UE and the network can negotiate usage of either the single-connection mode (SCM) or the multi-connection mode (MCM) as described in 3GPP TS 23.402 [6].

NOTE: UE requesting neither SCM nor MCM acts in transparent single-connection mode (TSCM). No UE extensions are needed for TSCM.

The negotiation consists of the following steps:

a) The 3GPP AAA server indicates support of TSCM, SCM, MCM or any combination of them as described in subclause 6.4.3.5.

b) The UE requests usage of SCM or MCM as described in subclause 6.4.2.6 or acts in TSCM.

c) The 3GPP AAA server either accepts or rejects the UE request as described in subclause 6.4.3.5.

6.4.2 UE procedures

6.4.2.1 Identity Management

The user identities to be used by the UE in the authentication and authorization for accessing EPC via a trusted non-3GPP access are the Root-NAI (permanent identity), decorated NAI, Fast-Reauthentication NAI (Fast-Reauthentication Identity) and Pseudonym Identity and these identities are described in subclause 4.4.

6.4.2.2 EAP-AKA and EAP-AKA' based Authentication

The UE shall support EAP-AKA based authentication as specified in IETF RFC 4187 [33] and EAP-AKA' based authentication as specified in IETF RFC 5448 [38]. 3GPP TS 33.402 [15] specifies the conditions under which one or the other of these two methods is used.

During network access authentication, the UE may provide an explicit indication for IPMS by adding an attribute in the EAP-AKA or EAP-AKA' payload as defined in subclause 6.3.3.

During network access authentication, the 3GPP AAA server may provide the ANID to the UE, see subclause 6.4.2.4.

6.4.2.3 Full Authentication and Fast Re-authentication

The UE shall support both full authentication and fast re-authentication for EAP AKA as specified in IETF RFC 4187 [33] and for EAP-AKA' as specified in IETF RFC 5448 [38].

Full authentication is performed to generate new keys. The initial authentication shall be a full authentication as specified in 3GPP TS 33.402 [15]. For a full authentication either the Permanent Identity or the Pseudonym Identity is used.

According to 3GPP TS 33.402 [15] the fast re-authentication procedure uses the Fast Re-authentication Identity and is used for renewing the session keys.

The Permanent Identity is based on the IMSI of the UE. The Fast Re-authentication Identity is provided to the UE by the 3GPP AAA server during the previous authentication procedure. The UE shall use the Fast Re-authentication Identity only once. A Pseudonym Identity provided to the UE by the 3GPP AAA Server during a previous authentication procedure can be reused in later authentications until the UE receives a new Pseudonym identity from the 3GPP AAA Server.

NOTE: The 3GPP AAA Server will assign a new Pseudonym Identity with a frequency dictated by operator's policy. The allocation of new pseudonyms is required to prevent that the user's movements are tracked by an unauthorized party.

If during an authentication request, the UE receives an EAP-Request/AKA-Identity message containing AT_PERMANENT_ID_REQ, the UE shall return the Permanent Identity in the AT_IDENTITY attribute of the EAP-Response/AKA_Identity. If the UE receives an EAP-Request/AKA'-Identity message containing AT_PERMANENT_ID_REQ, the UE shall return the Permanent Identity in the AT_IDENTITY attribute of the EAP-Response /AKA'-Identity message.

If during an authentication request, the UE receives an EAP-Request/AKA-Identity message which contains AT_FULLAUTH_ID_REQ, the UE shall return the Pseudonym Identity as the AT_IDENTITY within EAP-Response/AKA_Identity message if available. If the UE receives an EAP-Request/AKA'-Identity message containing AT_FULLAUTH_ID_REQ, the UE shall return the Pseudonym Identity as the AT_IDENTITY within the EAP-Response /AKA'-Identity message if available. Otherwise the UE shall return the Permanent Identity.

If during an authentication request, the UE receives an EAP-Request/AKA-Identity message or EAP-Request/AKA'-Identity message respectively, which contains AT_ANY_ID_REQ, the UE shall return the Fast Re-authentication Identity if available as the AT_IDENTITY. Otherwise the UE shall return the Pseudonym Identity.

6.4.2.4 Handling of the Access Network Identity

6.4.2.4.1 General

The 3GPP AAA server provides the UE with the ANID in EAP signalling. The UE can also obtain the ANID by access network specific means, which are out of scope of the present document. For some access networks the ANID can also be configured into the UE and the 3GPP AAA server.

NOTE: According to 3GPP TS 33.402 [15], the ANID is used by HSS and UE to generate transformed authentication vectors and therefore the ANID needs to be identical in the HSS and in the UE. The trusted non-3GPP access network first sends the ANID to the 3GPP AAA server via the STa reference point and the 3GPP AAA server sends the ANID to HSS via the SWx reference point, see 3GPP TS 29.273 [17], and to the UE as specified in this specification.

6.4.2.4.2 ANID indication from 3GPP AAA server to UE

When the 3GPP AAA server sends an EAP Request' or AKA-Challenge' message to the UE, the 3GPP AAA server shall include the ANID to be used when generating transformed authentication vectors, using the AT_KDF_INPUT attribute as described in subclause 8.2.2. The value and coding of this attribute is described in subclause 8.1.1.

6.4.2.4.3 UE check of ANID for HRPD CDMA 2000® access networks

The UE shall apply the rules for comparison of the locally determined ANID and the one received over EAP-AKA' as specified in IETF RFC 5448 [38]. The UE, or the user, may use the ANID as a basis for an optional decision whether

the access network is authorized to serve the UE. E.g. the UE may compare the ANID against a list of preferred or barred ANIDs.

When the UE can locally determine based on physical layer or access network procedures that the UE is connected to a eHRPD network, the locally determined ANID is "HRPD". If the comparison check is successful and if either the optional access network authorization decision in the UE is positive or is not performed, the UE shall proceed; otherwise the UE shall abort the access procedure.

6.4.2.4.4 UE check of ANID for WiMAX access networks

The UE shall apply the rules for comparison of the locally determined ANID and the one received over EAP-AKA' as specified in IETF RFC 5448 [38]. The UE, or the user, may use the ANID as a basis for an optional decision whether the access network is authorized to serve the UE. E.g. the UE may compare the ANID against a list of preferred or barred ANIDs.

When the UE can locally determine based on physical layer or access network procedures that the UE is connected to a WiMAX access network, the locally determined ANID is "WIMAX". If the comparison check is successful and if either the optional access network authorization decision in the UE is positive or is not performed, the UE shall proceed; otherwise the UE shall abort the access procedure.

6.4.2.4.5 UE check of ANID for WLAN access networks

The UE shall apply the rules for comparison of the locally determined ANID and the one received over EAP-AKA' as specified in IETF RFC 5448 [38]. The UE, or the user, may use the ANID as a basis for an optional decision whether the access network is authorized to serve the UE. E.g. the UE may compare the ANID against a list of preferred or barred ANIDs.

When the UE can locally determine based on physical layer or access network procedures that the UE is connected to a WLAN network, the locally determined ANID is "WLAN". If the comparison check is successful and if either the optional access network authorization decision in the UE is positive or is not performed, the UE shall proceed; otherwise the UE shall abort the access procedure.

6.4.2.4.6 UE check of ANID for ETHERNET access networks

The UE shall apply the rules for comparison of the locally determined ANID and the one received over EAP-AKA' as specified in IETF RFC 5448 [38]. The UE, or the user, may use the ANID as a basis for an optional decision whether the access network is authorized to serve the UE. E.g. the UE may compare the ANID against a list of preferred or barred ANIDs.

When the UE can locally determine based on physical layer or access network procedures that the UE is connected to a Ethernet network, the locally determined ANID is "ETHERNET". If the comparison check is successful and if either the optional access network authorization decision in the UE is positive or is not performed, the UE shall proceed; otherwise the UE shall abort the access procedure.

6.4.2.5 Full name for network and short name for network

When receiving the EAP-Request/AKA-Challenge message when the EAP-AKA is used or the EAP-Request/AKA'-Challenge message when the EAP-AKA' is used, and the AT_FULL_NAME_FOR_NETWORK attribute, the AT_SHORT_NAME_FOR_NETWORK attribute or both are included, then the UE may use the contents to update appropriate information stored within the UE.

6.4.2.6 TWAN connection modes

6.4.2.6.1 General

Editor's note (WI:eSaMOG_St3, CR#0248): it is FFS whether the UE is mandated to support SCM, MCM or both or whether both SCM and MCM are optional.

Editor's note (WI:eSaMOG_St3, CR#0248): it is FFS whether usage of SCM and MCM is subject to UE subscription for SCM and MCM.

NOTE: No UE extensions are needed for TSCM.

6.4.2.6.2 Usage of single-connection mode (SCM)

If the UE supports the SCM, if the EAP-Request/AKA'-Challenge message includes the AT_TWAN_CONN_MODE attribute as described in subclause 8.2.7.1 wherein the message field as described in subclause 8.1.4.1:

- contains the message type field indicating CONNECTION_CAPABILITY; and
- contains the item list field including the CONNECTION_MODE_CAPABILITY item as described in subclause 8.1.4.8 indicating support of SCM;

and if the UE requests usage of the SCM, then the UE:

a) shall include the AT_TWAN_CONN_MODE attribute according to subclause 8.2.7.1 in the EAP-Response/AKA'-Challenge message. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the UE shall:

   1) set the message type field to SCM_REQUEST; and

   2) in the item list field:

      A) include a CONNECTIVITY_TYPE item according to subclause 8.1.4.3 indicating the requested connectivity type(s) - PDN connection, NSWO, or both; and

      B) if a PDN connection is requested:

         i) include a ATTACHMENT_TYPE item according to subclause 8.1.4.4 indicating whether an initial attach or a handover attach is requested;

         ii) if a PDN connection for an APN other than the default APN is requested, include an APN item according to subclause 8.1.4.5 indicating the requested APN;

         iii) if initial attach is requested, include a PDN_TYPE item according to subclause 8.1.4.6 indicating the requested PDN type;

         iv) if handover attach is requested, include a PDN_TYPE item according to subclause 8.1.4.6 indicating the PDN type supported in the PDN connection to be handed over; and

         v) if the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network, include a PROTOCOL_CONFIGURATION_OPTIONS item according to subclause 8.1.4.9; and

b) if a PDN connection is requested, shall include the AT_RESULT_IND attribute in the EAP-Response/AKA'-Challenge message.

NOTE: If the UE does not include the AT_RESULT_IND attribute in the EAP-Response/AKA'-Challenge message, in case of successful authentication, then EAP-Request/AKA'-Notification message is not received and the UE is only informed about success using EAP-Success.

Upon receiving the EAP-Request/AKA'-Notification message including the AT_TWAN_CONN_MODE attribute as described in subclause 8.2.7.1 wherein the message field as described in subclause 8.1.4.1:

- contains the message type field indicating SCM_RESPONSE; and
- contains the item list field;

the UE:

a) if the AT_NOTIFICATION attribute indicates success, then determines the authorized connectivity type in the CONNECTIVITY_TYPE item as described in subclause 8.1.4.3 included in the item list field. If the authorized connectivity type is PDN connection, the UE:

   1) determines the selected APN in the APN item as described in subclause 8.1.4.5 included in the item list field;

2) determines the PDN type supported in the PDN connection in the PDN_TYPE item as described in subclause 8.1.4.6 included in the item list field; and

3) if a PROTOCOL_CONFIGURATION_OPTIONS item as described in subclause 8.1.4.9 is included in the item list field, determines the protocol configuration options in the PROTOCOL_CONFIGURATION_OPTIONS item; and

b) if the AT_NOTIFICATION attribute indicates failure, then determines the cause of failure in the CAUSE item as described in subclause 8.1.4.10 included the item list field.

6.4.2.6.3 Usage of multi-connection mode (MCM)

If the UE supports the MCM, if the EAP-Request/AKA'-Challenge message includes the AT_TWAN_CONN_MODE attribute as described in subclause 8.2.7.1 wherein the message field as described in subclause 8.1.4.1:

- contains the message type field indicating CONNECTION_CAPABILITY; and
- contains the item list field including the CONNECTION_MODE_CAPABILITY item as described in subclause 8.1.4.8 indicating support of MCM;

and if the UE requests usage of the MCM, then the UE:

a) shall include the AT_TWAN_CONN_MODE attribute according to subclause 8.2.7.1 in the EAP-Response/AKA'-Challenge message. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the UE shall set the message type field to MCM_REQUEST; and

b) unless the UE refrains from usage of NSWO, shall include the AT_RESULT_IND attribute in the EAP-Response/AKA'-Challenge message.

NOTE: If the UE does not include the AT_RESULT_IND attribute in the EAP-Response/AKA'-Challenge message, in case of successful authentication, then EAP-Request/AKA'-Notification message is not received and the UE is only informed about success using EAP-Success.

Upon receiving the EAP-Request/AKA'-Notification message including the AT_TWAN_CONN_MODE attribute as described in subclause 8.2.7.1 where the message field as described in subclause 8.1.4.1:

- contains the message type field indicating MCM_RESPONSE; and
- contains the item list field;

the UE:

a) if the AT_NOTIFICATION attribute indicates success, then determines the NSWO authorization in the AUTHORIZATIONS item as described in subclause 8.1.4.7 included in the item list field; and

b) if the AT_NOTIFICATION attribute indicates failure, then determines the cause of failure in the CAUSE item as described in subclause 8.1.4.10 included in the item list field.

6.4.3 3GPP AAA server procedures

6.4.3.1 Identity Management

The 3GPP AAA selects the pseudonym identity or the Fast Re-authentication Identity and returns the identity to the UE during the Authentication procedure as specified in 3GPP TS 33.402 [15]. The 3GPP AAA server shall maintain a mapping between the UE's permanent identity and the pseudonym identity and between the UE's permanent identity and the Fast Re-authentication Identity.

6.4.3.2 EAP-AKA and EAP-AKA' based Authentication

The 3GPP AAA server shall support EAP AKA based authentication as specified in IETF RFC 4187 [33] and EAP-AKA' based authentication as specified in IETF RFC 5448 [38]. 3GPP TS 33.402 [15] specifies the conditions under which one or the other of these two methods is used. If the UE provides an explicit indication for the supported mobility

protocols and the network supports multiple IP mobility mechanisms, the network shall select the protocol to be used and communicate the decision to the UE as defined in subclause 6.3.3.1.2.

6.4.3.3 Full authentication and Fast Re-authentication

The 3GPP AAA shall support full re-authentication and fast re-authentication as specified in IETF RFC 4187 [33].

The decision to use the fast re-authentication process is taken by the home network (i.e. the 3GPP AAA server) and is based on operator policies. If fast re-authentication is to be used, the home network shall indicate this to the UE by providing the Fast Re-authentication Identity to the UE during the authentication process.

When initiating an authentication, the home network shall indicate the type of authentication required by including either AT_PERMANENT_ID_REQ or AT_FULLAUTH_ID_REQ for Full authentication and AT_ANY_ID_REQ for Fast re-authentication in the EAP-Request/AKA_Identity message or the EAP-Request/AKA'-Identity message respectively.

The home network (i.e. the 3GPP AAA server) may upon receiving the Fast Re-authentication Identity in AT_IDENTITY, decide to proceed with the fast re-authentication or choose instead to initiate a full authentication. This decision is based on operator policies.

6.4.3.4 Full name for network and short name for network

The 3GPP AAA server may include the AT_FULL_NAME_FOR_NETWORK attribute, the AT_SHORT_NAME_FOR_NETWORK attribute or both in the EAP-Request/AKA-Challenge message when the EAP-AKA is used and in the EAP-Request/AKA'-Challenge message when the EAP-AKA' is used.

The detailed coding of the AT_FULL_NAME_FOR_NETWORK attribute and the AT_SHORT_NAME_FOR_NETWORK is described in subclause 8.2.5.

6.4.3.5 TWAN connection modes

6.4.3.5.1 General

The 3GPP AAA server may support the single-connection mode (SCM).

The 3GPP AAA server may support the multi-connection mode (MCM).

If the network supports SCM, MCM or both, the 3GPP AAA server shall include the AT_TWAN_CONN_MODE attribute according to subclause 8.2.7.1 and the AT_RESULT_IND attribute in the EAP-Request/AKA'-Challenge message. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the 3GPP AAA server shall:

a) set the message type field to CONNECTION_CAPABILITY; and

b) in the item list field, include a CONNECTION_MODE_CAPABILITY item according to subclause 8.1.4.8 indicating whether the network supports TSCM, SCM, MCM or any combination of them.

6.4.3.5.2 Usage of single-connection mode (SCM)

If

- the 3GPP AAA server supports SCM;

- the EAP-Response/AKA'-Challenge message includes the AT_TWAN_CONN_MODE attribute as described in subclause 8.2.7.1 wherein the message field as described in subclause 8.1.4.1 contains the message type field indicating SCM_REQUEST; and

- the authentication was successful;

then the 3GPP AAA server triggers the TWAN to establish the connectivity of one of the requested connectivity type(s) according to 3GPP TS 23.402 [6].

If the 3GPP AAA authorizes the requested connectivity, and if the EAP-Response/AKA'-Challenge message includes the AT_RESULT_IND attribute, then the 3GPP AAA server shall invoke an EAP-Request/AKA'-Notification dialogue. The 3GPP AAA server shall construct the EAP-Request/AKA'-Notification message as follows:

a) indicate success in the AT_NOTIFICATION attribute; and

b) include the AT_TWAN_CONN_MODE attribute described in subclause 8.2.7.1. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the 3GPP AAA server shall:

   1) set the message type field to SCM_RESPONSE; and

   2) in the item list field:

      A) include a CONNECTIVITY_TYPE item as described in subclause 8.1.4.3 indicating the authorized connectivity type. Only one connectivity type is indicated; and

      B) if a PDN connection was authorized:

         i) include an APN item according to subclause 8.1.4.5 indicating the APN of the authorized PDN connection;

         ii) include a PDN_TYPE item according to subclause 8.1.4.6 indicating the PDN type(s) selected in the authorized PDN connection; and

         iii) if the 3GPP AAA server wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE, include a PROTOCOL_CONFIGURATION_OPTIONS item according to subclause 8.1.4.9.

If the 3GPP AAA does not authorize the requested connectivity, then the 3GPP AAA server shall invoke an EAP-Request/AKA'-Notification dialogue. The 3GPP AAA server shall construct the EAP-Request/AKA'-Notification message as follows:

a) indicate failure in the AT_NOTIFICATION attribute; and

b) include the AT_TWAN_CONN_MODE attribute described in subclause 8.2.7.1. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the 3GPP AAA server shall:

   1) set the message type field to SCM_RESPONSE; and

   2) in the item list field, include a CAUSE item according to subclause 8.1.4.10 indicating the cause of failure.

6.4.3.5.3 Usage of multi-connection mode (MCM)

If:

a) the 3GPP AAA server supports MCM;

b) if the EAP-Response/AKA'-Challenge message includes:

   1) the AT_TWAN_CONN_MODE attribute as described in subclause 8.2.7.1 wherein the message field as described in subclause 8.1.4.1 contains the message type field indicating MCM_REQUEST; and

   2) the AT_RESULT_IND attribute;

c) the 3GPP AAA authorizes the request; and

d) the authentication was successful;

then the 3GPP AAA server shall invoke an EAP-Request/AKA'-Notification dialogue. The 3GPP AAA server shall construct the EAP-Request/AKA'-Notification message as follows:

a) indicate success in the AT_NOTIFICATION attribute; and

b) include the AT_TWAN_CONN_MODE attribute according to subclause 8.2.7.1. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the 3GPP AAA server shall:

1) set the message type field to MCM_RESPONSE; and

2) in the item list field, include an AUTHORIZATIONS item according to subclause 8.1.4.7 indicating whether UE is authorized to use NSWO.

If the 3GPP AAA does not authorize the request, then the 3GPP AAA server shall invoke an EAP-Request/AKA'-Notification dialogue. The 3GPP AAA server shall construct the EAP-Request/AKA'-Notification message as follows:

a) indicate failure in the AT_NOTIFICATION attribute; and

b) include the AT_TWAN_CONN_MODE attribute described in subclause 8.2.7.1. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the 3GPP AAA server shall:

1) set the message type field to MCM_RESPONSE; and

2) in the item list field, include a CAUSE item according to subclause 8.1.4.10 indicating the cause of failure.

