ETSI TS 124 234 V12.1.0 (2015-01)

Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP system to Wireless Local Area Network (WLAN) interworking;
WLAN User Equipment (WLAN UE) to network protocols;
Stage 3
(3GPP TS 24.234 version 12.1.0 Release 12)

Reference
RTS/TSGC-0124234vc10

Keywords
LTE,UMTS

ETSI

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

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

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

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://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.

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

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

Contents

Foreword

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

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the network selection, including authentication and access authorization using authentication, authorization and accounting (AAA) procedures used for the interworking of the 3GPP system and WLANs. In addition to these, the present document also specifies the tunnel management procedures used for establishing an end-to-end tunnel from the WLAN UE to the 3GPP network via the Wu reference point.

The present document is applicable to the WLAN user equipment (UE) and the network. In this technical specification the network includes the WLAN and 3GPP network.

Tunnel management signalling is carried between WLAN-UE and WLAN by WLAN access technology specific protocols, however this signalling is transparent to the WLAN.

Tunnel management procedures are defined to be independent of the underlying WLAN access technology and as such can be reused independently of the underlying technology.

The present document specifies procedures within I-WLAN necessary in order for IMS emergency calls to be supported when I-WLAN is used as the underlying access network. These involve both network selection as well as tunnel management procedures.

WLAN Network Selection supersedes I-WLAN for UE WLAN selection as specified in 3GPP TS 24.302 [28] from Rel-12 onwards.

No further changes to this specification are intended. If any future evolution of the procedures in this specification is necessary, it should be documented in other specifications.

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 TS 23.122: "Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".

[1A] 3GPP TS 23.003: "Numbering, addressing and identification".

[1B] 3GPP TS 23.002: "Network architecture".

[1C] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[3] 3GPP TS 29.234, Release 11: "3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3".

[3A] 3GPP TS 29.161: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services with Wireless Local Area Network (WLAN) Access and Packet Data Networks (PDN)".

[4] Void

[5] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".

[6] IETF RFC 3748 (June 2004): "Extensible Authentication Protocol (EAP)".

[7] IETF RFC 1035 (November 1987): "Domain names - implementation and specification".

[8] Void

[9] IETF RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP AKA)".

[10] IETF RFC 4186 (January 2006): "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)".

[11] IEEE Std 802.11 (2007: "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".

[12] IETF RFC 4284 (January 2006): "Identity selection hints for Extensible Authentication Protocol (EAP)".

[13] 3GPP TS 31.102: "Characteristics of the USIM application".

[14] IETF RFC 5996 (September 2010): "Internet Key Exchange Protocol Version 2 (IKEv2)".

[15] IETF RFC 4303 (December 2005): "IP Encapsulating Security Payload (ESP)".

[16] IETF RFC 4739 (November 2006): "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".

[16A] IETF RFC 5216 (March 2008): "The EAP-TLS Authentication Protocol".

[17] IETF RFC 3629 (November 2003): "UTF-8, a transformation format of ISO 10646".

[18] IETF RFC 2474 (December 1998): "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[19] IETF RFC 2475 (December 1998): "An Architecture for Differentiated Services".

[20] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[21] GSMA PRD IR 34: "Inter-PLMN Backbone Guidelines".

[22] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[23] IEEE Std 802.11u™-2011: "Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 9: Interworking with External Networks".

[24] OMA-DDS-DM_ConnMO_WLAN-V1_0-20081024-A: "Standardized Connectivity Management Objects WLAN Parameters", Approved Version 1.0 – 24 Oct 2008.

[25] Void

[26] 3GPP TS 24.235: "3GPP System to Wireless Local Area Network (WLAN) interworking Management object".

[27] Void

[28] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP acces networks; Stage3".

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 [1C] 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 [1C].

active scanning: Capability of a WLAN UE to actively solicit support for a WLAN specific identifier (WSID) by for probing it.

Associated WSID: WSID that the WLAN UE uses for association with a WLAN AP.

Available WSID: WSID that the WLAN UE has found after scanning.

EAP AKA: EAP mechanism for authentication and session key distribution using the UMTS AKA authentication mechanism using the universal subscriber identity module (USIM) (see IETF RFC 4187 [9]).

EAP SIM: EAP mechanism for authentication and session key distribution using the GSM subscriber identity module (SIM) (see IETF RFC 4186 [10]).

External AAA server: The AAA server is located in an external packet data network. The PDG interworks with the external AAA server via the Wi reference point that is described in 3GPP TS 29.161 [3A].

Home PLMN (HPLMN): The home PLMN of the user.

Passive scanning: Capability of a WLAN UE to look for the support for a specific WSID by listening to the WSIDs broadcast in the beacon signal.

Public land mobile network (PLMN) selection: Procedure for the selection of a PLMN, via a WLAN, either manually or automatically.

Selected WSID: This is the WSID that has been selected according to subclause 5.1, either manually or automatically.

Selected PLMN: This is the PLMN that has been selected according to subclause 5.2, either manually or automatically.

Supported PLMN: A PLMN of a roaming partner (i.e. to which the WLAN operator has a direct roaming relationship).

Switch on: Action of activating a WLAN UE client.

Switch off: Action of deactivating a WLAN UE client.

WLAN specific identifier (WSID): Identifier for the WLAN.
For WLANs compliant with IEEE 802.11 [11] this is the SSID.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [1B] apply:

WLAN UE
3GPP AAA proxy
3GPP AAA server
Packet Data Gateway (PDG)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.234 [2] apply:

3GPP - WLAN Interworking (WLAN-3GPP IW)
Interworking WLAN
W-APN
WLAN 3GPP IP Access
WLAN Direct IP Access

For the purposes of the present document, the following terms and definitions given in3GPP TS 23.003 [1A] apply:

Alternative NAI

Decorated NAI
Emergency NAI
Emergency realm
Root NAI

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Wa	Reference point between a WLAN and a 3GPP AAA Server/Proxy (control signalling)
Wd	Reference point between a 3GPP AAA Server and 3GPP AAA Proxy (control signalling)
Wu	Reference point between a WLAN UE and a PDG

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization and Accounting
AKA	Authentication and Key Agreement
ANQP	Access Network Query Protocol
APN	Access Point Name
DNS	Domain Name System
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
H-ANDSF	Home ANDSF
HLR	Home Location Register
HPLMN	Home PLMN
HSS	Home Subscriber Server
I-WLAN	Interworking – WLAN
IKE	Internet Key Exchange
IPsec	IP security
NAI	Network Access Identifier
NI	Network Identifier
OI	Operator Identifier
PDG	Packet Data Gateway
PLMN	Public Land Mobile Network
SIM	Subscriber Identity Module
SSID	Service Set ID
UE	User Equipment
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
W-APN	WLAN - APN
WLAN	Wireless Local Area Network
WSID	WLAN Specific Identifier

4 General

4.1 3GPP WLAN interworking system

Within this specification, no distinction is made between roaming and non-roaming scenarios. Therefore, within the scope of this specification, the Wa and Wd reference points defined in 3GPP TS 23.234 [2] are considered identical.

The WLAN UE is equipped with a universal integrated circuit card (UICC) in order to access the WLAN interworking service. For emergency cases, and dependent on local regulations, access shall be possible even if the WLAN UE is not equipped with a valid SIM or valid USIM.

NOTE: IMS emergency call can fail due to local regulation and or roaming agreements. Even after the failure of the IMS emergency call a WLAN UE can further attempt the IMS emergency call following the procedures for when the WLAN UE is not equipped with a valid SIM or a valid USIM.

The 3GPP AAA server procedures covered in the present document are:

- Authentication of the 3GPP subscriber based on the SIM/USIM credentials; and
- Access authorization of the 3GPP subscriber based on the WLAN access authorization information retrieved from HLR/HSS.

Other functionalities of the 3GPP AAA server are covered in 3GPP TS 29.234 [3].

WLAN technologies other than those compliant with IEEE 802.11 1999 [11], such as HiperLAN or Bluetooth, are not described specifically in this version of the present document. However, they are not excluded.

4.2 WLAN UE identities

4.2.1 General

WLAN UEs use network access identifier (NAI) as identification towards the 3GPP WLAN AAA server in the EAP Response/Identity message. The NAI is structured according to 3GPP TS 23.003 [1A].

4.2.2 Root NAI

This is the NAI format used by the WLAN UE when it attempts to authenticate directly to HPLMN (see IETF RFC 4284 [12] and 3GPP TS 23.234 [2]). The root NAI format is specified in 3GPP TS 23.003 [1A] subclause 14.3. The usage of the root NAI is specified in clause 5.

4.2.3 Decorated NAI

This is the NAI format used by the WLAN UE when it attempts to authenticate to HPLMN via VPLMN (see IETF RFC 4284 [12] and 3GPP TS 23.234 [2]). The decorated NAI format is specified in 3GPP TS 23.003 [1A] subclause 14.4. The usage of the decorated NAI is specified in clause 5.

4.2.4 Alternative NAI

This is the NAI format used by the WLAN UE when it attempts to obtain a list of available PLMNs during a manual selection procedure. The alternative NAI format is specified in 3GPP TS 23.003 [1A] subclause 14.6. The usage of alternative NAI is specified in clause 5.

4.2.4A Emergency NAI

This is the NAI format used by the WLAN UE when it attempts to authenticate for making an IMS emergency call. The emergency NAI format is specified in 3GPP TS 23.003 [1A] subclause 14.8. The usage of the emergency NAI is specified in clauses 4, 6 and 8.

4.2.5 Username

The generation of, and the rules for the use of the username part of an NAI in the WLAN UE are defined in subclause 6.1. The format of the username part of an NAI is defined in 3GPP TS 23.003 [1A].

4.3 Scanning procedures

4.3.1 IEEE 802.11 WLANs

For IEEE 802.11 [11] WLANs, the WLAN name is provided in the SSID information element.

The WLAN UE becomes aware of the supported WSIDs of the WLAN by performing scanning procedures as specified in IEEE 802.11-2007 [11].

There are two types of scanning procedures specified in IEEE 802.11-2007 [11]:

i) Passive scanning.

ii) Active scanning.

The WLAN UE shall support passive scanning according to IEEE 802.11-2007 [11]. If active scanning is supported then, the WLAN UE should use active scanning according to IEEE 802.11-2007 [11].

In order to assist PLMN selection procedure, the WLAN UE shall create a list of available WSIDs. The list of available WSIDs consists of all WSIDs found in passive scanning and all WSIDs received as a result of active scanning.

The WLAN UE may support additional active scanning procedures as defined in IEEE Std 802.11u™-2011 [23]. If the WLAN UE and WLAN support the IEEE Std 802.11u™-2011 [23] procedures, the list of available PLMNs may be constructed through the use of the Access Network Query Protocol (ANQP).

4.3.2 Other WLAN technologies

Other WLAN technologies, such as HiperLAN or Bluetooth, are not described in this TS but are not excluded.

4.4 Network discovery

4.4.1 General

Network discovery can be performed in three ways:

1) if the "HPLMN Direct Access Indicator" as specified in subclause 7.11 allows direct access, then direct connection from the I-WLAN to HPLMN using internet where authentication has been performed using a none IEEE 802.1x authentication mechanism;

2) via a PLMN using IEEE 802.1x authentication access; or

3) via IEEE Std 802.11u™-2011 [23] ANQP.

In case 1) the WLAN UE once it has obtained I-WLAN access shall perform tunnel management procedures per the clause 8 to access the HPLMN.

In case 2) when IEEE 802.1x authentication mechanisms are used, the network discovery procedure shall be executed between the WLAN UE and the local AAA for the purpose of sending to the WLAN UE the supported PLMNs list for WLAN access for the manual selection procedure. The WLAN UE shall support the identity selection hints for EAP procedure as specified in IETF RFC 4284 [12]. The WLAN UE shall send the alternative NAI to the local AAA to trigger the network discovery procedure. If the I-WLAN is unable to route the WLAN UE's EAP authentication signalling to the 3GPP AAA server based on the NAI sent in the initial EAP-Response/Identity message and if the local AAA:

a) supports identity selection hints for EAP procedure as described in IETF RFC 4284 [12], then the I-WLAN sends a subsequent EAP-Request/Identity message to the WLAN UE including the supported PLMNs list for WLAN access; or

b) does not support identity selection hints for EAP procedure as described in IETF RFC 4284 [12], then the I-WLAN sends an EAP-Failure message to the WLAN UE.

In case 3) for WLANs and WLAN UEs that support IEEE Std 802.11u™-2011 [23], the WLAN UE shall use ANQP to trigger the sending of the generic container. If the WLAN supports advertisement of PLMNs via IEEE Std 802.11u™-2011 [23] the WLAN shall send back an ANQP response to the WLAN UE including the supported PLMNs list, using the format defined in Annex A. If the WLAN UE receives alternative ANQP responses, where the "Info ID" is not "3GPP Cellular Network information", the behaviour of the WLAN UE is outside the scope of this specification.

