Wi-Fi Roaming Guidelines
Version 14.0
28 May 2021

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Scope

The main purpose of this document is to describe the Wi-Fi Access to the

- Evolved 3GPP Evolved Packet Core (EPC) as defined in the 3GPP specifications TS 23.402 and TS 24.302, e.g. for devices based on GSMA PRD IR.51. For EPC, the document is based on 3GPP Release 11 and unless otherwise stated.
- 3GPP 5G Core (5GC) as defined in the 3GPP specifications TS 23.501 and TS 23.502, e.g. for devices based on GSMA PRD NG.115. For 5GC, the document is based on 3GPP Release 15 and subsequent releases where appropriate.

The document concentrates on the roaming scenarios but also it includes some non-roaming scenarios to give the overall picture, including the mobility between both E-UTRAN and pre-E-UTRAN, as well as between both NR and E-UTRAN, policy control and charging, and authentication.

The main focuses of the current version of the document are:

- For EPC, S2b and S2a interfaces using GTP. Out of scope are the S2c interface and usage of PMIP (for both S2b and S2a).
- For 5GC, the interfaces (typically N2 and N3) supported by the Untrusted Non-3GPP interworking function for 5GC access

Note: The case of Non-seamless or non-CN integrated offload (i.e. data traffic directly to a data network without passing through EPC or 5GC) is not explicitly defined in this PRD.

2 Abbreviations and Terminology

Abbreviation	Term	Description
	Access Independence	The WLAN UE is able to establish WLAN 3GPP IP Access connectivity and access 3GPP PS services without prior authentication to WLAN 3GPP Direct Access.
	Accounting	The process of collecting resource usage measurements and apportioning charges for joint service between interworking and/or co-operating service/network providers.
	Billing	A function whereby Call Detail Records generated by the charging function are transformed into bills requiring payment.
	Customer	A business entity or an individual with a direct contractual relation to receive the Service from the Home Wi-Fi Service Provider.

Abbreviation	Term	Description
	Home Wi-Fi	The network operated by the Home Wi-Fi Service Provider-.
	RADIUS Roaming Proxy (WLAN Roaming Proxy)	RADIUS Roaming Proxy (or WLAN Roaming Proxy) shall mean a component transporting RADIUS messages from the visited Wi-Fi Service Provider to Home Wi-Fi Service Provider (and vice versa). This component typically also carries out some security functions. The interface between RADIUS Roaming Proxies is an inter-operator interface described in this document.
	Roaming Agreement	Agreement between two parts to enable the end users of each one to utilize the other network parts using their Home account service provider authentication parameters.
	Roaming Partner	The WO who has entered into a Roaming Agreement with another WO.
	Roaming Service	Roaming Service in this document means provision of Internet service over WLANs for customers of another WO, also known as the Roaming Partner. The Roaming Service enables customers from Roaming Partners to access at least their subscribed services through each other's network by using the same authentication credentials as in its Home WLAN
	User	The individual receiving the Service.
	Visited Wi-Fi	The network operated by the Visited Wi-Fi Service Provider -
	Non-seamless WLAN Access/Offload Note: This is to use the same terminology as 3GPP and also to avoid any confusion with "WiFi Direct" feature now supported by some UEs.	The WLAN UE has an access to an IP network directly from a WLAN AN without passing data to a PMN (e.g. EPC) via a tunnel. It is a non-EPC based solution.
	WLAN 3GPP IP Access	The WLAN UE is allowed to access 3GPP PS based services provided via WLAN. The data traffic gets always routed.
3GPP AAA-Proxy		3GPP defined RADIUS and Diameter AAA proxy for the 3GPP Rel-6
3GPP AAA-Server		3GPP defined RADIUS and Diameter AAA server for the 3GPP Rel-6
5GC(N)	5G Core (Network)	The CN specified in 3GPP TS 23.501. It connects to a 5G Access Network
802.1X PAE	IEEE 802.1X Port Access Entity	The logical port controlling the flow of user data on an 802.1X enabled Access Point till authentication is complete.

Abbreviation	Term	Description
AC	Access Controller	
Alternative NAI	Alternative Network Access Identifier	A NAI that shall have the form of: '<any_non_null_string>@unreachable.3gppnetwork.org'
ANDSF	Access Network & Discovery & Selection Function	3GPP framework comprising of a network entity (ANDSF Server) and a UE entity (ANDSF Client) that supports operator's policies for network selection and traffic steering between 3GPP and non-3GPP accesses (e.g. WLAN).
ANDSP	Access Network & Discovery & Selection Policy	Policy used by the UE for selecting non-3GPP accesses and for selection of the N3IWF in the PLMN
AP	Access Point	Interface between the radio network part and the wired network part of a WLAN network, offering wireless connectivity to MTs
Decorated NAI	Decorated Network Access Identifier	A NAI that shall have the form 'Homerealm!username@visitedrealm'
Diameter		Authentication, Authorization and Accounting (AAA) protocol
DN(N)	Data Network (Name)	The data network (name) of the network connected to the UPF over N6
EAP	Extensible Authentication Protocol	A protocol to transfer authentication information between a MT and a Home WO AAA-server.
EAP-AKA	Extensible Authentication Protocol using a USIM profile	Extensible Authentication Protocol with Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (AKA) mechanism method as standardized in RFC 5448
EAP-AKA'	Extensible Authentication Protocol using a USIM profile	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement as standardized in RFC 5448
EAP-SIM	Extensible Authentication Protocol using a SIM profile	Authentication method used with EAP to support authentication using a SIM, as standardized in RFC 4186
EAP-TLS	Extensible Authentication Protocol using a certificate	Authentication method used with EAP to support authentication through Transport Layer Security, in which secure digital certificates are used to mutually identify a user and a server's identity, as standardized in RFC 5216

Abbreviation	Term	Description
EAP-TTLS	Extensible Authentication Protocol using Username/Password	Authentication method used with EAP to support authentication through Tunnelled Transport Layer Security, in which secure digital certificates are used to identify a server's identity (and optionally, a device's or user's identity), establish a tunnel, and then allow for user identification over the encrypted tunnel, as standardized in RFC 5281 tools. Note: that there is often an inner EAP method used with EAP-TTLS, such as MSCHAPv2 (see RFC 2759).
EPC	Evolved Packet Core	EPC is an end-to-end packet core architecture for 4G Long-Term Evolution (LTE) that provides a converged voice and data networking framework to connect users to an LTE network
ePDG	Evolved Packet Data Gateway	IPsec GW that connects UE to Untrusted Non-3GPP network
EPS	Evolved Packet System	
Fast Re-authentication NAI	Fast Re-authentication Network Access Identifier	A NAI that is optionally used only during the EAP-SIM/AKA/AKA' fast re-authentication procedure. The NAI shall have the form of: '<any_string>@realm' or just '<string>'
FQDN	Fully Qualified Domain Name	An unambiguous (absolute) domain name that specifies the node's position in the DNS tree hierarchy
Home Wi-Fi SP	Home Wi-Fi Service Provider	The Party contracting to provide the Service to its own Customers and authenticates and charges the customer.
HR	Home Routed	Roaming configuration where the core network gateway connected to the data network is in the HPMN while the user is roaming (in the VPMN)
HS2.0	HotSpot 2.0	WFA standardized protocol for the automated network discovery in Wi-Fi networks
IARP	Inter-APN Routing Policy	Operator rules determining which traffic should be routed across which PDN connection and which traffic should be non-seamlessly offloaded to WLAN
IKEv2	Internet Key Exchange version 2	Version 2 of the Internet Key Exchange protocol, which is used to negotiate a Security Association at the outset of an IPsec session.
IPSec	IP Security	A suite of protocols for securing IP communications by authenticating and/or encrypting each IP packet in a data stream.
IREG	International Roaming Experts Group	Working Group within GSMA (now renamed NG, Networks Group)
LBO	Local BreakOut	Roaming configuration where the core network gateway connected to the data network is in the VPMN while the user is roaming (in the VPMN).

Abbreviation	Term	Description
MAC	Message Authentication Codes	These are unique cryptographic values computed and attached to each protocol message to provide message authenticity.
MAP	Mobile Application Part	Mobile related SS7 application protocol that is used in the GSM Core Network to talk to the AuC/HLR.
MNO	Mobile Network Operator	Wireless Cellular service provider having all the necessary equipment to offer related services.
MT	Mobile Terminal	End system equipment providing the interface towards human beings through a set of applications NOTE: The MT includes, among other things, the functions and protocols necessary to provide and handle the communication to the WLAN network, as well as against other networks, services, and applications.
MTP	Message Transfer Part	Layer 1,2,3 of the SS7 stack
N3IWF	Non-3GPP InterWorking Function	The interworking function specified to connect an Untrusted Non-3GPP access to a 5GC(N). It looks (almost) like a 3GPP NR AN to the 5GC
NAS	Non-Access Stratum	Communication path between a UE and core network (functionally transparent to RAN) used to convey non-radio signalling information
NG-RAN	Next Generation Radio Access Network	A 3GPP RAN that supports one or more of the following 4 options with the common characteristics that connects to 5GC (and not to EPC): Stand-Alone NR (New Radio), NR as anchor with E-UTRA extensions, Stand-Alone E-UTRA and E-UTRA as anchor with NR extensions
PCRF	Policy Charging and Rules Function	LTE network functionality that supports service data flow detection, policy enforcement and flow-based charging
PDG	Packet Data Gateway	A 3GPP flavoured IKEv2 IPsec gateway
PDN Gateway / PGW	Packet Data Node Gateway	Gateway acts as the interface between the LTE network and other packet data networks
PDU	Protocol Data Unit	Single unit of information transmitted (using a protocol) between peer network entities
PLMN	Public Land Mobile Network	A specific operator (in a specific country) offering wireless cellular communication services. Referred by GSMA as PMN (Public Mobile Network).
PSPL	Preferred Service Providers List	A prioritised list of service providers preferred by the UE's (3GPP) home operator for WLAN roaming.
Root NAI	Root Network Access Identifier	A NAI, that shall have the form ‘username@realm’.
SA	Security Association	An establishment of shared security information between two network entities to support secure communication.

