3GPP TSG-CN Meeting #26 **NP-040508**
8th – 10th December 2004. Athens, Greece.

Source: **TSG CN WG1**

Title: **CRs to Rel-6 WI "WLAN" for TS 23.234**

Agenda item: **9.17**

Document for: **APPROVAL**

This document contains **9 CRs on Rel-6 Work Item "WLAN"**, that have been agreed by TSG CN WG1 CN#36 meeting and forwarded to TSG CN Plenary meeting #26 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Version	WI	Rel
N1-042035	Alignment of the WLAN identities' lists	24.234	001	1	F	6.0.0	WLAN	Rel-6
N1-042036	I-WLAN Parameters coding – Pseudonym and re-authentication identity	24.234	002	1	F	6.0.0	WLAN	Rel-6
N1-042112	References clean-up	24.234	003	2	F	6.0.0	WLAN	Rel-6
N1-042060	Introduction of protected result indications	24.234	004	1	F	6.0.0	WLAN	Rel-6
N1-041734	Removal of the PDG Redirection feature	24.234	006		F	6.0.0	WLAN	Rel-6
N1-042034	Restructuring of clause 5	24.234	008	1	F	6.0.0	WLAN	Rel-6
N1-042040	Cleaning of Editors Notes	24.234	009	1	D	6.0.0	WLAN	Rel-6
N1-042113	Timers in Scenario 3	24.234	011	2	B	6.0.0	WLAN	Rel-6
N1-042044	Editorial change to chapter 8	24.234	014	1	D	6.0.0	WLAN	Rel-6

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-041734

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **006** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Removal of the PDG Redirection feature
Source:	⌘	Ericsson, Nokia
Work item code:	⌘	WLAN
Date:	⌘	15/10/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	At present, the IKEv2 protocol does not include any functionality for the PDG to provide the WLAN UE with an alternative PDG IP address. Therefore, no solution exists in IKEv2 in order to provide the needed functionality to implement the PDG redirection feature by CN1. In order to provide the PDG redirection feature by CN1, either the IKEv2 must be modify by IETF, which will likely delay the completion date of the stage 3 work on I-WLAN to be done by CN WGs or a private version of the IKEv2 protocol must be specified by 3GPP, which would result in considerable additional work and potentially the creation of not interoperable 3GPP version of the IKEv2 protocol. All the above solutions will delay the completion date of the I-WLAN work to be done by the CN WGs for Rel-6. Additionally, the modification of the current IKEv2 protocol would result in a delay of the acceptance of the IKEv2 internet draft, which already has been approved by IESG and is in the RFC queue. Finally, The PDG redirection feature is only an enhancement feature and its removal does not remove any fundamental functionality from WLAN Interworking.
Summary of change:	⌘	The sub-clauses related to the PDG redirection feature are deleted.
Consequences if	⌘	No solution in place for the PDG redirection feature at stage 3 for Rel-6.

not approved:	Furthermore, the modification of the current IKEv2 protocol would result in a delay of the acceptance of the IKEv2 internet draft, which already has been approved by IESG and is in the RFC queue. The other alternative to fulfil the PDG redirection requirements, i.e. a private version of the IKEv2 protocol to be specified by 3GPP, would result in considerable additional work and potentially the creation of not interoperable 3GPP version of the IKEv2 protocol.

Clauses affected:	⌘	8.2.1.5, 8.2.2.4			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	This contribution is related to DISC in N1-041733			

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

1st Change

8.2 Tunnel establishment procedures

8.2.1 UE procedures

8.2.1.1 General

After successful EAP authentication and 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 DNS procedure as mentioned in clause 8.3.1.2.

The WLAN UE shall support IKEv2 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 [14] 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 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. See TS 23.003 [1a]. Details on the construction of W-APN in the different roaming scenarios are specified in 3GPP TS 23.234 [2].

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 dependant.

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 draft-ietf-ipsec-ikev2-15 [14]. In order to set up an IKE connection between the UE and the PDG, the UE shall initiate the signalling procedure by sending the IKE_SA_INIT request message defined in IKE_v2 [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 in IKE_v2 [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.

NOTE: The username part of the NAI included in IDi payload may be an IMSI, pseudonym or re-authentication ID. There is no requirement to use full authentication mechanism for the 1st tunnel establishment. 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 Subsequent tunnel establishment

Editor's note: From 3GPP TS 23.234: 'In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process (for example, a shorter re-authentication process should be used). This is ffs in Stage 3 work.'

8.2.1.5 Void~~Redirection~~

~~Editor's note: WLAN UE functionality to support redirection procedure as specified in 3GPP TS 23.234, clause 7.9.1.~~

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 dependant.

