ETSI TS 124 502 V15.0.0 (2018-06)

5G;
Access to the 3GPP 5G Core Network (5GCN)
via non-3GPP access networks
(3GPP TS 24.502 version 15.0.0 Release 15)

Reference
DTS/TSGC-0124502vf00

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies non-3GPP access network discovery and selection procedures, the access authorization procedure used for accessing untrusted non-3GPP access networks.

The present document also specifies the security association management procedures used for establishing IKEv2 and IPSEC security associations from the UE to the N3IWF and the procedures for transporting messages between the UE N3IWF over the non-3GPP access networks.

The present document is applicable to the UE and the network. In this technical specification the network refers to the 3GPP 5GCN and the untrusted non-3GPP access network.

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".

[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 24.5xx: "UE policies for 5G System (5GS)".

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

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

[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 mobile terminals and mobile users".

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].

NWu: In this specification, 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
PDU Session

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

NAI

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

SUPI

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
ANDS	Access Network Discovery and Selection
ANDSP	Access Network Discovery and Selection Policy
AUSF	Authentication Server Function
CP	Control Plane
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
N3AN	Non-3GPP Access Network
N3IWF	Non-3GPP InterWorking Function

NAI	Network Access Identifier
QFI	QoS Flow Identifier
SA	Security Association
SPI	Security Parameters Index
SUPI	Subscription Permanent Identifier
UL	Uplink
UP	User Plane
UPF	User Plane Function
WLANSP	WLAN Selection Policy

4 General

4.1 Overview

The 5G core network supports the connectivity of the UE via non-3GPP access networks. In this release of specification, only untrusted non-3GPP access is supported.

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.

SUPI can take two types of representations: IMSI (see 3GPP TS 23.003 [8]) or NAI as defined in 3GPP TS 23.003 [8]. When used over non-3GPP access, IMSI representation can be contained within the NAI for the SUPI.

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

Editor's note: NAI format for 5GCN is FFS by CT4.

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.

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 untrusted 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.

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 untrusted non-3GPP access procedure, the UE or network requested PDU session modification via untrusted 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, the N3IWF determines the number of IPsec child SAs to establish and the QoS profiles associated with each IPsec child SA. The N3IWF then initiates IPsec SA creation procedure to establish Child SAs associating to the QoS flows of the PDU session.

4.4.2.3 QoS differentiation in user plane

For uplink, the UE associates an uplink user data packet with a QFI as specified in 3GPP TS 24.501 [4]. The UE shall then the uplink user data packet with 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.

For downlink, the UPF maps the user data packet to a QoS flow. 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.

4.4.2.4 Reflective QoS

Reflective QoS is also supported when the UE accesses the 5GCN via untrusted non-3GPP access network as specified in 3GPP TS 23.502 [3]. If the N3IWF receives a downlink user packet associated with Reflective QoS Indicator (RQI), the N3IWF shall set the RQI in the GRE header when the N3IWF encapsulates the downlink user data packet into a GRE encapsulated user data packet as specified in subclause 8.3.

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.

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.

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 24.5xx [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 both HPLMN and VPLMN, the UE gives priority to the valid WLANSP rules from the VPLMN. 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 (see subclause 5.3.2.2). 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:

- 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 5.3.2.3); and
- 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 5.3.2.4).

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;

b) if the UE is roaming over 3GPP access, the UE may have valid WLANSP policies from both the VPLMN and the HPLMN. WLANSP rules from the HPLMN will have lower priority from the WLANSP rules from the VPLMN.

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

a) use the procedures specified in the IEEE 802.11-2012 [19] to discover the available WLANs. The UE may perform ANQP procedures as specified in the IEEE 802.11-2012 [19] or the Hotspot 2.0 [20] to discover the attributes and capabilities of available WLANs; and

b) 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 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: If there are multiple highest priority selection criteria, it is up to the UE implementation which one to use.

2) if HomeNetworkInd is not set to "1" in the included group of selection criteria, within a valid WLANSP rule, 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. If there are multiple highest priority selection criteria, it is up to the UE implementation which one to use; and

3) if HomeNetworkInd is set to "1" in the included group of selection criteria, then the UE shall create a list of available WLANs that directly interwork with the home operator 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 domain name list (see IEEE 802.11-2012 [19]) includes:

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

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

4) for both 2) and 3) above, the priority of a WLAN in the available WLANs list is set to the WLAN priority defined in the preferredSSIDlist of the matching selection criteria. There may be one or more selected WLANs in the list.

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

6.2 Untrusted Accesses

In this release of specification, only untrusted non-3GPP access is supported.

6.3 Authentication and authorization for accessing 5GS via an untrusted 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.