Abbreviation	Term	Description
SBA	Service Based Architecture	3GPP based service based architecture for communication for CP entities of the 5GC
SCCP	Signalling Control Connection Part	Control part of SS7 protocol that manages Signalling Transfer Points (STPs)
S-GW	Serving Gateway	Routes data packets through the access network.
SS7	Signalling System 7	Circuit Switched Network Signalling Protocol for connection management.
TADIG	Transferred Account Data Interchange Group	Working Group within GSMA. Underlying tasks now roughly handled by IDS (Interoperability Data specifications and Settlement) working group of GSMA
TCAP	Transfer Capabilities Application Part	Mobile related SS7 protocol that is used in the GSM Core Network to talk to the AuC/HLR.
TFT	Traffic Flow Template	Information structure that is used to map a Service Data Flows to a specific Radio Bearer
TWAG	Trusted WLAN Access Gateway	Gateway that interfaces P-GW using S2a.
TWAN	Trusted WLAN Access Network	Trusted WLAN network that does not require the use of IPsec with the UE. The detailed functional split within a TWAN is out of scope of 3GPP. Whether a Non-3GPP access is trusted or not (to the EPC) is left for the (AAA server of the) Home operator to decide.
TWAP	Trusted WLAN AAA Proxy	Relays AAA information between TWAN and 3GPP AAA Server (or Proxy in case of roaming) using the STa (Swd) interface.
UPF	User Plane Function	Data Gateway of 5GC used to access a DN
URSP	UE Route Selection Policy	Policy used by the UE to determine if a detected application can be associated to an established PDU Session, can be seamlessly offloaded or can trigger the establishment of a new PDU Session
Visited Wi-Fi Service Operator	Visited Wi-Fi Service Provider	The Party providing the Roaming Service to the Customer of the other Party.
WAG	WLAN Access Gateway	A 3GPP flavoured Access Controller
W-APN	WLAN APN	WLAN equivalent for GPRS Access Point Name (APN)
WFA	Wi-Fi Alliance	Organization that promotes Wi-Fi technology and certifies Wi-Fi products
Wi-Fi SP	Wi-Fi Service Provider	Owner and/or Provider of Wi-Fi network infrastructure. This entity could be a Mobile Network Operator (MNO) or a Wireless Internet Service Provider (WISP).
WISP	Wireless LAN Internet Service Provider	Internet Service Provider with a network based on WLAN
WLAN	Wireless Local Area Network	Usually referred to the IEEE 802.11 product family.

Abbreviation	Term	Description
WLANSP	WLAN Selection Policies	Operator rules that determine which WLAN AP to select
WLAN UE	WLAN User Equipment	A terminal with WLAN capability
WLCP	WLAN Control Plane (protocol)	Control (only) protocol between UE and TWAG to (dynamically) setup / release a PDN connection when under trusted WLAN access.
WPA	Wi-Fi Protected Access	This is a Wi-Fi Alliance promoted WLAN device security feature set. It includes IEEE 802.1X support, Support for portions of the IEEE 802.11i draft specification namely TKIP and optional AES cipher suite support.
WPA2	Wi-Fi Protected Access II	Security protocols and security certification programs developed by the WFA to secure Wi-Fi based networks, with encryption enhancement compared to plain WPA.
WSOLU	Wholesale SOLUtions	Working Group within GSMA. Underlying tasks now roughly handled by WAS (Wholesale Agreements & Solutions) Working Group of GSMA.

3 References

Document	Name
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
RFC 2869	RADIUS Extensions
RFC 2607	Proxy Chaining and Policy Implementation in Roaming
RFC 5247	PPP Extensible Authentication Protocol (EAP)
RFC 4186	EAP SIM Authentication
RFC 3579	Radius support for Extensible Authentication Protocol
RFC 3580	IEEE 802.1X RADIUS Usage Guidelines
RFC 1851	The ESP Triple DES Transform
RFC 2401	Security Architecture for the Internet Protocol
RFC 4372	The Chargeable User Identity
RFC 4284	Identity Selection Hints for the Extensible Authentication Protocol (EAP)
RFC 4282	The Network Access Identifier
RFC 4306	Internet Key Exchange (IKEv2) Protocol
RFC 5448	EAP-AKA and EAP-AKA' Authentication
RFC 5216	The EAP-TLS Authentication Protocol
RFC 5281	The EAP-TTLS Authentication Protocol
RFC 5580	Carrying Location Objects in RADIUS and Diameter
PRD AA.80	Agreement for IP Packet eXchange (IPX) Services
PRD IR.21	Roaming Database, Structure and Updating Procedures
PRD IR.33	GPRS Roaming Guidelines
PRD IR.34	Inter-PLMN Backbone Guidelines
PRD IR.40	Guidelines for IPv4 Addressing and AS Numbering for GPRS Network Infrastructure and Mobile Terminals
PRD IR.51	IMS Profile for Voice, Video and SMS over Wi-Fi
PRD IR.67	DNS Guidelines for Operators
PRD IR.88	LTE and EPC Roaming Guidelines
3GPP TS 23.003	Numbering, addressing and identification
3GPP TS 23.402	Architecture enhancements for non-3GPP accesses
3GPP TS 24.244	Wireless LAN Control Plane protocol for trusted WLAN access to EPC
3GPP TS 24.302	Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks
3GPP TS 24.312	Access Network Discovery and Selection Function (ANDSF) Management Object

Document	Name
3GPP TS 24.234	WLAN User Equipment (WLAN UE) to network protocols
3GPP TS 29.234	3GPP System to Wireless Local Area Network (WLAN) Interworking; Stage 3; Release-7
3GPP TS 33.234	Wireless Local Area Network (WLAN) interworking security; Release-7
3GPP TS 33.402	Security aspects of non-3GPP accesses
3GPP TS 36.331	Radio Resource Control (RRC); Protocol specification
3GPP TS 25.331	Radio Resource Control (RRC); Protocol specification
3GPP TS 36.304	Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode
3GPP TS 25.304	User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode
IETF RFC 4555	IKEv2 Mobility and Multihoming Protocol (MOBIKE)
3GPP TS 23.501	System Architecture for the 5G System
3GPP TS 23.502	Procedures for the 5G System
3GPP TS 23.503	Policy and Charging Control Framework for the 5G System
PRD NG.113	5GS Roaming Guidelines

4 EPC Overview (Informative)

4.1 EPC Access Overview

3GPP Rel-8 introduced the Enhanced Packet Core (EPC) as part of EPS and the integration of non-3GPP accesses (e.g. WLAN access) into EPC. It also supports home routing and local breakout for the services when UE is roaming.

General guidelines for the EPC roaming environment using 3GPP accesses are described in GSMA PRD IR.88.

4.1.1 EPC-integrated Wi-Fi Overview

Integration of Wi-Fi Access into EPC enables Mobile Services to be available through Wi-Fi. Release-11 and later makes it possible to use mobile services, like IMS-based voice and video, MMS and SMS over IP over the Wi-Fi Access.

Wi-Fi Access is divided into two types of scenarios, one for Trusted Wi-Fi Access and one for Untrusted Wi-Fi Access. In case of Trusted Wi-Fi Access, the Wi-Fi connects directly to the PDN Gateway via S2a interface, using GTP.

In Untrusted Wi-Fi Access an additional IPsec tunnel is established between the UE and the ePDG using a SWn interface. After a successful IPsec tunnel setup, the ePDG forwards the user traffic to the PDN GW via S2b interface using GTP. The HSS/3GPP AAA Server in HPLMN makes the decision of whether a Wi-Fi Access is used as Trusted or Untrusted Wi-Fi

Access. The HSS/3GPP AAA Server may take the VPLMN's policy and capability returned from the 3GPP AAA Proxy and roaming agreement into account.

Figure 1 and figure 1b illustrate the overall home routing and local breakout roaming architectures respectively for EPC when using the interfaces S8, S2a and S2b as specified in 3GPP TS 23.402. SWd is required as a roaming interface. For required EPC/LTE roaming interfaces, please refer to GSMA PRD IR.88.

Note: According to GSMA PRD IR.88, the S9 interface implementation is not necessary.

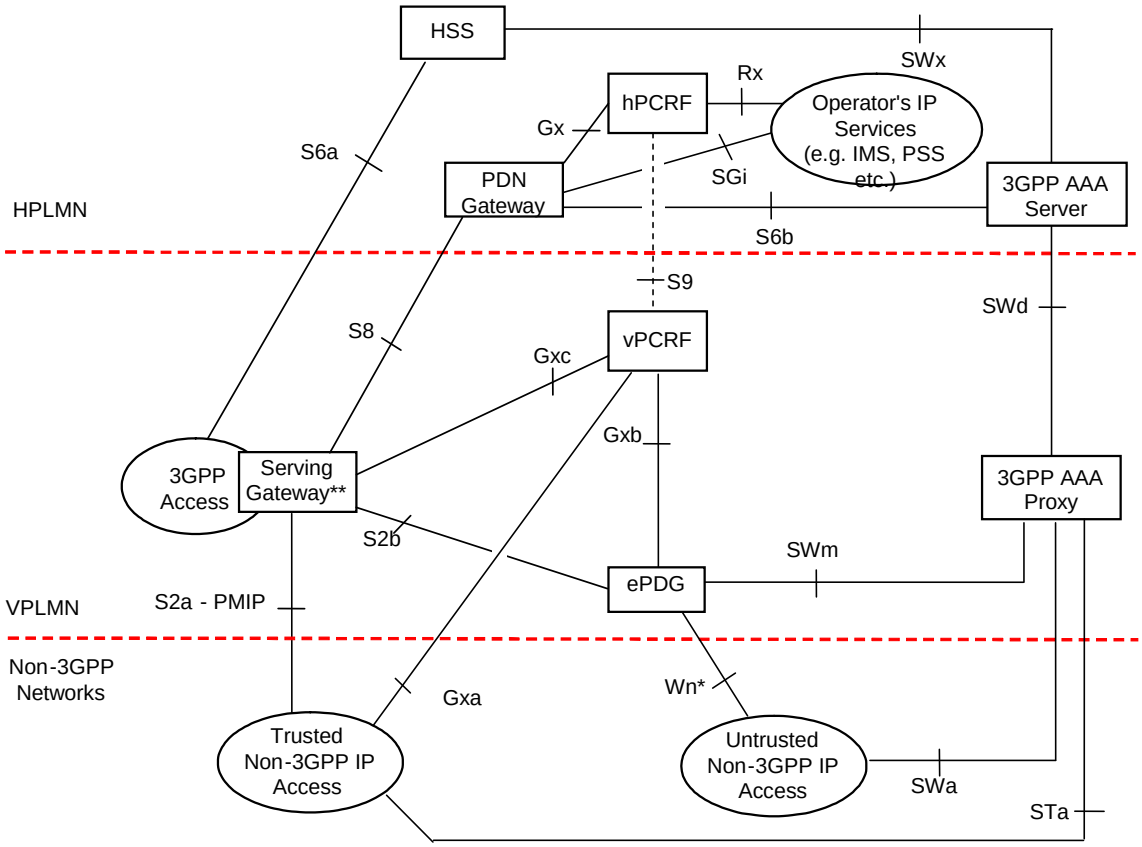

Figure 1: Roaming Architecture for EPC using S8, S2a, S2b – Home Routing (from 3GPP TS 23.402)