6.4.4 Multiple PDN support for trusted non-3GPP access

Connectivity to multiple PDNs via trusted non-3GPP access is supported in the EPS when the network policies, the non-3GPP access and the user subscription allow it.

NOTE 1: In 3GPP, there is a limitation to the maximum number of simultaneous PDN connections per UE which is 11 (caused by the EPS bearer identity, see 3GPP TS 24.007 [48]). Not complying with this limitation when accessing non-3GPP access can lead to unexpected consequences, e.g. connectivity loss in case of handover to 3GPP access.

If the UE supports dynamic mobility management selection the UE shall use the same mobility protocol when multiple connections are established, see 3GPP TS 23.402 [6].

When using the S2a interface to establish connections to additional PDNs the UE shall send a trigger for additional PDN connectivity specific to the non-3GPP access. The UE shall include an APN in this trigger to connect to the desired PDN. The UE shall also indicate the Attach Type to the trusted non-3GPP access during additional PDN connectivity. The Attach Type shall distinguish between Initial Attach and Handover Attach. For the multi-connection mode used via trusted WLAN access network, the PDN connection establishment procedures are specified in 3GPP TS 24.244 [56].

NOTE 2: The indication about Attach Type is non-3GPP access network specific and its coding is out of scope of this specification.

NOTE 3: The trigger for additional PDN connectivity is non-3GPP access network specific and its coding is out of scope of this specification.

When using the S2c interface, the UE shall follow the procedures described in 3GPP TS 24.303 [11] to connect to multiple PDNs.

If the UE is handing over from a source access network to a target non-3GPP access using S2a and the UE has more than one PDN connection to a given APN in the source access network, the UE shall transfer all the PDN connections for the given APN to the target trusted non-3GPP access network as specified in 3GPP TS 23.402 [6].

If multiple PDN connections to a single APN are not supported over the target trusted non-3GPP access network, only one PDN connection to the given APN shall be established in the target non-3GPP access as specified in 3GPP TS 23.402 [6]. If multiple PDN connection requests to the same APN are received but the target trusted non-3GPP access network does not support multiple PDN connections to the same APN, the network shall reject the additional PDN connection requests to the same APN received from the UE when one PDN connection to the same APN has already been established. The UE shall determine which PDN connection is re-established in the non-3GPP access based on the home address information (i.e. IPv4 address or IPv6 prefix or both) provided by the network.

NOTE 4: The protocol details of the PDN connection reject procedure is non-3GPP access network specific and its coding is outside the scope of this specification. For the multi-connection mode used via trusted WLAN access network, the protocol details of the PDN connection reject procedure is specified in 3GPP TS 24.244 [56]

NOTE 5: When UE supporting IP address preservation for NBM with multiple PDN connections to the same APN hands over to the non-3GPP access network, the UE can, as an implementation option, prioritise the re-establishment for a particular PDN connection before re-establishing the remaining PDN connections. The way a UE prioritizes a particular PDN connection is non-3GPP access network specific and its coding is out of scope of this specification. Another implementation option can be to send multiple re-establishment requests concurrently.

NOTE 6: Any unsuccessful re-establishment of any of the multiple PDN connections to the same APN can be managed in an implementation specific manner avoiding UE making repeated re-establishment attempts to the network.

If the UE did not handover all the PDN connections for a given APN to the target trusted non-3GPP access network, the network may disconnect the remaining PDN connections for that given APN after an implementation dependent time.

6.5 Authentication and authorization for accessing EPC via an untrusted non-3GPP access network

6.5.1 General

In order to attach to the evolved packet core network (EPC) via untrusted non-3GPP IP access, the UE first needs to be configured with a local IP address from the untrusted non-3GPP access network.

During the attach to the untrusted non-3GPP access, the operator of the non-3GPP access network may optionally require to perform a 3GPP based access authentication as specified in 3GPP TS 33.402 [15].

Once the UE is configured with a local IP address, the UE shall select the Evolved Packet Data Gateway (ePDG) as described in subclause 7.2.1 and shall initiate the IPsec tunnel establishment procedure as described in subclause 7.2.2. During these steps authentication and authorization for access to EPC shall be performed.

6.5.2 Full authentication and authorization

6.5.2.1 General

During the establishment of the IPSec tunnel between the UE and the ePDG, 3GPP based authentication signalling for untrusted non-3GPP access to the EPC shall be exchanged between the UE and the 3GPP AAA server in the EPC to ensure mutual authentication of the user and the EPC.

Authorization of EPC access shall be performed by the 3GPP AAA server upon successful user authentication.

The access authentication signalling between the UE and the 3GPP AAA server shall be based on EAP-AKA as specified in IETF RFC 4187 [33] and is further detailed in 3GPP TS 33.402 [15], 3GPP TS 29.273 [17] and procedural descriptions in subclauses 7.2.2 and 7.4.4.

6.5.2.2 UE procedures

When accessing the EPC via the ePDG, the UE shall exchange EAP-AKA signalling with the 3GPP AAA server as specified in 3GPP TS 33.402 [15].

NOTE: the EAP payload exchanged between UE and 3GPP AAA server is transported within the IKEv2 messages exchanged with ePDG as described in subclause 7.2.2.

6.5.2.3 3GPP AAA server procedures

During the authentication of the UE for accessing the EPC via the ePDG, the 3GPP AAA server shall initiate EAP-AKA based authentication with the UE as specified in 3GPP TS 33.402 [15].

6.5.3 Multiple PDN support for untrusted non-3GPP access network

Connectivity to multiple PDNs via untrusted non-3GPP access is supported in the EPS when the network policies, the non-3GPP access and the user subscription allow it.

NOTE 1: In 3GPP, there is a limitation to the maximum number of simultaneous PDN connections per UE which is 11 (caused by the EPS bearer identity, see 3GPP TS 24.007 [49]). Not complying with this limitation when accessing non-3GPP access can lead to unexpected consequences, e.g. connectivity loss in case of handover to 3GPP access.

If the UE supports dynamic mobility management selection the UE shall use the same mobility protocol when multiple connections are established, see 3GPP TS 23.402 [6].

When using the S2b interface to establish additional PDN connections, the UE shall establish an IPSec tunnel with the same ePDG for each PDN connection. For each tunnel establishment procedure, the UE shall indicate to the ePDG an APN to the desired PDN and an attach type indication as specified in subclause 7.2.2.

When using the S2c interface, the UE shall follow the procedures described in 3GPP TS 24.303 [11] when establishing multiple PDN connections. For multiple PDN connections over the S2c interface, the UE shall establish only one IPsec tunnel to the ePDG.

If the UE had more than one PDN connection to a given APN in the source access network and the UE is performing a handover to a target untrusted non-3GPP access network via an ePDG that supports the S2b interface, the UE shall transfer all the PDN connections for the given APN to the target untrusted non-3GPP access network as specified in 3GPP TS 23.402 [6].

If multiple PDN connections to a single APN are not supported over the target untrusted non-3GPP access network, only one PDN connection to that given APN shall be established in the target non-3GPP access network as specified in 3GPP TS 23.402 [6] if NBM is used. The UE, if supporting IP address preservation for NBM, shall include the home address information during the tunnel establishment procedure as specified in subclause 7.2.2. If multiple PDN connection requests to the same APN are received but the network does not support multiple PDN connections to the same APN, the ePDG shall reject the additional PDN connection requests to the same APN received from the UE as described in subclause 7.4.1, in the following circumstances:

- when one PDN connection to the same APN has already been established;
- only after the network has successfully established one PDN connection in the case that the additional PDN connections requests were received prior to the successful establishment of a single PDN connection.

In the above cases, the UE shall determine which PDN connection is re-established in the non-3GPP access based on the home address information provided by the network.

The UE behaviour, when PDN connection re-establishment is rejected by the network during handover to the untrusted non-3GPP access network, is described in sublause 7.2.2.

NOTE 2: When a UE supporting IP address preservation for NBM with multiple PDN connections to the same APN hands over to the non-3GPP access network, the UE can, as an implementation option, prioritise the re-establisment for a particular PDN connection before re-establishing the remaining PDN connections. The UE indicates the prioritised PDN connection by including both the APN in the IDr payload and the home address information in the Handover Attach indicator as specified in subclause 7.2.2. Another implementation option can be to send multiple re-establishment requests concurrently.

If the UE did not handover all the PDN connections for a given APN to the target untrusted non-3GPP access network, the source network may disconnect the remaining PDN connections for that given APN after an implementation dependent time.

6.6 UE - 3GPP EPC (cdma2000® HRPD Access)

6.6.1 General

3GPP2 X.S0057 [20] defines the interworking architecture for access to the EPC via cdma2000® HRPD access networks. In particular, 3GPP2 X.S0057 [20] describes support for a UE using the cdma2000® HRPD air interface to access the EPC architecture defined in 3GPP TS 23.402 [6] by:

- specifying the use of the interface across the S2a reference point between the 3GPP2 HRPD Serving Gateway (HSGW) and the PDN Gateway (P-GW) in the EPC by referencing 3GPP TS 29.275 [18];
- specifying the use of the interface across the S101 reference point between the eAN/PCF in the 3GPP2 HRPD access network and the MME in the EPC by referencing 3GPP TS 29.276 [19];
- specifying the use of the user plane interface across the S103 reference point between the EPC Serving Gateway (S-GW) and the HSGW by referencing 3GPP TS 29.276 [19]; and
- describing the internal functions and responsibilities of the HSGW.

3GPP2 C.S0087 [21] defines the signalling requirements and procedures for UEs accessing the EPC via 3GPP2 HRPD access networks using the cdma2000® HRPD air interface. In particular, 3GPP2 C.S0087 [21]:

- defines the signalling extensions to the cdma2000® HRPD air interface defined in 3GPP2 C.S0024 [23] necessary to support interworking with the EPC and E-UTRAN; and
- defines the UE and eAN/PCF procedures and signalling formats to support bidirectional handoff between E-UTRAN and cdma2000® HRPD.

6.6.2 Non-emergency case

6.6.2.1 General

Subclauses 6.6.2.2 through 6.6.2.7 describe the particular requirements for access to the EPC via a cdma2000® HRPD access network in support of non-emergency accesses and services.

6.6.2.2 UE identities

The UE and network shall use the root NAI as specified in 3GPP TS 23.003 [3] for EPC access authentication when the UE obtains service via a cdma2000® HRPD access network connected to an EPC in the UE's HPLMN.

Additionally, the UE and network shall use the Fast-Reauthentication NAI and the Pseudonym Identity as described in subclause 4.4.

6.6.2.3 cdma2000® HRPD access network identity

The access network identity is described in 3GPP TS 23.003 [3] and in subclause 6.4.2.4 of this specification. For a cdma2000® HRPD network, the value and encoding of the access network identity is described in subclause 8.1.1. The 3GPP AAA server, HSS, and any visited network AAA proxy shall use the access network identity during EAP-AKA' authentication procedures (see 3GPP TS 33.402 [15]).

6.6.2.4 PLMN system selection

The UE shall rely on information provisioned by the home operator to facilitate the PLMN system selection process described in 3GPP TS 23.122 [4].

6.6.2.5 Trusted and untrusted accesses

The UE shall determine the trust relationship for access to the EPC via a cdma2000® HRPD access network as described in subclause 4.1.

6.6.2.6 IP mobility mode selection

The UE and network shall perform IP mobility mode selection as described in subclauses 6.3.3.1 and 6.4.3.2

6.6.2.7 Authentication and authorization for accessing EPC

The UE and 3GPP AAA server shall perform authentication and authorization procedures for access to the EPC as defined in 3GPP TS 33.402 [15].

6.6.3 Emergency case

6.6.3.1 General

Subclauses 6.6.3.2 through 6.6.3.3 describe the particular requirements for access to the EPC via a cdma2000® HRPD access network in support of an emergency session in course of handover from E-UTRAN to HRPD.

In this release of the specification no emergency session related handling other than the handover of an emergency session from E-UTRAN to an S2a based cdma2000® HRPD access network is specified.

6.6.3.2 UE identities

When the UE obtains emergency services via a cdma2000® HRPD access network connected to an EPC in the UE's HPLMN, then the UE and the network shall use the NAI for EPC access authentication as follows:

- if IMSI is available and authenticated , then the UE and the network shall use the root NAI as specified in 3GPP TS 23.003 [3];
- if IMSI is not available or unauthenticated, then the emergency NAI as specified in 3GPP TS 23.003 [3] shall be used.

Additionally, the UE and the network shall use the Fast-Reauthentication NAI and the Pseudonym Identity as described in subclause 4.4.1.

6.6.3.3 Authentication and authorization for accessing EPC

If IMSI is available, then the authentication and authorization procedures via STa are executed if the local regulation and network operator option requires authenticating the UE.

If the authentication and authorization procedures fail, then it depends on local regulation and network operator option to allow or reject the emergency services for the UE.

If IMSI is not available, the authentication and authorization procedures via STa are not executed.

6.7 UE - 3GPP EPC (WiMAX Access)

6.7.1 General

The WiMAX system and its access network subsystem are described within WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 2 [24]. The protocol architecture and signalling of the WiMAX system is specified in WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25]. This protocol architecture and signalling supports the air interface defined in WiMAX Forum Mobile System Profile Release 1.0 Approved Specification Revision 1.4.0 [26] which specifies selected profiles of IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005 [27].

6.7.2 Non-emergency case

6.7.2.1 General

Subclauses 6.7.2.2 through 6.7.2.7 describe the particular requirements for access to the EPC via a WiMAX access network in support of non-emergency accesses and services.

6.7.2.2 UE identities

The UE and network shall use the root NAI as specified in 3GPP TS 23.003 [3] for EPC access authentication when the UE obtains service via a WiMAX access network connected to an EPC in the UE's HPLMN.

Additionally, the UE and network shall use the Fast-Reauthentication NAI and the Pseudonym Identity as described in subclause 4.4.

6.7.2.3 WiMAX access network identity

The access network identity is described in 3GPP TS 23.003 [3] and in subclause 6.4.2.4 of this specification. For a WiMAX network, the value and encoding of the access network identity is described in subclause 8.1.1. The 3GPP AAA server, HSS, and any visited network AAA proxy shall use the access network identity during EAP-AKA authentication procedures (see 3GPP TS 33.402 [15]).

6.7.2.4 Selection of the Network Service Provider

The UE shall use WIMAX-specific procedures described in WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] to discover and select the highest priority Network Service Provider (NSP) which is available and allowable.

6.7.2.5 Trusted and untrusted accesses

The UE shall determine the trust relationship for access to the EPC via a WiMAX access network as described in subclause 4.1.

6.7.2.6 IP mobility mode selection

The UE and network shall perform IP mobility mode selection as described in subclauses 6.3.3.1 and 6.4.3.2.

6.7.2.7 Authentication and authorization for accessing EPC

NOTE: In line with 3GPP TS 33.402 [15], in this present specification, no particular security provisions are specified for interworking between WiMAX and EPS. Any access specific security procedures for WiMAX as a non-3GPP access network to EPC will be in accordance with WiMAX Forum Network Architecture Release 1.0 version 1.2 – Stage 3 [25] and WiMAX Forum Mobile System Profile Release 1.0 Approved Specification Revision 1.4.0 [26].

6.7.3 Emergency case

NOTE: Procedures for handling emergency accesses or services are not specificed within this release of the specification

6.8 Communication over the S14

6.8.1 General

In order to assist the UE with performing access network discovery and selection, ANDSF provides a set of information to the UE. This information contains:

- the access network discovery and selection information to assist the UE with selecting the access network;
- ISMP to control and assist the UE with performing the inter-system change or both;
- ISRP information to control and assist a UE with selecting the access network to be used for routing different IP flows over different access networks, establishing PDN connections and identifying IP flows applicable for non-seamless WLAN offload; or
- IARP information to control and assist a UE with selecting a prioritised APN which is associated with an existing PDN connection for routing different IP flows. The IARP provided by ANDSF can also include information for identifying IP flows applicable for non-seamless offload to WLAN.

The ANDSF can provide ISRP and IARP to a UE independently of the UE's support for IFOM, MAPCON, NSWO or Inter-APN routing. A UE that does not support any of: IFOM, MAPCON, NSWO and Inter-APN routing, shall not apply the ISRP received from the ANDSF.

This set of information can either be provisioned in the UE by the home operator, or provided to the UE by the ANDSF over the S14 reference point via pull or push mechanisms as defined in 3GPP TS 23.402 [6] by means of the access network discovery and selection procedures as described in subclause 6.8.2. While roaming, the UE can receive a set of information from H-ANDSF or V-ANDSF or both. The V-ANDSF shall not provide any IARP to a roaming UE. If the roaming UE receives any IARP delivered by a V-ANDSF then the roaming UE shall ignore it.

The UE, located in the home PLMN, needs to discover the H-ANDSF by means of the discovery procedure as described in subclause 6.8.2.2.1. The UE, located in the visited PLMN, needs to discover the H-ANDSF or V-ANDSF or both by means of the discovery procedure as described in subclause 6.8.2.2.1.

Through push mechanisms the ANDSF can provide assistance information to the UE e.g. if the UE has previously used pull based ANDSF procedure or if OMA-DM bootstrapping is used as described in subclause 6.8.2.2.1A. Through pull mechanisms the UE can send a request to the ANDSF in order to get assistance information for access network discovery and selection.

ANDSF shall comply with local, national and regional requirements regarding the privacy and confidentiality of location information.

NOTE: The regulation and legislations of the home operator of the ANDSF server determines whether the ANDSF server can store the user's location information.

6.8.2 Interaction with the Access Network Discovery and Selection Function

6.8.2.1 General

The S14 interface enables IP level communication between the UE and ANDSF. The protocols supported by the S14 interface are realized above the IP level. Both pull and push mechanisms may be supported for communication between the UE and the ANDSF. A combination of pull and push mechanisms may also be supported. The communication security over the S14 interface is specified in 3GPP TS 33.402 [15].

The UE, located in a home PLMN, can communicate securely with the H-ANDSF. The UE, located in a visited PLMN, can communicate securely with H-ANDSF or V-ANDSF or both.

The information is transferred between the UE and ANDSF using OMA DM as defined in OMA-ERELD-DM-V1_2 [39] with the management object as specified in 3GPP TS 24.312 [13].

6.8.2.2 UE procedures

6.8.2.2.1 UE discovering the ANDSF

The IP address of the H-ANDSF can be configured in the UE by the home operator.

When the UE is in its HPLMN or equivalent HPLMN, the UE may use DNS lookup as specified in IETF RFC 1035 [35] or DHCP query as specified in IETF RFC 6153 [37] to discover the IP address of the H-ANDSF.

If the UE implements DHCP query, the preference between DNS lookup and DHCP query is UE implementation dependent. .

When the UE is in a visited PLMN, the UE shall use DNS lookup to discover the IP address of the ANDSF.

When performing a DNS lookup resolution for ANDSF, the UE shall apply the following procedures:

- For the H-ANDSF discovery, the UE shall build a Fully Qualified Domain Name (FQDN) that shall be set to the ANFSF-SN FQDN as defined in 3GPP TS 23.003 [3] for the DNS request and select the IP address of the H-ANDSF included in the DNS response message.
- For the V-ANDSF discovery, the V-ANDSF IP address by which the UE can contact the V-ANDSF is obtained by the UE through a DNS lookup by name as specified in IETF RFC 1035 [35]. The QNAME shall be set to the ANDSF-SN FQDN and included in the DNS Request as defined in 3GPP TS 23.003 [3], and select the IP address of the V-ANDSF included in the DNS response message.

6.8.2.2.1A ANDSF communication security

According to 3GPP TS 33.402 [15], for the pull model, the UE and ANDSF shall use PSK TLS with GBA based shared key-based mutual authentication to establish a secure connection between UE and ANDSF as specified by subclause 5.4 of 3GPP TS 33.222 [44].

According to 3GPP TS 33.402 [15], for the push model, the UE and ANDSF shall use PSK TLS with GBA push based shared key-based mutual authentication to establish a secure connection between the UE and the ANDSF as specified by subclause 5.1 of 3GPP TS 33.223 [47].

In accordance with 3GPP TS 29.109 [43], the BSF shall provide either the UE's IMSI or IMPI to NAF, ie the ANDSF server.