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 over non-3GPP access network.

ANDSP consists of:

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

The UE uses the WLANSP for selecting the WLAN access network.

NOTE: In this release of the specification, ANDSP contains configuration for selecting a WLAN access network. Configuration for selecting other types of non-3GPP access networks is not specified.

The UE uses the Non-3GPP access network (N3AN) node configuration for selecting a N3AN node.

When roaming, the UE can receive ANDSP from h-PCF or v-PCF or both.

The structure and the content of ANDSP are defined in 3GPP TS 24.xxx [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-evalaute 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 dependant. 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) provided by PCF to determine the selected WLAN as described in subclause 5.3:

6.8.2.3 Use of N3AN node information

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

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 can be initiated by the UE or the N3IWF as specified in 3GPP TS 33.501 [5].

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 configured by the HPLMN in the UE and based on the UE's knowledge of the country the UE is located in and the PLMN the UE is attached to.

7.2.2 N3AN node configuration information

The N3AN node configuration information is provided to the UE either by PCF or via implementation specific means. Implementation specific means apply only if the configurations from PCF are not present.

The N3AN node configuration information shall consist of the following:

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

The N3AN node configuration information is provisioned in "N3AN node" as specified in 3GPP TS 24.5xx [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 N3IWF selection procedure, the UE shall stop the N3IWF selection. Once the UE determines the country the UE is located in, the UE shall proceed with N3IWF 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 broadcasted on the BCCH of the 3GPP access against the UE's IMSI to determine if they belong to the same country, as defined in 3GPP TS 23.122 [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 based on the country the UE is located in

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].

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; and

- the N3AN ePDG preferred parameter in the N3AN node selection information.

The UE shall proceed as follows:

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

   1) if the N3AN node selection information is provisioned in the N3AN node configuration information and if an entry for the HPLMN is available in the N3AN node selection information, the UE shall construct an N3IWF FQDN based on configured FQDN format of HPLMN as specified in 3GPP TS 23.003 [8]:

   2) if the N3AN node selection information is not provisioned in the N3AN node configuration information or if the N3AN node selection information is provisioned and an entry for the HPLMN is not available in the N3AN node selection information, the UE shall:

i) if Home N3IWF identifier is provisioned in the N3AN node configuration information, use the configured IP address to select the N3IWF, or if configured IP address is not available, construct an N3IWF FQDN using the configured FQDN; and

ii) if the Home N3IWF identifier is not provisioned in the N3AN node configuration information, 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

3) if the N3AN node configuration information is not configured on the UE, or the N3AN node configuration information is configured but empty, 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 cases a) through c), 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 an IP address of an N3IWF with the same IP version as its local IP address;

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

1) if the N3AN node selection information is provisioned in the N3AN node configuration information and if the UE is registered to a VPLMN via 3GPP access:

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

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

and for case i) and ii), 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 an 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 configured;
- the N3AN node selection information is not provisioned in the N3AN node configuration information; or
- the UE is registered to a VPLMN via 3GPP access and an entry for the VPLMN is not available in the N3AN node selection information and an 'Any_PLMN' entry is not available in the N3AN node selection information,

the UE shall perform a DNS query (see 3GPP TS 23.003 [8]) as specified in subclause 7.2.4.2.2 to determine if the visited country mandates the selection of N3IWF in this country:

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

A) if the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is included in one of the returned DNS records, the UE shall select an N3IWF in this VPLMN by constructing an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the VPLMN 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 DNS records:

- if the N3AN node selection information is provisioned, the UE shall select an N3IWF from a PLMN included in the DNS response that has highest PLMN priority (see 3GPP TS 24.5xx [17]) in the N3AN node selection information and construct an N3IWF FQDN based on the configured FQDN format of the PLMN entry as specified in 3GPP TS 23.003 [8]; and
- if the N3AN node selection information is not provisioned or the N3AN node selection information does not contain any of the PLMNs in the DNS response, selection of the PLMN is UE implementation specific. The UE shall select an N3IWF from a PLMN included in the DNS

response and construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the 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 an IP address of an N3IWF with the same IP version as its local IP address;

ii) if the DNS response contains no records, selection of N3IWF in visited country is not mandatory:

A) if the N3AN node selection information is provisioned and contains one or more PLMNs in the visited country, the UE shall select an N3IWF from a PLMNs that has highest PLMN priority (see 3GPP TS 24.5xx [17]) in the N3AN node selection information;

B) if the N3AN node selection information is not provisioned or if the N3AN node selection information is provisioned and contains no PLMNs in the visited country, the UE shall select an N3IWF in the HPLMN as follows:

- if the Home N3IWF identifier is provisioned in the N3AN node configuration information (see 3GPP TS 24.5xx [17]), the UE shall use the configured IP address to select the N3IWF, or if configured IP address is not available, use the configured FQDN and run DNS query to obtain the IP address(es) of the N3IWF(s); and

- if the Home N3IWF identifier 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, 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 an 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 N3IWF 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 selecting an N3IWF in the HPLMN fails, 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.

