ETSI TS 124 502 V16.6.0 (2021-01)

5G;
Access to the 3GPP 5G Core Network (5GCN) via non-3GPP access networks
(3GPP TS 24.502 version 16.6.0 Release 16)

Reference
RTS/TSGC-0124502vg60

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

Copyright Notification

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

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:

Non 5G capable over WLAN (N5CW) device
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. Different types of trusted connectivity can be advertised so that the UE can discover the non-3GPP access networks that can provide trusted connectivity to one or more PLMNs:

a) information about PLMN list with 5G connectivity using trusted non-3GPP access;

b) information about PLMN list with 5G connectivity without NAS using trusted non-3GPP access; or

c) information about PLMN list with S2a connectivity using trusted non-3GPP access (access via non-3GPP access to EPC).

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].