ETSI TS 124 302 V14.9.0 (2019-01)

Universal Mobile Telecommunications System (UMTS);
LTE;
Access to the 3GPP Evolved Packet Core (EPC)
via non-3GPP access networks;
Stage 3
(3GPP TS 24.302 version 14.9.0 Release 14)

Reference
RTS/TSGC-0124302ve90

Keywords
LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

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

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

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.

[2A] 3GPP TS 23.002: "Network architecture".

[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 v12.2.0: "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".

[14A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[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".

[16B] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol specification".

[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 v2.0: "E-UTRAN - HRPD Connectivity and Interworking: Core Network Aspects".

contains only the requirements for the prior release of this specification.

[21] 3GPP2 C.S0087-A v4.0: "E-UTRAN – HRPD and CDMA2000 1x Connectivity and Interworking: Air Interface Aspects".

[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] Void.

[55] Void.

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

[57] IEEE Std 802.11-2012: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[58] IEEE Std 802-2014: "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture", 30th June 2014.

[59] Void.

[60] IETF RFC 4284 (January 2006): "Identity Selection Hints for the Extensible Authentication Protocol (EAP)".

[61] IEEE Std 802.1X™-2010: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Port-based Network Access Control".

[62] IETF RFC 4282: "The Network Access Identifier".

[63] ITU-T Recommendation E.212: "The international identification plan for mobile terminals and mobile users".

[64] IETF RFC 7651 (September 2015): "3GPP IP Multimedia Subsystems (IMS) Option for the Internet Key Exchange Protocol Version 2 (IKEv2)".

[65] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[66] 3GPP TS 23.380: "IMS Restoration Procedures".

[67] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[68] 3GPP TS 23.161: "Network-Based IP Flow Mobility (NBIFOM); Stage 2".

[69] 3GPP TS 24.161: "Network-Based IP Flow Mobility (NBIFOM); Stage 3".

[70] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[70A] IETF RFC 4309 (December 2005): "Internet Key Exchange Protocol Version 2 (IKEv2)".

[70B] IETF RFC 7296 (October 2014): "Internet Key Exchange Protocol Version 2 (IKEv2)".

[71] IETF RFC 6696 (July 2012): "EAP Extensions for the EAP Re-authentication Protocol (ERP)".

[72] IETF RFC 3948 (January 2005): "UDP Encapsulation of IPsec ESP Packets".

[73] IETF RFC 2234 (November 1997): "Augmented BNF for Syntax Specification: ABNF".

[74] IETF RFC 5279 (July 2008): "A Uniform Resource Name (URN) Namespace for the 3rd Generation Partnership Project (3GPP)".

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.

ANDSF rules: In this specification, ANDSF rules refers to the set of ANDSF policies defined in 3GPP TS 24.312 [13] for WLAN access selection and traffic routing between E-UTRAN or UTRAN and WLAN. ANDSF rules can contain RAN validity conditions for RAN-assisted WLAN interworking.

Emergency session: In this specification, an emergency session refers to an emergency PDN connection established in E-UTRAN and handed over to a S2a based cdma2000® HRPD access network, or an emergency PDN connection established over trusted or untrusted WLAN access, or an emergency PDN connection established in 3GPP access and handed over to trusted or untrusted WLAN access.

Equivalent home service provider: In this specification, equivalent home service provider is a service provider that is equivalent to HPLMN in regard to service provider selection over WLAN.

Equivalent visited service provider: In this specification, equivalent visited service provider is a service provider that is equivalent to the V-PLMN in regard to service provider selection over WLAN.

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

Offload Preference Indicator (OPI): In this specification, Offload Preference Indicator (OPI) is a bitmap (i.e. a one-dimensional bit array) that can be used by UEs in an E-UTRA or UTRA cell to determine when to move certain traffic (e.g. certain IP flows) to WLAN access or to 3GPP access. The meaning of each bit in this bitmap is operator specific and is not defined in 3GPP specifications.

Offloadable PDN connection: In this specification, an offloadable PDN connection is a PDN connection, established in (or previously handed over to) 3GPP access, such that:

- the WLAN offload indication information element (see 3GPP TS 24.301 [10] and 3GPP TS 24.008 [46]) last received for the PDN connection has the "offloading the traffic of the PDN connection via a WLAN when in S1 mode is acceptable" value and the UE is in S1 mode; or

- the WLAN offload indication information element (see 3GPP TS 24.301 [10] and 3GPP TS 24.008 [46]) last received for the PDN connection has the "offloading the traffic of the PDN connection via a WLAN when in UTRAN Iu mode is acceptable" value and the UE is in UTRAN Iu mode.

Preferred Service Providers List (PSPL): In this specification, the Preferred Service Providers List refers to a prioritized list of service provider realms other than equivalent home service providers preferred by the UE's 3GPP home operator for WLAN.

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.

RAN Assistance Information: In this specification, RAN Assistance Information refers to the set of thresholds and parameters that can be provided by E-UTRAN or UTRAN to the UE for assisting WLAN access selection and traffic routing. The RAN assistance information can include 3GPP access thresholds, WLAN access thresholds, an Offload Preference Indicator (OPI) value and WLAN identifiers as defined in 3GPP TS 25.331 [14A] and 3GPP TS 36.331 [16B].

RAN rules: In this specification, RAN rules refers to the set of RAN assistance parameter and RAN steering command handling, access network selection and traffic steering procedures defined in 3GPP TS 36.304 [16], 3GPP TS 25.304 [14] and 3GPP TS 36.331 [16B] for the steering of traffic between E-UTRAN or UTRAN and WLAN associated with RAN-controlled LTE-WLAN interworking or RAN-assisted WLAN interworking.

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.

Unauthenticated IMSI: In this specification, the term "unauthenticated IMSI" or the term "IMSI is unauthenticated" is only pertinent to the network. The knowledge that a UE's IMSI is unauthenticated or that the UE has an unauthenticated IMSI, is not available to the UE.

WLAN Selection Policy (WLANSP): In this specification, the WLAN Selection Policy is a set of operator-defined rules that determine how the UE selects/reselects a WLAN access network.

WLAN selection information: In this specification, WLAN selection information refers to the information received from ANDSF including WLAN Selection Policy (WLANSP), rule selection information, Home Network Preference information and Visited Network Preference information as specified in 3GPP TS 24.312 [13].

Visited PLMNs with preferred rules: In this specification, visited PLMNs with preferred rules included in the rule selection information refers to a list of identifiers of visited PLMNs provided by HPLMN, so that the UE roaming in such visited PLMN prefers ISMP, ISRP or WLANSP rules provided by the visited PLMN over ISMP, ISRP or WLANSP rules provided the HPLMN. In ANDSF MO, the visited PLMNs with preferred rules correspond to the ANDSF/RuleSelectionInformation/VPLMNswithPreferredRules interior node.

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

Acceptable cell
EHPLMN
Home PLMN
Limited service state
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

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.312 [13] apply:

Active rule
Valid rule

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.003 [3] that relate to access to 3GPP evolved packet core via non-3GPP access networks, apply:

NAI
Alternative NAI
Decorated NAI

Emergency NAI
Fast-Reauthentication NAI
Pseudonym Identity
Root NAI

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2A] apply:

3GPP AAA Proxy
3GPP AAA Server

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.161 [68] apply:

NBIFOM
Routing Rule
UE-inititaed NBIFOM
Network-initiated NBIFOM
Multi-access PDN connection

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
ANQP	Access Network Query Protocol
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
ERP	EAP Re-authentication Protocol
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
NBIFOM	Network-Based IP Flow Mobility
NBM	Network based mobility management
NSP	Network Service Provider
NSWO	Non-Seamless WLAN Offload
OMA	Open Mobile Alliance
OPI	Offload Preference Indicator
PCO	Protocol Configuration Options
P-GW	PDN Gateway
PDU	Protocol Data Unit
PSPL	Preferred Service Provider List
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
WLANSP	WLAN Selection Policy
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 the UE accesses EPC via S2c is used; or

- an IPSec tunnel needs to be established with the same ePDG for each PDN connection when the UE accesses EPC via S2b 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].

4.3A WLAN

WLAN is an access network developed under the auspices of IEEE Computer Society. WLAN is compliant with IEEE 802.11-2012 [57], which define air interface aspects.

IEEE 802.11-2012 [57] defines Access Network Query Protocol (ANQP). A UE can receive from an AP ANQP-elements in response to an ANQP query. The ANQP query response is received in a generic advertisement service response frame or a protected management frame.

Where needed, the current specification further describes the structure and contents of payload of ANQP-elements specified in IEEE 802.11-2012 [57] (see annex H and annex I).

4.4 Identities

4.4.1 User identities

The user identification shall be either the root NAI, or the decorated NAI, when the UE accesses the EPC via non-3GPP access networks, and gets authentication, authorization and accounting services from the EPC.

For emergency services over WLAN:

- if IMSI is not available (i.e. a UE without USIM), the IMEI shall be used for the identification, as user part of the emergency NAI and the UE shall use a specific domain in the realm part of the NAI as specified in 3GPP TS 23.003 [3]; or

- if the UE has an IMSI, it shall use the IMSI for the identification, as user part of the emergency NAI.

NOTE 1: If the IMSI is unauthenticated on the network side and the network supports emergency session for unauthenticated IMSI, the IMEI is used for the identification on the network side (see subclause 6.4.3.1A).

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.

The UE's Mobile Identity IMEI or IMEISV is conveyed to the network (see subclause 6.4 and subclause 7) and used to enable consistent services for the UE accessing the network via non-3GPP access or to support the emergency services over WLAN for the unauthenticated UEs.

NOTE 2: IMEI and IMEISV are untrusted identities stored on the UE.

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 is to be used as the permanent identity as specified in 3GPP TS 33.402 [15].

- The Fast-Reauthentication NAI 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 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 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 either provisioned by the home operator or constructed by UE in either the Operator Identifier FQDN format or the Tracking/Location Area Identity FQDN format as described in subclause 4.5.4.2 of 3GPP TS 23.402 [6], 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 via S2a using a trusted non-3GPP access network, the UE uses 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 broadband access interworking, the EPC network procedures are specified in 3GPP TS 24.139 [51].

The UE procedures for support of fixed broadband access are specified in 3GPP TS 24.139 [51] and can be used when the EPC network uses the fixed broadband access interworking or the fixed broadband access convergence.

The architecture of the fixed broadband access convergence is specified in 3GPP TS 23.203 [5A].

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.

4.7 Provision and handling of local emergency numbers

It is a UE implementation option to support the procedures of this subclause.

Once the UE has a secure connection to a PLMN through non-3GPP access, the UE supports obtaining local emergency numbers by one of the following ways:

i) when the UE is connected to a PLMN through trusted non-3GPP access, the local emergency numbers is provided through ANQP, within the ANQP payload. The signalling protocol and methods for use of ANQP is as specified in IEEE 802.11-2012 [57]. See also annex I;

ii) when the UE is connected to a PLMN through untrusted non-3GPP access, local emergency numbers can be provided through DNS query. See annex J; or

iii) when the UE is connected to a PLMN through untrusted non-3GPP access, local emergency numbers can be provided through IKEv2. See annex K.

Upon receiving the local emergency numbers through any of the methods indicated above, the UE shall store the local emergency numbers:

a) if the Non-3GPP emergency number indicator within the Non-3GPP NW provided polices IE through registration procedures over 3GPP access is set to "use of non-3GPP emergency numbers permitted", and:

   - if the UE is connected to a PLMN through non-3GPP access and also registered to same PLMN or different PLMN through 3GPP access in the same country, then provide these local emergency numbers to upper layers for the detection of UE initiated emergency call;

   - if the UE is connected to a PLMN through non-3GPP access but is also registered to different PLMN through 3GPP access that is not in the same country, then do not use the received local emergency numbers;

b) if the Non-3GPP emergency number indicator within the Non-3GPP NW provided polices IE through registration procedures over 3GPP access is set to "use of non-3GPP emergency numbers not permitted", or if no Non-3GPP NW provided polices IE was provided through registration procedures over 3GPP access, then:

   - do not use the received local emergency numbers for the detection of UE initiated emergency call over 3GPP access; and

c) if the UE:

   - is connected to a PLMN through non-3GPP access;

   - is not registered to any PLMN through 3GPP access;

   - is not in limited service state camped on an acceptable cell of any PLMN through 3GPP access; and

   - can determine that the MCC information of the local emergency numbers received over non-3GPP access corresponds to the country in which the UE is located;

   then, as an implementation option, provide these local emergency numbers to upper layers for the detection of UE initiated emergency call.

NOTE: The UE determination of the country in which the UE is located, is UE implementation specific.

The local emergency numbers, received in any of the methods indicated above:

- are only valid in the country where these local emergency numbers were provided;

- replace only the stored local emergency numbers received over non-3GPP access, if any;

- shall be deleted when UE moves to a country different from where the local emergency numbers were received; and at switch off or removal of the USIM.

5 Network Discovery and Selection

5.0 General

The following aspects are included when selecting an EPC network and routing traffic via the EPC network:

- access network discovery and selection procedures as defined in subclause 5.1;

- EPC network selection as defined in subclause 5.2; and

- data traffic routing of IP flows as defined in subclause 5.4.

If the UE perform reselection of the access network as defined in subclause 5.3 and the UE reselects to a different access network, the UE performs the second item and third item of the above bulleted list.

5.1 Access network discovery and selection procedures

5.1.1 General

If PLMN selection specified in 3GPP TS 23.122 [4] is applicable (e.g., at switch-on, recovery from lack of 3GPP coverage, or user selection of applicable 3GPP access technology), the PLMN selection to select the highest priority PLMN according to these specifications is performed before any access network discovery. Procedures for EPC selection over non-3GPP access are specified in subclause 5.2. In particular, for WLAN access, service provider selection function is specified in the WLAN specific procedures in subclause 5.2.3.2

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 determines the presence of several access networks and then selects between them. If a higher priority access network is found connected to the selected service provider or a higher priority service provider, the UE will attempt to attach via that access 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 subclause 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.

If the RAN rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, the UE uses the information described in subclause 6.10.4 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].

5.1.3.2.3 WLAN selection

5.1.3.2.3.1 General

The purpose of this procedure is to create a prioritized list of selected WLAN(s).

The user preferences are used to select between the automatic WLAN selection procedure or the manual WLAN selection procedure.

The UE shall determine the prioritized list of selected WLAN(s):

1) if user preferences are present, in accordance with the manual mode WLAN selection procedure (see subclause 5.1.3.2.3.2); and

2) if user preferences are not present, in accordance with the automatic mode WLAN selection procedure (see subclause 5.1.3.2.3.3).

The UE shall use the prioritized list of selected WLAN(s) to select the service provider in the procedure in subclause 5.2.3.2.

5.1.3.2.3.2 Manual mode WLAN selection

The UE creates a prioritized list of selected WLAN(s). The creation of the prioritized list is implementation specific.

5.1.3.2.3.3 Automatic mode WLAN selection

If the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, then the selected WLAN(s) are WLAN(s) that fulfil the selection criteria with the highest priority configured in the active ANDSF WLANSP rule.

If the RAN rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, then the selected WLAN(s) are WLAN(s) matching WLAN identifiers in an entry of the list of the WLAN identifiers received along with the move-traffic-to-WLAN indication as described in subclause 6.10.4.

The UE determines the selected WLAN(s) according to the following steps:

1) the UE shall construct prioritized list of available WLANs as follows:

   a) if the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, the UE shall use the procedures specified in IEEE 802.11-2012 [57] to discover the available WLANs. The UE may perform ANQP procedures as specified in IEEE 802.11-2012 [57] to discover the attributes and capabilities of available WLANs. The UE shall compare the attributes and capabilities of the available WLANs with the highest priority selection criterion that has not been used yet in the active WLANSP rule, and construct a prioritized list of available WLANs that fulfil the selection criteria. If there are multiple highest priority selection criteria, it is up to the UE implementation which one to use. In particular, if:

      - the group of selection criteria include the HomeNetworkIndication and it is set to "1" (see 3GPP TS 24.312 [13]); and

      - the HomeNetworkPreference:

        i) does not include 3GPP_RPLMN_Preferred; or

        ii) includes 3GPP_RPLMN_Preferred and it is set to "0" (see 3GPP TS 24.312 [13]);

      then a WLAN is included, if:

      - the other selection criteria in the active WLANSP rule are met; and

- the domain name list (see IEEE 802.11-2012 [57]) includes:

  i) the home domain name derived from its IMSI; or

  ii) any realm in the EquivalentHomeSPs as specified in 3GPP TS 24.312 [13].

The priority of a WLAN in the list is set to the WLAN priority defined in the preferredSSIDlist of the matching selection criteria. There may be one or more selected WLANs in the list; and

b) if the RAN rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, the UE shall use the procedures specified in IEEE 802.11-2012 [57] to discover available WLANs. The UE shall construct a prioritized list of available WLANs and populate it with each discovered WLAN which matches all WLAN identifiers included in an entry of the list of the WLAN identifiers received along with the move-traffic-to-WLAN indication as described in subclause 6.10.4. The priority of a discovered WLAN in the prioritized list of available WLANs is decided by the UE in an implementation specific way;

2) if the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, and if the following conditions are fulfilled:

- the UE supports the PDN connection establishment over WLAN using the applicable S2a procedures specified in 3GPP TS 23.402 [6];
- the "S2a connection preference" indicator exists and indicates that PDN connection establishment over WLAN using the applicable S2a procedures specified in 3GPP TS 23.402 [6] is preferred; and
- one or more WLANs in the list constructed in step 1) is a trusted non-3GPP IP access network;

then the UE considers the WLANs that have the highest priority and indicate the HPLMN or RPLMN in the PLMN list with S2a connectivity IE (see annex H) as the selected WLAN(s).

Otherwise, the UE considers the WLAN(s) that has or have the highest priority as the selected WLAN(s). And

NOTE 1: WLAN advertises PLMN(s) towards which the S2a connectivity is supported using ANQP-element "3GPP Cellular Network" with the PLMN List with S2a Connectivity IE in the payload, according to annex H.

NOTE 2: Advertising S2a connectivity over a WLAN using EAP signalling is not supported in this version of the specification.

3) if the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, if there are no WLAN(s selected in step 2), the UE may repeat the procedure from step 1) taking into consideration selection criteria with lower priority from the active WLANSP rule.

NOTE 3: UE implementation can optimize the steps described above, e.g. by combining the ANQP procedures.

5.2 EPC network selection over non-3GPP access

5.2.1 General

The following EPC network selection procedures over non-3GPP access 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) WLAN specific procedures in clause 5 apply: the procedures detail selecting one or more WLANs and (subsequently) selecting one service provider offering services via the WLAN (see subclause 5.2.3.2). When the operator of the WLAN requires authentication and the authentication succeeds (see subclause 6.4 and 6.5.1), the UE follows the procedures defined for connecting with the EPC. 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) using a root NAI as defined in 3GPP TS 23.003 [3] 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 performs the appropriate EPC selection procedure over non-3GPP access when the non-3GPP radio becomes enabled. If the UE needs to establish emergency session over untrusted access, the UE shall select an ePDG that supports emergency services as described in subclause 7.2.1 and 3GPP TS 23.402 [6].

NOTE: The UE can perform the appropriate EPC selection procedure over non-3GPP access based on other implementation-specific triggers, e.g. regaining non-3GPP access network coverage or connectivity.

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.

5.2.2 Generic EPC network selection procedure over non-3GPP access

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 EPC network selection

5.2.2.2.1 UE selection modes

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

5.2.3.1.2.1 UE selection modes

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

5.2.3.2 EPC network selection procedures for WLAN

5.2.3.2.1 UE selection modes

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

The UE follows one of the following two procedures defined in subclause 5.2.3.2.2 and 5.2.3.2.3 depending on its implementation.

The service provider selected in accordance with these procedures determines the WLAN that is selected. When the selected WLAN is a trusted WLAN IP access and the UE decides to access EPC via S2a using trusted WLAN IP access, the UE shall derive a NAI from the identity of the selected service provider and use the NAI as the identity for authentication and authorization with the service provider and usage of the WLAN (see subclause 6.4).

5.2.3.2.1A Service provider solicitation

The UE shall determine which service providers are available from the available list of WLANs as constructed using the WLAN selection procedure described in subclause 5.1.3.2.3 using following procedures:

i) the UE selects a WLAN from the list of selected WLAN(s) constructed using the WLAN selection procedure described in subclause 5.1.3.2.3;

ii) if the WLAN selected in step i):

   a) supports ANQP specified in IEEE Std 802.11-2012 [57] and if the UE did not obtain a list of realms using ANQP in subclause 5.1.3.2.3.3 item 1, the UE sends an ANQP request for a list of realms (i.e. ANQP-elements "NAI Realm") and/or PLMN identities (i.e. ANQP-element "3GPP Cellular Network"); and

NOTE 1: The UE uses procedures defined in IEEE Std 802.11-2012 [57] to determine if the WLAN supports ANQP and to send the ANQP query request for ANQP-elements "NAI Realm" and/or "3GPP Cellular Network", as specified in IEEE Std 802.11-2012 [57].

   b) does not support ANQP (see IEEE Std 802.11-2012 [57]) or the UE does not receive a list of realms in item a), an EAP-Request/Identity is received and the EAP-request/Identity does not include one or more of realms and/or PLMN identities of service providers (encoded in accordance with IETF RFC 4284 [60]), the UE supports IEEE 802.1x authentication (see IEEE Std 802.1X™-2010 [61]), the UE shall request a list of realms and/or PLMN identities of service providers interworking with that WLAN by sending the EAP-Response/Identity message including as identity the alternative NAI; and

iii) the UE repeats this procedure for all WLANs from the available list of WLANs as constructed using the WLAN selection procedure described in subclause 5.1.3.2.3.

NOTE 2: The list with realms and/or PLMN identities of service providers received in accordance with procedures in IETF RFC 4284 [60], is of limited size and might not contain all the realms and/or PLMN identities of service providers available via the WLAN.

The UE shall convert any received PLMN identities into PLMN realms using the rules defined in 3GPP TS 23.003 [3].

5.2.3.2.2 Manual Service Provider selection mode procedure

The UE indicates to the user the service providers which are available for WLAN. The UE may obtain the service providers available for WLAN using procedures as described in subclause 5.2.3.2.1A. The UE will select the service provider based on the user preference.

5.2.3.2.3 Automatic mode service provider selection procedure

The purpose of this procedure is to:

- select a service provider over WLAN; and
- construct a NAI for use with authentication signalling with the selected service provider in order for the UE to be authorised to use the WLAN.

If the RAN rules control the WLAN access selection and traffic routing as described in subclause 6.10.2:

- if the RPLMN or an equivalent PLMN (see 3GPP TS 24.301 [10] or 3GPP TS 24.008 [46]) is available as described in subclause 5.2.3.2.1A via a WLAN from the selected WLAN(s) constructed using the WLAN selection procedure described in subclause 5.1.3.2.3, the highest priority service provider is the RPLMN or an equivalent PLMN (see 3GPP TS 24.301 [10] or 3GPP TS 24.008 [46]);
- if the RPLMN and an equivalent PLMN (see 3GPP TS 24.301 [10] or 3GPP TS 24.008 [46]) are not available as described in subclause 5.2.3.2.1A via a WLAN from the selected WLAN(s) constructed using the WLAN selection procedure described in subclause 5.1.3.2.3 and Home PLMN or an EHPLMN is available, the highest priority service provider is Home PLMN or an EHPLMN; and
- if the RPLMN, an equivalent PLMN (see 3GPP TS 24.301 [10] or 3GPP TS 24.008 [46]), Home PLMN and an EHPLMN are not available as described in subclause 5.2.3.2.1A via a WLAN from the selected WLAN(s) constructed using the WLAN selection procedure described in subclause 5.1.3.2.3, the highest priority service provider is a PLMN selected in an implementation-dependent way.

If the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, a service provider is the highest priority service provider if the service provider is available via a WLAN from the selected WLAN(s) constructed using the WLAN selection procedure described in subclause 5.1.3.2.3 and if:

i) the service provider is selected in item 3; or

ii) the conditions in item 3 are not met, and:

   - the service provider is the HPLMN;
   - the service provider is an equivalent home service provider (i.e. the service provider's realm matches a realm in the EquivalentHomeSPs as specified in 3GPP TS 24.312 [13]); or
   - no WLAN of the selected WLAN(s) provides access to a higher priority service provider.

Until the highest priority service provider is found, the UE shall verify if a service provider available over a WLAN of the selected WLAN(s) is the highest priority service provider:

1) Void

2) Using the service providers which are available for WLAN as described in subclause 5.2.3.2.1A, the UE uses the PLMN realms as the service provider realms in the remaining steps of this subclause.

3) If the following conditions are fulfilled:

   - the "3GPP RPLMN preferred" indicator is configured to prioritize 3GPP RPLMN; and
   - the realm of the RPLMN or the realm of an equivalent visited service provider included in the EquivalentVisitedSPs as specified in 3GPP TS 24.312 [13] is included in the list of realms created in subclause 5.2.3.2.1A, step ii);

   then the UE shall select the RPLMN or the equivalent visited service provider. The RPLMN shall be selected with higher priority than the equivalent visited service provider. If the RPLMN is selected, the UE shall convert

the RPLMN identity into selected PLMN realm using the rules defined in 3GPP TS 23.003 [3] and use it as the service provider realms in the remaining steps of this subclause.

4) if the condition in step 3) is not satisfied, the UE shall select a service provider in the following order:

   i) HPLMN matching a realm in the list of realms received in step ii) as described in subclause 5.2.3.2.1A;

   ii) realm found both in the list of realms received in step ii) as described in subclause 5.2.3.2.1A and in the EquivalentHomeSPs as specified in 3GPP TS 24.312 [13]; and

   iii) realm found both in the list of realms received in step ii) as described in subclause 5.2.3.2.1A and in the PSPL as specified in 3GPP TS 24.312 [13] with the priority higher than any other service provider's priority indicated as available via the WLAN.

   If a UE used the procedures in IETF RFC 4284 [60] (see subclause 5.2.3.2.1A) to obtain a list of service providers, then the UE is only required to select the HPLMN (if available) or an available equivalent home service provider.

NOTE 1: A UE using procedures in IETF RFC 4284 [60] to obtain a list of service providers is only required to select the HPLMN (if available) or an available equivalent home service provider. If the UE selects another service provider, the UE could be roaming even though the HPLMN or equivalent home service provider is available at the access point.

The UE shall select the WLAN providing access to the highest priority service provider.

If a highest priority service provider could not be determined, the UE proceeds in implementation-dependent way.

The UE shall construct a NAI for authentication with the highest priority service provider as described in 3GPP TS 23.003 [3]. Specifically, the UE constructs the:

a) root NAI corresponding to the HPLMN, if the highest priority service provider is the HPLMN advertised using a PLMN identity;

b) decorated NAI with double decoration including the realm of the highest priority service provider and the realm of the RPLMN, if the highest priority service provider is an equivalent visited service provider; or

c) decorated NAI including the realm of the highest priority service provider, otherwise.

NOTE 2: UE implementation can optimize the steps described above, e.g. by combining the ANQP procedures described in subclause 5.2.3.2.1A with the ANQP procedures in subclause 5.1.3.2.3.3.

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]. For WLAN access, the UE configured with a WLANSP rule specified in 3GPP TS 24.312 [13], shall use the access network selection procedure and a PLMN selection procedure defined in this document which are different from and shall not be used in conjunction with the procedures for I-WLAN access specified 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.

If the RAN rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, if the UE receives move-traffic-to-WLAN indication, along with the list of the WLAN identifiers as described in subclause 6.10.4, the UE shall perform the procedure in subclause 6.10.4.

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. The IARP can be statically provisioned in the 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 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;
- user preference settings;
- the RAN assistance information (including OPI);
- the measurements corresponding to the thresholds in the RAN assistance information; and
- indications received from access stratum as described in subclause 6.10.4.

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

5.4.2.1 ANDSF rules control the WLAN access selection and traffic routing

This subclause applies if the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2.

When selecting the access technologies or access networks or both to route the data traffic of IP flows:

1) if a UE supporting IFOM or non-seamless WLAN offload is provided with user preferences and has IARP rule for NSWO, ISRP or Local Operating Environment Information or any combination of them, the user preference settings shall take precedence over IARP rule for NSWO (if present), ISRP (if present) and Local Operating Environment Information (if present).

2) if a UE supporting IFOM or non-seamless WLAN offload hasIARP rule for NSWO, ISRP and Local Operating Environment Information and no user preference settings and if based on the content of Local Operating Environment the UE 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.

3) if a UE supporting IFOM or non-seamless WLAN offload having Local Operating Environment Information but no available ISRP, IARP rule for NSWO and no user preference settings, the UE may evaluate 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) and IARP rule (if present).

The user preference settings shall take precedence over IARP (if present).

5.4.2.2 RAN rules control the WLAN access selection and traffic routing

Access technology or access network selection procedures in subclause 6.10.4 apply if the RAN rules control the WLAN access selection and traffic routing as described in subclause 6.10.2.

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, EAP-AKA' or EAP-3GPP-LimitedService based access authentication (i.e. EAP-AKA, EAP-AKA' or EAP-3GPP-LimitedService) 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' and EAP-3GPP-LimitedService) 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 or EAP-Request/3GPP-LimitedService-Init-Info 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) or UEs initiating emergency session but whose IMSI authentication cannot proceed. 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 or conditions described in subclause 13.4 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.

When the UE decides to access EPC via S2c using non-3GPP IP access, 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].

The UE may support ERP as described in IETF RFC 6696 [71] and 3GPP TS 33.402 [15]. In this release of this specification, only the ERP Implicit Bootstrapping mode defined in IETF RFC 6696 [71] is supported.

After a UE successfully completes authentication and authorization for accessing EPC via the trusted non-3GPP access network, the UE may receive as part of an ANQP query to the access point, an ANQP-element in a protected frame with management frame protection enabled. If the ANQP-element is an Emergency Call Number ANQP-element encoded in accordance with Annex I, the UE considers the content of the Emergency Call Number field valid.

6.4.1A TWAN connection modes

As part of EAP-AKA' authentication via TWAN or EAP-3GPP-LimitedService 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 6.4.2.6.2 and subclause 6.4.2.6.3, acts in TSCM or aborts the EAP authentication as described in subclause 6.4.2.6.4.

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

If EAP-AKA' authentication is skipped during emergency call via TWAN for unauthenticated UEs and the EAP-3GPP-LimitedService authentication via TWAN is performed, the UE and the network can negotiate usage of either the single-connection mode (SCM) or the multi-connection mode (MCM) as follows:

a) The 3GPP AAA server indicates support of SCM, MCM or any combination of them as described in subclause 6.4.3.5.1A.

b) The UE requests usage of SCM or MCM as described in subclause 6.4.2.6.2A and subclause 6.4.2.6.3A, or aborts the EAP authentication as described in subclause 6.4.2.6.4.

