ETSI TS 124 502 V16.5.0 (2020-10)

5G;
Access to the 3GPP 5G Core Network (5GCN)
via non-3GPP access networks
(3GPP TS 24.502 version 16.5.0 Release 16)

Reference
RTS/TSGC-0124502vg50

Keywords
5G

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.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 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

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 7
1 Scope 8
2 References 8
3 Definitions, symbols and abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 11
4 General 12
4.1 Overview 12
4.2 Untrusted access 12
4.3 Identities 12
4.3.1 User identities 12
4.3.2 FQDN for N3IWF Selection 12
4.4 Quality of service support 13
4.4.1 General 13
4.4.2 QoS differentiation in non-3GPP access 13
4.4.2.1 General 13
4.4.2.2 QoS signalling 13
4.4.2.3 QoS differentiation in user plane 13
4.4.2.4 Reflective QoS 14
4.4.2.5 QoS enforcement 14
4.5 Trusted access 14
4.6 Forbidden PLMNs for non-3GPP access to 5GCN 14
5 Network discovery and selection 15
5.1 General 15
5.2 Access network discovery procedure 15
5.2.1 General 15
5.2.2 Discovering availability of WLAN access networks 15
5.3 Access network selection procedure 16
5.3.1 General 16
5.3.2 WLAN selection procedure 16
5.3.2.1 General 16
5.3.2.2 Manual mode WLAN selection 16
5.3.2.3 Automatic mode WLAN selection 16
5.3A PLMN selection procedures using trusted non-3GPP access 18
5.3A.1 General 18
5.3A.2 PLMN solicitation 18
5.3A.3 Manual PLMN selection mode procedure 19
5.3A.4 Automatic mode PLMN selection procedure 19
5.3A.4.1 General 19
5.3A.4.2 Attempting to select HPLMN or equivalent HPLMN 20
5.3A.4.3 NAI construction 20
5.3B PLMN selection procedures using wireline access 20
5.4 Access network reselection procedure 21
5.4.1 General 21
5.4.2 WLAN reselection procedure 21
6 UE - 5GC network protocols 21
6.1 General 21
6.2 Void 21
6.3 Authentication and authorization for accessing 5GS via non-3GPP access network 21

6.3.1 General....21
6.3.2 Authentication of N5GC device behind a CRG over wireline access....22
6.4 Handling of ANDSP Information....22
6.4.1 General....22
6.4.2 UE procedures....23
6.4.2.1 General....23
6.4.2.2 Use of WLAN selection information....23
6.4.2.3 Use of N3AN node configuration information....23
6.4.3 ANDSP information from the network....23
7 Security association management procedures....23
7.1 General....23
7.2 N3AN node selection procedure....24
7.2.1 General....24
7.2.2 N3AN node configuration information....24
7.2.3 Determination of the country the UE is located in....24
7.2.4 N3AN node selection....24
7.2.4.1 General....24
7.2.4.2 Determine if the visited country mandates the selection of N3IWF in this country....25
7.2.4.3 UE procedure when the UE only supports connectivity with N3IWF....25
7.2.4.4 UE procedure when the UE supports connectivity with N3IWF and ePDG....27
7.2.4.4.1 General....27
7.2.4.4.2 N3AN node selection for IMS service....28
7.2.4.4.3 N3AN node selection for Non-IMS service....31
7.2.5 Selection of an N3AN node in an SNPN....34
7.3 IKE SA establishment procedure for untrusted non-3GPP access....34
7.3.1 General....34
7.3.2 IKE SA and signalling IPsec SA establishment procedure....35
7.3.2.1 IKE SA and signalling IPsec SA establishment initiation....35
7.3.2.2 IKE SA and signalling IPsec SA establishment accepted by the network....35
7.3.2.3 IKE SA and signalling IPsec SA establishment not accepted by the network....37
7.3.3 EAP-5G session over non-3GPP access....38
7.3.3.1 General....38
7.3.3.1A EAP-5G session initiation....38
7.3.3.2 EAP-5G session completion initiated by the network....39
7.3.3.3 EAP-5G session completion initiated by the UE....39
7.3.4 Abnormal cases in the UE....40
7.3.5 Abnormal cases in the N3IWF....40
7.3A IKE SA establishment procedure for trusted non-3GPP access....40
7.3A.1 General....40
7.3A.2 EAP session over non-3GPP access....42
7.3A.2.1 General....42
7.3A.2.2 Identity transaction....42
7.3A.2.3 EAP-5G session initiation....42
7.3A.2.4 EAP-5G session completion initiated by the network....43
7.3A.2.5 EAP-5G session completion initiated by the UE....43
7.3A.3 IKE SA and signalling IPsec SA establishment procedure....43
7.3A.3.1 IKE SA and signalling IPsec SA establishment initiation....43
7.3A.3.2 IKE SA and signalling IPsec SA establishment accepted by the network....43
7.3A.3.3 IKE SA and signalling IPsec SA establishment not accepted by the network....43
7.3A.4 Procedure for devices without NAS support....43
7.3A.4.1 General....43
7.3A.4.2 N5CW device registration over trusted WLAN access network....44
7.4 IKEv2 SA deletion procedure....44
7.4.1 General....44
7.4.2 IKE SA deletion procedure initiated by the N3IWF and the TNGF....45
7.4.2.1 IKE SA deletion initiation....45
7.4.2.2 IKE SA deletion accepted by the UE....45
7.4.2.3 Abnormal cases in the N3IWF and the TNGF....45
7.4.3 IKE SA deletion procedure initiated by the UE....46
7.4.3.1 IKE SA deletion initiation....46
7.4.3.2 IKE SA deletion accepted by the N3IWF and the TNGF....46

7.4.3.3 Abnormal cases in the UE 46
7.5 User plane IPsec SA creation procedure 46
7.5.1 General 46
7.5.2 Child SA creation procedure initiation 47
7.5.3 Child SA creation procedure accepted by the UE 47
7.5.4 Child SA creation procedure not accepted by the UE 47
7.5.5 Abnormal cases in the UE 48
7.5.6 Abnormal cases in the N3IWF and the TNGF 48
7.6 IPsec SA modification procedure 48
7.6.1 General 48
7.6.2 N3IWF and TNGF procedure for IPsec child SA modification 48
7.6.3 UE procedure for IPsec child SA modification 48
7.7 IPSec SA deletion procedure 49
7.7.1 General 49
7.7.2 N3IWF-initated and TNGF-initiated child SA deletion procedure 49
7.7.2.1 N3IWF-initiated and TNGF-initiated child SA deletion procedure initiation 49
7.7.2.2 N3IWF-initiated and TNGF-initiated child SA deletion procedure accepted by the UE 49
7.7.2.3 Abnormal cases in the N3IWF and the TNGF 49
7.7.3 UE-initiated child SA deletion procedure 50
7.7.3.1 UE-initiated child SA deletion procedure initiation 50
7.7.3.2 UE-initiated child SA deletion procedure accepted by the N3IWF and the TNGF 50
7.7.3.3 Abnormal cases in the UE 50
7.7.4 Abnormal cases in the UE 50
7.7.5 Abnormal cases in the N3IWF and the TNGF 50
7.8 UE-initiated liveness check procedure 50
7.8.1 General 50
7.8.2 UE-initiated liveness check procedure initiation 50
7.8.3 UE-initiated liveness check procedure completion 51
7.8.4 Abnormal cases 51
7.9 Network-initiated liveness check procedure 51
7.9.1 General 51
7.9.2 Network-initiated liveness check procedure initiation 51
7.9.3 Network-initiated liveness check procedure completion 51
7.9.4 Abnormal cases 51
7.10 IKE SA rekeying procedure 52
7.10.1 General 52
7.10.2 N3IWF-initiated and TNGF-initiated IKE SA rekeying procedure 52
7.10.2.1 N3IWF-initiated and TNGF-initiated IKE SA rekeying procedure initiation 52
7.10.2.2 N3IWF-initiated and TNGF-initiated IKE SA rekeying procedure completion 52
7.10.2.3 Abnormal cases 52
7.10.3 UE-initiated IKE SA rekeying procedure 52
7.10.3.1 UE-initiated IKE SA rekeying procedure initiation 52
7.10.3.2 UE-initiated IKE SA rekeying procedure completion 53
7.10.3.3 Abnormal cases 53
7.11 IPsec SA rekeying procedure 53
7.11.1 General 53
7.11.2 N3IWF-initiated and TNGF-initiated IPsec SA rekeying procedure 53
7.11.2.1 N3IWF-initiated and TNGF-initiated IPsec SA rekeying procedure initiation 53
7.11.2.2 N3IWF-initiated and TNGF-initiated IPsec SA rekeying procedure completion 53
7.11.2.3 Abnormal cases 54
7.11.3 UE-initiated IPsec SA rekeying procedure 54
7.11.3.1 UE-initiated IPsec SA rekeying procedure initiation 54
7.11.3.2 UE-initiated IPsec SA rekeying procedure completion 54
7.11.3.3 Abnormal cases 54
7A EAP-5G session over wireline access 54
7A.1 General 54
7A.2 EAP-5G session initiation 55
7A.3 EAP-5G session completion initiated by the network 55
7A.4 EAP-5G session completion initiated by the 5G-RG 56
8 Message transport procedures 56

8.1 General 56
8.2 Transport of NAS messages over control plane 57
8.2.1 General 57
8.2.2 TCP packet encapsulation 57
8.2.3 Establishment of TCP connection for transport of NAS messages 59
8.2.3A Re-establishment of TCP connection for transport of NAS messages 59
8.2.4 Transport of NAS messages over TCP connection 59
8.2.5 Release of TCP connection for transport of NAS messages 59
8.3 Transport of messages over user plane 60
8.3.1 General 60
8.3.2 Generic routing encapsulation (GRE) 60

9 Parameters and coding 62
9.1 General 62
9.2 3GPP specific coding information 62
9.2.1 GUAMI 62
9.2.2 Establishment cause for non-3GPP access 62
9.2.3 PLMN ID 63
9.2.4 IKEv2 Notify Message Type value 64
9.2.4.1 General 64
9.2.4.2 Private Notify Message - Error Types 64
9.2.4.3 Private Notify Message - Status Types 64
9.2.5 TNGF IPv4 contact info 65
9.2.6 TNGF IPv6 contact info 66
9.2.7 NID 66
9.3 IETF RFC coding information 67
9.3.1 IKEv2 Notify payloads 67
9.3.1.1 5G_QOS_INFO Notify payload 67
9.3.1.2 NAS_IP4_ADDRESS Notify payload 73
9.3.1.3 NAS_IP6_ADDRESS Notify payload 73
9.3.1.4 UP_IP4_ADDRESS Notify payload 74
9.3.1.5 UP_IP6_ADDRESS Notify payload 75
9.3.1.6 NAS_TCP_PORT Notify payload 75
9.3.1.7 N3GPP_BACKOFF_TIMER Notify payload 76
9.3.2 EAP-5G method 76
9.3.2.1 General 76
9.3.2.2 Message format 76
9.3.2.2.1 EAP-Request/5G-Start message 76
9.3.2.2.2 EAP-Response/5G-NAS message 77
9.3.2.2.3 EAP-Request/5G-NAS message 79
9.3.2.2.4 EAP-Request/5G-Stop message 80
9.3.2.2.5 EAP-Request/5G-Notification message 81
9.3.2.2.6 EAP-Response/5G-Notification message 83
9.3.3 GRE encapsulated user data packet 84
9.4 NAS message envelope 85

Annex A (informative): Change history 87

History 91

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 non-3GPP access network discovery and selection procedures, the access authorization procedure used for accessing non-3GPP access networks. These non-3GPP access networks can be trusted non-3GPP access networks, untrusted non-3GPP access networks or wireline access networks.

The present document also specifies the security association management procedures used for establishing IKEv2 and IPsec security associations:

- between the UE and the N3IWF and the procedures for transporting messages between the UE and the N3IWF over the non-3GPP access networks; and
- between the UE and the TNGF and the procedures for transporting messages between the UE and the TNGF over the non-3GPP access networks.

The present document also specifies the EAP-5G procedures used for exchange of NAS messages via trusted non-3GPP access and wireline access network before the UE or the 5G-RG is authenticated and authorized to use the trusted non-3GPP access or the wireline access network.

The present document is applicable to the UE, the 5G-RG, the W-AGF acting on behalf of the FN-RG or the W-AGF acting on behalf of the N5GC device and the network. In this technical specification the network refers to the 3GPP 5GCN and the trusted non-3GPP access, untrusted non-3GPP access, or wireline access network.

NOTE: The present document is not applicable to the FN-RG.

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] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 24.501: "Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[4A] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[5] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[6] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[7] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[8] 3GPP TS 23.003: "Numbering, addressing and identification".

[9] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[10] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses."

[11] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[12] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[13] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[14] IETF RFC 2784: "Generic Routing Encapsulation (GRE)".

[15] IETF RFC 2890: "Key and Sequence Number Extensions to GRE".

[16] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

[17] 3GPP TS 24.526: "User Equipment (UE) policies for 5G System (5GS); Stage 3".

[18] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[19] IEEE Std 802.11-2016: "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".

[20] Wi-Fi Alliance: "Hotspot 2.0 (Release 2) Technical Specification, version 1.0.0", 2014-08-08.

[21] ITU-T Recommendation E.212: "The international identification plan for public networks and subscriptions", 2016-09-23.

[22] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

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

[24] IETF RFC 791: "INTERNET PROTOCOL".

[25] IETF RFC 8200: "Internet Protocol, Version 6 (IPv6) Specification".

[26] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[27] IETF RFC 793: "Transmission Control Protocol".

[28] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[29] 3GPP TS 38.413: "NG Application Protocol (NGAP)".

[30] 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".

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

[32] IETF RFC 1661: "The Point-to-Point Protocol (PPP)".

[33] IETF RFC 1570: "PPP LCP Extensions".

[34] IETF RFC 2410: " The NULL Encryption Algorithm and Its Use With IPsec".

[35] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[36] CableLabs WR-TR-5WWC-ARCH-V02-200430: "5G Wireless Wireline Converged Core Architecture Technical Report".

[37] IETF RFC 7542: "The Network Access Identifier".

[38] 3GPP TS 24.368: "Non-Access Stratum (NAS) configuration Management Object (MO)".

[39] 3GPP TS 29.413: "Application of the NG Application Protocol (NGAP) to non-3GPP access".

[40] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

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].

MTU: Maximum transmission unit (MTU) is the largest PDU size which can be transmitted and received by a network entity in one single IP packet without any need for IP fragmentation.

NWt: NWt is the reference point between the UE and the TNGF for establishing secure tunnel(s) between the UE and the TNGF so that control-plane and user-plane exchanged between the UE and the 5G core network is transferred securely over trusted non-3GPP access.

NWu: NWu is the reference point between the UE and the N3IWF for establishing secure tunnel(s) between the UE and the N3IWF so that control-plane and user-plane exchanged between the UE and the 5G core network is transferred securely over untrusted non-3GPP access.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [2] apply:

5G Access Network
5G Core Network
5G QoS flow
5G QoS identifier
5G System
Network identifier (NID)
PDU Session
Stand-alone Non-Public Network
TNGF

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.003 [8] apply:

Global Line Identifier (GLI)
Global Cable Identifier (GCI)NAI

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.501 [5] apply:

SUPI
SUCI

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.302 [7] apply:

S2a connectivity

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.501 [4] apply:

W-AGF acting on behalf of the N5GC device

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.316 [40] apply:

W-CP EAP connection
W-CP signalling 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].

5GCN	5G Core Network
5GS	5G System
5G-AN	5G Access Network
5QI	5G QoS Identifier
AMF	Access and Mobility Management Function
AN	Access Network
ANDS	Access Network Discovery and Selection
ANDSP	Access Network Discovery and Selection Policy
AUSF	Authentication Server Function
CP	Control Plane
CRG	Cable Residential Gateway
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DNS	Domain Name System
DSCP	Differentiated Services Code Point
ePDG	Evolved Packet Data Gateway
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
H-PCF	A PCF in the HPLMN
IP	Internet Protocol
IPsec	Internet Protocol Security
N3AN	Non-3GPP Access Network
N3IWF	Non-3GPP InterWorking Function
N5CW	Non 5G Capable over WLAN
N5GC	Non-5G Capable
NAI	Network Access Identifier
NAS	Non Access Stratum
NID	Network Identifier
PCF	Policy control Function
PDU	Protocol Data Unit
QFI	QoS Flow Identifier
RQI	Reflective QoS Indicator
SA	Security Association
SNPN	Stand-alone Non-Public Network
SPI	Security Parameters Index
SUPI	Subscription Permanent Identifier
SUCI	Subscription Concealed Identifier
TCP	Transmission Control Protocol
TNAN	Trusted Non-3GPP Access Network
TNAP	Trusted Non-3GPP Access Point
TNGF	Trusted Non-3GPP Gateway Function
TWAN	Trusted WLAN Access Network
TWAP	Trusted WLAN Access Point
TWIF	Trusted WLAN Interworking Function
UL	Uplink
UP	User Plane
UPF	User Plane Function
V-PCF	A PCF in the VPLMN
WLAN	Wireless Local Area Network
WLANSP	WLAN Selection Policy

4 General

4.1 Overview

The 5G core network (5GCN) supports the connectivity of the UE via non-3GPP access networks. These non-3GPP access networks can be trusted non-3GPP access networks, untrusted non-3GPP access networks or wireline access networks. A trusted or untrusted non-3GPP access network can advertise the PLMNs for which it supports trusted connectivity and the type of supported trusted connectivity (i.e. information about PLMN list with 5G connectivity using trusted non-3GPP access) so that the UE can discover the non-3GPP access networks that can provide trusted connectivity to one or more PLMNs.

NOTE: A wireline access network does not indicate PLMNs for which it supports connectivity.

4.2 Untrusted access

For an untrusted non-3GPP access network, the communication between the UE and the 5GCN is not trusted to be secure.

For an untrusted non-3GPP access network, to secure communication between the UE and the 5GCN, a UE establishes secure connection to the 5G core network over untrusted non-3GPP access via the N3IWF. The UE performs registration to the 5G core network during the IKEv2 SA establishment procedure as specified in 3GPP TS 24.501 [4] and IETF RFC 7296 [6]. After the registration, the UE supports NAS signalling with 5GCN using the N1 reference point as specified in 3GPP TS 24.501 [4]. The N3IWF interfaces the 5GCN CP function via the N2 interface to the AMF and the 5GCN UP functions via N3 interface to the UPF as described in 3GPP TS 23.501 [2].

4.3 Identities

4.3.1 User identities

When the UE accesses the 5GCN over non-3GPP access networks, the same permanent identities for 3GPP access are used to identify the subscriber for non-3GPP access authentication, authorization and accounting services.

The Subscription Permanent Identifier (SUPI) is defined in 3GPP TS 33.501 [5]. The SUPI can contain an IMSI, a network specific identifier, a GCI or a GLI as specified in 3GPP TS 23.501 [2]. A SUPI containing an IMSI is defined in 3GPP TS 23.003 [8]. A SUPI containing a network specific identifier, a GCI or a GLI always takes the form of a NAI as defined in 3GPP TS 23.003 [8].

The Subscription Concealed Identifier (SUCI) is a privacy preserving identifier containing the concealed SUPI as specified in 3GPP TS 33.501 [5]. SUCI is calculated from SUPI. When the SUPI contains an IMSI, the corresponding SUCI is derived as specified in 3GPP TS 23.003 [8]. When the SUPI contains a network specific identifier, a GCI or a GLI, the corresponding SUCI in NAI format is derived as specified in 3GPP TS 23.003 [8].

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

4.3.2 FQDN for N3IWF Selection

An N3IWF FQDN is either provisioned by the home operator or constructed by the UE in either the Operator Identifier FQDN format or the Tracking Area Identity FQDN format as specified in 3GPP TS 23.003 [8].

The N3IWF FQDN is used as input to the DNS mechanism for N3IWF selection.

In order to access PLMN services via an SNPN, a UE operating in SNPN access mode registered to an SNPN has the following restrictions on N3IWF FQDN:

a) the UE shall only use TAIs from a PLMN to construct a Tracking Area Identity based N3IWF FQDN; and

b) the UE shall not consider an N3IWF FQDN for N3IWF selection configured by an SNPN.

4.4 Quality of service support

4.4.1 General

When the UE accesses the 3GPP 5G System (5GS) via non-3GPP access networks, the same QoS flow based 5G QoS model and principles are followed as described in 3GPP TS 23.501 [2]. For PDU sessions that were established over non-3GPP access, the QoS flow remains to be the finest granularity of QoS differentiation in the PDU Session.

4.4.2 QoS differentiation in non-3GPP access

4.4.2.1 General

For untrusted non-3GPP access, the N3IWF is the access network node that provides QoS signalling to support QoS differentiation and mapping of QoS flows to non-3GPP access resources.

For trusted non-3GPP access, the TNGF is the access network node that provides QoS signalling to support QoS differentiation and mapping of QoS flows to non-3GPP access resources.

For wireline access, the W-AGF serving the 5G-RG is the access network node that provides QoS signalling to support QoS differentiation and mapping of QoS flows to non-3GPP access resources.

4.4.2.2 QoS signalling

A QoS flow is controlled by the SMF and can be preconfigured, or established via the UE requested PDU Session establishment via non-3GPP access procedure, the UE or network requested PDU session modification via non-3GPP access procedure (see 3GPP TS 23.502 [3]) .

During PDU session establishment, based on local policies, pre-configuration and the QoS profiles received:

a) the N3IWF or the TNGF (depending on whether the UE is connected to untrusted non-3GPP access or trusted non-3GPP access, respectively):

   1) shall determine the number of IPsec child SAs to establish and the QoS profiles associated with each IPsec child SA; and

   2) shall then initiate IPsec SA creation procedure to establish child SAs associating to the QoS flows of the PDU session; or

b) the W-AGF serving the 5G-RG:

   1) shall determine the number of W-UP resources to establish and the QoS profiles associated with each W-UP resource; and

   2) shall initiate creation of one or more W-UP resources using means out of scope of the present document. The W-AGF serving the 5G-RG shall associate each W-UP resource with a PDU session, zero or more QFIs, and optionally an indication of whether the W-UP resource is the default W-UP resource. For each W-UP resource, the 5G-RG becomes aware using means out of scope of the present document about association of the W-UP resource and the PDU session, the zero or more QFIs, and optionally the indication of whether the W-UP resource is the default W-UP resource.

In order to support QoS differentiation in case of access to PLMN services via an SNPN and access to SNPN services via a PLMN, the N3IWF is preconfigured with one or more QoS profiles requiring a dedicated IPsec child SA which can be associated with a DSCP value.

4.4.2.3 QoS differentiation in user plane

For uplink of trusted and untrusted non-3GPP accesses, the UE associates an uplink user data packet with a QFI as specified in 3GPP TS 24.501 [4]. In both cases of untrusted non-3GPP access and trusted non-3GPP access, the UE shall then encapsulate the uplink user data packet and the QFI associated with the uplink user data packet in the GRE header and select IPsec child SA based on PDU session and QFI associated with the uplink user data packet as specified in subclause 8.3. In case of trusted non-3GPP access, the UE shall reserve non-3GPP access network QoS resources for

the IPsec child SA according to the received Additional QoS Information when the selected IPsec child SA is established. In case of untrusted non-3GPP access, the UE may receive an Additional QoS Information from the N3IWF during IPsec child SA establishment. If the UE receives the Additional QoS Information from the N3IWF, the UE may reserve non-3GPP access network QoS resources for the IPsec child SA according to the received Additional QoS Information when the selected IPsec child SA is established.

For uplink of wireline access, the 5G-RG associates an uplink user data packet with a QFI as specified in 3GPP TS 24.501 [4], shall select a W-UP resource based on the PDU session and the QFI associated with the uplink user data as specified in subclause 8.3 and shall transport the uplink user data packet via the selected W-UP resource using means out of scope of the present specification.

For downlink of trusted and untrusted non-3GPP accesses, the UPF maps the user data packet to a QoS flow. In case of untrusted non-3GPP access, the N3IWF shall determine the IPsec child SA to use for sending of the downlink user data packet over NWu based on mapping of the QoS flow to the IPsec child SA based on QFI of the QoS flow of the user data packet and the identity of the PDU session of the user data packet. In case of trusted non-3GPP access, the TNGF shall determine the IPsec child SA to use for sending of the downlink user data packet over NWt based on mapping of the QoS flow to the IPsec child SA based on QFI of the QoS flow of the user data packet and the identity of the PDU session of the user data packet. Futhermore, TNGF may reserve non-3GPP access network QoS resources for the IPsec child SA.

For downlink of wireline access, the UPF maps the user data packet to a QoS flow. In case of wireline access, the W-AGF serving the 5G-RG shall select a W-UP resource for a downlink user data packet based on mapping of the QoS flow to the W-UP resources, based on QFI of the QoS flow of the user data packet and the identity of the PDU session of the user data packet, and shall transport the downlink user data packet and the QFI associated with the downlink user data packet via the selected W-UP resource using means out of scope of the present specification.

4.4.2.4 Reflective QoS

Reflective QoS is also supported when the UE accesses the 5GCN via non-3GPP access network as specified in 3GPP TS 23.502 [3]. If the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access receives a downlink user packet associated with Reflective QoS Indicator (RQI), the N3IWF or the TNGF shall set the RQI in the GRE header when encapsulating the downlink user data packet into a GRE encapsulated user data packet as specified in subclause 8.3. If the W-AGF serving the 5G-RG receives a downlink user packet associated with Reflective QoS Indicator (RQI), the W-AGF shall transport the RQI together with the downlink user data packet and the QFI associated with the downlink user data packet via the selected W-UP resource over NWu, as described in subclause 4.4.2.3.

4.4.2.5 QoS enforcement

If the UE is provided with maximum flow bit rate (MFBR) for UL for a QFI as specified in 3GPP TS 24.501 [4], the UE should send user data packets associated with the QFI with a bitrate lower than or equal to the maximum flow bit rate (MFBR) for UL.

4.5 Trusted access

For a trusted non-3GPP access network, the communication between the UE and the 5GCN is secure. A trusted non-3GPP access network is connected to the 5GCN via a trusted non-3GPP gateway function (TNGF) as specified in 3GPP 23.501 [2]. The TNGF interfaces the 5GCN CP function via the N2 interface to the AMF and the 5GCN UP functions via N3 interface to the UPF as described in 3GPP TS 23.501 [2].

For a trusted non-3GPP access network, the UE establishes secure connection to the 5GCN over trusted non-3GPP access to the TNGF. The UE uses 3GPP-based authentication for connecting to a non-3GPP access and establishes an IPsec Security Association (SA) with the the TNGF in order to register to the 5GCN by using the registration procedure as specified in 3GPP TS 24.501 [4]. After the registration, the UE supports NAS signalling with the 5GCN using the N1 reference point as specified in 3GPP TS 24.501 [4].

4.6 Forbidden PLMNs for non-3GPP access to 5GCN

A list of "forbidden PLMNs for non-3GPP access to 5GCN" contains a list of VPLMNs, 5GCN of which the UE is forbidden to access via non-3GPP access.

The HPLMN (if the equivalent HPLMN list is not present or is empty) or an equivalent HPLMN (if equivalent HPLMN list is present) shall not be stored on the list of "forbidden PLMNs for non-3GPP access".

3GPP TS 24.501 [4] specifies when a VPLMN is added to the list of "forbidden PLMNs for non-3GPP access to 5GCN".