Upon reception of a DNS response containing one or more IP addresses of N3IWFs, the UE shall select an IP address of N3IWF with the same IP version as its local IP address. If the UE does not receive a response to an IKE_SA_INIT request message sent towards to any of the received IP addresses of the selected N3IWF, 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 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 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 Node selection for IMS service

If the node selection is required for an IMS service, the UE shall use the N3AN ePDG preferred parameter in 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 and

1) if the N3AN node selection information is provisioned in the N3AN node configuration information and if an entry for the HPLMN is available in the N3AN node selection information:

i) if the N3AN ePDG preferred parameter for the HPLMN entry indicates that N3IWF is preferred:

A) if the Home N3IWF identifier is provisioned in the N3AN node configuration information, shall use the configured IP address to select the N3IWF, or if configured IP address is not available, construct an N3IWF FQDN using the configured FQDN; and

B) if the Home N3IWF identifier is not provisioned in the N3AN node configuration information, the UE shall construct an N3IWF FQDN based on configured FQDN format of HPLMN as specified in 3GPP TS 23.003 [8]; and

ii) if the N3AN ePDG preferred parameter for the HPLMN entry indicates that ePDG is preferred:

A) if the Home ePDG identifier is provisioned in the N3AN node configuration information, use the configured IP address to select the ePDG, or if configured IP address is not available, construct an ePDG FQDN using the configured FQDN; and

B) if the Home ePDG identifier is not provisioned in the N3AN node configuration information, the UE shall construct an ePDG FQDN based on configured FQDN format of HPLMN as specified in 3GPP TS 23.003 [8]:

2) if the N3AN node selection information is not provisioned in the N3AN node configuration information or if the N3AN node selection information is provisioned and an entry for the HPLMN is not available in the N3AN node selection information, the UE shall:

i) if Home N3IWF identifier is provisioned in the N3AN node configuration information, use the configured IP address to select the N3IWF, or if configured IP address is not available, construct an N3IWF FQDN using the configured FQDN; and

ii) if the Home N3IWF identifier is not provisioned but Home ePDG identifier is provisioned in the N3AN node configuration information, use the configured IP address to select the ePDG, or if configured IP address is not available, construct an ePDG FQDN using the configured FQDN; and

iii) if neither the Home N3IWF identifier nor the Home ePDG identifier is provisioned in the N3AN node configuration information, 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

Editor's note: The procedure needs to be updated to take into account usage of 'any PLMN' entry configuration.

3) if the N3AN node configuration information is not configured on the UE, or the N3AN node configuration information is configured but empty, 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 cases a) through c), 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 an IP address of an N3IWF or an ePDG with the same IP version as its local IP address;

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

1) if the N3AN node selection information is provisioned in the N3AN node configuration information and if the UE is registered to a VPLMN via 3GPP access:

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

A) if the N3AN ePDG preferred parameter for the VPLMN entry indicates that N3IWF is preferred, the UE shall construct an N3IWF FQDN based on configured FQDN format of the VPLMN as specified in 3GPP TS 23.003 [8]: and

B) if the N3AN ePDG preferred parameter for the HPLMN entry indicates that ePDG is preferred, the UE shall construct an ePDG FQDN based on configured FQDN format of the VPLMN as specified in 3GPP TS 23.003 [8]: and

ii) if an entry for the VPLMN is not available in the N3AN node selection information, and an 'Any_PLMN' entry is available in the N3AN node selection information:

A) if the N3AN ePDG preferred parameter for the 'Any_PLMN' entry indicates that N3IWF is preferred, the UE shall construct an N3IWF FQDN based on configured FQDN format of the 'Any_PLMN' as specified in 3GPP TS 23.003 [8]: and

B) if the N3AN ePDG preferred parameter for the 'Any_PLMN' entry indicates that ePDG is preferred, the UE shall construct an ePDG FQDN based on configured FQDN format of the 'Any_PLMN' as specified in 3GPP TS 23.003 [8],

and for case i) and ii), 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 an 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 configured;
- the N3AN node selection information is not provisioned in the N3AN node configuration information; or
- the UE is registered to a VPLMN via 3GPP access and an entry for the VPLMN is not available in the N3AN node selection information and an 'Any_PLMN' entry is not available in the N3AN node selection information,