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.

If the UE supports ERP, the identity to be used by the UE during the re-authentication procedure using ERP is the "KeyName-NAI" as described in 3GPP TS 23.003 [3].

6.4.2.1A Identity Management - emergency session

When initiating emergency session via trusted non-3GPP access, if the UE has no valid subscriber data available (USIM not available, or USIM is considered invalid by the UE), the UE shall provide its IMEI in an EAP Response/Identity message based on emergency NAI format specified in 3GPP TS 23.003 [3].

If the UE receives EAP-Request/3GPP-LimitedService-Init-Info message from the network requesting IMEI, the UE provides IMEI as specified in subclause 6.4.2.7.

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.

For WLAN access, after the UE has been successfully authenticated from WLAN, the UE may receive EAP-Request/AKA'-Notification dialogue with AT_NOTIFICATION attribute value 1031 "User has not subscribed to the requested service" as defined in IETF RFC 4187 [33]. Then the UE shall not initiate the EPC access procedure to the same WLAN until switching off or the UICC containing the USIM is removed.

NOTE: Switching off and USIM change conditions are implemented taking into consideration the user experience aspect.

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

The UE may support SCM. The UE may support MCM.

NOTE 1: The UE is allowed to support both MCM and SCM. The UE is allowed to support neither MCM nor SCM.

NOTE 2: No UE extensions are needed for TSCM.

6.4.2.6.2 Usage of single-connection mode (SCM)

If:

a) the UE supports the SCM;

b) 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:

   1) contains the message type field indicating CONNECTION_CAPABILITY; and

   2) contains the item list field:

      A) including the CONNECTION_MODE_CAPABILITY item as described in subclause 8.1.4.8 indicating support of SCM; and

      B) if the UE requests an emergency attach or an emergency handover, including the CONNECTION_MODE_CAPABILITY item as described in subclause 8.1.4.8 indicating that emergency services are supported; and

c) 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 - PDN connection, or NSWO; 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, a handover attach, an emergency attach, or an emergency handover is requested;

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

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

         iv) if the handover attach or the emergency handover 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 1: 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, shall determine 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) if the initial attach, or the handover attach is requested, shall determine the selected APN in the APN item as described in subclause 8.1.4.5 included in the item list field;

   2) shall determine 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;

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

   4) if a IPV4_ADDRESS item as described in subclause 8.1.4.11 is included in the item list field, shall determine the IPv4 address allocated to the UE for the PDN connection in the IPV4_ADDRESS item;

5) if a IPV6_INTERFACE_IDENTIFIER item as described in subclause 8.1.4.12 is included in the item list field, shall determine the IPv6 interface identifier allocated to the UE for the PDN connection in the IPV6_INTERFACE_IDENTIFIER item and shall use it when building the IPv6 link local address; and

6) shall determine the TWAG user plane MAC address in the TWAG_UP_MAC_ADDRESS item as described in subclause 8.1.4.14 included in the item list field, and shall use the TWAG user plane MAC address for encapsulating user plane packets according to 3GPP TS 23.402 [6]; and

b) if the AT_NOTIFICATION attribute indicates failure with value 0 "General failure after authentication" or value 16384 - "General failure" as defined in IETF RFC 4187 [33] and the ACCESS_CAUSE item is included:

1) shall determine the cause of failure in the ACCESS_CAUSE item as described in subclause 8.1.4.17 included the item list field:

2) if the initial attach, or the handover attach is requested, and the cause of failure is #2 "Non-3GPP access to EPC not allowed" as defined in subclause 8.1.4.17, shall not retry the authentication procedure to any WLANs until switching off or the UICC containing the USIM is removed;

3) if the cause of failure is #11 "PLMN _NOT_ALLOWED" as defined in subclause 8.1.4.17, shall not retry the authentication procedure from the same PLMN via WLANs according to the network selection procedures as defined in subclause 5.2.2;

4) if the initial attach, or the handover attach is requested, and the cause of failure is #3 "RAT type not allowed" as defined in subclause 8.1.4.17, the UE shall not retry the authentication procedure to any WLANs until switching off or the UICC containing the USIM is removed;

5) if the cause of failure is #6 "Illegal ME" as defined in subclause 8.1.4.17, shall not retry the authentication procedure from the same PLMN until switching off or the UICC containing the USIM is removed; and

NOTE 2: Switching off and USIM change conditions are implemented taking into consideration the user experience aspect.

c) if the AT_NOTIFICATION attribute indicates failure as defined in bullet b) and the CAUSE item is included:

1) shall determine the cause of failure in the CAUSE item as described in subclause 8.1.4.10 included the item list field;

2) if the initial attach, or the handover attach is requested, the cause of failure is #26 "Insufficient resources" and the Tw1 item is included in the item list field, shall take different actions depending on the timer value received in the Tw1 item as follows:

A) if the timer value indicates neither zero nor deactivated, shall stop timer Tw1 associated with the corresponding APN, if it is running. The UE shall start timer Tw1 (see 3GPP TS 24.244 [56]) with the value provided in the Tw1 value IE and not send another SCM_REQUEST message with the CONNECTIVITY_TYPE item indicating PDN connection and with APN item indicating the same APN until timer Tw1 expires, the timer Tw1 is stopped, or the USIM is removed;

B) if the timer value indicates that this timer is deactivated, shall not send another SCM_REQUEST message with the CONNECTIVITY_TYPE item indicating PDN connection and with APN item indicating the same APN until the UE is switched off or the USIM is removed;

C) if the timer value indicates zero, may send another SCM_REQUEST message with the CONNECTIVITY_TYPE item indicating PDN connection and with APN item indicating the same APN; and

D) if the WLAN radio is disabled when the timer Tw1 is running and if the USIM in the UE remains the same when the WLAN radio is enabled, shall behave as follows when the WLAN radio is enabled:

- let t1 be the time remaining for Tw1 timeout when the WLAN radio was disabled and let t be the time elapsed since the WLAN radio was disabled until the WLAN radio was enabled. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1;

3) if the cause of failure is #26 "Insufficient resources" and the Tw1 item is not included in the item list field, may send a SCM_REQUEST message with the CONNECTIVITY_TYPE item indicating PDN connection and with APN item indicating the same APN;

4) if the initial attach, or the handover attach is requested, and the cause of failure is #38 "Network failure" as defined in subclause 8.1.4.10.2:

   A) if the Tw1 item is included in the item list field, shall behave as follows:

      i) if the timer value received in the Tw1 item indicates neither zero nor deactivated, shall start the Tw2 timer with the timer value provided in the Tw1 item, and shall not try again until the backoff timer expires or the UE is switched off or the UICC containing the USIM is removed;

      ii) if the timer value received in the Tw1 item indicates that this timer is deactivated, shall not try again until the UE is switched off or the UICC containing the USIM is removed; and

      iii) if the timer value received in the Tw1 item indicates zero, may send another SCM_REQUEST message with the CONNECTIVITY_TYPE item indicating PDN connection and with APN item indicating the same APN; and

   B) if the Tw1 item is not included in the item list field, shall start an implementation specific backoff timer and not try again until the backoff timer expires or the UE is switched off or the UICC containing the USIM is removed; and

NOTE 3: Existing Tw1 item can be reused by the network to provide back off timer value to start Tw2 timer.

5) if the initial attach, or the handover attach is requested, and the cause of failure is #27 "Unknown APN" as defined in subclause 8.1.4.10.2:

   a) if the Tw1 item is included in the item list field, shall behave as follows:

      i) if the timer value received in the Tw1 item indicates neither zero nor deactivated, shall start the Tw2 timer with the timer value provided in the Tw1 item, and shall not send another SCM_REQUEST message with the CONNECTIVITY_TYPE item indicating PDN connection and with APN item indicating the same APN to the same PLMN until the backoff timer expires or the UE is switched off or the UICC containing the USIM is removed;

      ii) if the timer value received in the Tw1 item indicates that this timer is deactivated, shall not send another SCM_REQUEST message with the CONNECTIVITY_TYPE item indicating PDN connection and with APN item indicating the same APN to the same PLMN until the UE is switched off or the UICC containing the USIM is removed; and

      iii) if the timer value received in the Tw1 item indicates zero, may send another SCM_REQUEST message with the CONNECTIVITY_TYPE item indicating PDN connection and with APN item indicating the same APN; and

   b) if the Tw1 item is not included in the item list field, shall not retry the authentication procedure with the same WLAN for the same APN to the same PLMN until the UE is switched off or the UICC containing the USIM is removed, unless the UE has an implementation specific backoff timer. In that case, the UE shall not retry until that implementation specific timer expires.

6.4.2.6.2A Usage of single-connection mode (SCM) - emergency

If the UE needs to establish an IMS emergency session over trusted WLAN access, the UE shall:

1) if the UE already has active PDN connection, the UE shall detach first (see 3GPP TS 23.402 [6]) and then follow item 2) below to start initial attach procedure for emergency service; and

2) if the UE does not have an active PDN connection and requests usage of the SCM, the UE shall start initial attach procedure for emergency service using the procedures specified in subclause 6.4.2.6.2. In addition,

   a) upon receiving EAP-Request/AKA'-Challenge message:

      - if the CONNECTION_MODE_CAPABILITY item in the item list field indicates support of emergency services, the UE shall respond with the EAP-Response/AKA'-Challenge message with the ATTACHMENT_TYPE item in the item list field set to "emergency attach" or "emergency handover"; or

- if the CONNECTION_MODE_CAPABILITY item in the item list field does not indicate support of emergency services, the UE shall respond with the EAP-Response/AKA'-Client-Error message as described in subclause 6.4.2.6.4. The UE shall re-initiate initial attach procedure for emergency service by selecting a different WLAN supporting emergency service; or

b) upon receiving EAP-Request/3GPP-LimitedService-Init-Info message including the AT_TWAN_CONN_MODE attribute with the message type of message field indicating CONNECTION_CAPABILITY and message field contains CONNECTION_MODE_CAPABILITY item in the item list field indicating support of SCM and emergency services,

- if the UE supports the SCM and requests the usage of the SCM, the UE shall respond with the EAP-Response/3GPP-LimitedService-Init-Info message and shall include the AT_TWAN_CONN_MODE attribute with the message type field set to SCM_REQUEST and in the item list field shall:

i) include a ATTACHMENT_TYPE item indicating whether an emergency attach or emergency handover is requested;

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

iii) if emergency 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

iv) 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

c) upon receiving the EAP-Request/3GPP-LimitedService-Notif message including the AT_TWAN_CONN_MODE attribute with the message type field of the message field indicating SCM_RESPONSE and the item list field:

- the UE shall:

i) determine 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;

ii) determine the protocol configuration options in the PROTOCOL_CONFIGURATION_OPTIONS item if a PROTOCOL_CONFIGURATION_OPTIONS item as described in subclause 8.1.4.9 is included in the item list field;

iii) if a IPV4_ADDRESS item as described in subclause 8.1.4.11 is included in the item list field, determine the IPv4 address allocated to the UE for the PDN connection in the IPV4_ADDRESS item;

iv) if a IPV6_INTERFACE_IDENTIFIER item as described in subclause 8.1.4.12 is included in the item list field, determine the IPv6 interface identifier allocated to the UE for the PDN connection in the IPV6_INTERFACE_IDENTIFIER item and use it when building the IPv6 link local address; and

v) determine the TWAG user plane MAC address in the TWAG_UP_MAC_ADDRESS item as described in subclause 8.1.4.14 included in the item list field, and use the TWAG user plane MAC address for encapsulating user plane packets according to 3GPP TS 23.402 [6]; and

d) if the UE had requested emergency attach or emergency handover of an emergency session, upon receiving the EAP-Request/AKA'-Notification message, if the AT_NOTIFICATION attribute indicates failure, the UE shall detach and then perform initial attach procedure for emergency service by selecting a different WLAN supporting emergency service.

6.4.2.6.3 Usage of multi-connection mode (MCM)

If:

a) the UE supports the MCM;

b) 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:

1) contains the message type field indicating CONNECTION_CAPABILITY; and

2) contains the item list field:

A) including the CONNECTION_MODE_CAPABILITY item as described in subclause 8.1.4.8 indicating support of MCM;

B) including the SUPPORTED_WLCP_TRANSPORTS item as described in subclause 8.1.4.15; and

C) if the UE requests an emergency attach or an emergency handover, including the CONNECTION_MODE_CAPABILITY item as described in subclause 8.1.4.8 indicating that emergency services are supported;

c) at least one WLCP transport indicated as supported in the SUPPORTED_WLCP_TRANSPORTS item is also supported by the UE; and

d) 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:

1) shall set the message type field to MCM_REQUEST; and

2) in the item list field:

A) if the UE requests an emergency attach or an emergency handover, shall include an ATTACHMENT_TYPE item according to subclause 8.1.4.4 indicating whether an emergency attach, or an emergency handover is requested; and

b) shall include the AT_RESULT_IND attribute in the EAP-Response/AKA'-Challenge message.

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:

1) shall determine the NSWO authorization in the AUTHORIZATIONS item as described in subclause 8.1.4.7 included in the item list field;

2) shall determine the TWAG control plane address(es) in the TWAG_CP_ADDRESS item as described in subclause 8.1.4.13 included in the item list field; and

3) shall derive the WLCP key as described in Annex A.3 in 3GPP TS 33.402 [15]; and

NOTE: After receiving EAP Success message terminating the EAP procedures after successful authentication and authorization for MCM access to EPC, the UE establishes a DTLS connection with the TWAG and initiates WLCP procedures according to 3GPP TS 24.244 [56].

b) if the AT_NOTIFICATION attribute indicates failure, shall determine the cause of failure in the ACCESS_CAUSE or CAUSE item as described in subclause 8.1.4.17 and 8.1.4.10 included in the item list field.

6.4.2.6.3A Usage of multi-connection mode (MCM) - emergency

If the UE needs to establish an IMS emergency session over trusted WLAN access, the UE shall:

1) if the UE already has active PDN connection:

- if the TWAN does not supports emergency service, the UE shall detach first and then follow item 2) below to start initial attach procedure for emergency service and selecting a WLAN supporting Emergency service; or

- if the connected TWAN supports emergency service, the UE shall initiate PDN connectivity establishment procedures as specified in 3GPP TS 24.244 [56].

2) if the UE does not have an active PDN connection and requests usage of the MCM, the UE shall start initial attach procedure for emergency service using the procedures specified in subclause 6.4.2.6.3. In addition,

   a) upon receiving EAP-Request/AKA'-Challenge message:

      - if the CONNECTION_MODE_CAPABILITY item in the item list field indicates support of emergency services, the UE shall respond with the EAP-Response/AKA'-Challenge message with the ATTACHMENT_TYPE item in the item list field set to "emergency attach" or "emergency handover"; or

      - if the CONNECTION_MODE_CAPABILITY item in the item list field does not indicate support of emergency services, the UE shall respond with the EAP-Response/AKA'-Client-Error message as described in subclause 6.4.2.6.4. The UE shall re-initiate initial attach procedure for emergency service by selecting a different WLAN supporting emergency service; or

   b) upon receiving EAP-Request/3GPP-LimitedService-Init-Info message including the AT_TWAN_CONN_MODE attribute with the message type of message field indicating CONNECTION_CAPABILITY and message field contains CONNECTION_MODE_CAPABILITY item in the item list field indicating support of MCM and emergency services,

      - if the UE supports the MCM and requests the usage of the MCM and

         i) message field of the AT_TWAN_CONN_MODE attribute contains SUPPORTED_WLCP_TRANSPORTS item as described in subclause 8.1.4.15; and

         ii) at least one WLCP transport indicated as supported in the SUPPORTED_WLCP_TRANSPORTS item is also supported by the UE,

      the UE shall respond with the EAP-Response/3GPP-LimitedService-Init-Info message and shall:

         i) include the AT_TWAN_CONN_MODE attribute with the message type field set to MCM_REQUEST;

   c) upon receiving the EAP-Request/3GPP-LimitedService-Notif message including the AT_TWAN_CONN_MODE attribute with the message type of message field indicating MCM_RESPONSE and the item list field:

      - the UE shall:

         i) determine the TWAG control plane address(es) in the TWAG_CP_ADDRESS item as described in subclause 8.1.4.13 included in the item list field;

         ii) derive the WLCP key as described in Annex A.3 in 3GPP TS 33.402 [15].

NOTE: After receiving EAP Success message terminating the EAP procedures after successful authentication and authorization for MCM access to EPC, the UE establishes a DTLS connection with the TWAG and initiates WLCP procedures according to 3GPP TS 24.244 [56].

   d) if the UE had requested emergency attach or emergency handover of an emergency session, upon receiving the EAP-Request/AKA'-Notification message, if the AT_NOTIFICATION attribute indicates failure, the UE shall detach and then perform initial attach procedure for emergency service by selecting a different WLAN supporting emergency service.

6.4.2.6.3B Usage of transparent single-connection mode (TSCM) - emergency

The emergency session is not supported for the UE using TSCM mode.

NOTE: If the UE in TSCM mode already has active PDN connection, the UE remains connected.

6.4.2.6.4 Network support not available

If the EAP-Request/AKA'-Challenge message does not include the AT_TWAN_CONN_MODE attribute as described in subclause 8.2.7.1, then only TSCM is available.

If the UE supports SCM, the UE does not support MCM, and 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:

1) contains the message type field indicating CONNECTION_CAPABILITY; and

2) contains the item list field including the CONNECTION_MODE_CAPABILITY item as described in subclause 8.1.4.8 not indicating support of SCM;

then only TSCM is available.

If the UE does not support SCM, the UE supports MCM, and 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:

1) contains the message type field indicating CONNECTION_CAPABILITY; and

2) contains the item list field including the CONNECTION_MODE_CAPABILITY item as described in subclause 8.1.4.8 not indicating support of MCM;

then only TSCM is available.

If the UE does not support SCM, the UE supports MCM, 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:

1) contains the message type field indicating CONNECTION_CAPABILITY; and

2) contains the item list field:

   A) including the CONNECTION_MODE_CAPABILITY item as described in subclause 8.1.4.8 indicating support of MCM; and

   B) including the SUPPORTED_WLCP_TRANSPORTS item as described in subclause 8.1.4.15;

and none of the WLCP transport indicated as supported in the SUPPORTED_WLCP_TRANSPORTS item is also supported by the UE, then only TSCM is available.

If only TSCM is available:

a) if the UE does not request an emergency attach, the UE does not request an emergency handover and the UE is willing to use TSCM, the UE shall act as in TSCM; and

b) if the UE requests an emergency attach or the UE requests an emergency handover or the UE is unwilling to use TSCM, the UE shall send EAP-Response/AKA'-Client-Error message.

NOTE: In TSCM, successful EAP-AKA' authentication triggers creation of a PDN connection to the default APN. The UE can be unwilling to use the PDN connection to the default APN e.g. because the UE needs to perform handover of a PDN connection, because the UE needs to establish a PDN connection to an APN other than the default APN, because the UE needs to establish multiple PDN connections, or because the UE has no usage for the PDN connection to the default APN and wants to avoid any possible charges related to the PDN connection to the default APN.

If the UE requests an emergency attach or an emergency handover, and 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:

1) contains the message type field indicating CONNECTION_CAPABILITY; and

2) contains the item list field including the CONNECTION_MODE_CAPABILITY item as described in subclause 8.1.4.8 not indicating support of emergency services;

then the UE shall send EAP-Response/AKA'-Client-Error message.

6.4.2.7 Mobile Equipment Identity Signalling

If the UE receives:

- an EAP-Request/AKA'-Challenge message; or
- an EAP-Request/3GPP-LimitedService-Init-Info message;

containing the AT_DEVICE_IDENTITY attribute and the Identity Type field of the received AT_DEVICE_IDENTITY attribute is set to either 'IMEI' or 'IMEISV' and the Identity Value field is empty, then if the UE's Mobile Equipment Identity IMEI or IMEISV is available, the UE shall include IMEI or IMEISV in the AT_DEVICE_IDENTITY attribute in:

- the EAP-Response/AKA'-Challenge message; or
- the EAP-Response/3GPP-LimitedService-Init-Info message;

as follows:

- if IMEISV are available, the UE shall include IMEISV in the AT_DEVICE_IDENTITY attribute. The Identity Type field of the AT_DEVICE_IDENTITY attribute shall be set to 'IMEISV': and
- if IMEI is available and IMEISV is not available, the UE shall include IMEI in the AT_DEVICE_IDENTITY attribute. The Identity Type field of the AT_DEVICE_IDENTITY attribute shall be set to 'IMEI'.

The AT_DEVICE_IDENTITY attribute shall be sent as an encrypted attribute and included in the value field of the AT_ENCR_DATA attribute as described in IETF RFC 4187 [33].

The detailed coding of the AT_DEVICE_IDENTITY attribute is described in subclause 8.2.8.1.

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.

6.4.3.1A Identity Management - emergency session

Upon receiving a request from the UE for emergency session establishment, if

- IMSI is provided to the network but IMSI authentication cannot proceed or IMSI authentication has failed or the 3GPP AAA server cannot determine if authentication is successful; and
- the 3GPP AAA server is configured to accept unauthenticated emergency session over WLAN,

the 3GPP AAA server requests IMEI from the UE as specified in subclause 6.4.3.6 using the EAP-Request/3GPP-LimitedService-Init-Info message.

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.

For WLAN access, after the UE has been successfully authenticated and the EPC access and Non-Seamless WLAN Offload are not authorized for the UE, the 3GPP AAA Server shall invoke an EAP-Request/AKA'-Notification dialogue and indicate this to the UE by using the AT_NOTIFICATION attribute value 1031 – "User has not subscribed to the requested service" as defined in IETF RFC 4187 [33].

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:

   1) 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 and indicating whether the network supports the emergency services; and

   2) if the network supports MCM, include a SUPPORTED_WLCP_TRANSPORTS item according to subclause 8.1.4.15 indicating WLCP transport(s) supported by the TWAG.

6.4.3.5.1A Emergency session connection mode negotiation for unauthenticated UEs

If the 3GPP AAA server is configured to accept unauthenticated emergency session over WLAN and IMEI was received or IMSI was received but IMSI authentication cannot proceed, the 3GPP AAA server shall initiate connection mode negotiation with the UE as follows:

- if the 3GPP AAA server supports SCM, MCM or both, the 3GPP AAA server shall include the AT_TWAN_CONN_MODE attribute according to subclause 8.2.7.1 in the EAP-Request/3GPP-LimitedService-Init-Info 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:

1) include a CONNECTION_MODE_CAPABILITY item according to subclause 8.1.4.8 indicating whether the network supports SCM, MCM or any combination of them, and indicating emergency service is supported; and

2) if the network supports MCM, include a SUPPORTED_WLCP_TRANSPORTS item according to subclause 8.1.4.15 indicating WLCP transport(s) supported by the TWAG.

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:

- if the ATTACHMENT_TYPE item according to subclause 8.1.4.4 indicating an emergency attach, or an emergency handover is included in the item list field of the message field, shall identify that the attach is for emergency services; and
- shall trigger the TWAN to establish the connectivity of the requested connectivity type according to 3GPP TS 23.402 [6].

If:

- the 3GPP AAA server authorizes the requested connectivity; and
- 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) if the initial attach, or the handover attach is requested, 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;

         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;

         iv) if an IPv4 address is allocated to the UE for the PDN connection, include a IPV4_ADDRESS item according to subclause 8.1.4.11;

         v) if an IPv6 interface identifier is allocated to the UE for the PDN connection, include a IPV6_INTERFACE_IDENTIFIER item according to subclause 8.1.4.12; and

vi) include a TWAG_UP_MAC_ADDRESS item according to subclause 8.1.4.14.

If the 3GPP AAA server does not authorize the requested connectivity and if:

- the attach is not for emergency session; or
- the attach is for emergency session and if the 3GPP AAA server is not configured to accept unauthenticated emergency session over WLAN,

NOTE: The case where the 3GPP AAA server does not authorize the request but is configured to accept unauthenticated emergency session over WLAN is specified in subclause 6.4.3.5.2A.

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;

2) in the item list field, include a ACCESS_CAUSE or CAUSE item according to subclause 8.1.4.17 and 8.1.4.10 indicating the cause of failure;

3) if the initial attach, or the handover attach is requested, the cause of failure is #26 "Insufficient resources" and a value of backoff timer is to be provided to the UE for the PDN connection, include a Tw1 item according to subclause 8.1.4.16;

3A) if the initial attach, or the handover attach is requested, the cause of failure is #38 "Network failure" or #27 "unknown APN" and a value of backoff timer is to be provided to the UE for the PDN connection, include a Tw1 item according to subclause 8.1.4.16;

4) if the 3GPP AAA Server receives DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION sent by the HSS as specified in 3GPP TS 29.273 [17], indicate this to the UE by using "Non-3GPP access to EPC not allowed" value in the ACCESS_CAUSE item;

5) if the 3GPP AAA Server receives DIAMETER_ERROR_ROAMING_NOT_ALLOWED sent by the HSS as specified in 3GPP TS 29.273 [17], indicate this to the UE by using "PLMN not allowed" value in the ACCESS_CAUSE item;

6) if the 3GPP AAA Server receives DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION sent by the HSS as specified in 3GPP TS 29.273 [17], indicate this to the UE by using #27 "Unknown APN" value in the CAUSE item;

7) if the 3GPP AAA Server receives DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED sent by the HSS as specified in 3GPP TS 29.273 [17], indicate this to the UE by using #3 "RAT type not allowed" value in the ACCESS_CAUSE item; and

8) if the 3GPP AAA Server receives DIAMETER_UNABLE_TO_COMPLY sent by HSS as specified in 3GPP TS 29.273 [17], indicate this to the UE by using #38 "Network failure" in the CAUSE item.

6.4.3.5.2A Usage of single-connection mode (SCM) - emergency

If the 3GPP AAA Server supports IMS Emergency sessions over WLAN, the 3GPP AAA server shall:

- if IMSI was received and IMSI authentication can proceed, the 3GPP AAA server invokes an EAP-Request/AKA'-Notification dialogue to indicate success or failure to the UE as described in subclause 6.4.3.5.2;
- if IMSI was received but IMSI authentication cannot proceed, then

A) if the 3GPP AAA server is configured to accept unauthenticated emergency session over WLAN:

a) the 3GPP AAA server sends EAP Request/3GPP-LimitedService-Init-Info message as specified in subclause 6.4.3.5.1A;

b) upon receiving the EAP-Response/3GPP-LimitedService-Init-Info message including the AT_TWAN_CONN_MODE attribute with the message type of message field indicating SCM_REQUEST and the item list field, the 3GPP AAA server shall include the AT_TWAN_CONN_MODE attribute according to subclause 8.2.7.1 in the EAP-Request/3GPP-LimitedService-Notif message. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the 3GPP AAA server shall:

i) set the message type field to SCM_RESPONSE; and

ii) in the item list field:

1) include the PDN type supported in the PDN connection in the PDN_TYPE item as described in subclause 8.1.4.6 in the item list field;

2) include the protocol configuration options in the PROTOCOL_CONFIGURATION_OPTIONS item if a PROTOCOL_CONFIGURATION_OPTIONS item as described in subclause 8.1.4.9 is in the item list field;

3) if an IPv4 address is allocated to the UE for the PDN connection, include a IPV4_ADDRESS item according to subclause 8.1.4.11;

4) if an IPv6 interface identifier is allocated to the UE for the PDN connection, include a IPV6_INTERFACE_IDENTIFIER item according to subclause 8.1.4.12; and

5) include a TWAG_UP_MAC_ADDRESS item according to subclause 8.1.4.14; and

c) upon receiving the EAP-Response/3GPP-LimitedService-Notif message, the 3GPP AAA server shall generate the MSK using IMEI as described in subclause 13.4 in 3GPP TS 33.402 [15] and send EAP Success message to the UE to allow the UE to proceed with emergency session establishment; or

B) if the 3GPP AAA server is not configured to accept unauthenticated emergency session over WLAN, the 3GPP AAA server shall reject the emergency session request and return an EAP Failure message to the UE; or

- if IMEI was received,

A) if the 3GPP AAA server is configured to accept unauthenticated emergency session over WLAN:

a), the 3GPP AAA server sends EAP Request/3GPP-LimitedService-Init-Info message to as specified in subclause 6.4.3.5.1A;

b) upon receiving the EAP-Response/3GPP-LimitedService-Init-Info message including the AT_TWAN_CONN_MODE attribute with the message type of message field indicating SCM_REQUEST and the item list field, the 3GPP AAA server shall include the AT_TWAN_CONN_MODE attribute according to subclause 8.2.7.1 in the EAP-Request/3GPP-LimitedService-Notif message. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the 3GPP AAA server shall:

i) set the message type field to SCM_RESPONSE; and

ii) in the item list field:

1) include the PDN type supported in the PDN connection in the PDN_TYPE item as described in subclause 8.1.4.6 in the item list field;

2) include the protocol configuration options in the PROTOCOL_CONFIGURATION_OPTIONS item if a PROTOCOL_CONFIGURATION_OPTIONS item as described in subclause 8.1.4.9 is in the item list field;

3) if an IPv4 address is allocated to the UE for the PDN connection, include a IPV4_ADDRESS item according to subclause 8.1.4.11;

4) if an IPv6 interface identifier is allocated to the UE for the PDN connection, include a IPV6_INTERFACE_IDENTIFIER item according to subclause 8.1.4.12; and

5) include a TWAG_UP_MAC_ADDRESS item according to subclause 8.1.4.14; and

c) upon receiving the EAP-Response/3GPP-LimitedService-Notif message, the 3GPP AAA server shall generate the MSK using IMEI as described in subclause 13.4 in 3GPP TS 33.402 [15] and send EAP Success message to the UE to allow the UE to proceed with emergency session establishment; or

B) if the 3GPP AAA server is not configured to accept unauthenticated emergency session over WLAN, the 3GPP AAA server shall reject the emergency session request and return an EAP Failure message to the UE.

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 server authorizes the request. If the ATTACHMENT_TYPE item according to subclause 8.1.4.4 indicating an emergency attach, or an emergency handover is included in the item list field of the message field, the 3GPP AAA server shall identify that the attach is for emergency services; 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:

A) include an AUTHORIZATIONS item according to subclause 8.1.4.7 indicating whether UE is authorized to use NSWO; and

B) include a TWAG_CP_ADDRESS item according to subclause 8.1.4.13 indicating the TWAG control plane address.

If the 3GPP AAA server does not authorize the request and if

- the attach is not for emergency services; or

- the attach is for emergency services and if the 3GPP AAA server is not configured to accept unauthenticated emergency session over WLAN,

NOTE: The case where the 3GPP AAA server does not authorize the request but is configured to accept unauthenticated emergency session over WLAN is specified in subclause 6.4.3.5.3A.