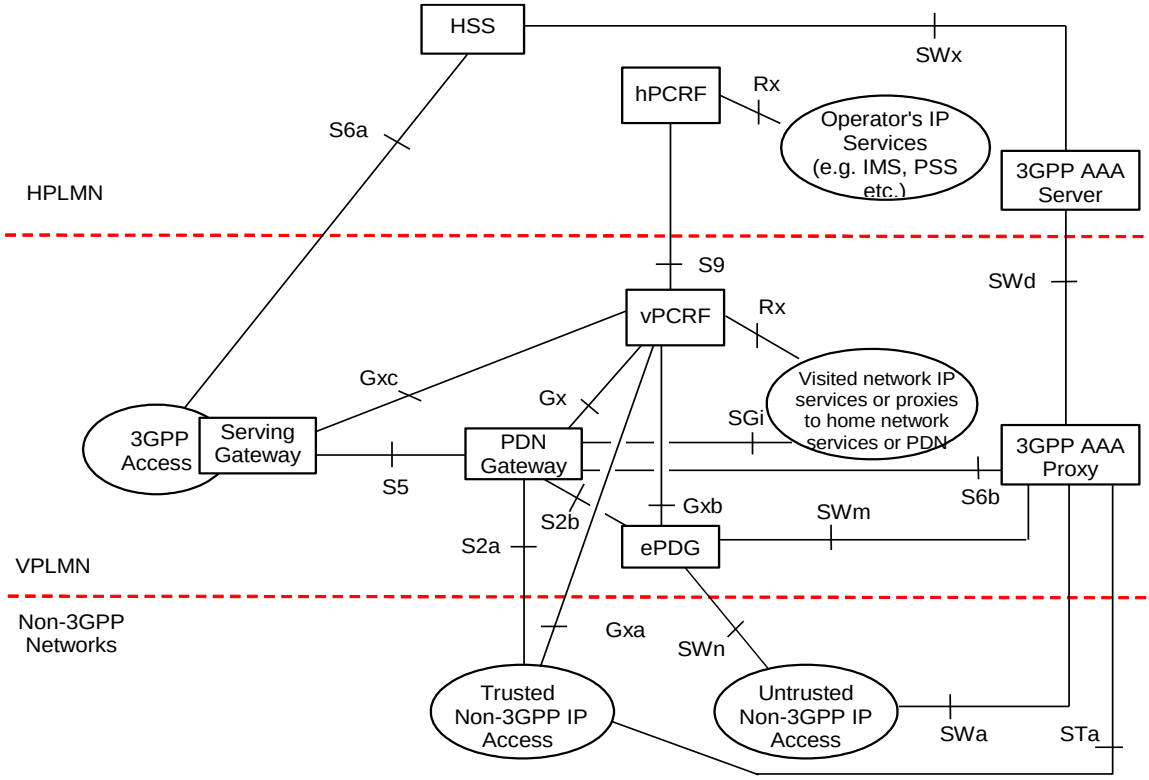

Figure 1b: Roaming Architecture for EPC using S5, S2a, S2b – Local Breakout (from 3GPP TS 23.402)

4.1.2 EPC Specific Nodes

The following list briefly describes the key EPC components.

- PDN Gateway EPC supports the GPRS Tunnelling Protocol for the control plane and the user plane to provide PDN connectivity to the UEs using trusted or untrusted Wi-Fi Access.
- ePDG is placed at the border between the Untrusted Wi-Fi Access and the PLMN. It is used to create an IPsec tunnel to the UE and it is connected to the PDN Gateway via S2b interface when using Untrusted Wi-Fi Access.(see above figures)
- For S2a, the functional structure of the trusted WLAN access network is summarised in Figure 2. In this case there is no need for an IPSec tunnel between the UE and Trusted WLAN Access Gateway (TWAG): It leverages the appropriate security provided by IEEE 802.11-2012 (802.11i, AES) over the air interface (SWw) between UE and the WLAN Access Network. The TWAP (Trusted WLAN AAA Proxy) relays AAA information between the TWAN and 3GPP AAA Server (and via a 3GPP Proxy AAA when roaming). The internal structure and interfaces of the Trusted Non-3GPP Access Network (e.g. fixed BB Access for WLAN support) are out of scope of 3GPP.

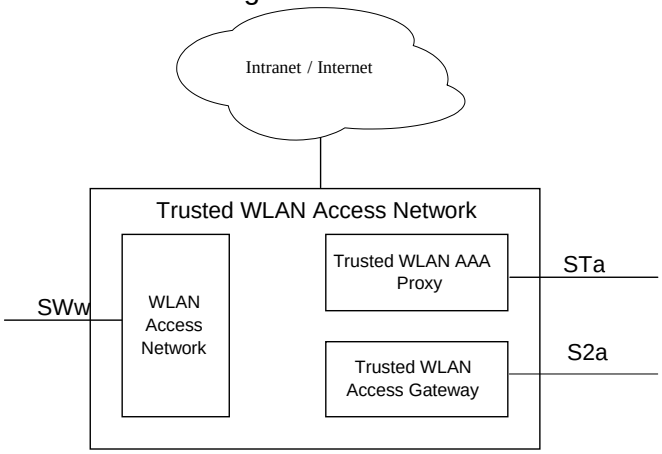

Figure 2: Trusted WLAN Access Network functions (from 3GPP TS 23.402)

PCRF is a Policy Charging and Rules Function. Among its responsibilities are the need to provide QoS information and charging policies information to the PDN Gateway and to manage and control sessions.

4A 5GC Overview (Informative)

4A.1 5GC Overview

3GPP Release-15 introduced the 5G Core (5GC) as part of EPS and the integration of Untrusted Non-3GPP access into 5GC (3GPP TS 23.501). It also supports home routing and local breakout for the services when UE is roaming.

Note: The current version of this PRD is restricted to Untrusted Non-3GPP access connected to 5GC.

General guidelines for the 5GC roaming environment using 3GPP accesses are described in GSMA PRD NG.113.

4A.1.15GC integrated WLAN Overview

Integration of Wi-Fi Access into 5GC enables mobile services to be available through Wi-Fi. 3GPP Release-15 makes it possible to use mobile services, like IMS-based voice video and messaging over IP over an Untrusted WLAN access (as an Untrusted Non-3GPP Access).

An Untrusted non-3GPP access is connected to the 5GC via a new 3GPP NF called N3IWF (see section 4A.1.2) and

- is seen and handled almost exactly like a 3GPP NG-RAN by the 5GC (different to ePDG/EPC) and
- offers N2 and N3 interfaces to access 5GC Control-Plane (CP) and User Plane (UP) functions respectively

UE that accesses 5GC shall (after its attachment) support NAS signalling with 5GC CP functions using N1. The UE can have at most one N1 instance over NG-RAN and at most one N1 instance over non-3GPP access.

There is a secured tunnel (IPSec/IKEv2) established between UE and N3IWF (over NWu) so that N3IWF presents a secured access to 5GC (as for 3GPP access)

Besides non-roaming, both Local Breakout (LBO) and Home Routed (HR) roaming configurations are possible when using Untrusted Non-3GPP Access connected to 5GC.

The following scenarios involving Untrusted Non-3GPP access are identified as described in 3GPP TS 23.501:

- 1. Untrusted Non-3GPP Access connected to 5GC:
  - [1.0] - Untrusted Non-3GPP Access to 5GC for Non-Roaming case
  - [1.1a] - Untrusted Non-3GPP Access to 5GC for LBO Roaming case with N3IWF in VPMN
  - [1.1b] - Untrusted Non-3GPP Access to 5GC for LBO Roaming case with N3IWF in different PMN from 3GPP access
  - [1.2a] - Untrusted Non-3GPP Access to 5GC for HR Roaming case with N3IWF in same VPMN as 3GPP access
  - [1.2b] - Untrusted Non-3GPP Access to 5GC for HR Roaming case with N3IWF in different PMN from 3GPP access but not in HPMN
  - [1.2c] - Untrusted Non-3GPP Access to 5GC for HR Roaming case with N3IWF in HPMN
- 2. Interworking between 5GC via Untrusted Non-3GPP access and E-UTRAN connected to EPC:
  - [2.0] - Interworking between 5GC via non-3GPP access and EPC/E-UTRAN for Non-Roaming case
  - [2.1] - Interworking between 5GC via non-3GPP access and EPC/E-UTRAN for LBO Roaming Case
  - [2.2] - Interworking between 5GC via non-3GPP access and EPC/E-UTRAN for HR Roaming case
- 3. Interworking between ePDG connected to EPC and 5GS:
  - [3.0] - Interworking between ePDG/EPC and 5GS for Non-roaming case
  - [3.1] - Interworking between ePDG/EPC and 5GS for LBO Roaming case
  - [3.2] - Interworking between ePDG/EPC and 5GS for HR Roaming case

The following figures illustrate the above scenarios for the roaming case (the non-roaming cases are described in section 4A.1.2):

