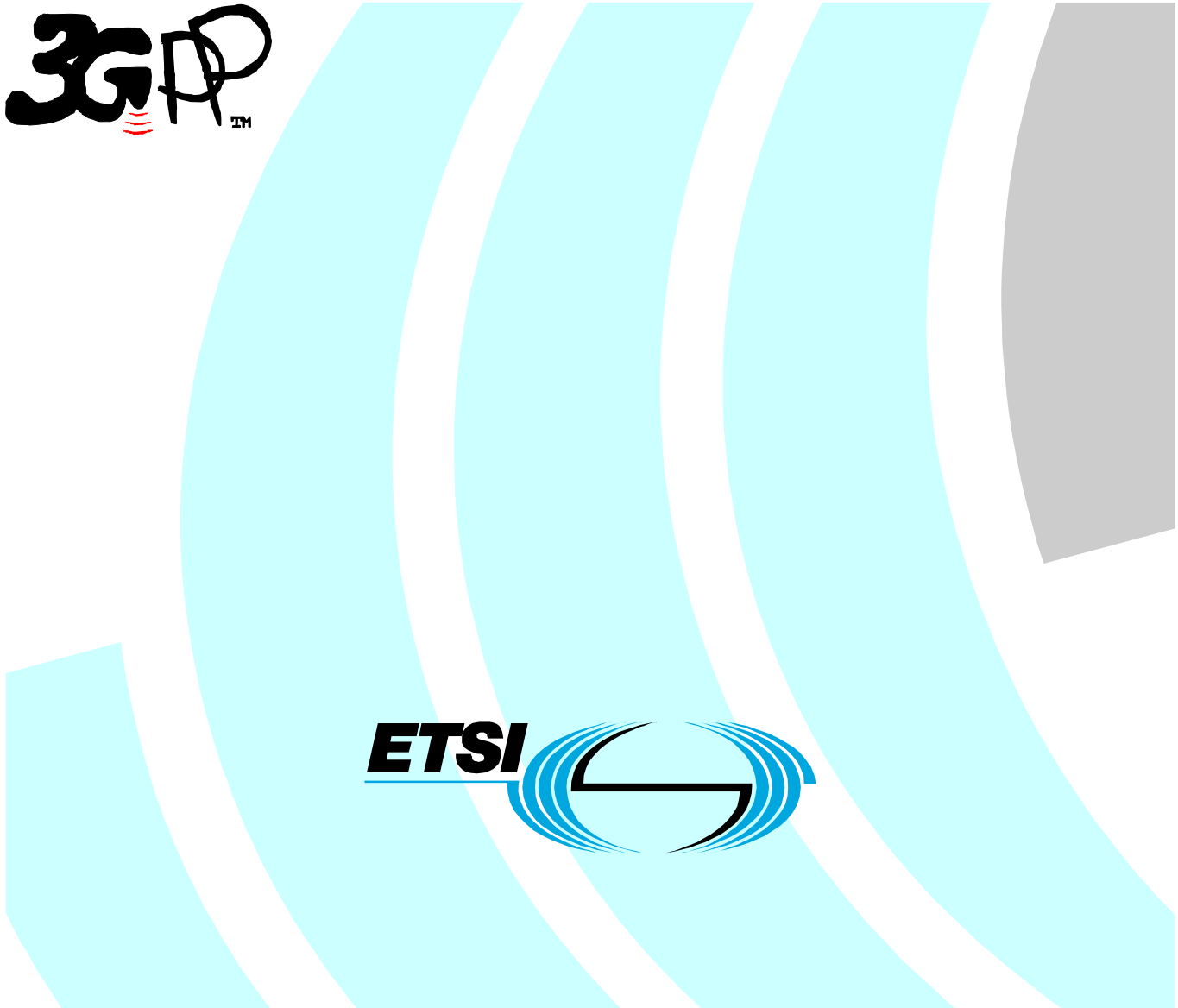
ETSI TS 124 234 V6.4.0 (2005-09)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
3GPP system to Wireless Local Area Network (WLAN) interworking;
User Equipment (UE) to network protocols;
Stage 3
(3GPP TS 24.234 version 6.4.0 Release 6)



Reference
RTS/TSGC-0124234v640

Keywords
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://webapp.etsi.org/IPR/home.asp).

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 .

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.

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".

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

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

[4] Void

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

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

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

[8] IETF RFC 2486 (January 1999): "The Network Access Identifier".

[9] draft-arkko-pppext-eap-aka-13 (October 2004): " Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP AKA)".

[10] draft-haverinen-pppext-eap-sim-14 (October 2004): "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)".

[11] IEEE Std 802.11 (1999): "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] draft-adrangi-eap-network-discovery-05 (October 2004): " Identity selection hints for Extensible Authentication Protocol (EAP)".

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

[14] draft-ietf-ipsec-ikev2-17.txt (October 2004): "Internet Key Exchange (IKEv2) Protocol".

[15] draft-ietf-ipsec-esp-v3-09.txt, (September 2004): "IP Encapsulating Security Payload (ESP)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

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 draft-arkko-pppext-eap-aka [9]).