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;

2) in the item list field, include a ACCESS_CAUSE or CAUSE item according to subclause 8.1.4.17 and 8.1.4.10 indicating the cause of failure;

3) if the 3GPP AAA Server receives DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION sent by the HSS as specified in 3GPP TS 29.273 [17], indicate this to the UE by using "Non-3GPP access to EPC not allowed" value in the ACCESS_CAUSE item;

4) if the 3GPP AAA Server receives DIAMETER_ERROR_ROAMING_NOT_ALLOWED sent by the HSS as specified in 3GPP TS 29.273 [17], indicate this to the UE by using "PLMN not allowed" value in the ACCESS_CAUSE item;

5) if the 3GPP AAA Server receives DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION sent by the HSS as specified in 3GPP TS 29.273 [17], indicate this to the UE by using #27 "Unknown APN" value in the CAUSE item;

6) if the 3GPP AAA Server receives DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED sent by the HSS as specified in 3GPP TS 29.273 [17], indicate this to the UE by using #3 "RAT type not allowed" value in the ACCESS_CAUSE item; and

7) if the 3GPP AAA Server receives DIAMETER_UNABLE_TO_COMPLY sent by HSS as specified in 3GPP TS 29.273 [17], indicate this to the UE by using #38 "Network failure" in the CAUSE item.

6.4.3.5.3A Usage of multi-connection mode (MCM) - emergency

If the 3GPP AAA Server supports IMS Emergency sessions over WLAN, the 3GPP AAA server shall:

- if IMSI was received and IMSI authentication can proceed, the 3GPP AAA server invokes an EAP-Request/AKA'-Notification dialogue to indicate success to the UE as described in subclause 6.4.3.5.3;

- if IMSI was received but IMSI authentication cannot proceed, then

  A) if the 3GPP AAA server is configured to accept unauthenticated emergency session over WLAN:

     a), the 3GPP AAA server sends EAP Request/3GPP-LimitedService-Init-Info message as specified in subclause 6.4.3.5.1A;

     b) upon receiving the EAP-Response/3GPP-LimitedService-Init-Info message including the AT_TWAN_CONN_MODE attribute with the message type of message field indicating SCM_REQUEST and the item list field, the 3GPP AAA server shall include the AT_TWAN_CONN_MODE attribute according to subclause 8.2.7.1 in the EAP-Request/3GPP-LimitedService-Notif message. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the 3GPP AAA server shall:

        i) set the message type field to SCM_RESPONSE; and

        ii) in the item list field:

           1) include the TWAG control plane address(es) in the TWAG_CP_ADDRESS item as described in subclause 8.1.4.13 in the item list field; and

     c) upon receiving the EAP-Response/3GPP-LimitedService-Notif message, the 3GPP AAA server shall generate the MSK using IMEI as described in subclause 13.4 in 3GPP TS 33.402 [15] and send EAP Success message to the UE to allow the UE to proceed with emergency session establishment; or

  B) if the 3GPP AAA server is not configured to accept unauthenticated emergency session over WLAN, the 3GPP AAA server shall reject the emergency session request and return an EAP Failure message to the UE; or

- if IMEI was received,

  A) if the 3GPP AAA server is configured to accept unauthenticated emergency session over WLAN:

     a), the 3GPP AAA server sends EAP Request/3GPP-LimitedService-Init-Info message as specified in subclause 6.4.3.5.1A;

     b) upon receiving the EAP-Response/3GPP-LimitedService-Init-Info message including the AT_TWAN_CONN_MODE attribute with the message type of message field indicating MCM_REQUEST and the item list field, the 3GPP AAA server shall include the AT_TWAN_CONN_MODE attribute according to subclause 8.2.7.1 in the EAP-Request/3GPP-

LimitedService-Notif message. In the message field according to subclause 8.1.4.1 of the AT_TWAN_CONN_MODE attribute, the 3GPP AAA server shall:

i) set the message type field to MCM_RESPONSE; and

ii) in the item list field:

1) include the TWAG control plane address(es) in the TWAG_CP_ADDRESS item as described in subclause 8.1.4.13 in the item list field; and

c) upon receiving the EAP-Response/3GPP-LimitedService-Notif message, the 3GPP AAA server shall generate the MSK using IMEI as described in subclause 13.4 in 3GPP TS 33.402 [15] and send EAP Success message to the UE to allow the UE to proceed with emergency session establishment; or

B) if the 3GPP AAA server is not configured to accept unauthenticated emergency session over WLAN, the 3GPP AAA server shall reject the emergency session request and return an EAP Failure message to the UE.

6.4.3.5.3B Usage of transparent single-connection mode (TSCM) - emergency

The emergency session is not supported for the UE using TSCM mode.

6.4.3.5.4 Network support not available

NOTE: If the network does not support a TWAN connection mode and the UE needs to request usage of the not supported TWAN connection mode, upon sending EAP-Request/AKA'-Challenge message, the network receives EAP-Response/AKA'-Client-Error message. Handling defined in IETF RFC 5448 [38] applies for the EAP-Response/AKA'-Client-Error message.

6.4.3.6 Mobile Equipment Identity Signalling

If the network supports Mobile Equipment Identity signalling over trusted WLAN, the 3GPP AAA server shall include the AT_DEVICE_IDENTITY attribute in:

- the EAP-Request/AKA'-Challenge message; or
- the EAP-Request/3GPP-LimitedService-Init-Info message;

with the Identity Type field set to either 'IMEI' or 'IMEISV' and an empty Identity Value field to request the UE to provide the Mobile Equipment Identity indicated in the Identity Type.

Upon receiving:

- the EAP-Response/AKA'-Challenge message; or
- the EAP-Response/3GPP-LimitedService-Init-Info message;

from the UE, if the AT_DEVICE_IDENTITY attribute is included and Identity Type field is set to either 'IMEI' or 'IMEISV', then the 3GPP AAA server shall forward the received Mobile Equipment Identity to the TWAN as specified in 3GPP TS 29.273 [17].

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 the UE accesses EPC via S2a using trusted non-3GPP IP access and establishes 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 the UE accesses EPC via S2c using non-3GPP IP access, the UE shall follow the procedures described in 3GPP TS 24.303 [11] to connect to multiple PDNs.

If the UE accesses EPC via S2a using non-3GPP IP access and it is handing over from a source access network to a target non-3GPP IP access 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, ePDG 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 6.5.2.2, 6.5.2.4 and 6.5.2.3.

6.5.2.2 UE procedures

6.5.2.2.1 General

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.

After the UE has been successfully authenticated, the UE may receive EAP-Request/AKA-Notification dialogue with AT_NOTIFICATION attribute value 1031 – "User has not subscribed to the requested service" as defined in IETF RFC 4187 [33]. Then the UE shall not initiate the EPC access procedure to same ePDG until switching off or the UICC containing the USIM is removed.

NOTE: Swittching off and USIM change conditions are implemented taking into consideration the user experience aspect.

6.5.2.2.2 EAP AKA

6.5.2.2.2.1 Identity management

The support of user identity privacy as defined in IETF RFC 4187 [33] and based on temporary identity is mandatory for the UE.

As defined in 3GPP TS 33.402 [15], the UE sends the user identity (in the IDi payload) in the first message of the IKE_AUTH phase. The user identity sent by the UE in the IDi payload depends on the presence of the temporary identity as defined in IETF RFC 4187 [33]:

- If valid fast re-authentication identity is available, the UE shall use the fast re-authentication NAI;
- Otherwise if valid pseudonym is available, the UE shall use the pseudonym NAI;
- Otherwise the UE shall use the permanent IMSI-based or IMEI-based NAI.

The temporary identities shall be in the form of a NAI, as specified in 3GPP TS 23.003 [3] clause 19. The permanent identity shall be in the form of a NAI in which username is derived from IMSI or IMEI as defined in 3GPP TS 23.003 [3]. IETF RFC 4187 [33] defines the leading digits to identify the authentication mechanism. The leading digit defined for EAP-AKA authentication shall be used in the NAI for both the temporary identities and the permanent identity.

The UE after successful EAP authentication may store the new temporary identity(ies) received in AT_ENCR_DATA attribute together with the fast re-authentication parameters (new master key, transient EAP keys and counter value) in the non-volatile memory of the UE or in the USIM as specified in 3GPP TS 31.102 [45]. In this later case the pseudonym is stored in the "Pseudonym" data file and the fast re-authentication identity, new master key, transient EAP keys and counter value in the "Re-authentication identity" data file.

If no new temporary identity was received in AT_ENCR_DATA attribute of a successful EAP authentication, the stored temporary identity becomes invalid and the UE shall not send this temporary identity at the next EAP authentication. In case the temporary identity is stored in the USIM, the UE shall set the username of the corresponding temporary

identity field to the "deleted" value (hexadecimal value FF) to indicate that this temporary identity is invalid as specified in 3GPP TS 23.003 [3].

6.5.2.2.2.2 Protected result indications

The UE shall support protected result indications (i.e. MAC protected) as specified in IETF RFC 4187 [33].

6.5.2.3 3GPP AAA server procedures

6.5.2.3.1 General

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].

After the UE has been successfully authenticated and the EPC access is not authorized for the UE, the 3GPP AAA Server shall invoke an EAP-Request/AKA-Notification dialogue and indicate this to the UE by using the AT_NOTIFICATION attribute value 1031 – "User has not subscribed to the requested service" as defined in IETF RFC 4187 [33].

6.5.2.3.2 EAP-AKA

6.5.2.3.2.1 Identity management

The support of user identity privacy is mandatory for the 3GPP AAA server. The usage of this feature depends on operator's policies.

If user identity privacy is used, the 3GPP AAA server shall send new encrypted temporary identity (pseudonym and/ or fast re-authentication identity) to the UE in every EAP authentication procedure. 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.

6.5.2.3.2.2 EAP AKA based authentication

The 3GPP AAA server shall support EAP AKA based authentication as specified in IETF RFC 4187 [33].

6.5.2.3.2.3 Fast re-authentication

The 3GPP AAA server shall support fast re-authentication as specified in the IETF RFC 4187 [33]. Fast re-authentication should be enabled in the 3GPP AAA server. The decision of using fast re-authentication is taken in the 3GPP AAA server depending on operator's policies. The 3GPP AAA server indicates to the UE the decision of using fast re-authentication by means of sending the fast re-authentication identity in the EAP authentication procedure (i.e. in EAP-Request/AKA/Challenge or EAP-Request/AKA-re-authentication). When the 3GPP AAA server sends a fast re-authentication identity to the UE, the 3GPP AAA server shall also include a pseudonym when allowed by the IETF RFC 4187 [33]. In this way, the UE retains a pseudonym if the 3GPP AAA server defers to full authentication.

6.5.2.3.2.4 Protected result indications

The 3GPP AAA server should support protected result indications (i.e. MAC protected) for EAP AKA as specified in IETF RFC 4187 [33]. The usage of this feature depends on operator's policies.

6.5.2.4 ePDG procedures

During the authentication of the UE for accessing the EPC via the ePDG, the ePDG shall initiate EAP-AKA based authentication between the UE and the 3GPP AAA server as specified in 3GPP TS 33.402 [15]. The ePDG shall extract the EAP messages received from the UE over IKEv2, and send them to the 3GPP AAA Server and shall send the EAP message received from the 3GPP AAA Server to the UE over IKEv2 messages as defined in 3GPP TS 33.402 [15].

At the reception of the first message of the IKE_AUTH phase from the UE, indicating to the ePDG that the UE wants to use EAP over IKEv2 (i.e. AUTH parameter absent), the ePDG sends the Authentication and Authorization request to the 3GPP AAA server including the EAP_resp/Identity in the EAP payload, with the User Identity retrieved from the IDi payload and the APN information retrieved from the IDr payload of the incoming message from the UE.

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 the UE accesses EPC via S2b using untrusted non-3GPP IP access, and the UE establishes additional PDN connections, the UE shall establish a new 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 establishing an additional PDN connection, the UE shall not indicate the INITIAL_CONTACT notification.

NOTE 2: When using the S2b interface to establish an additional PDN connection, the new IPSec tunnel establishment includes a new IKEv2 authentication and security association establishment as specified in subclause 7.2.2.

When the UE accesses EPC via S2c using untrusted non-3GPP IP access, the UE shall follow the procedures described in 3GPP TS 24.303 [11] when establishing multiple PDN connections. For multiple PDN connections, 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 accessing an EPC via 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 3: 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 between the 3GPP2 HRPD Serving Gateway (HSGW) and the PDN Gateway (P-GW) in the EPC by referencing 3GPP TS 29.275 [18], when the HSGW supports UEs accessing EPC via S2a;
- 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 cdma2000® HRPD access network supporting access S-GW or PDN GW via S2a-interface 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;
- if IMSI is not available or unauthenticated, then the emergency NAI 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;
- 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;
- 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 WLAN offload.
- WLAN Selection Policy to assist the UE with selecting the WLAN access network;
- Home Network Preference information to assists the UE in selecting a WLAN and a service provider for 3GPP-based authentication over WLAN;
- Visited Network Preference information to assist the UE in selecting a WLAN and a service provider for 3GPP-based authentication over WLAN when the UE is roaming in a V-PLMN; or
- Rule selection information to assist the roaming UE with selecting the active ANDSF rules to be used.

The ANDSF can provide ISRP rules to a UE independently of the UE's support for IFOM, MAPCON, NSWO, RAT differentiation in ISRP or RAN-assisted WLAN interworking. Handling of ISRP nodes unsupported by the UE is described in in 3GPP TS 24.312 [13].

The ANDSF can provide IARP rules to a UE independently of the UE's support for NSWO, Inter-APN routing or RAN-assisted WLAN interworking. Handling of IARP nodes unsupported by the UE is described in in 3GPP TS 24.312 [13].

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 or rule selection information to a roaming UE. If the roaming UE receives any IARP or rule selection information 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.

If the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, then the access stratum layer of the 3GPP access can provide RAN assistance parameters and corresponding (E-)UTRAN measurements which are used in accordance with the ANDSF MO defined in 3GPP TS 24.312 [13].

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, ISRP, IARP, WLANSP 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].

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 updatedISMP, ISRP, IARP, WLANSP 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) of these 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.

6.8.2.2.4 UE using information provided by ANDSF

6.8.2.2.4.1 General

ANDSF may provide various types of information to the UE, including access network discovery information, WLAN selection information, ePDG configuration information, inter-system mobility policy, the inter-system routing policies and the inter-APN routing policies. The UE may retain and use this ANDSF information until new or updated information is received.

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 discovering and 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 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 UE may also receive WLAN selection information including WLAN Selection Policy (WLANSP) from H-ANDSF or V-ANDSF or both, rule selection information, and Home Network Preference information from H-ANDSF. The UE may receive Visited Network Preference information from V-ANDSF. The UE may also receive ePDG configuration information from H-ANDSF. The formats of the above information 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 received from the H-ANDSF.

If a UE supporting IFOM, MAPCON, or non-seamless WLAN offload (or any combination of these featureshas ISMP and ISRP available, and if the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, 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, and if the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, 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 or one or more APNs are restricted by the IARP for routing the IP flow, then ISRP shall be used for the routing of IP traffic. When one or more APNs are restricted by the IARP, if a rule for NSWO is matched in the active ISRP rule that restricts the use of the selected WLAN (or any WLAN) for routing the IP flow, then the UE selects a not restricted APN to route the IP flow.

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, and if the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, the ISMP shall be used.

For a UE not supporting any of IFOM, MAPCON capabilities or with all those capabilities disabled, if ISMP, ISRP and IARP are available, and if the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, the IARP and ISMP shall be used. In this case, the UE shall firstly apply ISMP followed by IARP as follows:

- If the 3GPP access is selected by ISMP policy, then the UE shall use the active IARP rule to determine if the IP flow is routed to the PDN connection corresponding to a certain APN. The non-seamless WLAN offload policy, defined in the IARP, shall not be used for routing of IP traffic; and

- If the WLAN access is selected by ISMP policy, then the UE shall use the active IARP rule to determine if the IP flow is routed to the PDN connection corresponding to a certain APN or using the non-seamless WLAN offload.

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

If the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, irrespective of whether any rule in ANDSF policies is 'active' or not, the UE shall periodically re-evaluate ANDSF policies. The value of the periodic re-evaluation timer is implementation dependant. The additional trigger for (re-)evaluating rules is that the 'active' rule becomes invalid (conditions no longer fulfilled), or other manufacturer specific trigger. When the UE receives ANDSF information it shall re-evaluate the available rules along with the new information.

6.8.2.2.4.2 Use of Inter-system Mobility Policy

This subclause applies if the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2.

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.

When the UE is roaming and receives Inter-system Mobility Policies from both H-ANDSF and V-ANDSF, the set of Inter-system Mobility Policies used by the UE is selected as follows:

- If there is rule selection information provisioned in the UE by the H-ANDSF, and if the RPLMN identity is equal to one of the VPLMNs included in the visited PLMNs with preferred rules, the set of Inter-system Mobility Policies from V-ANDSF is selected by the UE.

  If the preferred access technology according to the Inter-system Mobility Policy is WLAN access technology, and if there is no WLANs matching the WLANSP rule(s) from the V-ANDSF, the set of of Inter-system Mobility Policies from H-ANDSF is selected by the UE. However, if at least one WLAN matching one or more groups of selection criteria in the VPLMN's WLANSP rule becomes available, the UE should re-use the WLANSP policies and Inter-system Mobility Policies from V-ANDSF.

- If there is rule selection information provisioned in the UE by the H-ANDSF, and if the RPLMN identity is not equal to any of the VPLMNs included in the visited PLMNs with preferred rules, the set of Inter-system Policies from H-ANDSF is selected by the UE.

  If the preferred access technology according to the Inter-system Mobility Policy is WLAN access technology, and if there is no WLANs matching the WLANSP rule(s) from the H-ANDSF, the set of of Inter-system Mobility Policies from V-ANDSF is selected by the UE. However, if at least one WLAN matching one or more groups of selection criteria in the HPLMN's WLANSP rule becomes available, the UE should re-use the WLANSP policies and Inter-system Mobility Policies from H-ANDSF.

NOTE: How frequently the UE performs the discovery and reselection procedure depends on the UE implementation.

The Inter-system Mobility Policy with the highest priority among the set of Inter-system Mobility Policies selected above is selected as the active Inter-system Mobility Policy. A UE uses the ISMP to decide if the most preferred available WLAN based on the WLANSP rule has higher priority than the 3GPP RAT. If so, the UE shall connect to EPC via WLAN access. Otherwise, the UE shall connect to EPC via 3GPP access. The prioritized list of WLAN in the active ISMP rule shall not be used for WLAN selection.

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 subclause 5.2.3.2;
- 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

This subclause applies if the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2.

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. 3GPP RATs can be prioritized with respect to WLAN access but this prioritization does not influence 3GPP RAT selection; WLAN access networks can be prioritized with respect to 3GPP RATs but those WLANs do not influence WLAN selection; 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. 3GPP RATs can be prioritized with respect to WLAN access but this prioritization does not influence 3GPP RAT selection; WLAN access networks can be prioritized with respect to 3GPP RATs but those WLANs do not influence WLAN selection; 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.

NOTE: After selecting WLAN access for routing user plane traffic by this prioritised list of access technologies, a UE can use an implementation dependent way to prevent the traffic from being routed back to the original RAT again in a short period of time to avoid ping-pong behaviour.

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; WLAN access networks defined in routing rule do not influence WLAN selection; and

- decide if the selected 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. If not, the selected WLAN can be used to perform NSWO.

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.

When the UE is roaming and receives Inter-system Routing Policies from both H-ANDSF and V-ANDSF, the set of Inter-system Routing Policies used by the UE is selected as follows:

- If there is rule selection information provisioned in the UE by the H-ANDSF, and if the RPLMN identity is equal to one of the VPLMNs included in the visited PLMNs with preferred rules, the set of Inter-system Routing Policies fromV-ANDSF is selected by the UE.

  If there is no WLANs matching the WLANSP rule(s) from the V-ANDSF, the set of Inter-system Routing Policy from the H-ANDSF is re-selected. However, if at least one WLAN matching one or more groups of selection criteria in the WLANSP rule of the VPLMN becomes available, the UE should re-use the WLANSP policies and Inter-system Routing Policies from V-ANDSF.

- If there is rule selection information provisioned in the UE by the H-ANDSF, and if the RPLMN identity is not equal to any of the VPLMNs included in the visited PLMNs with preferred rules, the set of Inter-system Routing Policies from H-ANDSF is selected by the UE,

  If there is no WLANs matching the WLANSP rule(s) from the H-ANDSF, the set of Inter-system Routing Policy from the V-ANDSF is be re-selected. However, if at least one WLAN matching one or more groups of selection criteria in the WLANSP rule of the HPLMN becomes available, the UE should re-use the WLANSP policies and Inter-system Routing Policies from H-ANDSF.

NOTE: How frequently the UE performs the discovery and reselection procedure depends on the UE implementation.

The Inter-system Routing Policy with the highest priority among the set of Inter-system Routing Policies selected above is selected as the active Inter-system Routing Policy.

The UE shall periodically re-evaluate the flow distribution rules of the 'active' ISRP rule. The value of the periodic re-evaluation timer is implementation dependant.

6.8.2.2.4.5 Use of Inter-APN Routing Policies

The UE shall use the IARP for APN if available.

The UE shall use the IARP for non-seamless WLAN offload if available, and the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2.

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 with the exception that the UE shall apply IARP provided by the H-ANDSF.

If no valid IARP present, then Inter-APN routing policy configuration is UE implementation dependent.

6.8.2.2.4.6 Use of WLAN selection information

The UE uses the WLAN selection information provided by ANDSF to determine the selected WLAN and the selected service provider.

The UE first uses WLAN Selection Policy (WLANSP) and the visited PLMNs with preferred rules to determine the active WLANSP rule. When roaming, if the UE is configured to prefer WLAN selection rules provided by the HPLMN, WLANSP provided by HPLMN is used. Otherwise, WLANSP provided by VPLMN is used. The UE selects the highest priority and valid WLANSP rule as the active WLANSP rule.

During power-up, while the UE has not registered to any PLMN, the UE shall use WLANSP provided by the HPLMN as valid.

The UE determines the selected WLAN(s) as specified in subclause 5.1.3.2. If there are no selected WLANs according to active WLANSP rule of the VPLMN/HPLMN, then the UE uses the WLANSP policies from the HPLMN/VPLMN as active WLANSP rule. However, if at least one WLAN that matches one or more groups of selection criteria in the WLANSP rule of the VPLMN or the /HPLMN becomes available, the UE should re-use the WLANSP policies from the VPLMN or the HPLMN as active WLANSP rule.

NOTE: How frequently the UE performs the discovery and reselection procedure depends on the UE implementation.

Home Network Preference information and Visited Network Preference information can be configured in the ANDSF MO to assist the UE in selecting a service provider over the selected WLAN(s) and constructing an appropriate NAI when attempting authentication with the selected service provider.

The UE uses the list of selected WLANs and the Home Network Preference information (or the Visited Network Preference information if available and if the UE is roaming) to select a WLAN service provider as specified in subclause 5.2.3.2.

6.8.2.2.4.7 Use of ePDG information

If the UE accesses EPC via the ePDG, the UE shall use the ePDG configuration information during the tunnel establishment procedure to determine the home operator preference on ePDG connection as described in subclause 7.2.1.

6.8.2.2.4.8 Use of LWA co-existence Information

The H-ANDSF can configure the LWA co-existence information about the preference between the WLANSP, ISRP and IARP for NSWO rules, on the one hand, and the LWA/RCLWI/LWIP procedures defined in the RAN, on the other hand, according to TS 23.402 [6]. The LWA co-existence information is configured in the ANDSF/HomeNetworkPreference/RanMobilitySetUsed node.

If the UE:

- has not selected a WLAN according to the WLANSP rules or user preferences, including when the UE has not selected any WLAN; or
- has selected a WLAN according to the WLANSP rules and is connected to a PLMN/WLAN combination configured in the ANDSF/HomeNetworkPreference/RanMobilitySetUsed node,

the UE shall use the WLAN mobility set (see 3GPP TS 36.300 [70]) and ignore the WLANSP, ISRP and IARP for NSWO rules. In order to apply the WLAN mobility set, the UE may disconnect from the WLAN it is currently connected to and connect to a WLAN identified by the RAN-configured WLAN mobility set.

If the UE:

- has selected a WLAN according to the WLANSP rules and is not connected to a PLMN/WLAN combination configured in the ANDSF/HomeNetworkPreference/RanMobilitySetUsed node; or
- has selected a WLAN based on user preferences,

the UE shall ignore the WLAN mobility set and apply the WLANSP, ISRP and IARP for NSWO rules.

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, RAN validity condition. 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 a valid 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 ISMP, ISRP, IARP, WLANSP or information related to available access networks in the vicinity of 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.

Except for the trusted WLAN access, 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], 3GPP TS 29.274 [50] and 3GPP TS 29.275 [18]. Except for the trusted WLAN access, the specification of PCO signalling in the non-3GPP access network is access network specific and not in the scope of 3GPP.

When the UE access EPC via trusted WLAN access network,

- if SCM is used, the PCO is supported as described in subclause 6.4.2.6, 3GPP TS 29.274 [50] and 3GPP TS 29.275 [18];
- if MCM is used, the PCO is supported as described in 3GPP TS 24.244 [56], 3GPP TS 29.274 [50] and 3GPP TS 29.275 [18];and
- if TSCM is used, the PCO is not supported by the UE.

6.10 Integration with access stratum layer of 3GPP access

6.10.1 General

The subclause describes the additional procedures for integration with access stratum layer of 3GPP access.

If the RAN assistance information is supported by the UE and the E-UTRAN or UTRAN, the E-UTRAN or UTRAN can provide RAN assistance information to the UE as described in 3GPP TS 25.331 [14A] and 3GPP TS 36.331 [16B].

6.10.2 Selection of control of WLAN access selection and traffic routing

The WLAN access selection and traffic routing can be controlled either by ANDSF rules or by RAN rules.

The ANDSF rules control the WLAN access selection and traffic routing if:

a) the UE has ANDSF rules but no RAN rules; or

b) the UE has both ANDSF rules and RAN rules; and:

   1) the UE is not capable to simultaneously route IP traffic to both 3GPP access and WLAN; and:

      A) the UE is not roaming and the UE has at least one ISMP rule from HPLMN;

      B) the UE is roaming in a VPLMN contained in the visited PLMNs with preferred rules and the UE has at least one ISMP rule from VPLMN; or

      C) the UE is roaming in a VPLMN not contained in the visited PLMNs with preferred rules and the UE has at least one ISMP rule from HPLMN; or

   2) the UE is capable to simultaneously route IP traffic to both 3GPP access and WLAN; and:

      A) the UE is not roaming and the UE has an valid ISRP rule from HPLMN;

      B) the UE is roaming in a VPLMN contained in the visited PLMNs with preferred rules and the UE has a valid ISRP rule from VPLMN; or

      C) the UE is roaming in a VPLMN not contained in the visited PLMNs with preferred rules and the UE has a valid ISRP rule from HPLMN.

The RAN rules control the WLAN access selection and traffic routing if:

a) the UE has RAN rules but no ANDSF rules; or

b) the UE has both ANDSF rules and RAN rules; and:

   1) the UE is not capable to simultaneously route IP traffic to both 3GPP access and WLAN; and:

      A) the UE is not roaming and the UE has no ISMP rules from HPLMN;

      B) the UE is roaming in a VPLMN contained in the visited PLMNs with preferred rules and the UE has no ISMP rules from VPLMN; or

      C) the UE is roaming in a VPLMN not contained in the visited PLMNs with preferred rules and the UE has no ISMP rules from HPLMN; or

   2) the UE is capable to simultaneously route IP traffic to both 3GPP access and WLAN, and:

A) the UE is not roaming and the UE has no valid ISRP rule from HPLMN;

B) the UE is roaming in a VPLMN contained in the visited PLMNs with preferred rules and the UE has no valid ISRP rule from VPLMN; or

C) the UE is roaming in a VPLMN not contained in the visited PLMNs with preferred rules and the UE has no valid ISRP rule from HPLMN.

6.10.3 Additional procedures when WLAN access selection and traffic routing is controlled by ANDSF rules

If the ANDSF rules control the WLAN access selection and traffic routing as described in subclause 6.10.2, the access stratum layer of the 3GPP access provides the received RAN assistance parameters to this layer and the UE shall store the RAN assistance parameters and then use the RAN assistance information together with ANDSF rules specified in 3GPP TS 24.312 [13] and measurements results to make traffic routing decisions to move traffic to WLAN or to E-UTRAN or UTRAN by:

- comparing the received RAN assistance thresholds with corresponding measurement results; and
- comparing the received OPI value with the provisioned OPI value provided by the ANDSF.

The following thresholds can be used for traffic routing from E-UTRAN or UTRAN to WLAN:

- ThreshServingOffloadWLANLowP;
- ThreshServingOffloadWLANLowQ;
- ThreshChUtilWLANLow;
- ThreshBackhRateDLWLANHigh;
- ThreshBackhRateULWLANHigh; and
- ThreshBeaconRSSIWLANHigh.

The following thresholds can be used for traffic routing from WLAN to E-UTRAN or UTRAN:

- ThreshServingOffloadWLANHighP;
- ThreshServingOffloadWLANHighQ;
- ThreshChUtilWLANHigh;
- ThreshBackhRateDLWLANLow;
- ThreshBackhRateULWLANLow; and
- ThreshBeaconRSSIWLANLow.

Offload Preference Indication (OPI) parameter can be used for traffic routing in both directions, from E-UTRAN or UTRAN to WLAN or from WLAN to E-UTRAN or UTRAN.

6.10.4 Additional procedures when WLAN access selection and traffic routing is controlled by RAN rules

This subclause applies if the RAN rules control the WLAN access selection and traffic routing as described in subclause 6.10.2.

The access stratum layer of the 3GPP access can provide:

1) move-traffic-to-WLAN indication, along with list of WLAN identifiers. An entry in the list of the WLAN identifiers consists of SSID, BSSID, HESSID, or any combination of them; and

2) move-traffic-from-WLAN indication.

The user preferences take precedence over the indications provided by the access stratum layer of the 3GPP access.

NOTE 1: Handling of the move-traffic-from-WLAN indication and the move-traffic-to-WLAN indication for a multi-access PDN connection where the network-initiated NBIFOM mode is the selected NBIFOM mode, is specified in 3GPP TS 24.161 [69].