OMA-DM's application level authentication mechanism does not need to be used with ANDSF, since mutual security association is already established on transport level using PSK-TLS as specified in 3GPP TS 33.402 [15]. According to OMA-ERELD-DM-V1_2 [39], however, each Managed Object (MO) shall have an access control list (ACL) that lists authorized OMA DM servers. In order to comply with OMA-ERELD-DM-V1_2 [39], the ANDSF-SN FQDN shall be used as server name in the ACL list.

If the UE does not support the ANDSF security mechanism as specified in 3GPP TS 33.402 [15], or if the operator does not implement the GAA bootstrap framework specified in 3GPP TS 33.220 [42], appropriate communication security can be established with the ANDSF using OMA-DM's bootstrap, secure http (https) mechanism and WAP Push according to OMA-ERELD-DM-V1_2 [39].

6.8.2.2.2 Role of UE for Push model

The UE shall implement the push model of ANDSF in accordance with OMA-ERELD-DM-V1_2 [39] using WAP Push, which is applicable for 3GPP access networks only.

If the UE operates according to the GAA bootstrap framework specified in 3GPP TS 33.220 [42] and if the UE supports GBA Push as specified in 3GPP TS 33.223 [47], the UE shall accept the SMS as a valid ANDSF notification SMS if:

- the notification SMS contains valid GBA Push Information (GPI) as specified in 3GPP TS 24.109 [52],
- the X-WAP-Application-ID field (Push Application ID) in the WSP header indicates ANDSF,
- the WSP payload contains only the header part defined in 3GPP TS 24.109 [52] and the GPI parameter without any additional identifiers and
- the NAF FQDN in GPI conforms to the ANDSF-SN specified in 3GPP TS 23.003 [3].

The short code for the X-WAP-Application-ID is specified in subclause 8.1.3.

If the UE operates according to OMA DM bootstrap procedures as specified in OMA DM Enabler Release v.1.2, see OMA-ERELD-DM v1_2 [39], the UE shall accept the SMS as a valid ANDSF notification SMS if it contains an OMA DM General Package #0 message according to OMA-ERELD-DM v1_2 [39].

In the push model of communication, if the UE receives a valid ANDSF notification SMS from the ANDSF, the UE shall establish a secure data connection using the information received in the notification SMS.

If the UE receives an invalid ANDSF notification SMS it shall be ignored by the UE.

Upon establishing a secure connection between the UE and ANDSF, the UE may be provided with updated ISMP, information about available access networks, IARP and ISRP. The list of the information is described in subclause 6.8.1 and 6.8.2.3.3 and the correspondent ANDSF MO is defined in 3GPP TS 24.312 [13].

In addition, the ANDSF may provide a list of Inter-APN Routing Policies to a UE for routing IP traffic.

6.8.2.2.3 Role of UE for Pull model

In the pull model of communication, the UE sends a query to ANDSF to retrieve or update inter-system mobility policy or information about available access networks in its vicinity or inter-APN routing policy or any combination of them. A UE supporting IFOM, MAPCON, NSWO or any combination of these may also request ISRP. A UE may request IARP. The UE will wait for an implementation dependent time for an answer from the ANDSF. If ANDSF does not respond within that time, further action by the UE is implementation dependent. The UE may provide to ANDSF the UE's location information including, if available, the location parameters (for example, cell identities or the MAC address of the WLAN AP) associated with the Radio Access Networks the UE has discovered in its current location at the time the UE sends a query to ANDSF; the format of the location information is described as UE_Location in ANDSF MO defined in 3GPP TS 24.312 [13].

After communicating with ANDSF, the UE may be provided with updated inter-system policy, ISRP and IARP, and information about available access networks. The list of the information is described in subclause 6.8.1 and 6.8.2.3.3 and the correspondent ANDSF MO is defined in 3GPP TS 24.312 [13].

The UE may start Pull model communication with ANDSF based upon the information previously received from the ANDSF (e.g. based on the value of UpdatePolicy leaf defined in 3GPP TS 24.312 [13]). The UE capable of IFOM, MAPCON, or non-seamless WLAN offload (or any combination of these capabilities) can have all these capabilities disabled and have no ISRP. If the UE enables one (or more) of these capabilities, the UE may start Pull model communication with ANDSF. The UE capable of IFOM, MAPCON, or non-seamless WLAN offload (or any combination of these capabilities) can have one (or more) ofthese capabilities enabled and have no ISMP. If the UE disables all these capabilities, the UE may start Pull model communication with ANDSF. If the UE has no IARP, the UE may start Pull model communication with ANDSF.

NOTE: Mechanisms to limit the frequency of queries transmission from the UE to the ANDSF are implementation dependant.

In addition, the ANDSF may provide a list of Inter-APN Routing Policies to a UE for routing IP traffic.

6.8.2.2.4 UE using information provided by ANDSF

6.8.2.2.4.1 General

Network detection and selection shall take into account the access network specific requirements and the UE's local policy, e.g. user preference settings, access history, etc, along with the information provided by the ANDSF when selecting an access network. The local policy and the information provided by the ANDSF shall be used by the UE in an implementation dependent way to limit the undesired alternating between access systems, e.g. ping-pong type of inter-system changes. However, the use of such information from the ANDSF shall not be in contradiction to functions specified in 3GPP TS 23.122 [4], 3GPP TS 24.234 [9], 3GPP TS 25.304 [14] and 3GPP TS 36.304 [16].

If the UE is roaming in a VPLMN, the UE may receive Inter-system mobility policies or Access network discovery information or ISRP or combinations of these from H-ANDSF or V-ANDSF or both. The UE may also receive the IARP from H-ANDSF. If IARP is received from V-ANDSF, the UE shall ignore it. The formats of the Inter-system mobility policies, Access network discovery information, IARP and ISRP are defined in 3GPP TS 24.312 [13].

The maximum number of sets of Inter-system mobility polices or Access network discovery information or ISRP or IARP or combinations of these that the UE may keep is implementation dependent. However, the UE shall retain at least one set of Inter-system mobility policies and one set of Access network discovery information from the same ANDSF. In addition, a UE supporting IFOM, MAPCON, or non-seamless WLAN offload shall retain at least one ISRP rule from the same ANDSF. Additionally, a UE shall retain at least one set of IARP from the same ANDSF.

If a UE supporting IFOM, MAPCON, or non-seamless WLAN offload (or any combination of these featureshas ISMP and ISRP available, then ISRP shall be used for the routing of IP traffic. The relation between ISRP and user preferences is described in subclause 5.4.2.

For a UE with IFOM, MAPCON or non-seamless WLAN offload (or any combination of these capabilities) enabled, if ISMP, ISRP and IARP are available, then IARP and ISRP shall be used. In this case, the UE shall first apply IARP followed by ISRP as follows:

- If non-seamless WLAN offload is selected by IARP then the IP flow is routed to the non-seamless WLAN offload and ISRP shall not be used for the routing of IP traffic.

- If a certain APN is selected by IARP then the IP flow is routed to the PDN connections corresponding to this APN. If there is a ForFlowBased ISRP rule matching the IP flow after the APN is selected, then the UE shall use the ForFlowBased ISRP rule matching the IP flow to select the access for this IP flow.

- If neither certain APN nor non-seamless WLAN offload is selected by IARP, then ISRP shall be used for the routing of IP traffic.

The relation between IARP and user preferences is described in subclause 5.4.2.

For a UE not supporting any of IFOM, MAPCON or non-seamless offload capabilities or with all those capabilities disabled, if ISMP and ISRP are available, the ISMP shall be used.

This information shall be deleted if there is a change of USIM. This information may be deleted when UE is switched off.

6.8.2.2.4.2 Use of Inter-system Mobility Policy

If more than one set of Inter-system mobility policies is available in the UE, the UE shall only use one set of Inter-system mobility policies at any one time. If available, the inter-system mobility policy of the RPLMN takes precedence. For example, when roaming, the Inter-system mobility policy from V-ANDSF of the RPLMN, if available, takes precedence over the Inter-system mobility policy from H-ANDSF. When applying the Inter-system mobility policy the following requirements apply:-

- the requirements on periodic network reselection as described in subclause 5.3.4 of the present specification;

- the PLMN selection rules specified in 3GPP TS 23.122 [4] and in 3GPP TS 24.234 [9];

- the selection rules specified in 3GPP2 C.P0016-D [23a]; and

- the 3GPP RAT selection, cell selection and reselection rules specified in 3GPP TS 25.304 [14], 3GPP TS 36.304 [16] and 3GPP TS 45.008 [16a].

6.8.2.2.4.3 Use of Access Network Discovery Information

The UE may use the received Access network discovery information of both the H-ANSDF and V-ANDSF for network discovery and detection. The Access network discovery information received from:-

a) the H-ANDSF provides guidance for the UE on access networks that have connectivity to the HPLMN or equivalent HPLMNs or both; and

b) the V-ANDSF provides guidance for the UE on access networks that have connectivity to the corresponding VPLMN or equivalent PLMNs or both.

6.8.2.2.4.4 Use of Inter-System Routing Policies

A UE supporting IFOM, MAPCON, or non-seamless WLAN offload (or any combination of these features) shall use the ISRP if available.

A UE supporting IFOM uses the ISRP to:

- select an access technology or an access network or both for routing user plane traffic matching specific IP flows on a specific or any APN identified in the ISRP; and

- decide if an access technology or access network or both are restricted for a specific IP flows on a specific or any APN identified in the ISRP.

A UE supporting MAPCON uses the ISRP to:

- select an access technology or an access network or both for routing user plane traffic matching a specific APN or any APN identified in the ISRP; and

- decide if an access technology or an access network or both are restricted for a specific APN or any APN identified in the ISRP.

A UE supporting non-seamless WLAN offload uses the ISRP to:

- select a WLAN access network for routing, without traversing the EPC, user plane traffic matching specific IP flows for a specific APN or any APN identified in the ISRP; and

- decide if a WLAN access network is restricted for routing, without traversing the EPC, a specific IP flows for a specific APN or any APN identified in the ISRP.

When the UE supporting IFOM identifies an access technology or an access network or both over which an IP flow can be routed based on the ISRP, the UE shall apply the IFOM procedures specified in 3GPP TS 24.303 [11] to move an on-going IP flow from the source access technology or access network to the identified access technology or access network, if required.

If more than one set of ISRP is available in the UE, the UE shall only use one ISRP at any one time. If available, the ISRP of the RPLMN takes precedence. When applying ISRP the same requirements defined for inter-system mobility policy in subclause 6.8.2.2.4.2 applies.

6.8.2.2.4.5 Use of Inter-APN Routing Policies

The UE shall use the IARP if available.

A UE uses the IARP to:

- select an APN or non-seamless WLAN offload for routing user plane traffic matching specific IP flows; and

- decide if an APN or non-seamless WLAN offload is restricted for routing a specific IP flows.

An IARP for APN can be applied only when it steers IP traffic to an existing (i.e. already established) PDN connection. Also, the scenario where multiple PDN connections via the same access network are associated with the same APN is not specified in the present document.

When applying IARP the same requirements defined for inter-system mobility policy in subclause 6.8.2.2.4.2 applies.

6.8.2.3 ANDSF procedures

6.8.2.3.1 General

Both the H-ANDSF and the V-ANDSF can provide information about inter-system mobility policy or information about available access networks in the vicinity of the UE or ISRP for the UE or combinations of these. The H-ANDSF may also provide IARP for the UE. The V-ANDSF shall not provide any IARP to a roaming UE. The inter-system mobility policies may be organized in a hierarchy and a priority order among multiple policies may determine which policy has the highest priority. The policies may indicate preference of one access network over another or may restrict inter-system mobility to a particular access network under certain conditions. The ANDSF may also specify validity conditions which indicate when a policy is valid. Such conditions may be based on time duration, location, etc. The ANDSF may limit the information provided to the UE. This can be based on UE's current location, UE capabilities other than the capability of routing IP traffic simultaneously over multiple radio access interfaces (e.g. IFOM capability or MAPCON capability or non-seamless WLAN offload capability), etc. How the ANDSF decides how much information to provide to the UE is dependent on network implementation.

6.8.2.3.2 Role of ANDSF for Push model

If there is no existing valid PSK TLS connection between the UE and ANDSF, the ANDSF, not implementing GBA Push, may send a notification SMS to the UE, without establishing a data connection with the UE.

If there is no existing valid PSK TLS connection between the UE and ANDSF, the ANDSF, implementing GBA Push, shall send a message via SMS to the UE to establish a secure connection between the UE and ANDSF. The contents of the message shall contain a GBA Push Information as specified in 3GPP TS 33.223 [47].

After a secure connection is established according to subclause 6.8.2.2.1A, or if there is avalid PSK TLS connection between the UE and ANDSF, the ANDSF shall use the connection to provision ANDSF information to the UE.

6.8.2.3.3 Role of ANDSF for Pull model

When the UE connects to an ANDSF, the ANDSF may provide the UE with inter-system mobility policy or information related to available access networks in the vicinity of the UE or ISRP or IARP for the UE, or combinations of these. In case of information about available access networks, the ANDSF provides the following information about each available access network in the form of a list containing:

1) Type of Access network (e.g. WLAN, WiMAX);

2) Location of Access Network (e.g. 3GPP location, WLAN location);

3) Access Network specific information (e.g WLAN information, WiMAX information); and

4) Operator differentiated text field (if supported, e.g. if WNDS MO defined in 3GPP TS 24.312 [13] is used).

The detailed list of information is described in 3GPP TS 24.312 [13].

6.9 Handling of Protocol Configuration Options information

The Protocol Configuration Options (PCO) information element is specified in 3GPP TS 24.008 [46].

The support of PCOs is optional for the UE and the non-3GPP access network.

The content syntax of PCOs for the non-3GPP access UE and non-3GPP access network is access network specific and not in the scope of 3GPP, but if PCO is supported, the UE and the PDN-GW shall handle the PCO contents in accordance with 3GPP TS 24.008 [46].

PCO information is exchanged between the UE and the PDN-GW, see 3GPP TS 23.402 [6] and 3GPP TS 29.275 [18]. The specification of PCO signalling in the non-3GPP access network is access network specific and not in the scope of 3GPP.

7 Tunnel management procedures

7.1 General

The purpose of tunnel management procedures is to define the procedures for establishment or disconnection of an end-to-end tunnel between the UE and the ePDG. The tunnel establishment procedure is always initiated by the UE, whereas the tunnel disconnection procedure can be initiated by the UE or the ePDG.

The tunnel is an IPsec tunnel (see IETF RFC 4301 [30]) established via an IKEv2 protocol exchange IETF RFC 5996 [28] between the UE and the ePDG. The UE may indicate support for IETF RFC 4555 [31]. The security mechanisms for tunnel setup using IPsec and IKEv2 are specified in 3GPP TS 33.402 [15].

7.2 UE procedures

7.2.1 Selection of the ePDG

For dynamic selection of the ePDG the UE shall support the implementation of standard DNS mechanisms in order to retrieve the IP address(es) of the ePDG. The input to the DNS query is an ePDG FQDN as specified in subclause 4.4.3 and in 3GPP TS 23.003 [3]. The ePDG FQDN contains a PLMN ID as Operator Identifier. The UE selects the PLMN ID used in the ePDG FQDN based on the conditions described below.

1. If the UE is EPS attached or GPRS attached (see 3GPP TS 23.122 [4]) to a Visited PLMN and:

1a) if the UE is not provided with a list of available PLMN ID(s), the UE shall use the PLMN identity of the RPLMN or an equivalent PLMN (see 3GPP TS 24.301 [10] or 3GPP TS 24.008 [46]) in the creation of the ePDG FQDN (see 3GPP TS 23.003 [3]);. If the DNS query with FQDN constructed using RPLMN identity does not return any IP address, then the UE as an implementation option may try again with FQDN constructed using an equivalent PLMN.

1b) if the UE is provided with a list of available PLMN ID(s) served by the access network, e.g. through the access specific signalling as specified in 3GPP TS 24.234 [9], and the current RPLMN or an equivalent PLMN is contained in the list of available PLMN ID(s), the UE shall include this PLMN identity in the creation of the ePDG FQDN (see 3GPP TS 23.003 [3]); or

1c) in all other cases, the UE shall include the PLMN identity of the Home PLMN or EHPLMN in the ePDG FQDN. The HPLMN or EHPLMN shall be chosen based on the PLMN selection policy for the access network the UE is accessing e.g. see 3GPP TS 24.234 [9] subclause 5.2.4.

2. If the UE is EPS attached or GPRS attached to the Home PLMN or EHPLMN and:

2a) if the UE is not provided with a list of available PLMN ID(s), the UE shall use the PLMN identity of the Home PLMN or EHPLMN in the creation of the ePDG FQDN; or

2b) if the UE is provided with a list of available PLMN ID(s) served by the access network e.g. through the access specific signalling as specified in 3GPP TS 24.234 [9], and the Home PLMN or EHPLMN is contained in the list of available PLMN ID(s), then the UE shall use this PLMN identity in the ePDG FQDN;

2c) in all other cases, the UE behaviour is implementation specific; or

3. If the UE is not attached to any PLMN, the UE performs PLMN selection as described in subclause 5.2.1 and:

3a) if the UE is provided with a list of available PLMN ID(s) served by the access network e.g. through the access specific signalling as specified in 3GPP TS 24.234 [9], and neither Home PLMN nor EHPLMN is contained in the list, use the PLMN identity of the selected PLMN from PLMN selection in the ePDG FQDN; or

3b) otherwise, the UE shall include the identity of the Home PLMN or EHPLMN in the ePDG FQDN.

Upon reception of a DNS response containing one or more IP addresses of ePDGs, the UE shall select an IP address of ePDG with the same IP version as its local IP address.

The UE shall select only one ePDG also in case of multiple PDN connections.

NOTE: During handover between two untrusted non-3GPP access networks, the UE can initiate tunnel establishment to another ePDG while still being attached to the current ePDG.

7.2.2 Tunnel establishment

Once the ePDG has been selected, the UE shall initiate the IPsec tunnel establishment procedure using the IKEv2 protocol as defined in IETF RFC 5996 [28] and 3GPP TS 33.402 [15].

The UE shall send an IKE_SA_INIT request message to the selected ePDG in order to setup an IKEv2 security association. Upon receipt of an IKE_SA_INIT response, the UE shall send an IKE_AUTH request message to the ePDG, including the type of IP address (IPv4 address or IPv6 prefix or both) that needs to be configured in an IKEv2 CFG_REQUEST Configuration Payload. If the UE requests for both IPv4 address and IPv6 prefix, it shall send two configuration attributes in the CFG_REQUEST Configuration Payload, one for the IPv4 address and the other for the IPv6 prefix. The IKE_AUTH request message shall contain in "IDr" payload the APN and in the "IDi" payload the NAI. The UE indicates a request for the default APN by omitting IDr payload, which is in accordance with IKEv2 protocol as defined in IETF RFC 5996 [28]. The IKE_AUTH request message may contain in a notify payload an indication that MOBIKE is supported by the UE. The UE may also include the INTERNAL_IP6_DNS or the INTERNAL_IP4_DNS attribute in the CFG_REQUEST Configuration Payload. The UE can obtain zero or more DNS server addressed in the CFG_REPLY payload as specified in IETF RFC 5996 [28].

During the IKEv2 authentication and security association establishment, if the UE supports explicit indication about the supported mobility protocols, it shall provide the indication as described in subclause 6.3.

During the IKEv2 authentication and tunnel establishment for initial attach, the UE shall provide an indication about Attach Type, which indicates Initial Attach. To indicate attach due to initial attach, the UE shall include either the INTERNAL_IP4_ADDRESS or the INTERNAL_IP6_ADDRESS attribute or both in the CFG_REQUEST Configuration Payload within the IKE_AUTH request message. The INTERNAL_IP4_ADDRESS shall contain no value and the length field shall be set to 0. The INTERNAL_IP6_ADDRESS shall contain no value and the length field shall be set to 0.

During the IKEv2 authentication and tunnel establishment for handover, the UE not supporting IP address preservation for NBM shall indicate Initial Attach as described in the previous paragraph.