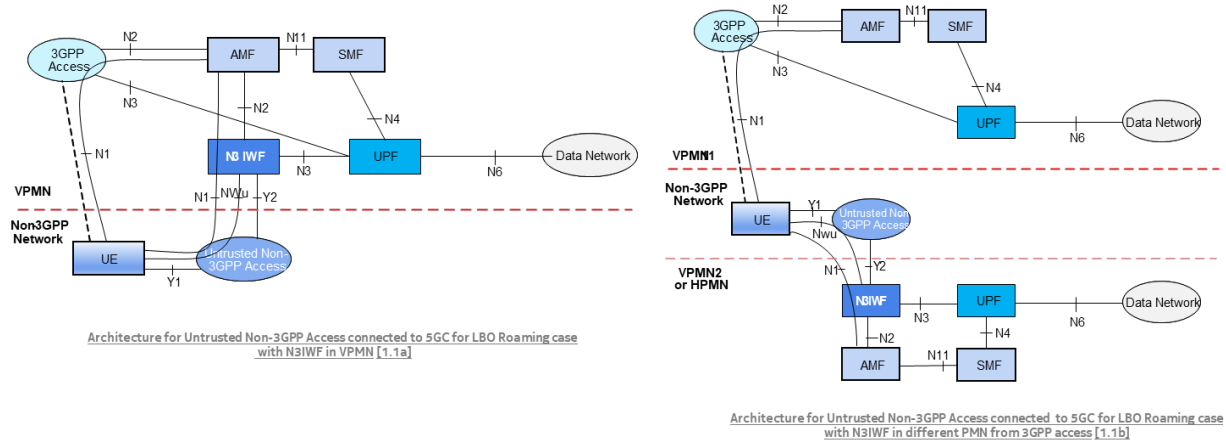

Figure 3: Untrusted Non-3GPP Access connected to 5GC – LBO Roaming Cases

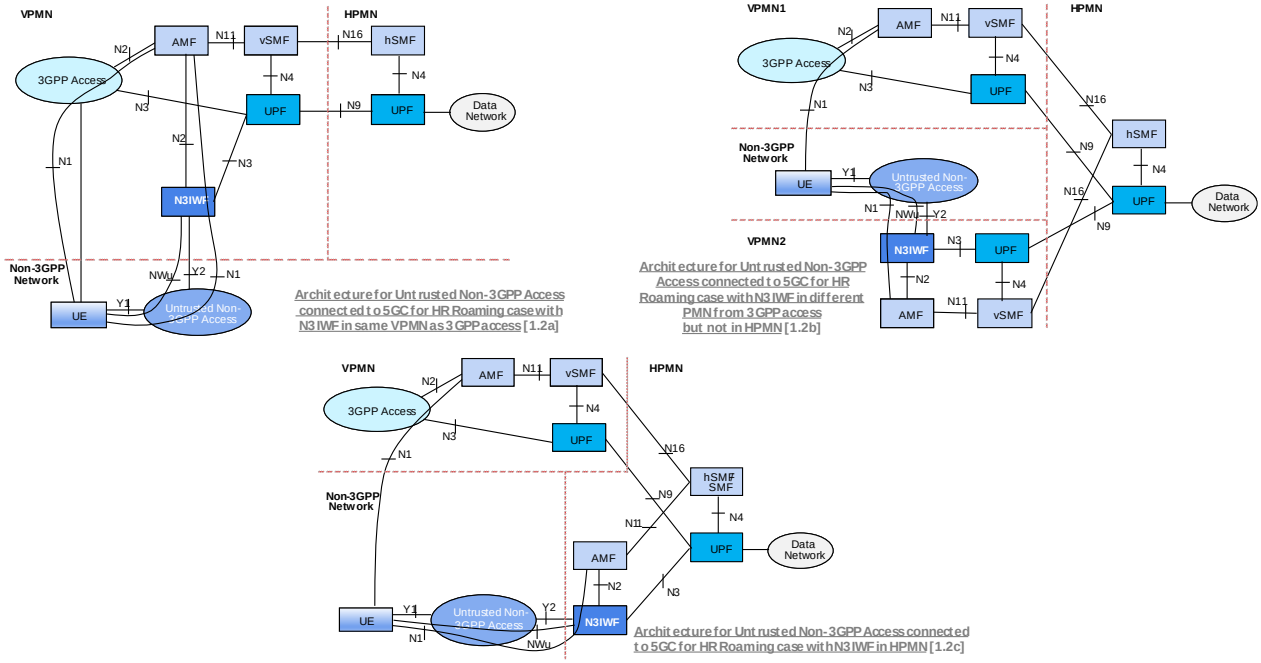

Figure 4: Untrusted Non-3GPP Access connected to 5GC – HR Roaming Cases

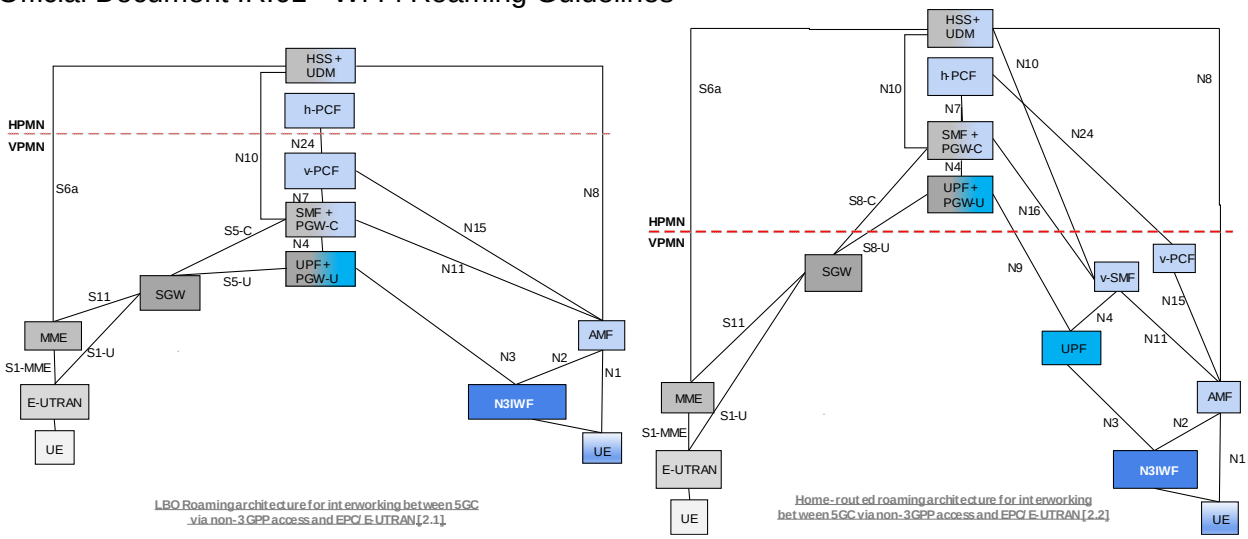

Figure 5: Interworking between 5GC via Untrusted Non-3GPP access & E-UTRAN/EPC – LBO & HR Roaming Cases

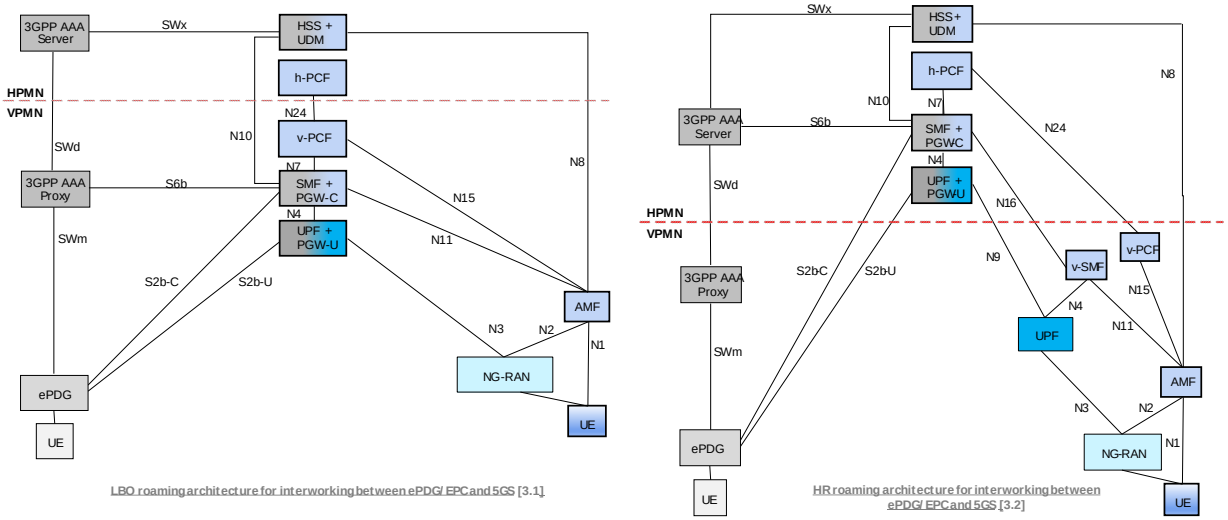

Figure 6: Interworking between ePDG connected to EPC and 5GS – LBO & HR Roaming Cases

4A.1.2 5GC Specific Nodes

The new 3GPP NF (Network Function) introduced for Untrusted WLAN access (as a Non-3GPP access) to connect to the 5GC is the N3IWF (Non-3GPP InterWorking Function).

The figure below illustrates this using the simplest configuration (non-roaming case for Untrusted Non-3GPP Access connected to 5GC, from 3GPP TS 23.501).

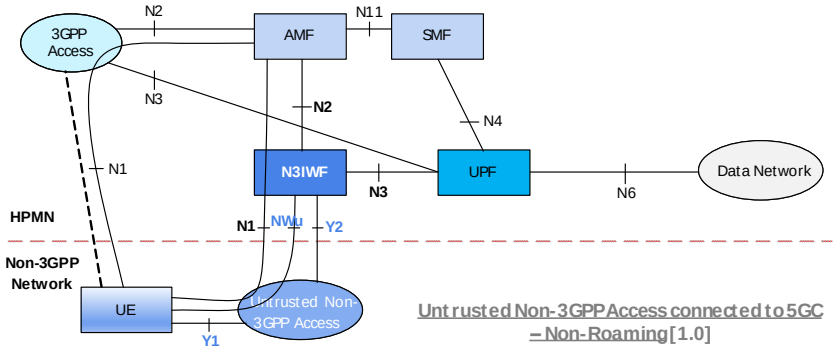

Figure 7: Untrusted Non-3GPP Access connected to 5GC for Non-Roaming case

The new interfaces introduced for Untrusted Non-3GPP access connected to 5GC are:

- Y1 Reference point between the UE and the non-3GPP access (e.g. WLAN). It is outside the scope of 3GPP.
- Y2 Reference point between untrusted non-3GPP access and the N3IWF for the transport of NWu traffic.
- NWu Reference point between UE and N3IWF for establishing secure tunnel(s) (IPSec/IKEv2) between UE and N3IWF so that CP & UP information exchanged between UE and 5GC is transferred securely over untrusted non-3GPP access.