Upon:

- receiving move-traffic-to-WLAN indication, along with the list of the WLAN identifiers, if the user preferences are not present; or
- establishment of a new PDN connection in 3GPP access, if the PDN connection is an offloadable PDN connection, the access stratum indicated move-traffic-to-WLAN, the access stratum has not indicated the move-traffic-from-WLAN indication after indicating of the move-traffic-to-WLAN indication and the user preferences are not present;

and:

- the UE is capable to simultaneously route IP traffic to both 3GPP access and WLAN and has at least one PDN connection which is not a multi-access PDN connection or where the UE-initiated NBIFOM mode is the selected NBIFOM mode as specified in 3GPP TS 24.161 [69]; or
- the UE is not capable to simultaneously route IP traffic to both 3GPP access and WLAN, and all the PDN connections of the UE in 3GPP access are offloadable PDN connections;

the UE:

a) shall perform the procedure in subclause 5.1.3.2.3 and in subclause 5.2.3.2 to select the selected WLAN and the NAI for authentication;

b) if not authenticated yet with the selected WLAN using the NAI for authentication in subclause 6.4, shall authenticate with the selected WLAN using the NAI for authentication in subclause 6.4. During authentication, if the selected WLAN is a trusted WLAN, SCM is supported by both UE and network, MCM is not supported by UE, network or both, and if:

   - the UE is capable to simultaneously route IP traffic to both 3GPP access and WLAN and has at least one PDN connection which is not a multi-access PDN connection or where the UE-initiated NBIFOM mode is the selected NBIFOM mode as specified in 3GPP TS 24.161 [69]; or
   - the UE is not capable to simultaneously route IP traffic to both 3GPP access and WLAN, and the UE has only one PDN connection;

   shall handover one PDN connection:

   - which is an offloadable PDN connection; and
   - which is not a multi-access PDN connection or where the UE-initiated NBIFOM mode is the selected NBIFOM mode as specified in 3GPP TS 24.161 [69];

   from 3GPP access to the WLAN access using procedures in subclause 6.4.2.6.2;

NOTE 2: When the UE already has one PDN connection established via WLAN in SCM, and if move-traffic-to-WLAN indication is received, it is up to the UE implementation to determine whether to offload a PDN connection from 3GPP access to WLAN. In that case, it is also up to the UE implementation to determine which one of the offloadable PDN connections will be offloaded.

c) if the selected WLAN is a trusted WLAN, and MCM is supported by both UE and network, shall handover all the PDN connections:

   - which are offloadable PDN connections; and
   - which are not a multi-access PDN connection or where the UE-initiated NBIFOM mode is the selected NBIFOM mode as specified in 3GPP TS 24.161 [69];

   from 3GPP access to the WLAN access using procedures of 3GPP TS 24.244 [56];

d) if the selected WLAN is an untrusted WLAN, and if the UE supports access to EPC via untrusted WLAN, shall handover all the PDN connections:

- which are offloadable PDN connections; and
- which are not a multi-access PDN connection or where the UE-initiated NBIFOM mode is the selected NBIFOM mode as specified in 3GPP TS 24.161 [69];

from 3GPP access to the WLAN access using procedures in subclause 7.2.1 and subclause 7.2.2; and

e) if the UE has a valid IARP rule for APN, shall use the IARP for APN using the procedures in subclause 6.8.2.2.4.5.

Upon receiving move-traffic-from-WLAN indication, and if the user preferences are not present, the UE shall handover all the PDN connections:

- established in (or previously handed over to) WLAN access; and
- which are not a multi-access PDN connection or where the UE-initiated NBIFOM mode is the selected NBIFOM mode as specified in 3GPP TS 24.161 [69];

from WLAN access to the 3GPP access using procedures in 3GPP TS 24.301 [10].

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

7.2.1.1 General

The UE performs ePDG selection based on the ePDG configuration information configured by the home operator in the UE either via H-ANDSF or via USIM or via implementation specific means. Implementation specific means apply only if the configurations via H-ANDSF and USIM are not present. The ePDG configuration information may consist of home ePDG identifier or ePDG selection information or both:

- when available in ANDSF MO, the ePDG configuration information is provisioned in ePDG node under Home Network Preference as specified in 3GPP TS 24.312 [13]; and
- when available in USIM, the ePDG configuration information is provisioned in EF_{ePDGId} and $EF_{ePDGSelection}$ files as specified in 3GPP TS 31.102 [45].

The ePDG configuration information provided by ANDSF may also be pre-configured by the home operator on the ME or provisioned on the UICC. The UE shall use the information in the following order of precedence:

1) ePDG configuration information provided by the ANSDF server to the ME;
2) ePDG configuration information configured on the UICC;
3) ePDG configuration information pre-configured on the ME.

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].

7.2.1.2 Determination of the country the UE is located in

If the UE cannot determine whether it is located in the home country or not in a visited country, as required by the ePDG selection procedure specified in 3GPP TS 23.402 [6], the UE shall stop the ePDG selection.

NOTE: It is out of scope of the present specification to define how the UE determines whether it is located in the home country or in a visited country. When the UE is in coverage of a 3GPP RAT, it can, for example, use the information derived from the available PLMN(s). In this case, the UE can match the MCC broadcasted on the BCCH of the 3GPP access against the UE's IMSI to determine if they belong to the same country, as defined in 3GPP TS 23.122 [4]. If the UE is not in coverage of a 3GPP RAT, the UE can use other techniques, including user-provided location, for determining whether it is located in its home country or not.

7.2.1.3 Handling of ePDG selection based on the country the UE is located in

The UE shall proceed as follows:

1) if the UE is located in its home country and

   a) if the ePDG selection information is provisioned in the ePDG configuration information and if an entry for the HPLMN is available in the ePDG selection information, the UE shall construct an ePDG FQDN based on configured FQDN format of HPLMN as described in 3GPP TS 23.402 [6] and encoding in 3GPP TS 23.003 [3]:

   b) if the ePDG selection information is not provisioned in the ePDG configuration information or if the ePDG selection information is provisioned and an entry for the HPLMN is not available in the ePDG selection information, the UE shall:

      i) if Home ePDG identifier is provisioned in the ePDG configuration information, use the configured IP address to select the ePDG, or if configured IP address is not available, construct an ePDG FQDN using the configured FQDN; and

      ii) if the Home ePDG identifier is not provisioned in the ePDG configuration information, construct an ePDG FQDN based on the Operator Identifier FQDN format using the PLMN ID of the HPLMN as described in 3GPP TS 23.003 [3];

   c) if the ePDG configuration information is not configured on the UE, or the ePDG configuration information is configured but empty, the UE shall construct the ePDG FQDN based on the Operator Identifier FQDN format using the PLMN ID of the HPLMN stored on the USIM; and

   d) If the ePDG selection is for establishing emergency bearer services and the UE is not equipped with a UICC, the UE may construct the Operator Identifier FQDN format based on a PLMN ID obtained via implementation specific means,

   and for the cases a) through d), the UE shall use the DNS server function to resolve the contructed ePDG FQDN to the IP address(es) of the ePDG(s). The UE shall select an IP address of an ePDG with the same IP version as its local IP address;

2) if the UE is not located in its home country and

   a) if the ePDG selection information is provisioned in the ePDG configuration information and if the UE is attached to a VPLMN via 3GPP access:

      i) if an entry for the VPLMN is available in the ePDG selection information, the UE shall construct an ePDG FQDN based on configured FQDN format of the VPLMN as described in 3GPP TS 23.402 [6] and encoding in 3GPP TS 23.003 [3];

      ii) if an entry for the VPLMN is not available in the ePDG selection information, and an 'Any_PLMN' entry is available in the ePDG selection information, the UE shall construct an ePDG FQDN based on the configured FQDN format of the 'Any_PLMN' entry as described in 3GPP TS 23.402 [6] and encoding in 3GPP TS 23.003 [3],

      and for case i) and ii), the UE shall use the DNS server function to resolve the contructed ePDG FQDN to the IP address(es) of the ePDG(s). The UE shall select an IP address of an ePDG with the same IP version as its local IP address; and

b) if one of the following is true:

- the UE is not attached to a PLMN via 3GPP access and the UE uses WLAN;
- the ePDG configuration information is not configured;
- the ePDG selection information is not provisioned in the ePDG configuration information; or
- the UE is attached to a VPLMN via 3GPP access and an entry for the VPLMN is not available in the ePDG selection information and an 'Any_PLMN' entry is not available in the ePDG selection information,

the UE shall perform a DNS query (see 3GPP TS 23.003 [3]) as specified in subclause 7.2.1.4 to determine if the visited country mandates the selection of ePDG in this country:

i) if selection of ePDG in visited country is mandatory:

- if the UE is attached to a VPLMN via 3GPP access and the PLMN ID of VPLMN is included in one of the returned DNS records, the UE shall select an ePDG in this VPLMN by constructing an ePDG FQDN based on the Operator Identifier FQDN format using the PLMN ID of the VPLMN as described in 3GPP TS 23.003 [3]; and
- if the UE is not attached to a PLMN via 3GPP access or the UE is attached to a VPLMN via 3GPP access and the PLMN ID of VPLMN is not included in any of the DNS records:
  - if the ePDG selection information is provisioned, the UE shall select an ePDG from a PLMN included in the DNS response that has highest PLMN priority (see 3GPP TS 24.312 [13]) in the ePDG selection information and construct an ePDG FQDN based on the configured FQDN format of the PLMN entry as described in 3GPP TS 23.402 [6] and encoding in 3GPP TS 23.003 [3]; and
  - if the ePDG selection information is not provisioned or the ePDG selection information does not contain any of the PLMNs in the DNS response, selection of the PLMN is UE implementation specific. The UE shall select an ePDG from a PLMN included in the DNS response and construct an ePDG FQDN based on the Operator Identifier FQDN format using the PLMN ID of the PLMN as described in 3GPP TS 23.003 [3],

and for the above cases, the UE shall use the DNS server function to resolve the contructed ePDG FQDN to the IP address(es) of the ePDG(s). The UE shall select an IP address of an ePDG with the same IP version as its local IP address;

ii) if the DNS response contains no records, selection of ePDG in visited country is not mandatory:

- if the ePDG selection information is provisioned and contains one or more PLMNs in the visited country, the UE shall select an ePDG from a PLMNs that has highest PLMN priority (see 3GPP TS 24.312 [13]) in the ePDG selection information;
- if the ePDG selection information is not provisioned or if the ePDG selection information is provisioned and contains no PLMNs in the visited country, the UE shall select an ePDG in the HPLMN as follows:
  - if the Home ePDG identifier is provisioned in the ePDG configuration information (see 3GPP TS 24.312 [13]), the UE shall use the configured IP address to select the ePDG, or if configured IP address is not available, use the configured FQDN and run DNS query to obtain the IP address(es) of the ePDG(s); and
  - if the Home ePDG identifier is not provisioned in the ePDG configuration information, the UE shall construct an ePDG FQDN based on the Operator Identifier FQDN format using the PLMN ID of the HPLMN as described in 3GPP TS 23.003 [3], and
- if the ePDG selection is for establishing emergency bearer services and the UE is not equipped with a UICC, the UE may construct the Operator Identifier FQDN format based on a PLMN ID obtained via implementation specific means.

and for the above cases, the UE shall use the DNS server function to resolve the contructed ePDG FQDN to the IP address(es) of the ePDG(s). The UE shall select an IP address of an ePDG with the same IP version as its local IP address; and

iii) if no DNS response is received, the UE shall terminate the ePDG selection procedure.

If selecting an ePDG in the HPLMN fails, and the selection of ePDG in the HPLMN is performed using Home ePDG identifier configuration and there are more pre-configured ePDGs in the HPLMN, the UE shall repeat the tunnel establishment attempt using the next FQDN or IP address(es) of the ePDG in the HPLMN.

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. If the UE does not receive a response to an IKE_SA_INIT request message sent towards to any of the received IP addresses of the selected ePDG, then the UE shall repeat the ePDG selection as described in this subclause, excluding the ePDG for which the UE did not receive a response to the IKE_SA_INIT request message.

NOTE 1: The time the UE waits before reattempting access to another ePDG or to an ePDG that it previously did not receive a response to an IKE_SA_INIT request message, is implementation specific.

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

NOTE 2: 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.

7.2.1.4 Determine if the visited country mandates the selection of ePDG in this country

In order to determine if the visited country mandates the selection of ePDG in this country (see 3GPP TS 23.402 [6]), the UE shall perform the DNS NAPTR query using Visited Country FQDN as specified in 3GPP TS 23.003 [3].

If the result of this query is:

- a set of one or more records containing the service instance names of the form "*epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org*", the UE shall determine thst the visited country mandates the selection of the ePDG in this country; and

NOTE: The (<MCC>, <MNC>) pair in each record represents PLMN Id (see 3GPP TS 23.003 [3]) in the visited country which can be used for ePDG selection in subclause 7.2.1.3.

- no records containing the service instance names of the form "*epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org*", the UE shall determine that the visited country does not mandate the selection of the ePDG in this country.

7.2.1A Selection of the ePDG for emergency bearer services

The UE performs ePDG selection for emergency bearer services based on the ePDG configuration information provided by the home operator in the UE via H-ANDSF or via USIM, or via implementation specific means.

The ePDG configuration information used for selecting the ePDG for emergency bearer services includes:

- when available in ANDSF MO, Emergency_ePDG_Identifier and ePDG selection information are provisioned in ePDG node under Home Network Preference as specified in 3GPP TS 24.312 [13]; and

- when available in the USIM, the Emergency ePDG Identifier and ePDG selection information are provisioned in $EF_{ePDGIdEm}$ and $EF_{ePDGSelection}$ files as specified in 3GPP TS 31.102 [45].

NOTE: Implementation specific means apply only if the configurations via H-ANDSF and USIM are not present.

When performing ePDG selection for establishing emergency bearer services, the UE shall proceed by following the general ePDG selection procedure specified in subclause 7.2.1 except:

- Emergency_ePDG_Identifier shall be used instead of Home ePDG identifier;

- All ePDG FQDNs and visited country FQDNs for DNS query shall be constructed based on the ePDG FQDN format defined for emergency services as defined in 3GPP TS 23.003 [3]; and

- If the ME is not equipped with a UICC, the UE shall consider the ePDG configuration information as not available.

7.2.2 Tunnel establishment

7.2.2.1 Tunnel establishment accepted by the network

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, the UE shall send two configuration attributes in the CFG_REQUEST Configuration Payload: one for the IPv4 address and the other for the IPv6 prefix;

- The "IDr" payload, containing the APN in the Identification Data, for non-emergency session establishment. For emergency session establishment, the UE shall format the "IDr" payload according to subclause 7.2.5. The UE shall set the ID Type field of the "IDr" payload to ID_FQDN as defined in IETF RFC 5996 [28]. The UE indicates a request for the default APN by omitting the "IDr" payload, which is in accordance with IKEv2 protocol as defined in IETF RFC 5996 [28]; and

- The "IDi" payload containing the NAI.

The IKE_AUTH request message may also contain:

- An indication in a notify payload that MOBIKE is supported by the UE;

- 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 within the IKE_AUTH response message as specified in IETF RFC 5996 [28]; or

- The P_CSCF_IP6_ADDRESS attribute, the P_CSCF_IP4_ADDRESS attribute or both in the CFG_REQUEST Configuration Payload. The UE can obtain zero or more P-CSCF server addresses in the CFG_REPLY Configuration Payload within the IKE_AUTH response message as specified in IETF RFC 7651 [64].

The UE may support the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in subclause 8.2.4.2. If the UE supports the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute, the UE shall include the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute indicating support of receiving timeout period for liveness check in the CFG_REQUEST configuration payload within the IKE_AUTH request message. If the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in subclause 8.2.4.2 indicating the timeout period for the liveness check is included in the CFG_REPLY configuration payload within the IKE_AUTH response message or if the UE has a pre-configured timeout period, the UE shall perform the tunnel liveness checks as described in subclause 7.2.2A.

NOTE: The timeout period for liveness check is pre-configured in the UE in implementation-specific way.

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]. If the previously allocated home address information consists of both an IPv4 address and an IPv6 prefix, then the UE shall include the INTERNAL_IP4_ADDRESS attribute and the INTERNAL_IP6_ADDRESS attribute in the CFG_REQUEST configuration payload within the IKE_AUTH request message. 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).

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 within the IKE_AUTH request message. 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 within the IKE_AUTH request message, 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.

During the IKEv2 authentication and security association establishment, following the UE's initial IKE_AUTH request message to the ePDG, if the UE subsequently receives an IKE_AUTH response message from the ePDG containing the EAP-Request/AKA-Challenge, after verifying the received authentication parameters and successfully authenticating the ePDG as specified in 3GPP TS 33.402 [15], the UE shall send a new IKE_AUTH request message to the ePDG including the EAP-Response/AKA-Challenge. In addition, the UE shall provide the requested mobile device identity if available, as specified in subclause 7.2.6.

If the UE supports P-CSCF restoration extension for untrusted WLAN as specified in 3GPP TS 23.380 [66], the UE shall send its capability indication of the support of P-CSCF restoration to the ePDG by including the P-

CSCF_RESELECTION_SUPPORT Notify payload within an IKE_AUTH request message. The content of the P-CSCF_RESELECTION_SUPPORT Notify payload is described in subclause 8.2.9.4.

7.2.2.2 Tunnel establishment not accepted by the network

If the UE receives the IKE_AUTH response message from an ePDG of the HPLMN including a Notify payload with a Private Notify Message Type NON_3GPP_ACCESS_TO_EPC_NOT_ALLOWED or USER_UNKNOWN or PLMN_NOT_ALLOWED or AUTHORIZATION_REJECTED or RAT_TYPE_NOT_ALLOWED or ILLEGAL_ME as defined in subclause 8.1.2, then after the UE authenticates the network by using ePDG certificate and AUTH parameters as specified in 3GPP TS 33.402 [15], the UE shall close the related IKEv2 security association states and shall not retry the authentication procedure to an ePDG from the same PLMN until switching off or the UICC containing the USIM is removed.

If the above Private Notify Message Type is received from the VPLMN's ePDG and the UE authenticates the network by using ePDG certificate and AUTH parameters as specified in 3GPP TS 33.402 [15]:

- If the received Notify Message Type is NON_3GPP_ACCESS_TO_EPC_NOT_ALLOWED or USER_UNKNOWN or AUTHORIZATION_REJECTED or RAT_TYPE_NOT_ALLOWED or ILLEGAL_ME, the UE may retry the authentication procedure with an ePDG deployed by the HPLMN if allowed according to the ePDG selection procedure in subclause 7.2.1 and subclause 7.2.1A; or

- If the received Private Notify Message Type is PLMN_NOT_ALLOWED, the UE should retry the authentication procedure with an ePDG deployed by the HPLMN if allowed according to the ePDG selection procedure in subclause 7.2.1 and subclause 7.2.1A.

If the UE receives from the ePDG the IKE_AUTH response message, including a Notify payload with a Private Notify Message Type "NETWORK_FAILURE" as defined in subclause 8.1.2 then after the UE authenticates the network, the UE shall close the related IKEv2 security association states and:

a) if the received IKE_AUTH response message from ePDG contains a Notify payload with the BACKOFF_TIMER Notify payload as defined in subclause 8.2.9.1, the UE shall behave as follows:

   i) if the timer value indicates neither zero nor deactivated, start the Tw3 timer with the value provided and not retry the authentication procedure to the same ePDG until timer Tw3 expires or the UE is switched off or the UICC containing the USIM is removed;

   ii) if the timer value indicates that this timer is deactivated, not retry the authentication procedure to the same ePDG until the UE is switched off or the UICC containing the USIM is removed; and

   iii) if the timer value indicates zero, may retry the authentication procedure to an ePDG from the same PLMN; or

b) if the BACKOFF_TIMER Notify payload is not included in the received IKE_AUTH response message from ePDG, the UE shall start an implementation specific backoff timer. The UE shall not re-try the authentication procedure with the same ePDG until the backoff timer expires or the UE is switched off or the UICC containing the USIM is removed.

If the UE receives from the ePDG an IKE_AUTH response message including a Notify Payload with a Private Notify Message Error Type "NO_APN_SUBSCRIPTION" as defined in subclause 8.1.2 then after the UE authenticates the network, the UE shall close the related IKEv2 security association states and:

a) if the received IKE_AUTH response message from ePDG contains a Notify payload with the BACKOFF_TIMER Notify payload as defined in subclause 8.2.9.1, the UE shall behave as follows:

   i) if the timer value indicates neither zero nor deactivated, start the Tw3 timer with the value provided and not retry the authentication procedure to the same PLMN for the same APN until timer Tw3 expires or the UE is switched off or the UICC containing the USIM is removed;

   ii) if the timer value indicates that this timer is deactivated, not retry the authentication procedure to the same PLMN for the same APN until the UE is switched off or the UICC containing the USIM is removed; and

   iii) if the timer value indicates zero, may retry the authentication procedure to an ePDG from the same PLMN for the same APN; or

b) if the BACKOFF_TIMER Notify payload is not included in the received IKE_AUTH response message from ePDG, the UE shall not retry the authentication procedure with the same PLMN for the same APN the UE is

switched off or the UICC containing the USIM is removed, unless the UE has an implementation specific backoff timer. In that case, the UE shall not retry until that implementation specific timer expires.

NOTE 1: The UE can perform NSWO from the current untrusted WLAN access network even though the tunnel establishment procedure to the ePDG is not accepted by the network.

NOTE 2: Switching off and USIM change conditions are implemented taking into consideration the user experience aspect.

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 with the same IP address 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, then after the UE authenticates the network, 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, then after the UE authenticates the network, 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.

7.2.2A Liveness check procedure

If the UE supports the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in subclause 8.2.4.2 and the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in subclause 8.2.4.2 was included in the CFG_REPLY configuration payload within the IKE_AUTH response message received in subclause 7.2.2 the UE shall set the timeout period for the liveness check to the value of the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute.

If the UE does not support the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in subclause 8.2.4.2 or the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in subclause 8.2.4.2 was not included in the CFG_REPLY configuration payload within the IKE_AUTH response message received in subclause 7.2.2 then:

1) if the LivenessCheckPeriod node as specified in 3GPP TS 24.312 [13] is configured, the UE shall use the timeout period for the liveness check indicated by the LivenessCheckPeriod node; and

2) if the LivenessCheckPeriod node as specified in 3GPP TS 24.312 [13] is not configured, the UE shall use the pre-configured value of the timeout period for liveness check.

NOTE: The timeout period is pre-configured in the UE in implementation-specific way.

If the UE has not received any cryptographically protected IKEv2 or IPSec message for the duration of the timeout period for liveness check, the UE shall send an INFORMATIONAL request with no payloads as per IETF RFC 5996 [28]. If an INFORMATIONAL response is not received, the UE shall deem the IKEv2 security association to have failed.

7.2.2B Handling of NBIFOM

If the IKEv2 authentication and security association establishment is triggered by procedures in 3GPP TS 24.161 [69], the UE shall include the NBIFOM_GENERIC_CONTAINER Notify payload (see subclause 8.1.2.3)in the IKE_AUTH request message. The UE shall set the NBIFOM container contents field of the NBIFOM_GENERIC_CONTAINER Notify payload as specified in 3GPP TS 24.161 [69].

7.2.2C Rekeying procedure

The UE may support rekeying as defined in IETF RFC 5996 [28].

To trigger rekeying, the UE shall use the rekeying time parameter (see IETF RFC 5996 [28]) if it is configured by the RekeyingTime node as specified in 3GPP TS 24.312 [13]. If the rekeying time parameter is not configured, the UE shall use an implementation-specific rekeying time (e.g. 18 hours).

7.2.2D NAT keep alive procedure

The UE may support NAT keep alive handling as defined in IETF RFC 5996 [28] and IETF RFC 3948 [72].

To control the NAT-keepalive packet sending, the UE shall use the parameter M (see IETF RFC 3948 [72]]) if it is configured by the NATKeepAliveTime node as specified in 3GPP TS 24.312 [13]. If the parameter M is not configured, the UE shall use an implementation-specific time.

7.2.3 Tunnel modification

7.2.3.1 UE-initiated 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.

This procedure is also used during the UE-initiated IP flow mobility procedure (see subclause 6.3.3.3 of 3GPP TS 23.161 [68]) or the NBIFOM IP flow mapping procedure (see subclause 6.4.3 of 3GPP TS 23.161 [68]).

If the UE-initiated modification is triggered by procedures in 3GPP TS 24.161 [69], the UE shall include the NBIFOM_GENERIC_CONTAINER Notify payload (see subclause 8.1.2.3) in the INFORMATIONAL request to the ePDG. The UE shall set the NBIFOM container contents field of the NBIFOM_GENERIC_CONTAINER Notify payload as specified in 3GPP TS 24.161 [69].

7.2.3.2 UE behaviour towards ePDG initiated modification

This procedure is used if P-CSCF restoration extension for untrusted WLAN is supported as specified in 3GPP TS 23.380 [66].

If the UE receives the P_CSCF_IP6_ADDRESS attribute, the P_CSCF_IP4_ADDRESS attribute or both as specified in IETF RFC 7651 [64] in the CFG_REQUEST configuration payload within the INFORMATIONAL request from the ePDG and the UE supports P-CSCF restoration extension for untrusted WLAN as specified in 3GPP TS 23.380 [66], the UE shall reply with an INFORMATIONAL response and proceed as specified in subclause 5.6.5.2 of 3GPP TS 23.380 [66]. The INFORMATIONAL response shall include the received P_CSCF_IP6_ADDRESS attribute or the P_CSCF_IP4_ADDRESS attribute or both in the CFG_REPLY Configuration Payload. The P_CSCF_IP6_ADDRESS attribute shall contain no value and the length field shall be set to 0. The P_CSCF_IP4_ADDRESS shall contain no value and the length field shall be set to 0.

Upon of receipt of the NBIFOM_GENERIC_CONTAINER Notify payload (see subclause 8.1.2.3) in an INFORMATIONAL request, the UE shall reply with an INFORMATIONAL response and if required by procedures in 3GPP TS 24.161 [69], the UE shall include the NBIFOM_GENERIC_CONTAINER Notify payload (see subclause 8.1.2.3) in the INFORMATIONAL response. The UE shall set the NBIFOM container contents field of the NBIFOM_GENERIC_CONTAINER Notify payload as specified in 3GPP TS 24.161 [69].

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.

If the INFORMATIONAL request message including the DELETE payload contains the REACTIVATION_REQUESTED_CAUSE Notify payload, the UE shall re-establish the IPsec Tunnel for the corresponding PDN connection after its release. The coding of the P-CSCF_RESELECTION_SUPPORT Notify payload is described in subclause 8.2.9.6.

NOTE: For an IMS PDN connection, the re-establishment of the IPSec tunnel is part of the "Re-establishment of the IP-CAN used for SIP signalling procedure" specified in 3GPP TS 24 229 [67] subclause R.2.2.1B.

7.2.4.3 Local tunnel disconnection initiated from 3GPP access

A PDN connection over untrusted WLAN over S2b can be released locally in the UE, i.e. without any peer-to-peer signalling between the ePDG and the UE, based on the trigger received from the 3GPP access, e.g. during the P-CSCF restoration procedure for NBIFOM PDN connections (see 3GPP TS 23.380 [66]).

Upon receiving over the 3GPP access:

- a DEACTIVATE EPS BEARER CONTEXT REQUEST message with the EPS bearer context of a default EPS bearer context and ESM cause #39 "reactivation requested" (see 3GPP TS 24.301 [10]); or

- a DETACH REQUEST message with the detach type "re-attach required" (see 3GPP TS 24.301 [10])

to release the resources for a PDN connection over the 3GPP access, the UE shall:

a) close the related IKEv2 security association for the IPsec tunnel associated with this PDN connection; and

b) consider that the ePDG is no longer responding (see RFC 5996 [28]) and not send any messages to the ePDG.

7.2.5 Emergency session establishment

If the UE needs to establish an IMS emergency session over untrusted non-3GPP access as specified in 3GPP TS 24.229 [67], the UE shall:

- if the UE is not connected to an ePDG yet, select an ePDG that supports emergency services as described in subclause 7.2.1A;

- if the UE is already connected to an ePDG that has indicated its capability of support emergency services as specified in subclause 7.4.1.1 and the ePDG is located in the same country where the UE is currently located, reuse ePDG for emergency session; and

- if the UE is already connected to an ePDG but the ePDG does not support the emergency services or ePDG is not located in the same country where the UE is currently located, first follow procedure described in subclause 7.2.4.1 to disconnect existing IPsec tunnel. The UE shall then select an ePDG that supports emergency services as described in subclause 7.2.1A.

Once the UE selects an ePDG that supports emergency services as specified in subclause 7.2.1A, or if the UE is already connected to an ePDG and the ePDG is reused for emergency session, the UE shall initiate an IKEv2 tunnel establishment procedure towards this ePDG as described in subclause 7.2.2. Upon receipt of an IKE_SA_INIT response, the UE shall send an IKE_AUTH request message to the ePDG according to subclause 7.2.2.1 with the "IDr" payload containing the string "EMERGENCY", using capital letters only, in the Identification Data. The UE shall set the ID Type field of the "IDr" payload to ID_FQDN.

NOTE: In this procedure, the only scenario in which the UE is not in the same country as the ePDG it is connected to, is when the UE is not in the country of its HPLMN and the ePDG is in the country of the HPLMN.

In order to establish a new emergency session over an untrusted WLAN, the UE shall include:

- an INTERNAL_IP4_ADDRESS attribute with the length field set to zero;

  an INTERNAL_IP6_ADDRESS attribute with the length field set to zero; or

- both of the above;

in the CFG_REQUEST Configuration Payload within the IKE_AUTH request message.

In order to perform handover of an emergency session from a 3GPP access network to untrusted WLAN, the UE shall include:

- the INTERNAL_IP4_ADDRESS attribute set to the IPv4 address of the previously allocated home address information;

  the INTERNAL_IP6_ADDRESS attribute set to the IPv6 address of the previously allocated home address information; or

- both of the above;

in the CFG_REQUEST Configuration Payload within the IKE_AUTH request message. If the previously allocated home address information consists of both an IPv4 address and an IPv6 prefix, then the UE shall include the INTERNAL_IP4_ADDRESS attribute and the INTERNAL_IP6_ADDRESS attribute in the CFG_REQUEST configuration payload within the IKE_AUTH request message.

If the UE does not receive a response to an IKE_SA_INIT request message sent towards the selected ePDG, then the UE shall repeat the ePDG search as described in 3GPP TS 23.402 [6], excluding the ePDG for which the UE did not receive a response to the IKE_SA_INIT request message. The UE shall stop the establishment of emergency session if it is unable to select an ePDG for emergency bearer services.

If after sending an IKE_AUTH request message to the ePDG to initiate emergency session, the UE receives IKE_AUTH response message from the ePDG containing a Notify payload with a Private Notify Message Type "UNAUTHENTICATED_EMERGENCY_NOT_SUPPORTED", the UE shall follow the steps above to select a new ePDG for emergency session establishment by excluding the ePDGs from which the emergency session request was previously not accepted or by implementation specific means.

If the UE receives the Notify Message Type IMEI_NOT_ACCEPTED as defined in subclause 8.1.2.2, the UE shall not retry the authentication procedure from the same PLMN until switching off, the UICC containing the USIM is replaced, or a UICC containing the USIM is inserted.