When the UE is configured to use timer T3245 (see 3GPP TS 24.368 [38] or 3GPP TS 31.102 [35]), the UE adds a PLMN identity to the list of "forbidden PLMNs for non-3GPP access to 5GCN" and timer T3245 (see 3GPP TS 24.008 [28]) is not running, then the UE shall start timer T3245 as specified in 3GPP TS 24.008 [28], subclause 4.1.1.6.

The list of "forbidden PLMNs for non-3GPP access to 5GCN" is deleted when the MS is switched off or the UICC containing the USIM is removed.

A VPLMN is removed from the list of "forbidden PLMNs for non-3GPP access to 5GCN" if:

- there is a successful registration as specified in 3GPP TS 24.501 [4] over a non-3GPP access after a manual selection of the VPLMN for non-3GPP access connected to 5GCN;
- the value of the PLMN-specific attempt counter for non-3GPP access for the PLMN has a value greater than zero and less than the UE implementation-specific maximum value as defined in subclause 5.3.20 in 3GPP TS 24.501 [4] and T3247 expires; or
- upon expiry of the timer T3245 if the UE is configured to use timer T3245.

5 Network discovery and selection

5.1 General

The following aspects are included when selecting a 5GC network and routing traffic via the 5GC network:

a) access network discovery procedures as defined in subclause 5.2;

b) access network selection procedures as defined in subclause 5.3; and

c) access network reselection procedures as defined in subclause 5.4.

5.2 Access network discovery procedure

5.2.1 General

If PLMN selection specified in 3GPP TS 23.122 [13] 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.

In the access network discovery procedure, the UE can get ANDSP information on available access networks in its vicinity and can 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.

NOTE: The procedure for the automatic mode WLAN selection by using ANDSP rules as defined in subclause 5.3.2.3 does not apply to an N5CW device that is not registered or cannot register via NG-RAN.

5.2.2 Discovering availability of WLAN access networks

The UE may obtain WLAN Selection Policy (WLANSP) rules information by pre-configuration or by downloading the policy information from the PCF as specified in 3GPP TS 23.503 [16]. The policy contains the UE access network

discovery and selection related policy information to help the UE in discovering and selecting a WLAN access network (see 3GPP TS 24.526 [17]).

The UE may receive multiple valid WLANSP rules. When the UE is in the home PLMN, the UE uses the valid WLANSP rules from the home PLMN to select an available WLAN. When the UE is roaming and the UE has valid rules from several of the home PLMN, a visited PLMN and a PLMN equivalent to the visited PLMN, the UE uses the WLANSP rules in the following order of decreasing priority:

a) the valid WLANSP rules from the visited PLMN;

b) the valid WLANSP rules from the equivalent PLMN in which the UE last received WLANSP; and

c) the valid WLANSP rules from the home PLMN.

A WLANSP rule is valid if it meets the validity conditions included in the WLANSP rule (if provided).

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

In addition, the UE may obtain information on operator preferred WLAN access networks via ANDSP.

5.3 Access network selection procedure

5.3.1 General

In this release of the specification, only selection of WLAN access network is supported. The ANDSP policy contains WLANSP rules for the UE to select a WLAN access network. Rules for selecting other types of non-3GPP access networks are not specified.

5.3.2 WLAN selection procedure

5.3.2.1 General

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

The UE shall perform WLAN selection based on the user preferences and WLANSP rules. The UE may be provisioned with WLANSP rules from multiple PLMNs. User preferences take precedence over the WLANSP rules.

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

a) if user preferences are present, the UE shall determine the prioritized list of selected WLAN(s) using the manual mode WLAN selection procedure (see subclause 5.3.2.2); or

b) if user preferences are not present or if there is no user-preferred WLAN access network available, the UE shall determine the prioritized list of selected WLAN(s) using the automatic mode WLAN selection procedure (see subclause 5.3.2.3).

5.3.2.2 Manual mode WLAN selection

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

5.3.2.3 Automatic mode WLAN selection

The UE shall first determine valid WLANSP rules for WLAN selection:

a) if the UE is not roaming over 3GPP access, the UE shall use the valid WLANSP rules from the HPLMN; or

b) if the UE is roaming over 3GPP access, the UE may have valid WLANSP rules from several of the visited PLMN, a PLMN equivalent to the visited PLMN and the home PLMN. The UE uses the WLANSP rules in the following order of decreasing priority:

1) the valid WLANSP rules from the visited PLMN;

2) the valid WLANSP rules from the equivalent PLMN in which the UE last received WLANSP; and

3) the valid WLANSP rules from the home PLMN.

The UE shall then determine the selected WLAN(s) according to the following steps:

a) use the procedures specified in the IEEE 802.11 [19] to discover the available WLANs. The UE may perform ANQP procedures as specified in the IEEE 802.11 [19] or the Hotspot 2.0 [20] to discover the attributes and capabilities of available WLANs. If the UE supports ANQP procedures, the UE may send an ANQP request for lists of service providers (i.e. ANQP-elements "Domain Name", see IEEE 802.11 [19]) and PLMN identities (i.e. ANQP-element "3GPP Cellular Network", see 3GPP TS 24.302 [7] annex H); and

b) if the UE has performed ANQP procedures to discover the attributes and capabilities of available WLANs, compare the attributes and capabilities of the available WLANs with the group of selection criteria of the valid WLANSP rules and construct a prioritized list of available WLANs that fulfill the selection criteria.

1) when there are multiple valid WLANSP rules the UE evaluates the valid WLANSP rules in priority order. The UE evaluates first if an available WLAN access meets the selection criteria of the highest priority valid WLANSP rule. The UE then evaluates if an available WLAN access meets the selection criteria of the next priority valid WLANSP rule;

NOTE 1: Each WLANSP rule can include one or more groups of selection criteria in priority order. If there are multiple highest priority groups of selection criteria in the valid WLANSP rule, it is up to the UE implementation which one to use.

2) if the Home network ind bit is not set to "1" in the group of selection criteria (see 3GPP TS 24.526 [17]), the WLAN(s) that match the group of selection criteria with the highest priority are considered as the most preferred WLANs, the WLAN(s) that match the group of selection criteria with the second highest priority are considered as the second most preferred WLANs;

3) if the Home network ind bit is set to "1" in the group of selection criteria (see 3GPP TS 24.526 [17]), then the UE shall create a list of available WLANs and shall apply the group of selection criteria to all the WLANs in this list. A WLAN is included in this list, if

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

ii) the UE received a lists of service providers (i.e. ANQP-elements "Domain Name") and PLMN identities (i.e. ANQP-element "3GPP Cellular Network"), and:

I) if the list with PLMNs that can be selected from the WLAN (see 3GPP TS 24.302 [7]) includes:

A) the HPLMN derived from its IMSI; or

B) a PLMN matching an entry in the UE's list of equivalent PLMNs; or

II) if the domain name list (see IEEE 802.11 [19]) includes:

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

B) the domain name derived from its list of equivalent PLMNs; and

NOTE 2: If the Home network ind bit is set to "1" in a group of selection criteria then this group of selection criteria is not expected to include the preferred roaming partner list and the preferred SSID list.

NOTE 3: WLAN advertises PLMN(s) towards which the S2a connectivity or the 5G connectivity using trusted non-3GPP access is supported by using the ANQP-element "3GPP Cellular Network" with the PLMN List with S2a Connectivity IE, the PLMN List with trusted 5G connectivity IE or the PLMN List with trusted 5G connectivity-without-NAS IE in the payload (see 3GPP TS 24.302 [7] Annex H). The PLMN List with trusted 5G connectivity-without-NAS IE is only used by N5CW devices.

Editor's note: It is FFS which sort of trusted non-3GPP access is preferred for the case when both "S2a connectivity" and "trusted 5G connectivity" are indicated.

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

5.3A PLMN selection procedures using trusted non-3GPP access

5.3A.1 General

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

The UE follows one of the following two procedures defined in subclause 5.3.2.2 and subclause 5.3.2.3 depending on its implementation. The N5CW device that is not registered or cannot register via NG-RAN performs manual mode WLAN selection procedure as defined in subclause 5.3.2.2.

The PLMN selected in accordance with these procedures determines the WLAN that is selected. When the selected WLAN is a trusted non-3GPP IP access and the UE decides to access 5GC via trusted non-3GPP IP access, the UE shall derive a NAI from the identity of the selected PLMN and use the NAI as the identity for authentication and authorization with the PLMN and usage of the WLAN.

The procedures described in this subclause 5.3A shall apply to the UE and the N5CW device.

5.3A.2 PLMN solicitation

The UE shall determine which PLMNs are available from each WLAN on the list of available WLANs constructed using the WLAN selection procedure described in subclause 5.3.2 using the following procedures:

i) the UE selects a WLAN from the list of selected WLAN(s) constructed using the WLAN selection procedure described in subclause 5.3.2;

NOTE 1: An N5CW device that is not registered or cannot register via NG-RAN uses only the manual mode WLAN selection procedure described in subclause 5.3.2.

ii) if both the WLAN selected in step i) and the UE support ANQP specified in IEEE Std 802.11 [19] and if the UE did not obtain a list of realms using ANQP in subclause 5.3.2.3 item 1, the UE shall send 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 2: The UE uses procedures defined in IEEE Std 802.11 [19] to determine if the WLAN supports ANQP and to send the ANQP request for ANQP-elements "NAI Realm" and/or "3GPP Cellular Network", as specified in IEEE Std 802.11 [19].

iii) if either the WLAN selected in step i) or the UE does not support ANQP (see IEEE Std 802.11 [19]) or the UE does not receive a list of realms in item ii), an EAP-Request/Identity is received and the EAP-Request/Identity does not include one or more of realms and/or PLMN identities (encoded in accordance with IETF RFC 4284 [31]), the UE supports IEEE 802.1x authentication (see IEEE Std 802.1X™ [30]), the UE shall request a list of realms and/or PLMN identities interworking with that WLAN by sending the EAP-Response/Identity message including as identity the alternative NAI; and

iv) the UE repeats this procedure for all WLANs from the available list of WLANs as constructed using the WLAN selection procedure described in subclause 5.3.2.

NOTE 3: The list with realms and/or PLMN identities received in accordance with procedures in IETF RFC 4284 [31], is of limited size and might not contain all the realms and/or PLMN identities available via the WLAN.

The UE shall convert any received PLMN identities into realms of the PLMNs using the rules defined in clause 19 and clause 28 of 3GPP TS 23.003 [8]. The N5CW device shall convert any received PLMN identities into realms of the PLMNs using the rules defined in clause 28 of 3GPP TS 23.003 [8].

5.3A.3 Manual PLMN selection mode procedure

The UE indicates to the user the PLMNs which are available via the WLAN. The UE may obtain the PLMNs available for WLAN access using procedures as described in subclause 5.3A.2. The UE selects the PLMN based on the user preference.

5.3A.4 Automatic mode PLMN selection procedure

5.3A.4.1 General

The purpose of this procedure is to:

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

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

1) using the PLMNs which are available for WLAN as described in subclause 5.3A.2, the UE uses the realms of the PLMN in the remaining steps of this subclause;
2) if the UE is registered over 3GPP access, the realm of the RPLMN of the 3GPP access is included in the list of realms created in subclause 5.3A.2 and the realm of the RPLMN of the 3GPP access does not match a realm converted from any PLMN ID in the list of "forbidden PLMNs for non-3GPP access to 5GCN", the UE shall select the RPLMN of the 3GPP access;
3) if the UE is registered over 3GPP access, the realm of the RPLMN of the 3GPP access is not included in the list of realms created in subclause 5.3A.2, the PLMN is in the "N3AN node selection information" (see 3GPP TS 24.526 [17]) and the PLMN is not in the list of "forbidden PLMNs for non-3GPP access to 5GCN" then the UE shall select the RPLMN of the 3GPP access and performs N3AN node selection with the RPLMN as defined in subclause 7.2;
4) if the condition in steps 2) and 3) are not satisfied, the UE shall select a PLMN in the following order:
   i) if the UE used the procedures in IETF RFC 4284 [31] (see subclause 5.3A.2) to obtain a list of realms, then the UE is only required to select the realm of the HPLMN (if available);
   ii) if the UE can determine the country it is located in (see subclause 7.2.3) and the UE determines it is located in the home country, the UE follows the procedures in subclause 5.3A.4.2;
   iii) if the UE can determine the country it is located in (see subclause 7.2.3) and the UE determines it is located in a visited country, the UE determines whether it is mandatory to select a PLMN in the visited country.

Editor's note: the procedure for determining whether it is mandatory to select a PLMN in the visited country involves TS 23.003, DNS, cached DNS responses, and is FFS.

If the UE determines that it is not mandatory to select a PLMN in the visited country, the UE shall follow the procedures in subclause 5.3A.4.2;

If the UE determines that it is mandatory to select a PLMN in the visited country, the UE shall select, in priority order, a PLMN from the list of realms created in subclause 5.3A.2, if:

I) the PLMN is in the User Controlled PLMN Selector list (see 3GPP TS 31.102 [35]); or

II) the PLMN is in the Operator Controlled PLMN Selector list (see 3GPP TS 31.102 [35]).

If no match is found in either of the lists, the UE may perform N3AN node selection as defined in subclause 7.2.

The UE shall construct a NAI for authentication with the highest priority PLMN as follows:

Editor's note: the rules for creating the root or decorated NAI for 5GS are yet to be specified in TS 23.003.

1) if the PLMN selected was selected from:

   i) a list of realms obtained using IETF RFC 4284 [31]; or

   ii) a list of PLMNs obtained from the PLMN List IE (see annex H of 3GPP TS 24.302 [7]), and the PLMN was neither present in the PLMN List with S2a Connectivity IE, in the PLMN List with trusted 5G Connectivity IE nor the PLMN List with trusted 5G connectivity-without-NAS IE;

   then the UE constructs a NAI as specified in subclause 5.3A.4.3 and in accordance to the rules of 3GPP TS 23.003 [8];

Editor's note: It is FFS whether the UE uses rules in clause 19 (EPC) or clause 28 (5GS) of TS 23.003 to construct a NAI.

2) if the PLMN selected was selected from a list of PLMNs obtained from the PLMN List with trusted 5G Connectivity IE or the PLMN List with trusted 5G connectivity-without-NAS IE (see annex H of 3GPP TS 24.302 [7]) then the UE constructs a NAI as specified in sucblause 5.3A.4.3 and in accordance to the rules in clause 28 of 3GPP TS 23.003 [8]; or

3) if the PLMN selected was selected from a list of PLMNs obtained from the PLMN List with S2a Connectivity IE (see annex H of 3GPP TS 24.302 [7]) then the UE constructs a NAI as specified in sucblause 5.3A.4.3 and in accordance to the rules in clause 19 of 3GPP TS 23.003 [8] and proceeds processing as defined in 3GPP TS 24.302 [7].

NOTE 1: UE implementations can optimize the steps described above, e.g. by combining the ANQP procedures described in subclause 5.3A.2 with the ANQP procedures in subclause 5.3.2.3.

NOTE 2: Selecting a WLAN from multiple WLANs advertising support for the selected PLMN is UE implementation specific.

NOTE 3: The N5CW device which is not registered or cannot register via NG-RAN only uses the PLMN List with trusted 5G connectivity-without-NAS IE, and the PLMN List with trusted 5G connectivity-without-NAS IE is only used by the N5CW devices.

5.3A.4.2 Attempting to select HPLMN or equivalent HPLMN

If the realm of the HPLMN is included in the list of realms created in subclause 5.3A.2 then the UE shall select the HPLMN.

If the realm of the HPLMN is not included in the list of realms created in subclause 5.3A.2, but a realm of an equivalent HPLMN is included, then the UE shall select the equivalent HPLMN.

If neither realm is included in the list of realms created in subclause 5.3A.2, then the UE aborts its attempt to use trusted non-3GPP IP access.

5.3A.4.3 NAI construction

The UE constructs the following NAI:

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

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

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

5.3B PLMN selection procedures using wireline access

Roaming support for wireline access is not defined in the present version of the present document.

The 5G-RG, the W-AGF acting on behalf of the FN-RG and the W-AGF acting on behalf of the N5GC device shall consider that the HPLMN is available on each wireline access network and shall select HPLMN on the wireline access network.

5.4 Access network reselection procedure

5.4.1 General

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

The access network reselection procedure can also be triggered by the UE during periodical re-evaluation of ANDSP policies (see subclause 6.4.2), or if the 'active' rule becomes invalid (conditions no longer fulfilled), or other manufacturer specific trigger.

NOTE: How frequently the UE performs the discovery and reselection procedure is UE implementation specific.

5.4.2 WLAN reselection procedure

For WLAN access network reselection, the UE configured with a WLANSP rule shall use the access network selection procedure as specified in subclause 5.3.2. The UE first uses WLAN Selection Policy (WLANSP) to determine the active WLANSP rule. The UE selects the highest priority and valid WLANSP rule as the active WLANSP rule.

The access network reselection procedure can be in automatic mode or manual mode. The manual mode reselection shall follow the behaviour described in subclause 5.3.2.3 and the automatic mode reselection shall follow the behaviour described in subclause 5.3.2.4.

6 UE - 5GC network protocols

6.1 General

This subclause specifies the related procedures performed between the UE and untrusted or trusted non-3GPP access network or wireline access network.

6.2 Void

6.3 Authentication and authorization for accessing 5GS via non-3GPP access network

6.3.1 General

In order to register to the 5G core network (5GCN) 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 (N3AN).

Once the UE is configured with a local IP address, the UE shall select the Non-3GPP InterWorking Function (N3IWF) as described in subclause 7.2 and shall initiate the IKEv2 SA establishment procedure as described in subclause 7.3. During the IKEv2 SA establishment procedure, authentication and authorization for access to 5GCN is performed.

NOTE: The trust relationship indicator (see 3GPP TS 24.302 [7]), which can be received during EAP extension authentication during IKEv2 SA, does not indicate the WLAN is a trusted non-3GPP access network connected to the 5GCN.

In a trusted non-3GPP access, a UE shall first connect to a TNAN using a link layer protocol and shall initiate EAP authentication. During EAP authentication, authentication and authorization for access to 5GCN is performed by

exchange of EAP-5G message the link layer protocol between the UE and the TNAN, see subclause 7.3A.2.1. Upon completion of EAP authentication, the UE shall be assigned an IP address by that TNAN. Once the UE is configured with an IP address, it shall initiate the IKEv2 SA establishment procedure as described in subclause 7.3A.

In a wireline access, the 5G-RG shall first establish W-CP EAP connection with a W-AGF serving the 5G-RG using means out of scope of the present document and shall initiate EAP authentication. During EAP authentication, authentication and authorization for access to 5GCN is performed by exchange of EAP-5G messages via W-CP EAP connection, see clause 7A. Once the EAP authentication succeeds, the 5G-RG shall establish a W-CP signalling connection.

In wireline access, authentication and authorization of an N5GC device behind a CRG for access to 5GCN is performed as described in subclause 6.3.2.

6.3.2 Authentication of N5GC device behind a CRG over wireline access

In order to register to 5GCN via wireline access, the N5GC device first establishes a layer-2 connection to W-AGF via the CRG as specified in CableLabs WR-TR-5WWC-ARCH- V02-200430 [36]. Once the layer-2 connection is established, authentication and authorization for access to 5GCN is performed.

The W-AGF initiates an exchange of EAP-Request/Identity message and EAP-Response/Identity message as specified in IETF RFC 3748 [9] for obtaining the identity of the N5GC device. In wireline access, the W-AGF and the N5GC device exchange EAP-Request/Identity message and EAP-Response/Identity message via the CRG, encapsulated in the link layer protocol packets.

Upon reception of EAP-Request/Identity message, the N5GC device shall:

a) construct an EAP-Response/Identity message as described in IETF RFC 3748 [9] containing an NAI username@realm as specified in IETF RFC 7542 [37]; and

NOTE: If subscription identifier privacy protection is to be used, the "username" part is either omitted or set to "anonymous".

b) transmit the EAP-Response of identity type encapsulated in the link layer protocol packets towards the W-AGF.

The CRG conveys the information provided by the N5GC device to the W-AGF which initiates the registration on behalf of the N5GC device as described in 3GPP TS 24.501 [4]. The SUPI of the N5GC device contains a network specific identifier. For the registration, the W-AGF uses the NULL scheme as specified in 3GPP TS 33.501 [5], to construct a SUCI from the SUPI which was received as the NAI from the N5GC device in the EAP-Response/Identity message.

An exchange of the EAP request and EAP response as described in IETF RFC 3748 [9] occurs until the N5GC device is authenticated by the 5GCN with the EAP authentication described in 3GPP TS 33.501 [5].

Upon completion of successful authentication and on reception of the authentication result from the AMF, the W-AGF serving the N5GC device shall complete the procedure by sending an EAP-Success message encapsulated in the link layer protocol packets.

6.4 Handling of ANDSP Information

6.4.1 General

The Access Network Discovery & Selection policy (ANDSP) is used to control UE behavior related to access network discovery and selection of trusted and untrusted non-3GPP access network.

NOTE: ANDSP does not influence access network discovery and selection of wireline access network.

ANDSP consists of:

- WLAN Selection Policy (WLANSP); and
- Non-3GPP access network (N3AN) node configuration information.

The UE uses the WLANSP for selecting the WLAN.

The UE uses the Non-3GPP access network (N3AN) node configuration information for selecting a N3AN node (i.e. N3IWF or ePDG).

When roaming, the UE can receive ANDSP including WLANSP from H-PCF or V-PCF or both. The ANDSP including N3AN node configuration information is provided by -PCF only. The UE shall ignore the N3AN node configuration information in the ANDSP if the ANDSP is provided by V-PCF.

The structure and the content of ANDSP are defined in 3GPP TS 24.526 [17].

6.4.2 UE procedures

6.4.2.1 General

When ANDSP is modified based on information received from network as specified in 3GPP TS 24.501 [4] Annex D, the UE shall re-evaluate the ANDSP.

The received ANDSP information shall not impact the PLMN selection and reselection procedures specified in 3GPP TS 23.122 [13].

The UE shall periodically re-evaluate ANDSP. The value of the periodic re-evaluation timer is implementation dependent. The additional trigger for (re-)evaluating ANDSP is when the active WLANSP rule becomes invalid (conditions no longer fulfilled), or other manufacturer specific trigger.

6.4.2.2 Use of WLAN selection information

During automatic mode WLAN selection, the UE shall use the WLAN selection policy (WLANSP), if provided by the PCF, to determine the selected WLAN as described in subclause 5.3.

6.4.2.3 Use of N3AN node configuration information

If the UE accesses 5GCN via the non-3GPP access, the UE shall use the N3AN node configuration information to select an N3AN node as described in subclause 7.2, to be used for establishing IKEv2 security association as described in subclause 7.3.

6.4.3 ANDSP information from the network

ANDSP information is provided by the network to the UE using the UE policy delivery procedure described in Annex D of 3GPP TS 24.501 [4].

7 Security association management procedures

7.1 General

The purpose of the security association management procedures is to define the procedures for establishment or disconnection of end-to-end security association between the UE and the N3IWF via an IKEv2 protocol exchange specified in IETF RFC 7296 [6]. The IKE SA and child signalling IPsec SA establishment procedure is always initiated by the UE, whereas the child user plane IPsec SA creation procedures shall be initiated by the N3IWF as specified in 3GPP TS 23.502 [3].

The UE selects an N3IWF according to the procedure in subclause 7.2. Once the N3IWF has been selected, the security associations are established and managed according to the procedures in subclause 7.3 to subclause 7.7.

If a non-3GPP access network does not support transport of IP fragments, the maximum size of an IKEv2 message including the IP header is equal to the path MTU between the UE and N3IWF.

EXAMPLE: If a non-3GPP access network is an IPv6 only network which does not support transport of IP fragments and the path MTU between the UE and the N3IWF is 1280 octets then the maximum size of an IKEv2 message including IP header is 1280 octets.

7.2 N3AN node selection procedure

7.2.1 General

The UE performs N3AN node selection procedure based on the N3AN node configuration information provisioned to the UE by the HPLMN, based on the UE's knowledge of the country the UE is located in and the PLMN the UE is registered to via 3GPP access and based on the list of "forbidden PLMNs for non-3GPP access to 5GCN".

Subclauses 7.2.1, 7.2.2, 7.2.3, and 7.2.4 are applicable to a UE selecting an N3AN node in a PLMN. For a UE accessing PLMN services via an SNPN, restrictions on N3IWF FQDN are specified in subclause 4.3.2.

Subclause 7.2.5 is applicable to a UE selecting an N3AN node in an SNPN.

7.2.2 N3AN node configuration information

The N3AN node configuration information is provisioned to the UE either by H-PCF or via implementation specific means. The UE shall apply the N3AN node configuration information provisioned via implementation specific means only if the N3AN node configuration information provisioned by the H-PCF is not present in the UE.

The N3AN node configuration information shall consist of the following:

- N3AN node selection information;
- optionally, home N3IWF identifier configuration; and
- optionally, home ePDG identifier configuration.

The N3AN node selection information consists of N3AN node selection information entries. Each N3AN node selection information entry contains a PLMN ID and information for the PLMN ID. The N3AN node selection information contains at least an N3AN node selection information entry with information for the HPLMN and an N3AN node selection information entry for "any_PLMN".

The N3AN node configuration information provisioned by H-PCF is as specified in 3GPP TS 24.501 [4] annex D and 3GPP TS 24.526 [17].

The UE shall support the implementation of standard DNS mechanisms in order to retrieve the IP address(es) of the N3IWF or ePDG. The input to the DNS query is an N3IWF FQDN or ePDG FQDN as specified in 3GPP TS 23.003 [8].

7.2.3 Determination of the country the UE is located in

If the UE cannot determine whether it is located in the home country or in a visited country, as required by the N3AN node selection procedure, the UE shall stop the N3AN node selection. Once the UE determines the country the UE is located in, the UE shall proceed with N3AN node selection as specified in subclause 7.2.4.

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 or in a location that does not belong to any 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 of the PLMN to which a cell belongs, broadcast 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 [13]. If the UE is not in coverage of a 3GPP RAT, the UE can use other techniques, including user-provided location.

7.2.4 N3AN node selection

7.2.4.1 General

When the UE supports connectivity with N3IWF but does not support connectivity with ePDG, the UE shall perform the procedure in subclause 7.2.4.3 for selecting an N3IWF.

When the UE supports connectivity with N3IWF and ePDG, the UE shall perform the procedure in subclause 7.2.4.4 for selecting either an N3IWF or an ePDG.

7.2.4.2 Determine if the visited country mandates the selection of N3IWF in this country

In order to determine if the visited country mandates the selection of N3IWF in this country, the UE shall perform the DNS NAPTR query using Visited Country FQDN as specified in 3GPP TS 23.003 [8] via the non-3GPP access network.

If the result of this query is:

- a set of one or more records containing the service instance names of the form "*n3iwf.5gc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org*", the UE shall determine that the visited country mandates the selection of the N3IWF in this country; and

NOTE: The (<MCC>, <MNC>) pair in each record represents PLMN Id (see 3GPP TS 23.003 [8]) in the visited country which can be used for N3IWF selection in subclause 7.2.4.3 and subclause 7.2.4.4.

- no records containing the service instance names of the form "*n3iwf.5gc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org*", the UE shall determine that the visited country does not mandate the selection of the N3IWF in this country.

7.2.4.3 UE procedure when the UE only supports connectivity with N3IWF

If the UE only supports connectivity with N3IWF and does not support connectivity with ePDG, the UE shall ignore the following ePDG related configuration parameters if available in the N3AN node configuration information when selecting an N3IWF:

- the home ePDG identifier configuration; and

- the preference parameter in each N3AN node selection information entry in the N3AN node selection information.