Note: SBA (Service Based Architecture) to be used where appropriate (e.g. between AMF and SMF).

The main functionalities of the N3IWF are summarized below.

- Support of IPSec tunnel establishment with the UE: N3IWF terminates the IKEv2/IPSec protocols with the UE over NWu and relays over N2 the information needed to authenticate the UE and authorise its access to the 5GCN
- Termination of N2 and N3 interfaces to 5GCN for CP and UP respectively
- Relaying UL and DL CP NAS (N1) signalling between the UE and AMF
- Handling of N2 signalling from SMF (relayed by AMF) related to PDU Sessions and QoS
- Establishment of IPsec Security Association (IPsec SA) to support PDU Session traffic
- Relaying UL and DL UP packets between the UE and UPF (including decapsulation/ encapsulation of packets for IPSec and N3 tunneling)
- Enforcing QoS corresponding to N3 packet marking, taking into account QoS requirements associated to such marking received over N2
- N3 UP packet marking in the UL
- Local mobility anchor within Untrusted Non-3GPP access networks using IETF's MOBIKE (RFC 4555)
- Support of AMF selection

Scenarios related to interworking ([2.X] and [3.X]) make use of so called "Combo EPC/5GC" concept / functionalities as illustrated below:

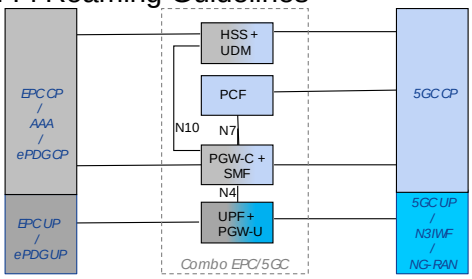

Figure 8: The "Combo EPC/5GC" concept for interworking scenarios

This concept is used e.g. in the following non-roaming scenarios for interworking:

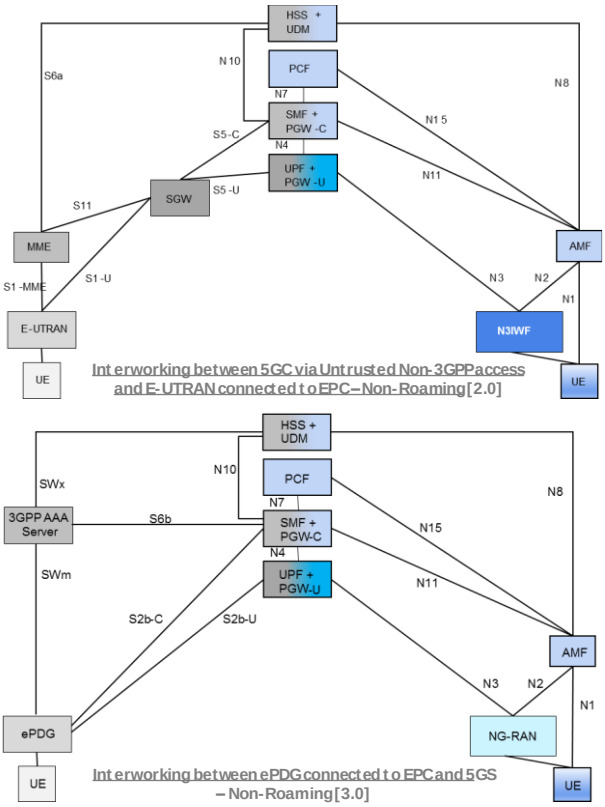

Figure 9: Interworking scenarios for Non-Roaming

5 Access Interface

5.1 Interactions between AAA & HSS

The interaction between 3GPP AAA server and HSS in the HPLMN via SWx reference point for Wi-Fi Access is described in 3GPP TS 23.402 chapter 7. It defines the Location Management procedures, Subscriber Profile Management procedures as well as Authentication Procedures.

Location Management procedures are common to all Wi-Fi Accesses, whether Trusted or Untrusted, and are independent of the mobility protocol used.

The Subscriber Profile Management is invoked by the HSS when the subscriber profile has been modified and needs to be sent to the 3GPP AAA Server. This may happen due to a modification of the user profile data in the HSS.

The 3GPP AAA Server may also request the user profile data from the HSS. This procedure is invoked when the subscription profile of a subscriber is lost or needs to be updated.

The authentication procedures between HSS and 3GPP AAA Server are described in 3GPP TS 33.402 chapter 8.

NOTE: fast re-authentication is FFS

The authentication procedures define the process in which the 3GPP AAA Server interacts with the HSS to acquire necessary data (i.e. Authentication Vectors for EAP-AKA, RFC 4187 or EAP-AKA', RFC 5448) from the HSS to successfully authenticate the user to access the Wi-Fi system.

For supporting multiple PDN connections, all PDN connections shall be setup either as Trusted or as Untrusted, i.e. it shall not be possible to use the procedure to access one PDN using the Wi-Fi Access Network via a Trusted Wi-Fi Access, while using the same procedure to access another PDN using the same Wi-Fi Access as Untrusted Wi-Fi Access

5.2 Wi-Fi Access Network Selection

5.2.1 Wi-Fi Access Selection

NOTE: For support and status of I-WLAN refer to Annex A introductory note.

5.2.2 ANDSF Support

The Access Network Discovery and Selection Function (ANDSF) may be used to support access Wi-Fi selection and traffic steering over WLAN and 3GPP accesses.

The ANDSF is a framework consisting of a UE client and a network (EPC) server defined by 3GPP. It is specified in 3GPP TS 23.402, 3GPP TS 24.302 and 3GPP TS 24.312. With 3GPP Release 12, ANDSF provides a complete and consistent set of rules for both WLAN selection and Traffic Steering.

The simplified architecture of this framework is illustrated below. The interface between the UE and ANDSF server (S14) is based on OMA-DM (Device Management) and runs on an IP based network and reachable via 3GPP or WLAN access. ANDSF is applicable for both trusted and untrusted accesses.

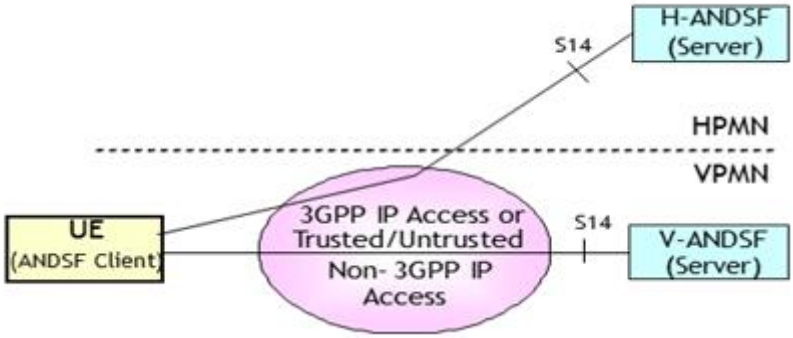

Figure 10: ANDSF Architecture

ANDSF (Release 12) supports policy for WLAN access selection and policy for traffic steering between WLAN and 3GPP access network and for NSWO (Non-Seamless WLAN Offload) for both S2a and S2b. Release-12 ANDSF may support RAN assistance information defined in 3GPP TS 36.304 and 3GPP TS 25.304 provided by RAN (E-UTRAN and UTRAN respectively) as specified in 3GPP TS 36.331 and 3GPP TS 25.331.

5.2.3 RAN rules

The RAN rules (i.e. access network selection and traffic steering rules) has been defined in Release-12 of 3GPP TS 36.304 clause 5.6.2.. For traffic steering via RAN rules, the MME may provide information to the UE indicating which PDN Connection can be offloaded to WLAN as specified in 3GPP TS 23.401 clause 4.3.23. As specified in the same clause, traffic steering decisions using RAN rules are not applicable to non-seamless WLAN offload. For E-UTRAN the RAN assistance information defined in 3GPP TS 36.304 clause 5.6.3 are provided to the UE by the E-UTRAN as specified in 3GPP TS 36.331 clause 5.6.12. For UTRAN the RAN assistance information defined in 3GPP TS 25.304 clause 5.10.3 are provided to the UE by the UTRAN as specified in 3GPP TS 25.331.

5.2.4 ANDSF and RAN rules co-existence

The WLAN access selection and the traffic routing behaviour of a UE within a single PLMN shall be controlled either by the ANDSF rules or by the RAN rules but not by both, The only exception is that when a UE applies the RAN rules, it shall be possible to simultaneously apply the IARP for APN rules, defined in TS 24.312 clause 4.2.11, provided by HPLMN as specified in 3GPP TS 23.402 clause 4.8.6.4 and 3GPP TS 24.302 clause 6.10.

When the UE has both ANDSF rules and RAN rules, it shall select which rules to apply according to the procedures defined in 3GPP TS 23.402 clause 4.8.6.4 and TS 24.302 clause 6.10.

5.3 EPC-integrated Wi-Fi Access Authentication and Security

EPC-integrated Wi-Fi Access authentication defines the process that is used for Access Control (i.e. to permit or deny a subscriber to attach to and use the resources of an EPC-integrated Wi-Fi Access). Access authentication signalling is executed between the UE and the 3GPP AAA server/HSS. The authentication signalling may pass through AAA proxies and the UE must support both EAP-AKA and EAP-AKA'.

3GPP based access authentication is executed across a SWa/STa reference point as depicted in the EPC architecture diagram. The following principles shall apply in this case:

- The Wi-Fi access only ensures relaying of authentication signalling (in EAP) and does not need to interpret this signalling.
- The 3GPP based access authentication signalling shall be based on IETF protocols, (e.g., Extensible Authentication Protocol (EAP) as specified in RFC 3748).