During the IKEv2 authentication and security association establishment for handover, the UE supporting IP address preservation for NBM, shall provide an indication about Attach Type, which indicates Handover Attach. To indicate attach due to handover, the UE shall include the previously allocated home address information during the IPSec tunnel establishment. Depending on the IP version, the UE shall include either the INTERNAL_IP4_ADDRESS or the INTERNAL_IP6_ADDRESS attribute or both in the CFG_REQUEST Configuration Payload within the IKE_AUTH request message to indicate the home address information which is in accordance with IKEv2 protocol as defined in IETF RFC 5996 [28]. The UE shall support IPSec ESP (see IETF RFC 4303 [32]) in order to provide secure tunnels between the UE and the ePDG as specified in 3GPP TS 33.402 [15].

The UE may support multiple authentication exchanges in the IKEv2 protocol as specified in IETF RFC 4739 [49] in order to support authentication and authorization with an external AAA server allowing the UE to support PAP authentication procedure, or CHAP authentication procedure, or both, as described in 3GPP TS 33.402 [15].

If NBM is used and the UE wishes to access an external PDN and therefore needs to perform authentication and authorization with an external AAA server, the UE shall:

- If the IKE_SA_INIT response contains a "MULTIPLE_AUTH_SUPPORTED" Notify payload, then include a "MULTIPLE_AUTH_SUPPORTED" Notify payload in the IKE_AUTH request as described in IETF RFC 4739 [49] and perform the additional authentication steps as specified in 3GPP TS 33.402 [15]; and

- If the IKE_SA_INIT response does not contain a "MULTIPLE_AUTH_SUPPORTED" Notify payload, then perform the UE initiated disconnection as defined in subclause 7.2.4.1. The subsequent UE action is implementation dependent (e.g. select a new ePDG).

If NBM is used and if the UE receives from the ePDG an IKE_AUTH response message containing a Notify Payload with a Private Notify Message Type PDN_CONNECTION_REJECTION as specified in subclause 8.1.2 that includes an IP address information in the Notification Data field, the UE shall not attempt to re-establish this PDN connection while connected to the current ePDG and the UE shall close the related IKEv2 security association states.

If NBM is used and if the UE receives from the ePDG an IKE_AUTH response message containing a Notify Payload with a Private Notify Message Type PDN_CONNECTION_REJECTION as specified in subclause 8.1.2 and no Notification Data field, the UE shall not attempt to establish additional PDN connections to this APN while connected to the current ePDG. The UE shall close the related IKEv2 security association states. Subsequently, the UE can attempt to establishment additional PDN connections to the given APN if one or more existing PDN connections to the given APN are released. While connected to the current ePDG, if this PDN connection is the first PDN connection for the given APN, the UE shall not attempt to establish PDN connection to the given APN.

If NBM is used and if the UE receives from the ePDG an IKE_AUTH response message containing a Notify Payload with a Private Notify Message Type MAX_CONNECTION_REACHED as specified in subclause 8.1.2, the UE shall not attempt to establish any additional PDN connections while connected to the current ePDG. The UE shall close the related IKEv2 security association states. Subsequently, the UE can attempt to establishment additional PDN connections if one or more existing PDN connections are released.

After the successful authentication with the 3GPP AAA server, the UE receives from the ePDG an IKE_AUTH response message containing a single CFG_REPLY Configuration Payload including the assigned remote IP address information (IPv4 address or IPv6 prefix) as described in subclause 7.4.1. Depending on the used IP mobility management mechanism the following cases can be differentiated:

- If DSMIPv6 is used for IP mobility management, the UE configures a remote IP address based on the IP address information contained in the INTERNAL_IP4_ADDRESS or INTERNAL_IP6_SUBNET attribute of the CFG_REPLY Configuration Payload. The UE uses the remote IP address as Care-of-Address to contact the HA.

- If NBM is used for IP mobility management and the UE performs an initial attach, the UE configures a home address based on the address information from the CFG_REPLY Configuration Payload. Otherwise, if NBM is used and the UE performs a handover attach, the UE continues to use its IP address configured before the handover, if the address information provided in the CFG_REPLY Configuration Payload does match with the UE's IP address configured before the handover. If the UE's IP address does not match with the address information of the CFG_REPLY Configuration Payload, the UE shall configure a new home address based on the IP address information contained in the INTERNAL_IP4_ADDRESS or INTERNAL_IP6_SUBNET attribute of the CFG_REPLY Configuration Payload. In the latter case, the IP address preservation is not possible.

If the UE supports DSMIPv6, the UE may request the HA IP address(es), by including a corresponding CFG_REQUEST Configuration Payload containing a HOME_AGENT_ADDRESS attribute. The HOME_AGENT_ADDRESS attribute content is defined in subclause 8.2.4.1. The HA IP address(es) requested in this attribute are for the APN for which the IPsec tunnel with the ePDG is set-up. In the CFG_REQUEST, the UE sets respectively the IPv6 address field and the optional IPv4 address field of the HOME_AGENT_ADDRESS attribute to 0::0 and to 0.0.0.0. If the UE can not obtain the IP addresses of the HA via IKEv2 signalling, it uses the home agent address discovery as specified in 3GPP TS 24.303 [11].

In case the UE wants to establish multiple PDN connections and if the UE uses DSMIPv6 for mobility management, the UE shall use DNS as defined in 3GPP TS 24.303 [11] to discover the HA IP address(es) for the additional PDN connections after IKEv2 security association was established to the ePDG.

7.2.3 Tunnel modification

This procedure is used if MOBIKE as defined in IETF RFC 4555 [31] is supported by the UE.

When there is a change of local IP address for the UE, the UE shall update the IKE security association with the new address, and shall update the IPsec security association associated with this IKE security association with the new address. The UE shall then send an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification to the ePDG.

If, further to this update, the UE receives an INFORMATIONAL request with a COOKIE2 notification present, the UE shall copy the notification to the COOKIE2 notification of an INFORMATIONAL response and send it to the ePDG.

7.2.4 Tunnel disconnection

7.2.4.1 UE initiated disconnection

The UE shall use the procedures defined in the IKEv2 protocol (see IETF RFC 5996 [28]) to disconnect an IPsec tunnel to the ePDG. The UE shall close the incoming security associations associated with the tunnel and instruct the ePDG to do the same by sending the INFORMATIONAL request message including a "DELETE" payload. The DELETE payload shall contain either:

i) Protocol ID set to "1" and no subsequent Security Parameters Indexes (SPIs) in the payload. This indicates closing of IKE security association, and implies the deletion of all IPsec ESP security associations that were negotiated within the IKE security association; or

ii) Protocol ID set to "3" for ESP. The Security Parameters Indexes included in the payload shall correspond to the particular incoming ESP security associations at the UE for the given tunnel in question.

7.2.4.2 UE behaviour towards ePDG initiated disconnection

On receipt of the INFORMATIONAL request message including "DELETE" payload, indicating that the ePDG is attempting tunnel disconnection, the UE shall:

i) Close all security associations identified within the DELETE payload (these security associations correspond to outgoing security associations from the UE perspective). If no security associations were present in the DELETE payload, and the protocol ID was set to "1", the UE shall close the IKE security association, and all IPsec ESP security associations that were negotiated within it towards the ePDG; and

ii) The UE shall delete the incoming security associations corresponding to the outgoing security associations identified in the "DELETE" payload.

The UE shall send an INFORMATIONAL response message. If the INFORMATIONAL request message contained a list of security associations, the INFORMATIONAL response message shall contain a list of security associations deleted in step (ii) above.

If the UE is unable to comply with the INFORMATIONAL request message, the UE shall send INFORMATION response message with either:

i) A NOTIFY payload of type "INVALID_SPI", for the case that it could not identify one or more of the Security Parameters Indexes in the message from the ePDG; or

ii) A more general NOTIFY payload type. This payload type is implementation dependent.

7.3 3GPP AAA server procedures

The UE – 3GPP AAA server procedures are as specified in 3GPP TS 29.273 [17] and 3GPP TS 33.402 [15].

7.4 ePDG procedures

7.4.1 Tunnel establishment

Upon receipt of an IKE_AUTH request message from the UE requesting the establishment of a tunnel, the ePDG shall proceed with authentication and authorization. The basic procedure described in 3GPP TS 33.402 [15], while further details are given below.

During the UE's authentication and authorization procedure, the 3GPP AAA server provides to the ePDG an indication about the selected IP mobility mechanism as specified in 3GPP TS 29.273 [17].

The ePDG shall proceed with IPsec tunnel setup completion and shall relay in the IKEv2 Configuration Payload (CFG_REPLY) of the final IKE_AUTH response message the remote IP address information to the UE. If NBM is used as IP mobility mechanism, the ePDG shall assign either an IPv4 address or an IPv6 Home Network Prefix or both to the UE via a single CFG_REPLY Configuration Payload. If the UE requests for both IPv4 address and IPv6 prefix, but the ePDG only assigns an IPv4 address or an IPv6 Home Network Prefix due to subscription restriction or network preference, the ePDG shall include the assigned remote IP address information (IPv4 address or IPv6 prefix) via a single CFG_REPLY Configuration Payload. If the ePDG assigns an IPv4 address, the CFG_REPLY contains the INTERNAL_IP4_ADDRESS attribute. If the ePDG assigns an IPv6 Home Network Prefix, the CFG_REPLY contains the INTERNAL_IP6_SUBNET configuration attribute. The ePDG obtains the IPv4 address and/or the IPv6 Home Network Prefix from the PDN GW. If the UE does not provide an APN to the ePDG during the tunnel establishment, the ePDG shall include the default APN in the IDr payload of the IKE_AUTH response message. If the UE included the INTERNAL_IP6_DNS or the INTERNAL_IP4_DNS in the CFG_REQUEST Configuration payload, the ePDG shall include the same attribute in the CFG_REPLY Configuration payload including zero or more DNS server addresses as specified in IETF RFC 5996 [28].

If DSMIPv6 is used as IP mobility mechanism, depending on the information provided by the UE in the CFG_REQUEST payload the ePDG shall assign to the UE either a local IPv4 address or local IPv6 address (or a local IPv6 prefix) via a single CFG_REPLY Configuration Payload. If the ePDG assigns a local IPv4 address, the CFG_REPLY contains the INTERNAL_IP4_ADDRESS attribute. If the ePDG assigns a local IPv6 address or a local IPv6 prefix the CFG_REPLY contains correspondingly the INTERNAL_IP6_ADDRESS or the INTERNAL_IP6_SUBNET attribute. If the UE provided an APN to the ePDG during the tunnel establishment, the ePDG shall not change the provided APN and shall include the APN in the IDr payload of the IKE_AUTH response message. An IPsec tunnel is now established between the UE and the ePDG.

If NBM is used and if the ePDG needs to reject a PDN connection due to conditions as specified in 3GPP TS 29.273 [17] or the network policies or the ePDG capabilities to indicate that no more PDN connection request of the given APN can be accepted for the UE, the ePDG shall include, in the IKE_AUTH response message, a Notify Payload with a Private Notify Message Type PDN_CONNECTION_REJECTION as specified in subclause 8.1.2. Additionally if the IKE_AUTH request message from the UE indicated Handover Attach as specified in subclause 7.2.2, the Notification Data field of the Notify Payload shall include the IP address information from the Handover Attach indication. If the UE indicated Initial Attach, the Notification Data field shall be omitted. If the ePDG

needs to reject a PDN connection due to the network policies or capabilities to indicate that no more PDN connection request with any APN can be accepted for the UE, the ePDG shall include in the IKE_AUTH response message containing the IDr payload a Notify Payload with a Private Notify Message Type MAX_CONNECTION_REACHED as specified in subclause 8.1.2. If the ePDG determines that UE is not allowed to access EPC due to reasons specified in 3GPP TS 29.273 [17], the ePDG shall include, in the IKE_AUTH response message, a Notify Payload with a Notify Message Type AUTHENTICATION_FAILED as specified in IETF RFC 5996 [28].

If the UE indicates Handover Attach by including the previously allocated home address information and the ePDG obtains one or more PDN GW identities from the 3GPP AAA server, the ePDG shall use these identified PDN GWs in the subsequent PDN GW selection process. If the UE indicates Initial Attach i.e. home address information not included, the ePDG may run its initial PDN GW selection process to determine the PDN GW without using the received PDN GW identities.

The ePDG shall support IPSec ESP (see IETF RFC 4303 [32]) in order to provide secure tunnels between the UE and the ePDG as specified in 3GPP TS 33.402 [15].

During the IKEv2 authentication and tunnel establishment, if the UE requested the HA IP address(es) and if DSMIPv6 was chosen and if the HA IP address(es) are available, the ePDG shall provide the HA IP address(es) (IPv6 address and optionally IPv4 address) for the corresponding APN as specified by the "IDr" payload in the IKE_AUTH request message by including in the CFG_REPLY Configuration Payload a HOME_AGENT_ADDRESS attribute. In the CFG_REPLY, the ePDG sets respectively the IPv6 Home Agent address field and optionally the IPv4 Home Agent address field of the HOME_AGENT_ADDRESS attribute to the IPv6 address of the HA and to the IPv4 address of the HA. If no IPv4 HA address is available at the ePDG or if it was not requested by the UE, the ePDG shall omit the IPv4 Home Agent Address field. If the ePDG is not able to provide an IPv6 HA address for the corresponding APN, then the ePDG shall not include a HOME_AGENT_ADDRESS attribute in the CFG_REPLY.

The ePDG may support multiple authentication exchanges in the IKEv2 protocol as specified in IETF RFC 4739 [49] in order to support additional authentication and authorization of the UE with an external AAA server.

If the ePDG supports authentication and authorization of the UE with an external AAA server, on receipt of an IKE_SA_INIT message the ePDG shall include a Notify payload of type "MULTIPLE_AUTH_SUPPORTED" in the IKE_SA_INIT response message to the UE.

On successful completion of authentication and authorization procedure of the UE accessing EPC and on receipt of an IKE_AUTH request containing a Notify payload of type "ANOTHER_AUTH_FOLLOWS", the ePDG shall send an IKE_AUTH response containing the "AUTH" payload.

Upon receipt of a subsequent IKE_AUTH request from the UE containing the user identity in the private network within the "IDi" payload, the ePDG shall:

- if PAP authentication is required, then send an EAP-GTC request to the UE within an IKE_AUTH response message. Upon receipt of an EAP-GTC response from the UE, the ePDG shall use the procedures defined in 3GPP TS 29.275 [18] and 3GPP TS 29.274 [50] to authenticate the user with the external AAA server; and

- if CHAP authentication is required, then send an EAP MD5-Challenge request to UE. Upon receipt of EAP MD5-Challenge response within an IKE_AUTH request message from the UE, the ePDG shall use the procedures defined in 3GPP TS 29.275 [18] and 3GPP TS 29.274 [50] to authenticate the user with the external AAA server. If the ePDG receives Legacy-Nak response containing EAP–GTC type from the UE (see IETF RFC 3748 [29]) the ePDG may change the authentication and authorization procedure. If the ePDG does not change the authentication and authorization procedure or if the ePDG receives a Legacy-Nak response not containing EAP-GTC, the ePDG shall send an EAP-Failure to the UE.

NOTE: The signalling flows for authentication and authorization with an external AAA server are described in 3GPP TS 33.402 [15].

7.4.2 Tunnel modification

When receiving an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification, the ePDG shall check the validity of the IP address and update the IP address in the IKE security association with the values from the IP header. The ePDG shall reply with an INFORMATIONAL response.

The ePDG may initiate a return routability check for the new address provided by the UE, by including a COOKIE2 notification in an INFORMATIONAL request and send it to the UE. When the ePDG receives the INFORMATIONAL

response from the UE, it shall check that the COOKIE2 notification payload is the same as the one it sent to the UE. If it is different, the ePDG shall close the IKE security association by sending an INFORMATIONAL request message including a "DELETE" payload.

If no return routability check is initiated by the ePDG, or if a return routability check is initiated and is successfully completed, the ePDG shall update the IPsec security associations associated with the IKE security association with the new address.

7.4.3 Tunnel disconnection

7.4.3.1 ePDG initiated disconnection

The ePDG shall use the procedures defined in the IKEv2 protocol (see IETF RFC 5996 [28]) to disconnect an IPsec tunnel to the UE. The ePDG shall close the incoming security associations associated with the tunnel and instruct the UE to do likewise by sending the INFORMATIONAL request message including a "DELETE" payload. The DELETE payload shall contain either:

i) Protocol ID set to "1" and no subsequent Security Parameter Indexes in the payload. This indicates that the IKE security association, and all IPsec ESP security associations that were negotiated within it between ePDG and UE shall be deleted; or

ii) Protocol ID set to "3" for ESP. The SECURITY PARAMETERS INDEXES s included in the payload shall correspond to the particular incoming ESP SECURITY ASSOCIATION at the UE for the given tunnel in question.

7.4.3.2 ePDG behaviour towards UE initiated disconnection

On receipt of the INFORMATIONAL request message including "DELETE" payload indicating that the UE is initiating tunnel disconnect procedure, the ePDG shall:

i) Close all security associations identified within the DELETE payload (these security associations correspond to outgoing security associations from the ePDG perspective). If no security associations were present in the DELETE payload, and the protocol ID was set to "1", the ePDG shall close the IKE security association, and all IPsec ESP security associations that were negotiated within it towards the UE; and

ii) The ePDG shall delete the incoming security associations corresponding to the outgoing security associations identified in the "DELETE" payload.

The ePDG shall send an INFORMATIONAL response message. This shall contain a list of security associations deleted in step (ii) above.

If the ePDG is unable to comply with the INFORMATIONAL request message, the ePDG shall send INFORMATION response message with either:

i) a NOTIFY payload of type "INVALID_SPI", for the case that it could not identify one or more of the SECURITY PARAMETERS INDEXES in the message from the UE; or

ii) a more general NOTIFY payload type. This payload type is implementation dependent.

8 PDUs and parameters specific to the present document

8.0 General

The least significant bit of a field is represented by the lowest numbered bit of the highest numbered octet of the field. When the field extends over more than one octet, the order of bit values progressively decreases as the octet number increases.

Figure 8.0-1 shows an example of a field where the most significant bit of the field is marked MSB and the least significant bit of the field is marked LSB.

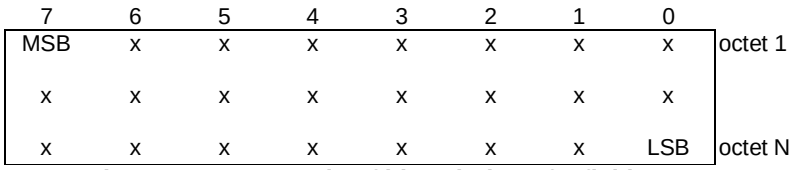

Figure 8.0-1: Example of bit ordering of a field

NOTE: IETF RFCs adopted different numbering of bits, such that the least significant bit of a field is represented by the highest numbered bit of the field.

8.1 3GPP specific coding information defined within present document

8.1.1 Access Network Identity format and coding

8.1.1.1 Generic format of the Access Network Identity

The Access Network Identity shall take the generic format of an octet string without terminating null characters. The length indicator for the ANID is 2 bytes long, see IETF RFC 5448 [38]. Representation as a character string is allowed, but this character string shall be converted into an octet string of maximum length 253 according to UTF-8 encoding rules as specified in IETF RFC 3629 [34] before the Access Network Identity is input to the Key Derivation Function, as specified in 3GPP TS 33.402 [15], or used in the Access Network Identity indication from 3GPP AAA server to UE, cf. subclause 8.2.2. The ANID is structured as an ANID Prefix and none, one or more ANID additional character strings separated by the colon character ":". In case additional ANID strings are not indicated the complete ANID consists of the ANID Prefix character string only. The ANID shall be represented by Unicode characters encoded as UTF-8 as specified in IETF RFC 3629 [34] and formatted using Normalization Form KC (NFKC) as specified in Unicode 5.1.0, Unicode Standard Annex #15; Unicode Normalization Forms [41].

8.1.1.2 Definition of Access Network Identities for Specific Access Networks

Table 8.1.1.2 specifies the list of Access Network Identities defined by 3GPP in the context of non-3GPP access to EPC.