The UE shall proceed as follows:

a) if the UE is located in its home country:

   1) if the N3AN node configuration information is provisioned:

      i) if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information and contains an IP address, the UE shall use the IP address of the home N3IWF identifier configuration as the IP address of the N3IWF;

      ii) if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information and does not contain an IP address, the UE shall use the FQDN of the home N3IWF identifier configuration as the N3IWF FQDN; and

      iii) if the home N3IWF identifier configuration is not provisioned in the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on the FQDN format of the HPLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the HPLMN stored on the USIM as specified in 3GPP TS 23.003 [8]; and

   2) if the N3AN node configuration information is not provisioned on the UE, the UE shall construct the N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the HPLMN stored on the USIM;

   and for the above cases constructing or using an N3IWF FQDN, the UE shall use the DNS server function to resolve the N3IWF FQDN to the IP address(es) of the N3IWF(s). The UE shall select as the IP address of the N3IWF a resolved IP address of an N3IWF with the same IP version as its local IP address; and

b) if the UE is not located in its home country:

1) if the N3AN node configuration information is provisioned, the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is not included in the list of "forbidden PLMNs for non-3GPP access to 5GCN":

   i) if an N3AN node selection information entry for the VPLMN is available in the N3AN node selection information of the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on FQDN format of the VPLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the VPLMN as specified in 3GPP TS 23.003 [8]; and

   ii) if an N3AN node selection information entry for the VPLMN is not available in the N3AN node selection information of the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on the FQDN format of the 'Any_PLMN' N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the VPLMN as specified in 3GPP TS 23.003 [8];

   and for the above cases, the UE shall use the DNS server function to resolve the constructed N3IWF FQDN to the IP address(es) of the N3IWF(s). The UE shall select as the IP address of the N3IWF a resolved IP address of an N3IWF with the same IP version as its local IP address; and

2) if one of the following is true:

   - the UE is not registered to a PLMN via 3GPP access and the UE uses WLAN;

   - the N3AN node configuration information is not provisioned; or

   - the N3AN node configuration information is provisioned, the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is included in the list of "forbidden PLMNs for non-3GPP access to 5GCN";

   the UE shall perform a DNS query (see 3GPP TS 23.003 [8]) as specified in subclause 7.2.4.2 to determine if the visited country mandates the selection of N3IWF in this country and:

   i) if selection of N3IWF in visited country is mandatory:

      A) if the UE is registered to a VPLMN via 3GPP access, the PLMN ID of VPLMN is included in one of the returned DNS records and is not included in the list of "forbidden PLMNs for non-3GPP access to 5GCN", the UE shall construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the VPLMN in 3GPP access as described in 3GPP TS 23.003 [8]; and

      B) if the UE is not registered to a PLMN via 3GPP access or the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is not included in any of the returned DNS records or is included in the list of "forbidden PLMNs for non-3GPP access to 5GCN":

         - if the N3AN node configuration information is provisioned, the UE shall select a PLMN included in the DNS response that has highest PLMN priority (see 3GPP TS 24.526 [17]) in the N3AN node selection information of the N3AN node configuration information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" and the UE shall construct an N3IWF FQDN based on the FQDN format of the selected PLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the selected PLMN as specified in 3GPP TS 23.003 [8]; and

         - if the N3AN node configuration information is not provisioned or the N3AN node selection information of the N3AN node configuration information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" does not contain any of the PLMNs in the DNS response, selection of a PLMN of the visited country is UE implementation specific. If the UE does not select a PLMN, the UE shall terminate the N3AN node selection procedure. If the UE selects a PLMN, the UE shall construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the selected PLMN as described in 3GPP TS 23.003 [8];

      and for the above cases, the UE shall use the DNS server function to resolve the constructed N3IWF FQDN to the IP address(es) of the N3IWF(s). The UE shall select as the IP address of the N3IWF a resolved IP address of an N3IWF with the same IP version as its local IP address;

   ii) if the DNS response contains no records, the UE shall further determine if the visited country mandates the selection of ePDG in the visited country using the procedure specified in subclause 7.2.1.4 of 3GPP TS 24.302 [7].

If the UE determines that the visited country mandates the selection of ePDG in the visited country, the UE shall assume that the selection of N3IWF in the visited country is mandatory and shall terminate the N3AN node selection procedure.

- If the UE determines that the visited country does not mandate the selection of ePDG in the visited country, the UE shall assume that the selection of N3IWF in the visited country is not mandatory, then the UE shall proceed as below:

  A) if the N3AN node configuration information is provisioned and the N3AN node selection information of the N3AN node configuration information contains one or more PLMNs in the visited country which are not in the list of "forbidden PLMNs for non-3GPP access to 5GCN", the UE shall select a PLMN that has highest PLMN priority (see 3GPP TS 24.526 [17]) in the N3AN node selection information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" and the UE shall construct an N3IWF FQDN based on the FQDN format of the selected PLMN's N3AN node selection information entry in the N3AN node selection information as specified in 3GPP TS 23.003 [8] using the PLMN ID of the selected PLMN; and

  B) if the N3AN node configuration information is not provisioned or the N3AN node configuration information is provisioned and the N3AN node selection information of the N3AN node configuration information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" contains no PLMNs in the visited country:

     - if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information (see 3GPP TS 24.526 [17]) and contains an IP address, the UE shall use the IP address of the home N3IWF identifier configuration as the IP address of the N3IWF;

     - if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information (see 3GPP TS 24.526 [17]) and does not contain an IP address, the UE shall use the FQDN of the home N3IWF identifier configuration as the N3IWF FQDN; and

     - if the home N3IWF identifier configuration is not provisioned in the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the HPLMN as described in 3GPP TS 23.003 [8];

  and for the above cases constructing or using an N3IWF FQDN, the UE shall use the DNS server function to resolve the N3IWF FQDN to the IP address(es) of the N3IWF(s). The UE shall select as the IP address of the N3IWF a resolved IP address of an N3IWF with the same IP version as its local IP address; and

iii) if no DNS response is received, the UE shall terminate the N3AN node selection procedure.

Following bullet a) and b) above, once the UE selected the IP address of the N3IWF, the UE shall initiate the IKEv2 SA establishment procedure as specified in subclause 7.3.

If the IKEv2 SA establishment procedure towards an N3IWF in the HPLMN fails due to no response to an IKE_SA_INIT request message, and the selection of N3IWF in the HPLMN is performed using home N3IWF identifier configuration and there are more pre-configured N3IWFs in the HPLMN, the UE shall repeat the tunnel establishment attempt using the next FQDN or IP address(es) of the N3IWF in the HPLMN.

If the IKEv2 SA establishment procedure towards to any of the received IP addresses of the selected N3IWF fails due to no response to an IKE_SA_INIT request message, then the UE shall repeat the N3IWF selection as described in this subclause, excluding the N3IWFs for which the UE did not receive a response to the IKE_SA_INIT request message.

NOTE: The time the UE waits before reattempting access to another N3IWF or to an N3IWF that it previously did not receive a response to an IKE_SA_INIT request message, is implementation specific.

7.2.4.4 UE procedure when the UE supports connectivity with N3IWF and ePDG

7.2.4.4.1 General

If the UE can support connectivity with N3IWF and with ePDG, the UE shall:

- if the N3AN node selection is required for an IMS service, follow steps specified in subclause 7.2.4.4.2 for N3AN node selection; and

- if the N3AN node selection is required for a non-IMS service, follow steps specified in subclause 7.2.4.4.3 for N3AN node selection.

NOTE: How the UE determines node selection is required for an IMS service or for a non-IMS service is implementation-specific.

7.2.4.4.2 N3AN node selection for IMS service

If the N3AN node selection is required for an IMS service, the UE shall use the preference parameter in the N3AN node selection information entries of the N3AN node selection information to determine whether selection of N3IWF or ePDG is preferred in a given PLMN.

The UE shall proceed as follows:

a) if the UE is located in its home country:

1) if the N3AN node configuration information is provisioned:

i) if the preference parameter in the HPLMN's N3AN node selection information entry of the N3AN node selection information indicates that N3IWF is preferred:

A) if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information and contains an IP address, the UE shall use the IP address of the home N3IWF identifier configuration as the IP address of the N3IWF;

B) if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information and does not contain an IP address, the UE shall use the FQDN of the home N3IWF identifier configuration as the N3IWF FQDN; and

C) if the home N3IWF identifier configuration is not provisioned in the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on the FQDN format of the HPLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the HPLMN stored on the USIM as specified in clause 28 of 3GPP TS 23.003 [8]; and

ii) if the preference parameter in the HPLMN's N3AN node selection information entry of the N3AN node selection information indicates that ePDG is preferred:

A) if the home ePDG identifier configuration is provisioned in the N3AN node configuration information and contains an IP address, the UE shall use the IP address of the home ePDG identifier configuration as the IP address of the ePDG;

B) if the home ePDG identifier configuration is provisioned in the N3AN node configuration information and does not contains an IP address, the UE shall use the FQDN of the home ePDG identifier configuration as the ePDG FQDN; and

C) if the home ePDG identifier configuration is not provisioned in the N3AN node configuration information, the UE shall construct an ePDG FQDN based on the FQDN format of HPLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the HPLMN stored on the USIM as specified in clause 19 of 3GPP TS 23.003 [8]; and

2) if the N3AN node configuration information is not provisioned on the UE, the UE shall construct the N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the HPLMN stored on the USIM;

and for the above cases constructing or using an N3IWF FQDN or ePDG FQDN, the UE shall use the DNS server function to resolve the N3IWF FQDN or ePDG FQDN to the IP address(es) of the N3IWF(s) or ePDG(s). The UE shall select as the IP address of the N3IWF or of the ePDG a resolved IP address of an N3IWF or an ePDG with the same IP version as its local IP address; and

b) if the UE is not located in its home country:

1) if the N3AN node configuration information is provisioned, the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is not included in the list of "forbidden PLMNs for non-3GPP access to 5GCN":

i) if an N3AN node selection information entry for the VPLMN is available in the N3AN node selection information of the N3AN node configuration information:

A) if the preference parameter in the VPLMN's N3AN node selection information entry of the N3AN node configuration information indicates that N3IWF is preferred, the UE shall construct an N3IWF FQDN based on the FQDN format of the VPLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the VPLMN as specified in clause 28 of 3GPP TS 23.003 [8]; and

B) if the preference parameter in the VPLMN's N3AN node selection information entry of the N3AN node configuration information indicates that ePDG is preferred, the UE shall construct an ePDG FQDN based on the FQDN format of the VPLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the VPLMN as specified in clause 19 of 3GPP TS 23.003 [8]; and

ii) if an N3AN node selection information entry for the VPLMN is not available in the N3AN node selection information of the N3AN node configuration information:

A) if the preference parameter in the 'Any_PLMN' N3AN node selection information entry of the N3AN node configuration information indicates that N3IWF is preferred, the UE shall construct an N3IWF FQDN based on the FQDN format of the 'Any_PLMN' N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the VPLMN as specified in clause 28 of 3GPP TS 23.003 [8]; and

B) if the preference parameter in the 'Any_PLMN' N3AN node selection information entry of the N3AN node configuration information indicates that ePDG is preferred, the UE shall construct an ePDG FQDN based on the FQDN format of the 'Any_PLMN' N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the VPLMN as specified in clause 19 of 3GPP TS 23.003 [8];

and for above case, the UE shall use the DNS server function to resolve the constructed N3IWF FQDN or ePDG FQDN to the IP address(es) of the N3IWF(s) or ePDG(s). The UE shall select as the IP address of the N3IWF or the ePDG a resolved IP address of an N3IWF or ePDG with the same IP version as its local IP address; and

2) if one of the following is true:

- the UE is not registered to a PLMN via 3GPP access and the UE uses WLAN;
- the N3AN node configuration information is not provisioned; or
- the N3AN node configuration information is provisioned, the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is included in the list of "forbidden PLMNs for non-3GPP access to 5GCN";

the UE shall perform a DNS query (see 3GPP TS 23.003 [8]) as specified in subclause 7.2.4.2 to determine if the visited country mandates the selection of N3IWF in this country and:

i) if selection of N3IWF in the visited country is mandatory:

A) if the UE is registered to a VPLMN via 3GPP access, the PLMN ID of VPLMN is included in one of the returned DNS records and is not included in the list of "forbidden PLMNs for non-3GPP access to 5GCN", the UE shall construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the VPLMN as described in clause 28 of 3GPP TS 23.003 [8]; and

B) if the UE is not registered to a PLMN via 3GPP access, or the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is not included in any of the returned DNS records or is included in the list of "forbidden PLMNs for non-3GPP access to 5GCN":

- if the N3AN node configuration information is provisioned, the UE shall select an a PLMN included in the DNS response that has highest PLMN priority (see 3GPP TS 24.526 [17]) in the N3AN node selection information of the N3AN node configuration information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" and the UE shall construct an N3IWF FQDN based on the FQDN format of the selected PLMN's N3AN node selection

information entry in the N3AN node selection information using the PLMN ID of the selected PLMN as specified clause 28 of in 3GPP TS 23.003 [8]; and

- if the N3AN node configuration information is not provisioned or the N3AN node selection information of the N3AN node configuration information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" does not contain any of the PLMNs in the DNS response, selection of the PLMN is UE implementation specific. The UE shall construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the selected PLMN as described clause 28 of in 3GPP TS 23.003 [8];

and for the above cases, the UE shall use the DNS server function to resolve the constructed N3IWF FQDN to the IP address(es) of the N3IWF(s). The UE shall select as the IP address of the N3IWF a resolved IP address of an N3IWF with the same IP version as its local IP address;

ii) if the DNS response contains no records, the UE shall further determine if the visited country mandates the selection of ePDG in the visited country using the procedure specified in subclause 7.2.1.4 of 3GPP TS 24.302 [7].

If the UE determines that the visited country mandates the selection of ePDG in the visited country, the UE shall assume that the selection of N3IWF in the visited country is mandatory and shall continue the ePDG selection procedure in the visited country, specified in subclause 7.2.1.3 of 3GPP TS 24.302 [7].

If the UE determines that the visited country does not mandate the selection of ePDG in the visited country, the UE shall assume that the selection of N3IWF in the visited country is not mandatory and the UE shall proceed as below:

A) if the N3AN node configuration information is provisioned and the N3AN node selection information of the N3AN node configuration information contains one or more PLMNs in the visited country which are not included in the list of "forbidden PLMNs for non-3GPP access to 5GCN", the UE shall select a PLMN that has highest PLMN priority (see 3GPP TS 24.526 [17]) in the N3AN node selection information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" and the UE shall construct an N3IWF FQDN based on the FQDN format of the selected PLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the selected PLMN as specified in clause 28 of 3GPP TS 23.003 [8]; and

B) if the N3AN node configuration information is not provisioned or the N3AN node configuration information is provisioned and the N3AN node selection information of the N3AN node configuration information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" contains no PLMN in the visited country:

- if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information (see 3GPP TS 24.526 [17]) and contains an IP address, the UE shall use the IP address of the home N3IWF identifier configuration as the IP address of the N3IWF;

- if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information (see 3GPP TS 24.526 [17]) and does not contains an IP address, the UE shall use the FQDN of the home N3IWF identifier configuration as N3IWF FQDN; and

- if the home N3IWF identifier configuration is not provisioned in the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the HPLMN as described in clause 28 of 3GPP TS 23.003 [8];

and for the above cases constructing or using an N3IWF FQDN, the UE shall use the DNS server function to resolve the N3IWF FQDN to the IP address(es) of the N3IWF(s). The UE shall select as the IP address of the N3IWF a resolved IP address of an N3IWF with the same IP version as its local IP address; and

iii) if no DNS response is received, the UE shall terminate the N3AN node selection procedure.

Following bullet a) and b) above, once the UE selected the IP address of the N3IWF or the ePDG:

a) if the IP address of N3IWF is selected, the UE shall:

i) initiate the IKEv2 SA establishment procedure as specified in subclause 7.3;

ii) if the IKEv2 SA establishment procedure towards an N3IWF in the HPLMN fails due to no response to an IKE_SA_INIT request message or the UE is informed during registration over non-3GPP access that the IMS voice over PS session is not supported over non-3GPP access, and the selection of N3IWF in the HPLMN is performed using home N3IWF identifier configuration and there are more pre-configured N3IWFs in the HPLMN, repeat the tunnel establishment attempt using the next FQDN or IP address(es) of the N3IWF in the HPLMN;

iii) if the IKEv2 SA establishment procedure towards any of the received IP addresses of the selected N3IWF fails due to no response to an IKE_SA_INIT request message or the UE is informed during registration over non-3GPP access that the IMS voice over PS session is not supported over non-3GPP access, attempt to select an ePDG in the same PLMN as specified in 3GPP TS 24.302 [7] instead; and

iv) if the UE fails to connect to either N3IWF or ePDG in the same PLMN, repeat the N3AN node selection as described in this subclause, excluding the N3IWFs 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 N3IWF or to an N3IWF that it previously did not receive a response to an IKE_SA_INIT request message, is implementation specific.

b) if the IP address of ePDG is selected, the UE shall:

i) initiate tunnel establishment as specified in 3GPP TS 24.302 [7];

ii) if tunnel establishment as specified in 3GPP TS 24.302 [7] towards an ePDG in the HPLMN fails due to no response to an IKE_SA_INIT request message, and the selection of ePDG in the HPLMN is performed using home ePDG identifier configuration and there are more pre-configured ePDG in the HPLMN, repeat the tunnel establishment attempt using the next FQDN or IP address(es) of the ePDG in the HPLMN;

iii) if tunnel establishment as specified in 3GPP TS 24.302 [7] towards any of the received IP addresses of the selected ePDG fails due to no response to an IKE_SA_INIT request message, attempt to select an N3IWF in the same PLMN instead; and

iv) if the UE fails to connect to either ePDG or N3IWF in the same PLMN, repeat the N3AN node selection as described in this subclause, excluding the ePDGs for which the UE did not receive a response to the IKE_SA_INIT request message.

NOTE 2: 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.

7.2.4.4.3 N3AN node selection for Non-IMS service

If the N3AN node selection is required for a non-IMS service, the UE shall ignore the preference parameter in the N3AN node selection information entries of the N3AN node selection information.

The UE shall proceed as follows:

a) if the UE is located in its home country:

1) if the N3AN node configuration information is provisioned:

i) if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information and contains an IP address, the UE shall use the IP address of the home N3IWF identifier configuration as the IP address of the N3IWF;

ii) if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information and does not contain an IP address, the UE shall use the FQDN of the home N3IWF identifier configuration as the N3IWF FQDN; and

iii) if the home N3IWF identifier configuration is not provisioned in the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on the FQDN format of the HPLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the HPLMN stored on the USIM as specified in clause 28 of 3GPP TS 23.003 [8]; and

2) if the N3AN node configuration information is not provisioned, the UE shall construct the N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the HPLMN stored on the USIM;

and for the above cases constructing or using an N3IWF FQDN, the UE shall use the DNS server function to resolve the N3IWF FQDN to the IP address(es) of the N3IWF(s) or ePDG(s). The UE shall select as the IP address of the N3IWF a resolved IP address of an N3IWF with the same IP version as its local IP address; and

b) if the UE is not located in its home country:

1) if the N3AN node configuration information is provisioned, the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is not included in the list of "forbidden PLMNs for non-3GPP access to 5GCN":

i) if an N3AN node selection information entry for the VPLMN is available in the N3AN node selection information of the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on the FQDN format of the VPLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the VPLMN as specified in clause 28 of 3GPP TS 23.003 [8]; and

ii) if an N3AN node selection information entry for the VPLMN is not available in the N3AN node selection information of the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on the FQDN format of the 'Any_PLMN' N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the VPLMN as specified in clause 28 of 3GPP TS 23.003 [8]; and

and for above case, the UE shall use the DNS server function to resolve the constructed N3IWF FQDN to the IP address(es) of the N3IWF(s). The UE shall select as the IP address of the N3IWF a resolved IP address of an N3IWF with the same IP version as its local IP address; and

2) if one of the following is true:

- the UE is not registered to a PLMN via 3GPP access and the UE uses WLAN;

- the N3AN node configuration information is not provisioned; or

- the N3AN node configuration information is provisioned, the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is included in the list of "forbidden PLMNs for non-3GPP access to 5GCN";

the UE shall perform a DNS query (see 3GPP TS 23.003 [8]) as specified in subclause 7.2.4.2 to determine if the visited country mandates the selection of N3IWF in this country and:

i) if selection of N3IWF in the visited country is mandatory:

A) if the UE is registered to a VPLMN via 3GPP access, the PLMN ID of VPLMN is included in one of the returned DNS records and is not included in the list of "forbidden PLMNs for non-3GPP access to 5GCN", the UE shall construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the VPLMN as described in clause 28 of 3GPP TS 23.003 [8]; and

B) if the UE is not registered to a PLMN via 3GPP access or the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is not included in any of the returned DNS records or is included in the list of "forbidden PLMNs for non-3GPP access to 5GCN":

- if the N3AN node configuration information is provisioned, the UE shall select an a PLMN included in the DNS response that has highest PLMN priority (see 3GPP TS 24.526 [17]) in the N3AN node selection information of the N3AN node configuration information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" and the UE shall construct an N3IWF FQDN based on the FQDN format of the selected PLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the selected PLMN as specified in clause 28 of 3GPP TS 23.003 [8]; and

- if the N3AN node configuration information is not provisioned or the N3AN node selection information of the N3AN node configuration information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" does not contain any of the PLMNs in the DNS response, selection of the PLMN is UE implementation specific. The UE shall construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the selected PLMN as described in clause 28 of 3GPP TS 23.003 [8];

and for the above cases, the UE shall use the DNS server function to resolve the constructed N3IWF FQDN to the IP address(es) of the N3IWF(s). The UE shall select as the IP address of the N3IWF a resolved IP address of an N3IWF with the same IP version as its local IP address;

ii) if the DNS response contains no records, the UE shall further determine if the visited country mandates the selection of ePDG in the visited country using the procedure specified in subclause 7.2.1.4 of 3GPP TS 24.302 [7].

determines that the visited country mandates the selection of ePDG in the visited country, the UE shall assume that the selection of N3IWF in the visited country is mandatory and shall continue the ePDG selection procedure in the visited country, specified in subclause 7.2.1.3 of 3GPP TS 24.302 [7].

If the UE determines that the visited country does not mandate the selection of ePDG in the visited country, the UE shall assume that the selection of N3IWF in the visited country is not mandatory and the UE shall proceed as follows:

A) if the N3AN node configuration information is provisioned and the N3AN node selection information of the N3AN node configuration information contains one or more PLMNs in the visited country which are not in the list of "forbidden PLMNs for non-3GPP access to 5GCN", the UE shall select a PLMN that has highest PLMN priority (see 3GPP TS 24.526 [17]) in the N3AN node selection information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" and the UE shall construct an N3IWF FQDN based on the FQDN format of the selected PLMN's N3AN node selection information entry in the N3AN node selection information using the PLMN ID of the selected PLMN as specified in clause 28 of 3GPP TS 23.003 [8]; and

B) if the N3AN node configuration information is not provisioned or the N3AN node configuration information is provisioned and the N3AN node selection information of the N3AN node configuration information excluding any PLMN in the list of "forbidden PLMNs for non-3GPP access to 5GCN" contains no PLMN in the visited country:

- if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information (see 3GPP TS 24.526 [17]) and contains an IP address, the UE shall use the IP address of the home N3IWF identifier configuration as the IP address of the N3IWF;

- if the home N3IWF identifier configuration is provisioned in the N3AN node configuration information (see 3GPP TS 24.526 [17]) and does not contains an IP address, the UE shall use the FQDN of the home N3IWF identifier configuration as N3IWF FQDN; and

- if the home N3IWF identifier configuration is not provisioned in the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the HPLMN as described in clause 28 of 3GPP TS 23.003 [8];

and for the above cases constructing or using an N3IWF FQDN, the UE shall use the DNS server function to resolve the N3IWF FQDN to the IP address(es) of the N3IWF(s). The UE shall select as the IP address of the N3IWF a resolved IP address of an N3IWF with the same IP version as its local IP address; and

iii) if no DNS response is received, the UE shall terminate the N3AN node selection procedure.

Following bullet a) and b) above, once the UE selected the IP address of the N3IWF:

a) if the IP address of N3IWF is selected, the UE shall:

1) initiate the IKEv2 SA establishment procedure as specified in subclause 7.3;

2) if the IKEv2 SA establishment procedure towards an N3IWF in the HPLMN fails due to no response to an IKE_SA_INIT request message, and the selection of N3IWF in the HPLMN is performed using home N3IWF identifier configuration and there are more pre-configured N3IWFs in the HPLMN, repeat the tunnel establishment attempt using the next FQDN or IP address(es) of the N3IWF in the HPLMN;

3) if the IKEv2 SA establishment procedure towards any of the IP addresses of the N3IWF of the selected PLMN fails due to no response to an IKE_SA_INIT request message, repeat the N3AN node selection as described in this subclause with N3IWF of another PLMN; and

4) if the IKEv2 SA establishment procedure towards any of the received IP addresses of the N3IWF of any fails due to no response to an IKE_SA_INIT request message, attempt to select an ePDG as specified in 3GPP TS 24.302 [7] and use tunnel establishment as specified in 3GPP TS 24.302 [7];

NOTE 1: The time the UE waits before reattempting access to another N3IWF or to an N3IWF that it previously did not receive a response to an IKE_SA_INIT request message, is implementation specific.

b) if the IP address of ePDG is selected, the UE shall:

i) initiate tunnel establishment as specified in 3GPP TS 24.302 [7];

ii) if tunnel establishment as specified in 3GPP TS 24.302 [7] towards an ePDG in the HPLMN fails due to no response to an IKE_SA_INIT request message, and the selection of ePDG in the HPLMN is performed using home ePDG identifier configuration and there are more pre-configured ePDG in the HPLMN, repeat the tunnel establishment attempt using the next FQDN or IP address(es) of the ePDG in the HPLMN;

iii) if tunnel establishment as specified in 3GPP TS 24.302 [7] towards any of the received IP addresses of the selected ePDG fails due to no response to an IKE_SA_INIT request message, attempt to select an N3IWF in the same PLMN instead; and

iv) if the UE fails to connect to either ePDG or N3IWF in the same PLMN, repeat the N3AN node selection as described in this subclause, excluding the ePDGs for which the UE did not receive a response to the IKE_SA_INIT request message.

NOTE 2: 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.

7.2.5 Selection of an N3AN node in an SNPN

In order to access SNPN services via a PLMN, an SNPN enabled UE registered to a PLMN uses a configured N3IWF FQDN to select an N3IWF in an SNPN.

7.3 IKE SA establishment procedure for untrusted non-3GPP access

7.3.1 General

The purpose of this procedure is to establish a secure connection between the UE and the N3IWF over NWu, which is used to securely exchange the NAS signalling messages between the UE and the AMF via the N3IWF. The UE establishes the secure connection by establishing an IKE SA and first child SA to the N3IWF. The IKE SA and first child SA, called signalling IPsec SA, are created between the UE and the N3IWF after the IKE_SA_INIT exchange and after the IKE_AUTH exchange (see IETF RFC 7296 [6]). The signalling IPsec established is used to transfer NAS signalling traffic. Additional child SAs (user plane IPsec SAs) can be established between the UE and the N3IWF to transfer user-plane traffic (see subclause 7.5).

Upon completion of the N3IWF selection procedure (subclause 7.2) the UE initiates an IKE_SA_INIT exchange as specified in IETF RFC 7296 [6]. Upon reception of the IKE_SA_INIT exchange the UE shall inform the upper layers that the access stratum connection is established.