NOTE: How the WLAN system obtains the Supported PLMN list when using IEEE Std 802.11u™-2011 [23] procedures is outside of the scope of this specification.

For PLMNs that support emergency optimizations, this is indicated via the inclusion of the emergency specific service realm as defined in 3GPP TS 23.003 [1A].

4.4.2 WLAN UE procedures

Upon reception of an IEEE Std 802.11u™-2011 [23] ANQP response or EAP-Request/Identity message including the supported PLMNs list for WLAN access, the WLAN UE shall:

1) perform PLMN selection according to subclause 5.2;

2) if not authenticating for the purposes of performing IMS emergency call:

   a) if the selected PLMN is the HPLMN, then use root NAI as specified in subclause 4.2.2; and

   b) if the selected PLMN is a PLMN other than the HPLMN, then use the decorated NAI as specified in subclause 4.2 and using the PLMN ID of the selected PLMN;

3) if authenticating for the purposes of performing IMS emergency call:

   a) use emergency NAI as specified in subclause 4.2.4A; and

4) attempt to authenticate as specified in subclause 6.1.1 and using the NAI determined in the prior step.

As an implementation option, the WLAN UE may store the supported PLMNs list for WLAN access.

5 Network selection

5.1 General

WLAN selection consists of two selection procedures: I-WLAN selection and PLMN selection. These procedures are applicable to initial network selection at WLAN UE switch on and following recovery from lack of WLAN radio coverage. In order to ensure that the result of network selection is the association with an I-WLAN that has direct connection to HPLMN, both procedures are linked to each other as specified in this clause.

Two 3GPP - WLAN interworking network selection modes are defined, automatic and manual. At switch on, if the WLAN UE provides the optional feature of user preferred PLMN selection operating mode then this operating mode shall be used. The support of additional network selection modes is implementation dependent.

For manual network selection procedures defined in subclause 5.2.3 the WLAN UE produces a list of available PLMNs. The list of PLMN shall be acquired by performing one of the following:

1) If the WLAN UE and WLAN supports IEEE Std 802.11u™-2011 [23] then ANQP shall be used each WSID;

2) If the WLAN UE and WLAN supports IEEE 802.1x authentication, the WLAN UE shall associate and perform EAP based network discovery with the available WSID using the Alternative NAI until every available WLAN has been associated with and EAP network discovery has been performed; or

3) If the WLAN does not support IEEE 802.1x authentication and the "HPLMN Direct Access Indicator" as specified in subclause 7.11 allows direct access and if the WLAN UE chooses to perform direct access to HPLMN, then the WLAN UE shall attempt to create a direct connection to the HPLMN using tunnel management procedures as defined in clause 8.

For automatic selection procedures defined in subclause 5.2.4.

As an alternative option to this, if the WLAN UE is in automatic network selection mode and it finds a WSID known to support connectivity to the HPLMN, the WLAN UE selects the HPLMN and does not return to the I-WLAN Last registered PLMN. The operator controls this by the "I-WLAN HPLMN Priority Indication" as specified in subclause 7.10 whether a WLAN UE that supports this option performs this alternative behaviour. If the HPLMN cannot be found, the WLAN UE returns to the I-WLAN last registered PLMN if available.

If there is no I-WLAN Last Registered PLMN, or if selection is not possible due to the PLMN being unavailable or selection failure, the WLAN UE shall use a WSID that has a direct connection to HPLMN. This is done by performing the procedures in 1) – 3) above with the available WSIDs until a WSID that has a direct connection to the HPLMN has been found. If a WSID that has direct connection to HPLMN is not found, then the WLAN UE attempts to select a WSID that has connection to one of the PLMNs in the preferred PLMNs lists. The order that the WLAN UE follows for association with the available WSIDs is determined by the "User Controlled WLAN Specific Identifier list", "Home I-WLAN Specific Identifier List" and "Operator Controlled WLAN Specific Identifier list", if available.

Network selection procedure is completely independent of the result of the PLMN selection under other radio access technologies that are specified in 3GPP TS 23.122 [1]. The signal quality shall not be used as a parameter for network selection.

To assist in selecting a PLMN a number of lists are defined: the"User Controlled PLMN Selector list for I-WLAN" and the "Operator Controlled PLMN Selector list for I-WLAN". If these lists are supported on the USIM then the WLAN UE shall read and use all the entries.

5.2 PLMN selection

5.2.1 WLAN UE I-WLAN selection procedure

The WLAN UE shall use scanning procedures as specified in subclause 4.3 in order to find the available WSIDs.

For the purpose of discovering the supported PLMNs:

1) If both the WLAN and WLAN UE supports IEEE Std 802.11u™-2011 [23] the WLAN UE shall use ANQP procedures sequentially with each WSID; and

2) The WLAN UE shall sequentially perform association with each WSID.

The above shall be performed using the list of available WSIDs in the following order:

a) If the "I-WLAN HPLMN Priority Indication" as specified in subclause 7.10 is available and is set then if the "Home I-WLAN Specific Identifier list" data file is available in the USIM, each WSID in the "Home I-WLAN Specific Identifier list" data file in the USIM (in priority order).

b) If the "User Controlled WLAN Specific Identifier list" data file is available in the USIM, each WSID in the "User Controlled WLAN Specific Identifier list" data file in the USIM (in priority order).

c) If the "Operator Controlled WLAN Specific Identifier list" data file is available in the USIM, each WSID in the "Operator Controlled WLAN Specific Identifier list" data file in the USIM (in priority order).

NOTE: Requirements for the presence of the "User Controlled WLAN Specific Identifier list" data file, "Home I-WLAN Specific Identifier list" and the "Operator Controlled WLAN Specific Identifier list" data file are defined in 3GPP TS 31.102 [13].

d) If neither "User Controlled WLAN Specific Identifier list", "Home I-WLAN Specific Identifier list" nor "Operator Controlled WLAN Specific Identifier list" data file is available in the USIM and the ME supports at least one of the optional "User Controlled WLAN Specific Identifier list", "Home I-WLAN Specific Identifier list" or "Operator Controlled WLAN Specific Identifier list" lists in the ME memory:

i) if the "I-WLAN HPLMN Priority Indication" as specified in subclause 7.10 is available and is set then each WSID in the "Home WLAN Specific Identifier list" data file in the ME (in priority order);

ii) each WSID in the "User Controlled WLAN Specific Identifier list" data file in the ME (in priority order);

iii) each WSID in the "Operator Controlled WLAN Specific Identifier list" data file in the ME (in priority order).

e) Other WSIDs supporting 3GPP - WLAN interworking in implementation specific order.

In the case of Automatic PLMN selection the WLAN UE shall stop performing association with other WLANs once a direct connection to the HPLMN has been found if there is:

1) no EHPLMN list present; or

2) the EHPLMN list is present but empty; or

3) the EHPLMN list has a single entry which is the PLMN derived from the IMSI.

In the case when the EHPLMN list is present and the list has:

1) a single entry that is not the PLMN derived from the IMSI then the WLAN UE shall stop performing association with other WLANs once a direct connection to the EHPLMN has been found; or

2) two or more entries, then the WLAN UE shall stop association with other WLANs when the highest priority EHPLMN has been found.

If no association with any I-WLAN is found, the WLAN UE behaviour is implementation dependent.

The PLMN identities thus found are used in the PLMN selection procedure.

5.2.2 Void

5.2.3 Manual PLMN selection mode procedure

In case of manual network selection mode, for WLANs that:

1) together with the WLAN UE support IEEE Std 802.11u™-2011 [23], the WLAN UE shall send an ANQP request to each WSID. If the WSID supports advertisement of PLMNS, it shall send back an ANQP response to the WLAN UE including the Supported PLMNs list for WLAN access. See Annex A. If the WLAN UE receives a ANQP response where the "Info ID" is not "3GPP Cellular Network information" the behaviour of the WLAN UE is outside the scope of this specification.

2) support IEEE 802.1x authentication, the WLAN UE shall request for a list of supported PLMNs by issuing an EAP-Response/Identity message to the WLAN including as identity the alternative NAI. See subclause 4.2.5.

3) do not support IEEE 802.1x authentication, if the "HPLMN Direct Access Indicator " as specified in subclause 7.11 allows direct access and if the WLAN UE chooses to perform direct access to HPLMN, then for HPLMN access the WLAN UE shall sequentially perform association and perform tunnel management procedures as specified in the clause 8 with each broadcast WSID that does not support IEEE 802.1x authentication.

NOTE: In case 3), if authentication is required to access the internet when accessing a WLAN that does not support IEEE 802.1x authentication then the procedures to do this are outside scope of this specification.

Based on the results of Items 1) - 3) above, the WLAN UE shall indicate to the user the PLMNs which are available. If more than one I-WLAN is capable of being used to establish a direct connection with a PLMN, the WLAN UE should indicate each of the candidate I-WLANs along with the PLMN to the user. If displayed, PLMNs from the Supported PLMNs list shall be presented in the following order:

a) HPLMN (if the EHPLMN list is not present, or is present and empty);

b) If one or more of the EHPLMNs are available then based on the optional "I-WLAN Equivalent HPLMN Presentation Indication" as specified in subclause 7.12 either the highest priority EHPLMN among those that are available is to be presented to the user or all available EHPLMNs are presented to the user in priority order;

c) If the "User Controlled PLMN Selector for I-WLAN access" data file is available, PLMNs in the "User Controlled PLMN Selector for I-WLAN access" data file in the USIM (in priority order).

d) If the "Operator Controlled PLMN Selector for I-WLAN access" data file is available, PLMNs in the "Operator Controlled PLMN Selector for I-WLAN access" data file in the USIM (in priority order).

e) If neither "User Controlled PLMN Selector for I-WLAN access" nor "Operator Controlled PLMN Selector for WLAN access" data file is available in the USIM or in case when SIM is inserted:

   i) each PLMN in the "User Controlled PLMN Selector with Access Technology" data file, if available in the USIM/SIM (in priority order);

   ii) each PLMN in the "Operator Controlled PLMN Selector with Access Technology" data file, if available in the USIM/SIM (in priority order).

f) If none of the PLMN selector lists in steps c, d and e is available and the ME supports at least one of the optional "User Controlled PLMN Selector for I-WLAN access" and "Operator Controlled PLMN Selector for I-WLAN access" lists in the ME:

   i) each PLMN in the "User Controlled PLMN Selector for I-WLAN access" data file in the ME (in priority order);

   ii) each PLMN in the "Operator Controlled PLMN Selector for I-WLAN access" data file in the ME (in priority order).

g) Any other PLMN in random order.

The HPLMN may provide on the USIM additional information on the available PLMNs. If this information is provided then the WLAN UE shall indicate it to the user. This information, provided as free text may include:

- preferred partner;
- roaming agreement status; and
- supported services.

Furthermore, the WLAN UE may indicate whether the available PLMNs are present on the EHPLMN list, the "User Controlled Selector for I-WLAN access" data file or the "Operator Controlled PLMN Selector for I-WLAN access" data file. The WLAN UE may also indicate that the PLMN is not present on any of these lists.

If a PLMN was selected before the procedure and if the user does not select a PLMN, the selected PLMN shall be the one that was selected before the PLMN selection procedure started.

If successful authentication is achieved, the WLAN UE shall indicate the selected PLMN. If the"I-WLAN Last Registered PLMN" data file is available in the USIM (see 3GPP TS 31.102 [13]) then the WLAN UE shall store the selected PLMN on the USIM else the WLAN UE shall store the selected PLMN on the ME.

If no PLMN is found, the WLAN UE behaviour is implementation dependent.

5.2.4 Automatic PLMN selection mode procedure

In case of automatic selection for WLANs that UE shall select and attempt to authenticate with an available and allowable PLMN. For WLANs that:

1) together with the WLAN UE support IEEE Std 802.11u™-2011 [23], the WLAN UE shall send an ANQP request to each WSID. If the WSID supports advertisement of PLMNS, it shall send back an ANQP response to the WLAN UE including the Supported PLMNs list for WLAN access. See Annex A. If the WLAN UE receives a ANQP response where the "Info ID" is not "3GPP Cellular Network information" the behaviour of the WLAN UE is outside the scope of this specification.

2) do not support IEEE 802.1x authentication, if the "HPLMN Direct Access Indicator" as specified in subclause 7.11 allows direct access and if the WLAN UE chooses to perform direct access to HPLMN, then the WLAN UE shall sequentially perform association and perform tunnel management procedures as specified in the clause 8 with each broadcast WSID that does not support IEEE 802.1x authentication.