If the UE is already connected to an ePDG selected by the procedure in subclause 7.2.1A, the UE is considered as attached for emergency bearer services. In such a case, the UE shall not initiate any addtional IKEv2 tunnel establishment procedure.

If the UE is connected to an ePDG selected by the procedure in subclause 7.2.1, and the ePDG has indicated its capability of support emergency service to the UE as specified in subclause 7.4.1.1 and is located in the same country where the UE is currently located, the UE, when it requires emergency services, shall initiate an IKEv2 tunnel establishment procedure towards the same ePDG to request for emergency session as specified in subclause 7.2.2 provided that an emergency PDN connection is not already active.

7.2.6 Mobile identity signaling

During the IKEv2 authentication and security association establishment, if the UE:

- receives IKE_AUTH response message from ePDG containing a Notify payload with the DEVICE_IDENTITY Notify Message Type and the Identity Type field of the DEVICE_IDENTITY Notify payload is set to either 'IMEI' or 'IMEISV' and the Identity Value field is empty;
- successfully authenticates the network or requests emergency session; and
- has Mobile Equipment Identity IMEI or IMEISV available,

the UE shall include the DEVICE_IDENTITY Notify payload in the new IKE_AUTH request message.

At any time after successful tunnel establishment, if the UE:

- receives INFORMATIONAL request message from ePDG containing a Notify payload with the DEVICE_IDENTITY Notify Message Type and the Identity Type field of the DEVICE_IDENTITY Notify payload is set to either 'IMEI' or 'IMEISV' and the Identity Value field is empty; and
- has the UE's Mobile Equipment Identity IMEI or IMEISV available,

the UE shall send INFORMATIONAL response containing a DEVICE_IDENTITY Notify payload.

The UE shall set the DEVICE_IDENTITY as follows:

- if IMEISV is available, the UE shall include IMEISV in the DEVICE_IDENTITY Notify payload. The Identity Type field of the DEVICE_IDENTITY Notify payload shall be set to 'IMEISV': and
- if IMEI is available and IMEISV is not available, the UE shall include IMEI in the DEVICE_IDENTITY attribute. The Identity Type field of the DEVICE_IDENTITY Notify payload shall be set to 'IMEI'.

The detailed coding of the DEVICE_IDENTITY Notify payload is described in subclause 8.2.9.2.

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

7.4.1.1 Tunnel establishment accepted by the network

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 as follows:

- 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; or

- 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; and

- 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 the UE included the P_CSCF_IP6_ADDRESS attribute, the P_CSCF_IP4_ADDRESS attribute or both in the CFG_REQUEST configuration payload, the ePDG may include one or more instances of the same attribute in the CFG_REPLY configuration payload as specified in IETF RFC 7651 [64]; and

- The ePDG may include the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in subclause 8.2.4.2 indicating the timeout period for liveness check in the CFG_REPLY configuration payload. Presence of the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute in the IKE_AUTH request can be used as input for decision on whether to include the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute.

If the UE does not provide an APN to the ePDG during the tunnel establishment of a non-emergency session, the ePDG shall include the default APN in the "IDr" payload of the IKE_AUTH response message. 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. The ePDG shall set the ID Type field of the "IDr" payload to ID_FQDN as defined in IETF RFC 5996 [28]. Handling of "IDr" payload in case of an emergency session is specified in subclause 7.4.4. An IPsec tunnel is now established between the UE and the ePDG.

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:

- if the PDN GW allocation type received from the 3GPP AAA server indicates the static allocation type, the received PDN GW identities shall be used to select PDN-GW; and

- if the PDN GW allocation type received from the 3GPP AAA server indicates the dynamic allocation type, the PDN GW is selected based on DNS query via the UE requested APN.

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].

If the IKE_AUTH request message contains a P-CSCF_RESELECTION_SUPPORT Notify payload as described in subclause 8.2.9.4 and if the ePDG supports the P-CSCF restoration extension (see 3GPP TS 23.380 [66]), the ePDG shall send a P-CSCF_RESELECTION_SUPPORT indication to the PGW.

If the ePDG supports emergency service, the ePDG shall send its capability indication of support emergency service to the UE by including the EMERGENCY_SUPPORT Notify payload within an IKE_AUTH response message. The content of the EMERGENCY_SUPPORT Notify payload is described in subclause 8.2.9.7.

7.4.1.2 Tunnel establishment not accepted by the network

During the tunnel establishment procedures, if the ePDG receives from the AAA Server the Authentication and Authorization Answer message with the Result code IE (as specified in 3GPP TS 29.273 [17]):

a) DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION, the ePDG shall include, in the IKE_AUTH response message to the UE, a Notify payload with a Private Notify Message Type NON_3GPP_ACCESS_TO_EPC_NOT_ALLOWED as defined in subclause 8.1.2;

b) DIAMETER_ERROR_USER_UNKNOWN, the ePDG shall include, in the IKE_AUTH response message to the UE, a Notify payload with a Private Notify Message Type USER_UNKNOWN as defined in subclause 8.1.2;

c) DIAMETER_AUTHORIZATION_REJECTED, the ePDG shall include, in the IKE_AUTH response message to the UE, a Notify payload with a Private Notify Message Type AUTHORIZATION_REJECTED as defined in subclause 8.1.2;

d) DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED, the ePDG shall include, in the IKE_AUTH response message to the UE, a Notify payload with a Private Notify Message Type RAT_TYPE_NOT_ALLOWED as defined in subclause 8.1.2;

e) DIAMETER_UNABLE_TO_ COMPLY, the ePDG shall include, in the IKE_AUTH response message to the UE, a Notify payload with a Private Notify Message Type NETWORK_FAILURE as defined in subclause 8.1.2 and the ePDG may also include a BACKOFF_TIMER Notify payload of the IKE_AUTH response message;

f) DIAMETER_ERROR_ROAMING_NOT_ALLOWED, the ePDG shall include, in the IKE_AUTH response message to the UE, a Notify payload with a Private Notify Message Type PLMN_NOT_ALLOWED as defined in subclause 8.1.2;

g) DIAMETER_ERROR_ USER_NO_APN_SUBSCRIPTION, the ePDG shall include, in the IKE_AUTH response message to the UE, a Notify Payload with a Private Notify Message Type NO_APN_SUBSCRIPTION

as defined in subclause 8.1.2 and the ePDG may also include a BACKOFF_TIMER Notify payload of the IKE_AUTH response message; or

h) DIAMETER_ERROR_ILLEGAL_EQUIPMENT, the ePDG shall include, in the IKE_AUTH response message to the UE, a Notify payload with a Private Notify Message Type ILLEGAL_ME as defined in subclause 8.1.2.

NOTE: In the cases a) through h), the ePDG still provides to the UE the information needed to authenticate 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, and the ePDG needs to reject a PDN connection for example due to the corresponding PDN GW identity not received for the APN, 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 and the Notification Data field with 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.

7.4.1A Liveness check

If the ePDG has not received any cryptographically protected IKEv2 or IPSec message for the duration of the timeout period for liveness check selected according to the local policy, the ePDG shall send an INFORMATIONAL request with no payloads IETF RFC 5996 [28]. If an INFORMATIONAL response is not received, the ePDG shall deem the IKEv2 security association to have failed.

7.4.1B Handling of NBIFOM

If the UE included the NBIFOM_GENERIC_CONTAINER Notify payload (see subclause 8.1.2.3) within the IKE_AUTH request message, and if required by procedures in 3GPP TS 24.161 [69], the ePDG shall include the same Notify payload within the IKE_AUTH response message as specified in 3GPP TS 24.161 [69]. The ePDG shall set the NBIFOM container contents field of the NBIFOM_GENERIC_CONTAINER Notify payload as specified in 3GPP TS 24.161 [69].

7.4.2 Tunnel modification

7.4.2.1 ePDG-initiated modification

The ePDG shall forward the list of available P-CSCF addresses received from the P-GW by including the P_CSCF_IP6_ADDRESS attribute, the P_CSCF_IP4_ADDRESS attribute or both as specified in IETF RFC 7651 [64] in the CFG_REQUEST configuration payload within the INFORMATIONAL request to the UE as specified in 3GPP TS 23.380 [66].

If the ePDG-initiated modification procedure is triggered by NBIFOM procedures in 3GPP TS 24.161 [69], the ePDG shall include the NBIFOM_GENERIC_CONTAINER Notify payload (see subclause 8.1.2.3) in the INFORMATIONAL request. The ePDG shall set the NBIFOM container contents field of the NBIFOM_GENERIC_CONTAINER Notify payload as specified in 3GPP TS 24.161 [69].

If the ePDG-initiated modification is initiated by a UE-initiated modification, i.e. by a received INFORMATIONAL request message, then the ePDG shall include in the sent INFORMATIONAL request message a PTI Notify payload as specified in subclause 8.1.2.3 with the Related Message ID field set to the Message ID field of the received INFORMATIONAL request message.

7.4.2.2 ePDG behaviour towards UE-initiated 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.

Upon of receipt of the NBIFOM_GENERIC_CONTAINER Notify payload (see subclause 8.1.2.3)in an INFORMATIONAL request, the ePDG shall reply with an INFORMATIONAL response and if required by procedures in 3GPP TS 24.161 [69], the ePDG shall include the NBIFOM_GENERIC_CONTAINER Notify payload in the INFORMATIONAL response. The ePDG shall set the NBIFOM container contents field of the NBIFOM_GENERIC_CONTAINER Notify payload as specified in 3GPP TS 24.161 [69].

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.

The INFORMATIONAL request message, in addition of the DELETE payload, may include the REACTIVATION_REQUESTED_CAUSE Notify payload.

If the ePDG receives the reactivation requested cause in a Delete Bearer Request over S2b, the ePDG shall include the REACTIVATION_REQUESTED_CAUSE Notify payload in the INFORMATIONAL request message containing a DELETE payload.

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.

7.4.3.3 Local tunnel disconnection initiated by PGW

A PDN connection over untrusted WLAN over S2b can be released locally in the ePDG, i.e. without any peer-to-peer signalling between the ePDG and the UE, based on the trigger received from the PGW, e.g. during the P-CSCF restoration procedure for NBIFOM PDN connections (see 3GPP TS 23.380 [66]).

Upon receiving a request from PGW to release the resources for a PDN connection with cause "local release" (see 3GPP TS 29.274 [50]) the ePDG shall:

a) close the related IKEv2 security association for the IPsec tunnel associated with this PDN connection; and

b) consider that the UE is no longer responding (see RFC 5996 [28]) and not send any messages to the UE.

7.4.4 Emergency session establishment

If the "IDr" payload containing the string "EMERGENCY", using capital letters only, in the Identification Data is included in the IKE_AUTH request message from the UE, the ePDG shall:

a) if:

   1) an INTERNAL_IP4_ADDRESS attribute with the length field set to zero;

   2) an INTERNAL_IP6_ADDRESS attribute with the length field set to zero; or

   3) both of the above;

   are included in the CFG_REQUEST Configuration Payload within the IKE_AUTH request message, handle the session establishment as an emergency session establishment;

b) if:

   1) an INTERNAL_IP4_ADDRESS attribute with the length field set to non-zero;

   2) an INTERNAL_IP6_ADDRESS attribute with the length field set to non-zero; or

   3) both of the above;

   are included in the CFG_REQUEST Configuration Payload within the IKE_AUTH request message, handle the session establishment as a handover of an emergency session;

c) in the IKE_AUTH response message, the ePDG shall not include the APN in the "IDr" payload; and

d) ignore the fact that the "EMERGENCY" string does not comply with the ID_FQDN ID Type, as described in IETF RFC 5996 [28].

In addition, if the IKE tunnel establishment is initiated for emergency session:

1) if IMSI is provided to the network but the ePDG receives from the AAA Server the Authentication and Authorization Answer message with the Result code IE indicating DIAMETER_ERROR_USER_UNKNOWN (see 3GPP TS 29.273 [17]), and thus the network considers the IMSI is unauthenticated:

   - if the ePDG is configured to support unauthenticated emergency session over WLAN and Mobile Equipment Identity signalling over untrusted WLAN, the ePDG shall request the IMEI from the UE using the Mobile Equipment Identity signalling procedure by including the DEVICE_IDENTITY Notify payload in the IKE_AUTH response message as specified in subclause 7.4.5; or

   - if the ePDG is not configured to support unauthenticated emergency session over WLAN or the ePDG is not configured to support Mobile Equipment Identity signalling over untrusted WLAN, the ePDG shall reject the requested PDN connection for emergency session. The ePDG shall include, in the IKE_AUTH response message, a Notify payload with a Private Notify Message Type "UNAUTHENTICATED_EMERGENCY_NOT_SUPPORTED" as specified in subclause 8.1.2; or

2) if IMSI is not provided to the network and the UE's IMEI is used as the User Identity in the IDi payload of the IKE_AUTH request message:

   - if the ePDG is configured to support emergency services from unauthenticated UE and the local policies and regulations allow unauthenticated emergency sessions, the ePDG forwards the EAP payload received from the UE to the 3GPP AAA Server serving the specific domain indicated in the realm part of NAI in the IDr payload; or

   - if the ePDG is not configured to support emergency services from unauthenticated UE or if the local policies and regulations do not allow unauthenticated emergency sessions, the ePDG shall reject the emergency services request from the UE with the Notify Message Type IMEI_NOT_ACCEPTED as specified in subclause 8.1.2.2.

7.4.5 Mobile identity signaling

If the network supports Mobile Equipment Identity signalling over untrusted WLAN, the ePDG may request the UE to provide the Mobile Equipment Identity by including the DEVICE_IDENTITY Notify payload with the Identity Type field set to either 'IMEI' or 'IMEISV' and an empty Identity Value field in:

- the IKE_AUTH response message to the initial IKE_AUTH request message received from the UE during the IKEv2 authentication and security association establishment; or

- the INFORMATIONAL request message at any time after successful IPSec tunnel establishment.

If the ePDG receives the following response message from the UE:

- the IKE_AUTH request message with the DEVICE_IDENTITY Notify payload; or

- the INFORMATIONAL response message with the DEVICE_IDENTITY Notify payload,

and the Identity Type field set to either 'IMEI' or 'IMEISV' and the Identity Value is not empty, the ePDG shall forward the received IMEI or IMEISV identity to the 3GPP AAA server as specified in 3GPP TS 29.273 [17] and to the PDN GW as specified in 3GPP TS 29.275 [18] and 3GPP TS 29.274 [50].

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.

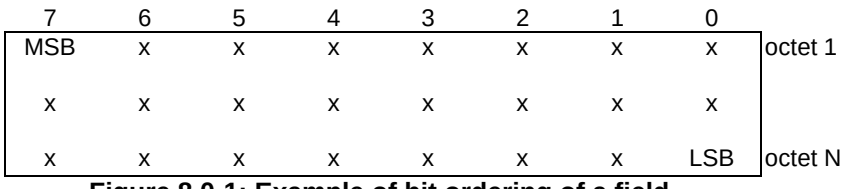

Figure 8.0-1: Example of bit ordering of a field

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 5996 [28].

The Notify Message Type with a value (in decimal) between 8192 and 16383 is reserved for private error usage.

The Notify Message Type with a value (in decimal) between 40960 and 65535 is reserved for private status usage.

Only the private IKEv2 Notify Message Types used for this specification are 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 (in decimal)	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.
NON_3GPP_ACCESS_TO_EPC_NOT_ALLOWED	9000	Corresponds to: - DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION Result code IE as specified in 3GPP TS 29.273 [17]; or - Other scenarios when the UE is not allowed to use non-3GPP access to EPC.
USER_UNKNOWN	9001	Corresponds to: - DIAMETER_ERROR_USER_UNKNOWN Result code IE as specified in 3GPP TS 29.273 [17]; or - Other scenarios when the user identified by the IMSI is unknown.
NO_APN_SUBSCRIPTION	9002	Corresponds to: - DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION Result code IE as specified in 3GPP TS 29.273 [17]; or - Other scenarios when the requested APN is not included in the user's profile, and therefore is not authorized for that user..
AUTHORIZATION_REJECTED	9003	Corresponds to: - DIAMETER_AUTHORIZATION_REJECTED Result code IE as specified in 3GPP TS 29.273 [17]; or - Other scenarios when the user is barred from using the non-3GPP access or the subscribed APN.
ILLEGAL_ME	9006	Corresponds to: - DIAMETER_ERROR_ILLEGAL_EQUIPMENT Result code IE as specified in 3GPP TS 29.273 [17]; or - Other scenarios when the ME used is not accepted by the network.
NETWORK_FAILURE	10500	Corresponds to: - DIAMETER_ERROR_UNABLE_TO_COMPLY Result code IE as specified in 3GPP TS 29.273 [17]; or - Other scenarios when the network has determined that the requested procedure cannot be completed successfully due to network failure.
RAT_TYPE_NOT_ALLOWED	11001	Corresponds to: - DIAMETER_RAT_TYPE_NOT_ALLOWED Result code IE as specified in 3GPP TS 29.273 [17]; or - Other scenarios when the access type is restricted to the user.
IMEI_NOT_ACCEPTED	11005	The emergency PDN connection request has been rejected since the network does not accept an emergency service request using an IMEI.

PLMN_NOT_ALLOWED	11011	Corresponds to: - DIAMETER_ERROR_ROAMING_NOT_ALLOWED Result code IE as specified in 3GPP TS 29.273 [17]; - The ePDG performs PLMN filtering (based on roaming agreements) and rejects the request from the UE; or - Other scenarios when the UE requests service in a PLMN where the UE is not allowed to operate.
UNAUTHENTICATED_ EMERGENCY_ NOT_SUPPORTED	11055	The emergency PDN connection request has been rejected due to authentication has failed or authentication cannot proceed at AAA server, and the ePDG does not support an emergency service request using an unauthenticated IMSI.

The private notify message error type values:

- between 9950 and 9999;
- between 10950 and 10999;
- between 11950 and 11999;
- between 12950 and 12999;
- between 13950 and 13999; and
- between 14950 and 14999;

will not be allocated to a Notify payload defined in the present specification.

8.1.2.3 Private Notify Message - Status Types

The Private Notify Message Status Types defined in table 8.1.2.3-1 are used to indicate status notifications or additional information in a Notify payload which may be added to an IKEv2 message or IKE_AUTH request or IKE_AUTH response message according to the procedures described in the present document. Refer to table 8.1.2.3-1 for more details on what each status type means.

Table 8.1.2.3-1: Private Status Types

Notify Message	Value (in decimal)	Descriptions
REACTIVATION_REQUESTED_CAUSE	40961	The IPsec tunnel associated to a PDN connection is released with a cause requesting the UE to reestablish the IPsec tunnel for the same PDN Connection after its release.
BACKOFF_TIMER	41041	The value of the backoff timer is included in the BACKOFF_TIMER Notify payload as specified in subclause 8.2.9.1.
DEVICE_IDENTITY	41101	The device identity type and/or identity value are included in the DEVICE_IDENTITY Notify payload as specified in subclause 8.2.9.2.
EMERGENCY_SUPPORT	41112	This status when present indicates that the ePDG supports emergency service. The EMERGENCY_SUPPORT Notify payload is coded according to subclause 8.2.9.7.
EMERGENCY_CALL_NUMBERS	41134	Additional local emergency call numbers that the UE may use for detecting UE initiated emergency calls. The EMERGENCY_CALL_NUMBERS Notify payload is coded according to subclause 8.2.9.8.
NBIFOM_GENERIC_CONTAINER	41288	The NBIFOM parameters are included in the NBIFOM_GENERIC_CONTAINER Notify payload as specified in subclause 8.2.9.3.
P-CSCF_RESELECTION_SUPPORT	41304	This status when present indicates that the UE supports the P-CSCF restoration extension for untrusted WLAN
PTI	41501	An INFORMATIONAL request message of an ePDG-initiated modification procedure is initiated by another INFORMATIONAL request message of an UE-initiated modification procedure. The PTI Notify payload is coded according to subclause 8.2.9.5.

The private notify message error type values:

- between 49950 and 49999;
- between 50950 and 50999;
- between 51950 and 51999;
- between 52950 and 52999;
- between 53950 and 53999; and
- between 54950 and 54999;

will not be allocated to a Notify payload defined in the present specification.

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	0x9071	The application identity indicates ANDSF

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.

The sending entity shall set value of spare bit to zero. The receiving entity shall ignore value of spare bit

8.1.4.1 Message

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

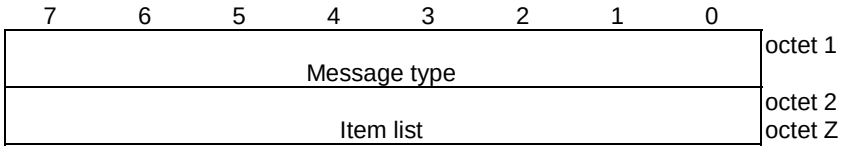

Figure 8.1.4.1-1: Message

Table 8.1.4.1-1: Message

Message type field is coded according to table 8.1.4.1-2. The message is ignored if Message type field containing a value other than those in table 8.1.4.1-2 is received. Optional Item list field contains sequence of items, each of which is coded according to subclause 8.1.4.2. The receiving entity does not assume that a certain order of items will be used in the Item list. When the receiving entity does not recognize an item in the Item list, that particular item is ignored, and the receiving entity continues to process the rest of the items in the Item list. 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

Message type 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:

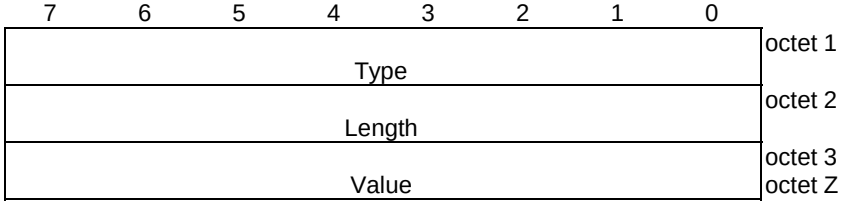

Figure 8.1.4.2-1: Item

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 entire Item is ignored. Length field indicates the number of octets in the Value field. Value field contains the parameter value of the type of item.

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
0	0	0	0	1	0	0	0	IPV4_ADDRESS
0	0	0	0	1	0	0	1	IPV6_INTERFACE_IDENTIFIER
0	0	0	0	1	0	1	0	TWAG_CP_ADDRESS
0	0	0	0	1	0	1	1	TWAG_UP_MAC_ADDRESS
0	0	0	0	1	1	0	0	SUPPORTED_WLCP_TRANSPORTS
0	0	0	0	1	1	0	1	Tw1
0	0	0	0	1	1	1	0	ACCESS CAUSE

8.1.4.3 CONNECTIVITY_TYPE item

When the Type field of this item, according to subclause 8.1.4.2, indicates the CONNECTIVITY_TYPE, then the Length field of this item is set to 1 and the Value field of this item is coded according to table 8.1.4.3-1.

Table 8.1.4.3-1: CONNECTIVITY_TYPE value

The Connectivity type value is coded as follows.

7	6	5	4	3	2	1	0	
0	0	0	0	0	0	0	1	PDN connection connectivity type
0	0	0	0	0	0	1	0	NSWO connectivity type

All other values are interpreted as "PDN connection connectivity type".

When the Connectivity Type item is received by the 3GPP AAA server, it indicates that the indicated connectivity type is requested.
When the Connectivity Type item is received by the UE, it indicates that the indicated connectivity type is authorized.

8.1.4.4 ATTACHMENT_TYPE item

When the Type field of this item according to subclause 8.1.4.2 indicates the ATTACHMENT_TYPE, then the Length field of this item is set to 1 and the Value field of this item is coded according to table 8.1.4.4-1.

Table 8.1.4.4-1: ATTACHMENT_TYPE value

The ATTACHMENT TYPE value is coded as follows.								
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
0	0	0	0	0	1	0	0	Emergency attach
0	0	0	0	0	1	1	0	Emergency handover
All other values are interpreted as "Initial attach".								

8.1.4.5 APN item

When the Type field of this item according to subclause 8.1.4.2 indicates the APN, then the Value field of this 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 this item according to subclause 8.1.4.2 indicates the PDN_TYPE, then the Length field of this item is set to 1 and the Value field of this item is coded according to table 8.1.4.6-1.

Table 8.1.4.6-1: PDN_TYPE value

The PDN type value is coded as follows.								
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.
All other values are interpreted as "IPv6".								

8.1.4.7 AUTHORIZATIONS item

When the Type field of this item according to subclause 8.1.4.2 indicates the AUTHORIZATIONS, then the Length field of this item is set to 1 and the Value field of this 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 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	NSWOA	octet 1

Figure 8.1.4.7-1: AUTHORIZATIONS value

Table 8.1.4.7-1: AUTHORIZATIONS value

The authorization 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 Bit 1 to bit 7 of octet 1 are spare.

8.1.4.8 CONNECTION_MODE_CAPABILITY item

When the Type field of this item according to subclause 8.1.4.2 indicates the CONNECTION_MODE_CAPABILITY, then the Length field of this item is set to 1 and the Value field of this 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 Spare	0 Spare	0 Spare	0 Spare	ES	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 Connection Mode Capability 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 Support of emergency services (ES) (octet 1, bit 3) 0 emergency services are not supported 1 emergency services are supported Bit 4 to bit 7 of octet 1 are spare.

8.1.4.9 PROTOCOL_CONFIGURATION_OPTIONS item

When the Type field of this item according to subclause 8.1.4.2 indicates the PROTOCOL_CONFIGURATION_OPTIONS, then the Value field of this item is coded as the value part (as specified in TS 24.007 [48] for type 4 IE) of the protocol configuration options information element defined in 3GPP TS 24.008 [46] subclause 10.5.6.3.

NOTE: The protocol configuration options IEI field and the length of protocol configuration options contents field of the protocol configuration options information element are not included in the Value field of the PROTOCOL_CONFIGURATION_OPTIONS item.

8.1.4.10 CAUSE item

8.1.4.10.1 General

When the Type field of this item according to subclause 8.1.4.2 indicates the CAUSE, then the Length field of this item is set to 1 and the Value field of this 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.

Semantics of the Cause values are defined in subclause 8.1.4.10.2.

Table 8.1.4.10-1: CAUSE value

The Cause value is coded as follows.

7	6	5	4	3	2	1	0	
0	0	0	0	1	0	0	0	Operator determined barring
0	0	0	1	1	0	1	0	Insufficient resources
0	0	0	1	1	0	1	1	Unknown APN
0	0	0	1	1	1	0	0	Unknown PDN type
0	0	0	1	1	1	0	1	User authentication failed
0	0	0	1	1	1	1	0	Request rejected by PDN GW
0	0	0	1	1	1	1	1	Request rejected, unspecified
0	0	1	0	0	0	0	0	Service option not supported
0	0	1	0	0	0	0	1	Requested service option not subscribed
0	0	1	0	0	0	1	0	Service option temporarily out of order
0	0	1	0	0	1	1	0	Network failure
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	0	1	1	0	1	1	0	PDN connection does not exist
0	1	1	0	1	1	1	1	Protocol error, unspecified
0	1	1	1	0	0	0	1	Multiple accesses to a PDN connection not allowed

All other values received by the UE are treated as 01101111, "Protocol error, unspecified".

8.1.4.10.2 Causes

Cause #8 - Operator determined barring

This cause is used by the network to indicate that the requested service was rejected due to operator determined barring.

Cause #26 - Insufficient resources

This cause is used by the network to indicate that the requested service cannot be provided due to insufficient resources.

Cause #27 - Unknown APN

This cause is used by the network to indicate that the requested service was rejected because the access point name could not be resolved.

Cause #28 - Unknown PDN type

This cause is used by the network to indicate that the requested service was rejected by the external packet data network because the PDN type could not be recognised.

Cause #29 - User authentication failed

This cause is used by the network to indicate that the requested service was rejected by the external packet data network due to a failed user authentication.

Cause #30 - Request rejected by PDN GW

This cause is used by the network to indicate that the requested service or operation was rejected by the PDN GW.

Cause #31 - Request rejected, unspecified

This cause is used by the network to indicate that the requested service or operation was rejected due to unspecified reasons.

Cause #32 - Service option not supported

This cause is used by the network when the UE requests a service which is not supported by the PLMN.

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 #34 - Service option temporarily out of order

This cause is sent when the network cannot service the request because of temporary outage of one or more functions required for supporting the service.

Cause #38 - Network failure

This cause is used by the network to indicate that the requested service was rejected due to an error situation in the network.

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 #54 – PDN connection does not exist

This value is used by the network at handover from a 3GPP access network to indicate that the network does not have any information about the requested PDN connection.

Cause #111 - Protocol error, unspecified

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

Cause #113 - Multiple accesses to a PDN connection not allowed

This value is used by the network to indicate that an additional access to the PDN connection as specified in 3GPP TS 24.161 [69] is not allowed.

This subclause shows the numbers in the decimal numeration system.

8.1.4.11 IPV4_ADDRESS item

When the Type field of this item according to subclause 8.1.4.2 indicates the IPV4_ADDRESS, then the Length field of this item is set to 4 and the Value field of this item contains an IPv4 address allocated to the UE for the PDN connection.

8.1.4.12 IPV6_INTERFACE_IDENTIFIER item

When the Type field of this item according to subclause 8.1.4.2 indicates the IPV6_INTERFACE_IDENTIFIER, then the Length field of this item is set to 8 and the Value field of this item contains an IPv6 interface identifier allocated to the UE for the PDN connection to be used to build the IPv6 link local address.

8.1.4.13 TWAG_CP_ADDRESS item

When the Type field of this item according to subclause 8.1.4.2 indicates the TWAG_CP_ADDRESS, then the Value field of this item contains one or two TWAG control plane addresses and is coded according to figure 8.1.4.13-1 and table 8.1.4.13-1.

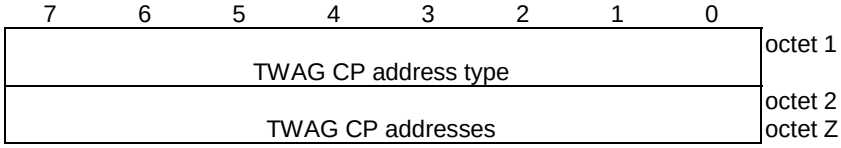

Figure 8.1.4.13-1: TWAG_CP_ADDRESS item value

Table 8.1.4.13-1: TWAG_CP_ADDRESS item value

The TWAG CP address type field (octet 1) is coded as follows.

7	6	5	4	3	2	1	0	
0	0	0	0	0	0	0	1	IPv4
0	0	0	0	0	0	1	0	IPv6
0	0	0	0	0	0	1	1	IPv4IPv6

All other values of the TWAG CP address type field are interpreted as "IPv4".