Upon establishment of the access stratum connection, the UE initiates IKE_AUTH exchange (see IETF RFC 7296 [6]) with EAP-5G encapsulation, as specified in subclause 7.3.2.

The UE encapsulates the initial NAS message and the AN parameters using the EAP-5G procedure as described in subclause 7.3.3. The signalling IPsec SA is established after completion of the EAP-5G procedure and IKE_AUTH exchange.

7.3.2 IKE SA and signalling IPsec SA establishment procedure

7.3.2.1 IKE SA and signalling IPsec SA establishment initiation

The UE proceeds with the establishment of IKE SA and signalling IPsec SA with the selected N3IWF by initiating an IKE_SA_INIT exchange according to IETF RFC 7296 [6].

The UE shall initiate an IKE_AUTH exchange as specified in IETF RFC 7296 [6] to establish an IKE SA and first child SA (signalling IPsec SA). The UE shall indicate the intention to use EAP by not including the AUTH payload in the initial IKE_AUTH request message as specified in IETF RFC 7296 [6].

NOTE: The IKE_AUTH exchange is sent after the IKE_SA_INIT exchange. The UE has already established the IKE_SA_INIT exchange after N3IWF selection has been completed.

Upon reception of the IKE_AUTH request message without AUTH payload, the N3IWF shall respond with an IKE_AUTH response message with an indication to start an EAP-5G session that will be used to convey the initial NAS messages. The EAP-5G procedure is described in subclause 7.3.3.

7.3.2.2 IKE SA and signalling IPsec SA establishment accepted by the network

If IKE SA and signalling IPsec SA establishment is accepted by the network, the UE receives from the N3IWF an IKE_AUTH response message containing an EAP-Success message (as shown in figure 7.3.2-1), which completes the EAP-5G session. No further EAP-5G packets are exchanged.

The UE completes the IKE SA and signalling IPsec SA (first child SA) establishment procedure by initiating an IKE_AUTH exchange including an AUTH payload computed based on the N3IWF key as described in 3GPP TS 33.501 [5]. In the IKE_AUTH request message the UE additionally includes:

- the UE shall include the INTERNAL_IP4_ADDRESS attribute, the INTERNAL_IP6_ADDRESS attribute, or both, indicating the type of IP address to be used for the IP tunnels, in the CFG_REQUEST configuration payload. The INTERNAL_IP4_ADDRESS attribute shall contain no value and the length field shall be set to 0. The INTERNAL_IP6_ADDRESS attribute shall contain no value and the length field shall be set to 0; and

- if the UE supports IETF RFC 4555 [23], the UE may include the MOBIKE_SUPPORTED notify payload as specified in IETF RFC 4555 [23].

The N3IWF shall include in the IKE_AUTH response message containing the AUTH payload:

- a single CFG_REPLY Configuration Payload including the INTERNAL_IP4_ADDRESS attribute with an IPv4 address assigned to the UE, the INTERNAL_IP6_ADDRESS attribute with an IPv6 address assigned to the UE, or both;

- the NAS_IP4_ADDRESS notify payload with an N3IWF IPv4 address assigned to transport of NAS messages, if the initial IKE_AUTH request message contained a CFG_REQUEST configuration payload with the INTERNAL_IP4_ADDRESS attribute and NAS messages are to be transmitted using IPv4 based inner IP tunnel;

- the NAS_IP6_ADDRESS notify payload with an N3IWF IPv6 address assigned to transport of NAS messages if the initial IKE_AUTH request message contained a CFG_REQUEST configuration payload with the INTERNAL_IP6_ADDRESS attribute and NAS messages are to be transmitted using IPv6 based inner IP tunnel;

- the NAS_TCP_PORT notify payload with an N3IWF TCP port number assigned to transport of NAS messages; and

- the MOBIKE_SUPPORTED notify payload as specified in IETF RFC 4555 [23], if the initial IKE_AUTH request message contained a MOBIKE_SUPPORTED configuration payload with the INTERNAL_IP4_ADDRESS attribute.

The UE may support the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in 3GPP TS 24.302 [7] 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.

The N3IWF may include the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in 3GPP TS 24.302 [7] subclause 8.2.4.2 indicating the timeout period for liveness check in the CFG_REPLY configuration payload of the IKE_AUTH response message containing the AUTH 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 in the IKE_AUTH response message containing the AUTH payload.

If the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in 3GPP TS 24.302 [7] 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 containing the AUTH payload or the UE has a pre-configured or configured timeout period, the UE shall perform the liveness check procedure as described in subclause 7.8.

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

This completes the establishment of the IKE SA and signalling IPsec SA (first child SA) between the UE and the N3IWF. Upon completion of the IKE SA and signalling IPsec SA (first child SA) establishment between the UE and the N3IWF, the UE and the N3IWF shall send further NAS messages over the TCP connection within the signalling IPsec SA (first child SA) (see example in figure 7.3.2.2-1).

An example of an IKE SA and first child SA establishment procedure is shown in figure 7.3.2.2-1.

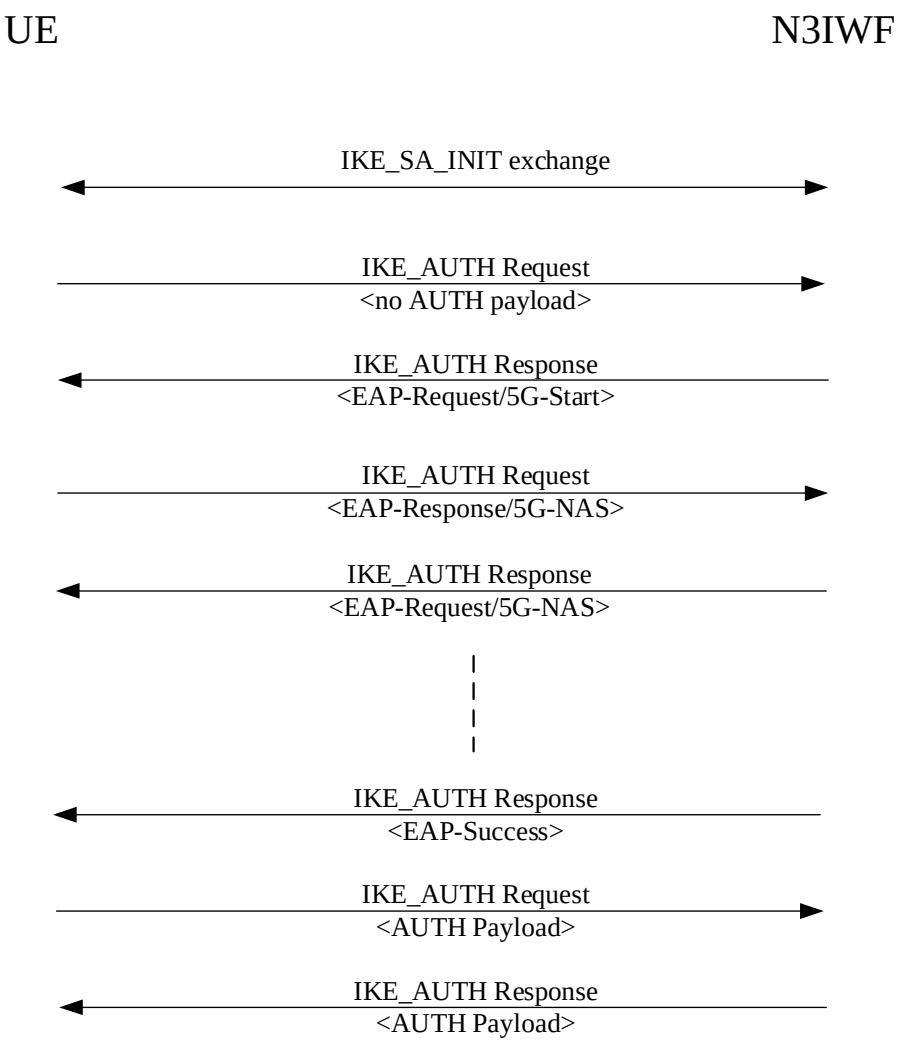

Figure 7.3.2.2-1: IKE SA and first child SA establishment procedure for UE registration over untrusted non-3GPP access

7.3.2.3 IKE SA and signalling IPsec SA establishment not accepted by the network

If IKE SA and signalling IPsec SA establishment is not accepted by the network, the UE receives from the N3IWF an IKE_AUTH response message including a Notify payload with an error type.

Upon receiving the IKE_AUTH response message with a Notify payload with an error type other than a CONGESTION Notify payload, the UE shall pass the error indication to the upper layer along with the encapsulated NAS messages, if any, within EAP/5G-NAS packet.

After the N3IWF receives from the UE an IKE_AUTH request message, if the N3IWF does not accept the IKE SA and signalling IPsec SA establishment due to:

a) the AMF congestion as indicated in the OVERLOAD START message; or

b) the requested NSSAI included in the IKE_AUTH request message, only including one or more S-NSSAIs indicated in the OVERLOAD START message;

where the OVERLOAD START message is specified in 3GPP TS 29.413 [39], the N3IWF shall construct an IKE_AUTH response message including a CONGESTION Notify payload as defined in subclause 9.2.4.2 and a N3GPP_BACKOFF_TIMER Notify payload as defined in subclause 9.3.1.7. The N3IWF shall send the IKE_AUTH response message to the UE.

NOTE: The N3IWF can also due to internal congestion construct an IKE_AUTH response message including a CONGESTION Notify payload as defined in subclause 9.2.4.2 and a N3GPP_BACKOFF_TIMER Notify payload as defined in subclause 9.3.1.7 and send it to the UE.

Upon reception of the IKE_AUTH response message including:

a) a CONGESTION Notify payload as defined in subclause 9.2.4.2; and

b) a N3GPP_BACKOFF_TIMER Notify payload as defined in subclause 9.3.1.7; and

after the UE authenticates the network or the N3IWF as specified in 3GPP TS 33.501 [5], the UE shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA as specified in IETF RFC 7296 [6]. In addition, the UE shall inform the upper layers that the access stratum connection has been released, and:

a) if the back-off timer value in N3GPP_BACKOFF_TIMER Notify payload indicates neither zero nor deactivated, the UE shall start the Tw3 timer with the value provided and the UE shall not retry the IKE SA and signalling IPsec SA establishment procedure to the same N3IWF until:

   - timer Tw3 expires;
   - the UE is switched off; or
   - the UICC containing the USIM is removed;

b) if the back-off timer value in N3GPP_BACKOFF_TIMER Notify payload indicates that this timer is deactivated, the UE shall not retry the IKE SA and signalling IPsec SA establishment procedure to the same N3IWF until:

   - the UE is switched off; or
   - the UICC containing the USIM is removed; and

c) if the back-off timer value in N3GPP_BACKOFF_TIMER Notify payload indicates zero, the UE may retry the IKE SA and signalling IPsec SA establishment procedure to an N3IWF from the same PLMN.

Upon receiving the IKE_AUTH response message with a Notify payload with an error type, if the EAP-5G session establishment has already been started, the UE shall perform a local termination of the EAP-5G session.

7.3.3 EAP-5G session over non-3GPP access

7.3.3.1 General

A vendor-specific EAP method (EAP-5G) is used to encapsulate NAS messages between the UE and the N3IWF. The EAP-5G packets utilize the "Expanded" EAP type and the existing 3GPP Vendor-Id registered with IANA under the SMI Private Enterprise Code registry (i.e. 10415). The EAP-5G method is utilized only for encapsulating the NAS messages. The EAP-5G method is not utilized to authenticate the UE in untrusted non-3GPP network.

7.3.3.1A EAP-5G session initiation

The UE and the N3IWF shall exchange EAP-5G messages within IKE_AUTH request and IKE_AUTH response messages. The N3IWF on reception of an IKE_AUTH request with no AUTH payload shall start an EAP-5G session by sending an EAP-Request/5G-Start message.

The UE acknowledges start of the EAP-5G session by sending an EAP-Response/5G-NAS message which shall include:

a) a NAS-PDU field containing a NAS message, for example, a REGISTRATION REQUEST message; and

b) an AN-parameters field containing access network parameters, such as GUAMI, selected PLMN ID, requested NSSAI, establishment cause and selected NID if the UE is accessing SNPN services via a PLMN (see 3GPP TS 23.502 [3]).

NOTE 1: If and how the UE includes the requested NSSAI as a part of the access type depends on the NSSAI inclusion mode IE as specified in 3GPP TS 24.501 [4].

The N3IWF, on reception of NAS messages from the UE within an EAP-Response/5G-NAS message, shall forward the NAS message to the AMF.

The N3IWF, on reception of NAS messages from the AMF, shall include the NAS message within an EAP-Request/5G-NAS message. The N3IWF shall transmit the EAP-Request/5G-NAS message to the UE.

NOTE 2: The N3IWF is transparent to the NAS messages and as an intermediate network entity only conveys transparently the NAS messages between the UE and the AMF.

The EAP-Request/5G-NAS message shall include a NAS-PDU field that contains a NAS message.

Further NAS messages between the UE and the AMF, via the N3IWF, shall be inserted in NAS-PDU field of an EAP-Response/5G-NAS (UE to N3IWF direction) and EAP-Request/5G-NAS (N3IWF to UE direction) message.

7.3.3.2 EAP-5G session completion initiated by the network

Upon completion of successful authentication and on reception of the N3IWF key from the AMF, the N3IWF shall complete the EAP-5G session by sending an EAP-Success message.

On reception of the EAP-Success message from the N3IWF, the UE proceeds to establish an IKE SA and signalling IPsec SA as described in subclause 7.3.2.

An example of an EAP-5G session after successful authentication is shown in figure 7.3.3.2-1.

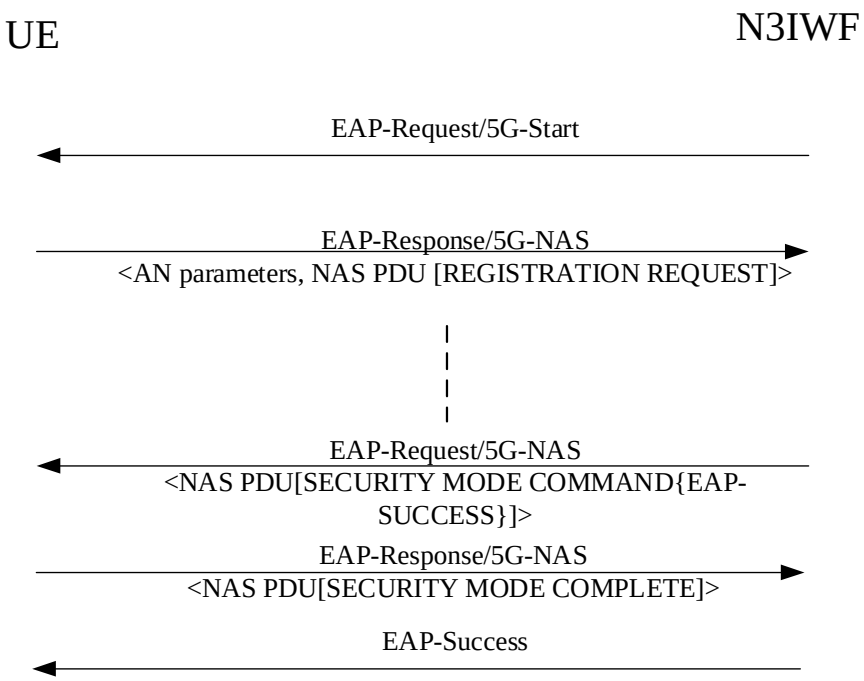

Figure 7.3.3.2-1: EAP-5G session for successful UE registration over untrusted non-3GPP access

7.3.3.3 EAP-5G session completion initiated by the UE

Upon receiving indication from the upper layer that no 5G-NAS messages need to be transmitted between the UE and N3IWF, the UE shall terminate the EAP-5G session by sending an EAP-Response/5G-Stop message to the N3IWF.

On reception of EAP-Response/5G-Stop message, the N3IWF shall complete the EAP-5G session by sending an EAP-Failure message to the UE.

On reception of the EAP-Failure message from the N3IWF, the UE shall delete any context related to IKE SA without requiring an explicit INFORMATIONAL exchange carrying a Delete payload as specified in IETF RFC 7296 [6].

Figure 7.3.3.3-1 shows an example the EAP-5G session completion after registration reject.

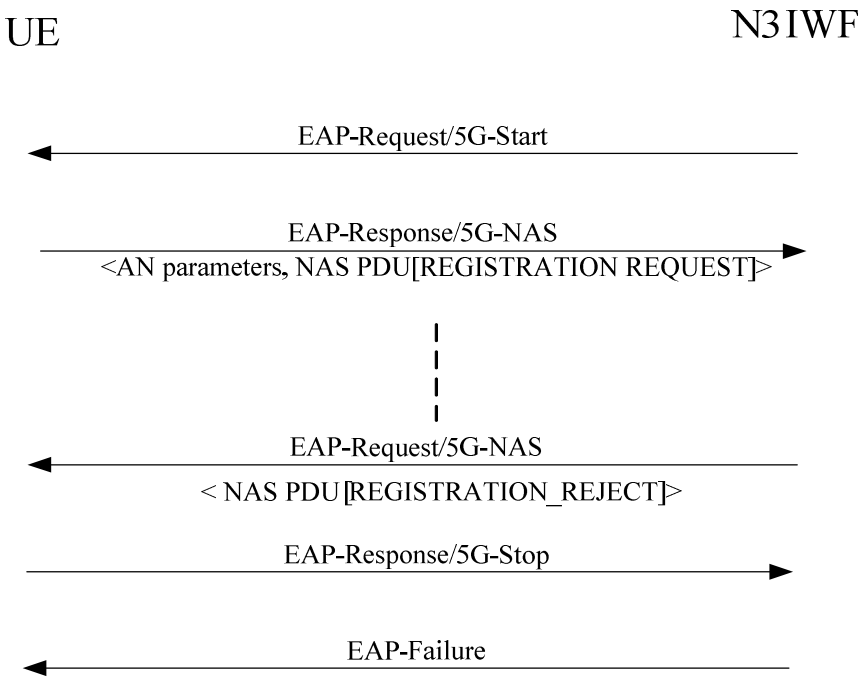

Figure 7.3.3.3-1: EAP-5G session when the UE's registration over untrusted non-3GPP access is rejected

7.3.4 Abnormal cases in the UE

Apart from the cases specified in IETF RFC 7296 [6], no abnormal cases have been identified.

7.3.5 Abnormal cases in the N3IWF

Apart from the cases specified in IETF RFC 7296 [6], no abnormal cases have been identified.

7.3A IKE SA establishment procedure for trusted non-3GPP access

7.3A.1 General

A trusted non-3GPP access network (TNAN) includes a trusted non-3GPP access point (TNAP) and a trusted non-3GPP gateway function (TNGF). The TNAN and a UE initiate an exchange of EAP-Request and EAP-Response messages including Identity as specified in IETF RFC 3748 [9] for link layer authentication of the UE by the TNAP. Upon completion of the EAP-Request/Response messages, an exchange of the EAP-5G messages are initiated once the UE receives an EAP-Request/5G-Start from the TNGF. The UE also at that time informs the upper layers that the access stratum connection is established.

An exchange of the NAS messages which are encapsulated in EAP-5G messages occur until the UE is authenticated by the 5GCN. Upon completion of the UE authentication and reception of the EAP-Success by the UE, the UE and the TNAP employs the TNAP key to establish access specific layer-2 security such as 4-way handshake in case IEEE 802.11 [19] is used between the TNAP and the UE.

Upon completion of successful establishment of access specific layer-2 security, the UE is configured with an IP address by TNAN by e.g. DHCP and the UE initiates an IKE_SA_INIT exchange as specified in IETF RFC 7296 [6].

The UE establishes the IP based secure connection by establishing an IKE SA and first child SA for NAS signalling traffic to the TNGF over NWt. Once the UE establishes the IKE SA and the signalling IPsec SA with the TNGF, the UE initiates establishment of a TCP connection for transport of NAS message with TNGF, secured using the signalling IPsec SA. The UE and the TNGF exchanges NAS messages over the TCP connection once it is established. Additional child SAs (user plane IPsec SAs) can be established to transfer user plane traffic (see subclause 7.5).

An example of an IKE SA and first child SA establishment procedure is shown in figure 7.3A.1-1.The figure illustrates that EAP messages are employed for the communication between the UE and the TNAP while the TNAP is transparent to the communication between the UE and the TNGF when employing EAP-5G messages. Link layer protocol is used to exchange these messages between the UE and the TNAN. The internal protocol used for the communications between the TNAP and the TNGF, is illustrated as dashed lines in this figure and is out of the scope of 3GPP.

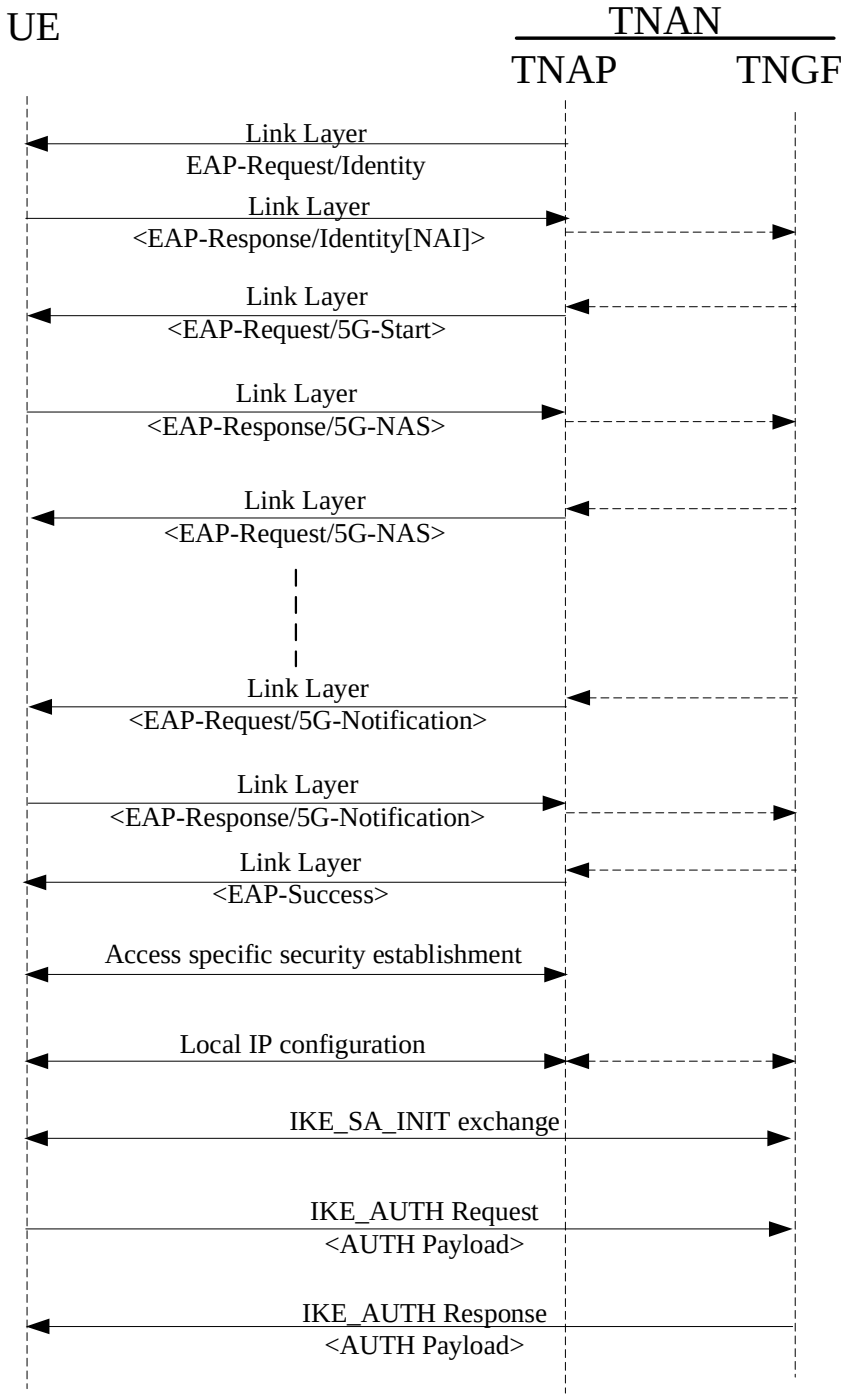

Figure 7.3A.1-1: IKE SA and first child SA establishment procedure for UE registration over trusted non-3GPP access

7.3A.2 EAP session over non-3GPP access

7.3A.2.1 General

The UE and the TNAN establishes a connection depending on the access link between the UE and the TNAP. For instance if the TNAP is a trusted WLAN access point, IEEE 802.11 [19] describes the connection between the UE and the TNAP. If the access link between the UE and the TNAP is Point-to-Point Protocol (PPP) as specified in IETF RFC 1661 [32], the Link Control Protocol (LCP) as specified in IETF RFC 1570 [33] describes the connection between the UE and the TNAP.

In the trusted non-3GPP access network:

a) the TNAP and the UE exchange EAP-request/Identity message and EAP-response/Identity message; and

b) the TNGF and the UE exchange EAP messages of EAP-5G method,

encapsulated in the link layer protocol packets such as IEEE 802.11/802.1x packets or PPP packets until successful authentication of the UE by the AMF. The link layer protocol packets are transmitted between the UE and the TNAN.

The EAP-5G method is utilized for encapsulating the NAS message to initiate the UE registration to the AMF via the TNGF. As described in subclause 7.3.3, the EAP-5G packets utilize the "Expanded" EAP type and the existing 3GPP Vendor-Id registered with IANA under the SMI Private Enterprise Code registry (i.e. 10415).

7.3A.2.2 Identity transaction

Upon reception of EAP-Request/Identity message (as described in IETF RFC 3748 [9]), encapsulated in the link layer protocol packets from the TNAP, the UE shall:

a) construct an EAP-Response/Identity message as described in IETF RFC 3748 [9] containing an NAI as specified in subclause 28.7.3 of 3GPP TS 23.003 [8] to request the PLMN with trusted 5G connectivity capability; and

b) transmit the EAP-Response of identity type encapsulated in the link layer protocol packets towards the TNAP.

7.3A.2.3 EAP-5G session initiation

The UE and the TNGF shall exchange EAP-5G messages. The TNGF on reception of the NAI by TNAP and passed on to TNGF, shall initiate EAP-5G session by sending an EAP-Request/5G-Start message. Upon reception of an EAP-Request/5G-Start message, the UE shall send an EAP-Response/5G-NAS message encapsulated in link layer protocol packets. In the EAP-Response/5G-NAS message, the UE shall include:

a) a NAS-PDU field containing a NAS message, for example, a REGISTRATION REQUEST message; and

b) an AN-parameters field containing access network parameters, such as UE identity, selected PLMN ID, requested NSSAI and establishment cause, see 3GPP TS 23.502 [3].

NOTE 1: If and how the UE includes the requested NSSAI as a part of the access type depends on the NSSAI inclusion mode IE as especified in 3GPP TS 24.501 [4].

The UE identity shall be 5GS mobile identity of type 5G-GUTI, if available, otherwise it shall be the 5GS mobile identity of type SUCI. The 5GS mobile identities of type 5G-GUTI and of type SUCI are specified in 3GPP TS 24.501 [4].

The TNGF on reception of EAP-Response/5G-NAS message, forwards the NAS message to the AMF.