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:

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

A) if the UE is registered to a VPLMN via 3GPP access and the PLMN ID of VPLMN is included in one of the returned DNS records, the UE shall select an N3IWF in this VPLMN by constructing an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the VPLMN 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 DNS records:

- if the N3AN node selection information is provisioned, the UE shall select an N3IWF from a PLMN included in the DNS response that has highest PLMN priority (see 3GPP TS 24.5xx [17]) in the N3AN node selection information and construct an N3IWF FQDN based on the configured FQDN format of the PLMN entry as specified in 3GPP TS 23.003 [8]; and

- if the N3AN node selection information is not provisioned or the N3AN node selection information does not contain any of the PLMNs in the DNS response, selection of the PLMN is UE implementation specific. The UE shall select an N3IWF from a PLMN included in the DNS response and construct an N3IWF FQDN based on the Operator Identifier FQDN format using the PLMN ID of the 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 an IP address of an N3IWF with the same IP version as its local IP address;

ii) if the DNS response contains no records, selection of N3IWF in visited country is not mandatory:

A) if the N3AN node selection information is provisioned and contains one or more PLMNs in the visited country, the UE shall select an N3IWF from a PLMN that has highest PLMN priority (see 3GPP TS 24.5xx [17]) in the N3AN node selection information;

B) if the N3AN node selection information is not provisioned or if the N3AN node selection information is provisioned and contains no PLMN in the visited country, the UE shall select an N3IWF in the HPLMN as follows:

- if the Home N3IWF identifier is provisioned in the N3AN node configuration information (see 3GPP TS 24.5xx [17]), the UE shall use the configured IP address to select the N3IWF, or if configured IP address is not available, use the configured FQDN and run DNS query to obtain the IP address(es) of the N3IWF(s); and

- if the Home N3IWF identifier 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, 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 an 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 N3IWF selection procedure.

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

a) if N3IWF is selected, the UE shall:

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

ii) if selecting an N3IWF in the HPLMN fails, 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 UE does not receive a response to an IKE_SA_INIT request message sent towards any of the received IP addresses of the selected N3IWF, attempt to select an ePDG in the same PLMN 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 2: 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 ePDG is selected, the UE shall:

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

ii) if selecting an ePDG in the HPLMN fails, and the selection of ePDG in the HPLMN is performed using Home ePDG identifier configuration and there are more pre-configured 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 the UE does not receive a response to an IKE_SA_INIT request message sent towards any of the received IP addresses of the selected ePDG, 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 3: 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 Node selection for Non-IMS service

If the node selection is required for a non-IMS service, the UE shall consider that N3IWF node is preferred regardless of the "Preference" parameter setting. The UE shall proceed as follows:

a) the UE shall follow steps specified in subclause 7.2.4.3 to select N3IWF by ignoring the N3AN ePDG preferred parameter setting; and

b) if the UE fails to connect to an N3IWF in any PLMN after step 1), the UE may repeat the N3AN node selection by following procedures specified in 3GPP TS 24.302 [7] and attempt to select an ePDG instead.

7.3 IKEv2 SA establishment procedure

7.3.1 General

The purpose of this procedure is to establish a secure connection between the UE and the N3IWF, which is used to securely exchange NAS signalling messages between the UE and the AMF, via the N3IWF. The UE establishes a 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] (see step 2 in the registration procedure for untrusted non-3GPP access in 3GPP TS 23.502 [3]). Upon reception of the IKE_SA_INIT exchange the UE shall inform the upper layers that the access stratum 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

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.

When the EAP-5G session is completed the UE receives from the N3IWF an IKE_AUTH response message with an EAP-Success message. 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].

This completes the establishment of the IKE SA and signalling IPsec SA between the UE and the N3IWF. The UE and the N3IWF shall send further NAS messages within the signalling IPsec SA (first child SA) (see example in figure 7.3.2-1).

Editor's note: It is FFS how the signalling IPsec SA is handled in case of rekeying of the IKE SA.

An example of an IKE SA and first child SA establishment procedure is shown in figure 7.3.2-1.