If the TWAG CP address type field indicates IPv4, then the TWAG CP addresses field contains one TWAG control plane address consisting of an IPv4 address in octet 2 to octet 5.

If the TWAG CP address type field indicates IPv6, then the TWAG CP addresses field contains one TWAG control plane address consisting of an IPv6 address in octet 2 to octet 17.

If the TWAG CP address type field indicates IPv4IPv6, then the TWAG CP addresses field contains two TWAG control plane addresses. The first TWAG control plane address consists of an IPv4 address in octet 2 to octet 5, the second TWAG control plane address consists of an IPv6 address in octet 6 to octet 21.

8.1.4.14 TWAG_UP_MAC_ADDRESS item

When the Type field of this item according to subclause 8.1.4.2 indicates the TWAG_UP_MAC_ADDRESS, then the Length field of this item is set to 6 and the Value field of this item contains a TWAG user plane MAC address allocated to the PDN connection. The MAC address is defined in subclause 8 of IEEE Std 802 [58].

8.1.4.15 SUPPORTED_WLCP_TRANSPORTS item

When the Type field of this item according to subclause 8.1.4.2 indicates the SUPPORTED_WLCP_TRANSPORTS, then the Length field of this item is set to 1 and the Value field of this item is coded according to figure 8.1.4.15-1 and table 8.1.4.15-1.

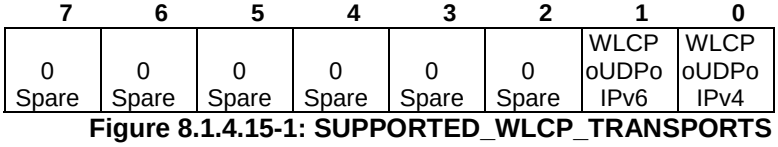

Figure 8.1.4.15-1: SUPPORTED_WLCP_TRANSPORTS value

Table 8.1.4.15-1: SUPPORTED_WLCP_TRANSPORTS value

The Supported WLCP transport value is coded as follows:
WLCP over UDP over IPv4 support (WLCPoUDPoIPv4) (octet 1, bit 0)
0 WLCP over UDP over IPv4 is not supported.
1 WLCP over UDP over IPv4 is supported.
WLCP over UDP over IPv6 support (WLCPoUDPoIPv6) (octet 1, bit 1)
0 WLCP over UDP over IPv6 is not supported.
1 WLCP over UDP over IPv6 is supported.
Bit 2 to bit 7 of octet 1 are spare.

8.1.4.16 Tw1 item

When the Type field of this item according to subclause 8.1.4.2 indicates the Tw1, then the Value field of this item is coded as the value part (as specified in TS 24.007 [48] for type 4 IE) of the GPRS timer 3 information element defined in 3GPP TS 24.008 [46] subclause 10.5.7.4a.

NOTE: The GPRS Timer 3 IEI field and the length of GPRS Timer 3 contents field of the GPRS timer 3 information element are not included in the Value field of the Tw1 item.

8.1.4.17 ACCESS_CAUSE item

8.1.4.17.1 General

When the Type field of this item according to subclause 8.1.4.2 indicates the ACCESS_CAUSE, then the Length field of this item is set to 1 and the Value field of this item is coded according to table 8.1.4.17-1.

Table 8.1.4.17-1: ACCESS_CAUSE value

The Access cause value is coded as follows.								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0	0	0	0	0	0	1	0	Non-3GPP access to EPC not allowed
0	0	0	0	0	0	1	1	RAT type now allowed
0	0	0	0	0	1	1	0	Illegal ME
0	0	0	0	1	0	1	1	PLMN not allowed

8.1.4.17.2 Access causes

Access cause #2- Non-3GPP access to EPC not allowed

This cause is used by the network to indicate that the requested service was rejected due to the user subscription data does not support EPS services from non-3GPP access.

Access cause #3- RAT type not allowed

This cause is used by the network to indicate that the requested service was rejected due to the WLAN is not allowed.

Access cause #6- Illegal ME

This cause is sent to the UE if the ME used is not acceptable to the network, e.g. blacklisted.

Access cause #11- PLMN not allowed

This cause is used by the network to indicate that the requested service was rejected due to the PLMN where the UE is roaming into is not allowed.

8.2 IETF RFC coding information defined within present document

8.2.1 IPMS attributes

8.2.1.1 AT_IPMS_IND attribute

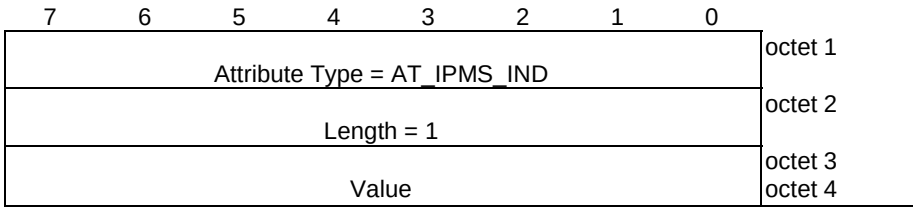

Figure 8.2.1.1: AT_IPMS_IND attribute

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

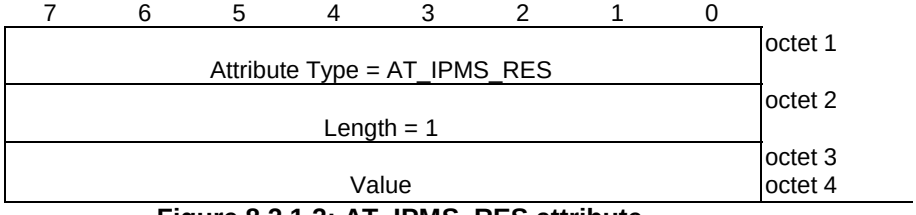

Figure 8.2.1.2: AT_IPMS_RES attribute.

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

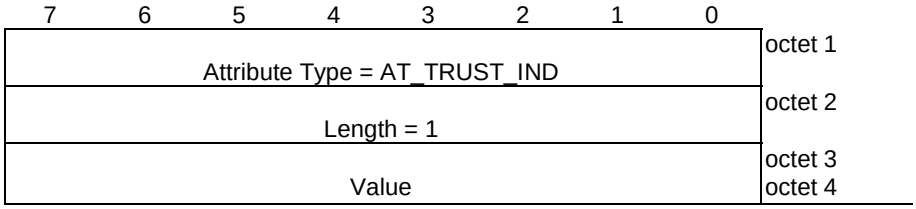

Figure 8.2.3.1-1: AT_TRUST_IND attribute

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.

8.2.4.2 TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute

The TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute is coded according to figure 8.2.4.2-1 and table 8.2.4.2-1.

Bits								
7	6	5	4	3	2	1	0	Octets
R	Attribute Type							1
Attribute Type								2
Length								3, 4
Timeout Period								5 - 8

Figure 8.2.4.2-1: TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute

Table 8.2.4.2-1: TIMEOUT_PERIOD_FOR_LIVENESS_CHECK value

Bit 7 of Octet 1 is the R bit defined in IETF RFC 5996 [28]. The R bit is the reserved bit set to zero. Bits 0 through 6 of Octet 1 and Octet 2 is the Attribute Type field. The Attribute Type field is set to value 24 to indicate the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK. Octet 3 and Octet 4 is the Length field. This field indicates the length in octets of the Timeout Period field. This field is set to 0 or 4. Octets 5, 6, 7 and 8 are the Timeout Period field. If the Timeout Period field is included, it indicates the timeout period for liveness check in seconds encoded in the binary format. If the Timeout Period field is not included in the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK configuration attribute by the UE, the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK indicates the UE's support of receiving the timeout period for liveness check.

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.

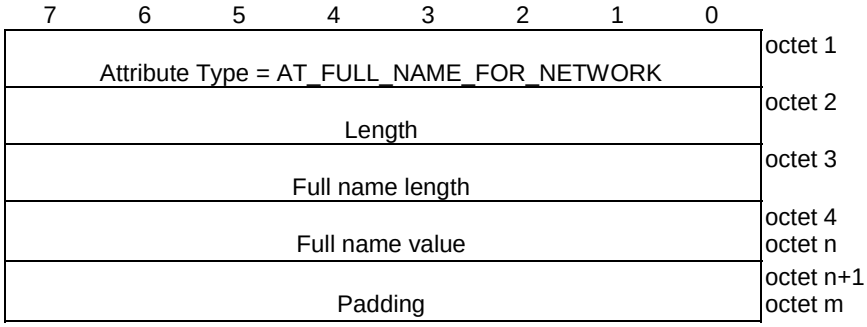

Figure 8.2.5.1-1: AT_FULL_NAME_FOR_NETWORK attribute

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.

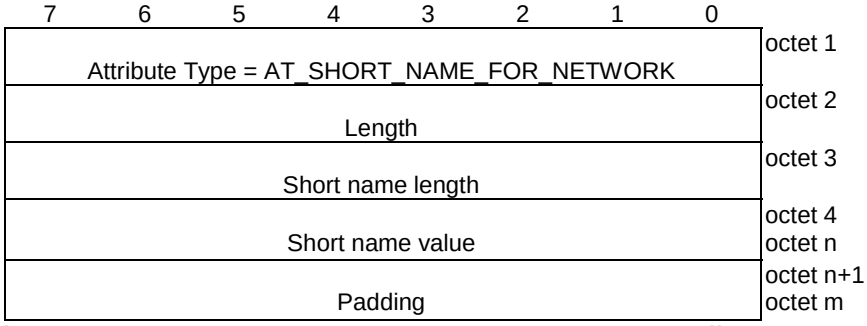

Figure 8.2.5.2-1: AT_SHORT_NAME_FOR_NETWORK attribute

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.

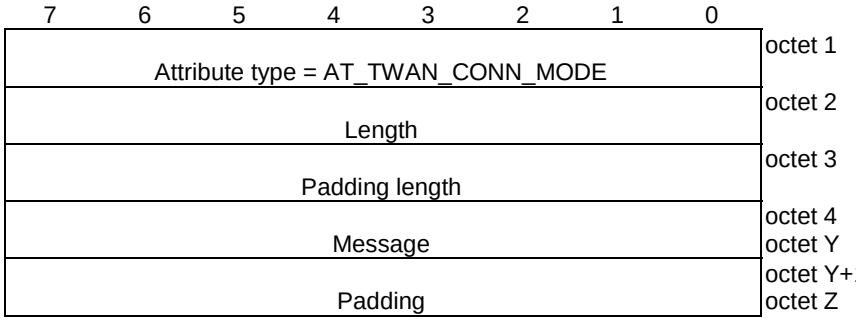

Figure 8.2.7.1-1: AT_TWAN_CONN_MODE attribute

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 144. 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.

8.2.8 Device Identity

8.2.8.1 AT_DEVICE_IDENTITY attribute

The AT_DEVICE_IDENTITY attribute is coded according to figure 8.2.8.1-1 and table 8.2.8.1-1.

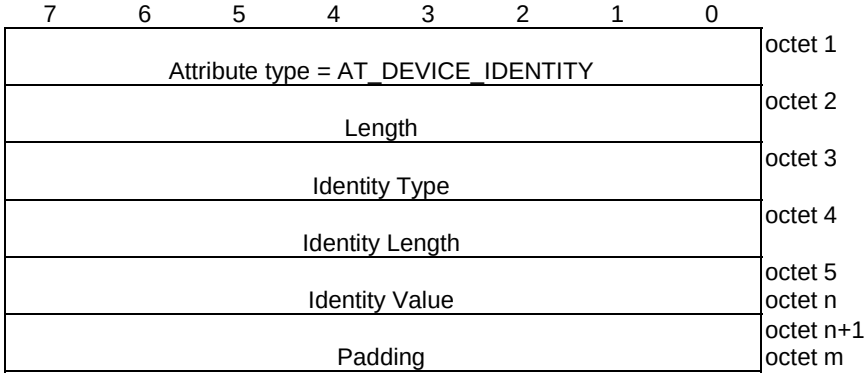

Figure 8.2.8.1-1: AT_DEVICE_IDENTITY attribute

Table 8.2.8.1-1: AT_DEVICE_IDENTITY attribute

Octet 1 indicates the type of attribute as AT_DEVICE_IDENTITY 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].

Octet 3 indicates the type of Device Identity.

Identity Type (octet 3)								
Bits								
7	**6**	**5**	**4**	**3**	**2**	**1**	0	
0	0	0	0	0	0	0	0	Reserved
0	0	0	0	0	0	0	1	IMEI
0	0	0	0	0	0	1	0	IMEISV
All other values are reserved.								

Octet 4 is Identity length field and contains the length of the Identity value in octets.

The Identity Value field starts at octet 5 and its length is indicated by the Identity length field. The Identity value field represents the device identity digits of the corresponding Identity type and is coded using BCD coding. The Identity Value field is optional.
For Identity Type 'IMEI' and 'IMEISV', Identity value digits are coded based on the IMEI and IMEISV structure defined in 3GPP TS 23.003 [3]. IMEI is 15 BCD digits and IMEISV is 16 BCD digits. Both IMEI and IMEISV are TBCD encoded. Bits 5 to 8 of octet i+4 (where i represents the octet of the IMEI(SV) being encoded) encodes digit 2i, bits 1 to 4 of octet i+4 encodes digit 2i-1 (i.e the order of digits is swapped in each octet compared to the digit order defined in 3GPP TS 23.003 [2]). Digits are packed contiguously with no internal padding. For IMEI, bits 5 to 8 of the last octet shall be filled with an end mark coded as '1111'.

The optional padding field starts after the last octet of the Identity value field. Each octet of this field is set to zero by sending entity and ignored by receiving entity.

8.2.9 IKEv2 Notify payloads

8.2.9.1 BACKOFF_TIMER Notify payload

The BACKOFF_TIMER Notify payload is used to indicate the value of the backoff timer. The BACKOFF_TIMER Notify payload type is 41041 (see subclause 8.1.2.3). The length of the BACKOFF_TIMER Notify payload is 6 octets.

The BACKOFF_TIMER Notify payload is coded according to figure 8.2.9.1-1 and table 8.2.9.1-1.

Bits								
7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3-4
Length=1								5
Backoff Timer Value								6

Figure 8.2.9.1-1: BACKOFF_TIMER Notify payload format

Table 8.2.9.1-1: BACKOFF_TIMER Notify payload value

Octet 1 is defined in IETF RFC 5996 [28] Octet 2 is SPI Size field. It is set to 0 and there is no Security Parameter Index field. Octet 3 and Octet 4 is the Notify Message Type field. The Notify Message Type field is set to value 41041 to indicate the Backoff Timer. Octet 5 is the Length field. This field indicates the length in octets of the Backoff Timer Value field. This field is set to 1. Octet 6 is the Backoff Timer Value field. This field indicates the value of Backoff Timer. It is coded as the value part (as specified in TS 24.007 [48] for type 4 IE) of the GPRS timer 3 information element defined in 3GPP TS 24.008 [46] subclause 10.5.7.4a (Note 1).
NOTE 1: The GPRS Timer 3 IEI field and the length of GPRS Timer 3 contents field of the GPRS timer 3 information element are not included in the value of the Backoff Timer.

8.2.9.2 DEVICE_IDENTITY Notify payload

The DEVICE_IDENTITY Notify payload is used to indicate the device identity. The DEVICE_IDENTITY Notify payload type is 41101 (see subclause 8.1.2.3).

The DEVICE_IDENTITY Notify payload is coded according to figure 8.2.2.9-1 and table 8.2.2.9-1.

Bits								
7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3-4
Length								5-6
Identity Type								7
Identity Value								8-n

Figure 8.2.9.2-1: DEVICE_IDENTITY Notify payload format

Table 8.2.9.2-1: DEVICE_IDENTITY Notify payload value

Octet 1 is defined in IETF RFC 5996 [28]

Octet 2 is SPI Size field. It is set to 0 and there is no Security Parameter Index field.

Octet 3 and Octet 4 is the Notify Message Type field. The Notify Message Type field is set to value 41101to indicate the DEVICE_IDENTITY.

Octet 5 and Octet 6 is the Length field. This field indicates the combined length in octets of the Identity Type and Identity Value fields.

Octet 7 is the Identity Type field. This field indicates the type of the device identity.

Identity Type (octet 7)								
Bits								
7	**6**	**5**	**4**	**3**	**2**	**1**	0	
0	0	0	0	0	0	0	0	Reserved
0	0	0	0	0	0	0	1	IMEI
0	0	0	0	0	0	1	0	IMEISV
All other values are reserved.								

Octet 8-n is the Identity Value field indicating the value of the device identity. The Identity value field represents the device identity digits of the corresponding Identity type and is coded using BCD coding. The Identity Value field is optional.
For Identity Type 'IMEI' and 'IMEISV', Identity value digits are coded based on the IMEI and IMEISV structure defined in 3GPP TS 23.003 [3]. IMEI is 15 BCD digits and IMEISV is 16 BCD digits. Both IMEI and IMEISV are TBCD encoded. Bits 5 to 8 of octet i+5 (where i represents the octet of the IMEI(SV) being encoded) encodes digit 2i, bits 1 to 4 of octet i+5 encodes digit 2i-1 (i.e the order of digits is swapped in each octet compared to the digit order defined in 3GPP TS 23.003 [2]). Digits are packed contiguously with no internal padding. For IMEI, bits 5 to 8 of the last octet shall be filled with an end mark coded as '1111'.

8.2.9.3 NBIFOM_GENERIC_CONTAINER Notify payload

The NBIFOM_GENERIC_CONTAINER Notify payload is used to contain the NBIFOM parameters.

The NBIFOM_GENERIC_CONTAINER Notify payload is coded according to figure 8.2.9.3-1 and table 8.2.9.3-1.

Bits								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**Octets**
Protocol ID								1
SPI Size								2
Notify Message Type								3 - 4
Length								5 - 6
NBIFOM container contents								7 - x

Figure 8.2.9.3-1: NBIFOM_GENERIC_CONTAINER Notify payload

Table 8.2.9.3-1: NBIFOM_GENERIC_CONTAINER Notify payload

Octet 1 is defined in IETF RFC 5996 [28]. Octet 2 is the SPI Size field. It is set to 0 and there is no Security Parameter Index field. Octet 3 and Octet 4 is the Notify Message Type field. The Notify Message Type field is set to value 41288 to indicate the NBIFOM_GENERIC_CONTAINER. Octet 5 and octet 6 is the Length field. The Length field indicates the length in octets of the NBIFOM container contents field. Octet 7 to octet x is the NBIFOM container contents field containing the NBIFOM parameter list as defined in 3GPP TS 24.161 [69], subclause 6.1.

8.2.9.4 P-CSCF_RESELECTION_SUPPORT Notify payload

The P-CSCF_RESELECTION_SUPPORT Notify payload is used to indicate the support by the UE of the P-CSCF restoration extension for untrusted WLAN.

The P-CSCF_RESELECTION_SUPPORT Notify payload is coded according to figure 8.2.9.4-1 and table 8.2.9.4-1.

Bits								
7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3-4

Figure 8.2.9.4-1: P-CSCF_RESELECTION_SUPPORT Notify Payload format

Table 8.2.9.4-1: P-CSCF_RESELECTION_SUPPORT Notify Payload field values

Octet 1 is defined in IETF RFC 5996 [28] Octet 2 is SPI Size field. It is set to 0 and there is no Security Parameter Index field. Octet 3 and Octet 4 is the Notify Message Type field. The Notify Message Type field is set to value 41304 to indicate the P-CSCF_RESELECTION_SUPPORT (see subclause 8.1.2.3).

8.2.9.5 PTI Notify payload

The PTI Notify payload is used to indicate that an INFORMATIONAL request message of an ePDG-initiated modification procedure is initiated by another INFORMATIONAL request message of an UE-initiated modification procedure.

The PTI Notify payload is coded according to figure 8.2.9.5-1 and table 8.2.9.5-1.

Bits								
7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3 - 4
Length								5 - 6
Related Message ID								7 - 10

Figure 8.2.9.5-1: PTI Notify payload

Table 8.2.9.5-1: PTI Notify payload

Octet 1 is defined in IETF RFC 5996 [28]. Octet 2 is the SPI Size field. It is set to 0 and there is no Security Parameter Index field. Octet 3 and Octet 4 is the Notify Message Type field. The Notify Message Type field is set to value 41501 (see subclause 8.1.2.3) to indicate the PTI. Octet 5 and octet 6 is the Length field. The Length field is set to 4. Octet 7 to octet 10 is the Related Message ID field containing the Message ID field of the INFORMATIONAL request message of the UE-initiated modification procedure which initiated the ePDG-initiated modification procedure.

8.2.9.6 REACTIVATION_REQUESTED_CAUSE Notify payload

The REACTIVATION_REQUESTED_CAUSE Notify payload is used to indicate the UE to re-establish the IPSec tunnel for the corresponding PDN connection after its release.

The REACTIVATION_REQUESTED_CAUSE Notify payload is coded according to figure 8.2.9.6-1 and table 8.2.9.6-1.

Bits 7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3-4

Figure 8.2.9.6-1: REACTIVATION_REQUESTED_CAUSE Notify payload format

Table 8.2.9.6-1: REACTIVATION_REQUESTED_CAUSE Notify payload field values

Octet 1 is defined in IETF RFC 5996 [28] Octet 2 is SPI Size field. It is set to 0 and there is no Security Parameter Index field. Octet 3 and Octet 4 is the Notify Message Type field. The Notify Message Type field is set to value 40961 to indicate the REACTIVATION_REQUESTED_CAUSE (see subclause 8.1.2.3).

8.2.9.7 EMERGENCY_SUPPORT Notify payload

The EMERGENCY_SUPPORT Notify payload is used to indicate the ePDG support of emergency service.

The EMERGENCY_SUPPORT Notify payload is coded according to figure 8.2.9.7-1 and table 8.2.9.7-1.

Bits 7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3-4

Figure 8.2.9.7-1: EMERGENCY_SUPPORT Notify Payload format

Table 8.2.9.7-1: EMERGENCY_SUPPORT Notify Payload field value

Octet 1 is defined in IETF RFC 5996 [28] Octet 2 is SPI Size field. It is set to 0 and there is no Security Parameter Index field. Octet 3 and Octet 4 is the Notify Message Type field. The Notify Message Type field is set to value 41112 to indicate the EMERGENCY_SUPPORT (see subclause 8.1.2.3).

8.2.9.8 EMERGENCY_CALL_NUMBERS Notify payload

The EMERGENCY_CALL_NUMBERS Notify payload is used:

a) by the ePDG to provide local emergency call numbers for use within the country indicated by the MCC information; and

b) by the UE to indicate support of retrieval of local emergency call numbers via IKEv2 procedures.

The EMERGENCY_CALL_NUMBERS Notify payload is coded according to figure 8.2.9.8-1 and table 8.2.9.8-1 with a minimum length of 4 octets and a maximum length of 55 octets.

Bits 7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3 - 4
MCC information								5
								6
Length								7
Local emergency numbers								8 - x

Figure 8.2.9.8-1: EMERGENCY_CALL_NUMBERS Notify payload

Table 8.2.9.8-1: EMERGENCY_CALL_NUMBERS Notify payload

Octet 1 is defined in IETF RFC 5996 [28]. Octet 2 is the SPI Size field. It is set to 0 and there is no Security Parameter Index field. Octet 3 and Octet 4 is the Notify Message Type field. The Notify Message Type field is set to value 41134 to indicate the EMERGENCY_CALL_NUMBERS. Octet 5 to octet 6 contains the MCC information of the country for which the emergency numbers indicated in the local emergency numbers field are applicable. If the EMERGENCY_CALL_NUMBERS Notify payload is included in the IKE_AUTH response message, then the MCC information field shall be populated. Octet 7 is the Length field. The Length field indicates the length in octets of the Local emergency numbers field. Octet 8 to octet x is the Local emergency numbers field containing the emergency call numbers is in the same format as the Emergency Number List defined in subclause 10.5.3.13 of 3GPP TS 24.008 [46], starting with octet 3. The MCC information field, length field and Local emergency numbers field are omitted when the UE sends the EMERGENCY_CALL_NUMBERS Notify payload to the network to indicate support of retrieval of local emergency call numbers.

The format of the MCC information item is shown in figure 8.2.9.8-2. Table 8.2.9.8-2 shows the coding of the MCC in the MCC information item.

7	6	5	4	3	2	1	0	
MCC digit 2				MCC digit 1				5
reserved				MCC digit 3				6

Figure 8.2.9.8-2: *MCC information* item

Table 8.2.9.8-2: *MCC information* item

MCC, Mobile country code (octet 5, octet 6 bits 1 to 4) The MCC field is coded as in ITU-T Rec. E212 [63], Annex A. Bits 5 to 8 of 6 shall be coded as "1111". Mobile equipment shall ignore bits 5 to 8 of octet 6.

8.2.10 EAP-3GPP-LimitedService method

8.2.10.1 General

The messages of EAP-3GPP-LimitedService method are EAP requests and EAP responses as specified in IETF RFC 3748 [29] subclause 4.1 and use coding of the expanded method type as described in IETF RFC 3748 [29] subclause 5.7.

The sending entity shall set value of a spare bit to zero. The receiving entity shall ignore value of a spare bit.

8.2.10.2 Message format

8.2.10.2.1 EAP-Request/3GPP-LimitedService-Init-Info message

EAP-Request/3GPP-LimitedService-Init-Info message is coded as specified in figure 8.2.10.2.1-1 and table 8.2.10.2.1-1.

Bits								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**Octets**
Code								1
Identifier								2
Length								3 - 4
Type								5
Vendor-Id								6 - 8
Vendor-Type								9 - 12
Message-Id								13
Spare								14
EAP-AKA attributes length								15 - 16
EAP-AKA attributes								17 - n
Extensions								n+1 - m

Figure 8.2.10.2.1-1: EAP-Request/3GPP-LimitedService-Init-Info message

Table 8.2.10.2.1-1: EAP-Request/3GPP-LimitedService-Init-Info message

Code field is set to 1 (decimal) as specified in IETF RFC 3748 [29] subclause 4.1 and indicates request. Identifier field is set as specified in IETF RFC 3748 [29] subclause 4.1. Length field is set as specified in IETF RFC 3748 [29] subclause 4.1 and indicates the length of the EAP-Request/3GPP-LimitedService-Init-Info message in octets. Type field is set to 254 (decimal) as specified in IETF RFC 3748 [29] subclause 5.7 and indicates the expanded type. Vendor-Id field is set to the 3GPP Vendor-Id of 10415 (decimal) registered with IANA under the SMI Private Enterprise Code registry. Vendor-Type field is set to EAP-3GPP-LimitedService method identifier of 2 (decimal) as specified in 3GPP TS 33.402 [15] annex C. Message-Id field is set to 3GPP-LimitedService-Init-Info-Id of 1 (decimal). Spare field consists of spare bits. EAP-AKA attributes length field indicates the length of EAP-AKA attributes field in octets. EAP-AKA attributes field contains attributes as specified in IETF RFC 4187 [33]. Extensions field is an optional field and consists of spare bits.

8.2.10.2.2 EAP-Response/3GPP-LimitedService-Init-Info message

EAP-Response/3GPP-LimitedService-Init-Info message is coded as specified in figure 8.2.10.2.2-1 and table 8.2.10.2.2-1.

Bits								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**Octets**
Code								1
Identifier								2
Length								3 - 4
Type								5
Vendor-Id								6 - 8
Vendor-Type								9 - 12
Message-Id								13
Spare								14
EAP-AKA attributes length								15 - 16
EAP-AKA attributes								17 - n
Extensions								n+1 - m

Figure 8.2.10.2.2-1: EAP-Response/3GPP-LimitedService-Init-Info message

Table 8.2.10.2.2-1: EAP-Response/3GPP-LimitedService-Init-Info message

Code field is set to 2 (decimal) as specified in IETF RFC 3748 [29] subclause 4.1 and indicates response. Identifier field is set as specified in IETF RFC 3748 [29] subclause 4.1. Length field is set as specified in IETF RFC 3748 [29] subclause 4.1 and indicates the length of the EAP-Response/3GPP-LimitedService-Init-Info message in octets. Type field is set to 254 (decimal) as specified in IETF RFC 3748 [29] subclause 5.7 and indicates the expanded type. Vendor-Id field is set to the 3GPP Vendor-Id of 10415 (decimal) registered with IANA under the SMI Private Enterprise Code registry. Vendor-Type field is set to EAP-3GPP-LimitedService method identifier of 2 (decimal) as specified in 3GPP TS 33.402 [15] annex C. Message-Id field is set to 3GPP-LimitedService-Init-Info-Id of 1 (decimal). Spare field consists of spare bits. EAP-AKA attributes length field indicates the length of EAP-AKA attributes field in octets. EAP-AKA attributes field contains attributes as specified in IETF RFC 4187 [33]. Extensions field is an optional field and consists of spare bits.

8.2.10.2.3 EAP-Request/3GPP-LimitedService-Notif message

EAP-Request/3GPP-LimitedService-Notif message is coded as specified in figure 8.2.10.2.3-1 and table 8.2.10.2.3-1.

Bits								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**Octets**
Code								1
Identifier								2
Length								3 - 4
Type								5
Vendor-Id								6 - 8
Vendor-Type								9 - 12
Message-Id								13
Spare								14
EAP-AKA attributes length								15 - 16
EAP-AKA attributes								17 - n
Extensions								n+1 - m

Figure 8.2.10.2.3-1: EAP-Request/3GPP-LimitedService-Notif message

Table 8.2.10.2.3-1: EAP-Request/3GPP-LimitedService-Notif message

Code field is set to 1 (decimal) as specified in IETF RFC 3748 [29] subclause 4.1 and indicates request. Identifier field is set as specified in IETF RFC 3748 [29] subclause 4.1. Length field is set as specified in IETF RFC 3748 [29] subclause 4.1 and indicates the length of the EAP-Request/3GPP-LimitedService-Notif message in octets. Type field is set to 254 (decimal) as specified in IETF RFC 3748 [29] subclause 5.7 and indicates the expanded type. Vendor-Id field is set to the 3GPP Vendor-Id of 10415 (decimal) registered with IANA under the SMI Private Enterprise Code registry. Vendor-Type field is set to EAP-3GPP-LimitedService method identifier of 2 (decimal) as specified in 3GPP TS 33.402 [15] annex C. Message-Id field is set to 3GPP-LimitedService-Notif-Id of 2 (decimal). Spare field consists of spare bits. EAP-AKA attribute length field indicates the length of EAP-AKA attributes field in octets. EAP-AKA attributes field contains attributes as specified in IETF RFC 4187 [33]. Extensions field is an optional field and consists of spare bits.

8.2.10.2.4 EAP-Response/3GPP-LimitedService-Notif message

EAP-Response/3GPP-LimitedService-Notif message is coded as specified in figure 8.2.10.2.4-1 and table 8.2.10.2.4-1.