The PDG shall support IPSec tunnelling using IKEv2, in order to establish trusted relationships (i.e. mutual authentication with the WLAN UE).

The PDG shall support IPSec ESP [15] in order to provide secure tunnels between the WLAN UE and the PDG as specified in 3GPP TS 33.234 [5].

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.

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 Subsequent tunnel establishment

Editor's note: From 3GPP TS 23.234: 'In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process (for example, a shorter re-authentication process should be used). This is ffs in Stage 3 work.'

8.2.2.4 Void~~Redirection~~

~~Editor's note: PDG functionality to support redirection procedure as specified in 3GPP TS 23.234, clause 7.9.1.~~

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-042034

was Tdoc N1-041819

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **008** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Restructuring of clause 5
Source:	⌘	Lucent Technologies
Work item code:	⌘	WLAN
Date:	⌘	26/10/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change: ⌘ 3GPP TS 23.234 clause 5 could benefit from some restructuring in order to make the material easier to present. This contribution makes a step in that direction. The core of clause 5 is the network selection in subclause 5.2.2. The essence of the proposal is to move that subclause up two levels to become clause 5, and move the displaced material appropriately.
Additionally the following issues have been addressed (primarily to remove collisions with other CRs during preparation):

1. At the beginning of the CN1 work on I-WLAN the list of forbidden PLMNs for WLAN access was introduced into the TS 24.234 to try to mimic a list which does exist in the PLMN selection specificacion for cellular protocols, i.e. TS 23.122. However, TS 24.234 has no description of the criteria for the WLAN UE to handle this list and, add or remove PLMNs to the list. Hence, TS 24.234 is itself inconsistent. Even though TS 24.234 states that "The contents of this file are specified in 3GPP TS 31.102", the list of "forbidden PLMNs for WLAN access" is not specified in TS 31.102, so not supported in the USIM application. This implies that the WLAN UE cannot implement the list of "forbidden PLMNs for WLAN access".
2. The correct reference to TS 23.122 is [1], not [3].
3. TS 22.234 (stage 1 on I-WLAN) and TS 23.234 (stage 2 on I-WLAN) specify differently than TS 24.234. According to stage 1 and 2 two lists are defined for the purpose of selecting the preferred I-WLAN. Not only this, but T3 also informs CN1 in the LS in T3-040608 that "two files are available in TS 31.102 for usage in WLAN selection procedures". These files are "User Controlled WLAN Specific Identitier list" and "Operator

Controlled WLAN Specific Identifier list".

4. In the current TS 24.234 there are several Editors' Notes which can be safely removed.
5. In order to obtain the Supported PLMNs list for WLAN access for manual network selection the definition of an 'Alternative NAI' should be used.
6. TS 24.234 in the sub-clause 5.2.2.4.2 '3GPP AAA Server procedures' mandates the 3GPP AAA server to release the old authentication status information when a new authentication request from the same user is received, even though the user has associate to a different AP in a different PLMN than the current mediating PLMN. This should be implementation dependent. That is to say, the 3GPP AAA Server implementation should be allowed to be implemented in such a way to have simultaneous connections from the same user in different PLMNs. The current requirement should be loosened in order to allow flexible implementations in the 3GPP AAA Server.
7. Addtionally, the current thext in the sub-clause 5.2.2.4.2 is incorrect, because it is stated that "the 3GPP AAA server may receive a new authentication request from the same user but with **different NAI** (i.e. the new Selected WLAN VPLMN will generate a new Decorated NAI)". Although, the user selects a different VPLMN (so a new Decorated NAI is generated), the 3GPP AAA server does not receive a different NAI. The Decorated NAI is converted by the 3GPP AAA proxy to 'user@wlan.mnc.mcc.3gppnetwork.org' when passing the NAI forward. Please have a look to the following text stated in the NAIbis Internet draft (i.e draft-ietf-radex-rfc2486bis): The use of the home realm MUST be the default unless otherwise configured. Where these conditions are fulfilled, an NAI such as user@homerealm.example.net MAY be represented as in homerealm.example.net!user@otherrealm.example.net. In this case, the part before the (non-escaped) '!' MUST be a realm name as defined in the ABNF in Section 2.1. When receiving such an NAI, the other realm MUST convert the format back to "user@homerealm.example.net" when passing the NAI forward, as well as applying appropriate AAA routing for the transaction. The conversion process may apply also recursively. That is, after the conversion the result may still have one or more '!' characters in the username. For instance, the NAI other2.example.net!home.example.net!user@other1.example.net would first be converted in other1.example.net to home.example.net!user@other2.example.net and then at other2.example.net finally to user@homerealm.example.net"