3) support IEEE 802.1x authentication, the WLAN UE shall request for a list of supported PLMNs by issuing an EAP-Response/Identity message to the WLAN including as identity the alternative NAI. See subclause 4.2.5.

Based on the results of Items 1) - 3) above, the WLAN UE shall choose an available and allowable PLMN in the following order:

a) If the "I-WLAN HPLMN Priority Indication" as specified in subclause 7.10 is available and set to prioritise HPLMN, then:

i) HPLMN (if the EHPLMN list is not present, or is empty);

ii) if the EHPLMN list is present and contains at least one entry the highest EHPLMN that is available; and

iii) if the "I-WLAN Last Registered PLMN" data file is available in the USIM, the PLMN in the "I-WLAN Last Registered PLMN" in the USIM;

else if the "I-WLAN Last Registered PLMN" data file is not available in the USIM and the ME supports the "I-WLAN Last Registered PLMN", the PLMN in the "I-WLAN Last Registered PLMN" in the ME;

b) If "I-WLAN HPLMN Priority Indication" as specified in subclause 7.10 is available and is not set or is not present on the USIM:

i) if the "I-WLAN Last Registered PLMN" data file is available in the USIM, the PLMN in the "I-WLAN last Registered PLMN" in the USIM;

else if the "I-WLAN Last Registered PLMN" data file is not available in the USIM and the ME supports the "I-WLAN Last Registered PLMN" and the last registered PLMN for I-WLAN is available and set to prefer the last registered PLMN, then the PLMN in the "I-WLAN Last Registered PLMN" in the ME;

ii) HPLMN (if the EHPLMN list is not present, or exists but is empty); or

iii) if the EHPLMN list is present and contains at least one entry the highest EHPLMN that is available.

c) If the "User Controlled PLMN Selector for I-WLAN access" data file is available in the USIM, each PLMN in the "User Controlled PLMN Selector for I-WLAN access" data file in the USIM (in priority order) ;

d) If the "Operator Controlled PLMN Selector for I-WLAN access" data file is available in the USIM, each PLMN in the "Operator Controlled PLMN Selector for I-WLAN access" data file in the USIM (in priority order);

NOTE: Requirements for the presence of the "User Controlled PLMN Selector for I-WLAN access" data file and the "Operator Controlled PLMN Selector for I-WLAN access" data file are defined in 3GPP TS 31.102 [13].

e) If neither "User Controlled PLMN Selector for I-WLAN access" nor "Operator Controlled PLMN Selector for I-WLAN access" data file is available in the USIM or in case when SIM is inserted:

i) each PLMN in the "User Controlled PLMN Selector with Access Technology" data file, if available in the USIM/SIM (in priority order);

ii) each PLMN in the "Operator Controlled PLMN Selector with Access Technology" data file, if available in the USIM/SIM (in priority order).

f) If none of the PLMN selector lists in steps b, c and d is available and the ME supports at least one of the optional "User Controlled PLMN Selector for I-WLAN access" or "Operator Controlled PLMN Selector for I-WLAN access" lists in the ME:

i) each PLMN in the "User Controlled PLMN Selector for I-WLAN access" data file in the ME (in priority order);

ii) each PLMN in the "Operator Controlled PLMN Selector for I-WLAN access" data file in the ME (in priority order).

g) Any other PLMN in random order.

If successful authentication is achieved, the WLAN UE shall indicate to the user the selected PLMN. If the "I-WLAN Last Registered PLMN" data file is available in the USIM, the WLAN UE shall store the selected PLMN on the USIM else the WLAN UE shall store the selected PLMN on the ME.

If no PLMN is selected, the WLAN UE behaviour is implementation dependent.

If the WLAN UE loses coverage with the associated access point, a new I-WLAN is discovered automatically using the I-WLAN association procedure in subclause 5.2.1.

5.2.5 Network selection for emergency case

5.2.5.1 General

For cases where the WLAN UE has already successfully performed I-WLAN network selection, authentication and authorization, the WLAN UE may reuse this connection for the purposes of performing IMS emergency calls if the selected VPLMN supports the emergency realm. Else the WLAN UE shall select another PLMN via the I-WLAN that supports the emergency realm.

5.2.5.2 Manual PLMN selection for emergency case

Manual PLMN selection shall take place as described in subclause 5.2.3. For those PLMNs that support the emergency specific service realm, the support for this emergency specific realm shall be listed as well as that of its parent PLMN.

5.2.5.3 Automatic PLMN selection mode procedure for emergency case

Automatic PLMN selection shall take place as described in subclause 5.2.4 however if the WLAN UE also supports any RAT defined by 3GPP (see 3GPP TR 21.905 [1C]), the WLAN UE shall ensure that the PLMN selected via I-WLAN, is in the same country as that discovered as the result of performing a wideband scan of RATs defined by 3GPP, i.e. the WLAN UE shall correlate the available PLMN country codes via RATs defined by 3GPP with those available via I-WLAN. If no networks are discovered as a result of performing the wideband scan of RATs defined by 3GPP, the WLAN UE shall select any PLMN supporting the emergency realm (see 3GPP TS 23.003 [1A]) in an implementation dependent way. For cases where no PLMN is advertised supporting the emergency realm, UE shall select any PLMN in an implementation dependent way.

5.2.5.4 Network selection in the case of a WLAN UE equipped with neither a valid SIM nor a valid USIM

For the case the WLAN UE is not equipped with a valid SIM or a valid USIM, when the WLAN UE also supports any RAT defined by 3GPP (see 3GPP TR 21.905 [1C]), the WLAN UE shall perform a wideband scan of RATs defined by 3GPP and shall store the available PLMN country codes. The WLAN UE shall then select any PLMN supporting the emergency realm (see 3GPP TS 23.003 [1A]) that is in the same country as any of the available PLMNs. In the following cases:

- no PLMNs via I-WLAN are in the same country as the available PLMNs via RATs defined by 3GPP;
- the WLAN UE does not support any RAT defined by 3GPP; or
- PLMNs from more than one country are available,

the WLAN UE shall select any PLMN supporting the emergency realm in an implementation dependent way.

For cases where no PLMN is advertised supporting the emergency realm, UE shall select any PLMN in an implementation dependent way.

5.3 Void

5.4 User reselection and steering of roaming

5.4.1 WLAN UE procedures

5.4.1.1 General

At any time the user or HPLMN via the steering of roaming feature can request the WLAN UE to initiate reselection onto a supported PLMN, according to the following procedures, dependent upon the PLMN selection mode (automatic or manual). In this case and in both PLMN selection modes, the WLAN UE shall:

- disassociate with the current associated WSID by initiating disassociation procedure as specified in IEEE 802.11 1999 [11];
- initiate association procedure as specified in IEEE 802.11 1999 [11], taking into account PLMN selection procedure as specified in subclause 5.2;
- depending on the PLMN selection mode (automatic or manual), perform a new PLMN selection as specified in subclauses 5.4.1.2 and 5.4.1.3.

5.4.1.2 Automatic network selection mode

The WLAN UE shall follow the automatic network selection mode procedure as specified in subclause 5.2.4 with the exception that the WLAN UE shall not chose the current mediating PLMN unless it is the only PLMN that is available.

5.4.1.3 Manual network selection mode

The WLAN UE shall follow the manual network selection mode procedure as specified in subclause 5.2.3

5.4.1.4 Steering of roaming

If the WLAN UE receives a USAT REFRESH command qualifier (see 3GPP TS 31.111 [22]) of type "Steering of Roaming for I-WLAN", and if the "Operator Controlled PLMN Selector for I-WLAN access" data file is available in the USIM the WLAN UE shall:

a) replace the highest priority entries in the "Operator Controlled PLMN Selector for I-WLAN access" list in the USIM and the ME, if available, with the list provided in the REFRESH command; and

b) attempt to obtain service on a different PLMN as specified in subclause 5.4.1.2

In order to avoid unnecessary signalling, repeateded using of steering of roaming of a particular WLAN UE should be avoided.

5.4.2 3GPP AAA server procedures

The WLAN UE may associate with a new access point and select a different PLMN than the current PLMN in which the WLAN UE has been authenticated. In this case the 3GPP AAA server may receive a new EAP authentication request from the same user but from a different PLMN (e.g. the new selected WLAN VPLMN will generate a new decorated NAI). The 3GPP AAA server shall proceed with the new EAP authentication request.

If the EAP authentication procedure triggered by the new EAP authentication request from the same user is successful, the 3GPP AAA server may either release the current stored authentication status information or keep both the current stored authentication status information and the new authentication status information obtained from the latest successful EAP authentication procedure.

6 WLAN UE to 3GPP network protocols

6.1 WLAN UE to 3GPP AAA server protocols

6.1.1 WLAN access authentication and authorization protocols

6.1.1.1 General

6.1.1.1.1 Non-emergency case

WLAN authentication signalling shall be executed between WLAN UE and 3GPP AAA server for the purpose of authenticating the end-user and enabling the access to the WLAN or to the WLAN and the 3GPP network.

WLAN authentication signalling for 3GPP - WLAN interworking shall be based on extensible authentication protocol (EAP) as specified in IETF RFC 3748 [6]).

The WLAN UE and the 3GPP AAA server shall support EAP authentication procedures as specified in IETF RFC 4187 [9] and IETF RFC 4186 [10].

Other EAP authentication methods than those specified in IETF RFC 4187 [9] and IETF RFC 4186 [10] may also be supported by the WLAN UE, but are not part of 3GPP - WLAN interworking; therefore these other EAP authentication methods are out of the scope of the present document.

WLAN access authorization shall be performed upon successful user authentication in the 3GPP AAA server and it includes access rules as defined by the operator (see subclause 6.1.1.3.6).

6.1.1.1.2 WLAN access authentication and authorization in the emergency case

For the case of access for the purpose of using I-WLAN as the access network for IMS emergency calls the WLAN UE and the 3GPP AAA server shall support extensible authentication protocol (EAP) as specified in IETF RFC 3748 [6]. Two different cases can be identified:

a) The WLAN UE is equipped with a valid SIM or valid USIM: The requirements as specified in subclause 6.1.1.1.1 shall apply with the following modification:

   WLAN access authorization shall not be performed.

b) The WLAN UE is not equipped with a valid SIM or valid USIM: The WLAN UE and the 3GPP AAA server shall use EAP-TLS based authentication as specified in IETF RFC 5216 [16A] in which client authentication is omitted (see 3GPP TS 33.234 [5]).

6.1.1.2 WLAN UE procedures

6.1.1.2.1 Identity management

In both EAP AKA and EAP SIM based authentications, the WLAN UE shall proceed as follows.

The WLAN UE shall always use the leading digits notation when building the username part of NAI from IMSI, as specified in 3GPP TS 23.003 [1A]. IETF RFC 4187 [9] and IETF RFC 4186 [10] each define the leading digits to identify their particular authentication mechanism.

In the first EAP-Response/Identity message the WLAN UE shall include a NAI which username is derived from IMSI. The format of such username is defined in 3GPP TS 23.003 [1A]. The WLAN UE shall include the root NAI or decorated NAI for authentication purposes. The WLAN UE shall include the alternative NAI for manual network selection procedure.

The WLAN UE shall support the mechanism for communicating its identity to the server using EAP/AKA and EAP/SIM messages as specified in EAP AKA and EAP SIM respectively.

If the WLAN UE receives an EAP-Request/AKA-Identity message or EAP-Request/SIM/Start message including an AT_PERMANENT_ID_REQ attribute after sending an identity response including the pseudonym, the WLAN UE shall respond to this new identification request by including a NAI in which username is derived from IMSI. This WLAN UE behaviour is defined in IETF RFC 4186 [10] and in IETF RFC 4187 [9].

6.1.1.2.2 User identity privacy

In both EAP AKA and EAP SIM based authentications, the support of user identity privacy is mandatory for the WLAN UE.

The reception of temporary identity(ies) (pseudonym and/or re-authentication identity) in any EAP authentication indicates to the WLAN UE that user identity privacy is enabled as described in subclause 6.1.1.3.2.

The WLAN UE shall not interpret the temporary identity(ies), but store the received identity(ies) and use it at the next EAP authentication.

If the WLAN UE receives temporary identity(ies) (pseudonym and/or re-authentication identity) during EAP authentication from the 3GPP AAA server (as specified in 3GPP TS 33.234 [5]), then the WLAN UE shall process the authentication challenge information (e.g. RAND, AUTN, MAC) received together with the temporary identity(ies). If the EAP authentication procedure is successful (i.e. EAP–Success message), the WLAN UE shall consider the new temporary identity(ies) as valid.