EAP SIM: EAP mechanism for authentication and session key distribution using the GSM Subscriber Identity Module (SIM) (see draft-haverinen-pppext-eap-sim [10]).

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 clause 5.1, either manually or automatically.

selected PLMN: this is the PLMN that has been selected according to clause 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 Roaming

For the purposes of the present document, the following terms and definitions given in draft-adrangi-eap-network-discovery [12] apply:

Decorated NAI
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
APN	Access Point Name
DNS	Domain Name System
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
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.

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 draft-adrangi-eap-network-discovery [12] and 3GPP TS 23.234 [2]). The Root NAI format is specified in 3GPP TS 23.003 [1A]. 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 draft-adrangi-eap-network-discovery-and-selection-00 [12]). The Decorated NAI format is specified in 3GPP TS 23.003 [1A]. 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]. The usage of Alternative NAI is specified in clause 5.

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 clause 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 network 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 802.11-1999 [11].

There are two types of scanning procedures specified in IEEE 802.11-1999 [11]:

i) Passive scanning.

ii) Active scanning.

The WLAN UE shall support passive scanning according to IEEE 802.11-1999 [11]. If active scanning is supported then, the WLAN UE should use active scanning according to IEEE 802.11-1999 [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.

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

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 Network discovery procedure as specified in draft-adrangi-eap-network-discovery [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 supports Identity selection hints for EAP procedure as described in draft-adrangi-eap-network-discovery [12], then the I-WLAN sends a subsequent EAP-Request/Identity message to the WLAN UE including the Supported PLMNs list for WLAN access.

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 does not support Identity selection hints for EAP procedure as described in draft-eap-network-discovery [12], then the I-WLAN sends an EAP-Failure message to the WLAN UE.

4.4.2 UE procedures

Upon reception of an EAP-Request/Identity message including the Supported PLMNs list for WLAN access the WLAN UE shall:

- Perform PLMN selection according to clause 5.2.
- Use the Decorated NAI as specified in clause 4.2 and using the PLMN ID of the Selected PLMN.
- Attempt to authenticate as specified in clause 6.1.1 and using the NAI determined in the prior step.

If the Selected PLMN is the HPLMN, then decoration shall not be performed as HPLMN ID is already contained in the Root NAI. As an implementation option, the WLAN UE may store the Supported PLMNs list for WLAN access.

5 Network Selection

5.1 General

In 3GPP WLAN interworking Network selection consists of two procedures: the UE I-WLAN selection procedure, and the UE PLMN selection procedure. 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. The support of additional network selection modes is implementation dependent.

For manual network selection procedures defined in clause 5.2.3 the WLAN UE produces a list of available PLMNs. This is done by associating and performing EAP based network discovery with the available WLANs using the Alternative NAI until every available WLAN has been associated with and EAP network discovery has been performed.

For automatic selection procedures defined in clause 5.2.4 the WLAN UE shall use a WSID that has a direct connection to HPLMN. This is done by associating and performing EAP based network discovery 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" 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.

5.2 PLMN selection

5.2.1 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.

The WLAN UE shall sequentially perform association with each access point for the purpose of discovering the supported PLMNs, using the list of available WSIDs in the following order:

a) 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).

b) 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 and the "Operator Controlled WLAN Specific Identifier list" data file are defined in 3GPP TS 31.102 [13].

c) If neither "User Controlled 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" or "Operator Controlled WLAN Specific Identifier list" lists in the ME memory:

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

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

d) 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 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, 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.

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.

b) 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).

c) 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).

d) 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).

e) 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" 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).

f) Any other PLMN in random order.

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

5.2.4 Automatic PLMN Selection Mode Procedure

In case of automatic selection the WLAN UE shall select and attempt to authenticate with an available and allowable PLMN, in the following precedence.

a) HPLMN.

b) 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).

c) 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].

d) 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).

e) 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).

f) Any other PLMN randomly.

If successful authentication is achieved, the WLAN UE shall indicate to the user the Selected PLMN.

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

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

5.3 Void

5.4 User reselection

5.4.1 UE procedures

5.4.1.1 General

At any time the user 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 clause 5.2;
- Depending on the PLMN selection mode (automatic or manual), perform a new PLMN selection as specified in clauses 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 clause 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 clause 5.2.3

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.

Editor's note: Further collision and abnormal cases may need to be considered. For example, it is FFS the response of the 3GPP AAA server upon reception of a new authentication request from the same user and with the same NAI.

6 UE to 3GPP Network protocols

6.1 UE to 3GPP AAA Server protocols

6.1.1 WLAN Access Authentication and Authorization protocols

6.1.1.1 General

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 network or to the WLAN and 3GPP network.

The WLAN UE and 3GPP AAA server shall support EAP authentication procedures as specified in draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [10].

Other EAP authentication methods than those specified in draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [10] may be supported by the WLAN UE but are not part of 3GPP WLAN IW therefore are out of the scope of the present document.

WLAN authentication signalling for 3GPP-WLAN interworking shall be based on Extensible Authentication Protocol (EAP) as specified in RFC 2284 [6]).

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 clause 6.1.1.3.6).