Table 8.1.1.2: Access Network Identities

Access Network Identity		Type of Access Network
ANID Prefix	**Additional ANID strings**	
"HRPD" constant character string, see NOTE 1 and NOTE 2	No additional ANID string, see NOTE 2 and NOTE 6	cdma2000® HRPD access network
"WIMAX" constant character string, see NOTE 1	No additional ANID string, see NOTE 3 and NOTE 6	WiMAX access network
"WLAN" constant character string, see NOTE 1	No additional ANID string, see NOTE 4 and NOTE 6	WLAN access network
"ETHERNET" constant character string, see NOTE 1	No additional ANID string, see NOTE 5 and NOTE 6	Fixed access network
All other character strings	Not applicable	Not defined, see NOTE 6 and Annex B

NOTE 1: The quotes are not part of the definition of the character string.

NOTE 2: The value of the ANID Prefix for cdma2000® HRPD access networks is defined in 3GPP2 X.S0057 [20]. 3GPP2 is responsible for specifying possible additional ANID strings applicable to the "HRPD" ANID Prefix.

NOTE 3: WiMAX Forum is responsible for specifying possible additional ANID strings applicable to the "WIMAX" ANID Prefix.

NOTE 4: IEEE 802 is responsible for specifying possible additional ANID strings applicable to the "WLAN" ANID Prefix.

NOTE 5: IEEE 802 is responsible for specifying possible additional ANID strings applicable to the "ETHERNET" ANID Prefix.

NOTE 6: Additional ANID Prefixes and ANID strings can be added to this table following the procedure described in the informative Annex B.

8.1.2 IKEv2 Notify Message Type value

8.1.2.1 Generic

The IKEv2 Notify Message Type is specified in IETF RFC 4306 [28]. The value of Notify Message Type between 8192 and 16383 is reserved for private Error usage. Only the private IKEv2 Notify Message Type used for this specification is specified in this subclause.

8.1.2.2 Private Notify Message - Error Types

The Private Notify Message, Error Types defined in table 8.1.2.2-1 are error notifications which indicates an error while negotiating an IKEv2 SA for the PDN connection to the APN requested by the UE. Refer to table 8.1.2.2-1 for more details on what each error type means.

Table 8.1.2.2-1: Private Error Types

Notify Message	Value	Descriptions
PDN_CONNECTION_REJECTION	8192	With an IP address information in Notification Data field: The PDN connection corresponding to the IP address information has been rejected. Without Notification Data field: The PDN connection corresponding to the requested APN has been rejected. No additional PDN connections to the given APN can be established. If the rejected PDN connection is the first PDN connection for the given APN, this APN is not allowed for the UE.
MAX_CONNECTION_REACHED	8193	The PDN connection has been rejected. No additional PDN connections can be established for the UE due to the network policies or capabilities. The maximum number of PDN connections per UE allowed to be established simultaneously is 11 due to a limitation in the network mobility procedures.

8.1.3 ANDSF Push Information

8.1.3.1 General

The values of the ANDSF Push Information sent to the UE using the GAA bootstrap framework for ANDSF Push as specified in subclause 6.8.2.2.2 are defined in this subclause.

8.1.3.2 ANDSF Push Information values

The ANDSF Push Information defined in table 8.1.3.2-1 indicates the X-WAP-Application-ID field (Push Application ID) for ANDSF in the WSP header.

Table 8.1.3.2-1: ANDSF Push Information values

WSP header attribute	Value	Short code	Descriptions
X-WAP-Application-ID	x-3gpp.gba.andsf.ua	To be added	The application identity indicates ANDSF

Editor's note: The Application Id "x-wap-3gpp:gba.andsf" has to be de-registered with OMA OMNA. The WSP short code for "x-3gpp.gba.andsf.ua" should be requested from OMA OMNA.

8.1.4 PDUs for TWAN connection modes

8.1.4.0 General

The PDUs defined in this subclause are used when SCM, MCM or both are supported.

8.1.4.1 Message

The message is coded according to figure 8.1.4.1-1 and table 8.1.4.1-1.

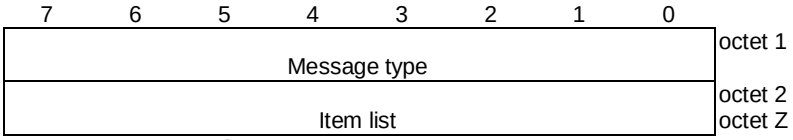

Figure 8.1.4.1-1: Message

Table 8.1.4.1-1: Message

Message type field is coded according to table 8.1.4.1-2. When value other than those listed in table 8.1.4.1-2 is indicated, the message is ignored. Optional item list field contains sequence of items, each of which is coded according to subclause 8.1.4.2. Order of the items in the item list field is not important. The item list field includes at maximum one item of each type described in subclause 8.1.4.2.

Table 8.1.4.1-2: Message type

The value is coded as follows.								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0	0	0	0	0	0	0	1	CONNECTION_CAPABILITY
0	0	0	0	0	0	1	0	SCM_REQUEST
0	0	0	0	0	0	1	1	SCM_RESPONSE
0	0	0	0	0	1	0	0	MCM_REQUEST
0	0	0	0	0	1	0	1	MCM_RESPONSE

8.1.4.2 Item

The item is coded according to figure 8.1.4.2-1 and table 8.1.4.2-1:

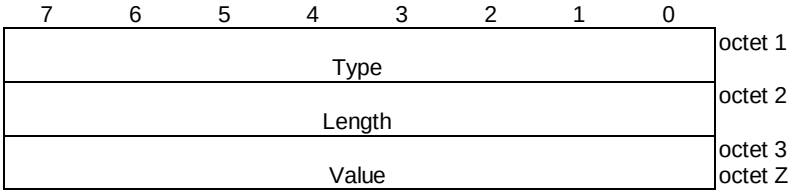

Figure 8.1.4.2-1: Item

Table 8.1.4.2-1: Item

Type field is coded according to the table 8.1.4.2-2. When the type field contains a type other than those specified in table 8.1.4.2-2, the item is ignored. Length field indicates the number of octets in the value field. Value field contains the value of the parameter indicated by the type field.

Table 8.1.4.2-2: Types of item

The type field is coded as follows.								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0	0	0	0	0	0	0	0	CONNECTIVITY_TYPE
0	0	0	0	0	0	0	1	ATTACHMENT_TYPE
0	0	0	0	0	0	1	0	APN
0	0	0	0	0	0	1	1	PDN_TYPE
0	0	0	0	0	1	0	0	AUTHORIZATIONS
0	0	0	0	0	1	0	1	CONNECTION_MODE_CAPABILITY
0	0	0	0	0	1	1	0	PROTOCOL_CONFIGURATION_OPTIONS
0	0	0	0	0	1	1	1	CAUSE

8.1.4.3 CONNECTIVITY_TYPE item

When the type field of the item according to subclause 8.1.4.2 indicates the CONNECTIVITY_TYPE, then the length field of the item is set to 1 and the value field of the item is coded according to figure 8.1.4.3-1 and table 8.1.4.3-1.

7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0	0	0	0	0	0	CT1	CT0	octet 1

Figure 8.1.4.3-1: CONNECTIVITY_TYPE value

Table 8.1.4.3-1: CONNECTIVITY_TYPE value

The value is coded as follows:

PDN connection connectivity type (CT0) (octet 1, bit 0)

0 PDN connection is not requested and not authorized.

1 When received by the 3GPP AAA server, the PDN connection is requested. When received by the UE, the PDN connection is authorized.

NSWO connectivity type (CT1) (octet 1, bit 1)

0 NSWO is not requested and not authorized.

1 When received by the 3GPP AAA server, NSWO is requested. When received by the UE, NSWO is authorized.

When received by the 3GPP AAA server and several bits are set to one, then it indicates that any of the indicated connectivity types is requested. When received by the UE and several bits are set to one, then all bits other than the lowest numbered bit set to one are interpreted as set to zero.

All other bits are ignored by receiving entity.

8.1.4.4 ATTACHMENT_TYPE item

When the type field of the item according to subclause 8.1.4.2 indicates the ATTACHMENT_TYPE, then the length field of the item is set to 1 and the value field of the item is coded according to table 8.1.4.4-1.

Table 8.1.4.4-1: ATTACHMENT_TYPE value

The value is coded as follows. All other values are interpreted as "Initial attach".								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0	0	0	0	0	0	0	1	Initial attach
0	0	0	0	0	0	1	0	Handover attach

8.1.4.5 APN item

When the type field of the item according to subclause 8.1.4.2 indicates the APN, then the value field of the item contains the APN as described in 3GPP TS 23.003 [3]. When received by the 3GPP AAA server, it indicates the requested APN. When received by the UE, it indicates the selected APN.

8.1.4.6 PDN_TYPE item

When the type field of the item according to subclause 8.1.4.2 indicates the PDN_TYPE, then the length field of the item is set to 1 and the value field of the item is coded according to table 8.1.4.6-1.

Table 8.1.4.6-1: PDN_TYPE value

The value is coded as follows. All other values are interpreted as "IPv6".								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0	0	0	0	0	0	0	1	IPv4 - when received by the 3GPP AAA server, it indicates that IPv4 is requested. When received by the UE, it indicates that IPv4 is supported.
0	0	0	0	0	0	1	0	IPv6 - when received by the 3GPP AAA server, it indicates that IPv6 is requested. When received by the UE, it indicates that IPv6 is supported.
0	0	0	0	0	0	1	1	IPv4v6 - when received by the 3GPP AAA server, it indicates that IPv4, IPv6 or both are requested. When received by the UE, it indicates that both IPv4 and IPv6 are supported.

8.1.4.7 AUTHORIZATIONS item

When the type field of the item according to subclause 8.1.4.2 indicates the AUTHORIZATIONS, then the length field of the item is set to 1 and the value field of the item is coded according to figure 8.1.4.7-1 and table 8.1.4.7-1.

7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0	0	0	0	0	0	0	NSWOA	octet 1

Figure 8.1.4.7-1: AUTHORIZATIONS value

Table 8.1.4.7-1: AUTHORIZATIONS value

The value is coded as follows:
UE authorization to use NSWO (NSWOA) (octet 1, bit 0)
0 UE is not authorized to use NSWO
1 UE is authorized to use NSWO
All other bits are ignored by receiving entity.

8.1.4.8 CONNECTION_MODE_CAPABILITY item

When the type field of the item according to subclause 8.1.4.2 indicates the CONNECTION_MODE_CAPABILITY, then the length field of the item is set to 1 and the value field of the item is coded according to figure 8.1.4.8-1 and table 8.1.4.8-1.

7	6	5	4	3	2	1	0	
0	0	0	0	0	TSMCI	MCMI	SMCI	octet 1

Figure 8.1.4.8-1: CONNECTION_MODE_CAPABILITY value

Table 8.1.4.8-1: CONNECTION_MODE_CAPABILITY value

The value is coded as follows:
Support of SCM (SCMI) (octet 1, bit 0)
0 SCM is not supported
1 SCM is supported
Support of MCM (MCMI) (octet 1, bit 1)
0 MCM is not supported
1 MCM is supported
Support of TSCM (TSCMI) (octet 1, bit 2)
0 TSCM is not supported
1 TSCM is supported
All other bits are ignored by receiving entity.

8.1.4.9 PROTOCOL_CONFIGURATION_OPTIONS item

When the type field of the item according to subclause 8.1.4.2 indicates the PROTOCOL_CONFIGURATION_OPTIONS, then the value field of the item is coded as the protocol configuration options information element defined in 3GPP TS 24.008 [46] subclause 10.5.6.3 except for the protocol configuration options IEI and the length of protocol config. options contents which are not included.

8.1.4.10 CAUSE item

8.1.4.10.1 General

When the type field of the item according to subclause 8.1.4.2 indicates the CAUSE, then the length field of the item is set to 1 and the value field of the item is coded according to table 8.1.4.10-1. If the CAUSE item is received by the 3GPP AAA server, the item is ignored.

Semantic of the values is defined in subclause 8.1.4.10.2.

Table 8.1.4.10-1: CAUSE value

The value is coded as follows. All other values received by the UE are treated as 01101111, "Protocol error, unspecified".								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0	0	1	0	0	0	0	1	Requested service option not subscribed
0	0	1	1	0	0	1	0	PDN type IPv4 only allowed
0	0	1	1	0	0	1	1	PDN type IPv6 only allowed
0	1	1	0	1	1	1	1	Protocol error, unspecified

8.1.4.10.2 Causes

Cause #33 - Requested service option not subscribed

This cause is sent when the UE requests a service option for which it has no subscription.

Cause #50 - PDN type IPv4 only allowed

This value is used by the network to indicate that only PDN type IPv4 is allowed for the requested PDN connectivity.

Cause #51 - PDN type IPv6 only allowed

This value is used by the network to indicate that only PDN type IPv6 is allowed for the requested PDN connectivity.

Cause #111 - Protocol error, unspecified

This value is used to report a protocol error event only when no other value applies.

Editor's note: It is FFS whether a cause code for "None of the requested connectivity type(s) is authorized" is needed.

This subclause shows the numbers in the decimal numeration system.

8.2 IETF RFC coding information defined within present document

8.2.1 IPMS attributes

8.2.1.1 AT_IPMS_IND attribute

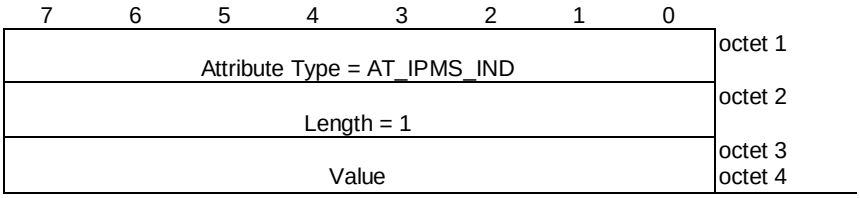

Figure 8.2.1.1: AT_IPMS_IND attribute

Table 8.2.1.1: AT_IPMS_IND attribute

Octet 1 indicates the type of attribute as AT_IPMS_IND with a value of 137.

Octet 2 is the length of this attribute which shall be set to 1 as per IETF RFC 4187 [33]

Octet 3 and 4 is the value of this attribute. Octet 3 is reserved and shall be coded as zero. Octet 4 shall be set as follows. All other values are reserved.

7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	Protocol Supported
0	0	0	0	0	0	0	1	DSMIPv6 only
0	0	0	0	0	0	1	0	NBM only
0	0	0	0	0	0	1	1	MIPv4 only
0	0	0	0	0	1	0	0	DSMIPv6 and NBM both supported
0	0	0	0	0	1	0	1	MIPv4 and NBM both supported
0	0	0	0	0	1	1	0	DSMIPv6 and NBM Supported;DSMIPv6 preferred
0	0	0	0	0	1	1	1	DSMIPv6 and NBM Supported; NBM preferred
0	0	0	0	1	0	0	0	MIPv4 and NBM supported; MIPv4 preferred
0	0	0	0	1	0	0	1	MIPv4 and NBM supported; NBM preferred
0	0	0	0	1	0	1	0	MIPv4 and DSMIPv6 supported; MIPv4 preferred
0	0	0	0	1	0	1	1	MIPv4 and DSMIPv6 supported; DSMIPv6 preferred
0	0	0	0	1	1	0	0	MIPv4, DSMIPv6 and NBM supported; MIPv4 preferred
0	0	0	0	1	1	0	1	MIPv4, DSMIPv6 and NBM supported; DSMIPv6 preferred
0	0	0	0	1	1	1	0	MIPv4, DSMIPv6 and NBM supported; NBM preferred

8.2.1.2 AT_IPMS_RES attribute

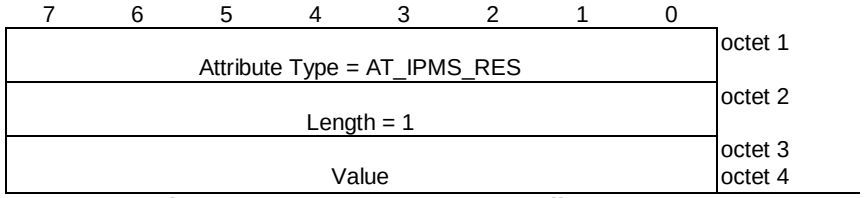

Figure 8.2.1.2: AT_IPMS_RES attribute.

Table 8.2.1.2: AT_IPMS_RES attribute

Octet 1 indicates the type of attribute as AT_IPMS_RES with a value of 138.

Octet 2 is the length of this attribute which shall be set to 1 as per IETF RFC 4187 [33]

Octet 3 and 4 is the value of this attribute. Octet 3 is reserved and shall be coded as zero. Octet 4 shall be set as follows. All other values are reserved.

7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	Protocol Selected
0	0	0	0	0	0	0	1	DSMIPv6
0	0	0	0	0	0	1	0	NBM
0	0	0	0	0	0	1	1	MIPv4

8.2.2 Access Network Identity indication attribute

8.2.2.1 Access Network Identity in the AT_KDF_INPUT attribute

The Access Network Identity is indicated in the Network Name Field of the AT_KDF_INPUT attribute as specified in IETF RFC 5448 [38]. The Network Name Field shall contain the Access Network Identity as specified in subclause 8.1.1 of this specification.

NOTE: IETF in IETF RFC 5448 [38] refers to this specification for the value of the Network Name field.

8.2.3 Trust relationship indication attribute

8.2.3.1 AT_TRUST_IND attribute

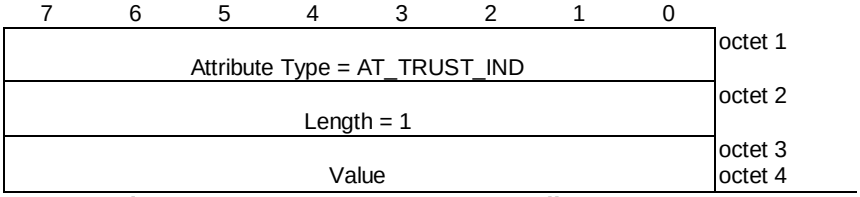

Figure 8.2.3.1-1: AT_TRUST_IND attribute

Table 8.2.3.1-1: AT_TRUST_IND attribute

Octet 1 indicates the type of attribute as AT_TRUST_IND with a value of 139.
Octet 2 is the length of this attribute which shall be set to 1 as per IETF RFC 4187 [33]
Octet 3 and 4 is the value of the attribute. Octet 3 is reserved and shall be coded as zero. Octet 4 shall be set as follows. All other values are reserved.

7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	Indicated Trust Relationship
0	0	0	0	0	0	0	1	Trusted
0	0	0	0	0	0	1	0	UnTrusted

8.2.4 IKEv2 Configuration Payloads attributes

8.2.4.1 HOME_AGENT_ADDRESS attribute

The HOME_AGENT_ADDRESS attribute is shown in figure 8.2.4.1-1. The length of the HOME_AGENT_ADDRESS attribute is 16 or 20 bytes. The IPv4 Home Agent Address field is optional. The HA's IPv6 and IPv4 addresses are laid out respectively in IPv6 Home Agent Address and IPv4 Home Agent Address fields in big endian order (aka most significant byte first, or network byte order), see IETF RFC 5996 [28].

Bits								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**Octets**
R	Attribute Type							1
Attribute Type								2
Length								3, 4
IPv6 Home Agent Address								5 - 20
IPv4 Home Agent Address								21 - 24

Figure 8.2.4.1-1: HOME_AGENT_ADDRESS attribute

The R bit in the first octet is defined in IETF RFC 5996 [28].

The Attribute Type indicating HOME_AGENT_ADDRESS is of the value 19.

8.2.5 Full name for network and short name for network

8.2.5.1 AT_FULL_NAME_FOR_NETWORK attribute

The AT_FULL_NAME_FOR_NETWORK attribute is coded according to figure 8.2.5.1-1 and table 8.2.5.1-1.