Summary of change: ⌘

- Move existing clause 5.2.2 up one level to become clause 5. This requires action on a number of existing subclauses as follows:
- Subclauses 4.2.2, 4.2.3 and 4.2.4 are reordered.
- Subclause 5.1.1. Move to form new subclause 4.3.
- Subclause 5.2.1. Paragraphs need to be moved to either clause 4 or to subclause 5.2.2.1. Note that in the 2nd moved paragraph, the text "3GPP WLAN interworking" has been inserted before "network selection" to correspond to the titles of subsequent subclauses. The paragraphs relating to manual and automatic have been reordered to correspond to the later swapping of related subclauses.
- Subclause 5.2.2.1, existing paragraphs are now deleted as they are superflous.
- Subclause 5.2.2.2 is moved to become new subclause 4.4.
- Subclause 5.2.1, additional clarification paragraph on format of subsequent clauses added at end.
- Existing subclause 5.2.2.3.2, deleted as now superfluous.
- The two PLMN Selection Mode Procedures (manual and automatic) are swapped.
- Subclause 5.3. Move to clause 7.
- A minor clarification is made in subclause 4.2.1 as to the nature of the message used.

		• The list of forbidden PLMNs for WLAN access is removed. • The existing “Preferred WSIDs list“ has been replaced by the “User Controlled WLAN specific identitier list” and “Operator Controlled WLAN specific identifier list”. • Removal of some of the editors notes • Addition of ‘Alternative NAI’ to enable WLAN UE to obtain list of Supported PLMNs list for WLAN access for manual network selection. In the clause 5 the addition of ‘Alternative NAI’ and the related usage of such different NAI types. • The requirement is modified allowing 3GPP AAA server implementations which keep both the old status information and the new one. This allows simultaneous connections from the same user.
Consequences if not approved:	⌘	Poorly structured specification. This CR currently makes no technical change. For list of forbidden PLMNs for WLAN access, misalignment among 3GPP specifications remains. Even though TS 24.234 states that “The contents of this file are specified in TS 31.102”, the list of "forbidden PLMNs for WLAN access" is not specified in TS 31.102, so not supported in the USIM application. This implies that the WLAN UE cannot implement the list of "forbidden PLMNs for WLAN access"as specified by TS 24.234. Incorrect references remain. For Preferred WSIDs list misalignment among stage 1, 2 and 3 specifications remains. Inconsistent set of specifications on the Network selection procedures for I-WLAN. Irrelevant editor's notes remain. The manual network selection will not work. Inflexibility in the 3GPP AAA server implementation remains. Simultaneous connections from the same user are not allowed.

Clauses affected:	⌘	3.1, 4.1, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.4, 5 (throughout), 7.3			
Other specs affected:	⌘	**Y** / **N**		⌘	
			X Other core specifications		
			X Test specifications		
			X O&M Specifications		
Other comments:	⌘	The approval of text regarding Alternative NAI definition and usage proposed by this CR depends on approval of CRs against TS 23.003.			

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

PROPOSED CHANGE

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 specific 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 (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])

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

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~~.2.2~~.1, either manually or automatically

selected PLMN: this is the PLMN that has been selected according to clause 5.~~2.3.~~3, 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 23.234 [2] apply.

3GPP - WLAN Interworking (WLAN-3GPP IW)
3GPP AAA server
3GPP AAA proxy
Interworking WLAN
W-APN
WLAN UE
WLAN Roaming

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

Decorated NAI
Root NAI

PROPOSED CHANGE

4 General

Editor's Note: Provides general overview of WLAN-3GPP IW system.

4.1 3GPP WLAN Interworking System

The 3GPP AAA server is located in the home network and it is responsible for access control. In a non-roaming scenario, the 3GPP AAA server interfaces a WLAN directly via the Wa reference point. In a roaming scenario, the 3GPP AAA server interfaces a 3GPP AAA proxy in another 3GPP network via the Wd reference point, and the 3GPP AAA proxy further communicates with the WLAN via the Wa reference point. The 3GPP AAA proxy transparently relays access control (authentication and access authorization) signalling to the home 3GPP AAA server. Within the scope of the present document, the Wa and Wd reference point are therefore identical.

The Wa and Wd reference points are defined in 3GPP TS 23.234 [2]. The WLAN-UE is equipped with an UICC (or SIM card) 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.

Editor's note: Figures 1 and 2 in Annex B show the Network Selection model applicable to the present document.

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 RFC 2486 [8].

The NAI realm shall be in the form of a domain name as specified in RFC 1035 [7], the NAI username shall comply with draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [10].