	Bits								
	7	6	5	4	3	2	1	0	Octets
Code									1
Identifier									2
Length									3 - 4
Type									5
Vendor-Id									6 - 8
Vendor-Type									9 - 12
Message-Id									13
Extensions									14 -m

Figure 8.2.10.2.4-1: EAP-Response/3GPP-LimitedService-Notif message

Table 8.2.10.2.4-1: EAP-Response/3GPP-LimitedService-Notif message

Code field is set to 2 (decimal) as specified in IETF RFC 3748 [29] subclause 4.1 and indicates response. Identifier field is set as specified in IETF RFC 3748 [29] subclause 4.1. Length field is set as specified in IETF RFC 3748 [29] subclause 4.1 and indicates the length of the EAP-Response/3GPP-LimitedService-Notif message message in octets. Type field is set to 254 (decimal) as specified in IETF RFC 3748 [29] subclause 5.7 and indicates the expanded type. Vendor-Id field is set to the 3GPP Vendor-Id of 10415 (decimal) registered with IANA under the SMI Private Enterprise Code registry. Vendor-Type field is set to EAP-3GPP-LimitedService method identifier of 2 (decimal) as specified in 3GPP TS 33.402 [15] annex C. Message-Id field is set to 3GPP-LimitedService-Notif-Id of 2 (decimal). Extensions field is an optional field and consists of spare bits.

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.

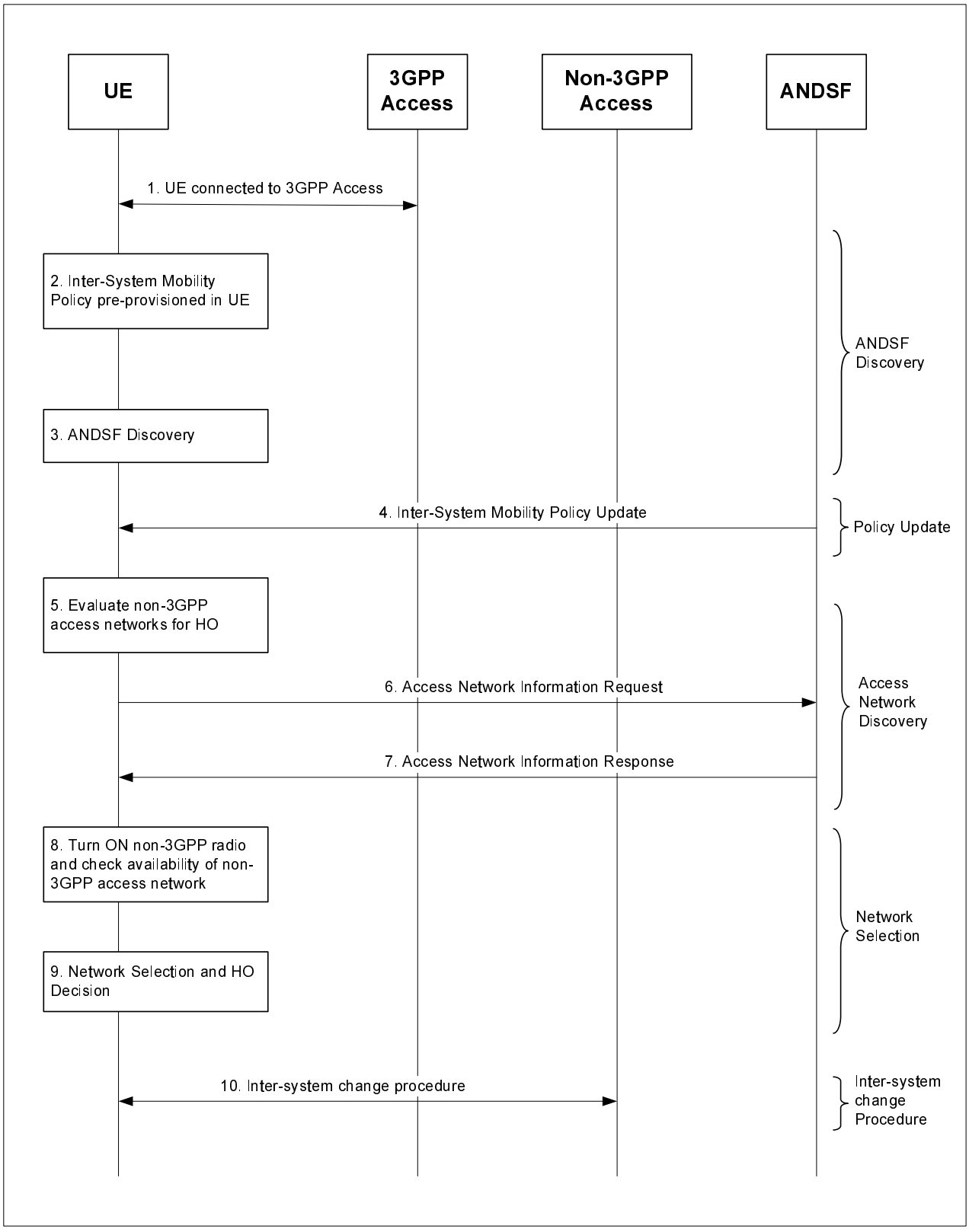

Figure A1. Procedure for Inter-system change between 3GPP access and non-3GPP using ANDSF

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 IP access 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 via the S2a or S2b, 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 does not 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 IP access 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 non-3GPP IP access access network.

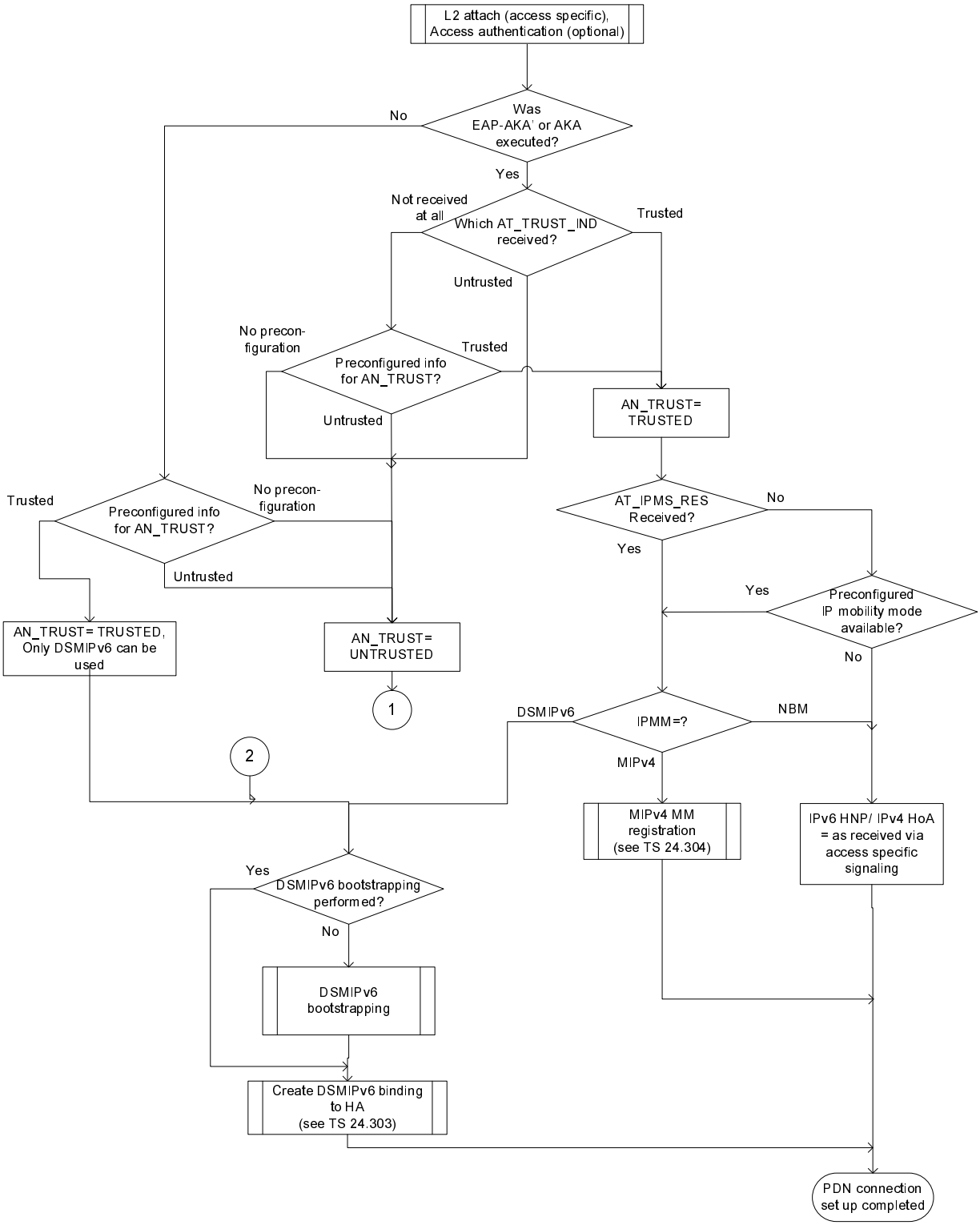

Figure E-1. Procedures to be followed by the UE depending on received and preconfigured information - part 1

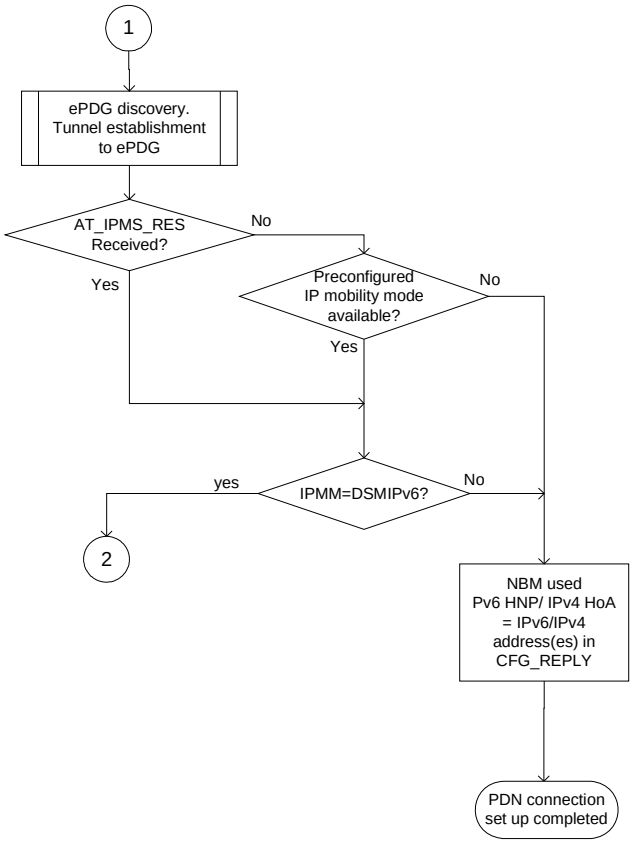

Figure E-2. Procedures to be followed by the UE depending on received and preconfigured information - part 2

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 TCP connection establishment is successful, the UE shall establish a TLS connection over the TCP connection according to the TLS profile specified in 3GPP TS 33.310 [65] annex E. 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 the TLS profile specified in 3GPP TS 33.310 [65] annex E.

The ePDG shall handle the TCP connection setup and shall handle the TLS connection establishment according to the TLS profile specified in 3GPP TS 33.310 [65] annex E.

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 the TLS profile specified in 3GPP TS 33.310 [65] annex E 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 the TLS profile specified in 3GPP TS 33.310 [65] annex E.

The ePDG shall handle the TCP connection setup and the TLS connection establishment according to the TLS profile specified in 3GPP TS 33.310 [65] annex E.

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 the TLS profile specified in 3GPP TS 33.310 [65] annex E, 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 the TLS profile specified in 3GPP TS 33.310 [65] annex E:

- 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 the TLS profile specified in 3GPP TS 33.310 [65] annex E:

- 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 the TLS profile specified in 3GPP TS 33.310 [65] annex E over an FTT of the UE.

The ePDG shall send the ESP envelope as TLS application data according to the TLS profile specified in 3GPP TS 33.310 [65] annex E 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 the TLS profile specified in 3GPP TS 33.310 [65] annex E 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 the TLS profile specified in 3GPP TS 33.310 [65] annex E.

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 the TLS profile specified in 3GPP TS 33.310 [65] annex E.

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 the TLS profile specified in 3GPP TS 33.310 [r33310] annex E.

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 the TLS profile specified in 3GPP TS 33.310 [65] annex E.

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.

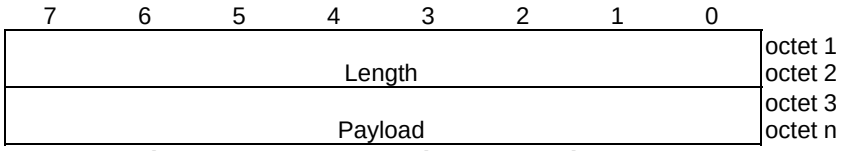

Figure F.3.2.1-1: Generic FTT envelope

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.

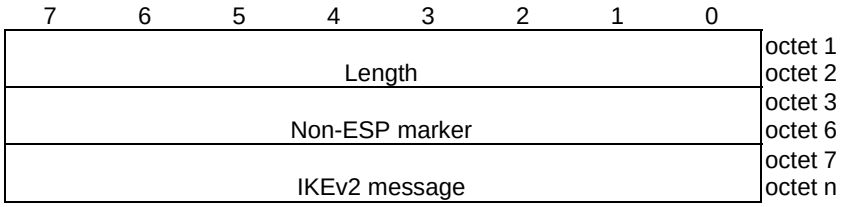

Figure F.3.2.2-1: IKEv2 envelope

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.

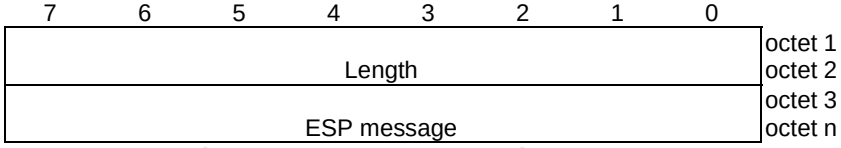

Figure F.3.2.3-1: ESP envelope

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.

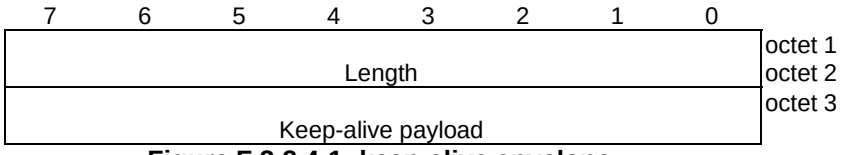

Figure F.3.2.4-1: keep-alive envelope

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.

Bits								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**Octets**
R	Attribute type							1
Attribute type								2
Length								3 - 4
Keep alive time								5 - 6

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 22. 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.

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

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)

G.2.3 AT_DEVICE_IDENTITY EAP-AKA attribute

In order to register the AT_DEVICE_IDENTITY 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_DEVICE_IDENTITY
- 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)

G.3 IKEv2 configuration attributes

G.3.1 General

This subclause contains information needed for registrations of IKEv2 configuration attributes with IANA.

G.3.2 TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute

In order to register the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK IKEv2 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 "IKEv2 Configuration Payload Attribute Types" of the "Internet Key Exchange Version 2 (IKEv2) Parameters" as shown at http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-21 and as specified in IETF RFC 4306 [70A] and updated by IETF RFC 5996 [28] and IETF RFC 7296 [70B].

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

The "IKEv2 Configuration Payload Attribute Types" of the "Internet Key Exchange Version 2 (IKEv2) Parameters" as shown at http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-21 and as specified in IETF RFC 4306 [70A] and updated by IETF RFC 5996 [28] and IETF RFC 7296 [70B].

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

This IKEv2 attribute is used to provide configuration for performing the liveness checks.

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

IETF RFC 4306 [70A] defines the registry for the "IKEv2 Configuration Payload Attribute Types".
IETF RFC 7296 [70B] and IETF RFC 5996 [28] refer to IETF RFC 4306 for the definition of the registry.

The following attribute is requested to be registered:

- value: (number to be assigned by IANA)
- attribute type: TIMEOUT_PERIOD_FOR_LIVENESS_CHECK
- multi-valued: no
- length: 4 octets
- reference: http://www.3gpp.org/ftp/Specs/html-info/24302.htm

Annex H (normative): Definition of generic container for ANQP payload

H.1 General

This subclause describes the structure and contents of the generic container used as the payload in the 3GPP Cellular Network ANQP-element specified in IEEE 802.11-2012 [57].

H.2 General structure

H.2.1 Structure

The general structure of the generic container is shown in figure H.2.1-1.

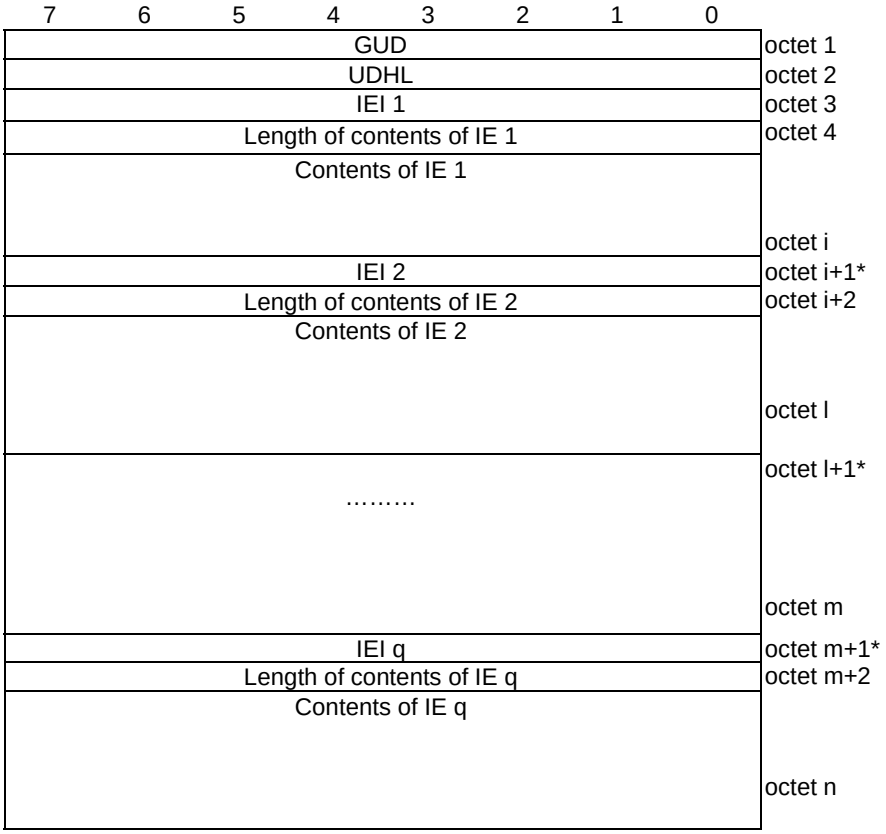

Figure H.2.1-1 – Structure of IEEE 802.11-2012 Generic Container

H.2.2 Generic container User Data (GUD)

Indicates the protocol version of the generic container

00000000 Version 1

00000001

To

11111111 Reserved

H.2.3 User Data Header Length (UDHL)

Indicates the number of octets in the generic container after the UDHL. This indication is encoded in binary format.

H.2.4 Information Elements

H.2.4.1 Information Element Identity (IEI)

Indicates the information element identity. The following values for IEI are defined in this version of the specification:

00000000 PLMN List

00000001 PLMN List with S2a connectivity

00000002

To

11111111 Reserved

H.2.4.2 PLMN List IE

The PLMN List information element is used by the network to indicate the PLMNs that can be selected from the WLAN. The format of the PLMN List information element coded according to 3GPP TS 24.007 [48] subclause 11.2.2.1 is shown in figure H.2.4.2-1.

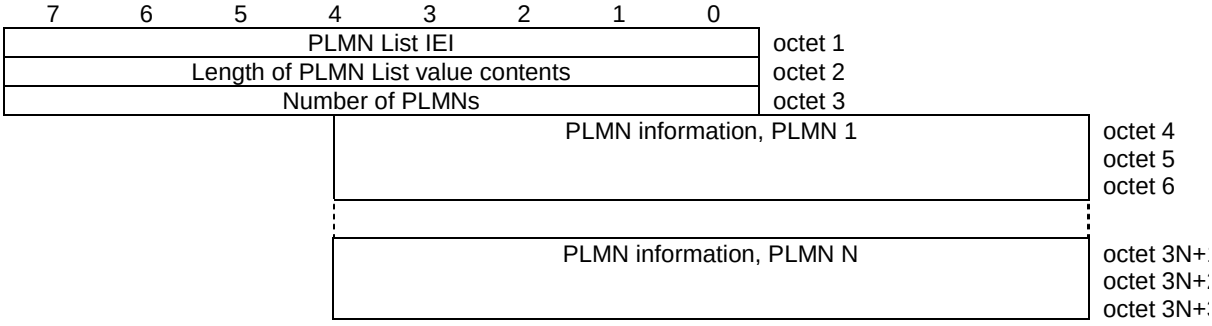

Figure H.2.4.2-1: *PLMN List* information element

The "Number of PLMNs" (octet 3) contains the number of PLMN information items in the list. Bit 7 of octet 3 is the most significant bit and bit 0 of octet 3 the least significant bit.

The format of the PLMN information item according to 3GPP TS 24.007 [48] subclause 11.2.2.1 is shown in figure H.2.4.2-2:

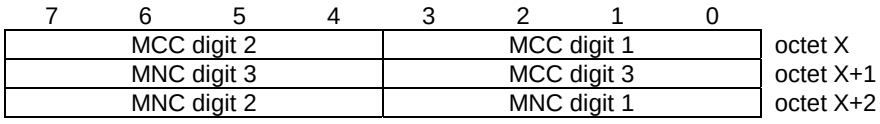

Figure H.2.4.2-2: *PLMN information* item of the PLMN List IE

Table H.2.4.2-1 shows the coding of the MCC and MNC in the PLMN information item.

Table H.2.4.2-1: *PLMN information* item of PLMN List IE

MCC, Mobile country code (octet X, octet X+1 bits 1 to 4) The MCC field is coded as in ITU-T Rec. E212 [63], Annex A. **MNC**, Mobile network code (octet X+2, octet X+1 bits 5 to 8). The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. For PCS 1900 for North America, Federal Regulation mandates that a 3-digit MNC shall be used. However a network operator may decide to use only two digits in the MNC over the radio interface. In this case, bits 5 to 8 of octet X+1 shall be coded as "1111". Mobile equipment shall accept MNC coded in such a way.

H.2.4.3 PLMN List with S2a Connectivity IE

The PLMN List with S2a connectivity information element is used by the WLAN to indicate the PLMNs to which the WLAN provides S2a connectivity.

The format of the PLMN List with S2a Connectivity information element is identical to the format of the PLMN List information element defined in subclause H.2.4.2.

Annex I (normative): Definition of the Emergency Call Number field's contents

I.1 General

The Emergency Call Number field is a variable-length UTF-8 (see RFC 3629 [34]) formatted field. The purpose of this field is to encode emergency call number(s) for use within the country where the field is received.

This subclause describes the formatting of the Emergency Call Number Unit field used in the Emergency Call Number ANQP-element specified in IEEE 802.11-2012 [57].

NOTE: According to IEEE 802.11-2012 [57] an ANQP server is not necessarily collocated with an AP. Where the TWAN provides access to multiple PLMNs, where a PLMN has configured the TWAN to provide different emergency numbers compared to another PLMN, it is an implementation option to ensure the Emergency Call Number field includes the emergency numbers configured by the PLMN the UE successfully authenticated and authorized with.

I.2 Formatting

I.2.1 General

For the purposes of aiding in detection of emergency call number and assigning the emergency type, the Emergency Call Number Unit field can contain an emergency call number and one or more emergency call labels.

The emergency call number and one or more emergency call labels shall be encoded as a namespace specific string for the namespace identifier equal to 3gpp (see RFC 5279 [74]). This specification further defines the namespace identifier equal to sos-anqp and parameters.

For the purposes of aiding in determining of the country where these local emergency numbers were provided, the Emergency Call Number field contains the MCC. The MCC represents the country in which the AP is located.

I.2.2 ABNF for the urn:3gpp:sos-anqp namespace and its parameters

Table I.2.2-1 contains the ABNF (RCF 2234 [73]) for the urn:3gpp:sos-anqp namespace and its parameters.

Table I.2.2-1: Syntax of urn:3gpp:sos-anqp

```
emergency-information   = "urn:3gpp:sos-anqp:" mcc *(":" number 1*(":" label ))
mcc                     = "mcc" DIGIT DIGIT (DIGIT)        ; exactly 2 or 3 digits
label                   = "sos" *("." sub-label)
number                  = DIGIT*DIGIT                      ; at least one DIGIT
sub-label               = let-dig [ *let-dig-hyp let-dig ]
let-dig-hyp             = let-dig / "-"
let-dig                 = ALPHA / DIGIT
ALPHA                   = %x41-5A / %x61-7A                ; A-Z / a-z
```

NOTE: While the syntax of table I.2.2-1 allows for many different sub-labels following "sos", when originating an emergency IMS session (see TS 24.229 [67]) based on detecting a match with dialed digits, the SIP INVITE will only contain one of the following service URNs: "urn:service:sos", "urn:service:sos.police", "urn:service:sos.ambulance", "urn:service:sos.fire", "urn:service:sos.marine", "urn:service:sos.mountain".

I.2.3 Semantics

According to the ABNF in table I.2.2-1:

- "urn:3gpp:sos-anqp:mcc310" is a valid expression: this expression indicates to the UE to overwrite any previously received list with Local WLAN emergency numbers with an empty list;

- "urn:3gpp:sos-anqp:mcc222:112:sos.police:sos.ambulance" is a valid expression: this expression indicates to the UE to that in the country with MCC 222 the number 112 is an emergency number. The corresponding labels sos.police and sos.ambulance are mapped in accordance with annex I.2.4.

I.2.4 Mapping Emergency Call Number field's contents to the Local WLAN Emergency Numbers List

When the Local WLAN Emergency Numbers List is to be encoded in the Local Emergency Numbers List format as defined in 3GPP TS 24.008 [46], subclause 10.5.3.13, the Emergency Call Number field's contents conforming to the ABNF for the urn:3gpp:sos-anqp namespace shall be mapped. The Local WLAN Emergency Numbers List for the PLMN with which the UE is connected via WLAN shall only be used when the contents are considered valid (see subclause 6.4.1).

The contents of the Emergency Call Number Unit field map to 4 bit encoded number digits and 5 bit encoded Emergency Service Category Value as follows. In addition to the rules in 3GPP TS 24.008 [46], the following mapping shall apply for a URN with UTF-8 (see RFC 3629 [34]) digits in the mcc ABNF portion that match the MCC of the PLMN with which the UE is connected via WLAN:

1) each UTF-8 digit in the emergency-number ABNF portion of the URN is converted into a corresponding 4-bit number digit of a set of octets part of an emergency number information; and

2) the label ABNF portion of the URN maps as follows:

   "sos": does not set bits of the 5 bit encoded Emergency Service Category Value of the emergency number information;

   "sos.police": sets bit 1 (police) of the 5 bit encoded Emergency Service Category Value of the emergency number information;

   "sos.ambulance": sets bit 2 (ambulance) of the 5 bit encoded Emergency Service Category Value of the emergency number information;

   "sos.fire": sets bit 3 (fire brigade) of the 5 bit encoded Emergency Service Category Value of the emergency number information;

   "sos.marine": sets bit 4 (marine guard) of the 5 bit encoded Emergency Service Category Value of the emergency number information;

   "sos.mountain": sets bit 5 (mountain rescue) of the 5 bit encoded Emergency Service Category Value of the emergency number information.

Annex J (normative): Emergency Call Numbers from DNS procedure

J.1 General

This subclause describes the retrieval of the Emergency Call Numbers field using DNS procedures.

The UE performs this procedure with a DNS server only, if the DNS server address is acquired from the ePDG using procedures in 3GPP TS 24.302 [156] subclause 7.2.2.1 and subclause 7.4.1, contained in the CFG_REPLY Configuration payload, and after mutual authentication of the UE and the network.

NOTE: The message carrying the emergency information is sent through the established IPsec tunnel to the 3GPP network.

The related Country based Emergency Numbers FQDN is specified in 3GPP TS 23.003 [3].

J.2 Retrieval of emergency call numbers

When a UE is connected to WLAN access, the UE may support the DNS mechanisms specified in this Annex to retrieve emergency call numbers and service types for use within the country indicated by the MCC information.

The UE shall construct an emergency number FQDN based on the Country based Emergency Numbers FQDN format as specified in 3GPP TS 23.003 [3] and then perform the DNS NAPTR query using the constructed emergency number FQDN as input.

If the result of this query is:

- a set of one or more records containing the replacement field of the form "<emergency-type>.<emergency-number>.sos.*en.epc.mcc*<*MCC*>.visited-country.*pub.3gppnework.org*", the UE shall consider the list of emergency-number(s) and type(s) as valid additional emergency call number(s) for the country indicated by the MCC information and store the emergency call number(s) and type(s) received;

NOTE: Even though a label named "visited-country" is present in the replacement field, the UE can use the mechanism to obtain emergency numbers and associated type(s) even when the UE is in its home country.

- no records containing the replacement field of the form "<emergency-number>.<emergency-type>.sos.*en.epc.mcc*<*MCC*>.visited-country.*pub.3gppnework.org*", the UE shall replace a Local Emergency Numbers List storing emergency call number(s) and type(s) received over WLAN with an empty Local Emergency Numbers List.

J.3 Void

Annex K (normative): Local Emergency Call Numbers from IKEv2 procedure

K.1 General

This subclause describes the retrieval of the local emergency call numbers using IKEv2 procedures.

The ePDG may support downloading local emergency call numbers using IKEv2 procedures.

The UE may support retrieval of local emergency call numbers using IKEv2 procedures.

K.2 Retrieval of local emergency call numbers

K.2.1 UE procedures

During the tunnel establishment procedure (see subclause 7.2.2), if the UE supports retrieval of local emergency call numbers via IKEv2 procedures, it shall include the EMERGENCY_CALL_NUMBERS Notify payload without the MCC information field, Length field and Local emergency numbers field (i.e. the octet 5 to octet x in figure 8.2.9.8-1) in the IKE_AUTH request message to indicate the support of retrieval of local emergency call numbers via IKEv2 procedures.