NOTE 2: The TNGF is transparent to the NAS messages and as an intermediate network entity only conveys transparently the NAS messages to the AMF.

The TNAN, on reception of the NAS messages from the AMF, shall send an EAP-Request/5G-NAS message encapsulated in the link layer protocol packets towards the UE via the TNAP.

The EAP-Request/5G-NAS message shall include a NAS-PDU field that contains a NAS message. Further NAS messages between the UE and the AMF, via the TNGF, shall be inserted in NAS-PDU field of an EAP-Response/5G-NAS (UE to TNGF direction) and EAP-Request/5G-NAS (TNGF to UE direction) message.

The UE, on reception of the EAP-Request/5G-NAS message including a NAS-PDU field containing a NAS message e.g. for security establishment, shall send a response with EAP-Response/5G-NAS message including a NAS-PDU field containing a NAS message related to the NAS security context to the TNGF.

The TNGF, on reception of the TNGF key shall construct an EAP-Request/5G-Notification message that includes an AN-parameters field containing the access network parameters, such as TNGF IPv4 contact information, TNGF IPv6 contact information, or both, see 3GPP TS 23.502 [3]. The TNGF shall send the EAP-Request/5G-Notification message encapsulated in the link layer protocol packets towards the UE via the TNAP. The UE shall acknowledge by sending an EAP-Response/5G-Notification message encapsulated in the link layer protocol packets.

7.3A.2.4 EAP-5G session completion initiated by the network

Upon completion of successful authentication and on reception of the acknowledgement from the UE that it had received the access network parameters, the TNAN shall send an EAP-Success message encapsulated in the link layer protocol packets towards the UE via the TNAP.

7.3A.2.5 EAP-5G session completion initiated by the UE

For trusted non-3GPP access, the procedure for when the EAP-5G session completion initiated by the UE, is the same as that of untrusted non-3GPP access as described in subclause 7.3.3.3 with the difference that the N3IWF shall be replaced by the TNGF.

7.3A.3 IKE SA and signalling IPsec SA establishment procedure

7.3A.3.1 IKE SA and signalling IPsec SA establishment initiation

In a trusted non-3GPP access network, once the EAP- 5G authentication is successfully complete and the UE is configured with a local IP address, the UE shall use the TNGF IP address received in the EAP-Request/5G-Notification message (see subclause 7.3A.2.3) to establish a secure connection between the UE and the TNGF over NWt to exchange NAS signalling messages with the AMF. The UE shall establish the secure connection by establishing an IKE SA and signalling IPsec SA (first child SA) by initiating the IKE_SA_INIT exchange and then IKE_AUTH exchange for mutual authentication with the TNGF and NULL encryption as specified in IETF RFC 2410 [34]. The UE shall set the IDi payload of the IKE_AUTH request message in the IKE_AUTH exchange (see IETF RFC 7296 [6]) to the NAI format of 5G-GUTI or the NAI format of SUCI as specified in 3GPP TS 23.003 [8], depending on the employed UE identity in the EAP-Response/5G-NAS message at the time of EAP-5G session initiation according to subclause 7.3A.2.3.

7.3A.3.2 IKE SA and signalling IPsec SA establishment accepted by the network

The UE shall establish the IKE SA and signalling IPsec SA (first child SA) according to subclause 7.3.2.2 with the difference that the N3IWF is replaced by the TNGF.

Upon completion of the IKE SA and signalling IPsec SA (first child SA) establishment between the UE and the TNGF, the UE and the TNGF shall send further NAS messages over the TCP connection within the signalling IPsec SA (first child SA).

7.3A.3.3 IKE SA and signalling IPsec SA establishment not accepted by the network

For trusted non-3GPP access, the procedure for when the IKE SA and signalling IPsec SA establishment are not accepted by the network, is the same as that of the untrusted non-3GPP access as described in subclause 7.3.2.3 with the difference that the N3IWF shall be replaced by the TNGF.

7.3A.4 Procedure for devices without NAS support

7.3A.4.1 General

A trusted non-3GPP access network (TNAN) may be implemented as a trusted WLAN access network (TWAN) which supports a WLAN access technology such as the one described in IEEE 802.11 [19]. A non 5G capable over WLAN (N5CW) device does not support 5G NAS signalling over WLAN, but may access 5GCN via a TWAN supporting a

trusted WLAN interworking function (TWIF). An N5CW device may be a 5G UE with capability for 5G NAS signalling over 3GPP access although it lacks capability of NAS signalling over WLAN.

7.3A.4.2 N5CW device registration over trusted WLAN access network

A trusted WLAN access network (TWAN) includes a trusted WLAN access point (TWAP) and a trusted WLAN interworking function (TWIF) as illustrated in figure 7.3A.4.2-1.

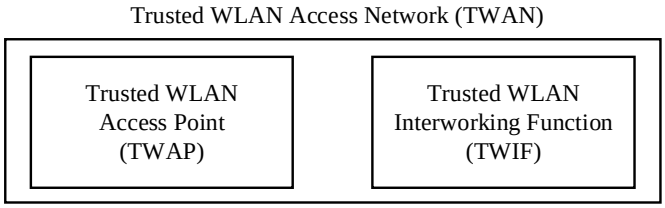

Figure 7.3A.4.2-1: Trusted WLAN Access Network

The EAP-AKA' authentication procedure is executed for connecting the N5CW device to a TWAN according to 3GPP TS 33.501 [5].

The TWAN and an N5CW device initiate an exchange of EAP-Request/Identity message and EAP-Response/Identity message as specified in IETF RFC 3748 [9] for link layer authentication of the UE by the TWAP. In the trusted WLAN access network, the TWAP and the N5CW device exchange EAP-Request/Identity message and EAP-Response/Identity message, encapsulated in the link layer protocol packets i.e. IEEE 802.11/802.1x packets.

Upon reception of EAP-Request/Identity message encapsulated in the IEEE 802.11/802.1x packets from the TWAP, the N5CW device shall:

a) construct an EAP-Response/Identity message as described in IETF RFC 3748 [9] containing an NAI as specified in subclause 28.7 of 3GPP TS 23.003 [8] to Request the PLMN with trusted 5G connectivity without NAS signalling capability; and

NOTE 1: The NAI includes the 5G-GUTI assigned to the N5CW device over 3GPP access, if the N5CW device is also a 5G UE and is already registered to 5GCN over 3GPP access.

b) transmit the EAP-Response of identity type encapsulated in the link layer protocol packets towards the TWAP.

The TWAP conveys the information provided by the N5CW device to the TWIF which initiates the registration and the PDU session establishment to obtain an IP address, on behalf of the N5CW device to an AMF according to 3GPP TS 24.501 [4].

NOTE 2: The communication protocol between the TWAP and the TWIF is outside of the scope of 3GPP.

An exchange of the EAP request and EAP response as described in IETF RFC 3748 [9] occurs until the N5CW device is authenticated by the 5GCN with the EAP authentication described in 3GPP TS 33.501 [5]. Upon completion of the N5CW device authentication and reception of the EAP-Success by the N5CW device, the N5CW device and the TWAP use the TWAP key to establish access specific layer-2 security 4-way handshake according to IEEE 802.11 [19].

7.4 IKEv2 SA deletion procedure

7.4.1 General

The purpose of the IKE SA deletion procedure via untrusted non-3GPP access and trusted non-3GPP access is to close the IKE SA between the UE and the N3IWFfor untrusted non-3GPP access and the TNGF for trusted non-3GPP access. In addition, deleting the IKE SA implicitly closes any remaining signalling IPsec child SAs and user plane IPsec child SAs associated with IKE SA.

This procedure shall be initiated either by the N3IWF, TNGF or by the UE.

The N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access initiate this procedure in the following cases:

a) N1 NAS signalling connection release;

b) N3IWF-initiated and TNGF-initiated IKE SA rekeying procedure failure;

c) N3IWF-initiated and TNGF-intiated IKE SA rekeying procedure completion

d) upon receipt of an INITIAL_CONTACT notification as specified in IETF RFC 7296 [6]; and

e) upon detecting an error in a response packet as specified in IETF RFC 7296 [6].

The UE initiates this procedure in the following cases:

a) UE-initiated IKE SA rekeying procedure failure;

b) UE-initiated IKE SA rekeying procedure completion;

c) upon receipt of an INITIAL_CONTACT notification as specified in IETF RFC 7296 [6]; and

d) upon detecting an error in a response packet as specified in IETF RFC 7296 [6].

7.4.2 IKE SA deletion procedure initiated by the N3IWF and the TNGF

7.4.2.1 IKE SA deletion initiation

The N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall initiate the IKE SA deletion procedure by sending an INFORMATIONAL request message including a Delete payload to the UE as specified in IETF RFC 7296 [6].

The Delete payload shall be defined with the Protocol ID set to "1" and no SPIs included in the Security Parameter Index field in the Delete payload. This indicates that the IKE security association and all IPsec ESP security associations that were negotiated within the IKE security association between:

a) the N3IWF for untrusted non-3GPP access; and

b) the TNGF for trusted non-3GPP access;

and the UE shall be deleted.

7.4.2.2 IKE SA deletion accepted by the UE

Upon reception of the INFORMATIONAL request message from the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access for deletion of the IKE SA, if the UE accepts the IKE SA deletion request, the UE shall send an empty INFORMATIONAL response message to the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access as specified in IETF RFC 7296 [6].

After sending the empty INFORMATIONAL response message, the UE shall close IKE SA and delete all IPsec child SAs associated with the IKE SA. In addition, the UE shall inform the upper layers that the access stratum connection has been released.

Upon receiving the empty INFORMATIONAL response message, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall close IKE SA and delete all IPsec child SAs associated with the IKE SA. In addition, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall inform the AMF that the access stratum connection has been released.

7.4.2.3 Abnormal cases in the N3IWF and the TNGF

If the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access does not receive any empty INFORMATIONAL response message from the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA. In addition, the N3IWF for untrusted non-3GPP access and the TNGF for untrusted non-3GPP access shall inform the AMF that the access stratum connection has been released.

7.4.3 IKE SA deletion procedure initiated by the UE

7.4.3.1 IKE SA deletion initiation

The UE shall initiate the IKE SA deletion procedure by sending an INFORMATIONAL request message including a Delete payload to the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access as specified in IETF RFC 7296 [6].

The Delete payload shall be defined with the Protocol ID set to "1" and no SPIs included in the Security Parameter Index field in the Delete payload. This indicates that the IKE security association and all IPsec ESP security associations that were negotiated within the IKE security association between:

a) the N3IWF for untrusted non-3GPP access; and

b) the TNGF for trusted non-3GPP access;

and the UE shall be deleted.

7.4.3.2 IKE SA deletion accepted by the N3IWF and the TNGF

Upon reception of the INFORMATIONAL request message from the UE for deletion of the IKE SA, if the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access accepts the IKE SA deletion request, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall send an empty INFORMATIONAL response message to the UE as specified in IETF RFC 7296 [6].

After sending the empty INFORMATIONAL response message, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall close the IKE SA and delete all IPsec child SAs associated with the IKE SA. In addition, the N3IWF for untrusted non-3GPP access and theTNGF for trusted non-3GPP access shall inform the AMF that the access stratum connection has been released.

Upon receiving the empty INFORMATIONAL response message, the UE shall close the IKE SA and delete all IPsec child SAs associated with the IKE SA. In addition, the UE shall inform the upper layers that the access stratum connection has been released.

7.4.3.3 Abnormal cases in the UE

If the UE does not receive any empty INFORMATIONAL response message from the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access, the UE shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA. In addition, the UE shall inform the upper layers that the access stratum connection has been released.

7.5 User plane IPsec SA creation procedure

7.5.1 General

The purpose of the user plane IPsec SA creation procedure is to establish a child SA associating to the QoS flows of the PDU session. This procedure shall be initiated by the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access.

One user plane IPsec SA can be associated with one or more QoS flows of the PDU session. During PDU session establishment or PDU session modification via:

a) untrusted non-3GPP access, the N3IWF; or

b) trusted non-3GPP access, the TNGF,

shall determine the number of user plane IPsec child SAs to establish and the QoS profiles associated with each child SA based on local policies, configuration and the QoS profiles received from the network.

7.5.2 Child SA creation procedure initiation

The N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall initiate the child SA creation procedure by sending a CREATE_CHILD_SA request message to the UE as specified in IETF RFC 7296 [6].

The CREATE_CHILD_SA request message shall include:

a) a UP_IP4_ADDRESS notify payload or a UP_IP6_ADDRESS notify payload; and

b) 5G_QOS_INFO Notify payload as specified in subclause 9.3.1.1, which contains:

   1) PDU session ID;

   2) zero or more QFIs;

   3) optionally a DSCP value;

   4) optionally an indication of whether the child SA is the default child SA. For a given PDU session ID, there can be only up to one child SA which is the default child SA; and

   5) if trusted non-3GPP access, Additional QoS Information or if untrusted non-3GPP access, optionally Additional QoS Information.

The IKE CREATE_CHILD_SA request message also contains the SA payload for the requested child SA.

7.5.3 Child SA creation procedure accepted by the UE

If the UE accepts the CREATE_CHILD_SA request message with a 5G_QOS_INFO Notify payload:

a) the UE shall send a CREATE_CHILD_SA response message as specified in IETF RFC 7296 [6]; and

b) the UE shall associate the created child SA with the:

   1) PDU session ID;

   2) zero or more QFIs (if indicated);

   3) DSCP value (if indicated); and

   4) indication of whether the child SA is the default child SA (if indicated);

in the 5G_QOS_INFO Notify payload; and

c) the UE:

   1) in case of trusted non-3GPP access, shall reserve non-3GPP access QoS resources for the created child SA based on the received Additional QoS Information; or

   2) in case of untrusted non-3GPP access, may reserve non-3GPP access QoS resources for the created child SA if the UE has received Additional QoS Information.

Any IKEv2 Notify payload indicating an error shall not be included in the CREATE_CHILD_SA response message.

7.5.4 Child SA creation procedure not accepted by the UE

If a user plane IPsec SA establishment for a PDU session is not accepted by the UE, the UE shall send a CREATE_CHILD_SA response message to the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access with a Notify payload with error type.

If the UE fails to reserve QoS resources over non-3GPP access for the QoS flows associated with the child SA according to the Additional QoS information in the 5G_QOS_INFO Notify payload, the UE shall include a Notify payload with a Private Notify Message Error Type "NO_RESOURCES_OVER_N3GPP" as defined in subclause 9.2.4.2 in the CREATE_CHILD_SA response message.

Upon receiving the CREATE_CHILD_SA response message with a Notify payload of error type:

- if PDU session establishment over non-3GPP access requires single user plane SA IPsec SA creation, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall stop user plane SA IPsec SA creation procedure and indicate the failure for PDU session establishment over non-3GPP access.

- if PDU session establishment over non-3GPP access requires multiple user plane SA IPsec SA creation, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access may choose to continue user plane SA IPsec SA creation procedure for other user plane IPsec SAs, or stop user plane SA IPsec SA creation procedure and indicate the failure for PDU session establishment over non-3GPP access.

If the CREATE_CHILD_SA request message contains a USE_TRANSPORT_MODE notification, the UE shall decline the request by not including USE_TRANSPORT_MODE notification as specified in IETF RFC 7296 [6].

7.5.5 Abnormal cases in the UE

Apart from the cases specified in IETF RFC 7296 [6], no abnormal cases have been identified.

7.5.6 Abnormal cases in the N3IWF and the TNGF

Apart from the cases specified in IETF RFC 7296 [6], no abnormal cases have been identified.

7.6 IPsec SA modification procedure

7.6.1 General

The user plane IPsec child SA modification procedure is to update a child SA associating to the QoS flows of the PDU session. The procedure may be initiated by the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access. The IPsec child SA modification may be accepted or rejected by the UE.

7.6.2 N3IWF and TNGF procedure for IPsec child SA modification

The N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall perform the IPsec child SA modification by sending an INFORMATIONAL request message as specified in IETF RFC 7296 [6] to the UE with an 5G_QOS_INFO Notify payload indicating modified content associated with the IPsec child SA.

7.6.3 UE procedure for IPsec child SA modification

Upon receipt of an INFORMATIONAL request message containing an 5G_QOS_INFO Notify payload:

a) if the content of the 5G_QOS_INFO Notify payload is accepted by the UE, the UE shall:

   i) send an empty INFORMATIONAL response message to the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access to acknowledge the reception of the INFORMATIONAL request message; and

   ii) update locally the IPsec child SA according to the content of the INFORMATIONAL request message; or

b) if the content of the 5G_QOS_INFO Notify payload is not accepted by the UE, the UE shall:

   i) send the reason for rejecting the IPsec SA modification in the content of an INFORMATIONAL response message; and

   ii) not update locally the IPsec child SA according to the content of the INFORMATIONAL request message.

If the UE fails to reserve QoS resources over non-3GPP access for the QoS flows associated with the child SA according to the Additional QoS information in the 5G_QOS_INFO Notify payload, the UE shall include a Notify Payload with a Private Notify Message Error Type "NO_RESOURCES_OVER_N3GPP" as defined in clause 9.2.4.2 in the INFORMATIONAL response message.

7.7 IPSec SA deletion procedure

7.7.1 General

The purpose of the child SA deletion procedure for PDU session release is to delete all the child SAs associated with the PDU session. This procedure shall be initiated either by the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access or by the UE.

The N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access initiates this procedure in the following cases:

a) upon PDU session release;

b) N3IWF-initiated and TNGF-intiated IPsec SA rekeying procedure failure;

c) N3IWF-initiated and TNGF-intiated IPsec SA rekeying procedure completion; and

d) upon detecting an error in a response packet as specified in IETF RFC 7296 [6].

The UE initiates this procedure in the following cases:

a) UE-initiated IPsec SA rekeying procedure failure;

b) UE-initiated IPsec SA rekeying procedure completion; and

c) upon detecting an error in a response packet as specified in IETF RFC 7296 [6].

7.7.2 N3IWF-initated and TNGF-initiated child SA deletion procedure

7.7.2.1 N3IWF-initiated and TNGF-initiated child SA deletion procedure initiation

The N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall initiate the child SA deletion procedure by sending an INFORMATIONAL request message including a Delete payload to the UE as specified in IETF RFC 7296 [6]. The Delete payload shall include:

a) the Protocol ID set to "3" for ESP; and

b) all the N3IWF's ESP SPI(s) for untrusted non-3GPP access and all the TNGF's EPS SPI(s) for trusted non-3GPP access, associated to the released PDU session.

7.7.2.2 N3IWF-initiated and TNGF-initiated child SA deletion procedure accepted by the UE

If the UE accepts the INFORMATIONAL request message for deletion of the child SAs, the UE shall send the INFORMATIONAL response message to the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access including the Delete payload received in the corresponding INFORMATIONAL request message as specified in IETF RFC 7296 [6].

Any IKEv2 Notify payload indicating an error shall not be included in the INFORMATIONAL response message.

7.7.2.3 Abnormal cases in the N3IWF and the TNGF

If the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access does not receive any INFORMATIONAL response message including a Delete payload from the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA. In addition, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall inform the AMF that the access stratum connection has been released.

7.7.3 UE-initiated child SA deletion procedure

7.7.3.1 UE-initiated child SA deletion procedure initiation

The UE shall initiate the child SA deletion procedure by sending an INFORMATIONAL request message including a Delete payload as specified in IETF RFC 7296 [6], to the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access. The Delete payload shall include:

a) the Protocol ID set to "3" for ESP; and

b) all the UE's ESP SPI(s) associated to the released PDU session.

7.7.3.2 UE-initiated child SA deletion procedure accepted by the N3IWF and the TNGF

If the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access accepts the INFORMATIONAL request message for deletion of the child SAs, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall send the INFORMATIONAL response message to the UE including the Delete payload received in the corresponding INFORMATIONAL request message as specified in IETF RFC 7296 [6].

Any IKEv2 Notify payload indicating an error shall not be included in the INFORMATIONAL response message.

7.7.3.3 Abnormal cases in the UE

If the UE does not receive any INFORMATIONAL response message including a Delete payload from the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access, the UE shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA. In addition, the UE shall inform the upper layers that the access stratum connection has been released.

7.7.4 Abnormal cases in the UE

Apart from the cases specified in IETF RFC 7296 [6] and subclause 7.7.3.3, no abnormal cases have been identified.

7.7.5 Abnormal cases in the N3IWF and the TNGF

Apart from the cases specified in IETF RFC 7296 [6] and subclause 7.7.2.3, no abnormal cases have been identified.

7.8 UE-initiated liveness check procedure

7.8.1 General

The UE-initiated liveness check procedure enables the UE to detect whether the N3IWF for untrusted non-3GPP access and the TNGFfor trusted non-3GPP access is alive.

7.8.2 UE-initiated liveness check procedure initiation

If the UE supports the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in 3GPP TS 24.302 [7] subclause 8.2.4.2 and the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in 3GPP TS 24.302 [7] subclause 8.2.4.2 was included in the CFG_REPLY configuration payload within the IKE_AUTH response message received in subclause 7.3 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 3GPP TS 24.302 [7] subclause 8.2.4.2 or the TIMEOUT_PERIOD_FOR_LIVENESS_CHECK attribute as specified in 3GPP TS 24.302 [7] subclause 8.2.4.2 was not included in the CFG_REPLY configuration payload within the IKE_AUTH response message received in subclause 7.3, then 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 7296 [6].

7.8.3 UE-initiated liveness check procedure completion

The N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall handle the INFORMATIONAL request with no payloads as per IETF RFC 7296 [6] and shall send an INFORMATIONAL response.

If an INFORMATIONAL response is received, the UE shall consider the UE-initiated liveness check procedure as successfully completed.

7.8.4 Abnormal cases

If an INFORMATIONAL response is not received, the UE shall deem the IKEv2 security association to have failed.

The UE shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA as specified in IETF RFC 7296 [6]. In addition, the UE shall inform the upper layers that the access stratum connection has been released.

7.9 Network-initiated liveness check procedure

7.9.1 General

The network-initiated liveness check procedure enables the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access to detect whether the UE is alive.

7.9.2 Network-initiated liveness check procedure initiation

If the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access 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 N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall send an INFORMATIONAL request with no payloads IETF RFC 7296 [6].

7.9.3 Network-initiated liveness check procedure completion

The UE shall handle the INFORMATIONAL request with no payloads as per IETF RFC 7296 [6] and shall send an INFORMATIONAL response.

If an INFORMATIONAL response is received, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall consider the liveness check procedure as successfully completed.

7.9.4 Abnormal cases

If an INFORMATIONAL response is not received, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall deem the IKEv2 security association to have failed.

The N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA as specified in IETF RFC 7296 [6]. In addition, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall inform the AMF that the access stratum connection has been released.

7.10 IKE SA rekeying procedure

7.10.1 General

The N3IWF for untrusted non-3GPP access, the TNGF for trusted non-3GPP access and the UE may support the IKE SA rekeying procedure as specified in IETF RFC 7296 [6]. If the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access and the UE support the IKE SA rekeying procedure, the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall proactively rekey the IKE SA. Upon rekeying of an IKE SA, the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall maintain the old SA for the incoming data while establishing the new one. The old SA shall be deleted upon the completion of the establishment of the new one by both the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access. The UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access are separately responsible for enforcing their time expiration policies to rekey the SA when needed. IETF RFC 7296 [6] describes how to avoid the simultaneous IPsec SA and IKE SA rekeying.

7.10.2 N3IWF-initiated and TNGF-initiated IKE SA rekeying procedure

7.10.2.1 N3IWF-initiated and TNGF-initiated IKE SA rekeying procedure initiation

The N3IWF for untrusted non-3GPP access, the TNGF for trusted non-3GPP access shall initiate the IKE SA rekeying procedure by sending a CREATE_CHILD_SA request message with a REKEY_SA Notify payload indicating an N3IWF's SPI for untrusted non-3GPP access or an TNGF's SPI for trusted non-3GPP access.

7.10.2.2 N3IWF-initiated and TNGF-initiated IKE SA rekeying procedure completion

Upon reception of the CREATE_CHILD_SA request message in the IKE SA with a REKEY_SA Notify payload indicating an N3IWF's SPI for untrusted non-3GPP access or an TNGF's SPI for trusted non-3GPP access, if the UE accepts the IKE SA rekeying request, the UE shall send a CREATE_CHILD_SA response message without an IKEv2 notify payload indicating an error, shall set the UE's SPI to the SPI created by the CREATE_CHILD_SA request/response pair and shall set:

a) the N3IWF's SPI for untrusted non-3GPP access to the N3IWF’s SPI; or

b) the TNGF's SPI for trusted non-3GPP access to the TNGF’s SPI;

created by the CREATE_CHILD_SA request/response pair.

7.10.2.3 Abnormal cases

If the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access receive a CREATE_CHILD_SA response message with an IKEv2 notify payload indicating an error from the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall delete the IKE SA and any associated child SAs as specified in subclause 7.4.

If the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access do not receive any CREATE_CHILD_SA response message from the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA. In addition, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall inform the AMF that the access stratum connection has been released.

7.10.3 UE-initiated IKE SA rekeying procedure

7.10.3.1 UE-initiated IKE SA rekeying procedure initiation

The UE shall initiate the IKE SA rekeying procedure by sending a CREATE_CHILD_SA request message with a REKEY_SA Notify payload indicating a UE's SPI.

7.10.3.2 UE-initiated IKE SA rekeying procedure completion

Upon reception of the CREATE_CHILD_SA request message in the IKE SA with a REKEY_SA Notify payload indicating a UE's SPI, if the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access accept the IKE SA rekeying request, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall send a CREATE_CHILD_SA response message without an IKEv2 notify payload indicating an error, shall set the N3IWF's SPI for untrusted non-3GPP access and the TNGF's SPI for trusted non-3GPP access to the SPI created by the CREATE_CHILD_SA request/response pair and shall set the UE's SPI to the UE's SPI created by the CREATE_CHILD_SA request/response pair.

7.10.3.3 Abnormal cases

If the UE receives a CREATE_CHILD_SA response message with an IKEv2 notify payload indicating an error from the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access, the UE shall delete the IKE SA and any associated child SAs as specified in subclause 7.4.

If the UE does not receive any CREATE_CHILD_SA response message from the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access, the UE shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA. In addition, the UE shall inform the upper layers that the access stratum connection has been released.

7.11 IPsec SA rekeying procedure

7.11.1 General

The N3IWF for untrusted non-3GPP access, the TNGF for trusted non-3GPP access and the UE may support the IPsec SA rekeying procedure as specified in IETF RFC 7296 [6]. If the N3IWF for untrusted non-3GPP access, the TNGF for trusted non-3GPP access and the UE support the IPsec SA rekying procedure, the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall proactively rekey the IPsec SA. Upon rekeying of an IPsec SA, the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall maintain the old IPsec for the incoming data while establishing the new one. The old IPsec shall be deleted upon the completion of the establishement of the new one by the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access. The UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access are separately responsible for enforcing their time expiration policies to rekey the IPsec when needed. IETF RFC 7296 [6] describes how to avoid the simultaneous IPsec SA and IKE SA rekeying.

7.11.2 N3IWF-initiated and TNGF-initiated IPsec SA rekeying procedure

7.11.2.1 N3IWF-initiated and TNGF-initiated IPsec SA rekeying procedure initiation

The N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall initiate the IPsec SA rekeying procedure by sending a CREATE_CHILD_SA request message with a REKEY_SA Notify payload including a Protocol ID set to "3" and the N3IWF's ESP SPI for untrusted non-3GPP access and the TNGF's ESP SPI for trusted non-3GPP access for the IPsec SA.