The WLAN UE after successful EAP authentication takes the following actions if new temporary identity(ies) was received in AT_ENCR_DATA attribute:

- if the temporary identity is a pseudonym, the WLAN UE shall store it in the "Pseudonym" data file in the USIM. If the "Pseudonym" data file is not available in the USIM, the WLAN UE shall store the pseudonym in the ME; and

- if the temporary identity is a re-authentication identity, the WLAN UE shall store it in the "Re-authentication identity", data file in the USIM together with new master key, transient EAP keys and counter value. If the "Re-authentication identity" data file is not available in the USIM, the WLAN UE shall store the re-authentication identity in the ME together with new master key, transient EAP keys and counter value.

The WLAN UE after successful EAP authentication takes the following actions if no new temporary identity(ies) was received in AT_ENCR_DATA attribute:

- Temporary identities are one-time identities. If the WLAN UE does not receive a new temporary identity(ies), the WLAN UE shall delete the corresponding temporary identity(ies) from the USIM/ME (i.e. the WLAN UE shall set the username of the corresponding temporary identity(ies) field to the "deleted" value to indicate no valid temporary identity(ies) exists as specified in 3GPP TS 23.003 [1A]). When the temporary identity(ies) stored in the USIM/ME indicates the "deleted" value in the username part, the WLAN UE shall consider the corresponding temporary identity(ies) as invalid and shall not send that temporary identity(ies) at the next EAP authentication.

Upon reception of an EAP-Request/Identity message, the WLAN UE shall take one of the following actions depending on the presence of the temporary identity(ies):

- if valid re-authentication identity is available, the WLAN UE shall use the re-authentication identity at the next EAP authentication. If not, then

- if valid pseudonym is available, the WLAN UE shall use the pseudonym at the next EAP authentication. If not, then

- The WLAN UE shall use the permanent IMSI-based identity at the next EAP authentication.

6.1.1.2.3 EAP AKA based authentication

The WLAN UE with USIM inserted shall support EAP AKA based authentication, and it shall attempt to authenticate using EAP AKA authentication as the first EAP method. The WLAN UE shall be able to accept EAP AKA based authentication in the EAP method negotiation.

6.1.1.2.4 EAP SIM based authentication

If the WLAN UE supports the ME-SIM interface, and if SIM has been inserted, then the WLAN UE shall support EAP SIM based authentication. In this case, the WLAN UE shall be able to accept EAP SIM based authentication as EAP method negotiation.

The EAP SIM based authentication does not require the ME-SIM interface, and therefore EAP SIM based authentication could also be performed using the 2G authentication and key agreement (AKA) functions on the USIM application. However, if a UICC with USIM has been inserted, then the default EAP method policy of the WLAN UE shall not accept EAP SIM based authentication.

6.1.1.2.4.1 Interoperability cases

If the WLAN UE does not accept EAP SIM based authentication when USIM has been inserted, then interoperability problems may occur with pre-release 6 AAA servers that only support EAP SIM based authentication. Therefore, ME implementations may allow configuring an EAP method policy that allows EAP SIM based authentication even if a UICC with USIM has been inserted.

6.1.1.2.5 Re-authentication

In both EAP AKA and EAP SIM based authentication, the support of re-authentication is mandatory for the WLAN UE.

The reception of re-authentication identity in any EAP authentication indicates to the WLAN UE that fast re-authentication is enabled as described in subclause 6.1.1.3.5.

If the WLAN UE receives a re-authentication identity from the 3GPP AAA server (as specified in 3GPP TS 33.234 [5]), then the WLAN UE shall process the authentication challenge information (e.g. Counter, NONCE, MAC) received together with the re-authentication identity. If the authentication challenge procedure is successful, the WLAN UE shall consider the new re-authentication identity as valid.

The WLAN UE after successful EAP authentication shall store the new re-authentication identity and associated security parameters and overwrite any previously stored re-authentication identity and associated security parameters as described in subclause 6.1.1.2.2.

The WLAN UE shall send the re-authentication identity during the re-authentication attempt to the 3GPP AAA Server, only if re-authentication identity, whose value is not set to "deleted", exists.

6.1.1.2.6 Protected result indications

The WLAN UE shall support protected result indications (i.e. MAC protected) for both EAP AKA and EAP SIM as specified in 3GPP TS 33.234 [5].

The reception of the result indication (i.e. AT_RESULT_IND attribute) at any EAP authentication indicates to the WLAN UE that the 3GPP AAA server requests to use protected success result indications.

If the WLAN UE receives a result indication in the EAP-Request/AKA-Challenge or EAP-Request/SIM-Challenge message during the EAP authentication, the WLAN UE shall process the challenge information. Then, the WLAN UE takes the following actions depending on the result of the EAP authentication procedure:

- if the EAP authentication is successful, the WLAN UE shall include the result indication along with the authentication response (e.g. MAC and RES) in the EAP-Response/AKA-Challenge or EAP-Response/SIM-Challenge message. Then, if the EAP authentication is also successful on the 3GPP AAA server side, the WLAN UE receives an EAP-Request/AKA-Notification or EAP-Request/SIM-Notification message, which contains a success notification and is MAC protected, prior the EAP-Success message.
- if the EAP authentication is unsuccessful, the WLAN UE shall send an EAP-Response/AKA-Client-Error or EAP-Response/SIM-Client-Error message. Then, the WLAN UE shall wait for the reception of the EAP Failure message to conclude the EAP authentication procedure.

Upon receipt of an EAP-Request/AKA-Notification or EAP-Request/SIM-Notification message, the WLAN UE shall acknowledge it by sending an EAP-Reponse/AKA-Notification or EAP-Response/SIM-Notification message. Then, the

WLAN UE shall wait for the reception of the EAP-Success or EAP-Failure message to conclude the EAP authentication procedure.

NOTE 1: The EAP-Request/AKA-Notification or EAP-Request/SIM-Notification message contains an indication of whether the EAP authentication procedure is successful or unsuccessful as specified in IETF RFC 4187 [9] and IETF RFC 4186 [10].

NOTE 2: The EAP AKA and EAP SIM signalling flows are described in 3GPP TS 33.234 [5].

6.1.1.2.7 UE procedures in the emergency case

For the purpose of using I-WLAN as the access network for IMS emergency calls two different cases can be identified:

a) The WLAN UE is equipped with a valid SIM or valid USIM: The requirements as specified in subclauses 6.1.1.2.1, 6.1.1.2.2, 6.1.1.2.3, 6.1.1.2.4, 6.1.1.2.5 and 6.1.1.2.6 shall apply with the following modification:

   On building the NAI in the first EAP-Response/Identity message, the WLAN UE shall use the emergency realm, if it is available, for a selected PLMN (see 3GPP TS 23.003 [1A]).

b) The WLAN UE is not equipped with a valid SIM or valid USIM: The WLAN UE shall support protected result indications (i.e. MAC protected) for extensible authentication protocol (EAP) as specified in IETF RFC 3748 [6] (see subclause 6.1.1.2.6).

   The WLAN UE shall include in the first EAP-Response/Identity message an emergency NAI.

   If the WLAN UE receives an EAP-Request/TLS message, the WLAN UE shall respond with an EAP-Response/TLS message (see IETF RFC 5216 [16A]).

NOTE: The EAP-TLS signalling flow for a WLAN UE not equipped with a valid SIM or valid USIM is described in 3GPP TS 33.234 [5].

6.1.1.3 3GPP AAA server procedures

6.1.1.3.1 Identity management

In both EAP AKA and EAP SIM based authentications, the 3GPP AAA server shall proceed as follows.

The 3GPP AAA server shall always (re)request the user identity, using EAP-Request/AKA-Identity or EAP-Request/SIM/Start, in order to ensure that it has an unmodified copy of the identity, regardless of the identity the 3GPP AAA server received in EAP-Response/Identity (see IETF RFC 4187 [9] and IETF RFC 4186 [10] for details on this requirement).

The 3GPP AAA Server shall use, if present, the leading digits part of IMSI based username to identify the proposed authentication mechanism, as specified in 3GPP TS 23.003 [1A].

6.1.1.3.2 User identity privacy

In both EAP AKA and EAP SIM based authentications, the support of user identity privacy is mandatory for the 3GPP AAA server. However, the usage of this feature is optional for the 3GPP AAA server.

The user identity privacy should be enabled in the 3GPP AAA server. If user identity privacy is enabled, the 3GPP AAA server shall send new encrypted temporary identity(ies) (pseudonym and/ or re-authentication identity) to the WLAN UE in every EAP authentication procedure. The description of temporary identity management is specified in 3GPP TS 33.234 [5].

When mapping a user temporary identity (pseudonym or re-authentication identity) to a permanent IMSI-based identity, the 3GPP AAA server shall only examine the username portion of the user temporary identity and ignore the realm portion of the identity.

NOTE: The realm portion of the temporary identity will always be the realm indicated by the 3GPP AAA server (see 3GPP TS 23.003 [1A]).

6.1.1.3.3 EAP SIM and EAP AKA based authentication

The 3GPP AAA server shall support both EAP SIM and EAP AKA based authentication as specified in IETF RFC 4187 [9] and IETF RFC 4186 [10].

6.1.1.3.4 3GPP AAA server operation in the beginning of authentication

The 3GPP AAA server shall support EAP method negotiation, as specified in EAP IETF RFC 3748 [6].

The EAP method policy of the 3GPP AAA server shall not accept EAP-SIM based authentication for USIM subscribers, and only accept EAP-SIM based authentication for SIM subscribers.

The procedure to select the EAP method to use for authentication is the following:

1) The format of the identity received in EAP-Response/Identity message may contain an indication of the EAP method to be used by the 3GPP AAA server as defined in 3GPP TS 23.003 [1A]. For example, if the identity format indicates EAP SIM, the leading character in the identity is "1" so, the identity might be a permanent IMSI-based identity for EAP SIM. The permanent identity format and the usage of leading digits for IMSI-based permanent identity are specified in IETF RFC 4187 [9] and IETF RFC 4186 [10]. The format of the pseudonyms and re-authentication identities are specified in 3GPP TS 33.234 [5].

2) If the 3GPP AAA server is not able to map the user identity received in EAP-Response/Identity message to a subscriber identity (e.g. an obsolete pseudonym), but it recognizes the EAP method, the 3GPP AAA server shall request a new identity using the EAP method indicated by the WLAN UE.

3) If the 3GPP AAA server is able to map the user identity received in EAP-Response/Identity message to a subscriber identity (IMSI), but the EAP method does not match with user's subscription information, the 3GPP AAA server shall use the EAP method indicated by user's subscription (with the exception specified in the subclause 6.1.1.3.4.1). For example, if the EAP method indicates EAP AKA, but the 3GPP AAA server has available information that subscriber's UICC only supports SIM based authentication, (e.g. received authentication vectors are triplets rather than quintuplets), then user's subscription shall prevail and the 3GPP AAA server shall propose EAP SIM as the first authentication method.

4) If the 3GPP AAA server is not able to recognize the user identity received in EAP-Response/Identity message and hence the EAP method, the EAP method to use is implementation dependent. If this EAP method does not match user's subscription in the WLAN UE, the WLAN UE shall respond with a Nak to the 3GPP AAA server. Then, the 3GPP AAA server shall use the other EAP method until a recognized identity is received.

6.1.1.3.4.1 Interoperability cases

3GPP AAA servers may be configured to support an EAP method policy that accepts EAP-SIM based authentication for USIM subscribers. This configuration option may be used, if many USIM subscribers are expected to use pre-release 6 ME implementations that do not support EAP AKA.

NOTE: When the operator issues USIM cards to subscribers, it is strongly recommended to upgrade the AAA servers to 3GPP release 6 and to support EAP-AKA.

6.1.1.3.5 Re-authentication

The 3GPP AAA server shall support re-authentication as specified in the 3GPP TS 33.234 [5].

Re-authentication should be enabled in the 3GPP AAA server. If re-authentication is enabled, the re-authentication may be full or fast, as follows:

- Full re-authentication means that a new full authentication procedure shall take place as the initial authentication procedure, where all keys are generated afresh in both the (U)SIM and network. Full re-authentication requires that the WLAN UE sends pseudonym or permanent IMSI-based identity.

- Fast re-authentication means that a new authentication procedure takes place in which Master Key and Transient EAP Keys are not generated in both the (U)SIM and network, but reused from the previous authentication process to generate the remaining keys necessary for this procedure. Fast re-authentication requires that the WLAN UE sends re-authentication identity.

The decision of using fast re-authentication is taken in the 3GPP AAA server depending on operator's policies. Operator's policies regarding fast re-authentication may contain for example, a timer to control start of fast re-authentication, a counter to control the maximum number of allowed fast re-authentications before a full EAP authentication shall be initiated towards the WLAN UE or a restriction on whether fast re-authentication is allowed to visiting subscribers.