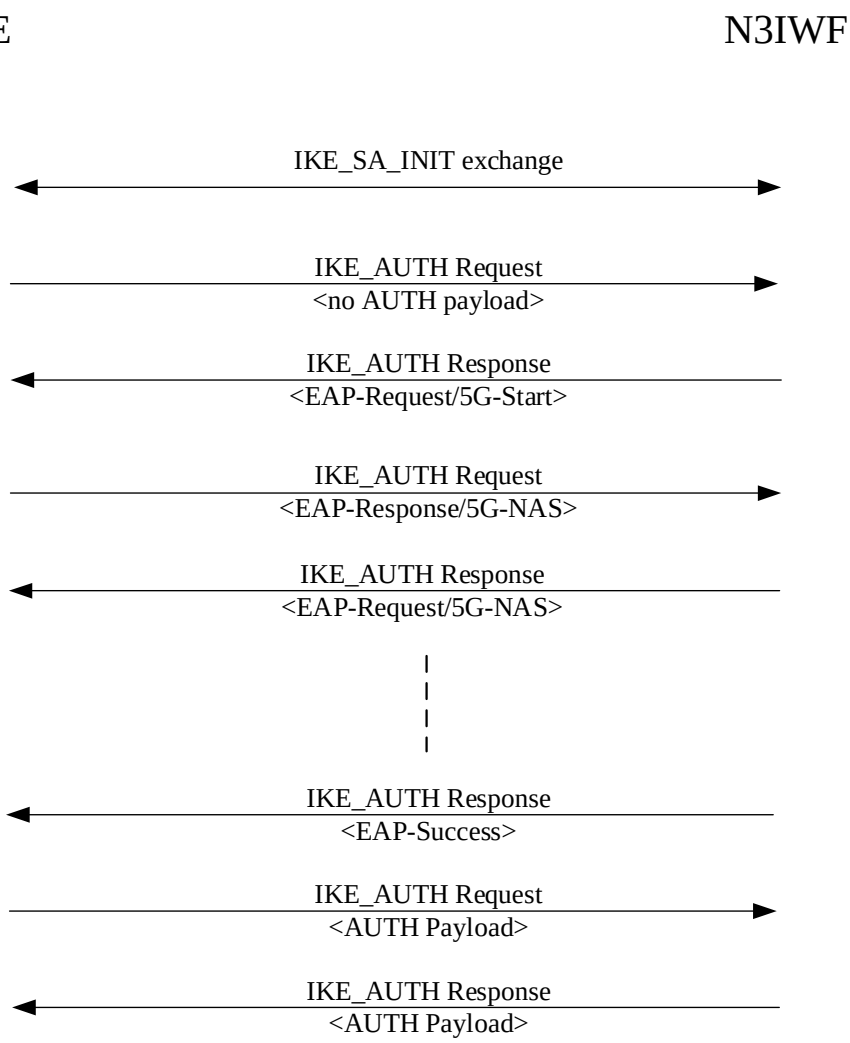

Figure 7.3.2-1: IKE SA and first child SA establishment procedure for UE registration over non-3GPP access

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

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 NAS messages (not for authentication).

The UE and the N3IWF 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 that contains a NAS message, for example, a REGISTRATION REQUEST message; and

b) an AN-parameters field that contains access network parameters, such as S-NSSAI, 5G-GUTI, etc. (see 3GPP TS 23.502 [3]).

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

a) 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.

On reception of the N3IWF key from the AMF, the N3IWF completes the EAP-5G procedure 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 procedure is shown in figure 7.3.3-1.

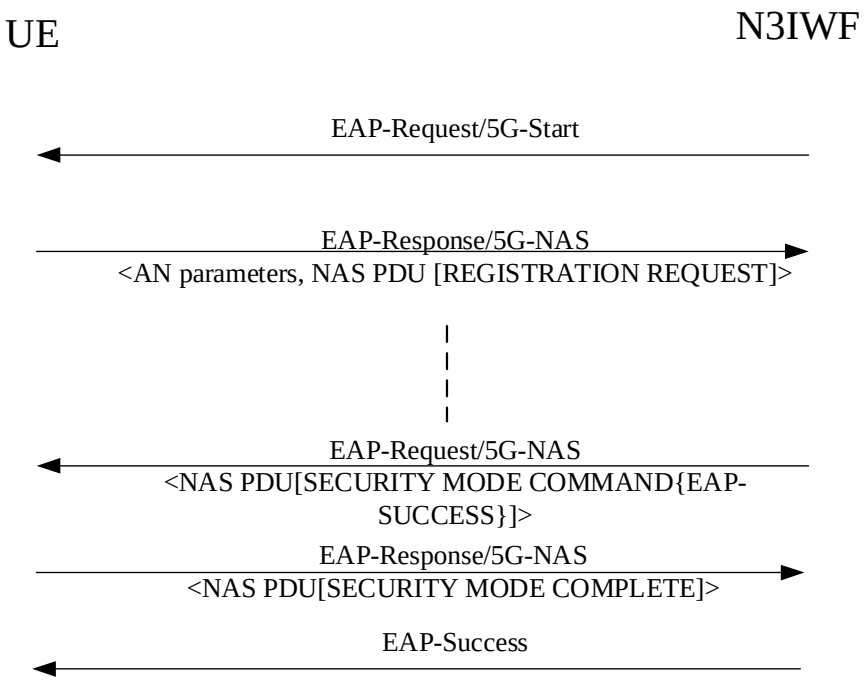

Figure 7.3.3-1: EAP-5G session for UE registration over non-3GPP access

7.3.4 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE for this specific procedure (not specified in IETF RFC 7296 [6]) are FFS.