6.1.1.2 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 TS 23.003 [1A]. draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [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 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 draft-haverinen-pppext-eap-sim [10] and in draft-arkko-pppext-eap-aka [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 clause 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 Key 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 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 authentication servers that only support EAP-SIM 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 clause 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 clause 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 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 draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [10].

NOTE 2: The EAP AKA and EAP SIM signalling flows are described in 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 draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [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 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 roam of the 3GPP AAA server.

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 draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [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 RFC 2284 [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 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 draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [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 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 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 clause 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 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 NACK 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 draft-haverinen-pppext-eap-sim [10] and draft-arkko-pppext-eap-aka [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 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 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 draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [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 draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [10]) and is MAC protected, prior the EAP-Failure message.

NOTE 1: Prior the EAP authentication challenge round takes place (as specified in draft-arkko-pppext-eap-aka [9] subclause 4.3 and draft-haverinen-pppext-eap-sim [10] subclase 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 draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [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 TS 33.234 [5].

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 WLAN access

The "User Controlled PLMN Selector for 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 WLAN access

The "Operator Controlled PLMN Selector for 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].

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].

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 UE shall structure this list as per the "realm-list" specified in draft-adrangi-eap-network-discovery-and-selection [12] and each "realm" in the "realm-list" shall be of the form of a home network domain name as defined in sub-clause 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].

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 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 WLAN UE (using the IMSI).

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

8.2 Tunnel establishment procedures

8.2.1 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 8.3.1.2.

The WLAN UE shall support the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [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 draft-ietf-ipsec-esp-v3 [15]) in order to provide secure tunnels between the WLAN UE and the PDG as specified 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 an 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 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 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 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 criteria for automatic selection is implementation dependent.

8.2.1.3 UE initiated tunnel establishment

In order to request the establishment of a tunnel to a certain W-APN, the WLAN UE shall comply with IKE_v2 protocol definitions as defined in the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [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 draft-ietf-ipsec-ikev2 [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 draft-ietf-ipsec-ikev2 [14]) to the selected PDG (see clause 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.

NOTE1: The username part of the NAI included in IDi payload may be an IMSI, pseudonym or re-authentication ID.

NOTE2: 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 of reception 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 clause 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 clause 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.

8.2.1.4 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 draft-ietf-ipsec-ikev2 [14] to rekey existing IKE and IPsec security association(s).

In order to rekey an existing IPsec ESP security association, the 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 draft-ietf-ipsec-ikev2 [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 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 draft-ietf-ipsec-ikev2 [14].

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 draft-ietf-ipsec-ikev2 [14]), in order to establish trusted relationships (i.e. mutual authentication with the WLAN UE).

The PDG shall support IPsec ESP (see draft-ietf-ipsec-esp-v3 [15]) in order to provide secure tunnels between the WLAN UE and the PDG as specified in 3GPP TS 33.234 [5].

The PDG shall support in place rekeying of security association as described in draft-ietf-ipsec-ikev2 [14]. The support for multiple IPsec ESP security association (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 UE initiated tunnel establishment

Upon reception 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' 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 set to 'AUTHENTICATION FAILED'.

8.2.2.3 Void

8.2.2.4 Void

8.2.2.5 Additional tunnel establishment and in place rekeying

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 draft-ietf-ipsec-ikev2 [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 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 user number of IPsec ESP security associations (I-WLAN tunnels) per user is less than the configured maximum number of IPsec ESP security associations (I-WLAN tunnels) per IKE, then the PDG shall proceed to set up the additional IPsec ESP security association (I-WLAN tunnel) as defined in draft-ietf-ipsec-ikev2 [14] and shall respond with the CREATE_CHILD response message. The PDG shall increment its maintained count of the number of IPsec ESP security associations (I-WLAN tunnels) for that user.

If the count of the number of IPsec ESP security associations (I-WLAN tunnels) for that user is greater than or equal to the configured maximum number of tunnels per IPsec ESP security association (I-WLAN tunnels), the PDG shall reject the establishment request by replying with a CREATE_CHILD_SA reponse 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 draft-ietf-ipsec-ikev2 [14] to setup the new IKE security association and shall subsequently delete the old IKE security association on successful completion of the procedure.

8.3 Tunnel disconnection procedures

8.3.1 UE procedures

8.3.1.1 General

WLAN UE shall use the procedures defined in the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [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.

ii) Protocol ID set to "3" for ESP. The Security Parameters Indexes 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 Security Parameters Indexes 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.

8.3.2 PDG procedures

8.3.2.1 General

PDG shall use the procedures defined in the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [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 Security Parameter Indexes 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.

ii) Protocol ID set to "3" for ESP. The SECURITY PARAMETERS INDEXES s 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 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.

8.4 Timers and counters for tunnel management

Timers are used as defined in draft-ietf-ipsec-ikev2-13.txt [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 WLAN UE-PDG reauthentication, IKE security association and IPsec ESP security association timers are simultaneously reset.

8.5 Void

Annex A (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

History

Document history		
V6.1.1	January 2005	Publication
V6.2.0	March 2005	Publication
V6.3.0	June 2005	Publication
V6.4.0	September 2005	Publication