The 3GPP AAA server indicates to the WLAN UE the decision of using fast re-authentication by means of sending the re-authentication identity in the EAP authentication procedure (i.e. in EAP-Request/AKA/Challenge or EAP-Request/AKA-re-authentication or EAP-Request/SIM/Challenge or EAP-Request/SIM/re-authentication messages). On each fast re-authentication procedure the 3GPP AAA server has the ultimate point of decision of whether to continue with the ongoing fast re-authentication procedure or to defer to a full re-authentication. Therefore, whenever the 3GPP AAA server sends a re-authentication identity to the WLAN UE, the 3GPP AAA server shall also include a pseudonym when allowed by the IETF RFC 4186 [10] and IETF RFC 4187 [9]. In this way, the WLAN UE retains a pseudonym if the 3GPP AAA server defers to full authentication.

NOTE 1: The use of fast re-authentication implies to save power consumption in the WLAN UE and processing time in both the WLAN UE and the 3GPP AAA server. However, when the fast re-authentication is used through a low trusted I-WLAN, it is strongly recommended to refresh the keys using full re-authentication. The use of fast re-authentication should be left for situations in which the user is accessing a high trusted I-WLAN.

The full and fast re-authentication signalling flows are described in 3GPP TS 33.234 [5].

6.1.1.3.6 WLAN access authorization

WLAN access authorization between the WLAN UE and the 3GPP AAA server shall be combined with the WLAN access authentication and performed before service authorization and transport IP address allocation.

The 3GPP AAA server shall perform access authorization once user authentication succeeds but before sending EAP-Success message to the WLAN UE.

The 3GPP AAA server shall check whether the user is allowed to use WLAN service based on the user's subscription and optionally, information about the I-WLAN (e.g. I-WLAN operator name, location and throughput). If the check is successful the 3GPP AAA server shall complete the authentication procedure by sending a positive response to the WLAN UE that is, an EAP-Success message.

Additionally, the 3GPP AAA server may apply certain access control rules (such as access scope limitation, time limitation, bandwidth control values, and/or user priority) based on user's subscription, the account status, O&M rules (e.g. blacklist, access limitation list), and local agreements or information about the I-WLAN.

6.1.1.3.7 Protected result indications

The 3GPP AAA server should support protected result indications (i.e. MAC protected) for both EAP AKA and EAP SIM as specified in 3GPP TS 33.234 [5]. If the 3GPP AAA server supports protected result indications, the usage of this feature is optional and depends on operator"s policies.

If the 3GPP AAA server wishes to protect the success result of the EAP authentication, the 3GPP AAA server shall send the result indication (i.e. AT_RESULT_IND attribute) to the WLAN UE along with authentication challenge information (e.g. RAND, AUTN, MAC) and possibly temporary identity(ies) in the EAP-Request/AKA-Challenge or EAP-Request/SIM-Challenge message.

Upon receipt of the EAP-Response/AKA-Challenge or EAP-Response/SIM-Challenge message, the 3GPP AAA server checks the validity of the response. Then, the 3GPP AAA server takes the following actions depending on the result of the EAP authentication procedure:

- if the EAP authentication is successful and the 3GPP AAA server has previously requested to use protected success result indications, the 3GPP AAA server shall send the EAP-Request/AKA-Notification or EAP-Request/SIM-Notification message, which contains the success notification (i.e. AT_NOTIFICATION code 32768 as specified in IETF RFC 4187 [9] and IETF RFC 4186 [10]) and is MAC protected, prior the EAP-Success message.

- if the EAP authentication is unsuccessful, the 3GPP AAA server shall send the EAP-Request/AKA-Notification or EAP-Request/SIM-Notification message, which contains the failure notification (i.e. AT_NOTIFICATION

with a code range from 0 to 32767 as specified in IETF RFC 4187 [9] and IETF RFC 4186 [10]) and is MAC protected, prior the EAP-Failure message.

NOTE 1: Prior the EAP authentication challenge round takes place (as specified in IETF RFC 4187 [9] subclause 4.3 and IETF RFC 4186 [10] subclause 6.10) the 3GPP AAA server may send an EAP-Request/AKA-Notification or EAP-Request/SIM-Notification message, which contains the failure notification (i.e. AT_NOTIFICATION with the Phase bit (P bit) set to 1 as specified in IETF RFC 4187 [9] and IETF RFC 4186 [10]) and is not MAC protected.

Upon receipt of the EAP-Response/AKA-Notification or EAP-Response/SIM-Notification message, the 3GPP AAA server shall send the EAP-Success or EAP-Failure message to conclude the EAP authentication procedure.

The 3GPP AAA server shall ignore the contents of the EAP-Response/AKA-Notification or EAP-Response/SIM-Notification message as an acknowledgement of a protected success result indication.

If the EAP authentication procedure is successful and the 3GPP AAA server has not requested to use protected success result indications (i.e. the AT_RESULT_IND attribute was not included in the EAP-Request/AKA-Challenge or EAP-Request/SIM-Challenge message), the 3GPP AAA server shall send an EAP-Success message to conclude the EAP authentication (i.e. the EAP-Request/AKA-Notification or EAP-Request/SIM-Notification message is not sent to the WLAN UE prior the EAP-Success).

Upon receipt of the EAP-Response/AKA-Client-Error or EAP-Response/SIM-Client-Error message, the 3GPP AAA server shall send the EAP-Failure message to conclude the EAP authentication procedure.

NOTE 2: The EAP AKA and EAP SIM signalling flows are described in 3GPP TS 33.234 [5].

6.1.1.3.8 3GPP AAA server procedures in the emergency case

For the case of using I-WLAN as the access network for IMS emergency calls two different cases can be identified:

a) The WLAN UE is equipped with a valid SIM or valid USIM: The requirements as specified in subclauses 6.1.1.3.1, 6.1.1.3.2, 6.1.1.3.3, 6.1.1.3.4, 6.1.1.3.5 and 6.1.1.3.7 shall apply.

NOTE 1: WLAN access authorization is not performed.

b) The WLAN UE is not equipped with a valid SIM or valid USIM: The 3GPP AAA server should support protected result indications (i.e. MAC protected) for extensible authentication protocol (EAP) as specified in IETF RFC 3748 [6]. If the 3GPP AAA server supports protected result indications, the usage of this feature is optional and depends on operator''s policies (see subclause 6.1.1.3.7).

If the user identity received in an EAP-Response/Identity message indicates the emergency NAI, the 3GPP AAA server shall send an EAP-Request/TLS message in order to initiate EAP-TLS based authentication (see 3GPP TS 29.234 [3]).

NOTE 2: The EAP-TLS signalling flow for a WLAN UE not equipped with a valid SIM or valid USIM is described in 3GPP TS 33.234 [5].

NOTE 3: The format of the NAI received in the EAP-Response/Identity message indicates whether the WLAN UE is using I-WLAN as the access network for IMS emergency calls and whether the WLAN UE accessing the network with IMSI or not as described in 3GPP TS 23.003 [1A], and 3GPP TS 29.234 [3].

7 Parameters coding

7.1 General

This clause specifies the parameters used for WLAN interworking. By default, unless otherwise specified for a particular procedure, the WLAN UE shall use the parameters described below as follows: if the parameter is available in the USIM, then the WLAN UE shall use it. If the parameter is not available in the USIM and it is present in the ME, then the WLAN UE shall use the parameter stored in ME.

7.2 Pseudonym

The format of the pseudonym is specified in 3GPP TS 33.234 [5]. The "deleted" value to indicate no valid psedonym exists in the USIM/ME is specified in 3GPP TS 23.003 [1A].

7.3 Void

7.4 User Controlled PLMN Selector for I-WLAN access

The "User Controlled PLMN Selector for I-WLAN access" file contains a list of PLMN codes preferred by the user. It shall be possible to store at least ten entries on the list. The contents of this file are specified in 3GPP TS 31.102 [13].

7.5 Operator Controlled PLMN Selector for I-WLAN access

The "Operator Controlled PLMN Selector for I-WLAN access" file contains a list of PLMN codes preferred by the operator. It shall be possible to store at least ten entries on the list. The contents of this file are specified in 3GPP TS 31.102 [13]. When stored in the ME, the contents may as an implementation option be stored in the PLMN_Realms leaf as specified in 3GPP TS 24.235 [26].

7.6 User Controlled WLAN Specific Identifier list

The "User Controlled WLAN Specific Identifier list" file contains a list of WSIDs related to I-WLAN preferred by the user. It shall be possible to store at least ten entries on the list. The contents of this file are specified in 3GPP TS 31.102 [13].

7.6a Operator Controlled WLAN Specific Identifier list

The "Operator Controlled WLAN Specific Identifier list" file contains a list of WSIDs related to I-WLAN preferred by the operator. It shall be possible to store at least ten entries on the list. The contents of this file are specified in 3GPP TS 31.102 [13]. When stored in the ME, the contents may as an implementation option be stored in the Access_ID leaf as specified in 3GPP TS 24.235 [26].

7.6b Home I-WLAN Specific Identifier List

The "Home I-WLAN Specific Identifier List" file contains a list of WSIDs related to I-WLANs that have a direct relationship with the HPLMN. It shall be possible to store at least ten entries on the list. The contents of this file are specified in 3GPP TS 31.102 [13]. When stored in the ME, the contents of this file may as an implementation option be specified inthe Home_Access_ID leaf as specified in 3GPP TS 24.235 [26].

7.7 Supported PLMNs list for WLAN access

The "Supported PLMNs list for WLAN access" file contains a list of PLMN codes of roaming partners (i.e. to which the WLAN operator has a direct roaming relationship). This list is per WSID and the WLAN UE shall store it for further

use. The list shall be deleted at WLAN UE switch off. The WLAN UE shall structure this list as per the "realm-list" specified in IETF RFC 4284 [12] and each "realm" in the "realm-list" shall be of the form of a home network domain name as defined in subclause 14.2 of 3GPP TS 23.003 [1A].

7.8 Re-authentication identity

The format of the re-authentication identity is specified in 3GPP TS 33.234 [5]. The "deleted" value to indicate no valid re-authentication identity exists in the USIM/ME is specified in 3GPP TS 23.003 [1A].

7.9 I-WLAN Last Registered PLMN

The "I-WLAN Last Registered PLMN" file contains the PLMN that was last successfully registered on via I-WLAN. The contents of this file are specified in 3GPP TS 31.102 [13].

7.10 I-WLAN HPLMN Priority Indication

The "I-WLAN HPLMN Priority Indication" identifies, if supported by the WLAN UE, that the HPLMN is expected to be chosen, if available, when "I-WLAN Last Registered PLMN" file is available in either the USIM or ME. The contents of this file are specified in 3GPP TS 31.102 [13]. When stored in the ME, the contents may as an implementation option be stored in the WLAN_HPLMN_Priority_Indication leaf as specified in 3GPP TS 24.235 [26].

7.11 HPLMN Direct Access Indicator

The "HPLMN Direct Access Indicator" identifies if the WLAN UE may attempt to select the HPLMN via WLANs that support non IEEE 802.1x authentication mechanisms. The "HPLMN Direct Access Indicator" is specified in 3GPP TS 31.102 [13]. When stored in the ME, the contents may as an implementation option be stored in the HPLMN_Direct_Access leaf as specified in 3GPP TS 24.235 [26].

7.12 I-WLAN Equivalent HPLMN Presentation Indication

The "I-WLAN Equivalent HPLMN Presentation Indication" indicates to the WLAN UE if only the highest priority EHPLMN among those that are available is to be presented to the user or all available EHPLMNs are presented to the user in priority order. The contents of this file are specified in 3GPP TS 31.102 [13]. When stored in the ME, the contents may as an implementation option be stored in the I-WLAN_Equivalent_HPLMN_Presentation_Indication leaf as specified in 3GPP TS 24.235 [26].

8 Tunnel management procedures

8.1 General

The purpose of tunnel management procedures is to define the procedures for establishment or disconnection of an end-to-end tunnel between the WLAN UE and the PDG. Tunnel establishment procedure is always initiated by a WLAN UE, whereas Tunnel Disconnection procedure can be initiated by the WLAN UE or network.

Tunnel establishment procedures can be initiated by a WLAN UE without having been previously authenticated for WLAN Direct IP Access. There is no requirement to use the full authentication mechanism for the first tunnel establishment if the WLAN UE is already authenticated for WLAN interworking. However, if the WLAN UE is attempting WLAN 3GPP IP Access without being authenticated earlier, i.e. not having received previously any temporary identity; full authentication mechanism shall be used by the 3GPP network and the WLAN UE (using the IMSI).

The security mechanisms for tunnel setup using IPsec and IKEv2 are specified in 3GPP TS 33.234 [5].