7.3.5 Abnormal cases in the N3IWF

Editor's note: The abnormal cases in the N3IWF for this specific procedure (not specified in IETF RFC 7296 [6]) are FFS.

7.4 IKEv2 SA deletion procedure

7.4.1 General

The purpose of the IKE SA deletion procedure for de-registration via untrusted non-3GPP access is to delete the IKE SA of the UE. This procedure shall be initiated by the N3IWF.

7.4.2 IKE SA deletion procedure initiation

The N3IWF 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 Protocol ID shall be set to "1" and no subsequent SPI in the Delete payload. This indicates that the IKE security association and all IPsec ESP security associations that were negotiated within it between the N3IWF and the UE shall be deleted.

7.4.3 IKE SA deletion procedure accepted by the UE

If the UE accepts the INFORMATIONAL request message for deletion of the IKE SA, the UE shall send an empty INFORMATIONAL response message to the N3IWF as specified in IETF RFC 7296 [6].

Upon accepting the request for deletion of the IKE SA the UE shall inform the upper layers that the access stratum connection has been released.

7.4.4 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE for this specific procedure (not specified in IETF RFC 7296 [6]) are FFS.

7.4.5 Abnormal cases in the N3IWF

Editor's note: The abnormal cases in the N3IWF for this specific procedure (not specified in IETF RFC 7296 [6]) are FFS.

7.5 User plane IPsec SA creation procedure

7.5.1 General

The purpose of the user plane IPsec SA creation procedure during the UE requested PDU session establishment is to establish a Child SA associating to the QoS flows of the PDU session. This procedure shall be initiated by the N3IWF.

One user plane IPsec SA can be associatedwith one or more QoS flows of the PDU session. During PDU session establishment or PDU session modification via untrusted non-3GPP access, the N3IWF 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 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) USE_TRANSPORT_MODE notification; and

b) 5G_QOS_INFO Notify payload which contains:

1) PDU session ID;

2) QFI(s); and

3) optionally a DSCP value.

The IKE Create_Child_SA request also contains the SA payload for the requested Child SA.

The content of 5G_QOS_INFO Notify payload is described in subclause 9.2.1.1.

Editor's note: How to handle the packet in transport mode is FFS.

7.5.3 Child SA creation procedure accepted by the UE

If the UE accepts the CREATE_CHILD_SA request message, the UE shall send a CREATE_CHILD_SA response message as specified in IETF RFC 7296 [6].

The CREATE_CHILD_SA response message shall include:

a) USE_TRANSPORT_MODE notification.

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 the UE does not accept the Child SA creation, the UE shall send a CREATE_CHILD_SA response message with the corresponding Notify payload of error type as specified in IETF RFC 7296 [6].

Editor's note: Whether 5G specific private Notify Message - Error Types needs to be defined is FFS.

Editor's note: The behaviour of the N3IWF is FFS upon receipt of the CREATE_CHILD_SA response message indicating failure of the procedure.

7.5.5 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE for this specific procedure (not specified in IETF RFC 7296 [6]) are FFS.

7.5.6 Abnormal cases in the N3IWF

Editor's note: The abnormal cases in the N3IWF for this specific procedure (not specified in IETF RFC 7296 [6]) are FFS.

7.6 IPSec SA modification procedure

This sub-clause will describe IPSec child SA modification procedure via untrusted non-3GPP access.

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 by the N3IWF.

7.7.2 Child SA deletion procedure initiation

The N3IWF 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 Security Parameter Index(es) associated to the released PDU session.

7.7.3 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 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.

Editor's note: The possible Notify messages for status type in the INFORMATIONAL response message are FFS.

7.7.4 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE for this specific procedure (not specified in IETF RFC 7296 [6]) are FFS.

7.7.5 Abnormal cases in the N3IWF

Editor's note: The abnormal cases in the N3IWF for this specific procedure (not specified in IETF RFC 7296 [6])

8 Message Transport procedures

8.1 General

The sub-clause provides general overview of message encapsulation procedures for non-3GPP access.