SWa interface must be used to connect the Untrusted Wi-Fi Access with the 3GPP AAA Server/Proxy and transport access authentication, authorization and charging-related information in a secure manner (see Figure 1).

STa interface connects the Trusted Wi-Fi Access with the 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters and charging-related information in a secure manner (see Figure 1).

The details of the access authentication procedure are defined in 3GPP TS 33.402 chapter 6.1, 6.2, 6.3 and chapter 8 and 3GPP TS 24.302 chapters 6.4 and 6.5.

For UE details see GSMA PRD IR.51.

5.4 Identities

In order to access the 3GPP Evolved Packet Core from Wi-Fi Accesses, and get Authentication, Authorization and Accounting services from the Evolved Packet Core, the RFC 4282 based user NAI (user identification) defined in 3GPP TS 23.003 shall be used.

5.5 IP Address Allocation

The following descriptions are about allocation of IP address for the data plane.

5.5.1 IP Address Allocation in Untrusted Wi-Fi Access

When an Untrusted Wi-Fi Access is used the following IP addresses are allocated to the UE

- An IP address, which is used by the UE within the Untrusted Wi-Fi Access Network to get IP connectivity towards the ePDG
- One or more IP address(es), which is used by the UE towards the external PDNs via the allocated PDN GW(s).

5.5.2 IP Address Allocation in Trusted Wi-Fi Access

When using Single-connection mode and Multi-connection mode, the UE sees the PDN Connection as a point-to-point link similar to how it is in 3GPP access. Shared link parameters such as netmask and default router IP address are not used.

In Transparent Single-connection Mode (3GPP Release 11 and above), TWAG shall act as DHCPv4/v6 server for the UE and handles the RS/RA signalling for Stateless Address AutoConfiguration.

In Single-connection mode and Multi-connection mode (both 3GPP Release 12):

- To support IPv4 connectivity, the IPv4 address shall be allocated and sent to the UE during PDN connection establishment.

- To support IPv6 connectivity, the PGW handles the RS/RA messages and to support IPv6 parameter configuration the UE may use stateless DHCPv6. The PGW acts as DHCPv6 server.

5.6 PDN Connectivity Service

5.6.1 Untrusted Access

5.6.1.1 Connectivity Services

For Wi-Fi Access to the EPC the PDN connectivity service is provided by IKEv2 and IPsec connectivity between the UE and the ePDG concatenated with S2b bearer(s) between the ePDG and the PGW. During this connection procedure the UE and the ePDG must support mutual authentication for the IPsec tunnel establishment between the UE and the ePDG (SWu reference point). The Tunnel authentication is using a SWm reference point to the AAA Proxy / Server. The use of S2b bearers is depicted in Figure 4.

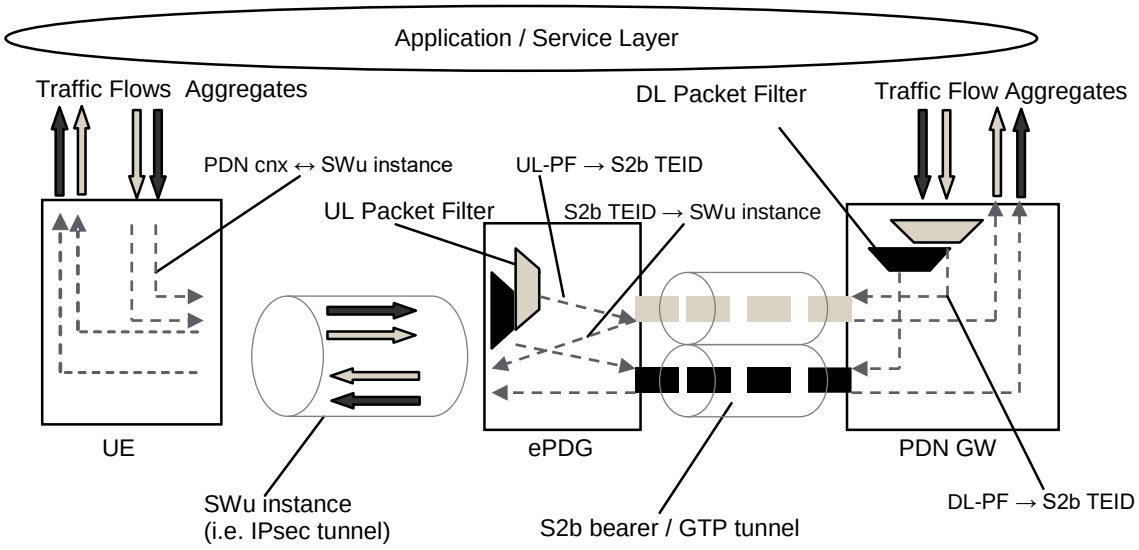

Figure 11: Two Unicast S2b bearers (GTP based S2b)

The UE must establish a separate SWu instance (i.e. a separate IPsec tunnel) for each PDN connection.

One default S2b bearer must be established on the S2b interface when the UE connects to a PDN, and that remains established throughout the lifetime of the PDN connection to provide the UE with always-on IP connectivity to that PDN. Additional dedicated S2b bearers may be established for the same PDN connection depending on operator policy. The PGW establishes dedicated S2b bearers for the same PDN connection based on PCC decisions as specified in 3GPP TS 23.203.

The ePDG must release the SWu instance when the default S2b bearer of the associated PDN connection is released.

The S2b bearer is realized by the following elements:

- A GTP tunnel on S2b transports the packets of an S2b bearer between the ePDG and a PDN GW;
- The ePDG stores the mapping between uplink packet filters it receives from the PGW (e.g. in the Create Bearer Request message) and the corresponding S2b bearer;
  The PDN GW stores the mapping between downlink packet filters and an S2b bearer.

In support for the UE connectivity with the PDN:

- A SWu instance (i.e. a IPsec tunnel) transports the packets of all S2b bearer(s) for the same PDN Connection between the UE and the ePDG.

The ePDG shall route uplink packets to the different bearers based on the uplink packet filters in the TFTs assigned to the bearers in the PDN connection, in the same way as a UE does for uplink traffic under 3GPP access. If no match is found, the uplink data packet shall be sent via the bearer that does not have any uplink packet filter assigned. If all bearers (including the default bearer for that PDN) have been assigned an uplink packet filter, the ePDG shall discard the uplink data packet.

The PDN GW shall route downlink packets to the different bearers based on the downlink packet filters in in the TFTs assigned to the S2b bearers in the PDN connection, in the same way as the PDN GW does on GTP-based S5/S8 bearers (see 3GPP TS 23.401 clause 4.7.2.2).

5.6.2 Trusted Access

The PDN connectivity service (Figure Y, from TS 23.402) is provided by the point-to-point connectivity between the UE and the TWAG concatenated with S2a bearer(s) between the TWAG and the PDN GW.

The bearer model of GTP based S2a interface is similar to that of GTP based S5/S8 interface and GTP based S2b interface. The TWAN handles the uplink packets based on the uplink packet filters in the TFTs received from the PDN GW for the S2a bearers of the PDN connection as depicted in Figure 5, in the same way as an ePDG does for GTP based S2b interface.

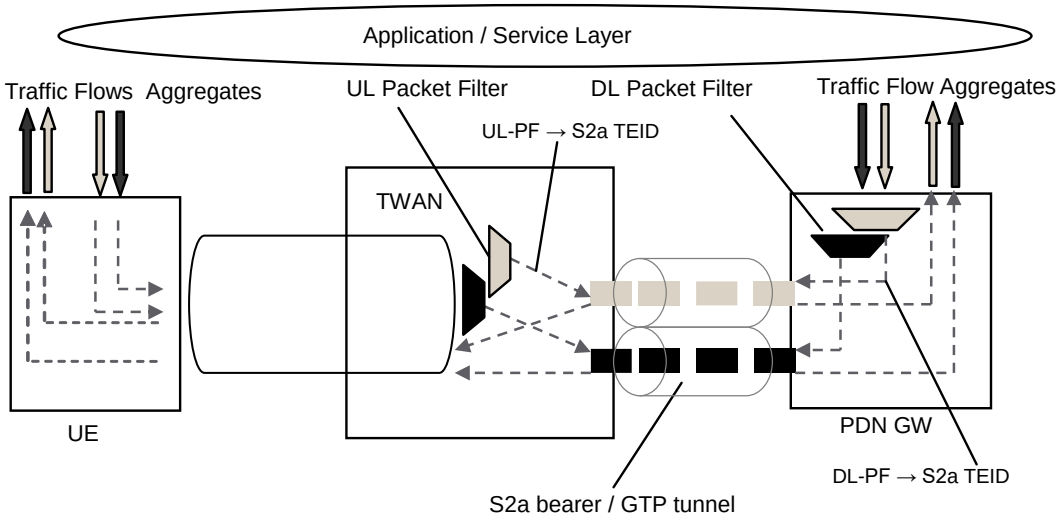

Figure 12: Two Unicast S2a bearers (GTP based S2a)

The trusted access can be used in the following modes:

- Non-Seamless offload mode (as from Release 11): this mode does not make use of a P-GW (EAP-AKA' however supported) and the traffic is routed directly to an external data network via the TWAG. It can also be considered as a specific case of a Single-connection mode.
- Transparent connection mode (as from Release 11): single connection to P-GW using S2a but without mobility support between 3GPP and WLAN. Selective offload (e.g. moving one PDN out of two from one access to another) is not possible. This nomadic PDN connectivity enables to have a consistent 3GPP service (re-use of P-GW functionalities) while using a WLAN.
- Single-connection mode (as from Release 12): support of a single connection at a time (non-seamless or with a single PDN connectivity). The use of the Single-Connection mode and the associated parameters of the connection can be negotiated during authentication over TWAN. Seamless mobility between accesses in this mode is possible.
- Multi-connection mode (as from Release 12): support of multiple connections simultaneously. One connection may be used for Non-Seamless offload and one or more simultaneous connections may be used for PDN connectivity. The use of the Multi-Connection mode can be negotiated during authentication over TWAN and a requested PDN connection can be setup with the WLCP (WLAN Control Plane protocol, as per 3GPP TS 24.244). This mode therefore enables the support of MAPCON (Multi-Access PDN Connectivity) where selective offload is possible (e.g. two PDN connections (e.g. IMS, Internet) over 3GPP and only one (e.g. Internet) needs to be moved to WLAN based on operator policy / rules). Seamless mobility in this mode between accesses is possible.