If QoS mechanisms are applied, Diffserv (see IETF RFC 2475 [19]) is used as the QoS mechansim between the WLAN UE and the PDG. Colouring the DS Field, i.e. the IPv4 header TOS octet or the IPv6 Traffic Class octet, is in conformance with the definition given in IETF RFC 2474 [18].

8.2 Tunnel establishment procedures

8.2.1 WLAN UE procedures

8.2.1.1 General

Before initiation of tunnel establishment the WLAN UE shall offer the possibility to the subscriber to select between direct access to external IP network from the WLAN or access through the PLMN. In case the user selects to access through the PLMN, the WLAN UE shall initiate the tunnel establishment procedure after selecting a remote tunnel endpoint using domain name system (DNS) procedure as mentioned in the subclause 8.2.1.2.

The WLAN UE shall support the IKEv2 protocol (see IETF RFC 5996 [14]) for IPsec tunnel negotiation as specified in 3GPP TS 33.234 [5], in order to establish trusted relationships (i.e. mutual authentication with the PDG).

The WLAN UE shall support IPsec ESP (see IETF RFC 4303 [15]) in order to provide secure tunnels between the WLAN UE and the PDG as specified in 3GPP TS 33.234 [5].

The WLAN UE may support authentication to an external AAA server as described in IETF RFC 4739 [16]. In this case, the WLAN UE shall support one of following authentication mechanisms i.e. EAP, PAP or CHAP procedures as described in 3GPP TS 33.234 [5].

8.2.1.2 Selection of remote tunnel endpoint

The WLAN UE shall support the implementation of standard DNS mechanisms in order to retrieve the IP address(es) of the remote tunnel endpoint, i.e. the PDG.

When performing W-APN resolution (i.e. building a fully qualified domain name (FQDN) for the DNS request), the WLAN UE shall include both W-APN network identifier (NI) and W-APN operator identifier (OI). If the user did not provide a value for W-APN OI, then the WLAN UE shall use the HPLMN ID or VPLMN ID as the W-APN OI, depending on internal configuration. The structure of the W-APN is defined in 3GPP TS 23.003 [1A].

NOTE: The W-APN NI identifies the IP network the user wants to access, e.g. operator service network or the Internet. The W-APN OI defines in which PLMN the PDG is located and it is used in WLAN-3GPP IW in order to select a PDG in VPLMN or a PDG in HPLMN. For this reason the W-APN OI usage in the DNS query is mandatory in WLAN-3GPP IW.

The initial selection of the remote tunnel endpoint is done in the WLAN UE. Upon reception of a DNS response containing one or more IP addresses of PDGs that support the requested W-APN, the WLAN UE shall select an IP address with the same IP version as its local IP address. This selection may be performed by the user (WLAN UE implementation option) or may be performed automatically by the WLAN UE. In the later case, the criterion for automatic selection is implementation dependent.

8.2.1.3 WLAN UE initiated tunnel establishment

8.2.1.3.1 WLAN UE initiated tunnel establishment with authentication to the 3GPP AAA server

In order to request the establishment of a tunnel to a certain W-APN, the WLAN UE shall comply with IKEv2 protocol definitions as defined in the IKEv2 protocol (IETF RFC 5996 [14]). In order to set up an IKE connection between the WLAN UE and the PDG, the WLAN UE shall initiate the signalling procedure by sending the IKE_SA_INIT request message defined in IETF RFC 5996 [14] to the PDG. On receipt of an IKE_SA_INIT response, the WLAN UE shall send a tunnel establishment request (IKE_AUTH request message defined in IETF RFC 5996 [14]) to the selected PDG (see subclause 8.2.1.2) including the W-APN and the NAI. The WLAN UE shall include in IDr payload the W-APN that was used in the DNS query and in the IDi payload the NAI.

NOTE 1: The username part of the NAI included in IDi payload may be an IMSI, pseudonym or re-authentication ID.

NOTE 2: Fast re-authentication mechanism is optional, and therefore is an implementation option in the WLAN UE and operator configuration issue (i.e. it also depends on whether the AAA server sent an re-authentication ID during previous EAP authentication) whether to use it during tunnel establishment.

Upon receipt of a response message with Notify payload of type "ERROR" i.e. indicating the failure of the tunnel establishment the WLAN UE may either:

- select a new PDG from the list received from the DNS server during remote tunnel endpoint selection (see subclause 8.2.1.2) and initiate a new tunnel establishment using this newly selected PDG; or
- perform a new remote tunnel endpoint selection requesting PDG IP addresses from HPLMN, select a new PDG from the list received from the DNS server (see subclause 8.2.1.2) and initiate a new tunnel establishment using this newly selected PDG; or
- stop the tunnel establishment attempt and release the security association (SA) with the PDG.

8.2.1.3.2 WLAN UE initiated tunnel establishment with additional authentication to an external AAA server

When the WLAN UE needs authentication to an external AAA server for WLAN 3GPP IP Access at a particular W-APN, the WLAN UE shall perform the actions as specified in subclause 8.2.1.3.1 with the following additions:

On receipt of an IKE_SA_INIT response from the PDG containing a Notify payload of type "MULTIPLE_AUTH_SUPPORTED", the WLAN UE shall include a "MULTIPLE_AUTH_SUPPORTED" Notify payload in the IKE_AUTH request as described in IETF RFC 4739 [16]. If the IKE_SA_INIT response from the PDG does not contain a Notify payload of type "MULTIPLE_AUTH_SUPPORTED", the WLAN UE shall use the procedures defined in subclause 8.3.1 to disconnect the tunnel. After that, the WLAN UE then may either:

- select a new PDG from the list received from the DNS server during remote tunnel endpoint selection (see subclause 8.2.1.2) and initiate a new tunnel establishment using this newly selected PDG; or
- perform a new remote tunnel endpoint selection requesting PDG IP addresses from HPLMN, select a new PDG from the list received from the DNS server (see subclause 8.2.1.2) and initiate a new tunnel establishment using this newly selected PDG; or
- perform an implementation specific action.

After successful EAP SIM or EAP AKA based authentication, the WLAN UE shall send an IKE_AUTH request with Authentication (AUTH) payload, and Notify payload of type "ANOTHER_AUTH_FOLLOWS".

Upon subsequent receipt of an IKE_AUTH response with AUTH payload only, the WLAN UE shall send an IKE_AUTH request to the PDG containing the user identity in the private network in the IDi payload encoded in UTF-8 format as described in IETF RFC 3629 [17]. The WLAN UE then takes the following actions, depending on the type of EAP request received from the PDG within the IKE_AUTH response and the credentials the WLAN UE has stored for the particular W-APN:

- If the WLAN UE receives an EAP-GTC request and the WLAN UE has PAP credentials, then the WLAN UE shall send EAP-GTC response to the PDG containing the user"s PAP password encoded in ASCII.
- If the WLAN UE receives an EAP-MD-5 request, and the WLAN UE has CHAP credentials, then the WLAN UE shall send an EAP MD5-Challenge response to the PDG
- If the WLAN UE receives a different EAP authentication type request for which the WLAN UE has credentials, then the WLAN UE shall send EAP response to the PDG.
- If the WLAN UE receives a different EAP authentication type request, which the WLAN UE does not support, then the WLAN UE shall send EAP-Legacy-Nak response to the PDG containing authentication types supported by the WLAN UE.

NOTE 1: The authentication and authorization to an external AAA server for WLAN 3GPP IP Access signalling flows are described in 3GPP TS 33.234 [5].

8.2.1.4 Void

8.2.1.5 Void

8.2.1.6 In place rekeying of existing security association

The WLAN UE may use the CREATE_CHILD_SA procedure as described in IETF RFC 5996 [14] to rekey existing IKE and IPsec security association(s).

In order to rekey an existing IPsec ESP security association, the security association (SA) payload is to type "ESP" and a Notify payload of type "REKEY_SA" is included in the CREATE_CHILD_SA request message.

In order to rekey the IKE security association, the SA payload is set to type "IKE" in the CREATE_CHILD_SA request message.

8.2.1.7 Additional tunnel establishment

The WLAN UE may use the CREATE_CHILD_SA procedure as described in IETF RFC 5996 [14] to establish additional tunnels inside an already established IKE security association:

In order to establish an additional IPsec ESP security association (I-WLAN tunnel), the WLAN UE shall set the SA payload to type "ESP".

If the WLAN UE receives a CREATE_CHILD_SA response message from the PDG with a Notify payload of type "NO_ADDITIONAL_SAS", this indicates that the WLAN UE already has the maximum number of IPsec ESP SAs allowed at that PDG per IKE security association. The WLAN UE shall not attempt to setup IPsec ESP security association to this PDG in excess of this number. All other error cases are treated according to IETF RFC 5996 [14].

8.2.1.8 WLAN UE procedures for the emergency case

In the case where IMS emergency calls will be established over the I-WLAN tunnel the requirements as specified in subclauses 8.2.1.1 shall apply with the exception of additional authentications to an external AAA server.

Additionally, when IMS emergency calls are established over the I-WLAN tunnel two different cases can be identified:

a) The WLAN UE is equipped with a valid SIM or valid USIM: The procedures as desribed in subclauses 8.2.1.2 and 8.2.1.3.1, 8.2.1.6 and 8.2.1.7 shall apply with the following additions:

For the purpose of making an IMS emergency call, the WLAN UE may reuse an existing I-WLAN tunnel only if the WLAN UE is not roaming (i.e. not accessing via a VPLMN).

NOTE 1: In case PDG and P-CSCF are in different countries, a notification will be sent back to the WLAN UE that the emergency IMS registration is required and therefore WLAN UE cannot reuse existing I-WLAN tunnel for an emergency call.

NOTE 2: When WLAN UE selects W-APN at tunnel set up the W-APN operator identifier (OI) contains either the HPLMN ID or the VPLMN ID.

If no suitable I-WLAN tunnel is available, then WLAN UE shall initiate the tunnel establishment as described in subclause 8.2.1.3.1. The WLAN UE shall build the W-APN for the support of IMS emergency calls as described in 3GPP TS 23.003 [1A]. For the non roaming case (i.e. WLAN UE has direct connectivity to HPLMN), the WLAN UE shall construct the W-APN with the W-APN OI corresponding to the HPLMN. In the roaming case (i.e. WLAN UE has connectivity to the HPLMN via a VPLMN), the WLAN UE shall build the W-APN with the W-APN OI corresponding to the VPLMN.

b) The WLAN UE is not equipped with a valid SIM or valid USIM: The procedure as described in subclause 8.2.1.2, 8.2.1.6 and 8.1.2.1.7 shall apply with the following modification:

The WLAN UE shall initiate the tunnel establishment as described in subclause 8.2.1.3.1 with the following modifications:

The WLAN UE shall indicate the desire of using EAP over IKEv2 by including an IDi payload but not an AUTH payload in the first IKE_AUTH request message (see IETF RFC 5996 [14]). On building the NAI to be included in the IKE_AUTH request message, the WLAN UE shall include an emergency NAI;

The WLAN UE shall build the W-APN for the support of IMS emergency calls as described in 3GPP TS 23.003 [1A] where the W-APN OI is constructed from a selected PLMN (subclause 5.2.5.4), and include it in the IDr payload of the first IKE_AUTH request message;

After successful EAP authentication, the WLAN UE shall send an IKE_AUTH request message with the AUTH payload which is generated by using the master session key (MSK) created by EAP authentication as described in IETF RFC 5996 [14]. If the WLAN UE needs to obtain a dynamically allocated remote IP address, the WLAN UE shall also send a Configuration (CP) payload of type "CFG_REQUEST" in the IKE_AUTH request message further details are described in IETF RFC 5996 [14].

8.2.1.9 QoS provisioning support

If QoS mechanisms are applied and based on the QoS required for the service, the WLAN UE shall use Diffserv and mark the DS field in the external IP header of a tunnel for uplink data stream.

On each IKEv2 Child-SA, the WLAN UE shall only send out packets belonging to a single QoS class. Thus multiple IKEv2 Child-SAs shall be established to carry packets belonging to services with different QoS levels.

The WLAN UE shall map the 3GPP traffic classes (see 3GPP TS 23.107 [20]) into DS codepoint (DSCP) codes following the GSMA specification GSMA PRD IR.34 [21].

8.2.2 PDG procedures

8.2.2.1 General

The PDG shall support the implementation of a VPN server application in order to assist tunnel establishment towards the WLAN UE. However, the selection of a particular VPN application is implementation dependent.

The PDG shall support IPsec tunnelling using the IKEv2 protocol (see IETF RFC 5996 [14]), in order to establish trusted relationships (i.e. mutual authentication with the WLAN UE).

The PDG shall support IPsec ESP (see IETF RFC 4303 [15]) in order to provide secure tunnels between the WLAN UE and the PDG as specified in 3GPP TS 33.234 [5].