7.11.2.2 N3IWF-initiated and TNGF-initiated IPsec SA rekeying procedure completion

Upon reception of the CREATE_CHILD_SA request message with a REKEY_SA Notify payload including a Protocol ID set to "3" and the N3IWF's ESP SPI for untrusted non-3GPP access or the TNGF's ESP SPI for trusted non-3GPP access for the IPsec SA, if the UE accepts the IPsec SA rekeying request, the UE shall send a CREATE_CHILD_SA response message without an IKEv2 notify payload indicating an error, shall set the UE's ESP SPI to the ESP SPI created by the CREATE_CHILD_SA request/response pair and shall set;

a) the N3IWF's ESP SPI for untrusted non-3GPP access; or

b) the TNGF's ESP SPI for trsuted non-3GPP access;

to the N3IWF's ESP SPI created by the CREATE_CHILD_SA request/response pair.

7.11.2.3 Abnormal cases

If the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access receive a CREATE_CHILD_SA response message with an IKEv2 notify payload indicating an error from the UE, the N3IWF shall delete the IPsec SA as specified in subclause 7.7. Additionally, if the IPsec SA is the signalling IPsec SA, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall delete the IKE SA as specified in subclause 7.4.

If the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access do not receive any CREATE_CHILD_SA response message from the UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA. In addition, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall inform the AMF that the access stratum connection has been released.

7.11.3 UE-initiated IPsec SA rekeying procedure

7.11.3.1 UE-initiated IPsec SA rekeying procedure initiation

The UE shall initiate the IPsec SA rekeying procedure by sending a CREATE_CHILD_SA request message with a REKEY_SA Notify payload including a Protocol ID set to "3" and the UE's ESP SPI for the IPsec SA.

7.11.3.2 UE-initiated IPsec SA rekeying procedure completion

Upon reception of the CREATE_CHILD_SA request message with a REKEY_SA Notify payload including a Protocol ID set to "3" and the UE's ESP SPI for the IPsec SA, if the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access accept the IPsec SA rekeying request, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall send a CREATE_CHILD_SA response message without an IKEv2 notify payload indicating an error, shall set:

a) the N3IWF's ESP SPI for untrusted non-3GPP access; and

b) the TNGF's ESP SPI for trusted non-3GPP access;

to the ESP SPI created by the CREATE_CHILD_SA request/response pair and shall set the UE's ESP SPI to the UE's ESP SPI created by the CREATE_CHILD_SA request/response pair.

7.11.3.3 Abnormal cases

If the UE receives a CREATE_CHILD_SA response message with an IKEv2 notify payload indicating an error from the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access, the UE shall delete the IPsec SA as specified in subclause 7.7. Additionally, if the IPsec SA is the signalling IPsec SA, the UE shall delete the IKE SA as specified in subclause 7.4.

If the UE does not receive any CREATE_CHILD_SA response message from the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access, the UE shall discard all states associated with the IKE SA and any child SAs that were negotiated using that IKE SA. In addition, the UE shall inform the upper layers that the access stratum connection has been released.

7A EAP-5G session over wireline access

7A.1 General

A vendor-specific EAP method (EAP-5G) is used to encapsulate NAS messages between the 5G-RG and the W-AGF serving the 5G-RG. The EAP-5G packets utilize the "Expanded" EAP type and the existing 3GPP Vendor-Id registered with IANA under the SMI Private Enterprise Code registry (i.e. 10415). The EAP-5G method is utilized only for encapsulating the NAS messages. The EAP-5G method is not utilized to authenticate the 5G-RG in wireline access network.

7A.2 EAP-5G session initiation

The 5G-RG and the W-AGF serving the 5G-RG shall exchange EAP-5G messages via W-CP EAP connection. The W-AGF on reception of a W-CP EAP connection establishment shall start an EAP-5G session by sending an EAP-Request/5G-Start message.

The 5G-RG acknowledges start of the EAP-5G session by sending an EAP-Response/5G-NAS message which shall include:

a) a NAS-PDU field containing a NAS message, for example, a REGISTRATION REQUEST message; and

b) an AN-parameters field containing access network parameters, such as GUAMI, selected PLMN ID, requested NSSAI and establishment cause (see 3GPP TS 23.502 [3]).

NOTE 1: If and how the UE includes the requested NSSAI as a part of the access type depends on the NSSAI inclusion mode IE as specified in 3GPP TS 24.501 [4].

The W-AGF, on reception of NAS messages from the 5G-RG within an EAP-Response/5G-NAS message, shall forward the NAS message to the AMF.

The W-AGF, on reception of NAS messages from the AMF, shall include the NAS message within an EAP-Request/5G-NAS message. The W-AGF shall transmit the EAP-Request/5G-NAS message to the 5G-RG.

NOTE 2: The W-AGF is transparent to the NAS messages and as an intermediate network entity only conveys transparently the NAS messages between the 5G-RG and the AMF.

The EAP-Request/5G-NAS message shall include a NAS-PDU field that contains a NAS message.

Further NAS messages between the 5G-RG and the AMF, via the W-AGF, shall be inserted in NAS-PDU field of an EAP-Response/5G-NAS (5G-RG to W-AGF direction) and EAP-Request/5G-NAS (W-AGF to 5G-RG direction) message.

7A.3 EAP-5G session completion initiated by the network

Upon completion of successful authentication and on reception of the W-AGF key from the AMF, the W-AGF serving the 5G-RG shall complete the EAP-5G session by sending an EAP-Success message.

On reception of the EAP-Success message from the W-AGF, the 5G-RG proceeds as specified in subclause 8.2.1.

An example of an EAP-5G session after successful authentication is shown in figure 7A.3-1.

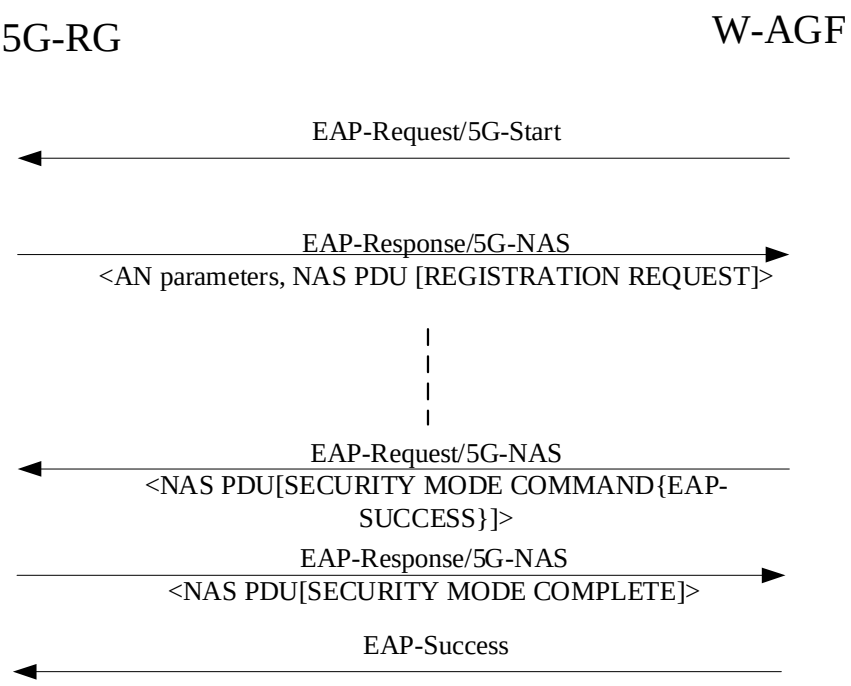

Figure 7A.3-1: EAP-5G session for successful 5G-RG registration over wireline access

7A.4 EAP-5G session completion initiated by the 5G-RG

Upon receiving indication from the upper layer that no 5G-NAS messages need to be transmitted between the 5G-RG and W-AGF, the 5G-RG shall terminate the EAP-5G session by sending an EAP-Response/5G-Stop message to the W-AGF.

On reception of EAP-Response/5G-Stop message, the W-AGF shall complete the EAP-5G session by sending an EAP-Failure message to the 5G-RG.

8 Message transport procedures

8.1 General

In trusted and untrusted non-3GPP access, the UE establishes IKE SA and signalling IPsec SA i.e. the first child SA for NAS message exchange. Thereafter the UE establishes other child SAs for exchange of the user data packets. IPsec tunnel mode is employed for all the established child SAs including the first child SA for the signalling, to protect and encrypt the original IP user data packets, the original IP signalling packets and the port numbers used for communications of such IP packets. This clause is to list the parameters and the procedures for such IP tunneling mode of the signalling IPsec SA and the user data child SAs.

In wireline access, the 5G-RG establishes W-CP signalling connection as described in clause 7A. Thereafter the W-AGF serving the 5G-RG and the 5G-RG establish W-UP bearers for exchange of the user data packets as specified in subclause 4.4.2.2.

8.2 Transport of NAS messages over control plane

8.2.1 General

In trusted and untrusted non-3GPP access, after the completion of IKE SA and establishment of signalling IPsec SA as specified in subclause 7.3 for untrusted non-3GPP access and subclause 7.3A for trusted non-3GPP access, the UE establishes with the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access a TCP connection for transport of NAS messages over the inner IP layer and the signalling IPsec SA as specified in subclause 8.2.3. Once the TCP connection for transport of NAS messages is established, the UE performs NAS procedures over the TCP connection for transport of NAS messages. All uplink and downlink NAS mobility management messages and NAS session management messages are relayed between the UE and the AMF via N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access using the TCP connection for transport of NAS messages as specified in subclause 8.2.4. Once the TCP connection is established and upon detection of a TCP connection failure, the UE and the N3IWF for untrusted non-3GPP access or the UE and the TNGF for trusted non-3GPP access re-establish the TCP connection as specified in subclause 8.2.3A. When the TCP connection for transport of NAS messages is no longer needed, the UE, the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access release the TCP connection as specified in subclause 8.2.5.

In wireline access, after completion of EAP-5G authentication as specified in clause 7A, all uplink and downlink NAS mobility management messages and NAS session management messages are relayed between the 5G-RG and the AMF via W-AGF serving the 5G-RG using the W-CP signalling connection without EAP-5G encapsulation. Transport using the W-CP signalling connection is out of scope of the present document.

8.2.2 TCP packet encapsulation

NOTE 1: This subclause is used for encapsulating of TCP packets when establishing TCP connection as described in subclause 8.2.3, when re-establishing TCP connection as described in subclause 8.2.3A, when transporting NAS messages over TCP connection as described in subclause 8.2.4, and when releasing TCP connection as described in subclause 8.2.5.

If a TCP packet is transported between the UE and the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access, and:

a) if the IKE_AUTH response message contained the INTERNAL_IP4_ADDRESS attribute and the NAS_IP4_ADDRESS notify payload, an inner IPv4 datagram shall be constructed where:

   1) the TCP packet shall be encapsulated in the inner IPv4 datagram with IPv4 header where:

      A) if the UE constructs the inner IPv4 datagram:

         - the source address field shall be set to the IPv4 address in the INTERNAL_IP4_ADDRESS attribute;
         - the destination address field shall be set to the IPv4 address in the NAS_IP4_ADDRESS notify payload; and
         - the destination port number shall be set to the NAS_TCP_PORT notify payload;

      B) if the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access constructs the inner IPv4 datagram:

         - the source address field shall be set to the IPv4 address in the NAS_IP4_ADDRESS notify payload;
         - the source port number shall be set to the NAS_TCP_PORT notify payload;
         - the destination address field shall be set to the IPv4 address in the INTERNAL_IP4_ADDRESS attribute; and
         - the destination port number shall be set to the UE's TCP port number; and

NOTE 2: Since the UE always initiates the NAS message exchange with the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access receive the UE's TCP port number in the TCP SYN packet exchange and use it when sending NAS messages towards the UE or when re-establishing the TCP connection upon failure.

C) the protocol field shall be set to 06H;

2) the inner IPv4 datagram shall be protected employing the ESP protocol in tunnel mode as specified in IETF RFC 4303 [11] where:

A) the SPI field in the ESP packet shall be set to the SPI of the signalling IPsec SA; and

B) the next header field in the ESP packet shall be set to 04H; and

3) the IP packet encapsulating the ESP protected inner IPv4 datagram shall be sent to the peer for the SPI of the signalling IPsec SA; or

b) if the IKE_AUTH response message contained the INTERNAL_IP6_ADDRESS attribute and the NAS_IP6_ADDRESS notify payload, an inner IPv6 datagram shall be constructed where:

1) the TCP packet shall be encapsulated in the inner IPv6 datagram with IPv6 header where:

A) if the UE constructs the inner IPv6 datagram:

- the source address field shall be set to the IPv6 address in the INTERNAL_IP6_ADDRESS attribute;
- the source port number shall be set to the UE's TCP port number;
- the destination address field shall be set to the IPv6 address in the NAS_IP6_ADDRESS notify payload; and
- the destination port number shall be set to the NAS_TCP_PORT notify payload;

B) if the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access constructs the inner IPv6 datagram:

- the source address field shall be set to the IPv6 address in the NAS_IP6_ADDRESS notify payload;
- the source port number shall be set to the NAS_TCP_PORT notify payload;
- the destination address field shall be set to the IPv6 address in the INTERNAL_IP6_ADDRESS attribute; and
- the destination port number shall be set to the UE's TCP port number; and

NOTE 3: Since the UE always initiates the NAS message exchange with the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access receive the UE's TCP port number in the TCP SYN packet exchange and use it when sending NAS messages towards the UE or when re-establishing the TCP connection upon failure.

C) the next header field shall be set to 06H;

2) the inner IPv6 datagram shall be protected employing the ESP protocol in tunnel mode as specified in IETF RFC 4303 [11] where:

A) the SPI field in the ESP packet shall be set to the SPI of the signalling IPsec SA; and

B) the next header field in the ESP packet shall be set to 29H, and

3) the IP packet encapsulating the ESP protected inner IPv6 datagram shall be sent to the peer for the SPI of the signalling IPsec SA.

If the UE receives an IKE_AUTH response message containing both NAS_IP4_ADDRESS and NAS_IP6_ADDRESS notify payload, the UE:

a) shall select and use either NAS_IP4_ADDRESS or NAS_IP6_ADDRESS;

b) shall not switch between NAS_IP4_ADDRESS and NAS_IP6_ADDRESS for TCP packet transport during the lifetime of the IKE SA; and

c) shall not switch between NAS_IP4_ADDRESS and NAS_IP6_ADDRESS when rekeying any child SA or IKE SA.

The ESP packet format is shown in figure 8.2.2-1 and figure 8.2.2-2:

Bits 8	7	6	5	4	3	2	1	Octets
Security Parameters Index (SPI)								1-4
Sequence Number								5-8
Payload data (inner IP packet containing TCP packet)								9-m
Padding								(m+1) - n
Padding length								n+1
Next header								n+2
Integrity Check Value (ICV)								(n+3) - x

Figure 8.2.2-1: ESP packet format for TCP packet (re-)establishing or releasing TCP connection

Bits 8	7	6	5	4	3	2	1	Octets
Security Parameters Index (SPI)								1-4
Sequence Number								5-8
Payload data (inner IP packet containing TCP packet encapsulating NAS message or partial NAS message)								9-m
Padding								(m+1) - n
Padding length								n+1
Next header								n+2
Integrity Check Value (ICV)								(n+3) - x

Figure 8.2.2-2: ESP packet format for TCP packet encapsulating NAS message or partial NAS message

8.2.3 Establishment of TCP connection for transport of NAS messages

For transport of NAS messages, the UE shall initiate establishment of a TCP connection as defined in IETF RFC793 [27]. The UE and the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall construct and transport TCP packets according to subclause 8.2.2.

8.2.3A Re-establishment of TCP connection for transport of NAS messages

The UE, the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access upon detection that the transport of a NAS message over the TCP connection is unsuccessful due to TCP connection failure, e.g. as indicated by the reception of a TCP error message, shall re-establish the TCP connection as defined in IETF RFC793 [27]. The UE and the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall construct and transport TCP packets according to subclause 8.2.2.

8.2.4 Transport of NAS messages over TCP connection

In order to transport a NAS message over the untrusted non-3GPP access between the UE and the N3IWF or over the trusted non-3GPP access between the UE and the TNGF:

a) the NAS message shall be framed in a NAS message envelope as defined in subclause 9.4;

b) the NAS message envelope shall be transported as a payload of one or more TCP packets using the TCP connection; and

c) the UE and the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall transport the one or more TCP packets encapsulating the NAS message envelope according to subclause 8.2.2.

8.2.5 Release of TCP connection for transport of NAS messages

In order to release the TCP connection for transport of NAS messages, the UE, the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access shall initiate release of the TCP connection as defined in IETF RFC 793 [27]. The UE, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access shall construct and transport TCP packets according to subclause 8.2.2.

8.3 Transport of messages over user plane

8.3.1 General

In trusted and untrusted non-3GPP access, after the completion of PDU session establishment via non-3GPP access, user plane IPsec SAs are established as specified in subclause 7.5. The UE is able to send and receive GRE encapsulated user data packets over non-3GPP access network via N3IWF in untrusted non-3GPP access and TNGF in trusted non-3GPP access. GRE encapsulation of user plane data packets is described in subclause 8.3.2.

In wireline access, after the completion of PDU session establishment via wireline access, one or more W-UP resources are established as specified in subclause 4.4.2.2. The 5G-RG is able to send and receive the user data packet, the QFI associated with the downlink user data packet, and RQI (in downlink direction only) via the selected W-UP resource and the W-AGF serving the 5G-RG as specified in subclause 4.4.2.2.

For an uplink user data packet associated with a PDU session ID and a QFI:

a) if there is a user plane IPsec SA or a W-UP resource:

   1) associated with a PDU session ID matching the PDU session ID associated with the uplink user data packet; and

   2) associated with a QFI matching the QFI associated with the uplink user data packet;

   the UE or the 5G-RG shall select that user plane IPsec SA or that W-UP resource, respectively;

b) otherwise, the UE or the 5G-RG shall select the user plane IPsec SA or the W-UP resource, respectively:

   1) associated with a PDU session ID matching the PDU session ID associated with the uplink user data packet; and

   2) associated with the indication that the child SA is the default child SA.

8.3.2 Generic routing encapsulation (GRE)

If a user data packet message is transmitted over non-3GPP access between the UE and the N3IWF for untrusted non-3GPP access and the TNGF for the trusted non-3GPP access, the user data packet message shall be encapsulated as a GRE user data packet with a GRE header as specified in subclause 9.3.3. In the GRE encapsulated user data packet:

a0) the protocol type field is set to zero;

a) the payload packet field is set to the user data packet;

b) the QFI field of the key field of the GRE header field is set to the QFI associated with the user data packet;

c) if the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access:

   1) needs to send RQI for a downlink user data packet, the RQI field of the key field of the GRE header is set to "RQI is indicated" as defined in table 9.3.3-3; or

   2) does not need to send RQI for a downlink user data packet, the RQI field of the key field of the GRE header is set to "RQI is not indicated" as defined in table 9.3.3-3; and

d) if the UE sends an uplink user data packet, the RQI field of the key field of the GRE header is set to "RQI is not indicated" as defined in table 9.3.3-3.

If the IKE_AUTH response message contains:

a) the INTERNAL_IP4_ADDRESS attribute and the CREATE_CHILD_SA request message creating the user plane IPsec SA contains the UP_IP4_ADDRESS notify payload in subclause 7.5.4, an inner IPv4 datagram shall be constructed where:

   1) the GRE user data packet shall be encapsulated as the payload of the inner IPv4 datagram with IPv4 header where:

A) if the UE constructs the inner IPv4 datagram, the source address field shall be set to the IPv4 address in the INTERNAL_IP4_ADDRESS attribute and the destination address field shall be set to the IPv4 address in the UP_IP4_ADDRESS notify payload;

B) if the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access constructs the inner IPv4 datagram, the source address field shall be set to the IPv4 address in the UP_IP4_ADDRESS notify payload and the destination address field shall be set to the IPv4 address in the INTERNAL_IP4_ADDRESS attribute; and

C) the protocol field shall be set to 2FH;

2) the inner IPv4 datagram shall be protected employing the ESP protocol in tunnel mode as specified in IETF RFC 4303 [11] where:

A) the SPI field in the ESP packet shall be set to the SPI of the user plane IPsec SA; and

B) the next header field in the ESP packet shall be set to 04H,

and the inner IPv4 datagram encapsulating the GRE encapsulated user data can be fragmented as described in IETF RFC 791 [24] before being protected by ESP protocol;

3) if the DSCP field is associated with the user plane IPsec SA, the DSCP field as specified in IETF RFC 2474 [26] of the IP packet encapsulating the ESP protected inner IPv4 datagram shall be set to the value of the DSCP field included in the 5G_QOS_INFO Notify payload; and

4) the IP packet encapsulating the ESP protected inner IPv4 datagram shall be sent to the peer for the SPI of the user plane IPsec SA; or

b) the INTERNAL_IP6_ADDRESS attribute and the CREATE_CHILD_SA request message creating the user plane IPsec SA contains the UP_IP6_ADDRESS notify payload in subclause 7.5.4, an inner IPv6 datagram shall be constructed where:

1) the GRE user data packet shall be encapsulated as the payload of the inner IPv6 datagram with IPv6 header where:

A) if the UE constructs the inner IPv6 datagram, the source address field shall be set to the IPv6 address in the INTERNAL_IP6_ADDRESS attribute and the destination address field shall be set to the IPv6 address in the UP_IP6_ADDRESS notify payload;

B) if the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access constructs the inner IPv6 datagram, the source address field shall be set to the IPv6 address in the UP_IP6_ADDRESS notify payload and the destination address field shall be set to the IPv6 address in the INTERNAL_IP6_ADDRESS attribute; and

C) the next header field shall be set to 2FH;

2) the inner IPv6 datagram shall be protected employing the ESP protocol in tunnel mode as specified in IETF RFC 4303 [11] where:

A) the SPI field in the ESP packet shall be set to the SPI of the user plane IPsec SA; and

B) the next header field in the ESP packet shall be set to 29H;

and the inner IPv6 datagram encapsulating the GRE encapsulated user data can be fragmented as described in IETF RFC 8200 [25] before being protected by ESP protocol; and

3) if the DSCP field is associated with the user plane IPsec SA, the DSCP field as specified in IETF RFC 2474 [26] of the IP packet encapsulating the ESP protected inner IPv6 datagram shall be set to the value of the DSCP field included in the 5G_QOS_INFO Notify payload; and

4) theIP packet encapsulating the ESP protected inner IPv6 datagram shall be sent to the peer for the SPI of the user plane IPsec SA.

If a user data packet message is transmitted over non-3GPP access between the UE and the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access, the user data packet message shall be encapsulated in the payload of an inner IP datagram which is further encapsulated by ESP protocol in tunnel mode as specified in

IETF RFC 4303 [11]. In order to avoid any IP fragmentation by the sending entity over the non-3GPP access network, the maximum inner IP datagram length shall be set by the sending entity such that the length of the resulting outer IP datagram does not exceed the MTU of the non-3GPP access network. If the length of the user data packet message exceeds the payload size corresponding to the maximum inner IP datagram length and IP fragmentation is needed:

a) the inner IP IPv4 datagram or inner IP IPv6 datagram shall be fragmented; and

b) the IP packet encapsulating the ESP protected inner IPv4 datagram and the IP packet encapsulating the ESP protected inner IPv6 datagram shall not be fragmented.

9 Parameters and coding

9.1 General

This subclause describes the encoding of the parameters which are exchanged between the UE and the network. This subclause is further divided into three subclauses; 3GPP specific coding information, IETF specific coding information and NAS message envelope.

The subclauses for the 3GPP specific coding information and IETF specific coding information describe how to encode the messages and parameters belonging to 3GPP and IETF. The subclause for NAS message envelope describes how to encode the NAS message envelope in order to frame a NAS message prior to its encapsulation within a TCP payload.

9.2 3GPP specific coding information

9.2.1 GUAMI

The purpose of the GUAMI information element is to provide the globally unique AMF ID.

The GUAMI information element is coded as shown in figures 9.2.1-1 and table 9.2.1-1.

The GUAMI is a type 3 information element with a length of 7 octets.

8	7	6	5	4	3	2	1	
GUAMI IEI								octet 1
MCC digit 2				MCC digit 1				octet 2
MNC digit 3				MCC digit 3				octet 3
MNC digit 2				MNC digit 1				octet 4
AMF region ID								octet 5
AMF set ID								octet 6
AMF set ID (continued)				AMF pointer				octet 7

Figure 9.2.1-1: GUAMI information element

Table 9.2.1-1: GUAMI information element

MCC, Mobile country code (octet 2, octet 3 bits 1 to 4) The MCC field is coded as in ITU-T Recommendation E.212 [21], Annex A. MNC, Mobile network code (octet 4, octet 3 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. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 3 shall be coded as "1111".

9.2.2 Establishment cause for non-3GPP access

The purpose of the Establishment cause for non-3GPP access information element is to provide the establishment cause for non-3GPP access.

The Establishment cause for non-3GPP access information element is coded as shown in figures 9.2.2-1 and table 9.2.2-1.

The Establishment cause for non-3GPP access is a type 3 information element with length of 2 octets.

8	7	6	5	4	3	2	1	
Establishment cause for non-3GPP access IEI								octet 1
0 Spare	0 Spare	0 Spare	0 Spare	N3AEC				octet 2

Figure 9.2.2-1: Establishment cause for non-3GPP access information element

Table 9.2.2-1: Establishment cause for non-3GPP access information element

Establishment cause for non-3GPP access (N3AEC) (octet 2 bits 1 to 4) Bits 4 3 2 1 0 0 0 0 emergency 0 0 0 1 highPriorityAccess 0 0 1 1 mo-Signalling 0 1 0 0 mo-Data 1 0 0 0 mps-PriorityAccess 1 0 0 1 mcs-PriorityAccess All other values are spare values. The receiving entity shall treat a spare value as 0100, "mo-Data".

9.2.3 PLMN ID

The purpose of the PLMN ID information element is to indicate the PLMN identity of the selected PLMN.

The PLMN ID is a type 4 information element with a length of 5 octets.

The PLMN ID information element is coded as shown in figure 9.2.3-1 and table 9.2.3-1.

8	7	6	5	4	3	2	1	
PLMN ID IEI								octet 1
Length of PLMN ID contents								octet 2
MCC digit 2				MCC digit 1				octet 3
MNC digit 3				MCC digit 3				octet 4
MNC digit 2				MNC digit 1				octet 5

Figure 9.2.3-1: PLMN ID information element

Table 9.2.3-1: PLMN ID information element

MCC, Mobile country code (octet 3, octet 4 bits 1 to 4) The MCC field is coded as in ITU-T Recommendation E.212 [42], Annex A MNC, Mobile network code (octet 5, octet 4 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. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 4 shall be coded as "1111". Mobile equipment shall accept MNC coded in such a way.

9.2.4 IKEv2 Notify Message Type value

9.2.4.1 General

The IKEv2 Notify Message Type is specified in IETF RFC 7296 [6].

The Notify Message Type with a value (in decimal) in the range 0 - 16383 is intended for reporting errors, where:

- value range between 0 and 8191 is defined in IETF RFC 7296 [6]; and
- value range between 8192 and 16383 is reserved for private error usage.

The Notify Message Type with a value (in decimal) in the range 16384 - 65535 is intended for reporting status, where:

- value range between 16384 and 40959 is defined in IETF RFC 7296 [6]; and
- value range between 40960 and 65535 is reserved for private status usage.