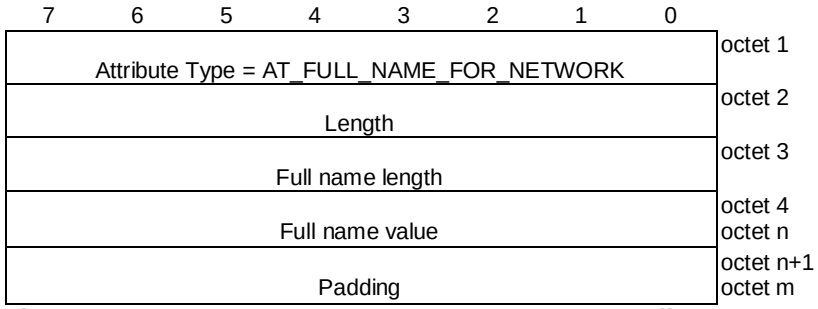

Figure 8.2.5.1-1: AT_FULL_NAME_FOR_NETWORK attribute

Table 8.2.5.1-1: AT_FULL_NAME_FOR_NETWORK attribute

Octet 1 indicates the type of this attribute as AT_FULL_NAME_FOR_NETWORK with a value of 141. Octet 2 is the length of this attribute in multiples of 4 octets as specified in RFC 4187 [33]. Octet 3 is the full name length field and contains the length of the full name value field in octets. The full name value field starts at octet 4 and its length is indicated by the full name length field. The full name value field indicates the "full length name of the network" that the network wishes the UE to associate with MCC and MNC in the realm of the NAI used during authentication. The structure of the full name value field is the same as the structure of the Network Name defined in 3GPP TS 24.008 [46] subclause 10.5.3.5a except for the Network Name IEI and the Length of Network Name contents which are not included. The optional padding field starts after the last octet of the full name value field. Each octet of this field is set to zero by sending entity and ignored by receiving entity.

8.2.5.2 AT_SHORT_NAME_FOR_NETWORK attribute

The AT_SHORT_NAME_FOR_NETWORK attribute is coded according to figure 8.2.5.2-1 and table 8.2.5.2-1.

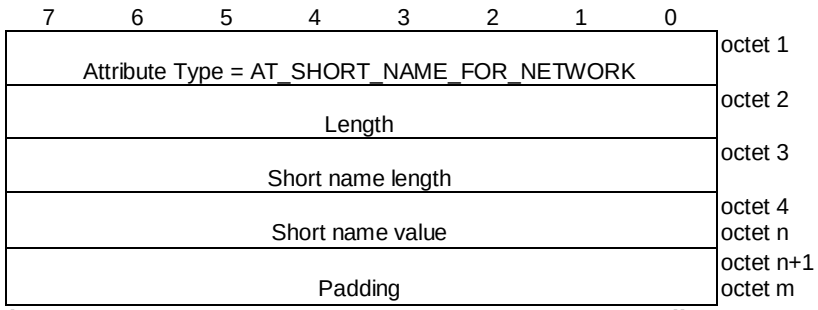

Figure 8.2.5.2-1: AT_SHORT_NAME_FOR_NETWORK attribute

Table 8.2.5.2-1: AT_SHORT_NAME_FOR_NETWORK attribute

Octet 1 indicates the type of this attribute as AT_SHORT_NAME_FOR_NETWORK with a value of 140. Octet 2 is the length of this attribute in multiples of 4 octets as specified in RFC 4187 [33]. Octet 3 is the short name length field and contains the length of the short name value field in octets. The short name value field starts at octet 4 and its length is indicated by the short name length field. The short name value field indicates the "abbreviated name of the network" that the network wishes the UE to associate with MCC and MNC in the realm of the NAI used during authentication. The structure of the short name value field is the same as the structure of the Network Name defined in 3GPP TS 24.008 [46] subclause 10.5.3.5a except for the Network Name IEI and the Length of Network Name contents which are not included. The optional padding field starts after the last octet of the short name value field. Each octet of this field is set to zero by sending entity and ignored by receiving entity.

8.2.6 Handling of the unknown protocol data

If the receiving entity receives an unknown value in a recognized skippable attribute in an EAP-AKA or EAP-AKA' message, the receiving entity shall ignore the attribute and shall handle the rest of the message. The definition of skippable attribute see the RFC 4187 [33]. The receiving entity handling of the unrecognized skippable attribute is as specified in RFC 4187 [33].

8.2.7 Attributes for TWAN connection modes

8.2.7.1 AT_TWAN_CONN_MODE attribute

The AT_TWAN_CONN_MODE attribute is coded according to figure 8.2.7.1-1 and table 8.2.7.1-1.

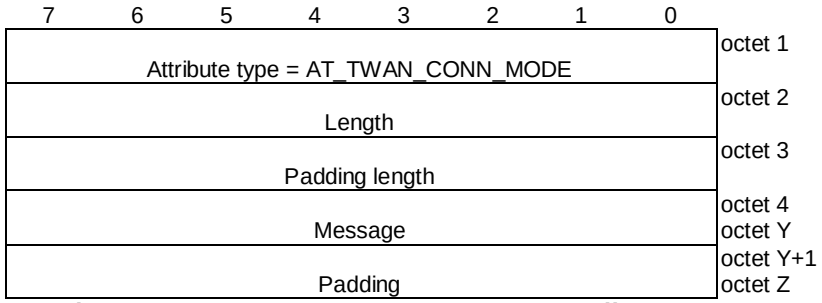

Figure 8.2.7.1-1: AT_TWAN_CONN_MODE attribute

Table 8.2.7.1-1: AT_TWAN_CONN_MODE attribute

Octet 1 indicates the type of attribute as AT_TWAN_CONN_MODE with a value of xxx. This attribute is skippable. Octet 2 is the length of this attribute in multiples of 4 octets as specified in RFC 4187 [33]. Padding length field contains the length of the padding field. Message field is coded according to subclause 8.1.4.1. The length of the message field is determined from the length field and the padding length field. Each octet of the padding field is set to zero by sending entity and ignored by receiving entity.

Annex A (informative): Example signalling flows for inter-system change between 3GPP and non-3GPP systems using ANDSF

A.1 Scope of signalling flows

This annex gives examples of signalling flows for mobility between 3GPP and non-3GPP systems. These signalling flows provide as example detailed information on Network Discovery and Selection aspects involving the use of ANDSF.

A.2 Signalling flow for inter-system change between 3GPP access network and non-3GPP access network

Figure A1 below shows an inter-system change procedure between 3GPP access network and non-3GPP access network using information obtained from ANDSF.

In this example the UE uses DHCP query to obtain the IP address of the ANDSF.

In this example flow, the communication between the UE and ANDSF does not imply use of any specific protocol.

The steps involved in inter-system change between 3GPP access network and non-3GPP access network are as follows.

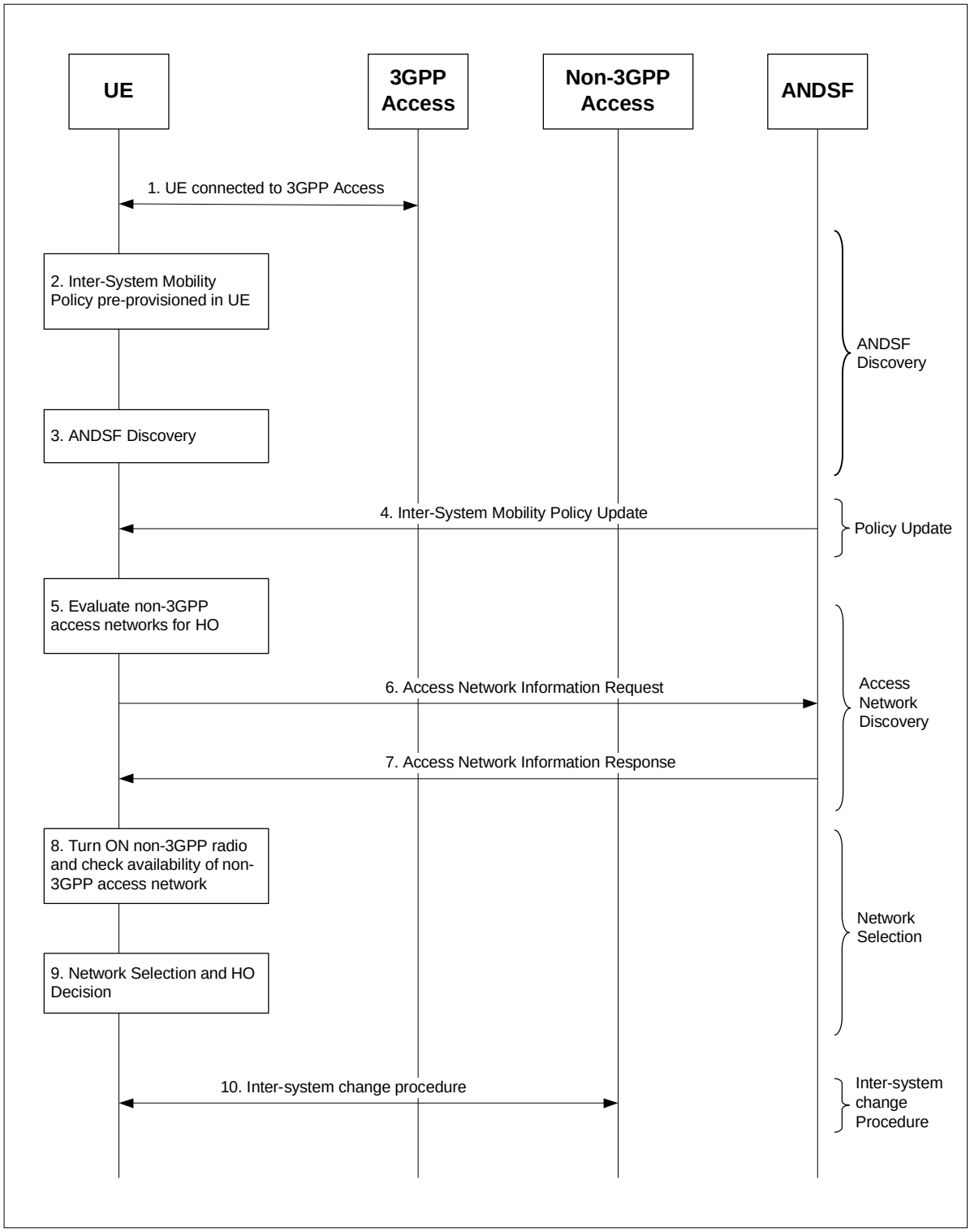

Figure A1. Procedure for Inter-system change between 3GPP access and non-3GPP using ANDSF

1. Initial connectivity

The UE is connected to 3GPP network. The current applications are supported over the 3GPP access network.

NOTE: The procedure remains the same if the UE is initially connected to non-3GPP access network and wants to change to 3GPP access network.

2. **Pre-provisioned policies**

   The inter-system mobility policy is pre-provisioned on the UE. Based on pre-provisioned operator policies the UE has preference for different non-3GPP networks such as WLAN, and WiMAX. The UE can select these access networks when they are available.

3. **ANDSF Discovery**

   ANDSF discovery is performed as described in subclause 6.8.2.2.1. The UE can discover ANDSF using DHCP query options as specified in IETF RFC 6153 [37], where ANDSF may be identified with a specific sub-option code. Optionally, the home operator can use OMA-DM's bootstrap mechanism as specified in OMA-ERELD-DM-V1_2 [39] to provide ANDSF information and security parameters for application layer authentication. Transport security is ensured by establishing an https tunnel between the UE and ANDSF,

4. **Policy Update based on Network Triggers**

   Based on network triggers the ANDSF sends an updated inter-system mobility policy to the UE. The inter-system mobility policy includes validity conditions, i.e. conditions indicating when the policy is valid. Such conditions can include time duration, location area, etc.

5. **Evaluate which non-3GPP networks to discover**

   The inter-system mobility policies specify the access networks that the UE can select; the UE has both WLAN and WiMAX radios. In this case, the inter-system mobility policy provided by the operator allows the UE to select either WLAN or WiMAX networks under all conditions. The UE, taking into account of the UE's local policy, e.g. user preference settings, access history, obtains information about availability of both WLAN and WiMAX access networks in its vicinity.

6. **Access Network Information Request**

   The UE sends a request to ANDSF to get information about available access networks. The UE also includes its location information in the request. ANDSF can limit the information sent to UE based on internal settings.

7. **Access Network Information Response**

   The ANDSF sends a response to the UE which includes the list of available access networks types (in order of operator preferences), access network identifier and PLMN identifier. In this case the ANDSF responds with availability of both WLAN and WiMAX network in the vicinity of the UE.

8. **Evaluate candidate non-3GPP networks**

   Based on the received information and UE's local policy, the UE evaluates if it is within the coverage area of the available access networks in the order of preferences. In this case,based on the history and radio quality of WiMAX, the UE prefers WiMAX over WLAN access type. The UE powers on the WiMAX radio and checks for the presence of WiMAX network. The UE can listen to WiMAX broadcast messages (uplink/downlink channel data messages) and determines the presence of WiMAX network. Since the WiMAX network is the preferred network and since the UE has verified the presence of WiMAX network, the UE does not check for presence of WLAN network.

9. **Non-3GPP Network Selection**

   The UE selects the most preferred available access network for inter-system mobility. In this case the UE selects the WiMAX access network.

10. **Inter-system change Procedure**

    The UE initiates inter-system change procedure to the selected non-3GPP access network. The details of the inter-system change procedure are described elsewhere, see 3GPP TS 23.402 [6].

Annex B (informative): Assignment of Access Network Identities in 3GPP

This annex describes the recommended assignment procedure of Access Network Identities within 3GPP.

B.1 Access Network Identities

According to 3GPP TS 23.003 [3] the encoding of the Access Network Identity is specified within 3GPP, but the Access Network Identity definition for each non-3GPP access network is under the responsibility of the corresponding standardisation organisation respectively.

If a standardisation organisation for a non-3GPP access network determines they need to define a new Access Network Identity Prefix or additional ANID strings, they can contact the 3GPP TSG-CT WG 1 via a Liaison Statement and indicate the specific values of the Access Network Identity Prefixes or the specific values of, or construction principles for, the additional ANID strings to be specified by 3GPP and give reference to the corresponding specification(s) of the requesting organisation. 3GPP TSG CT WG 1 will then specify the values for the Access Network Identities by updating Table 8.1.1.2 in this specification and inform the requesting standardisation organisation.

Annex C (informative): Example usage of ANDSF

C.1 Scope of ANDSF Example

This Annex gives an example of organization of ANDSF database and how it can be used to discover access network information. In this example the UE is in 3GPP network and is trying to discover available WiMAX networks. The ANDSF database is provided by the 3GPP operator with PLMN = PLMN_3GPP.

C.2 Organization of ANDSF Coverage Map for WiMAX Network discovery

Table C1 illustrates the organization of ANDSF database for discovering WiMAX and WiFi networks. The ANDSF database provides the coverage mapping information for WiMAX and WiFi networks based on 3GPP cell identifiers. In this example the UE_Location can be specified either in terms of 3GPP parameters (PLMN + Cell Identifier) or in terms of geo spatial co-ordinates.

Table C1: ANDSF Database Organization for PLMN = PLMN_3GPP

UE_Location - 3GPP (CellId) - Other (Geopriv)	**AccessType = WiMAX**	**AccessType = WiFi**
Locn_1 Cell_Id = Cell_1	NSP-ID= NSP_1: -NAP_ID = NAP_1 -NAP_ID = NAP_2 NSP-ID = NSP_2 -NAP_ID = NAP_2 -NAP_ID = NAP_3	SSID = WiFi1, BSSID = BS1 SSID = WiFi2, BSSID = BS2
Locn_2 Cell_Id = Cell_2	NSP-ID = NSP_2 - NAP_ID = NAP_3	N/A
Locn_3 Cell_Id = Cell_3	N/A	SSID = WiFi1, BSSID = BS3 SSID = WiFi4, BSSID = BS4
…..	…….	…….
Locn_n Cell_Id = Cell_n	NSP-ID = NSP_1 NAP_ID = NAP_2	SSID = WiFi6, BSSID = BS5

For WiMAX network the database provides information about WiMAX NSP and NAP that provide coverage in respective 3GPP cells. Thus for example in 3GPP Cell_1, WiMAX Service provider NSP_1 provides service to WiMAX radio access providers NAP_1 and NAP-2. Similarly WiMAX Service Provider NSP_2 provides service to Network access providers NAP-2 and NAP_3 as well. Similarly in 3GPP Cell_2 WiMAX Network Service Provider NSP_2 provides service to network Access Provider NAP_3. Further it can be seen that no WiMAX coverage is available in 3GPP cell Cell_3.

C.3 Parameters in Pull mode

The UE is currently in 3GPP network. The UE sends a query to OMA ANDSF server as follows:

ANDSF_Query (UE_Location, AccessNetworkType=WiMAX)

The UE specifies the UE_Location information in terms of current 3GPP Cell Id (e.g. Cell_2)

On receipt of the query message the ANDSF looks up the UE_Location (Cell_2) in the ANDSF database and searches for a prospective WiMAX entry. In this case the ANDSF retrieves WiMAX Service provider identifier (NSP-ID) NSP_2 and WiMAX Network Access Provider Identifier (NAP-ID) NAP_3. The ANDSF retrieves the network

parameters for this combination. The ANDSF fills these parameters in the WNDS MO and sends the information back to the UE.

ANDSF_Response (UE_Location, AccessNetworkInformationRef MO=WIMAXNDS).

Annex D (informative): Mismatch of static configuration of mobility mechanism in the UE and in the network

This annex describes the possible cases of mismatch between the statically configured mobility mechanisms in the UE and in the EPC as shown in table D1. Additionally the table shows whether the UE would be able to access EPC services as a consequence of the mismatch.

Table D1: Mismatch of static configuration of mobility mechanism in the UE and in the network

	NBM configured in the network	DSMIPv6 configured in the network	MIPv4 configured in the network
NBM configured in the UE	No mismatch	Mismatch. The UE is not able to access EPC services because the UE configures a local IP address and there is no connectivity to the PGW in the EPC. Depending on operator's policy and roaming agreements, local IP access services (e.g. Internet access) can be provided in the non-3GPP network using the local IP address. However, such local IP access services, where the user traffic does not traverse the EPC, are not described in this specification.	Mismatch. The UE is not able to access EPC services because the UE does not support communication with the Foreign Agent in the trusted non-3GPP network.
DSMIPv6 configured in the UE	Mismatch. The UE can be able to access EPC services. After attach to the non-3GPP network, the UE is on the home link and configures an IP address based on the HNP, however in some cases the UE cannot detect the home link. Since the UE is configured with DSMIPv6, the UE would initiate a DSMIPv6 bootstrapping: - If the network offers a HA function to the UE and if the bootstrapping is successful, the UE detects that it is attached to the home link. Depending of the UE capabilities and the network configuration, the UE can access EPC services via the S2a/S2b interface, but session continuity is not supported. - If the network does not offer a HA function or if the bootstrapping to the HA is not successful, the UE is not able to receive its Home Network Prefix and hence the UE cannot detect that it is on the home link. If no APN bound to the configured IP address was received and the access network doesn't support APN delivery, the UE would not recognize the mismatch and cannot access EPC services. If the access network supports APN delivery and the configured IP address is bound to an APN, the UE can access EPC services.	No mismatch	Mismatch. The UE is not able to access EPC services because the UE does not support communication with the Foreign Agent in the trusted non-3GPP network.
MIPv4 configured in the UE	Mismatch. The UE is not able to access EPC services because no Foreign Agent functionality is supported in the non-3GPP access network.	Mismatch. The UE is not able to access EPC services because no Foreign Agent functionality is supported in the non-3GPP access network.	No mismatch

Annex E (informative): UE procedures based on preconfigured and received information

The flow diagrams in figure E-1 and figure E-2 show examples of the procedures that the UE can follow in order to establish a PDN connection based on information available to the UE about the authentication method, received or pre-configured access network trust relationship information or received or preconfigured IP mobility mode selection information.

The following symbols are used:

AN_TRUST	trust relationship between the non-3GPP access network and the 3GPP EPC, considered to be applicable by the UE
IPMM	IP mobility mode, considered applicable by the UE

Initially, at the entry to flow chart the UE has established contact with the non-3GPP access network, but the UE does not know whether it is in a trusted or untrusted access network.