~~4.2.2 Username~~

~~The rules for the use of NAI username in the WLAN UE and for the generation and delivery of NAI username in 3GPP AAA server are defined in clause 6.1. The format of NAI username is defined in 3GPP TS 23.003 [1A].~~

4.2.2~~3~~ Root NAI

This is the NAI format when the WLAN UE authenticates directly to HPLMN (see draft-adrangi-eap-network-discovery-and-selection [12] and 3GPP TS 23.234 [2]). Root NAI format is specified in 3GPP TS 23.003 [1A]. The usage of Root NAI is specified in clause 5~~.2.2~~.

4.2.34 Decorated NAI

This is the NAI format when the WLAN authenticates to HPLMN via VPLMN (see draft-adrangi-eap-network-discovery-and-selection-00 [12]). Decorated NAI format is specified in 3GPP TS 23.003 [1A]. The usage of Decorated NAI is specified in clause 5.2.2.

4.2.4 Username

The rules for the use of NAI username in the WLAN UE and for the generation and delivery of NAI username in 3GPP AAA server are defined in clause 6.1. The format of NAI username is defined in 3GPP TS 23.003 [1A].

4.3 Scanning procedures

4.3.1 Case of IEEE 802.11 WLANs

In the case of 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 by 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 creates a list of AvailableWSIDs. 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 Case of other WLANs

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

4.4 Network discovery

4.4.1 General

The Network discovery procedure shall be executed between WLAN UE and the local AAA for the purpose of sending the WLAN UE the Supported PLMNs list for WLAN access for manual selection procedure. The WLAN UE shall support the Network discovery procedure as specified in draft-adrangi-eap-network-discovery [12]. The Network discovery is triggered by the reception of an Alternative NAI for manual selection procedure.

If the 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 WLAN sends a subsequent EAP-Request/Identity message to the WLAN UE including the Supported PLMNs list for WLAN access.

If the 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 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 5.3.
- 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 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.

PROPOSED CHANGE

~~5 UE to WLAN protocols~~

~~5.1 WLAN protocols~~

~~5.1.1 Scanning procedures~~

~~5.1.1.1 Case of IEEE 802.11 WLANs~~

~~In the case of 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 by 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 creates a list of AvailableWSIDs. The list of Available WSIDs consists of all WSIDs found in passive scanning and all WSIDs received in probe response messages.~~

~~5.1.1.2 Case of other WLANs~~

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

~~5.2 Network selection procedures~~

~~5.2.1 General~~

~~In 3GPP WLAN interworking Network selection consists of two procedures: the I-WLAN selection procedure, the network selection procedure. These procedures are applicable to initial network selection at WLAN UE switch on and following recovery from lack of WLAN radio coverage.~~

~~Two network selection modes are defined, automatic and manual. The support of additional network selection modes is implementation dependent.~~

~~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.~~

~~For automatic selection procedures defined in clause 5.2.2.3.3 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 "Preferred WSIDs list", if available.~~

~~For manual network selection procedures defined in clause 5.2.2.3.4 the WLAN UE produces a list of available PLMNs. This is done by associating and performing EAP based network discovery with the available WLANs until every available WLAN has been associated with and EAP network discovery has been performed.~~

~~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 [3]. The signal quality shall not be used as a parameter for network selection.~~

~~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.~~

5~~.2.2~~ Network Selection

5~~.2.2~~.1 General

~~The WLAN UE identifies itself to the WLAN by inserting its NAI in EAP-Response/Identity message. In the case when the WLAN cannot derive the 3GPP AAA Server where to route the WLAN UE's EAP authentication signalling to, it is said that the WLAN has no direct roaming relationship with the user's home network.~~

~~The WLAN uses realm part of NAI to route EAP authentication signalling to the Home 3GPP AAA server of the subscriber with whom the WLAN UE performs authentication. This procedure is out of the scope of the present document.~~

~~Upon reception of the first EAP-Request/Identity message, the WLAN UE shall respond with an EAP-Response/Identity message. The identity included in this first EAP-Response/Identity message shall include an indication of the subscriber's HPLMN and may include (implementation option) an indication on a preferred VPLMN. Therefore the WLAN UE has two options on the choice of the identity to include in the first EAP-Response/Identity message:~~

- ~~Root NAI: This identity may be included e.g. when the WLAN UE intends to trigger the Network Discovery procedure or when the WLAN UE is aware that the WLAN has direct connection to HPLMN.~~
- ~~Decorated NAI: This identity may be included either when the WLAN UE is aware that the associated WSID does not provide direct connection to HPLMN and it has information from previous authentications about the VPLMNs supported by this WSID or when a user during the manual selection procedure selects a different PLMN other than HPLMN.~~

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.