9.2.4.2 Private Notify Message - Error Types

The Private Notify Message Error Types defined in table 9.2.4.2-1 are error notifications which indicate an error while negotiating an IKEv2 SA or IPsec SA. Refer to table 9.2.4.2-1 for more details on what each error type means.

Table 9.2.4.2-1: Private Error Types

Notify Message	Value (in decimal)	Descriptions
CONGESTION	15500	This error type is used to indicate that the requested service was rejected because of congestion in the network.
NO_RESOURCES_OVER_N3GPP	15501	This error type is used by the UE to indicate the failure of reserving the QoS resources over non-3GPP access for the QoS flows associated with the child SA.

In the present specification, only the private notify message error type values between 15500 and 15599 shall be allocated to a Notify payload.

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;

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

9.2.4.3 Private Notify Message - Status Types

The Private Notify Message Status Types defined in table 9.2.4.3-1 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 9.2.4.3-1 for more details on what each status type means.

Table 9.2.4.3-1: Private Status Types

Notify Message	Value (in decimal)	Descriptions
5G_QOS_INFO	55501	This status when present indicates 5G_QOS_INFO Notify payload encoded according to subclause 9.3.1.1
NAS_IP4_ADDRESS	55502	This status when present indicates NAS_IP4_ADDRESS Notify payload encoded according to subclause 9.3.1.2.
NAS_IP6_ADDRESS	55503	This status when present indicates NAS_IP6_ADDRESS Notify payload encoded according to subclause 9.3.1.3.
UP_IP4_ADDRESS	55504	This status when present indicates UP_IP4_ADDRESS Notify payload encoded according to subclause 9.3.1.4.
UP_IP6_ADDRESS	55505	This status when present indicates UP_IP6_ADDRESS Notify payload encoded according to subclause 9.3.1.5.
NAS_TCP_PORT	55506	This status when present indicates NAS_TCP_PORT Notify payload encoded according to subclause 9.3.1.6.
N3GPP_BACKOFF_TIMER	55507	This status when present indicates N3GPP_BACKOFF_TIMER Notify payload encoded according to subclause 9.3.1.7.

In the present specification, only the private notify message error type values between 55500 and 55599 shall be allocated to a Notify payload.

The private notify message status 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;

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

9.2.5 TNGF IPv4 contact info

The purpose of the TNGF IPv4 contact info information element is to indicate the IPv4 address of the TNGF to be used for IKE SA establishment over trusted non-3GPP access network.

The TNGF IPv4 contact info is a type 4 information element with a length of 6 octets.

The TNGF IPv4 contact info information element is coded as shown in figure 9.2.5-1 and table 9.2.5-1.

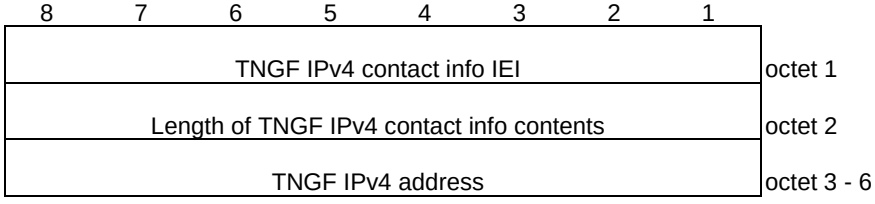

Figure 9.2.5-1: TNGF IPv4 contact info information element

Table 9.2.5-1: TNGF IPv4 contact info information element

TNGF IPv4 address contains IPv4 address of the TNGF for IKE SA establishment over trusted non-3GPP access network.

9.2.6 TNGF IPv6 contact info

The purpose of the TNGF IPv6 contact info information element is to indicate the IPv6 address of the TNGF to be used for IKE SA establishent.

The TNGF IPv6 contact info is a type 4 information element with a length of 18 octets.

The TNGF IPv6 contact info information element is coded as shown in figure 9.2.6-1 and table 9.2.6-1.

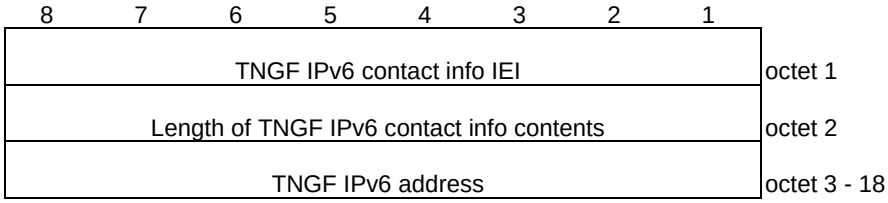

Figure 9.2.6-1: TNGF IPv6 contact info information element

Table 9.2.6-1: TNGF IPv6 contact info information element

TNGF IPv6 address contains IPv6 address of the TNGF for IKE SA establishment over trusted non-3GPP access network.

9.2.7 NID

The purpose of the NID information element is to indicate the NID of the selected SNPN.

The NID is a type 4 information element with a length of 8 octets.

The NID information element is coded as shown in figure 9.2.7-1 and table 9.2.7-1.

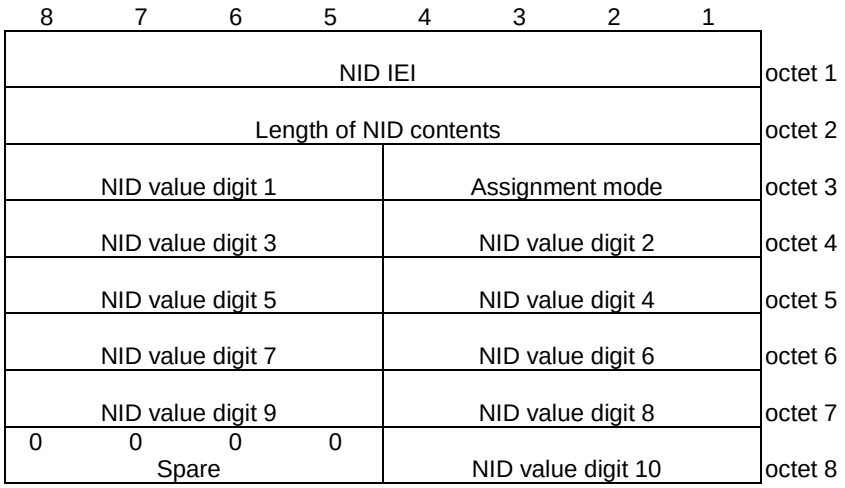

Figure 9.2.7-1: NID information element

Table 9.2.7-1: NID information element

Assignment mode (octet 3 bits 1 to 4) This field contains the binary encoding of the assignment mode of the NID as defined in 3GPP TS 23.003 [8]. NID value (octet 3 bits 5 to 8, octets 4 to 7, octet 8 bits 1 to 4) This field contains the binary encoding of each hexadecimal digit of the NID value as defined in 3GPP TS 23.003 [8]. Bits 5 to 8 of octet 8 are spare and shall be coded as zero.

9.3 IETF RFC coding information

9.3.1 IKEv2 Notify payloads

9.3.1.1 5G_QOS_INFO Notify payload

The 5G_QOS_INFO payload is used to indicate:

a) the PDU session identity;

b) zero or more QFIs;

c) optionally a DSCP value associated with the child SA;

d) whether the child SA is the default child SA; and

e) if trusted non-3GPP access, Additional QoS Information or if untrusted non-3GPP access, optionally Additional QoS Information.

The 5G_QOS_INFO payload is coded according to figure 9.3.1.1-1 and table 9.3.1.1-1.

Bits 7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3 - 4
Length								5
PDU Session Identity								6
Number of QFIs								7
QFI List								8* - x*
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	QoSI	DCSI	DSCPI	x+1
DSCP								x+2*
Additional QoS Information								x+3* - x+y*

Figure 9.3.1.1-1: 5G_QOS_INFO Notify payload format

Bits 7	6	5	4	3	2	1	0	Octets
Number of parameters								x+3
Parameters list								x+4 – x+y

Figure 9.3.1.1-2: Additional QoS Information

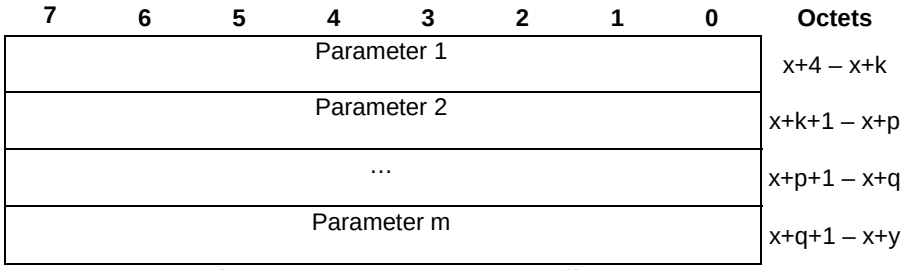

Figure 9.3.1.1-3: Parameters list

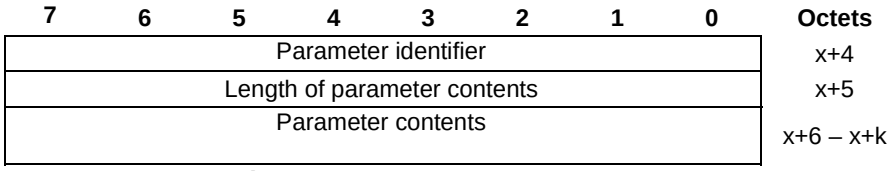

Figure 9.3.1.1-4: Parameter

Table 9.3.1.1-1: 5G_QOS_INFO Notify payload value

Octet 1 is defined in IETF RFC 7296 [6] 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 55501 to indicate the 5G_QOS_INFO. Octet 5 is the Length field. This field indicates the length in octets of the 5G_QOS_INFO Value field. Octet 6 is the PDU Session Identity field. This field indicates the PDU session associated with the child SA for user plane. Octet 7 is the Number of QFIs field. This field indicates the number of QFIs in the QFI list. Octet 8 to octet x is the QFI List field. This field indicates those QoS flows associated with the child SA. Every QFI is coded as the QFI field in the QoS rule defined in 3GPP TS 24.501 [4]. Octet x+1, bit 0 is the DSCP included field (DSCPI). 0 DSCP field is not included. 1 DSCP field is included. Octet x+1, bit 1 is the indication of whether the child SA is the default child SA (DCSI). 0 the child SA is not the default child SA. 1 the child SA is the default child SA. Octet x+1, bit 2 is the Additional QoS Information indication field (QoSI) 0 Additional QoS Information is not included. 1 Additional QoS Information is included. Octet x+2 is the DSCP field. If included, this field indicates the DSCP marking for all IP packets sent over this child SA. Octet x+3 to octet x+y is the Additional QoS Information field which is included if the access network is the trusted non-3GPP access network. This field is encoded as defined in table 9.3.1.1-2.

Table 9.3.1.1-2: Additional QoS Information

Octet x+3 is number of parameters
The number of parameters field contains the binary coding for the number of parameters in the parameters list field. The number of parameters field is encoded in bits 7 through 0 of octet x+3 where bit 7 is the most significant and bit 0 is the least significant bit.

The parameter identifier field is used to identify each parameter included in the parameters list and it contains the binary coding of the parameter identifier. Bit 7 of the parameter identifier field contains the most significant bit and bit 0 contains the least significant bit. The following parameter identifiers are specified:

Bits 7 6 5 4 3 2 1 0	
0 0 0 0 0 0 0 1	QoS characteristics;
0 0 0 0 0 0 1 0	Maximum Flow Bit Rate downlink (MFBR downlink);
0 0 0 0 0 0 1 1	Maximum Flow Bit Rate uplink (MFBR uplink);
0 0 0 0 0 1 0 0	Guaranteed Flow Bit Rate downlink (GFBR downlink);
0 0 0 0 0 1 0 1	Guaranteed Flow Bit Rate uplink (GFBR uplink);
0 0 0 0 0 1 1 0	Notification Control;
0 0 0 0 0 1 1 1	Maximum Packet Loss Rate downlink; and
0 0 0 0 1 0 0 0	Maximum Packet Loss Rate uplink.

All other values are spare.

If the parameters list contains a parameter identifier that is not supported by the receiving entity the corresponding parameter shall be discarded.

If the parameter identifier indicates QoS characteristics, the parameter contents field contains the following representation:

Octet 1 is the resource type with binary representation:
Bits
7 6 5 4 3 2 1 0
0 0 0 0 0 0 0 0 GBR
0 0 0 0 0 0 0 1 Delayed critical GBR
0 0 0 0 0 0 1 0 Non GBR
All other values are spare.

Octet 2 is the priority level with 1 as the highest priority and 127 as the lowest priority ((see subclause 9.3.1.84 in 3GPP TS 38.413 [29], see NOTE), and the binary representation is:
Bits
7 6 5 4 3 2 1 0
0 0 0 0 0 0 0 1
thru
0 1 1 1 1 1 1 1
All other values are spare.

Octets 3 and 4 are the packet delay budget and is a factor of 0.5ms (see subclause 9.3.1.80 in 3GPP TS 38.413 [29], see NOTE), where the factor has the following binary representation:
Bits
7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
thru
0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1
All other values are spare.

Octets 5 and 6 are the packet error rate where octet 5 is scalar and octet 6 represents exponent. The packet error rate is calculated as {scalar x10 – exponent} (see subclause 9.3.1.81 in 3GPP TS 38.413 [29]) The binary representation of scalar and exponent are:
Bits
7 6 5 4 3 2 1 0
0 0 0 0 0 0 0 0
thru
0 0 0 0 1 0 0 1
All other values are spare.

Octets 7 and 8 are the averaging window and is included if the resource type is GBR. Averaging window is a factor of 0.5ms with default value of 2000ms (see subclause 9.3.1.82 in 3GPP TS 38.413 [29], see NOTE), where the factor has the following binary representation:
Bits
7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
thru
0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1
All other values are spare.

Octets 9 and 10 are the maximum data burst volume and is included if the resource type is delayed critical GBR. Maximum data burst volume is the maximum number of the bytes for the data volume (see subclause 9.3.1.83 in 3GPP TS 38.413 [29], see NOTE), where the maximum number of bytes has the following binary representation:
Bits
7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
thru
0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1
All other values are spare.

For GBR and delayed critical GBR resource types if the parameter identifier indicates " GFBR downlink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for downlink followed by two octets containing the value of the guaranteed flow bit rate for downlink.
Unit of the guaranteed flow bit rate for downlink (octet 1)
Bits
7 6 5 4 3 2 1 0

0 0 0 0 0 0 0 0 value is not used
0 0 0 0 0 0 0 1 value is incremented in multiples of 1 Kbps
0 0 0 0 0 0 1 0 value is incremented in multiples of 4 Kbps
0 0 0 0 0 0 1 1 value is incremented in multiples of 16 Kbps
0 0 0 0 0 1 0 0 value is incremented in multiples of 64 Kbps
0 0 0 0 0 1 0 1 value is incremented in multiples of 256 Kbps
0 0 0 0 0 1 1 0 value is incremented in multiples of 1 Mbps
0 0 0 0 0 1 1 1 value is incremented in multiples of 4 Mbps
0 0 0 0 1 0 0 0 value is incremented in multiples of 16 Mbps
0 0 0 0 1 0 0 1 value is incremented in multiples of 64 Mbps
0 0 0 0 1 0 1 0 value is incremented in multiples of 256 Mbps
0 0 0 0 1 0 1 1 value is incremented in multiples of 1 Gbps
0 0 0 0 1 1 0 0 value is incremented in multiples of 4 Gbps
0 0 0 0 1 1 0 1 value is incremented in multiples of 16 Gbps
0 0 0 0 1 1 1 0 value is incremented in multiples of 64 Gbps
0 0 0 0 1 1 1 1 value is incremented in multiples of 256 Gbps
0 0 0 1 0 0 0 0 value is incremented in multiples of 1 Tbps
0 0 0 1 0 0 0 1 value is incremented in multiples of 4 Tbps
0 0 0 1 0 0 1 0 value is incremented in multiples of 16 Tbps
0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps
0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps
0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps
0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps
0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps
0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps
0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps
Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol.

Value of the guaranteed flow bit rate for downlink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for downlink in units defined by the unit of the guaranteed flow bit rate for downlink.

For GBR and delayed critical GBR resource types if the parameter identifier indicates " GFBR uplink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for uplink followed by two octets containing the value of the guaranteed flow bit rate for uplink.

Unit of the guaranteed flow bit rate for uplink (octet 1)
The coding is identical to that of the unit of the guaranteed flow bit rate for downlink.

Value of the guaranteed flow bit rate for uplink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for uplink in units defined by the unit of the guaranteed flow bit rate for uplink.

For GBR and delayed critical GBR resource types if the parameter identifier indicates " MFBR downlink", the parameter contents field contains one octet indicating the unit of the maximum flow bit rate for downlink followed by two octets containing the value of maximum flow bit rate for downlink.

Unit of the maximum flow bit rate for downlink (octet 1)
The coding is identical to that of the unit of the guaranteed flow bit rate for downlink.

Value of the maximum flow bit rate for downlink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for downlink in units defined by the unit of the maximum flow bit rate for downlink.

For GBR and delayed critical GBR resource types if the parameter identifier indicates " MFBR uplink", the parameter contents field contains one octet indicating the unit of the maximum flow bit rate for uplink followed by two octets containing the value of the maximum flow bit rate for downlink.

Unit of the maximum flow bit rate for uplink (octet 1)
The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.

Value of the maximum flow bit rate for uplink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for uplink in units defined by the unit of the maximum flow bit rate for uplink.
For GBR and delayed critical GBR resource types if the parameter identifier indicates "Notification Control", the parameter identifier shall be ignored in this release.

For GBR and delayed critical GBR resource types if the parameter identifier indicates "Maximum Packet Loss Rate downlink", the parameter contents field contains the ratio of the lost downlink packets per number of downlink packets sent, expressed in tenth of percent (see subclause 9.3.1.79 in 3GPP TS 38.413 [29], see NOTE), with the binary representation:
Bits
7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
thru
0 0 0 0 0 0 1 1 1 1 1 0 1 0 0 0
All other values are spare.

For GBR and delayed critical GBR resource types if the parameter identifier indicates "Maximum Packet Loss Rate uplink", the parameter contents field contains the ratio of the lost uplink packets per number of uplink packets sent, expressed in tenth of percent (see subclause 9.3.1.79 in 3GPP TS 38.413 [29]), with the binary representation:
Bits
7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
thru
0 0 0 0 0 0 1 1 1 1 1 0 1 0 0 0
All other values are spare.

NOTE: The protocol specified in 3GPP TS 29.413 [39] uses IEs specified in 3GPP TS 38.413 [29].

9.3.1.2 NAS_IP4_ADDRESS Notify payload

The NAS_IP4_ADDRESS payload is used to indicate the inner IPv4 address of the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access for NAS message transport.

The NAS_IP4_ADDRESS payload is coded according to figure 9.3.1.2-1 and table 9.3.1.2-1.

Bits								
7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3 - 4
IPv4 address								5 - 8

Figure 9.3.1.2-1: NAS_IP4_ADDRESS Notify payload format

Table 9.3.1.2-1: NAS_IP4_ADDRESS Notify payload value

Octet 1 is defined in IETF RFC 7296 [6]

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 55502 to indicate the NAS_IP4_ADDRESS.

Octet 5 to octet 8 is the IPv4 address field. The IPv4 address field contains the inner IPv4 address of the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access for NAS message transport.

9.3.1.3 NAS_IP6_ADDRESS Notify payload

The NAS_IP6_ADDRESS payload is used to indicate the inner IPv6 address of the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access for NAS message transport.

The NAS_IP6_ADDRESS payload is coded according to figure 9.3.1.3-1 and table 9.3.1.3-1.

Bits 7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3 - 4
IPv6 address								5 - 20

Figure 9.3.1.3-1: NAS_IP6_ADDRESS Notify payload format

Table 9.3.1.3-1: NAS_IP6_ADDRESS Notify payload value

Octet 1 is defined in IETF RFC 7296 [6] 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 55503 to indicate the NAS_IP6_ADDRESS. Octet 5 to octet 20 is the IPv6 address field. The IPv6 address field contains the inner IPv6 address of the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access for NAS message transport.

9.3.1.4 UP_IP4_ADDRESS Notify payload

The UP_IP4_ADDRESS payload is used to indicate the inner IPv4 address of the N3IWF for untrusted non-3GPP access and the TNGF for trusted on-3GPP access for GRE user data packet transport.

The UP_IP4_ADDRESS payload is coded according to figure 9.3.1.4-1 and table 9.3.1.4-1.

Bits 7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3 - 4
IPv4 address								5 - 8

Figure 9.3.1.4-1: UP_IP4_ADDRESS Notify payload format

Table 9.3.1.4-1: UP_IP4_ADDRESS Notify payload value

Octet 1 is defined in IETF RFC 7296 [6] 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 55504 to indicate the UP_IP4_ADDRESS. Octet 5 to octet 8 is the IPv4 address field. The IPv4 address field contains the inner IPv4 address of the N3IWF for untrusted non-3GPP access and the TNGF for trusted on-3GPP access for GRE user data packet transport.

9.3.1.5 UP_IP6_ADDRESS Notify payload

The UP_IP6_ADDRESS payload is used to indicate the inner IPv6 address of the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access for GRE user data packet transport.

The UP_IP6_ADDRESS payload is coded according to figure 9.3.1.5-1 and table 9.3.1.5-1.

Bits 7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3 - 4
IPv6 address								5 - 20

Figure 9.3.1.5-1: UP_IP6_ADDRESS Notify payload format

Table 9.3.1.5-1: UP_IP6_ADDRESS Notify payload value

Octet 1 is defined in IETF RFC 7296 [6] 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 55505 to indicate the UP_IP6_ADDRESS. Octet 5 to octet 20 is the IPv6 address field. The IPv6 address field contains the inner IPv6 address of the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access for GRE user data packet transport.

9.3.1.6 NAS_TCP_PORT Notify payload

The NAS_TCP_PORT payload is used to indicate the port number for the connection of the inner TCP transport protocol for the NAS message transport.

The NAS_TCP_PORT payload is coded according to figure 9.3.1.6-1 and table 9.3.1.6-1.

Bits 7	6	5	4	3	2	1	0	Octets
Protocol ID								1
SPI Size								2
Notify Message Type								3 – 4
Port Number								5 - 6

Figure 9.3.1.6-1: NAS_TCP_PORT Notify payload format

Table 9.3.1.6-1: NAS_TCP_PORT Notify payload value

Octet 1 is defined in IETF RFC 7296 [6] 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 55506 to indicate the NAS_TCP_PORT. Octet 5 and octet 6 are the Port Number field which contains the port number of the connection for the inner TCP transport protocol for the NAS message transport.

9.3.1.7 N3GPP_BACKOFF_TIMER Notify payload

The N3GPP_BACKOFF_TIMER Notify payload is used to indicate the value of the back-off timer.

The N3GPP_BACKOFF_TIMER Notify payload is coded according to figure 9.3.1.7-1 and table 9.3.1.7-1.

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

Figure 9.3.1.7-1: N3GPP_BACKOFF_TIMER Notify payload format

Table 9.3.1.7-1: N3GPP_BACKOFF_TIMER Notify payload value

Octet 1 is defined in IETF RFC 7296 [6] 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 55507 to indicate the N3GPP_BACKOFF_TIMER. Octet 5 is the Backoff Timer Value field. This field indicates the value of the back-off timer. It is coded as the value part (as specified in 3GPP TS 24.007 [22] for type 4 IE) of the GPRS timer 3 information element defined in 3GPP TS 24.008 [28] subclause 10.5.7.4a (NOTE).
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 of the back-off timer.

9.3.2 EAP-5G method

9.3.2.1 General

The messages of EAP-5G method are EAP requests and EAP responses as specified in IETF RFC 3748 [9] subclause 4.1 and use coding of the expanded method type as described in IETF RFC 3748 [9] subclause 5.7.

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

9.3.2.2 Message format

9.3.2.2.1 EAP-Request/5G-Start message

EAP-Request/5G-Start message is coded as specified in figure 9.3.2.2.1-1 and table 9.3.2.2.1-1.

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
Extensions								15 - m

Figure 9.3.2.2.1-1: EAP-Request/5G-Start message

Table 9.3.2.2.1-1: EAP-Request/5G-Start message

Code field is set to 1 (decimal) as specified in IETF RFC 3748 [9] subclause 4.1 and indicates request. Identifier field is set as specified in IETF RFC 3748 [9] subclause 4.1. Length field is set as specified in IETF RFC 3748 [9] subclause 4.1 and indicates the length of the EAP-Request/5G-Start message in octets. Type field is set to 254 (decimal) as specified in IETF RFC 3748 [9] 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-5G method identifier of 3 (decimal) as specified in 3GPP TS 33.402 [10] annex C. Message-Id field is set to 5G-Start-Id of 1 (decimal). Spare field consists of spare bits. Extensions field is an optional field and consists of spare bits.

9.3.2.2.2 EAP-Response/5G-NAS message

EAP-Response/5G-NAS message is coded as specified in figure 9.3.2.2.2-1 and table 9.3.2.2.2-1.

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
AN-parameters length								15-16
AN-parameters								17 - 17+x
NAS-PDU length								18+x - 19+x
NAS-PDU								20+x - n+x
Extensions								n+x+1 - z+x

Figure 9.3.2.2.2-1: EAP-Response/5G-NAS message

Table 9.3.2.2.2-1: EAP-Response/5G-NAS message

Code field is set to 2 (decimal) as specified in IETF RFC 3748 [9] subclause 4.1 and indicates response. Identifier field is set as specified in IETF RFC 3748 [9] subclause 4.1. Length field is set as specified in IETF RFC 3748 [9] subclause 4.1 and indicates the length of the EAP-Response/5G-NAS message in octets. Type field is set to 254 (decimal) as specified in IETF RFC 3748 [9] 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-5G method identifier of 3 (decimal) as specified in 3GPP TS 33.402 [10] annex C. Message-Id field is set to 5G-NAS-Id of 2 (decimal). Spare field consists of spare bits. AN-parameters length indicates the length of the AN-parameters field in octets AN-parameters field is coded according to figure 9.3.2.2.2-2 and table 9.3.2.2.2-2. NAS-PDU length field indicates the length of NAS-PDU field in octets. NAS-PDU field contains a NAS message from the UE as specified in 3GPP TS 24.501 [4]. Extensions field is an optional field and consists of spare bits.

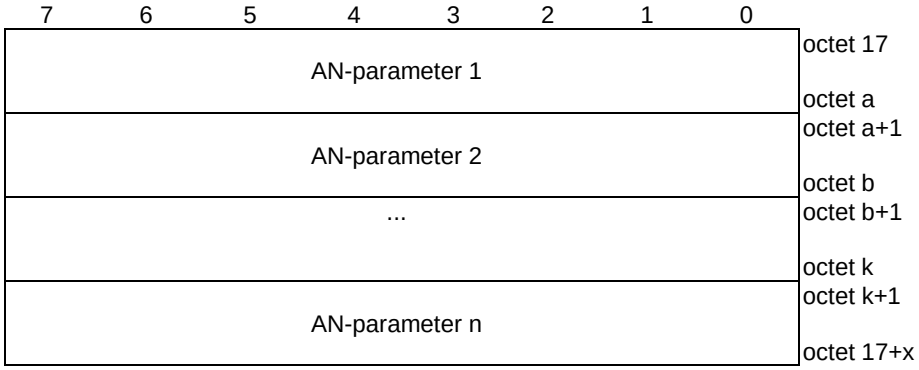

Figure 9.3.2.2.2-2: AN-parameters field

Table 9.3.2.2.2-2: AN-parameters field

Each AN-parameter field is coded according to figure 9.3.2.2.2.1-3 and table 9.3.2.2.2-3.