The above modes are managed in a consistent manner using ANDSF Release 12 and must all be supported by the network. UE-Network negotiation for the chosen mode is done during EAP-AKA' procedure. For the case of Non-seamless offload see section 6.4.

Seamless mobility (IP address preservation) is possible for trusted access using S2a as from Release 12 and this is possible with both Single-connection and Multi-connection modes. Mobility of a PDN connection between 3GPP and WLAN is not possible with Release 11 as no modifications to the UE was allowed for that release. This restriction has been removed for Release 12.

NOTE: It has been recommended by the GSMA / WBA Roaming Task Force to IREG (PACKET#66, July 2013) to support seamless mobility (IP address preservation). Delivery of voice and real time services over Wi-Fi will be the key drivers. Furthermore, besides the recommendation of using GTP as protocol to reach P-GW from a WLAN gateway, usage of Trusted WLAN Access was also mentioned as a priority.

NOTE: QoS support for real-time MMTel services as voice and video telephony is required to maintain an appropriate user experience over WLAN, in particular for seamless mobility support. QoS for these services is provided by the network (that can map QoS requirements received over GTP-C onto a proper DSCP to be used over the access leg). The UE is assumed to either derive the uplink QoS from the QoS of the downlink stream or to have the appropriate uplink QoS set by the application.

NOTE: TWAG discovery by the UE is not required as the UE just contacts the AP (beacon) and then the AP selects a TWAG. How the AP selects the TWAG is out of scope of 3GPP. When Multi-Connection Mode applies, the UE needs to contact directly the TWAG over IP (using WLCP).

5.7 ePDG Selection in VPLMN

When a UE is in a visited country, the UE shall perform the ePDG selection procedure according to 3GPP TS 23.402 clause 4.5.4.5 (Release 13).

In case of regulatory requirement for Lawful Interception in the visited country, this procedure provides the necessary selection of an ePDG in the visited country.

5A. Access Interface for 5GC

5A.1 WLAN Access Selection

The procedure for WLAN access network selection is defined in TS 23.503 clause 6.6.1.3, the procedure for N3IWF selection is defined in TS 23.501 clause 6.3.6.1.

The WLAN access network is selected by the UE with the use of the ANDSP (Access Network Discovery & Selection Policy, as defined in 3GPP TS 23.503 sections 6.1.2.2 and 6.6.1) may be used for direct traffic offload (i.e. non-seamless offload) and for registering to 5GC using the non-3GPP access network selection information. The ANDSP is an optional policy that may be provided to UE by the network. If the UE supports non-3GPP access to 5GC, it shall support ANDSP (3GPP TS 23.503 section 6.6.1.1).

Note: The policy used by the UE to determine how to route outgoing traffic at an application level granularity is the URSP (UE Route Selection Policy, as defined in 3GPP TS 23.503

section 6.6.2). Traffic can be routed to an established PDU Session, can be seamlessly offloaded or can trigger the establishment of a new PDU Session.

The ANDSP and URSP may be pre-configured in the UE or (when pre-configured policy is not available) may be provisioned to UE from PCF.

5A.2 5GC-integrated WLAN Access Authentication and Security

The method of authenticating the UE by the WLAN to access the DN without traffic using the N3IWF / UPF is not specified.

Note: Non-seamless offload is not described for 5GC in contrast to EPC in 3GPP specifications (though not detailed for EPC; authentication aspects are also left open).

5A.3 Identities

Authentication over Untrusted WLAN access (as untrusted Non-GPP access) uses the same mechanism as over 3GPP.

In order to access the 3GPP 5GC from WLAN access, and get Authentication, Authorization and Accounting services from the 5GC, IETF RFC 4282 based user NAI (user identification) defined in 3GPP TS 23.003 shall be used.

The UE shall provide either a

- 5G GUTI obtained from AMF over 3GPP access as defined in 3GPP TS 23.502 or a
- SUCI (ciphered SUPI) as defined in 3GPP TS 33.501

5A.4 IP Address Allocation

When an Untrusted WLAN Access is used the following IP addresses are allocated to the UE:

- An IP address, which is used by the UE within the Untrusted WLAN Access Network to get IP connectivity towards the N3IWF
- One or more IP address(es), which is used by the UE towards the external DNs via the allocated UPF(s).

Note: The UE gets an IP @ from 5GC (IP address to use on the DN) only in case the PDU Session type is “IP”. When the PDU Session type is “IP” the same address allocation mechanism as for 3GPP access are provided.

5A.5 PDU Session Connectivity Service

Data connectivity corresponds to

- IPSec tunnels established via IKE over NWu; A data connectivity may correspond to multiple security associations in order to support QoS flows providing different QoS levels.
- A N3 tunnel where the PDU Session is mapped to a single GTP-u tunnel
- Possibly N9 tunnel where the PDU Session is mapped to a single GTP-u tunnel
- Data connectivity over N6

The connectivity service may correspond to following PDU Session types: IP, Ethernet or Unstructured.

The corresponding protocol stack is defined in 3GPP TS 23.501 section 8.3.2 (User Plane for Untrusted non-3GPP Access).

The generic data connectivity for 5GC access is summarised in Figure 13.

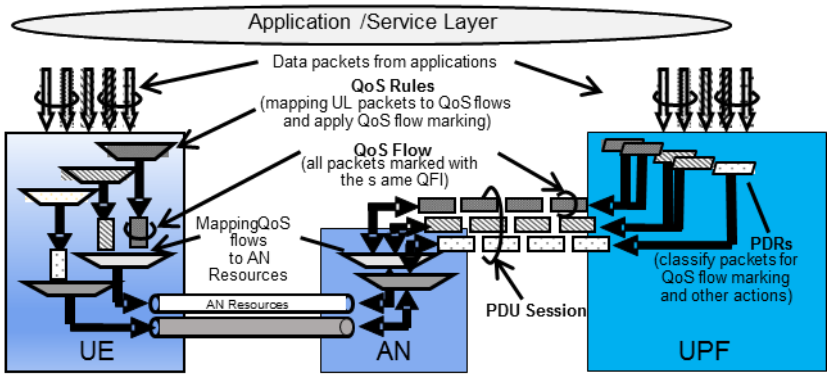

Figure 13: Connectivity Service to 5GC via AN (e.g. Untrusted WLAN / N3IWF)

6 Functional Description & Procedures of EPC-Integrated Wi-Fi

6.1 Overview

The EPC supports the use of Wi-Fi Access Networks. The PDN GW is an anchoring point of services (for all accesses), 3GPP services are available through Wi-Fi and there is a local breakout available. Also mobility between 3GPP Access Networks and Wi-Fi is possible.

6.2 Mobility Management

Depending on the operator policy the EPC network must support network-based mobility management mechanism based on GTP over S2b and (with 3GPP Release 12) over S2a reference points as specified in 3GPP TS 23.402. Connection modes supporting mobility using S2a are described in section 5.6.2.

The mobility management procedures are specified to handle mobility between 3GPP and Wi-Fi Accesses. This applies to UEs either supporting simultaneous radio transmission capability or not supporting it. EPC-based mobility between GERAN/UTRAN Access and Wi-Fi Access requires S4-based SGSNs.

NOTE: The handover indication as specified in 3GPP TS 23.402 chapter 8.6 is only supported in GTPv2.

For multiple PDN-GWs connecting to the same PDN, all the PDN GWs shall support the same mobility protocols.

The mobility procedure between WLAN APs for connection to the same ePDG is supported via Mobike as defined in 3GPP TS 24.302 and IETF RFC 4555. If the UE supports MOBIKE, the UE sends a notification as part of the IKEv2 authentication request informing that it supports MOBIKE to the ePDG. If ePDG supports MOBIKE, the ePDG sends a notification in reply to the UE informing that it also, supports MOBIKE.

6.3 Local Breakout

The EPC supports local breakout of traffic whether a roaming subscriber is accessing the EPC via a 3GPP or Wi-Fi Network according to the design principles described in TS 23.402 7.2.4, 7.4.3 and 7.4.4.

6.4 Non-seamless Wi-Fi Offload

Policies for non-seamless Wi-Fi offload must be either pre-defined by the home operator and reside on the UE or be provided via ANDSF according to Release 12 3GPP TS 23.402, that

- determine which traffic should be routed across different PDN connections and which traffic should be non-seamlessly offloaded to Wi-Fi.

6.5 Multi Access PDN Connectivity

The network must support Multi Access PDN Connectivity (MAPCON) as specified in 3GPP TS 23.402 and 3GPP TS 24.302. For UE details see GSMA PRD IR.51.

6A. Functional Description & Procedures of 5GC-Integrated Wi-Fi

6A.1 Overview

The 5GC supports the use of WLAN access networks as non-3GPP access. The UPF is an anchoring point of services (for all accesses), 3GPP services via 5GC are available through WLAN access. Also mobility between 3GPP Access Networks and WLAN access is possible.

6A.2 Mobility Management

The following cases for handover are identified based on the families (1,2 & 3) of scenarios identified previously and described in detail in 3GPP TS 23.402:

- Between N3IWFand NG-RAN (related to scenarios [1.X] and [1.Xy])
- Between N3IWF and EPS (via EPC/MME) (related to IWK scenarios [2.X])
- Between ePDG and 5GC/NG-RAN (related to IWK scenarios [3.X])

Note: There is no Interworking / Handover between N3IWF/5GC and ePDG/EPC specified by 3GPP (at least for Releases 15/16).

Depending on operator policy the 5GC network must support network-based mobility management mechanism specified in 3GPP TS 23.502.

6A.3 Local Breakout & Home Routing

The 5GC supports local breakout and home routing of traffic where a roaming subscriber is accessing the 5GC via a WLAN access network according to the design principles described in 3GPP TS 23.501 section 4.2.4

6A.4 Non-seamless Offload

Policies for non-seamless offload must be either pre-defined by the home operator and reside on the UE or be provided using ANDSP / URSP via PCF according 3GPP TS 23.503 section

6.6.2. The policies can determine which traffic should be routed across different DNs and which traffic should be non-seamlessly offloaded.