~~5.2.2.2 Network Advertisement~~

~~5.2.2.2.1 General~~

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

~~If the 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 it does not support Network Discovery procedure as described in draft-eap-network-discovery-and-selection [12], then the WLAN sends an EAP-Failure message to the WLAN UE.~~

~~5.2.2.2.2 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 5.2.2.3.~~
- ~~Decorate 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 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.~~

~~Editors note: Upon reception of an EAP-Failure message in response to an EAP-Identity/Response message, the exact behaviour of the WLAN UE is FFS. The WLAN UE may (i) attempt authentication via one of the preferred PLMNs or (ii) attempt access to another WLAN or (iii) do nothing.~~

5~~.2.2~~.2~~3~~ PLMN selection

5~~.2.2~~.2~~3~~.1 UE I-WLAN Selection procedure

The WLAN UE shall use scanning procedures as specified in subclause ~~5.1.1~~4.3 in order to find the available WSIDs.

The WLAN UE shall sequentially perform association with ~~a particular~~ 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 ~~In case the 'Preferred WSID list'~~ is available in the USIM, each WSID in the "User Controlled WLAN Specific Identifier list"~~'Preferred WSID 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].

~~b~~c) If neither "User Controlled WLAN Specific Identifier list" nor "Operator Controlled WLAN Specific Identifier list" data file is available in the USIM ~~In case when the 'Preferred WSIDs list' is not 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 ~~'Preferred WSIDs list'~~ in the ME memory~~, each WSID in the 'Preferred WSIDs list' data file in the ME in priority order.~~:

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).

~~c~~d) Other WSIDs ~~of WLAN APs~~ 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.

~~5.2.2.3.2 UE-PLMN Selection Procedures~~

~~In order to perform PLMN selection the WLAN UE shall discover the PLMNs supported by the available I-WLANs using the I-WLAN selection procedure in clause 5.2.2.3.1.~~

~~There are two modes for PLMN selection:~~

~~i) Automatic mode: this mode utilizes a list of PLMNs in priority order. The highest priority PLMN which is available and allowable is selected according to clause 5.2.2.3.3.~~

~~ii) Manual mode: here the WLAN UE indicates to the user a list of Available PLMNs according to clause 5.2.2.3.4. When the user makes a manual selection then the WLAN UE attempts to authenticate with the Selected PLMN.~~

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.

5.2.2.23.43 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 5.2.2.3.1.

5.2.2.3.4 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 Root NAI. See the clause 4.2.3.

~~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~~.2.2~~.4 User reselection

5~~.2.2~~.4.1 UE procedures

5~~.2.2~~.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~~.2.2~~.3.1;
- Depending on the PLMN selection mode (automatic or manual), perform a new PLMN selection as specified in clauses 5~~.2.2~~.4.1.2 and 5~~.2.2~~.4.1.3.

~~Editor's note: Disassociation if the WLAN UE can find a PLMN without disassociating needs to be clarified in the future.~~

5.2.2.4.1.2 Automatic Network Selection Mode

The WLAN UE shall follow the Automatic Network Selection Mode Procedure as specified in clause 5.2.2.3.3.2.4 with the exception that the WLAN UE shall not chose the current mediating PLMN unless it is the only PLMN that is available.

5.2.2.4.1.3 Manual Network Selection Mode

The WLAN UE shall follow the Manual Network Selection Mode Procedure as specified in clause 5.2.2.3.4..2.3

5.2.2.4.2 3GPP AAA Server procedures

The WLAN UE may associate with a new access point and select a different PLMN than the current mediating 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 with from a different NAI PLMN (ei.ge. 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 and 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 procedureonce the new authentication procedure has been successfully completed.

Editor's note: How the 3GPP AAA Server will find out that the mediating PLMN has changed for the same user, depends on the format of the Decorated NAI. Therefore, this issue will be specified further when NAI decoration format is more stable in IETF.

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.

5.3 List of forbidden PLMNs for WLAN access

The WLAN UE shall contain a list of "Forbidden PLMNs for WLAN access". The list shall be removed at switch off. The list is defined in clause 7.3.

The WLAN UE shall not use the "Forbidden PLMNs for WLAN access" available from other accesses for WLAN PLMN selection nor Authentication procedures.

Editor's note: When a WLAN UE receives an EAP-Failure message in response to an EAP-Response/Identity message, presently there is no such error cause like 'WLAN services not allowed in this PLMN' defined according to the draft-arkko-pppext-eap-aka-12 [9]. So the addition of PLMN identity (which was used to decorate the NAI in the EAP-Response/Identity message) to the list of forbidden PLMNs for WLAN access is FFS.