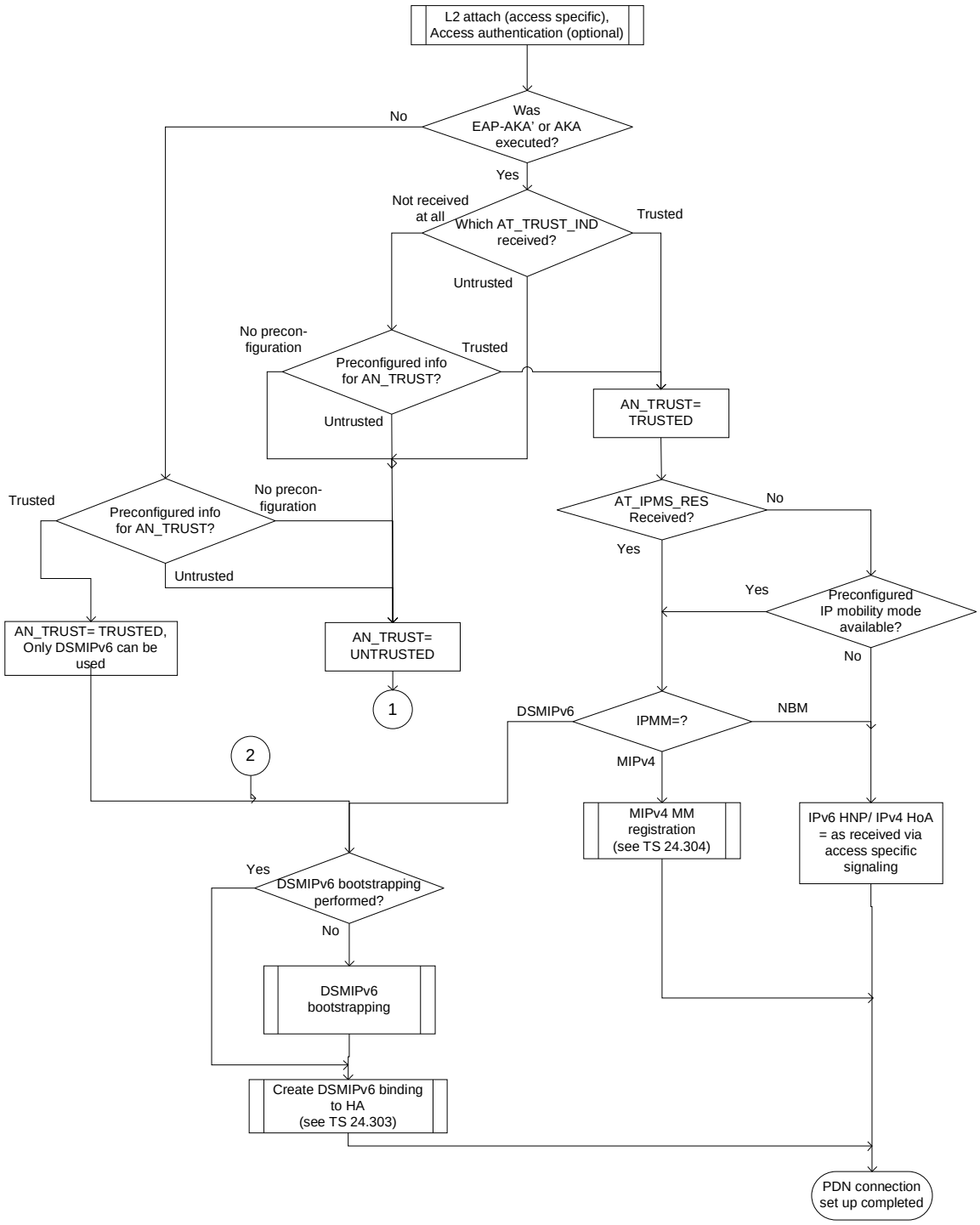

Figure E-1. Procedures to be followed by the UE depending on received and preconfigured information - part 1

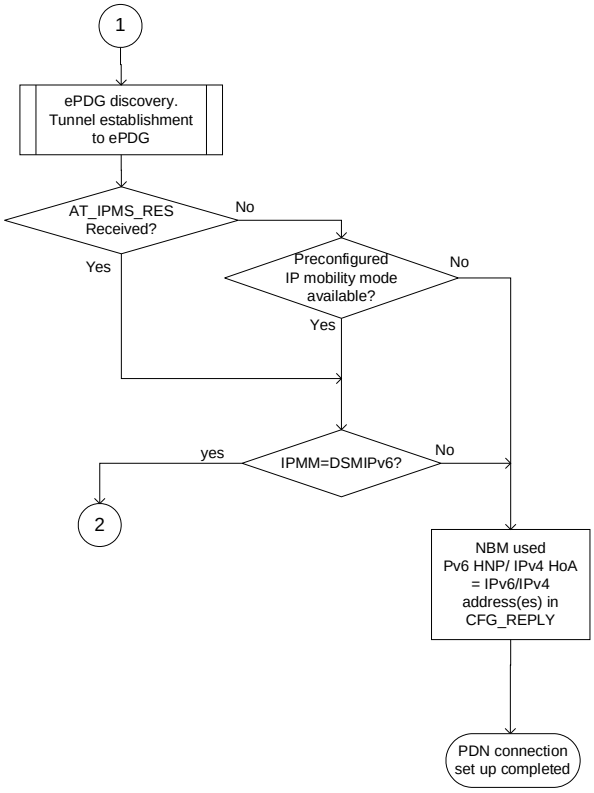

Figure E-2. Procedures to be followed by the UE depending on received and preconfigured information - part 2

Annex F (Normative): Access to EPC via restrictive non-3GPP access network

F.1 General

This annex specifies protocol for access to EPC via restrictive non-3GPP access network.

The procedures are specified for UE and ePDG. The UE may support the procedures for access to EPC via restrictive non-3GPP access network. The ePDG may support the procedures for access to EPC via restrictive non-3GPP access network.

F.2 UE – EPC network protocols

F.2.1 General

In order to access to EPC via restrictive non-3GPP access network, the UE and the ePDG shall establish a firewall traversal tunnel (FTT) using the UE requested FTT establishment procedure according to subclause F.2.2. Once the FTT is established, the UE shall initiate establishment of an IPSec tunnel via an IKEv2 protocol exchange according to IETF RFC 5996 [28].

The UE and the ePDG shall construct the IKEv2 messages according to clause 7 and according to subclause F.2.3.

The UE and the ePDG shall send the IKEv2 messages using the IKEv2 message transport procedure according to subclause F.2.2.3.

The UE and the ePDG shall send the encapsulating security payloads using the encapsulating security payload transport procedure according to subclause F.2.2.4.

If the UE has not sent a message over the FTT in the last FTT KAT seconds, the UE shall perform the UE requested keep-alive procedure according to subclause F.2.2.5.

When all IKEv2 security associations are closed, the UE shall perform the UE requested FTT release procedure according to subclause F.2.2.6.

When all IKEv2 security associations are closed, the network can perform the network requested FTT release procedure according to subclause F.2.2.7.

F.2.2 FTT protocol

F.2.2.1 General

The FTT protocol consists of the UE requested FTT establishment procedure, the IKEv2 message transport procedure, the encapsulating security payload transport procedure, the UE requested keep-alive procedure, the UE requested FTT release procedure and the network requested FTT release procedure.

F.2.2.2 UE requested FTT establishment procedure

F.2.2.2.1 General

The purpose of the UE requested FTT establishment procedure is to establish an FTT between the UE and the ePDG.

F.2.2.2.2 UE requested FTT establishment procedure initiation

If the UE is not configured with an HTTP proxy address, the UE shall follow the procedures in subclause F.2.2.2.3.

If the UE is configured with an HTTP proxy address, the UE shall follow the procedures in subclause F.2.2.2.4.

NOTE: UE configuration of an HTTP proxy address is out of scope of 3GPP.

F.2.2.2.3 UE requested FTT establishment procedure initiation via restrictive non-3GPP access network type I

In order to establish an FTT, the UE shall establish a TCP connection to the ePDG address and destination port 443. If the ePDG address is a FQDN, the UE shall include a TLS extension of type "server_name" in the TLS client hello message according to IETF RFC 6066 [55].

If the TCP connection establishment is successful, the UE shall establish a TLS connection over the TCP connection according to IETF RFC 5246 [54].

The ePDG shall handle the TCP connection setup and shall handle the TLS connection establishment according to IETF RFC 5246 [54].

F.2.2.2.4 UE requested FTT establishment procedure initiation via restrictive non-3GPP access network type II

If the UE is configured with HTTP proxy address, in order to establish an FTT, the UE shall send HTTP CONNECT request to the HTTP proxy address according to IETF RFC 2817 [53]. The UE shall populate Request-URI of the HTTP CONNECT request with the ePDG address and port 443.

Upon receiving HTTP 2xx response to HTTP CONNECT request, the UE shall establish TLS connection according to IETF RFC 5246 [54] over the TCP connection used for the HTTP CONNECT request transport. If the ePDG address is a FQDN, the UE shall include a TLS extension of type "server_name" in the TLS client hello message according to IETF RFC 6066 [55].

The ePDG shall handle the TCP connection setup and the TLS connection establishment according to IETF RFC 5246 [54].

F.2.2.2.5 UE requested FTT establishment procedure accepted by the network

When TLS Finished message is sent over the TCP connection according to IETF RFC 5246 [54], the ePDG shall use the connection as the FTT.

When valid TLS Finished message is received over the TCP connection, the UE shall use the connection as the FTT.

F.2.2.3 IKEv2 message transport procedure

F.2.2.3.1 General

The purpose of the IKEv2 message transport procedure is to transport an IKEv2 message over an FTT.

F.2.2.3.2 IKEv2 message transport procedure initiation

In order to send an IKEv2 message, the UE or the ePDG shall create an IKEv2 envelope as described in subclause F.3.2.2, shall populate the Non-ESP marker field with zero value and shall populate the IKEv2 message field of the IKEv2 envelope with the IKEv2 message.

The UE shall send the IKEv2 envelope as TLS application data according to IETF RFC 5246 [54]:

- if the IKEv2 message is an IKEv2 request, over an FTT of the UE; and
- if the IKEv2 message is an IKEv2 response of an IKEv2 request, over the FTT over which the IKEv2 request was received.

The ePDG shall send the IKEv2 envelope as TLS application data according to IETF RFC 5246 [54]:

- if the IKEv2 message is an IKEv2 request of an IKEv2 security association, over the FTT associated with the IKEv2 security association; and
- if the IKEv2 message is an IKEv2 response of an IKEv2 request, over the FTT over which the IKEv2 request was received.

F.2.2.3.3 IKEv2 message transport procedure accepted

Upon receiving the IKEv2 envelope as TLS application data over the FTT, the ePDG or the UE shall extract the IKEv2 message from the IKEv2 envelope as described in subclause F.3.2.2 and shall handle it according to IETF RFC 5996 [28]. If the IKEv2 message is a validated IKEv2 packet, the ePDG shall associate the FTT with the IKEv2 security association of the validated packet (replacing any FTT previously associated with the IKEv2 security association).

F.2.2.4 Encapsulating security payload transport procedure

F.2.2.4.1 General

The purpose of the encapsulating security payload transport procedure is to transport an encapsulating security payload over an FTT.

F.2.2.4.2 Encapsulating security payload transport initiation

In order to send an encapsulating security payload, the UE or the ePDG shall create a ESP envelope as described in subclause F.3.2.3 and shall populate the ESP message field of the ESP envelope with the encapsulating security payload.

The UE shall send the ESP envelope as TLS application data according to IETF RFC 5246 [54] over an FTT of the UE.

The ePDG shall send the ESP envelope as TLS application data according to IETF RFC 5246 [54] over the FTT associated with the IKEv2 security association which established the child security association of the encapsulating security payload.

F.2.2.4.3 Encapsulating security payload transport accepted

Upon receiving the ESP envelope over the FTT, the ePDG or the UE shall extract the encapsulating security payload from the ESP envelope as described in subclause F.3.2.3 and shall handle it according to IETF RFC 4303 [32].

F.2.2.5 UE requested keep-alive procedure

F.2.2.5.1 General

The purpose of the UE requested keep-alive procedure is to refresh binding in firewall (possibly including NAT) deployed between the restrictive non-3GPP access network and the EPC.

F.2.2.5.2 UE requested keep-alive procedure initiation

In order to send a keep-alive, the UE shall create a keep-alive envelope as described in subclause F.3.2.4.

The UE shall send the keep-alive envelope as TLS application data according to IETF RFC 5246 [54] over an FTT of the UE.

F.2.2.5.3 UE requested keep-alive procedure accepted by the network

The ePDG shall discard any keep-alive envelope received over the FTT.

F.2.2.6 UE requested FTT release procedure

F.2.2.6.1 General

The purpose of the UE requested FTT release procedure is to release an FTT when all IKEv2 security associations are closed.

F.2.2.6.2 UE requested FTT release procedure initiation

In order to release the FTT, the UE shall send TLS close_notify alert according to IETF RFC 5246 [54].

F.2.2.6.3 UE requested FTT release procedure accepted by the network

The ePDG shall handle the TLS close_notify alert according to IETF RFC 5246 [54].

F.2.2.7 Network requested FTT release procedure

F.2.2.7.1 General

The purpose of the network requested FTT release procedure is to release an FTT when all IKEv2 security associations are closed.

F.2.2.7.2 Network requested FTT release procedure initiation

In order to release the FTT, the ePDG shall send TLS close_notify alert according to IETF RFC 5246 [54].

F.2.2.7.3 Network requested FTT release procedure accepted by the UE

The UE shall handle the TLS close_notify alert according to IETF RFC 5246 [54].

F.2.3 Additional IKEv2 procedures when FTT is used

F.2.3.1 FTT KAT negotiation during tunnel establishment

The UE shall include the FTT_KAT configuration attribute according to subclause F.3.3.1 in the IKEv2 CFG_REQUEST configuration payload of the IKE_AUTH request message sent via FTT.

If the FTT_KAT configuration attribute is included in the IKEv2 CFG_REQUEST configuration payload, ePDG shall include the FTT_KAT configuration attribute according to subclause F.3.3.1 in the IKEv2 CFG_REPLY configuration payload.

If the FTT_KAT configuration attribute is not included in the IKEv2 CFG_REPLY configuration payload, the UE shall determine the firewall traversal tunnel keep-alive time (FTT KAT) as a random number uniformly distributed between lower bound and higher bound. The default value for lower bound is 672 seconds and the default value for higher bound is 840 seconds.

If the FTT_KAT configuration attribute is included in the IKEv2 CFG_REPLY configuration payload, the UE shall set the FTT KAT to the value of the Keep-alive time field of the FTT_KAT configuration attribute.

F.3 PDUs and parameters specific to the present annex

F.3.1 Void

F.3.2 Message types of FTT messages

F.3.2.1 Generic FTT envelope

Generic FTT envelope is coded according to figure F.3.2.1-1 and table F.3.2.1-1.

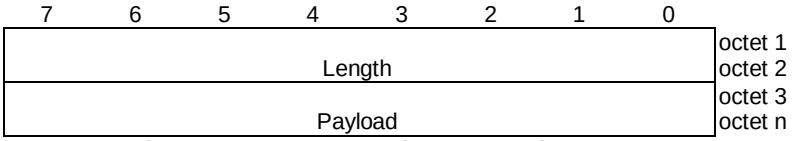

Figure F.3.2.1-1: Generic FTT envelope

Table F.3.2.1-1: Generic FTT envelope

Length field is in the octet 1 and the octet 2. The Length field indicates the length of the generic FTT envelope in octets. Payload field is in octets starting from octet 3 and its value depends on the message type.

F.3.2.2 IKEv2 envelope

IKEv2 envelope is coded according to figure F.3.2.2-1 and table F.3.2.2-1.

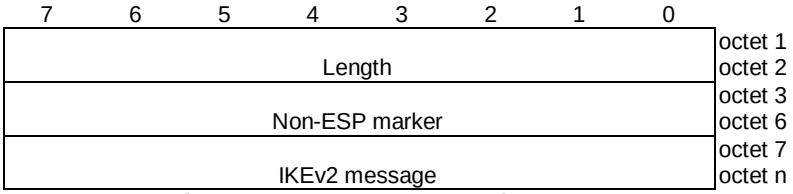

Figure F.3.2.2-1: IKEv2 envelope

Table F.3.2.2-1: IKEv2 envelope

Length field is described in subclause F.3.2.1. The Length field value is bigger than 6. Non-ESP marker field is in the octet 3, the octet 4, the octet 5 and the octet 6. The Non-ESP marker field value is zero. IKEv2 message field is in octets starting from octet 7. The IKEv2 message contains the IKEv2 message as defined in IETF RFC 5996 [28], section 3.1 in format as for transmission from UDP port 500.

F.3.2.3 ESP envelope

ESP envelope is coded according to figure F.3.2.3-1 and table F.3.2.3-1.

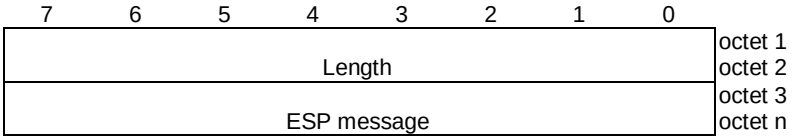

Figure F.3.2.3-1: ESP envelope

Table F.3.2.3-1: ESP envelope

Length field is described in subclause F.3.2.1. The Length field value is bigger than 6. ESP message field is in octets starting from octet 3. The ESP message contains the encapsulating security payload as defined in IETF RFC 4303 [32], section 2. The SPI field in the ESP header is not a zero value.

F.3.2.4 Keep-alive envelope

Keep-alive envelope is coded according to figure F.3.2.4-1 and table F.3.2.4-1.

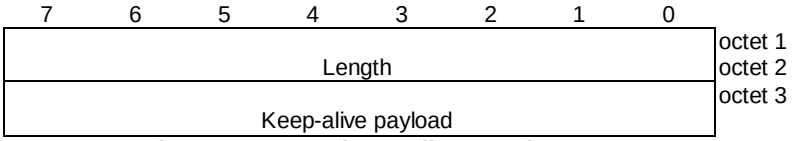

Figure F.3.2.4-1: keep-alive envelope

Table F.3.2.4-1: keep-alive envelope

Length field is described in subclause F.3.2.1. The Length field value is 3. Keep-alive payload field is in octet 3. The Keep-alive payload field value is 255.

F.3.3 IKEv2 configuration attributes

F.3.3.1 FTT_KAT configuration attribute

The FTT_KAT configuration attribute is coded according to figure F.3.3.1-1 and table F.3.3.1-1.

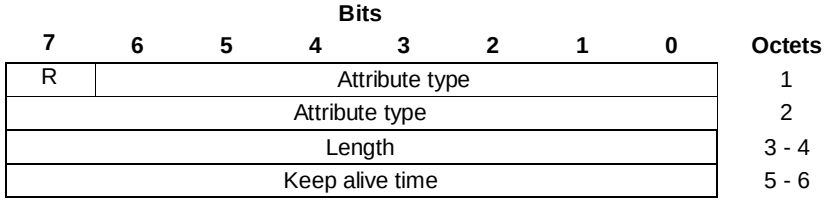

Figure F.3.3.1-1: FTT_KAT configuration attribute

Table F.3.3.1-1: FTT_KAT configuration attribute

R field is defined in IETF RFC 5996 [28]. Attribute type field has value XXX. Length field is defined in IETF RFC 5996 [28]. When FTT_KAT configuration attribute is included in the CFG_REQUEST configuration payload of IKEv2 security association, packets of which are transported via FTT, the Keep-alive time field indicates preferred maximum time in seconds between two envelopes (any of those described in subclause F.3.2) sent via FTT. When FTT_KAT configuration attribute is included in the CFG_REPLY configuration payload of IKEv2 security association, packets of which are transported via FTT, the Keep-alive time field indicates actual maximum time in seconds between two envelopes (any of those described in subclause F.3.2) sent via FTT.

Editor's note (WID: TURAN-CT, CR#0243): MCC is requested to register this IKEv2 configuration attribute with IANA when the TURAN-CT work item progress reaches 100%. The registration policy is "expert review" according to http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xml#ikev2-parameters-21

Annex G (Informative): IANA registrations

G.1 General

This annex contains information needed for registrations with IANA.

G.2 EAP-AKA attributes

G.2.1 General

This subclause contains information needed for registrations of EAP-AKA attributes with IANA.

G.2.2 AT_TWAN_CONN_MODE EAP-AKA attribute

Editor's note (WI eSaMOG_St3, CR#0248): when eSaMOG WI progress reaches 100%, MCC is requested to register the AT_TWAN_CONN_MODE attribute with IANA . After the AT_TWAN_CONN_MODE attribute is registered by IANA, this subclause can be removed. IANA registration policy is "Specification Required" according to http://www.iana.org/assignments/eapsimaka-numbers/eapsimaka-numbers.xhtml#eapsimaka-numbers-3 so RFC is not needed.