If the PDG supports a W-APN for which authentication to an external AAA server is required, the PDG shall support the capability for multiple authentications as described in IETF RFC 4739 [16].

The PDG shall support in place rekeying of security association as described in IETF RFC 5996 [14]. The support for multiple IPsec ESP security associations (I-WLAN tunnels) per IKE connection is dependent on operator configuration at the PDG. The PDG shall support an operator configurable parameter for the maximum number of tunnels per IKE security association and a per user count for the number of tunnels such that it is possible for the operator to configure a limit for the number of IPsec ESP security association (I-WLAN tunnels) per IKE security association.

8.2.2.2 WLAN UE initiated tunnel establishment

8.2.2.2.1 WLAN UE initiated tunnel establishment with authentication to the 3GPP AAA server

Upon receipt of an IKE_AUTH request message (tunnel establishment request) from the WLAN UE, the PDG shall contact the 3GPP AAA server as specified in 3GPP TS 29.234 [3] in order to retrieve service authorization and authentication information for the WLAN UE requesting the establishment of the tunnel.

Upon successful authorization and authentication, the PDG shall accept the tunnel establishment request by sending the IKE_AUTH response message and including the allocated remote IP address in the Configuration (CP) payload. The PDG shall increment its maintained count of the number of tunnels for that user

Upon authentication failure, the PDG shall reject the tunnel establishment request by sending the IKE_AUTH response message with the Notify payload of type "AUTHENTICATION FAILED".

8.2.2.2.2 WLAN UE initiated tunnel establishment with additional authentication to an external AAA server

When the PDG supports authentication to an external AAA server for WLAN 3GPP IP Access at a particular W-APN, the PDG shall perform the actions as specified in subclause 8.2.2.2.1 with the following additions.

On receipt of an IKE_SA_INIT message, the PDG shall include Notify payload of type "MULTIPLE_AUTH_SUPPORTED" in the IKE_SA_INIT response message.

On successful completion of EAP-SIM or EAP-AKA and on receipt of an IKE_AUTH request containing a Notify payload of type "ANOTHER_AUTH_FOLLOWS", the PDG shall send an IKE_AUTH response containing the AUTH payload.

Upon receipt of a subsequent IKE_AUTH request from the WLAN UE containing the user identity in the private network within the IDi payload, the PDG shall take the following actions depending on the the type of authentication required by the external AAA server:

- if EAP authentication is required, the PDG shall send an EAP request to the WLAN UE within an IKE_AUTH response message. Upon receipt of an EAP response, the PDG shall use the procedures defined on the Wi interface (see 3GPP TS 29.161 [3A]) to authenticate the user to the external AAA server.

- if PAP procedure is required, the PDG shall send an EAP-GTC request to the WLAN UE. Upon receipt of an EAP-GTC response within an IKE_AUTH request message from the WLAN UE, the PDG shall use the procedures defined on the Wi interface (see 3GPP TS 29.161 [3A]) to authenticate the user to the external AAA server. If the PDG receives EAP-Legacy-Nak response from the WLAN UE containing EAP–MD5 type, the PDG may, if the specified W-APN allows, change the authentication and authorization procedure to CHAP. If the specified W-APN does not allow CHAP procedures or the PDG receives EAP-Legacy-Nak response not containing EAP-MD5, the PDG shall send an EAP-Failure to the WLAN UE.

- if CHAP procedure is required, the PDG shall send an MD5-Challenge request to WLAN UE. Upon receipt of MD5-Challenge response within an IKE_AUTH request message from the WLAN UE, the PDG shall use the procedures defined on the Wi interface (see 3GPP TS 29.161 [3A]) to authenticate the user to the external AAA server. If the PDG receives EAP-Legacy-Nak response containing EAP–GTC type from the WLAN UE, the PDG may, if the specified W-APN allows, change the authentication and authorization procedure to PAP. If the specified W-APN does not allow PAP procedures or the PDG receives EAP-Legacy-Nak response not containing EAP-GTC, the PDG shall send an EAP-Failure to the WLAN UE.

NOTE 1: The authentication and authorization to an external AAA server for WLAN 3GPP IP Access signalling flows are described in 3GPP TS 33.234 [5].

8.2.2.3 Void

8.2.2.4 Void

8.2.2.5 Additional tunnel establishment and in place rekeying

Every active IKE security association shall be associated with a counter maintained by the PDG. The counter is used to indicate the number of IPsec ESP security associations (I-WLAN tunnels) inside an already established IKE security association.

On receipt of a CREATE_CHILD_SA request from the WLAN_UE, the PDG shall check:

If the SA payload is of type ESP and the message contains a Notify payload of type "REKEY_SA", the WLAN UE is attempting to rekey an existing IPsec security association (I-WLAN tunnel). The PDG shall use the procedures defined in IETF RFC 5996 [14] to setup the new IPsec ESP security association (I-WLAN tunnel) and shall subsequently delete the old IPsec ESP security association (I-WLAN tunnel) after successful completion of the procedure.

If the SA payload is of type ESP and the message does not contain a "REKEY_SA" Notify payload, then the WLAN UE is attempting to establish an additional IPsec ESP security association (I-WLAN tunnel). The PDG shall check:

If the number of IPsec ESP security associations (I-WLAN tunnels) inside the IKE security assocation is less than the configured maximum number of IPsec ESP security associations (I-WLAN tunnels) per IKE security assocation, then the PDG shall proceed to set up the additional IPsec ESP security association (I-WLAN tunnel) as defined in IETF RFC 5996 [14] and shall respond with the CREATE_CHILD_SA response message. The PDG shall increment its maintained count of the number of IPsec ESP security associations (I-WLAN tunnels) for that IKE security association.

If the count of the number of IPsec ESP security associations (I-WLAN tunnels) inside the IKE security assocation is greater than or equal to the configured maximum number of tunnels per IKE security assocation, the PDG shall reject the establishment request by replying with a CREATE_CHILD_SA reponse message with a Notify payload of type "NO_ADDITIONAL_SAS".

If the SA payload is of type IKE, then the user is attempting to rekey the existing IKE security association. The PDG shall use the procedures defined in IETF RFC 5996 [14] to setup the new IKE security association and shall subsequently delete the old IKE security association on successful completion of the procedure.

8.2.2.6 PDG procedures in the emergency case

In the case where WLAN UE is attempting to set up an I-WLAN tunnel to the W-APN for the support of IMS emergency calls the requirements as specified in subclauses 8.2.1.1 shall apply with the exception of additional authentications to an external AAA server.

Additionally, when WLAN UE is attempting to set up an I-WLAN tunnel to the W-APN for the support of IMS emergency calls two different cases can be identified:

a) The WLAN UE is equipped with a valid SIM or valid USIM: The procedures as described in subclauses 8.2.2.1, 8.2.2.2 and 8.2.2.5 shall apply with the following addition:

   On receipt of an IKE_AUTH request message (tunnel establishment request) from the WLAN UE, with IDr payload set to the W-APN for the support of IMS emergency calls (see 3GPP TS 23.003 [1A]), the PDG behaviour is specified in 3GPP TS 29.234 [3].

b) The WLAN UE is not equipped with a valid SIM or valid USIM: The procedures as described in subclauses 8.2.2.2.1 and 8.2.2.5 shall apply with the following modifications:

   If there is an already established IKE security association for the WLAN UE, then the PDG shall reject the tunnel establishment request by sending the IKE_AUTH response message with the Notify payload attributes as defined in annex B.

   The PDG shall use the MSK created by EAP authentication to check the AUTH payload provided by the WLAN UE. Further PDG behavior is specified in 3GPP TS 29.234 [3].

NOTE: The format of the NAI and the W-APN information received in the first IKE_AUTH request message indicates whether the WLAN UE is using I-WLAN as the access network for IMS emergency calls and whether the WLAN UE is accessing with IMSI or not as described in 3GPP TS 23.003 [1A], and 3GPP TS 29.234 [3].

8.2.2.7 QoS provisioning support

If QoS mechanisms are applied, the PDG will operate as a QoS Edge Function (see IETF RFC 2475 [19]) between a 3GPP - WLAN Interworking system and external networks. When applying receiver control DiffServ edge functions the authorized 3GPP WLAN QoS profile (as received from the 3GPP AAA Server) shall be enforced according to operator policies. This may result in re-classification (re-marking the DSCP) or discarding of IP packets.

The PDG shall map the 3GPP traffic classes (see 3GPP TS 23.107 [20]) into DSCP codes following the GSMA specification GSMA PRD IR.34 [21].

8.3 Tunnel disconnection procedures

8.3.1 WLAN UE procedures

8.3.1.1 General

WLAN UE shall use the procedures defined in the IKEv2 protocol (see IETF RFC 5996 [14]) to disconnect an IPsec tunnel to the PDG. The WLAN UE shall close the incoming security associations associated with the tunnel and instruct the PDG to do the same by sending the INFORMATIONAL request message including a Delete payload. The Delete payload shall contain either:

i) Protocol ID set to "1" and no subsequent security parameters indexes (SPIs) in the payload. This indicates closing of IKE security association, and implies the deletion of all IPsec ESP security associations that were negotiated within the IKE security association; or

ii) Protocol ID set to "3" for ESP. The SPIs included in the payload shall correspond to the particular incoming ESP security associations at the WLAN UE for the given tunnel in question.

NOTE: More than one tunnel may be disconnected in this message, via inclusion of multiple SPIs in one Delete payload or multiple Delete payloads in one INFORMATIONAL request message.

8.3.1.2 PDG initiated tunnel disconnection procedures

On receipt of the INFORMATIONAL request message including Delete payload, indicating that the PDG is attempting tunnel disconnection, the WLAN UE shall:

i) Close all security associations identified within the Delete payload (these security associations correspond to outgoing security associations from the WLAN UE perspective). If no security associations were present in the Delete payload, and the protocol ID was set to "1", the WLAN UE shall close the IKE security association, and all IPsec ESP security associations that were negotiated within it towards the PDG.

ii) The WLAN UE shall delete the incoming security associations corresponding to the outgoing security associations identified in the Delete payload.

The WLAN UE shall send an INFORMATIONAL response message. If the INFORMATIONAL request message contained a list of security associations, the INFORMATIONAL response message shall contain a list of security associations deleted in step (ii) above.

If the WLAN UE is unable to comply with the INFORMATIONAL request message, the WLAN UE shall send INFORMATION response message with either:

i) A Notify payload of type "INVALID_SPI", for the case that it could not identify one or more of the Security Parameters Indexes in the message from the PDG; or

ii) A more general Notify payload type. This payload type is implementation dependent.

8.3.1.3 WLAN UE procedures for emergency cases

When connected to the emergency W-APN for the purpose of making IMS emergency calls, the WLAN UE shall not tear down the tunnel until the IKE and ESP security association timers have expired. This is in order to allow call back from the PSAP.

8.3.2 PDG procedures

8.3.2.1 General

PDG shall use the procedures defined in the IKEv2 protocol (see IETF RFC 5996 [14]) to disconnect an IPsec tunnel to the WLAN UE. The PDG shall close the incoming security associations associated with the tunnel and instruct the WLAN UE to do likewise by sending the INFORMATIONAL request message including a Delete payload. The Delete payload shall contain either:

i) Protocol ID set to "1" and no subsequent SPIs in the payload. This indicates that the IKE security association, and all IPsec ESP security associations that were negotiated within it between PDG and WLAN UE shall be deleted; or

ii) Protocol ID set to "3" for ESP. The SPIs included in the payload shall correspond to the particular incoming ESP SECURITY ASSOCIATION at the WLAN UE for the given tunnel in question.

8.3.2.2 WLAN UE initiated tunnel disconnection procedures

On receipt of the INFORMATIONAL request message including Delete payload indicating that the WLAN UE is initiating tunnel disconnect procedure, the PDG shall:

i) Close all security associations identified within the Delete payload (these security associations correspond to outgoing security associations from the PDG perspective). If no security associations were present in the Delete payload, and the protocol ID was set to "1", the PDG shall close the IKE security association, and all IPsec ESP security associations that were negotiated within it towards the WLAN UE.

ii) The PDG shall delete the incoming security associations corresponding to the outgoing security associations identified in the Delete payload.

The PDG shall send an INFORMATIONAL response message. This shall contain a list of security associations deleted in step (ii) above.

If the PDG is unable to comply with the INFORMATIONAL request message, the PDG shall send INFORMATION response message with either:

i) a Notify payload of type "INVALID_SPI", for the case that it could not identify one or more of the SECURITY PARAMETERS INDEXES in the message from the WLAN UE; or

ii) a more general Notify payload type. This payload type is implementation dependent.