PROPOSED CHANGE

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 defined for EAP-AKA in draft-arkko-pppext-eap-aka [9] and for EAP-SIM in draft-haverinen-pppext-eap-sim [10]. Pseudonym generation in the 3GPP AAA server is specified in 3GPP TS 33.234 [5].

7.3 ~~Forbidden PLMNs for WLAN access~~Void

~~The *Forbidden PLMNs for WLAN access* file contains a list of PLMN codes to which the WLAN UE shall not attempt to authenticate in automatic mode. 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].~~

7.4 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 Operator Preferred WSID list

The *Preferred WSID 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 may store it for further use. The list shall be deleted at switch off. The format of this list is specified in draft-adrangi-eap-network-discovery-and-selection [12].

7.8 Re-authentication identity

The format of the re-authentication identity is specified in 3GPP TS 23.003 [1A].

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-042035
Revision of N1-041678

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **001** ⌘**rev** **1** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Alignment of the WLAN identities' lists
Source:	⌘	Ericsson, Samsung
Work item code:	⌘	WLAN
Date:	⌘	17/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	TS 22.234 (stage 1 on I-WLAN) and TS 23.234 (stage 2 on I-WLAN) specify differently than TS 24.234. According to stage 1 and 2 two lists are defined for the purpose of selecting the preferred I-WLAN. Not only this, but T3 also informs CN1 in the LS in T3-040608 that "two files are available in TS 31.102 for usage in WLAN selection procedures". These files are "User Controlled WLAN Specific Identitier list" and "Operator Controlled WLAN Specific Identifier list".
Summary of change:	⌘	The existing "Preferred WSIDs list" has been replaced by the "User Controlled WLAN specific identitier list" and "Operator Controlled WLAN specific identifier list".
Consequences if not approved:	⌘	Misalignment among stage 1, 2 and 3 specifications remains. Inconsistent set of specifications on the Network selection procedures for I-WLAN.

Clauses affected:	⌘	7.6, new 7.6a

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

1st Change

7.4 User Controlled PLMN Selector for WLAN access

The "User Controlled PLMN Selector for WLAN access"~~*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"~~*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~~Operator Preferred WSID list~~

The ~~*Preferred WSID*~~"User Controlled WLAN Specific Identifier list"~~ *list*~~ file contains a list of WSIDs related to I-WLAN preferred by the user~~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].

7.6a 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"~~*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 may store it for further use. The list shall be deleted at switch off. The format of this list is specified in draft-adrangi-eap-network-discovery-and-selection [12].

7.8 Re-authentication identity

The format of the re-authentication identity is specified in 3GPP TS 23.003 [1A].

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-042036
Revision of N1-041679

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **002** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	I-WLAN Parameters coding – Pseudonym and re-authentication identity
Source:	⌘	Ericsson
Work item code:	⌘	WLAN
Date:	⌘	17/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	TS 33.234 specifies the format and generation of the temporary identities, i.e. psedonym and re-authentication identity. Additionally, TS 23.003 specifies the "deleted" value of the temporary identities which indicates that no valid temporary identity exists in the USIM/ME. At present, the text in the sub-clauses 7.2 'Pseudonym' and 7.8 'Re-authentication identity' of TS 24.234 is not fully compliant with TS 33.234 and TS 23.003.
Summary of change:	⌘	The format and generation of the temporary identities point out to TS 33.234 and the reference to TS 23.003 is used to indicated where the "deleted" value is specified.
Consequences if not approved:	⌘	Misalignment among specifications remains. The text in TS 24.234 does not describe where the format, generation and the "deleted" value are specified for the case of the termporary identities, i.e. pseudonym and re-authentication identity.

Clauses affected:	⌘	7.2, 7.8

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	O&M Specifications

⌘

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

1st Change

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 ~~defined for EAP-AKA in draft-arkko-pppext-eap-aka [9] and for EAP-SIM in draft-haverinen-pppext-eap-sim [10]. Pseudonym generation in the 3GPP AAA server 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].

Next Change

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].

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-042040
was N1-041838

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **009** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Cleaning of Editors Notes
Source:	⌘	Samsung, Ericcson, Nokia
Work item code:	⌘	WLAN
Date:	⌘	04/11/2004
Category:	⌘	**D**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	In the current TS 24.234 there are several Editors' Notes which can be safely removed.
Summary of change:	⌘	Removal of some of the editors notes mentioned below after due discussions.
Consequences if not approved:	⌘	These editors notes are no more relevant or they have to be removed before closure of the spec for Rel-6.