8.2 Transport of NAS messages over control plane

8.2.1 General

After the completion of IKE SA and establishment of signalling IPsec SA as specified in subclause 7.3, the UE performs non-access stratum (NAS) procedures over the signalling IPsec security associations via an untrusted non-3GPP access network. All uplink and downlink NAS mobility management and session management messages are relayed between the UE and the AMF via N3IWF.

8.2.2 ESP encapsulation

When NAS messages are transported over Non-3GPP access between the UE and N3IWF, all the messages shall be encapsulated by ESP protocol in transport mode as specified in IETF RFC 4303 [11].

Editor's note: whether the UE and the N3IWF shall exchange the NAS messages via the TCP connection for exchange of NAS messages is FFS.

Editor's note: it is FFS towards which TCP port the UE establishes the TCP connection.

Editor's note: framing of NAS messages (i.e. determining when a particular NAS message ends and another NAS message starts) is FFS.

ESP packet format is shown in figure 8.2.2-1,

Figure 8.2.2-1: ESP packet format

Bits 7	6	5	4	3	2	1	0	Octets	ESP
Security Parameters Index (SPI)								1-4	
Sequence Number								5-8	
Payload data (NAS message)								9-m	
Padding								(m+1) - n	
Padding length								n+1	Security Index is
Next header								n+2	
Integrity Check Value (ICV)								(n+2) - x	

In the ESP packet,

a) the ESP Parameter corresponding to the signalling IPsec SA; and

b) the value of next header field shall be set to xxx.

Editor's note: The value of next header field is FFS.

8.3 Transport of messages over user plane

8.3.1 General

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

8.3.2 GRE encapsulation

A user data packet is transported in a GRE encapsulated user data packet as specified in subclause 9.3.3.

The GRE encapsulated user data packet is transported using ESP protocol in transport mode as specified in IETF RFC 4303 [11] between the UE and the N3IWF. In the ESP packet:

a) the ESP Security Parameter Index is corresponding to the user plane IPsec SA;

b) the value of next header field shall be set to 2FH; and

c) the payload data field shall contain the GRE encapsulated user data packet.

In the GRE encapsulated user data packet:

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 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"; and

d) if the N3IWF does not need to send RQI for a downlink user data packet or 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".

Due to the application of IPsec to IP fragments being prohibited for IPSec in transport mode (see IETF RFC 4301 [12]), the sending entity (UE or N3IWF) shall create an IP packet carrying the entire GRE encapsulated user data packet, irrespective of the path MTU between the UE and the N3IWF, and shall apply IPsec on the unfragmented IP packet carrying the entire GRE encapsulated user data packet.

NOTE: IP packet created by application of IPsec can be fragmented by the sending entity based on the path MTU between the UE and the N3IWF.

If a non-3GPP access network does not support transport of IP fragments, the maximum size of a user data packet is equal to the path MTU between the UE and N3IWF, decreased by the length of the IP header, the length of the ESP header and trailer and the length of the GRE header.

EXAMPLE: If a non-3GPP access network is an IPv6 only network which does not support transport of IP fragments, the path MTU between the UE and the N3IWF is 1280 octets and the length of IPv6 header is 40 octets then the maximum size of the user data packet is 1222 octets.

9 Parameters and coding

9.1 General

9.2 3GPP specific coding information

This sub-clause will describe coding information that are 3GPP specific, e.g. cause values, private message types.

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 the PDU session identity, QFI and optionally a DSCP value associated with the child SA.

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
DSCP								x+1

Figure 9.3.1.1-1: 5G_QOS_INFO Notify payload format

Table 9.3.1.1-1: 5G_QOS_INFO 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 xxxxx 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 PDU Session Identity field. This field indicates the PDU session associated with the child SA for user plane. Octet 7 is Number of QFIs field. This field indicates the number of QFIs in the QFI list. Octets 8 to octet x is 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 is the DSCP field. If included, this field indicates the DSCP marking for all IP packets sent over this child SA.

Editor's note: How to assign the value of Notify Message Type field is FFS.

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

9.3.2.2.2.1 General

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-parameter length								15-16
AN-parameter								17 - 16+x
NAS-PDU length								17+x - 18+x
NAS-PDU								19+x - n+x
Extensions								n+x+1 - z+x

Figure 9.3.2.2.2.1-1: EAP-Response/5G-NAS message

Table 9.3.2.2.2.1-1: 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 indicate the length of the AN-parameters field in octets AN-Parameters field is coded according to figure 9.3.2.2.2.1-2 and table 9.3.2.2.2.1-2. 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.