In order to register the AT_TWAN_CONN_MODE attribute, the following information will be inserted in form at http://www.iana.org/cgi-bin/assignments.pl:

Contact name:

<MCC Name>

Contact Email:

<MCC email>

What type of assignment/registration are you requesting?

New item in the "Attribute Types (Skippable Attributes 128-255)" of the "EAP-AKA and EAP-SIM Parameters" as shown at http://www.iana.org/assignments/eapsimaka-numbers/eapsimaka-numbers.xml#eapsimaka-numbers-3 and as specified in RFC 4187.

Which registry are you requesting this assignment/registration be made in?

The "Attribute Types (Skippable Attributes 128-255)" of the "EAP-AKA and EAP-SIM Parameters" as shown at http://www.iana.org/assignments/eapsimaka-numbers/eapsimaka-numbers.xml#eapsimaka-numbers-3 and as specified in RFC 4187.

If possible, please give a brief description of why you need this assignment/registration:

Further information needs to be provided during authentication using EAP-AKA'.

Additional Information. Please include a reference to the specification or RFC (if available) that defines this number or name space:

RFC 4187 defines the registry for the "Attribute Types (Skippable Attributes 128-255)" of the "EAP-AKA and EAP-SIM Parameters".

The following attribute is requested to be registered:

- numbering space: EAP-AKA and EAP-SIM Parameters, Attribute Types (Skippable Attributes 128-255)
- attribute description: AT_TWAN_CONN_MODE
- reference to specification where the attribute is described: http://www.3gpp.org/ftp/Specs/html-info/24302.htm
- attribute type: (number to be assigned by IANA)

Annex H (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2008-01					Draft skeleton provided in C1-080125 by rapporteur to CT1#51.		0.0.0
2008-02	CT1#51				Includes the following contribution agreed by CT1 at CT1#51: C1-080568	0.0.0	0.1.0
2008-02	CT1#51 bis				Includes the following contributions agreed by CT1 at CT1#51 bis: C1-080722, C1-080765, C1-080773, C1-080783, C1-080792, C1-080793	0.1.0	0.2.0
2008-04	CT1#52				Includes the following contributions agreed by CT1 at CT1#52:- C1-080921, C1-081391, C1-081392, C1-081393, C1-081394	0.2.0	0.3.0
2008-04	email review				Incomplete implementation C1-080921	0.3.0	0.3.1
2008-05	CT1#53				Includes the following contributions agreed by CT1 at CT1#53:- C1-081575, C1-082019, C1-082066, C1-082067, C1-082074, C1-082077, C1-082078, C1-082086, C1-082091, C1-082092, C1-082093.	0.3.1	0.4.0
2008-06	CT1#54				Includes the following contributions agreed by CT1 at CT1#54:- C1-082470, C1-082563, C1-082567, C1-082569, C1-082688, C1-082803, C1-082804, C1-082809.	0.4.0	0.5.0
2008-08	CT1#55				Includes the following contributions agreed by CT1 at CT1#55:- C1-082923, C1-082982, C1-083084, C1-083171, C1-083179, C1-083262, C1-083466, C1-083480, C1-083481, C1-083512, C1-083513, C1-083514, C1-083526, C1-083603, C1-083617	0.5.0	0.6.0
2008-09					Version 1.0.0 created for presentation to TSG CT#41 for information	0.6.0	1.0.0
2008-10	CT1#55bis				Includes the following contributions agreed by CT1 at CT1#55bis:- C1-083851; C1-083976; C1-084155; C1-084383; C1-084385; C1-084386; C1-084387; C1-084388; C1-084391; C1-084393; C1-084394; C1-084395; C1-084396; C1-084482	1.0.0	1.1.0
2008-11	CT1#56				Includes the following contributions agreed by CT1 at CT1#56:- C1-084934; C1-085322; C1-085327; C1-085328; C1-085329; C1-085331; C1-085333; C1-085335; C1-085336; C1-085338; C1-085516; C1-085526; C1-085534 Editorial corrections by the rapporteur to align with drafting rules	1.1.0	1.2.0
2008-11					Version 2.0.0 created for presentation to CT#42 for approval	1.2.0	2.0.0
2008-12	CT#42				Version 8.0.0 created after approval in CT#42	2.0.0	8.0.0
2009-03	CT#43	CP-090129	0001	2	Rapporteur's cleanup of editorial and typo mistakes	8.0.0	8.1.0
2009-03	CT#43	CP-090131	0002		Trust Relationship Detection	8.0.0	8.1.0
2009-03	CT#43	CP-090130	0005	1	Removing redundant and out-of-date editor's notes	8.0.0	8.1.0
2009-03	CT#43	CP-090129	0006	1	Missing specification text on WIMAX ANID	8.0.0	8.1.0
2009-03	CT#43	CP-090125	0007	3	ANDSF discovery and bootstrapping	8.0.0	8.1.0
2009-03	CT#43	CP-090127	0008	1	Corrections for authentication in trusted and untrusted access	8.0.0	8.1.0
2009-03	CT#43	CP-090128	0009	2	Incorrect protocol type and wrong reference	8.0.0	8.1.0
2009-03	CT#43	CP-090128	0011	4	Delivering HA-APN information to the UE	8.0.0	8.1.0
2009-03	CT#43	CP-090126	0012	2	Clarifications for IP mobility mode selection	8.0.0	8.1.0
2009-03	CT#43	CP-090130	0014		System selection	8.0.0	8.1.0
2009-03	CT#43	CP-090125	0017	2	ANDSF procedure - align with 24.312	8.0.0	8.1.0
2009-03	CT#43	CP-090129	0024	2	Clarifying the number of ePDGs	8.0.0	8.1.0
2009-03	CT#43	CP-090130	0027	1	Restructuring sub-clause 5.1	8.0.0	8.1.0
2009-03	CT#43	CP-090129	0028	2	Refining sub-clause 5.2 on EPC network selection	8.0.0	8.1.0
2009-03	CT#43	CP-090131	0029		Use of decorated NAI for cdma2000 access to EPC	8.0.0	8.1.0
2009-03	CT#43	CP-090126	0030		Clarification of AAA procedures for cdma2000 access	8.0.0	8.1.0
2009-03	CT#43	CP-090126	0034	1	Clarification on Tunnel establishment for Multiple PDNs	8.0.0	8.1.0
2009-03	CT#43	CP-090126	0038	1	Cleanup for Static Configuration of Inter-technology Mobility Mechanism	8.0.0	8.1.0
2009-03	CT#43	CP-090127	0042	1	Cleanup for UE discovering the ANDSF	8.0.0	8.1.0
2009-03	CT#43	CP-090130	0044	2	Selection of the ePDG – resolution of open issues	8.0.0	8.1.0
2009-06	CT#44	CP-090413	0043	3	Mismatch in the static configuration of IP mobility mechanisms in the UE and the EPC	8.1.0	8.2.0
2009-06	CT#44	CP-090357	0048	2	Refining UE procedures for IPSec tunnel management	8.1.0	8.2.0
2009-06	CT#44	CP-090413	0049	1	Access authentication for untrusted non-3GPP access	8.1.0	8.2.0
2009-06	CT#44	CP-090413	0051	1	Clarification about ANDSF usage	8.1.0	8.2.0
2009-06	CT#44	CP-090413	0055	1	IPMS indication to the ePDG and IP address assignment	8.1.0	8.2.0
2009-06	CT#44	CP-090413	0057	1	ANDSF DHCP Options	8.1.0	8.2.0

2009-06	CT#44	CP-090413	0058	1	Network selection and I-WLAN	8.1.0	8.2.0
2009-09	CT#45	CP-090654	0037	5	Clarifications on UE procedures	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0056	5	Handover of multiple PDN connections to one APN	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0060	2	Corrections and clarifications on identity usage	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0061	1	Periodic network selection attempts for non-3GPP accesses	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0062	1	Correcting ambiguity of EPC network selection for WLAN as a non-3GPP access	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0065	1	Correction on how UE uses ANDSF information in Annex A	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0066		Alignment of text for ANDSF and PLMN selection interaction	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0068	1	APN information in IKE message	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0069	1	IP address allocation during IPsec tunnel establishment procedure	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0070		Editorial corrections to subclause 7.2.2	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0071	2	Corrections in IP Mobility Mode selection	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0072	4	PCO handling on PMIP based interfaces	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0076	1	Attach to untrusted network correction	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0077	2	Corrections to sending of IPMS indication	8.2.0	8.3.0
2009-09	CT#45	CP-090654	0075	1	Description on ANDSF in roaming case	8.3.0	9.0.0
2009-12	CT#46	CP-090937	0079	1	ANDSF Discovery in roaming scenarios	9.0.0	9.1.0
2009-12	CT#46	CP-090937	0082	2	ANDSF discovery procedures performed by a UE	9.0.0	9.1.0
2009-12	CT#46	CP-090937	0083	3	Secure connection between UE and ANDSF	9.0.0	9.1.0
2009-12	CT#46	CP-090934	0087	6	Implementation of stage 2 requirements for MUPSAP	9.0.0	9.1.0
2009-12	CT#46	CP-090901	0090	1	Tunnel set up after WLAN PLMN selection	9.0.0	9.1.0
2009-12	CT#46	CP-090901	0091	2	UE behavior when connectin to v-ANDSF	9.0.0	9.1.0
2009-12	CT#46	CP-090901	0095	2	UE's IP configuration during IPsec tunnel establishemnet with ePDG	9.0.0	9.1.0
2009-12	CT#46	CP-090901	0097	2	PDN connection reject during the IPsec tunnel establishment	9.0.0	9.1.0
2009-12	CT#46	CP-090901	0099	1	Removal of outdated or redundant editor's notes ahead of CT#46	9.0.0	9.1.0
2009-12	CT#46	CP-090901	0102	1	Addition of abbreviations	9.0.0	9.1.0
2009-12					Editorial correction	9.1.0	9.1.1
2010-03	CT#47	CP-100107	0094	3	Removing version identifier from ANDSF information request	9.1.1	9.2.0
2010-03	CT#47	CP-100144	0100	4	Emergency session handling (for handovers to HRPD access)	9.1.1	9.2.0
2010-03	CT#47	CP-100107	0104	1	Completion of Network selection procedures	9.1.1	9.2.0
2010-03	CT#47	CP-100107	0106	1	Corrections to decodes of Value part of EAP attribute	9.1.1	9.2.0
2010-03	CT#47	CP-100150	0107	2	DHCP discovery of ANDSF for UE while roaming	9.1.1	9.2.0
2010-03	CT#47	CP-100150	0108	2	UE's use of V-ANDSF information vs H-ANDSF information	9.1.1	9.2.0
2010-03	CT#47	CP-100147	0109	1	Allowing UE optional behaviour towards networks not supporting MUPSAP	9.1.1	9.2.0
2010-03	CT#47	CP-100147	0110		Resolution of Editor's note on PDN connection rejection in section 6.4.4	9.1.1	9.2.0
2010-03	CT#47	CP-100147	0113	2	Handling of concurrent PDN connection requests at ePDG	9.1.1	9.2.0
2010-03	CT#47	CP-100107	0115	1	Correction on attachment with ePDG	9.1.1	9.2.0
2010-06	CT#48	CP-100339	0118		Correction to the Full Authentication and Fast Re-authentication procedures	9.2.0	9.3.0
2010-06	CT#48	CP-100339	0122		Reference Updates	9.2.0	9.3.0
2010-06	CT#48	CP-100354	0123	1	Corrections to PDN connection reject procedure for S2b interface	9.2.0	9.3.0
2010-06	CT#48	CP-100339	0125		Removing Editor's notes on AT_IPMS_IND, AT_IPMS_RES and AT_TRUST_IND	9.2.0	9.3.0
2010-06	CT#48	CP-100370	0119	2	Description of additionally used identifiers in non-3GPP access	9.3.0	10.0.0
2010-09	CT#49	CP-100485	0130		Removing editor's note on HOME AGENT ADDRESS	10.0.0	10.1.0
2010-09	CT#49	CP-100513	0131	3	24.302 procedures for Inter-System Routing Policies (ISRP)	10.0.0	10.1.0
2010-09	CT#49	CP-100509	0132	2	Corrections to UE and ANDSF Pull mode procedures	10.0.0	10.1.0
2010-12	CT#50	CP-100754	0134	4	Local operating environment for IFOM	10.1.0	10.2.0
2010-12	CT#50	CP-100754	0135	1	Introduction of Non-Seamless WLAN Offload	10.1.0	10.2.0
2010-12	CT#50	CP-100755	0136	2	Remove PMIP qualifier for S2b interface	10.1.0	10.2.0
2011-03	CT#51	CP-110163	0137	4	ePDG selection for known VPLMN	10.2.0	10.3.0
2011-03	CT#51	CP-110185	0139	4	Clarification of Multi-Access Capability Impact for Procedure between UE and ANDSF	10.2.0	10.3.0
2011-03	CT#51	CP-110200	0141	2	Information of data traffic routing used by MAPCON capable UE	10.2.0	10.3.0
2011-03	CT#51	CP-110200	0142	3	Abnormal case during the handover procedure	10.2.0	10.3.0
2011-03	CT#51	CP-110185	0146	1	Correction on multiple PDN support for IFOM	10.2.0	10.3.0
2011-03	CT#51	CP-110185	0147		Request of ISRP from UE	10.2.0	10.3.0
2011-03	CT#51	CP-110185	0148	1	Editor's notes in 24.302	10.2.0	10.3.0
2011-03	CT#51	CP-110200	0149	1	Clarification on use of ISRP for MAPCON capable UE	10.2.0	10.3.0
2011-03	CT#51				Correction of an error in the implementation of CR0141	10.3.0	10.3.1
2011-06	CT#52	CP-110459	0151	1	IP address allocation when using GTP on S2b	10.3.1	10.4.0
2011-06	CT#52	CP-110471	0152	1	Clarification on the relation of the user preferences with ISRP in a MAPCON UE	10.3.1	10.4.0
2011-06	CT#52	CP-110466	0155		UE retains the information received from ANDSF	10.3.1	10.4.0
2011-06	CT#52	CP-110453	0158	1	Reference Update for draft-das-mipshop-andsf-dhcp-options	10.3.1	10.4.0
2011-06	CT#52	CP-110478	0160	1	Correction on IFOM and MAPCON UE capability	10.3.1	10.4.0
2011-09	CT#53	CP-110660	0171	1	Removal of duplicate reference and correction of references	10.4.0	10.5.0
2011-09	CT#53	CP-110690	0161	5	Rejection of ePDG tunnel establishment request	10.5.0	11.0.0

2011-09	CT#53	CP-110690	0163	2	Restriction of max PDN connections for non-3GPP access	10.5.0	11.0.0
2011-09	CT#53	CP-110690	0165	2	Correction to Automatic EPC network selection	10.5.0	11.0.0
2011-09	CT#53	CP-110694	0168		Correction to references	10.5.0	11.0.0
2011-09	CT#53	CP-110690	0172		3GPP2 reference corrections	10.5.0	11.0.0
2011-12	CT#54	CP-110882	0173	4	Clarify interaction between ISRP and ISMP.	11.0.0	11.1.0
2011-12	CT#54	CP-110882	0175	3	Handling the absence of APN leaf in ForServiceBased ISRP	11.0.0	11.1.0
2011-12	CT#54	CP-110888	0180	2	Incorrect representation of EAP-AKA' message	11.0.0	11.1.0
2011-12	CT#54	CP-110888	0181	2	Support for access to external private networks via S2b	11.0.0	11.1.0
2011-12	CT#54	CP-110882	0182	1	ISRP usage	11.0.0	11.1.0
2011-12	CT#54	CP-110888	0184	3	Clarification of the UE location	11.0.0	11.1.0
2012-03	CT#55	CP-120113	0189	1	HA IP address from DNS	11.1.0	11.2.0
2012-06	CT#56	CP-120309	0190		NAI used for authentication	11.2.0	11.3.0
2012-06	CT#56	CP-120309	0192	1	Remove PMIP qualifier for S2a interface	11.2.0	11.3.0
2012-06	CT#56	CP-120309	0194		Security mechanisms for tunnel setup using IPsec and IKEv2	11.2.0	11.3.0
2012-06	CT#56	CP-120311	0195	2	Name for network provided over non-3GPP access network connected to EPC	11.2.0	11.3.0
2012-06	CT#56	CP-120318	0198		Conditions for the UE to provide indication for IPMS	11.2.0	11.3.0
2012-09	CT#57	CP-120584	0202	1	Corrections for Name for network provided over non-3GPP access network connected to EPC	11.3.0	11.4.0
2012-09	CT#57	CP-120592	0203		Reference for BBAI	11.3.0	11.4.0
2012-09	CT#57	CP-120584	0205		Correction on bit number	11.3.0	11.4.0
2012-09	CT#57	CP-120584	0209	2	Handling of unknown protocol data	11.3.0	11.4.0
2012-09	CT#57	CP-120584	0210	3	Clarification of IPSec tunnel established between the UE and the ePDG	11.3.0	11.4.0
2012-12	CT#58	CP-120794	0199	4	Clarification on DSMIP indication	11.4.0	11.5.0
2012-12	CT#58	CP-120794	0211		Editor's notes on attribute types for AT_SHORT_NAME_FOR_NETWORK and AT_FULL_NAME_FOR_NETWORK	11.4.0	11.5.0
2012-12	CT#58	CP-120794	0213	3	GBA Push realization not using General Package #0 format	11.4.0	11.5.0
2012-12	CT#58	CP-120794	0218	1	Clarification of the usage of the APN in the IKEv2 signaling	11.4.0	11.5.0
2013-03	CT#59	CP-130115	0222		Ignoring information element	11.5.0	11.6.0
2013-03	CT#59	CP-130125	0221	2	Clean-up and consolidation of repeated requirements	11.6.0	12.0.0
2013-06	CT#60	CP-130258	0228	2	APN forbidden by the UE	12.0.0	12.1.0
2013-06	CT#60	CP-130258	0229	2	EPC acess forbidden by the UE	12.0.0	12.1.0
2013-06	CT#60	CP-130258	0230	2	ISRP sent in PSK TLS connection	12.0.0	12.1.0
2013-06	CT#60	CP-130250	0233		Recommended application id for ANDSF GBA Push	12.0.0	12.1.0
2013-06	CT#60	CP-130418	0234	4	Specification of Tunnelling of UE Services over Restrictive Access Networks	12.0.0	12.1.0
2013-06	CT#60	CP-130258	0238	3	Trust relationship notification from the 3GPP AAA server	12.0.0	12.1.0
2013-06	CT#60	CP-130258	0241	1	Reject a PDN connection	12.0.0	12.1.0
2013-09	CT#61	CP-130512	0243	1	Tunnelling of UE Services over Restrictive Access Networks - cleanup and editor's note resolution	12.1.0	12.2.0
2013-09	CT#61	CP-130509	0246	2	IARP in roaming scenarios	12.1.0	12.2.0
2013-12	CT#62	CP-130754	0247	2	Bit order in fields of figures	12.2.0	12.3.0
2013-12	CT#62	CP-130754	0249	1	Incorrect message name	12.2.0	12.3.0
2013-12	CT#62	CP-130768	0250	4	The usage of APN in non-3GPP access	12.2.0	12.3.0
2013-12	CT#62	CP-130761	0251	2	Adding IARP in information provided by ANDSF	12.2.0	12.3.0
2013-12	CT#62	CP-130768	0254	1	Multiple PDN support for trusted WLAN	12.2.0	12.3.0
2013-12	CT#62	CP-130768	0248	5	EAP extensions for eSaMOG_St3	12.2.0	12.3.0
2013-12	CT#62	CP-130761	0252	3	Introduction of Inter-APN Routing Policies (IARP) for ANDSF	12.2.0	12.3.0
2013-12	CT#62	CP-130761	0257	1	The usage of IARP in determining the data traffic routing of IP flows	12.2.0	12.3.0
2013-12	CT#62	CP-130765	0253	6	Support of BBF convergence	12.2.0	12.3.0
2013-12	CT#62	CP-130803	0255	2	Clarifications and cleanup related to UE capabilities for ANDSF	12.2.0	12.3.0