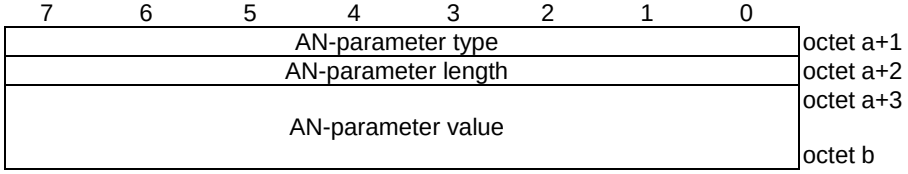

Figure 9.3.2.2.2-3: AN-parameter field

Table 9.3.2.2.2-3: AN-parameter field

The AN-parameter length field indicates the length of the AN-parameter value field. The AN-parameter type field indicates the type of the AN-parameter value field. Sending entity shall not set the AN-parameter type field to a spare value. Receiving entity shall ignore any AN-parameter field with the AN-parameter type field set to a spare value. The following AN-parameter type field values are specified: - 01H (GUAMI); - 02H (selected PLMN ID); - 03H (requested NSSAI); - 04H (establishment cause for non-3GPP access); - 05H (selected NID); and - 06H (UE identity). All other values of the AN-parameter type field are spare. Receiving entity shall ignore an AN-parameter field with the AN-parameter type field set to a spare value. When the AN-parameter type field indicates the GUAMI, the AN-parameter value field is coded as value part (as specified in 3GPP TS 24.007 [22] for type 3 information element) of GUAMI information element as specified in subclause 9.2.1. When the AN-parameter type field indicates the selected PLMN ID, the AN-parameter value field is coded according to value part of PLMN ID information element as specified in subclause 9.2.3. When the AN-parameter type field indicates the requested NSSAI, the AN-parameter value field is coded according to value part of NSSAI information element as specified in subclause 9.11.3.37 of 3GPP TS 24.501 [4]. When the AN-parameter type field indicates the establishment cause for non-3GPP access, the AN-parameter field is coded as value part (as specified in 3GPP TS 24.007 [22] for type 3 information element) of the Establishment cause for non-3GPP access information element as specified in subclause 9.2.2. When the AN-parameter type field indicates the selected NID, the AN-parameter value field is coded according to the value part of the NID information element as specified in subclause 9.2.7. When the AN-parameter type field indicates the UE identity, the AN-parameter value field is coded according to 5GS mobile identity information element for type of identity 5G-GUTI or for type of identity SUCI as specified in subclause 9.11.3.4 of 3GPP TS 24.501 [4].

9.3.2.2.3 EAP-Request/5G-NAS message

EAP-Request/5G-NAS message is coded as specified in figure 9.3.2.2.3-1, figure 9.3.2.2.3-2, and figure 9.3.2.2.3-3 and table 9.3.2.2.3-1, table 9.3.2.2.3-2, and table 9.3.2.2.3-3.

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
NAS-PDU length								15 - 16
NAS-PDU								17 - n
Extensions								n+1 - z

Figure 9.3.2.2.3-1: EAP-Request/5G-NAS message

Table 9.3.2.2.3-1: EAP-Request/5G-NAS message

Code field is set to 1 (decimal) as specified in IETF RFC 3748 [9] subclause 4.1 and indicates request. Identifier field is set as specified in IETF RFC 3748 [9] subclause 4.1. Length field is set as specified in IETF RFC 3748 [9] subclause 4.1 and indicates the length of the EAP-Request/5G-NAS message in octets. Type field is set to 254 (decimal) as specified in IETF RFC 3748 [9] 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-5G method identifier of 3 (decimal) as specified in 3GPP TS 33.402 [10] annex C. Message-Id field is set to 5G-NAS-Id of 2 (decimal). Spare field consists of spare bits. NAS-PDU length field indicates the length of NAS-PDU field in octets. NAS-PDU field contains a NAS message from the AMF as specified 3GPP TS 24.501 [4]. Extensions field is an optional field and consists of spare bits.

9.3.2.2.4 EAP-Request/5G-Stop message

EAP-Request/5G-Stop message is coded as specified in figure 9.3.2.2.4-1 and table 9.3.2.2.4-1.

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
Spare								14
Extensions								15 - m

Figure 9.3.2.2.4-1: EAP-Request/5G-Stop message

Table 9.3.2.2.4-1: EAP-Request/5G-Stop message

Code field is set to 1 (decimal) as specified in IETF RFC 3748 [9] subclause 4.1 and indicates request. Identifier field is set as specified in IETF RFC 3748 [9] subclause 4.1. Length field is set as specified in IETF RFC 3748 [9] subclause 4.1 and indicates the length of the EAP-Request/5G-Stop message in octets. Type field is set to 254 (decimal) as specified in IETF RFC 3748 [9] 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-5G method identifier of 3 (decimal) as specified in 3GPP TS 33.402 [10] annex C. Message-Id field is set to 5G-Stop-Id of 4 (decimal). Spare field consists of spare bits. Extensions field is an optional field and consists of spare bits.

9.3.2.2.5 EAP-Request/5G-Notification message

EAP-Request/5G-Notification message is coded as specified in figure 9.3.2.2.5-1 and table 9.3.2.2.5-1.

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
AN-parameters length								15 - 16
AN-parameters								17 – n
Extensions								n+1 - m

Figure 9.3.2.2.5-1: EAP-Request/5G-Notification message

Table 9.3.2.2.5-1: EAP-Request/5G-Notification message

Code field is set to 1 (decimal) as specified in IETF RFC 3748 [9] subclause 4.1 and indicates request. Identifier field is set as specified in IETF RFC 3748 [9] subclause 4.1. Length field is set as specified in IETF RFC 3748 [9] subclause 4.1 and indicates the length of the EAP-Request/5G-Notification message in octets. Type field is set to 254 (decimal) as specified in IETF RFC 3748 [9] 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-5G method identifier of 3 (decimal) as specified in 3GPP TS 33.402 [10] annex C. Message-Id field is set to 5G-Notification-Id of 3 (decimal). Spare field consists of spare bits. AN-parameters length indicates the length of the AN-parameters field in octets AN-Parameters field is coded according to figure 9.3.2.2.5-2 and table 9.3.2.2.5-2. Extensions field is an optional field and consists of spare bits.

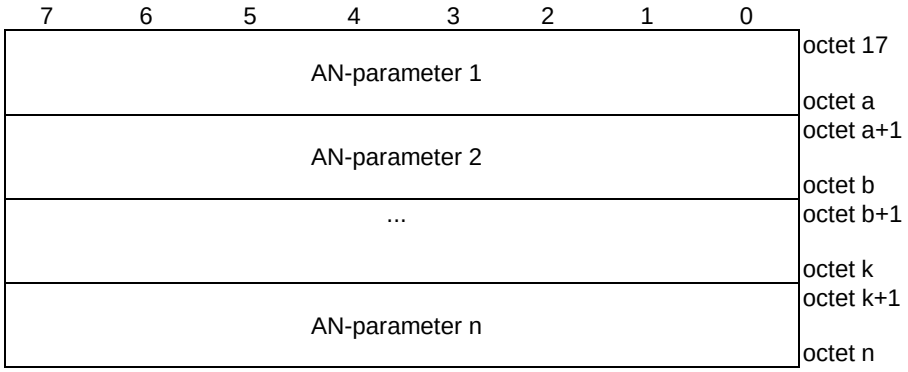

Figure 9.3.2.2.5-2: AN-parameters field

Table 9.3.2.2.5-2: AN-parameters field

Each AN-parameter field is coded according to figure 9.3.2.2.5-3 and table 9.3.2.2.5-3.

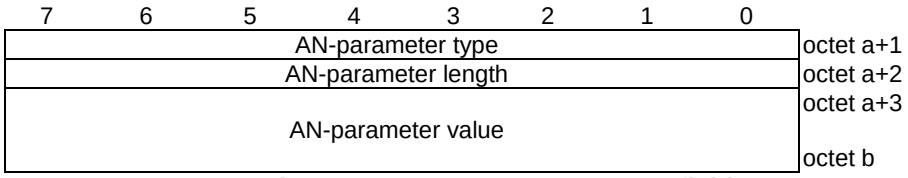

Figure 9.3.2.2.5-3: AN-parameter field

Table 9.3.2.2.5-3: AN-parameter field

The AN-parameter length field indicates the length of the AN-parameter value field. The AN-parameter type field indicates the type of the AN-parameter value field. Sending entity shall not set the AN-parameter type field to a spare value. Receiving entity shall ignore any AN-parameter field with the AN-parameter type field set to a spare value. The following AN-parameter type field values are specified: - 01H (TNGF IPv4 contact info); - 02H (TNGF IPv6 contact info); All other values of the AN-parameter type field are spare. Receiving entity shall ignore an AN-parameter field with the AN-parameter type field set to a spare value. When the AN-parameter type field indicates the TNGF IPv4 contact info, the AN-parameter value field is coded as value part (as specified in 3GPP TS 24.007 [22] for type 3 information element) of TNGF IPv4 contact info information element as specified in subclause 9.2.5. When the AN-parameter type field indicates the TNGF IPv6 contact info, the AN-parameter value field is coded as value part (as specified in 3GPP TS 24.007 [22] for type 3 information element) of TNGF IPv6 contact info information element as specified in subclause 9.2.6.

9.3.2.2.6 EAP-Response/5G-Notification message

EAP-Response/5G-Notification message is coded as specified in figure 9.3.2.2.6-1 and table 9.3.2.2.6-1.

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
Extensions								15-z

Figure 9.3.2.2.6-1: EAP-Response/5G-Notification message

Table 9.3.2.2.6-1: EAP-Response/5G-Notification message

Code field is set to 2 (decimal) as specified in IETF RFC 3748 [9] subclause 4.1 and indicates response. Identifier field is set as specified in IETF RFC 3748 [9] subclause 4.1. Length field is set as specified in IETF RFC 3748 [9] subclause 4.1 and indicates the length of the EAP-Response/5G-Notification message in octets. Type field is set to 254 (decimal) as specified in IETF RFC 3748 [9] 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-5G method identifier of 3 (decimal) as specified in 3GPP TS 33.402 [10] annex C. Message-Id field is set to 5G-Notification-Id of 3 (decimal). Spare field consists of spare bits. Extensions field is an optional field and consists of spare bits.

9.3.3 GRE encapsulated user data packet

GRE encapsulated user data packet is coded according to figure 9.3.3-1 and table 9.3.3-1.

Bits 7	6	5	4	3	2	1	0	Octets
GRE header								1 - 8
Payload packet								9 - x

Figure 9.3.3-1: GRE encapsulated user data packet

Table 9.3.3-1: GRE encapsulated user data packet

Octet 1 to octet 8 are the GRE header field defined in IETF RFC 2784 [14] and IETF RFC 2890 [15]. The GRE header field is coded according to figure 9.3.3-2 and table 9.3.3-2. Octet 9 to octet x are the Payload packet field. The Payload packet field contains one user data packet.

Bits 7	6	5	4	3	2	1	0	Octets
C	Reserved0	K	S	Reserved0				1
Reserved0						Ver		2
Protocol type								3 - 4
Key								5 - 8

Figure 9.3.3-2: GRE header field

Table 9.3.3-2: GRE header field

Bit 7 of octet 1 is the C bit defined in IETF RFC 2784 [14]. The C bit is set to zero. Bits 6, 3, 2, 1 and 0 of octet 1 and bits 7, 6, 5, 4, and 3 of octet 2 are the Reserved0 field defined in IETF RFC 2784 [14] and IETF RFC 2890 [15]. Bit 5 of octet 1 is the K bit defined in IETF RFC 2890 [15]. The K bit is set to one. Bit 4 of octet 1 is the S bit defined in IETF RFC 2890 [15]. The S bit is set to zero. Bits 2, 1 and 0 of octet 2 is the Ver field defined in IETF RFC 2784 [14]. Octet 3 and octet 4 are the Protocol Type field defined in IETF RFC 2784 [14]. The Protocol Type field is set to zero. (see NOTE) Octet 5 to octet 8 are the Key field defined in IETF RFC 2890 [15]. The Key field is coded according to figure 9.3.3-3 and table 9.3.3-3.
NOTE: The receiving entity shall ignore value of the Protocol Type field.

	Bits							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**Octets**
	0 Spare	0 Spare	QFI						5
	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	6
	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	7
	RQI	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	8

Figure 9.3.3-3: Key field of GRE header

Table 9.3.3-3: Key field of GRE header

RQI (octet 8, bit 7) Bit 7 0 RQI is not indicated 1 RQI is indicated QFI (octet 5, bits 5 to 0) Bits 5 4 3 2 1 0 0 0 0 0 0 0 QFI 0 to 1 1 1 1 1 1 QFI 63

9.4 NAS message envelope

NAS message envelope is used to frame the NAS message prior to its encapsulation as the TCP payload in the inner IP datagram.

NAS message envelope is encoded according to figure 9.4-1 and table 9.4-1.

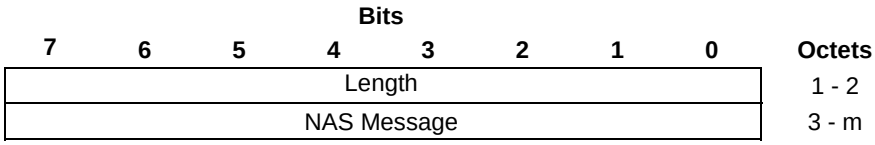

Figure 9.4-1: NAS message envelope format

Table 9.4-1: NAS message envelope value

Octet 1 and Octet 2 indicate the Length field. The Length field contains the length of the NAS message in bytes. Octet 3 to octet m indicate the NAS Message field. The NAS Message field contains the NAS message which is to be framed in prior to encapsulation as the TCP payload in the inner IP datagram of the transmitted IP packet.

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-10-23	CT1#106	C1-174508				Initial Draft provided to CT1#106.	0.0.0
2017-11	CT1#106	C1-174572				Includes the contribution agreed by CT1 at CT1#106.	0.1.0
2017-12	CT1#107	C1-175315, C1-174945, C1-174947, C1-174948, C1-175317				Incorporates the agreed P-CRs for TS 24.502 from CT1#107 plus editorial changes and reference updates by the rapporteur.	0.2.0
2017-12						Additional editorial changes by the rapporteur	0.2.1
2018-02	CT1#108	C1-180055, C1-180475, C1-180691, C1-180692, C1-180700				Incorporates the agreed P-CRs for TS 24.502 from CT1#108 plus editorial changes and reference updates by the rapporteur.	0.3.0
2018-03	CT1#109	C1-181454, C1-181704, C1-181249, C1-181327, C1-181489, C1-181490, C1-181491, C1-181498, C1-181499, C1-181600, C1-181602				Incorporates the agreed P-CRs for TS 24.502 from CT1#109 plus editorial changes, reference and styles updates by the rapporteur.	0.4.0
2018-04	CT1#110	C1-182494, C1-182175, C1-182403, C1-182680, C1-182700, C1-182722, C1-182794, C1-182807, C1-182818, C1-182819, C1-182843				Incorporates the agreed P-CRs from CT1#110 plus editorial changes, reference and styles updates by the rapporteur.	0.5.0
2018-05	CT1#111	C1-183037, C1-183040, C1-183046, C1-183047, C1-183733, C1-183734, C1-183735, C1-183783, C1-183828, C1-183829				Incorporates the agreed P-CRs from CT1#111 plus editorial changes, reference and styles updates by the rapporteur.	0.6.0
2018-06	CT-80	CP-181095				Version 1.0.0 created for presentation to TSG CT#80 for information and approval.	1.0.0
2018-06	CT-80					Version 15.0.0 created after approval	15.0.0
2018-09	CT-81	CP-182143	0001	2	F	Correction for providing GUAMI as part of AN parameters	15.1.0
2018-09	CT-81	CP-182143	0002	2	F	Correction for coding of non-3GPP access establishment cause AN parameter	15.1.0
2018-09	CT-81	CP-182143	0003	2	F	Correction for N3AN node selection	15.1.0
2018-09	CT-81	CP-182143	0004	1	B	Including GUAMI as AN-parameters during registration for non-3GPP access	15.1.0
2018-09	CT-81	CP-182143	0005	2	B	Coding of AN-parameters in EAP 5G-NAS message	15.1.0
2018-09	CT-81	CP-182143	0007	3	B	3GPP specific IKEv2 private Notify Message Types	15.1.0
2018-09	CT-81	CP-182143	0011	2	F	Changing Transport Mode to Tunnel Mode for IPsec Tunnel	15.1.0
2018-09	CT-81	CP-182143	0014	1	F	Clarification on ANDSP	15.1.0
2018-09	CT-81	CP-182143	0018		F	Definition of new notify payloads	15.1.0
2018-09	CT-81	CP-182143	0019	1	F	Corrections for liveness check	15.1.0
2018-09	CT-81	CP-182143	0022	3	F	Signalling IPsec SA establishment not accepted by the network	15.1.0
2018-09	CT-81	CP-182143	0023	1	B	User plane IPsec SA establishment not accepted	15.1.0
2018-09	CT-81	CP-182143	0024	2	F	NAI as identifier for non-3GPP access	15.1.0
2018-09	CT-81	CP-182143	0027	1	B	IKE SA deletion procedure handling	15.1.0
2018-09	CT-81					Editorial corrections	15.1.1
2018-12	CT-82	CP-183042	0029	2	F	Correction of name fields and protocol numbers	15.2.0

2018-12	CT-82	CP-183042	0030	2	F	Correction for default user plane SA indication	15.2.0
2018-12	CT-82	CP-183042	0031	1	F	Correction for DSCP in outer IP header carrying uplink user data packet	15.2.0
2018-12	CT-82	CP-183042	0032		F	Corrections for coding of establishment cause for non-3GPP access	15.2.0
2018-12	CT-82	CP-183042	0033	1	F	Removing an editor's note	15.2.0
2018-12	CT-82	CP-183042	0034		F	Editor's note on usage of Any_PLMN entry configuration	15.2.0
2018-12	CT-82	CP-183042	0036	2	F	Local deletion of IKE SA and child SAs	15.2.0
2018-12	CT-82	CP-183042	0037	2	F	IKE SA and child SAs deletion by UE due to rekeying failure	15.2.0
2018-12	CT-82	CP-183042	0038		F	Correction on child user plane IPsec SA establishment description	15.2.0
2018-12	CT-82	CP-183042	0039		F	Resolve the editor note on liveness check	15.2.0
2018-12	CT-82	CP-183042	0040	2	B	TCP protocol as inner transport layer protocol for NAS signaling	15.2.0
2018-12	CT-82	CP-183042	0041	1	F	Clarification and clean up	15.2.0
2018-12	CT-82	CP-183042	0043	1	F	Correction on N3AN node configuration information	15.2.0
2018-12	CT-82	CP-183042	0044		F	Correcting automatic and manual mode procedures	15.2.0
2018-12	CT-82	CP-183042	0045	2	F	SUPI and SUCI as user identities	15.2.0
2018-12	CT-82	CP-183042	0047	2	F	Correct determination of country the UE is located in	15.2.0
2018-12	CT-82	CP-183042	0049	1	F	Backoff timer in IKE_AUTH response	15.2.0
2019-03	CT-83	CP-190090	0050	1	F	AMF congestion when establishing security association and editors note	15.3.0
2019-03	CT-83	CP-190090	0051	1	B	AMF congestion when receiving NAS message	15.3.0
2019-03	CT-83	CP-190090	0053	2	F	Correcting the name of ITU-T Recommendation E.212	15.3.0
2019-03	CT-83	CP-190090	0054	1	F	Remove of an editorial note	15.3.0
2019-03	CT-83	CP-190090	0055	1	F	Correction on WLAN selection	15.3.0
2019-03	CT-83	CP-190090	0056	3	F	Establishment of TCP connection for transport of NAS messages	15.3.0
2019-03	CT-83	CP-190090	0059	2	F	Alignment of the PLMN determination	15.3.0
2019-03	CT-83	CP-190090	0060	2	F	Correct WLAN selection procedure	15.3.0
2019-03	CT-83	CP-190090	0062		D	Correction to definition of the PCF abbreviation	15.3.0
2019-03	CT-83	CP-190090	0063		F	Correct empty subclause	15.3.0
2019-06	CT-84	CP-191125	0065		F	Release of TCP connection for transport of NAS messages	15.4.0
2019-06	CT-84	CP-191125	0069	1	F	Clarification for untrusted non-3GPP access	15.4.0
2019-06	CT-84	CP-191125	0082	1	F	IPsec SA modification procedure	15.4.0
2019-06	CT-84	CP-191136	0066	1	F	Error in EAP-Response/5G-NAS message coding	16.0.0
2019-06	CT-84	CP-191137	0067	1	B	EAP-5G extensions for trusted non-3GPP access	16.0.0
2019-06	CT-84	CP-191137	0071	1	B	Update to the scope for trusted non-3GPP access	16.0.0
2019-06	CT-84	CP-191137	0072	2	B	Introduction of trusted non-3GPP access description	16.0.0
2019-06	CT-84	CP-191137	0073	5	B	QoS for non-3GPP access	16.0.0
2019-06	CT-84	CP-191137	0074	5	B	Authentication and authorization for accessing 5GS	16.0.0
2019-06	CT-84	CP-191137	0075	3	B	Update to WLAN selection procedure because of trusted non-3GPP access	16.0.0
2019-06	CT-84	CP-191148	0079		B	N3IWF FQDN configured in a UE to support access to PLMN/SNPN services via SNPN/PLMN	16.0.0
2019-06	CT-84	CP-191136	0080	1	D	Editorial changes	16.0.0
2019-06	CT-84	CP-191137	0081	2	F	Adding text to General section of subclause 9 entitled "Parameters and coding"	16.0.0
2019-06	CT-84	CP-191136	0083		D	Alignment of capitalizations	16.0.0
2019-06	CT-84	CP-191137	0084	3	B	TNAN and PLMN selection procedures using trusted WLAN	16.0.0
2019-06	CT-84	CP-191136	0085	1	F	Reference to IEEE Std 802.11	16.0.0
2019-06	CT-84	CP-191148	0086	1	B	A dedicated child SA and a DSCP value for QoS flows	16.0.0
2019-06	CT-84	CP-191137	0087	2	B	Update to the scope for wireline access networks	16.0.0
2019-09	CT-85	CP-192059	0068	5	B	UE registration for trusted non-3GPP access	16.1.0
2019-09	CT-85	CP-192058	0090	1	F	Adding a general subclause	16.1.0
2019-09	CT-85	CP-192059	0092	2	B	Text modification for trusted non-3GPP access	16.1.0
2019-09	CT-85	CP-192058	0093	1	F	Modification for untrusted non-3GPP access	16.1.0
2019-09	CT-85	CP-192059	0094	1	C	Address EN on PLMN Selector list	16.1.0
2019-09	CT-85	CP-192058	0095		B	Forbidden PLMNs for non-3GPP access to 5GCN	16.1.0
2019-09	CT-85	CP-192045	0097	1	A	Protocol type field in GRE encapsulated user data packet	16.1.0
2019-12	CT-86	CP-193100	0099		F	Remove the content under the void clause	16.2.0
2019-12	CT-86	CP-193100	0100	1	B	Registration, Session establishment and session release of 5G capable over WLAN (N5CW) device	16.2.0
2019-12	CT-86	CP-193100	0101	3	F	Removal of an editor's note	16.2.0

2019-12	CT-86	CP-193119	0102	1	F	FQDN for N3IWF selection to access PLMN services via an SNPN	16.2.0
2019-12	CT-86	CP-193092	0103	3	F	Apply ANDSP of equivalent PLMN	16.2.0
2019-12	CT-86	CP-193119	0104	3	F	Addition of NID to AN parameters	16.2.0
2019-12	CT-86	CP-193100	0106	1	B	WLAN and PLMN selection procedures for a N5CW device	16.2.0
2019-12	CT-86	CP-193100	0107		F	Scope correction	16.2.0
2019-12	CT-86	CP-193100	0108	1	B	PLMN selection for wireline access	16.2.0
2019-12	CT-86	CP-193100	0109		B	QoS handling for wireline access	16.2.0
2020-03	CT-87e	CP-200113	0110	3	B	EAP-5G handling and transport of NAS messages for wireline access	16.3.0
2020-03	CT-87e	CP-200113	0111	2	B	Additional QoS Information in an untrusted non-3GPP network	16.3.0
2020-03	CT-87e	CP-200113	0113	1	F	Removal of an editor's note	16.3.0
2020-03	CT-87e	CP-200129	0115		C	Updating length of NID	16.3.0
2020-03	CT-87e	CP-200113	0116	1	B	Support of authentication and registration of N5GC devices via wireline access	16.3.0
2020-03	CT-87e	CP-200113	0118	1	B	SUPI and SUCI for legacy wireline access	16.3.0
2020-06	CT-88e	CP-201090	0120	5	A	Correct N3AN node selection due to LI	16.4.0
2020-06	CT-88e	CP-201106	0121		F	Add handling for UE configured to use timer T3245 in 5GS for non-3GPP access	16.4.0
2020-06	CT-88e	CP-201108	0122	1	F	Inclusion of requested NSSAI in AN parameters	16.4.0
2020-06	CT-88e	CP-201108	0123	1	F	Removal of editor’s notes	16.4.0
2020-06	CT-88e	CP-201090	0125	2	A	Remove USE_TRANSPORT_MODE in response	16.4.0
2020-06	CT-88e	CP-201108	0126	1	B	Error type on failure of reserving QoS resources over non-3GPP access	16.4.0
2020-06	CT-88e	CP-201106	0130	1	F	Extending congestion notification to capture N3IWF or TNGF overload	16.4.0
2020-06	CT-88e	CP-201106	0131	1	F	Enable N3IWF to initiate TCP connection establishment upon failure	16.4.0
2020-06	CT-88e	CP-201108	0134	1	F	Access network parameters	16.4.0
2020-06	CT-88e	CP-201108	0135	1	F	Correction of TNGF procedure	16.4.0
2020-06	CT-88e	CP-201108	0143	1	B	SUPI/SUCI of N5GC devices	16.4.0
2020-06	CT-88e	CP-201108	0136	3	F	Correcting reference	16.4.0
2020-06	CT-88e	CP-201106	0138	1	F	Correcting editorial errors	16.4.0
2020-06	CT-88e	CP-201106	0139	1	F	Resolution of editor's notes under clauses 7.3.4 and 7.3.5	16.4.0
2020-06	CT-88e	CP-201108	0140	1	F	N5CW device registration and IP assignment	16.4.0
2020-06	CT-88e	CP-201106	0141	1	F	Resolution of editor's notes under clauses 7.5.5 and 7.5.6	16.4.0
2020-06	CT-88e	CP-201108	0142	1	F	Resolution of editor's note under clause 7.3A.4.2	16.4.0
2020-09	CT-89e	CP-202152	0144	1	F	W-CP connection in 24.502	16.5.0
2020-09	CT-89e	CP-202170	0148	1	F	Correction in N3AN node selection involving SNPN	16.5.0
2020-09	CT-89e	CP-202149	0150		F	Remove editor's notes of child SA deletion procedure	16.5.0
2020-09	CT-89e	CP-202149	0151	1	F	Corrections on encodings and typos in 24502	16.5.0
2020-09	CT-89e	CP-202149	0152		F	Corrections on the encoding of the 5G_QOS_INFO Notify payload	16.5.0

History

Document history		
V16.4.0	August 2020	Publication
V16.5.0	October 2020	Publication