After the successful authentication with the 3GPP AAA server, the UE receives from the ePDG an IKE_AUTH response message, if:

a) the EMERGENCY_CALL_NUMBERS Notify payload is included in that IKE_AUTH response message; and

b) the UE supports retrieval of local emergency call numbers via IKEv2 procedures,

the UE shall store the local WLAN emergency call numbers and corresponding emergency service categories contained in the EMERGENCY_CALL_NUMBERS Notify payload as additional emergency call numbers and categories. The additional emergency call numbers and categories can be used to detect a UE initiated emergency call if the MCC information in the EMERGENCY_CALL_NUMBERS Notify payload corresponds to the country in which the UE is located. The local WLAN emergency call numbers and corresponding emergency service categories stored in the user equipment shall be replaced on each receipt of an EMERGENCY_CALL_NUMBERS Notify payload with a MCC information field that has a non-zero value Length field.

If:

- no MCC information field;
- no Length field; or
- a Length field, set to a non-zero value, is present but no Local emergency numbers field;

is present in a received EMERGENCY_CALL_NUMBERS Notify payload, then the local WLAN emergency call numbers and corresponding emergency service categories, if available in the user equipment, shall be kept.

K.2.2 ePDG procedures

The ePDG may be configured by the operator with the local emergency call numbers and associated emergency service types along with the corresponding country information.

After the successful authentication between the UE and the 3GPP AAA server, if:

a) the ePDG is configured with the local emergency call numbers information; and

b) the ePDG supports downloading of local emergency call numbers via IKEv2;

the ePDG shall based on local policy:

a) if the UE has indicated support of retrieval of local emergency call numbers via IKEv2 procedures,

i) derive the current visited country from the IP address of the IKEv2 message, i.e. the IP address contained in the out most IP header field of the received IKEv2 message; and

ii) include the configured local emergency call numbers and the associated emergency service categories of the derived country, if available, in the EMERGENCY_CALL_NUMBERS Notify payload in the final IKE_AUTH response message; or

b) always

i) derive the current visited country from the IP address of the IKEv2 message, i.e. the IP address contained in the out most IP header field of the received IKEv2 message; and

ii) include the configured local emergency call numbers and the associated emergency service categories of the derived country, if available, in the EMERGENCY_CALL_NUMBERS Notify payload in the final IKE_AUTH response message.

Annex L (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
2014-03	CT#63	CP-140139	0258	2	UE unaware whether the network uses the fixed access broadband access interworking or the fixed broadband access convergence	12.3.0	12.4.0
2014-03	CT#63	CP-140151	0259	5	Editor's note on UE support of SCM and MCM	12.3.0	12.4.0
2014-03	CT#63	CP-140151	0260		Editor's note on cause for 'None of the requested connectivity type(s) is authorized'	12.3.0	12.4.0
2014-03	CT#63	CP-140151	0261		Editor's note on usage of SCM and MCM being subject to UE subscription	12.3.0	12.4.0
2014-03	CT#63	CP-140151	0262	2	Providing IPv4 address and IPv6 interface identifier	12.3.0	12.4.0
2014-03	CT#63	CP-140151	0263	3	Network capability not supporting UE request for MCM/SCM	12.3.0	12.4.0
2014-03	CT#63	CP-140151	0264	2	Causes defined for WLCP which are also applicable to SCM	12.3.0	12.4.0
2014-03	CT#63	CP-140141	0266		Correction to misleading requirement on provision of ISMP	12.3.0	12.4.0
2014-03	CT#63	CP-140151	0267	1	Providing TWAG control plane address	12.3.0	12.4.0
2014-03	CT#63	CP-140137	0270	1	Access Network reselection procedures	12.3.0	12.4.0
2014-03	CT#63	CP-140137	0271	4	Remove 24.234 from WLAN selection procedures	12.3.0	12.4.0
2014-03	CT#63	CP-140141	0274	1	Deleting the repeated description about UE capability	12.3.0	12.4.0
2014-03	CT#63	CP-140151	0276	2	Clarify handling of Protocol Configuration Options	12.3.0	12.4.0
2014-03	CT#63	CP-140141	0277	2	Clarification for UE requirements about ANDSF rule evaluation	12.3.0	12.4.0
2014-06	CT#64	CP-140336	0268	3	Clarification on UE procedures according to 3GPP RAT differentiation in ISRP	12.4.0	12.5.0
2014-06	CT#64	CP-140335	0273	7	Introduction of WLAN selection mechanism based on WLANSP	12.4.0	12.5.0
2014-06	CT#64	CP-140319	0279	1	Providing TWAG User Plane address for usage in single-connection mode	12.4.0	12.5.0

2014-06	CT#64	CP-140319	0280	1	Providing TWAG control plane address for usage in multi-connection mode	12.4.0	12.5.0
2014-06	CT#64	CP-140319	0281		Corrections of minor errors	12.4.0	12.5.0
2014-06	CT#64	CP-140325	0283		Correction in applying IARP	12.4.0	12.5.0
2014-06	CT#64	CP-140325	0284	2	Relation between IARP and ISMP	12.4.0	12.5.0
2014-06	CT#64	CP-140319	0286	1	Requested connectivity type in SCM	12.4.0	12.5.0
2014-06	CT#64	CP-140325	0289	1	Clarification and cleanup for IARP	12.4.0	12.5.0
2014-06	CT#64	CP-140335	0293	2	WLAN network selection terminologies	12.4.0	12.5.0
2014-06	CT#64	CP-140335	0294	3	UE usage of access network selection information	12.4.0	12.5.0
2014-06	CT#64	CP-140335	0296	3	Introduce service provider that is not a 3GPP service provider	12.4.0	12.5.0
2014-06	CT#64	CP-140335	0302	1	Manual PLMN selection function	12.4.0	12.5.0
2014-06	CT#64	CP-140335	0303	3	UE behaviour in access Network reselection procedures	12.4.0	12.5.0
2014-06	CT#64	CP-140335	0304	4	Modification on active rule selection mechanism	12.4.0	12.5.0
2014-06	CT#64	CP-140335	0307	3	WLAN selection and service provider selection procedures	12.4.0	12.5.0
2014-09	CT#65	CP-140650	0292	4	Congestion control in SCM	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0299	4	Preferred Service Provider List	12.5.0	12.6.0
2014-09	CT#65	CP-140661	0300	5	Removal of I-WLAN references from ePDG selection procedure	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0306	3	HomeNetwork indicator in WLAN selection	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0308	3	Reuse 3GPP defined EAP-AKA procedures	12.5.0	12.6.0
2014-09	CT#65	CP-140574	0309	4	Clarifying WLAN selection procedures in case of multiple candidate WLANs	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0310	3	Completing service provider discovery procedures based on EAP	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0311	2	Adding support for HPLMN identified with a non-PLMN realm	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0313		Repeated rule selection information	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0314	2	Selection of WLANSP during power-up	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0315	1	Selection of the active ISMP and ISRP	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0316	2	Usage of ISMP/ISRP	12.5.0	12.6.0
2014-09	CT#65	CP-140659	0320	1	User preference handling for data traffic routing	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0323	3	Clarifications to WLAN selection procedures	12.5.0	12.6.0
2014-09	CT#65	CP-140672	0324		Removal of editor's note on active WLANSP rule	12.5.0	12.6.0
2014-09	CT#65	CP-140678	0325	5	IEEE 802.11u generic container for ANQP payload	12.5.0	12.6.0
2014-09	CT#65	CP-140571	0326	4	3GPP access stratum layer controlling UE usage of WLAN	12.5.0	12.6.0
2014-09	CT#65	CP-140650	0330		Initiating IANA registration for AT_TWAN_CONN_MODE EAP-AKA attribute	12.5.0	12.6.0
2014-12	CT#66	CP-140854	0331	1	Removal of priority of WLAN identifiers provided by the RAN	12.6.0	12.7.0
2014-12	CT#66	CP-140854	0332	2	Correcting references to WLAN offload indication IE	12.6.0	12.7.0
2014-12	CT#66	CP-140854	0333	1	3GPP access stratum layer controlling UE usage of WLAN, in UEs NOT capable to simultaneously route IP traffic to both 3GPP access and WLAN access	12.6.0	12.7.0
2014-12	CT#66	CP-140840	0334		Corrections in procedures	12.6.0	12.7.0
2014-12	CT#66	CP-140840	0335	2	Corrections in data structures	12.6.0	12.7.0
2014-12	CT#66	CP-140840	0336	1	Correcting remaining cases of UE capabilities not matching network capabilities	12.6.0	12.7.0
2014-12	CT#66	CP-140832	0337	1	Fixing inconsistency in usage of VPLMNs with preferred rules	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0338	1	HotSpot2.0 Rel-2 reference update	12.6.0	12.7.0
2014-12	CT#66	CP-140854	0340	3	3GPP access stratum layer controlling UE usage of WLAN using OPI	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0341	2	Correcting error in IEEE 802.11u generic container	12.6.0	12.7.0
2014-12	CT#66	CP-140838	0342	2	IANA registration of FTT_KAT parameter	12.6.0	12.7.0
2014-12	CT#66	CP-140854	0343	2	Support of Beacon RSSI threshold as RAN assistance information	12.6.0	12.7.0
2014-12	CT#66	CP-140840	0347	1	DTLS key derivation for multi-connection mode	12.6.0	12.7.0
2014-12	CT#66	CP-140854	0350	5	RAN assistance information and traffic routing	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0353	1	Clarification on how to select an ePDG	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0354	4	Complete Manual Service Provider selection mode procedure	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0355	2	Complete Manual mode WLAN selection	12.6.0	12.7.0
2014-12	CT#66	CP-140840	0362	3	Removal of UDP info from TWAG_CP_ADDRESS	12.6.0	12.7.0
2014-12	CT#66	CP-140835	0363	1	The usage of the IARP rule and the ISRP rule	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0364	3	Automatic WLAN selection procedure cleanup	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0365	3	Service Provider selection cleanup	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0366	3	S2a WLAN selection must take PLMNs into account	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0367	2	Equivalent service provider clarification	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0371	3	Mode selection at switch-on	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0372	3	WLANSP/ISMP/ISRP rule re-selection	12.6.0	12.7.0
2014-12	CT#66	CP-140854	0374		Correction for Offload Preference Indicator (OPI)	12.6.0	12.7.0
2014-12	CT#66	CP-140832	0376	2	Update to reference IEEE 802	12.6.0	12.7.0
2014-12	CT#66	CP-140844	0368	1	Correction on root NAI usage during automatic mode service provider selection using WLAN	12.6.0	12.7.0
2014-12	CT#66	CP-140857	0346	1	Transport of P-CSCF addresses using signalling for access to EPC via WLAN connected using S2b	12.7.0	13.0.0
2015-03	CT#67	CP-150068	0381	1	Correcting references to 23.003	13.0.0	13.1.0
2015-03	CT#67	CP-150065	0383	1	IANA registration of AT_TWAN_CONN_MODE EAP-AKA attribute	13.0.0	13.1.0
2015-03	CT#67	CP-150075	0385		Correcting 3GPP access network terms	13.0.0	13.1.0

2015-03	CT#67	CP-150065	0387	2	Correcting description of semantic of unrecognized values	13.0.0	13.1.0
2015-03	CT#67	CP-150075	0389	1	Enforcement of RAN rules when new PDN connection is created in 3GPP access	13.0.0	13.1.0
2015-03	CT#67	CP-150068	0391	1	Cross reference update	13.0.0	13.1.0
2015-03	CT#67	CP-150075	0394	2	UE handling of ISRP and IARP rules for traffic routing	13.0.0	13.1.0
2015-03	CT#67	CP-150077	0396	1	WLANSP Information provided from ANDSF to the UE	13.0.0	13.1.0
2015-03	CT#67	CP-150061	0398	1	Reference update to IEEE 802.11u standard	13.0.0	13.1.0
2015-03	CT#67	CP-150042	0400	4	Usage of RAN rule in SCM	13.0.0	13.1.0
2015-03	CT#67	CP-150077	0401	1	UE retaining IARP from the H-ANDSF	13.0.0	13.1.0
2015-03	CT#67	CP-150077	0402	2	IKEv2 security associations when an additional PDN connection is setup via untrusted non-3GPP access network	13.0.0	13.1.0
2015-03	CT#67	CP-150075	0406	1	PLMN selection when using RAN rule	13.0.0	13.1.0
2015-03	CT#67	CP-150068	0413	1	Introduction of Visited Network Preference information	13.0.0	13.1.0
2015-06	CT#68	CP-150323	0414	1	ID Type field of IDr payload carrying APN	13.1.0	13.2.0
2015-06	CT#68	CP-150321	0415		draft-gundavelli-ipsecme-3gpp-ims-options reference update	13.1.0	13.2.0
2015-06	CT#68	CP-150323	0416	3	Correction to ePDG selection	13.1.0	13.2.0
2015-06	CT#68	CP-150323	0417	1	INITIAL_CONTACT notification when additional PDN connection is established	13.1.0	13.2.0
2015-06	CT#68	CP-150314	0421	3	Priority defined in preferredSSIDlist	13.1.0	13.2.0
2015-06	CT#68	CP-150323	0422	3	Cause value for EPC forbidden	13.1.0	13.2.0
2015-06	CT#68	CP-150308	0428	1	ANDSF information on visited PLMNs with preferred rules	13.1.0	13.2.0
2015-06	CT#68	CP-150305	0436	2	Timer Tw1	13.1.0	13.2.0
2015-06	CT#68	CP-150329	0438		Aligning TLS profiles used by CT1 specifications with SA3 agreed TLS profile	13.1.0	13.2.0
2015-06	CT#68	CP-150323	0443	3	Clarify when to use root NAI	13.1.0	13.2.0
2015-06	CT#68	CP-150323	0445	3	Adding a general subclause to clause 5	13.1.0	13.2.0
2015-06	CT#68	CP-150314	0448	1	Rule selection information	13.1.0	13.2.0
2015-06	CT#68	CP-150323	0449	2	IKEv2 liveness check	13.1.0	13.2.0
2015-06	CT#68	CP-150323	0450	4	Switch-on and switch-off for non-3GPP access	13.1.0	13.2.0
2015-09	CT#69	CP-150519	0453		Incorrect reference [28]	13.2.0	13.3.0
2015-09	CT#69	CP-150522	0458	1	IKEv2 extension for P-CSCF restoration over untrusted WLAN	13.2.0	13.3.0
2015-09	CT#69	CP-150533	0459	2	Support of Emergency services over WLAN access to EPC	13.2.0	13.3.0
2015-09	CT#69	CP-150524	0460	3	Support of IMEI signalling for trusted WLAN access	13.2.0	13.3.0
2015-09	CT#69	CP-150524	0461	1	Support of IMEI signalling via IKEv2 for un-trusted access	13.2.0	13.3.0
2015-09	CT#69	CP-150527	0463	3	DIAMETER_AUTHORIZATION_REJECTED for untrusted WLAN	13.2.0	13.3.0
2015-09	CT#69	CP-150527	0464	2	DIAMETER_AUTHORIZATION_REJECTED for trusted WLAN	13.2.0	13.3.0
2015-09	CT#69	CP-150527	0465	2	DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION	13.2.0	13.3.0
2015-09	CT#69	CP-150527	0466	2	DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION	13.2.0	13.3.0
2015-09	CT#69	CP-150527	0467	2	DIAMETER_UNABLE_TO_ COMPLY	13.2.0	13.3.0
2015-09	CT#69	CP-150527	0468	2	DIAMETER_UNABLE_TO_ COMPLY	13.2.0	13.3.0
2015-09	CT#69	CP-150527	0469	1	Clarify the re-established PDN connection	13.2.0	13.3.0
2015-09	CT#69	CP-150526	0470	1	Handling of NBIFOM during tunnel establishment procedure	13.2.0	13.3.0
2015-09	CT#69	CP-150526	0471	1	Handling of NBIFOM during tunnel modification procedure	13.2.0	13.3.0
2015-09	CT#69	CP-150519	0478	1	Correct bullets	13.2.0	13.3.0
2015-09	CT#69	CP-150527	0480	3	DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION error code mapping to IKEv2	13.2.0	13.3.0
2015-09	CT#69	CP-150515	0486	2	EAP-AKA procedures for untrusted non-3GPP access network	13.2.0	13.3.0
2015-09	CT#69	CP-150574	0487	3	Selection of ePDG for emergency bearer services	13.2.0	13.3.0
2015-12	CT#70	CP-150696	0456	7	Liveness check corrections	13.3.0	13.4.0
2015-12	CT#70	CP-150707	0491	2	DIAMETER_ERROR_ROAMING _NOT_ ALLOWED for trusted WLAN	13.3.0	13.4.0
2015-12	CT#70	CP-150714	0494	1	APN handling in Emergency session establishment	13.3.0	13.4.0
2015-12	CT#70	CP-150696	0495		Correction of IP address handling during handover to untrusted non-3GPP access	13.3.0	13.4.0
2015-12	CT#70	CP-150695	0496		draft-gundavelli-ipsecme-3gpp-ims-options became RFC7651	13.3.0	13.4.0
2015-12	CT#70	CP-150714	0497	3	ePDG selection configuration in USIM for emergency services	13.3.0	13.4.0
2015-12	CT#70	CP-150696	0498	2	UE handling of ANDSF information	13.3.0	13.4.0
2015-12	CT#70	CP-150707	0502	6	DIAMETER_ERROR_USER_UNKNOWN, DIAMETER_ERROR_ROAMING_NOT_ALLOWED, DIAMETER_AUTHORIZATION_REJECTED and DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED result codes for untrusted WLAN	13.3.0	13.4.0
2015-12	CT#70	CP-150691	0505	1	Correction for content of IDi payload	13.3.0	13.4.0
2015-12	CT#70	CP-150706	0506	1	NBIFOM_GENERIC_CONTAINER definition	13.3.0	13.4.0
2015-12	CT#70	CP-150706	0507		Reducing NBIFOM specific statements for untrusted non-3GPP access	13.3.0	13.4.0
2015-12	CT#70	CP-150696	0508	1	UE backoff Handling for trusted WLAN access to EPC using SCM	13.3.0	13.4.0
2015-12	CT#70	CP-150703	0509	1	Mid-call IMEI signaling for untrusted acess	13.3.0	13.4.0
2015-12	CT#70	CP-150696	0510	2	Reference UE authentication of ePDG to 33.402	13.3.0	13.4.0
2015-12	CT#70	CP-150710	0514	2	Reactivation Requested cause over untrusted WLAN	13.3.0	13.4.0
2015-12	CT#70	CP-150706	0515		Multiple accesses to a PDN connection not allowed for SCM	13.3.0	13.4.0
2015-12	CT#70	CP-150707	0516	2	Error cases for the trusted WLAN	13.3.0	13.4.0

2015-12	CT#70	CP-150707	0517	2	HO procedures without PGW ID	13.3.0	13.4.0
2015-12	CT#70	CP-150707	0518	1	Define AAA Server behaviour in procedure subclause	13.3.0	13.4.0
2015-12	CT#70	CP-150701	0519		Replace CFG SET/CFG_ACK with CFG_REQUEST/CFG_REPLY	13.3.0	13.4.0
2015-12	CT#70	CP-150877	0426	20	Selection of ePDG based on home operator preference	13.3.0	13.4.0
2016-03	CT#71	CP-160070	0511	7	Authentication Signalling Improvement with Backoff Timer for untrusted access	13.4.0	13.5.0
2016-03	CT#71	CP-160070	0512	10	Authentication Signalling Improvement with Backoff Timer for SCM	13.4.0	13.5.0
2016-03	CT#71	CP-160082	0521	1	Remove editor's note on ePDG selection	13.4.0	13.5.0
2016-03	CT#71	CP-160083	0523	4	Selecting ePDG for emergency services in WLAN	13.4.0	13.5.0
2016-03	CT#71	CP-160070	0524	1	Remove editor's notes	13.4.0	13.5.0
2016-03	CT#71	CP-160082	0526	1	Add cause values for SCM	13.4.0	13.5.0
2016-03	CT#71	CP-160082	0527	2	Confusing and misuse of the term and indication of "value"	13.4.0	13.5.0
2016-03	CT#71	CP-160070	0520	1	ASI_WLAN cleanup	13.4.0	13.5.0
2016-03	CT#71	CP-160082	0528	3	Replace undefined terms and reword untestable conditions	13.4.0	13.5.0
2016-03	CT#71	CP-160078	0530	1	Correction on IKEv2 messages carrying CFG_REQUEST and CFG_REPLY	13.4.0	13.5.0
2016-03	CT#71	CP-160078	0531	1	ePDG-initiated modification initiated by UE-initiated modification	13.4.0	13.5.0
2016-03	CT#71	CP-160077	0533	3	DEVICE_IDENTITY signalling using IKEv2 Notify payload	13.4.0	13.5.0
2016-03	CT#71	CP-160078	0532	1	Change NBIFOM_GENERIC_CONTAINER from Configuration payload to Notify payload	13.4.0	13.5.0
2016-03	CT#71	CP-160083	0537	3	Handling of emergency indication for emergency sessions over untrusted WLAN	13.4.0	13.5.0
2016-03	CT#71	CP-160082	0539		Capitalisation of field names and miscellaneous corrections	13.4.0	13.5.0
2016-03	CT#71	CP-160079	0540	3	IKEv2 extension for P-CSCF reselection support	13.4.0	13.5.0
2016-06	CT#72	CP-160316	0534	6	ePDG selection in support of Lawful Interception	13.5.0	13.6.0
2016-06	CT#72	CP-160316	0541		Editor's notes on registration of TIMEOUT_PERIOD_FOR_LIVENESS_CHECK with IANA	13.5.0	13.6.0
2016-06	CT#72	CP-160313	0542		Usage and definition of REACTIVATION_REQUESTED_CAUSE	13.5.0	13.6.0
2016-06	CT#72	CP-160308	0543	1	Correction of the name for the private Notify payloads	13.5.0	13.6.0
2016-06	CT#72	CP-160317	0544	2	Emergency ePDG identifier configuration	13.5.0	13.6.0
2016-06	CT#72	CP-160316	0546	1	ANDSF configuration for coexistence between WLANSP rules and LWA, RCLWI and LWIP	13.5.0	13.6.0
2016-06	CT#72	CP-160316	0550	2	ANDSF/UICC configuration precedence	13.5.0	13.6.0
2016-06	CT#72	CP-160316	0551	1	Clarification on ePDG configuration information	13.5.0	13.6.0
2016-06	CT#72	CP-160325	0552	1	Local release of NBIFOM PDN connection for untrusted WLAN	13.5.0	13.6.0
2016-06	CT#72	CP-160344	0549	1	Clarification on the use of the IKEv2 Error PLMN_NOT_ALLOWED	13.6.0	14.0.0

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2016-09	CT#73	CP-160516	0553	2	F	Reservation of a private notify message error type value range and a private notify message status type value range for usage out of scope of 3GPP	14.1.0
2016-09	CT#73	CP-160513	0554	1	B	Add a cause value to indicate the rejection of an illegal UE for trusted WLAN access	14.1.0
2016-09	CT#73	CP-160513	0555	2	B	Add a cause value to indicate the rejection of an illegal UE for untrusted WLAN access	14.1.0
2016-09	CT#73	CP-160507	0557	1	A	Remove EN on backoff timer	14.1.0
2016-09	CT#73	CP-160509	0559		A	Remove the editor's note on emergency service over WLAN	14.1.0
2016-09	CT#73	CP-160517	0560	2	B	ePDG selection for emergency services over WLAN	14.1.0
2016-09	CT#73	CP-160517	0561	3	B	Emergency session establishment for untrusted access	14.1.0
2016-09	CT#73	CP-160507	0564	1	A	Corrections to ePDG selection	14.1.0
2016-09	CT#73	CP-160517	0566	3	B	User Identification for emergency services over WLAN	14.1.0
2016-09	CT#73	CP-160517	0567	2	B	Support of Emergency session establishment for unauthenticated UEs	14.1.0
2016-09	CT#73	CP-160510	0569	1	F	Release-specific reference to 24.234	14.1.0
2016-09	CT#73	CP-160507	0571	1	A	Remove editor's note for the case when LWA co-existence info is not provisioned	14.1.0
2016-12	CT#74	CP-160798	0572	1	B	ePDG emergency service support indication to the UE	14.2.0
2016-12	CT#74	CP-160798	0573	4	B	New emergency PDN connection in TWAN and handover of emergency PDN connection from 3GPP access to TWAN	14.2.0
2016-12	CT#74	CP-160798	0574	2	B	Handover of emergency PDN connection from 3GPP access to untrusted non-3GPP access	14.2.0
2016-12	CT#74	CP-160735	0576	1	A	NBIFOM and WLAN access selection and traffic routing controlled by RAN rules	14.2.0
2016-12	CT#74	CP-160735	0579	1	A	Alignment to RAN-controlled LTE-WLAN interworking and RAN-assisted WLAN interworking	14.2.0
2016-12	CT#74	CP-160798	0580	2	B	Determining same country location for UE and the connected ePDG	14.2.0
2016-12	CT#74	CP-160798	0581	1	F	Correction to "IMSI is unauthenticated"	14.2.0
2016-12	CT#74	CP-160749	0583	2	F	NO_APN_SUBSCRIPTION backoff handling for untrusted access	14.2.0
2016-12	CT#74	CP-160749	0585	2	F	NO_APN_SUBSCRIPTION backoff handling for SCM	14.2.0
2016-12	CT#74	CP-160798	0587	1	B	IMEI not accepted cause for rejection of ES request via untrusted WLAN	14.2.0
2016-12	CT#74	CP-160798	0588	8	B	IMSI as identification for emergency services over WLAN	14.2.0
2016-12	CT#74	CP-160798	0589	1	B	NAI as user identity in the IDi payload of IKE_AUTH message	14.2.0
2016-12	CT#74	CP-160749	0591	2	F	Clarification on ePDG selection procedure	14.2.0
2016-12	CT#74	CP-160740	0592	1	B	Add optional ERP support to UE	14.2.0
2016-12	CT#74	CP-160798	0594	1	B	Request IMEI from UE with unauthenticated IMSI via untrusted WLAN	14.2.0
2016-12	CT#74	CP-160798	0595	3	B	Emergency session for UICC-less and unauthenticated UEs over untrusted access	14.2.0
2016-12	CT#74	CP-160798	0596	2	B	Support of Emergency session establishment over trusted access	14.2.0
2017-03	CT#75	CP-170134	0600		D	Correcting typo errors and "informal" text	14.3.0
2017-03	CT#75	CP-170134	0602	3	B	UE attached for emergency over untrusted WLAN	14.3.0
2017-03	CT#75	CP-170134	0603	1	F	Redundant description on handling of unauthenticated UE for emergency over untrusted WLAN	14.3.0
2017-03	CT#75	CP-170134	0605	1	F	Format of emergency NAI reference	14.3.0
2017-03	CT#75	CP-170124	0607	2	B	UE rekey procedure for WLAN	14.3.0
2017-03	CT#75	CP-170134	0609	1	B	Correction to the definition of emergency session	14.3.0

2017-03	CT#75	CP-170134	0610	1	B	Authentication exception during emergency session over trusted WLAN	14.3.0
2017-03	CT#75	CP-170134	0597	9	B	Identity management for emergency session over trusted WLAN	14.3.0
2017-03	CT#75	CP-170134	0601	4	B	AAA Server support of Emergency session establishment over trusted access	14.3.0
2017-03	CT#75	CP-170134	0611	3	B	Connection mode negotiation for emergency session over trusted WLAN	14.3.0
2017-06	CT#76	CP-171088	0599	5	F	Introduction of WLAN and ANQP	14.4.0
2017-06	CT#76	CP-171089	0608	8	B	Managing local emergency number over the non-3GPP access	14.4.0
2017-06	CT#76	CP-171089	0612	5	B	Handling of emergency call numbers for emergency session over WLAN access	14.4.0
2017-06	CT#76	CP-171089	0613		B	User identification for emergency session over WLAN access	14.4.0
2017-06	CT#76	CP-171089	0614	1	B	EAP-3GPP-LimitedService method coding	14.4.0
2017-06	CT#76	CP-171089	0618	1	B	Emergency call numbers via IKEv2	14.4.0
2017-06	CT#76	CP-171089	0619	1	F	IKEv2 private error type to indicate unauthenticated emergency service	14.4.0
2017-06	CT#76	CP-171089	0621	1	B	ePDG handling of unauthenticated emergency session	14.4.0
2017-06	CT#76	CP-171088	0623	1	F	Correction on PDN-GW selection during initial attach	14.4.0
2017-09	CT#77	CP-172111	0629	2	F	Remove double negation	14.5.0
2017-09	CT#77	CP-172099	0631	1	F	Only ERP Implicit Bootstrapping mode is supported in Rel-14	14.5.0
2017-09	CT#77	CP-172111	0633	3	F	Emergency call detection when the UE is connected only to non-3GPP access	14.5.0
2017-09	CT#77	CP-172111	0635	3	F	Minimum and maximum size for EMERGENCY_CALL_NUMBERS Notify payload	14.5.0
2017-12	CT#78	CP-173057	0637	3	F	Handling of emergency numbers received over non-3GPP access	14.6.0
2017-12	CT#78	CP-173057	0639	1	F	Resolve EN "It is FFS if the UE can still use these numbers when connected only to non-3GPP access"	14.6.0
2017-12	CT#78	CP-173057	0642	3	F	Correct MCC information usage and storage of Local Emergency Numbers List in Annex J	14.6.0
2017-12	CT#78	CP-173049	0651		A	Missing 't' in "epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnework.org"	14.6.0
2017-12	CT#78	CP-173057	0653		F	Correct mapping Emergency Call Number Unit field contents to Emergency Service Category Value	14.6.0
2017-12	CT#78	CP-173055	0655	1	F	Emergency ePDG selection for UE without UICC	14.6.0
2018-03	CT#79	CP-180063	0658		F	Corrections of errors in emergency PDU session establishment by UE without valid UICC using SCM in TWAN	14.7.0
2018-06	CT#80	CP-181051	0660	2	F	Emergency session establishment when the UE is connected to an ePDG	14.8.0
2018-12	CT#82	CP-183075	0674	1	D	No UE configuration parameters for connectivity to ePDG by UICC	14.9.0
2018-12	CT#82	CP-183072	0680		A	Resolving Editor's Notes: version of 3GPP2 X.S0057, 3GPP2 C.S0087	14.9.0
2018-12	CT#82	CP-183068	0686		A	Correct reference	14.9.0
2018-12	CT#82	CP-183069	0689	1	A	Clarify decorated NAI usage	14.9.0
2018-12	CT#82	CP-183073	0694	1	A	Resolving Editor's Note on application ID for ANDSF GBA Push	14.9.0
2018-12	CT#82	CP-183069	0698	1	A	Missing references to RFC 7296 and 4306	14.9.0

History

Document history		
V14.3.0	March 2017	Publication
V14.4.0	July 2017	Publication
V14.5.0	October 2017	Publication
V14.6.0	January 2018	Publication
V14.7.0	June 2018	Publication
V14.8.0	June 2018	Publication
V14.9.0	January 2019	Publication