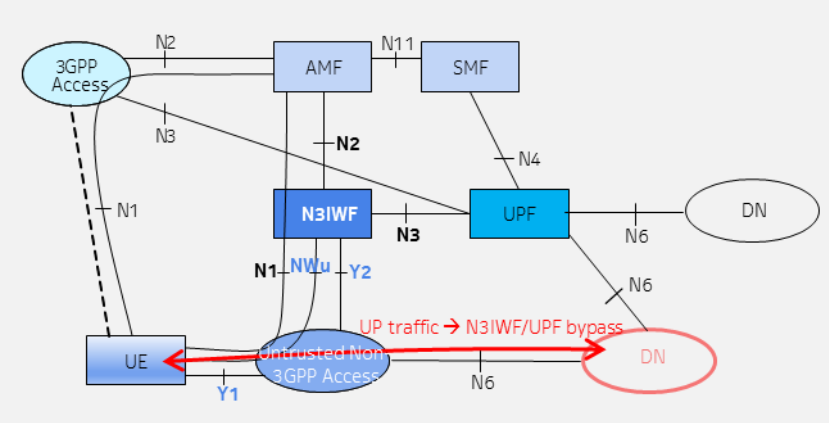

Figure 14 :Non-Seamless Offload in the Untrusted Non-3GPP / 5GC context

6A.5 Multi Access PDU Session Connectivity

The 5GC implicitly allows the UE to have simultaneously PDU session(s) on one access (e.g. 3GPP access) and other PDU session(s) on the another access (e.g. WLAN as non-3GPP access).

7 Roaming Interface

7.1 NNI Overview

EPC integrated Wi-Fi roaming reuses the general IP based NNI structure currently used by other systems and services, such as voice over IMS roaming and IMS interconnection.

As the EPC integrated Wi-Fi roaming uses the Local Breakout model in order to be aligned with the general model selected for the voice over IMS roaming, the interfaces carrying signalling over NNI are the main consideration for this document.

General requirements for IP addressing and routing are contained within GSMA PRDs IR.33, IR.34 and IR.40. General DNS guidelines are described in IR.67.

7.2 IPX Specifics

Generally speaking, the IPX (IP eXchange) as defined by GSMA PRD IR.34 is the preferred inter-Service Provider IP network for GSMA. Thus it should also be used EPC integrated Wi-Fi roaming purposes.

For further details on IPX, please see GSMA PRDs IR.34 and AA.80.

7.3 SWd

SWd runs between the 3GPP AAA Proxy and 3GPP AAA Server. The main purpose of this interface is to transport AAA signalling between home and visited networks. The actual SWd protocol is specified in 3GPP TS 29.273.

The SWd interface uses Diameter protocol as defined in RFC 3588. GSMA PRD IR.88 describes how Diameter is used in the EPC roaming environment, giving guidance for example on routing and identity related topics. Generally speaking the functionality of SWa, STa, SWm and S6b also applies to SWd. There is no specific Diameter application defined for SWd but it proxies the applications of the interfaces listed above.

As shown in the Figure 6 below, the 3GPP AAA Proxy in the Visited SP acts as a Diameter proxy agent and forwards Diameter commands between the roaming Diameter client and the Diameter server located in the Home SP. As described in GSMA PRD IR.88, Diameter traffic over NNI is strongly preferred to use DEA (Diameter Edge Agent) nodes at the border of the Service Provider core network to support scalability, resilience and maintainability.

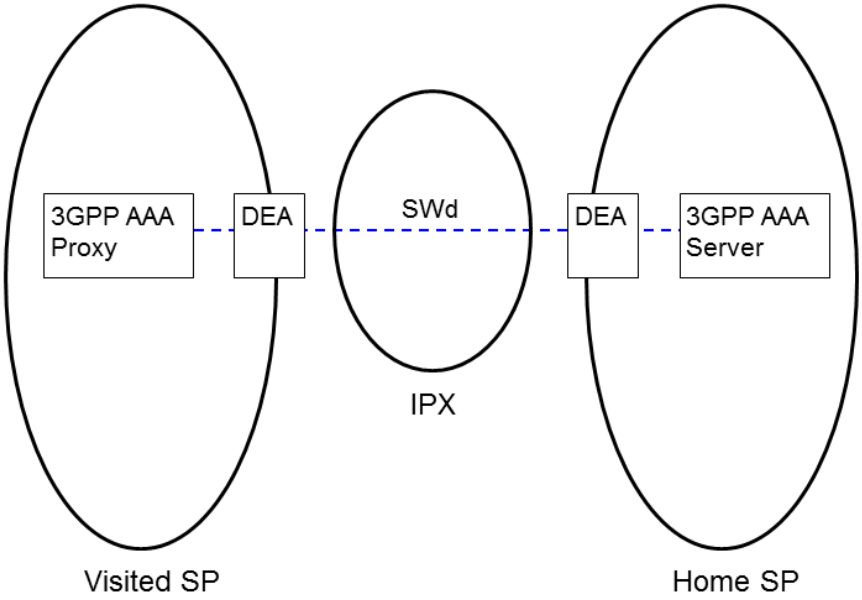

Figure 15: SWd Interface Overview

SWd is used for the following purposes:

- Carrying data for authentication signalling between 3GPP AAA Proxy and 3GPP AAA Server;
- Carrying data for authorization signalling between 3GPP AAA Proxy and 3GPP AAA Server;
- Carrying charging signalling per user;
- Carrying keying data for the purpose of radio interface integrity protection and encryption;
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption, for the case in which the ePDG is in the VPLMN;
- Carrying mapping of a user identifier and a tunnel identifier sent from the ePDG to the 3GPP AAA Proxy through the 3GPP AAA Server;
- Used for purging a user from the access network for immediate service termination;
- Enabling the identification of the operator networks amongst which the roaming occurs;

- If QoS mechanisms are applied: carrying data for AN QoS capabilities/policies (e.g. the supported 3GPP QoS profiles) within authentication request from 3GPP AAA Proxy to 3GPP AAA Server.
- Carrying the IP Mobility Capabilities between 3GPP AAA Proxy and 3GPP AAA Server.

7.4 Other Functions

Access Control:

Without an explicit agreement from the HPLMN, the VPLMN must block the access of inbound roamers into their Wi-Fi Access network. This is compulsory to ensure roamers will not experience any service disruption because the necessary technical requirements have not been implemented and tested with the HPLMN.

7A. Roaming Interface for 5GC

The roaming interfaces involved are standard 5GC ones whatever the roaming architecture or configuration. This is because of the N3IWF has been designed and specified to look (more or less) like a 3GPP RAN connected to the 5GC. Specificities related to these interfaces are therefore described in GSMA PRD NG.113.

However in a few cases, as illustrated section 4A.1.1, the following interfaces may be regarded as roaming interfaces from an architectural viewpoint when the N3IWF is located in the HPMN:

- N1 (NAS signalling beteen UE and AMF)
- NWu (uses Y2 (and Y1) for transporting WLAN based traffic)

Annex A Void

Note: I-WLAN related guidance is no longer described or supported since the version 13 of this PRD. Consequently Annex B has been removed.

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.0.1	June 6th, 2002	First draft created in WLAN TF ("version A")	EMC/IREG	
0.0.2	June 7th, 2002	Version after WLAN TF Stockholm meeting ("version B")	EMC/IREG	
0.0.3	July 4th, 2002	Version after WLAN TF conference call (4th of July) ("version C")	EMC/IREG	
0.0.4	August 22nd, 2002	Version after WLAN TF conference call ("version D"), presented to IREG plenary in Singapore	EMC/IREG	
0.0.5	September 19th, 2002	Version based on discussions and agreements in WLAN TF /(IREG) Singapore meeting ("version E")	EMC/IREG	
0.0.6	September 27th, 2002	Version approved by WLAN TF in Portland ("version F"), presented to Packet WP in Madrid (November 2002)	EMC/IREG	
0.0.7	January 17th, 2003	Version after Packet WP ad-hoc in Düsseldorf	EMC/IREG	
0.0.8	February 11th, 2003	Version after Packet WP Yokohama meeting (IREG Doc 026/03 Rev 1)	EMC/IREG	
3.0.0	April 23rd, 2003	Approved by EMC	EMC/IREG	
3.0.1	November 3rd, 2003	Incorporated PACKET Doc 074_03 (NCR 001 on IR.61)	EMC/IREG	
3.0.2	October 24th, 2003	Incorporated IREG Doc 46_028 (NCR 002 on IR.61)	EMC/IREG	
3.0.3	October 24th, 2003	Incorporated IREG Doc 46_029 (NCR 003 on IR.61)	EMC/IREG	

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
3.1.0	August 25th, 2004	Incorporated IREG Doc 47_019 (SCR 005 on IR.61) and IREG Doc 47_016 (NCR 004 on IR.61)	EMC/IREG	
4.0	June 25th, 2007	Incorporated IREG Doc 52_038 (3GPP Release-6 WLAN interworking)	EMC/IREG	
5.0	February 15th, 2012	DAG documents 088_028rev1, 88_029rev1, 88_030rev1, 88_031rev1, 88_032 and 88_033 incorporated	EMC/IREG	Marko Onikki TeliaSonera
6.0	2013	DAG Docs 99_016, 99_017	DAG99	Marko Onikki TeliaSonera
7.0	2014	Incorporated CR1001 (Support for EPC integrated Wi-Fi	IREG	Marko Onikki TeliaSonera
8.0	July 28th, 2014	Incorporated CR1002 and CR1003	IREG	Marko Onikki TeliaSonera
9.0	November 19th, 2014	Incorporated CR1004	IREG	Marko Onikki TeliaSonera
10.0	May 5th, 2015	Incorporated CR1005, 1006 and 1007	IREG	Marko Onikki TeliaSonera
11.0	October 18th, 2016	CR1008, CR1009	NG	Marko Onikki (Telia Company)
12.0	September 27th, 2017	CR1010	NG	Marko Onikki (Telia Company)
12.1	May 11th, 2020	CR1011	NG	Marko Onikki (Telia Company
13.0	13th October, 2020	CR1012, CR1013, CR1014	NG	Marko Onikki (Telia Company)
14.0	28th May 2021	CR1015	NG	Marko Onikki (Telia Company)

Other Information

Type	Description
Document Owner	NG
Editor / Company	Marko Onikki / Telia Company

Feedback

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.