Clauses affected:	⌘	1, 4, 4.1, 6.1.1, 6.1.1.2.2, 6.1.1.2.4.1, 6.1.1.3.4, 8.2.1.4, 8.2.2.3,8.5

Other specs affected:	Y	N		
⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

1st Change

1 Scope

The present document specifies the network selection, including Authentication and Access Authorization 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.

Details of the security framework for the end-to-end tunnel establishment are covered in 3GPP TS 33.234 [5]. The transport of the Tunnel management signalling between WLAN and 3GPP network; and within the 3GPP network (i.e. PDG, 3GPP AAA server and WAG) are covered in 3GPP TS 29.234 [3].

~~Editor's note: For tunnel management the work division in 3GPP groups is as follows. SA3 takes care of security considerations related to the tunnel establishment. CN1 takes care of tunnel management issues related. CN4 takes care of internal signalling (e.g. for re-direction, 3GPP AAA Server – PDG functionality).~~

2nd Change

4 General

~~Editor's Note: Provides general overview of WLAN 3GPP IW system.~~

4.1 3GPP WLAN Interworking System

The 3GPP AAA server is located in the home network and it is responsible for access control. In a non-roaming scenario, the 3GPP AAA server interfaces a WLAN directly via the Wa reference point. In a roaming scenario, the 3GPP AAA server interfaces a 3GPP AAA proxy in another 3GPP network via the Wd reference point, and the 3GPP AAA proxy further communicates with the WLAN via the Wa reference point. The 3GPP AAA proxy transparently relays access control (authentication and access authorization) signalling to the home 3GPP AAA server. Within the scope of the present document, the Wa and Wd reference point are therefore identical.

The Wa and Wd reference points are defined in 3GPP TS 23.234 [2]. The WLAN-UE is equipped with an UICC (or SIM card) 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.

~~Editor's note: Figures 1 and 2 in Annex B show the Network Selection model applicable to the present document.~~

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

3rd Change

6.1.1 WLAN Access Authentication and Authorization protocols

~~Editor's Note: Functionality in WLAN UE and 3GPP AAA server for identification, full authentication and re-authentication. Procedures are defined in [9] and [10]. This TS should specify the mandatory and optional features from SIM and AKA drafts. As an example Reauthentication and Privacy support are optional in the EAP-SIM and EAP-AKA drafts but mandatory for the WLAN UE and network.~~

4th Change

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.

~~Editor's note: The temporary identity(ies) format and the "deleted" value, which indicates the case when no valid temporary identity(ies) exists in the UE, requires definition in TS 23.003 [1A].~~

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.

5th Change

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.

~~Editor's note: The details and security aspects of ME policy configuration are for further study.~~

6th Change

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.

~~Editor's note: The details and security aspects of AAA server policy configuration are for further study.~~

7th Change

8.2.1.4 Void~~Subsequent tunnel establishment~~

~~Editor's note: From 3GPP TS 23.234: 'In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process (for example, a shorter re-authentication process should be used). This is ffs in Stage 3 work.'~~

8th Change

8.2.2.3 VoidSubsequent tunnel establishment

~~Editor's note: From 3GPP TS 23.234: 'In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process (for example, a shorter re-authentication process should be used). This is ffs in Stage 3 work.'~~

9th Change

8.5 VoidCause codes for tunnel management

~~Editor's note: it contains causes codes that are not covered in IETF specifications but that are needed for the purposes of 3GPP IW. For example when tunnel establishment failure reason is that the WLAN UE is not allowed to use a visited PDG to access the given W-APN.~~

End of Changes

3GPP TSG-CN WG1 Meeting #36 ***N1-042044***

Seoul, Korea. November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **14** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Editorial Changes to Chapter 8
Source:	⌘	Nokia
Work item code:	⌘	WLAN
Date:	⌘	18/11/04
Category:	⌘	**D**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	Incorrect specification
Summary of change:	8.3.2.2 is obviously an incorrect clause number.
Consequences if not approved:	Unclear spec

Clauses affected:	8.3.2

	Y	N		
Other specs affected:		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments:

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

**** First modified section ****

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.

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

After successful EAP authentication and 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 DNS procedure as mentioned in clause 8.3.1.2.

The WLAN UE shall support IKEv2 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 [14] 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 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. See TS 23.003 [1a]. Details on the construction of W-APN in the different roaming scenarios are specified in 3GPP TS 23.234 [2].

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 dependant.

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 draft-ietf-ipsec-ikev2-15 [14]. In order to set up an IKE connection between the UE and the PDG, the UE shall initiate the signalling procedure by sending the IKE_SA_INIT request message defined in IKE_v2 [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 in IKE_v2 [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.