8.3.2.3 PDG procedures in the emergency case

Where the WLAN UE has a tunnel to the emergency W-APN, the PDG shall not use tunnel disconnect procedures to tear down the tunnel until the IKE and ESP security association timers have expired.

8.4 Timers and counters for tunnel management

Timers are used as defined in IETF RFC 5996 [14].

It is recommended that IKE security association and ESP security association timers are set to be of the order of 3 (three) hours and that rekeying triggers the WLAN UE-3GPP AAA server reauthentication procedure. In this way, the WLAN UE-PDG re-authentication, IKE security association and IPsec ESP security association timers are simultaneously reset.

8.5 Void

Annex A (normative): Definition of Generic Container

A.1 General

The definition of the generic container used as the payload in the 3GPP Cellular Network ANQP-element, specified in IEEE Std 802.11u-2011 [23], is provided in 3GPP TS 24.302 [28].

A.2 Void

A.3 Void

Annex B (normative): IKEv2 Notify payload attributes

B.1 General

The WLAN UE not equipped with a valid SIM or valid USIM can attempt to set up an I-WLAN tunnel to the W-APN for the support of IMS emergency calls by sending an IKE_AUTH request message. If there is an already established IKE security association for the WLAN UE, then the PDG shall reject the tunnel establishment request by sending the IKE_AUTH response message (see IETF RFC 5996 [14]) with the Notify payload of type "UNABLE_TO_COMPLY".

The attribute type indicating "UNABLE_TO_COMPLY" is of the value 8193.

Annex C (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
22.09.03	*CN1#31*				First draft. TS number assigned by MCC. *Incorporates agreements from the following Tdocs: N1-031104, N1-031305, N1-031306, N1-031308, N1-031309 and N1-031310.*		*0.1.0*
12.11.03	*CN1#32*	*24.234*			*Second draft.* *TS sent to plenary for information.* *Incorporates agreements from the following Tdocs: N1-031536, N1-031685, N1-031686, N1-031691, N1-031692, N1-031693, N1-031694, N1-031695, N1-031696*	*0.1.0*	*0.2.0*
01.02.04	*CN1#32-bis*				*Incorporates agreements from the following Tdocs: N1-040191, N1-040192, N1-040193, N1-040194, N1-040195, N1-040048.*	*1.0.0*	*1.1.0*
24.02.04	CN1#33				*Incorporates agreements from the following Tdocs: N1-040447, N1-040448, N1-040452, N1-040477, N1-040489, N1-040490, N1-040491, N1-040492.*	1.1.0	1.2.0
23.04.04	CN1#33-bis				Incorporates agreements from the following Tdocs: N1-040640,N1-040703,N1-040707,N1-040708,N1-040710,N1-040712,N1-040713,N1-040718,N1-040724,N1-040725,N1-040726,N1-040742,N1-040743,N1-040744,N1-040745,N1-040746,N1-040748,N1-040749	1.2.0	1.3.0
24.05.04	CN1#34				Incorporates agreements from the following Tdocs: N1-040929, N1-040930, N1-041018, N1-041043, N1-041044, N1-041046, N1-041048, N1-041049, N1-041051		
25.05.04	CN1#34				Correction to 041044	1.4.0	1.4.1
2.07.04	CN1#34bis				Incorporates agreed CRs N1-041178, N1-041191, N1-041197, N1-041221, N1-041242, N1-041246, N1-041247, N1-041287, N1-041298, N1-041299, N1-041309	1.4.1	1.5.0
25.08.04	CN1 #35				Incorporates agreed CRs N1-041556, N1-041557, N1-041560, N1-041637, N1-041466	1.5.0	1.6.0
09-2004					Version 2.0.0 created for Plenary approval, editorial changes done	1.6.0	2.0.0
09-2004	CN#25	NP-040365			The draft was approved and TS 23.234 was formally brought under the change control; v6.0.0 is created.	2.0.0	6.0.0
12-2004	CN#26	NP-040508	001	1	Alignment of the WLAN identities" lists	6.0.0	6.1.0
12-2004	CN#26	NP-040508	002	1	I-WLAN Parameters coding –Pseudonym and re-authentication identity	6.0.0	6.1.0
12-2004	CN#26	NP-040508	003	2	References clean-up	6.0.0	6.1.0
12-2004	CN#26	NP-040508	004	1	Introduction of protected result indications	6.0.0	6.1.0
12-2004	CN#26	NP-040508	006		Removal of the PDG Redirection feature	6.0.0	6.1.0
12-2004	CN#26	NP-040508	008	1	Restructuring of clause 5	6.0.0	6.1.0
12-2004	CN#26	NP-040508	009	1	Cleaning of Editors Notes	6.0.0	6.1.0
12-2004	CN#26	NP-040508	011	2	Timers in Scenario 3	6.0.0	6.1.0
12-2004	CN#26	NP-040508	014	1	Editorial change to chapter 8	6.0.0	6.1.0
01-2005					Fix Word problem	6.1.0	6.1.1
03-2005	CN#27	NP-050080	017	3	On 3GPP IP access independence	6.1.1	6.2.0
03-2005	CN#27	NP-050079	019	1	PLMN selection for WLAN	6.1.1	6.2.0
03-2005	CN#27	NP-050115	020	3	Fallback to full authentication	6.1.1	6.2.0
03-2005	CN#27	NP-050079	021	1	Correction of Abbreviation Usage	6.1.1	6.2.0
06-2005	CP-28	CP-050064	022	1	Clarifications to network discovery & selection to enable successful inter-operator AAA	6.2.0	6.3.0
06-2005	CP-28	CP-050065	023	1	Pointer to new W-APN definition in 24.234	6.2.0	6.3.0
06-2005	CP-28	CP-050064	024	1	Revision of definitions	6.2.0	6.3.0
06-2005	CP-28	CP-050064	025	1	Limiting of IP sec SA per IKE SA in scenario 3	6.2.0	6.3.0
09-2005	CP-29	CP-050358	026	2	Modifications to 24.234 to allow multiple IPSec SA per IKE_SA	6.3.0	6.4.0
12-2005	CP-30				Version 7.0.0 created by MCC due to TISPAN references	6.4.0	7.0.0
12-2005	CP-30	CP-050541	028		Removal of RFC 2486 reference	6.4.0	7.0.0
12-2005	CP-30	CP-050541	029	1	Correction of TS 24.234	6.4.0	7.0.0
03-2005	CP-31	CP-060112	032	1	Corrections to the counter used for additional tunnel establishment	7.0.0	7.1.0
03-2005	CP-31	CP-060112	034	-	IETF References Update	7.0.0	7.1.0
06-2006	CP-32	CP-060277	035	4	Additional text for I-WLAN Private Network Access	7.1.0	7.2.0
09-2006	CP-33	CP-060458	037		Removal of Editor's notes in 24.234	7.2.0	7.3.0
11-2006	CP-34	CP-060659	038	3	Addition of basic Emergency call related requirements to 24.234	7.3.0	7.4.0
11-2006	CP-34	CP-060659	039	1	Addition of emergency call related tunnel management procedures to 24.234	7.3.0	7.4.0
11-2006	CP-34	CP-060670	040	1	Correction of temporary identity mapping	7.3.0	7.4.0
11-2006	CP-34	CP-060671	041	2	Diffserv support between WLAN UE and PDG	7.3.0	7.4.0
03-2007	CP-35	CP-070146	0042		References update	7.4.0	7.5.0

03-2007	CP-35	CP-070134	0043	1	Correction of UE behavior on emergency call related tunnel management procedur	7.4.0	7.5.0
03-2007	CP-35	CP-070134	0044	1	Clean up of Emergency network selection	7.4.0	7.5.0
06-2008	CP-40	CP-080340	0051		Removal of Editor"s notes in 24.234	7.5.0	7.6.0
06-2008	CP-40	CP-080358	0047	2	Requirement for presentation of additional information in manual mode	7.6.0	8.0.0
06-2008	CP-40	CP-080358	0050	2	Steering of Roaming for PLMNs connected by I-WLAN.	7.6.0	8.0.0
06-2008	CP-40	CP-080358	0052		Incorporate RPLMN and EHPLMN functionality	7.6.0	8.0.0
06-2008	CP-40	CP-080361	0045	2	Network Selection Clarification	7.6.0	8.0.0
06-2008	CP-40	CP-080361	0046	1	Editorial clean up Emergency network selection.	7.6.0	8.0.0
09-2008	CP-41	CP-080530	0054		Implementation error of CR 0052	8.0.0	8.1.0
09-2008	CP-41	CP-080530	0055	1	Network selection mode at switch-on	8.0.0	8.1.0
09-2008	CP-41	CP-080530	0056	1	SSID support connectivity to HPLMN	8.0.0	8.1.0
09-2008	CP-41	CP-080536	0057	3	Incorporation 802.11u network discovery procedures	8.0.0	8.1.0
12-2008	CP-42	CP-080873	0058	1	802.11u clean up	8.1.0	8.2.0
12-2008	CP-42	CP-080850	0059	2	Clean up Network discovery	8.1.0	8.2.0
12-2008	CP-42	CP-080850	0060		Correction of misimplementation of previous CR's	8.1.0	8.2.0
12-2008	CP-42	CP-080850	0061	1	Read all WLAN files from USIM	8.1.0	8.2.0
12-2008	CP-42	CP-080976	0063	4	Correction to use of I-WLAN selection USIM data files	8.1.0	8.2.0
12-2008	CP-42				Editorial cleanup by MCC	8.1.0	8.2.0
09-2009	CP-45	CP-090655	0064	4	Provision of "Home WLAN Specific Identifier List" via ANDSF MO	8.2.0	8.3.0
09-2009	CP-45	CP-090679	0065	2	Corrections to PLMN selection	8.2.0	8.3.0
12-2009	CP-46				Upgrade to Rel-9	8.3.0	9.0.0
09-2010	CP-49	CP-100490	0069	1	11u Reference Update	9.0.0	9.1.0
12-2010	CP-50	CP-100741	0071	2	Alignment with new 802.11u terminologies and functionality	9.1.0	9.2.0
12-2010	CP-50	CP-100741	0072	2	Alignment with new 802.11u terminologies and functionality	9.2.0	10.0.0
03-2011	CP-51	CP-110202	0073	3	Formal definition of WLAN ME files	10.0.0	10.1.0
03-2011	CP-51	CP-110167	0076	1	Missing Automatic Network Selection HPLMN Functionality	10.0.0	10.1.0
03-2011	CP-51	CP-110197	0078	1	Support for ANDSF ISRP	10.0.0	10.1.0
06-2011	CP-52	CP-110464	0080		Reverting the implementation of non-approved CR0078R1	10.1.0	10.2.0
09-2011	CP-53	CP-110675	0083	4	Management Object interactions	10.2.0	10.3.0
09-2011	CP-53	CP-110668	0095	1	Clarification of ANDSF file to use	10.2.0	10.3.0
09-2011	CP-53	CP-110675	0105	2	Using files in ME.	10.2.0	10.3.0
09-2011	CP-53	CP-110709	0091	2	Correction to the IEEE 802.11u™ reference	10.3.0	11.0.0
09-2011	CP-53	CP-110738	0092	2	Correction to references	10.3.0	11.0.0
09-2011	CP-53	CP-110739	0093	2	Clarifications and editorials	10.3.0	11.0.0
09-2011	CP-53	CP-110694	0096	1	Network selection clarifications	10.3.0	11.0.0
09-2011	CP-53	CP-110695	0104	1	802.11 reference updates	10.3.0	11.0.0
12-2011	CP-54	CP-110882	0106	1	Correction to radio access technology supported by a WLAN UE	11.0.0	11.1.0
12-2011	CP-54	CP-110877	0107	1	IMS emergency calls for the case of WLAN UE equipped with neither a valid SIM nor a valid USIM	11.0.0	11.1.0
12-2011	CP-54	CP-110882	0108	1	Network selection for emergency calls	11.0.0	11.1.0
03-2012	CP-55	CP-120125	0109	1	"HPLMN Direct Access Indicator" and 802.1x usage	11.1.0	11.2.0
06-2012	CP-56	CP-120309	0110	1	NAI used for authentication	11.2.0	11.3.0
06-2012	CP-56	CP-120309	0111	2	Correction on network selection procedure	11.2.0	11.3.0
06-2014	CP-64	CP-140303	0113	4	Deletion of reference to ANDSF MO	11.3.0	11.4.0
09-2014	CP-65	CP-140672	0115	4	Reference to generic container in 24.302	11.4.0	12.0.0
12-2014	CP-66	CP-140836	0120	3	I-WLAN feature maintenance	12.0.0	12.1.0
12-2014	CP-66	CP-140836	0122	2	Correction of reference	12.0.0	12.1.0

History

Document history		
V12.0.0	October 2014	Publication
V12.1.0	January 2015	Publication