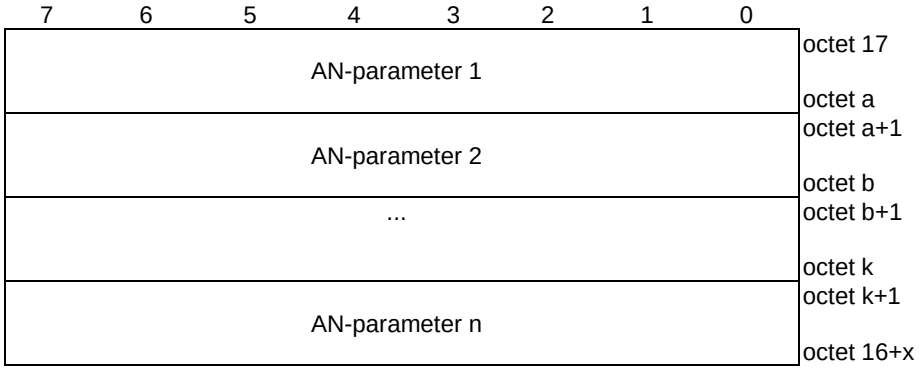

Figure 9.3.2.2.2.1-2: AN-parameters field

Table 9.3.2.2.2.1-2: AN-parameters field

Each AN-parameter field is coded according to figure 9.3.2.2.2.1-3 and table 9.3.2.2.2.1-3.

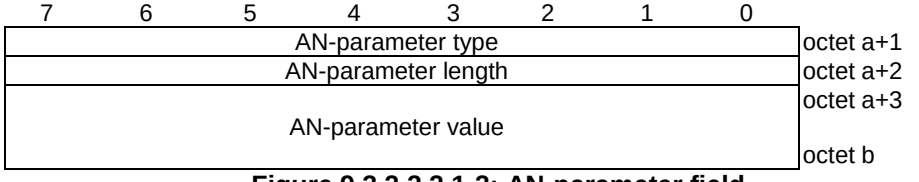

Figure 9.3.2.2.2.1-3: AN-parameter field

Table 9.3.2.2.2.1-3: 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 (5GS mobile identity); - 02H (selected PLMN ID); - 03H (requested NSSAI); and - 04H (establishment cause). All other values of the AN-parameter type field are spare. When the AN-parameter type field indicates the 5GS mobile identity, the AN-parameter value field is set to FFS. When the AN-parameter type field indicates the selected PLMN ID, the AN-parameter field is coded according to subclause 9.3.2.2.2.2. When the AN-parameter type field indicates the requested NSSAI, the AN-parameter value field is set to FFS. When the AN-parameter type field indicates the establishment cause, the AN-parameter field is set to FFS.

Editor's Note: FFS whether to indicate 5GS mobile identity by reusing the 5GS mobile identity IE specified in 3GPP TS 24.501, or whether to reuse any RAN2 specified coding.

Editor's Note: FFS whether to indicate requested NSSAI by reusing the NSSAI IE specified in 3GPP TS 24.501, or whether to reuse any RAN2 specified coding.

Editor's Note: FFS whether to indicate establishment cause by reusing any RAN2 specified coding or whether to define own coding.

9.3.2.2.2.2 Selected PLMN ID AN-parameter field

7	6	5	4	3	2	1	0	
AN-parameter type								octet a+3
AN-parameter length								octet a+4
MCC digit 2				MCC digit 1				octet a+5
MNC digit 3				MCC digit 3				octet a+6
MNC digit 2				MNC digit 1				octet a+7

Figure 9.3.2.2.2.2-1: Selected PLMN ID AN-parameter field

Table 9.3.2.2.2.2-1: Selected PLMN ID AN-parameter field

The AN-parameter type field is set to the selected PLMN ID according to subclause 9.3.2.2.2.1. The AN-parameter length field is set to three according to subclause 9.3.2.2.2.1. MCC, Mobile country code (octet a+5, octet a+6 bits 0 to 3) The MCC field is coded as in ITU-T Recommendation E.212 [21], Annex A. MNC, Mobile network code (octet a+7, octet a+6 bits 4 to 7). 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 5 shall be coded as "1111".

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 and table 9.3.2.2.3-1.

Bits 7	6	5	4	3	2	1	0	Octets
Code								1
Identifier								2
Length								3 - 4
Type								5
Vendor-Id								6 - 8
Vendor-Type								9 - 12
Message-Id								13
Spare								14
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.

9.3.3 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 8 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 XXX. 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.

Editor's note: value of the Protocol Type field is FFS. the protocol type field contains an EtherType, to be reserved by IEEE at http://standards.ieee.org/develop/regauth/ethertype/index.html.

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

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

History

Document history		
V15.0.0	June 2018	Publication