NOTE: The username part of the NAI included in IDi payload may be an IMSI, pseudonym or re-authentication ID. There is no requirement to use full authentication mechanism for the 1st tunnel establishment. 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 Subsequent tunnel establishment

Editor's note: From 3GPP TS 23.234: 'In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process (for example, a shorter re-authentication process should be used). This is ffs in Stage 3 work.'

8.2.1.5 Redirection

Editor's note: WLAN UE functionality to support redirection procedure as specified in 3GPP TS 23.234, clause 7.9.1.

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 dependant.

The PDG shall support IPSec tunnelling using IKEv2, in order to establish trusted relationships (i.e. mutual authentication with the WLAN UE).

The PDG shall support IPSec ESP [15] [AvT22]in order to provide secure tunnels between the WLAN UE and the PDG as specified in 3GPP TS 33.234 [5].

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.

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 Subsequent tunnel establishment

Editor's note: From 3GPP TS 23.234: 'In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process (for example, a shorter re-authentication process should be used). This is ffs in Stage 3 work.'

8.2.2.4 Redirection

Editor's note: PDG functionality to support redirection procedure as specified in 3GPP TS 23.234, clause 7.9.1.

8.3 Tunnel disconnection procedures

8.3.1 UE procedures

WLAN UE shall use the procedures defined in IKEv2 [14] to disconnect an IPSec tunnel to the PDG. The 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 SA.

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.

8.3.1.1 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 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

PDG shall use the procedures defined in IKEv2 [14] to disconnect an IPSec tunnel to the UE. The PDG shall close the incoming Security Associations associated with the tunnel and instruct the 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 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 UE for the given tunnel in question.

8.3.2.1~~2~~ UE Initiated Tunnel Disconnection Procedures

On receipt of the INFORMATIONAL request message including "DELETE" payload indicating that the 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 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 UE; or

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

8.4 Timers and counters for tunnel management

Editor's note: it contains timers and counters that are not covered in IETF specifications but that are needed for the purposes of 3GPP IW.

8.5 Cause codes for tunnel management

Editor's note: it contains causes codes that are not covered in IETF specifications but that are needed for the purposes of 3GPP IW. For example when tunnel establishment failure reason is that the WLAN UE is not allowed to use a visited-PDG to access the given W-APN.

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-042060
Revision of N1-041681

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **004** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Introduction of protected result indications
Source:	⌘	Ericsson
Work item code:	⌘	WLAN
Date:	⌘	17/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	At SA3#34 the CR in S3-040670 on 'Introduction of protected result indications' was agreed and now, implemented in the latest version of TS 33.234 v6.2.1. Finally, during the implementation between TS 24.234 v1.5.0 and v1.6.0, which became v6.0.0 after approval at TSG CN (#25), the heading number of the sub-clause 6.1.1.2.5 was changed without reason to 6.1.1.2.4.2.
Summary of change:	⌘	Introduction of protected result indications into TS 24.234. The heading number of the sub-clause 6.1.1.2.4.2 is corrected.
Consequences if not approved:	⌘	Misalignment with stage 2 (i.e. TS 33.234) remains.

Clauses affected:	⌘	6.1.1.2.4.2, new 6.1.1.2.6, new 6.1.1.3.7

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

1st Change

6.1.1.2.5~~4.2~~ 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].

Next Change

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].

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-042112
Revision of N1-042037

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **003** ⌘ **rev** **2** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	References clean-up
Source:	⌘	Ericsson, Samsung
Work item code:	⌘	WLAN
Date:	⌘	19/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	The reference to IKEv2 [14] is obsolete. TS 24.234 refers to the reference [15] which does not exist in the reference clause of the specification. The correct reference to TS 23.122 is [1], not [3]. Several Internet drafts have been updated by IETF, e.g. EAP AKA, EAP SIM.
Summary of change:	⌘	The reference number [14] is updated. The reference number [15] is introduced into TS 24.234 to make the text in this specification consistent. The reference to TS 23.122 is corrected. Update of several Internet drafts, i.e. references [9], [10] and [12].
Consequences if not approved:	⌘	Obsolete references remain, i.e. [14], [9], [10], [12]. TS 24.234 refers to [15] which does not exist. TS 23.122 refers to incorrect 3GPP document.

Clauses affected:	⌘	2, 3.1, 4.2.4, 8.2.1.1, 8.2.1.2, 8.2.1.3, 8.2.2.1, 8.3.1, 8.3.1.1, 8.3.2

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

1st Change

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".

[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~~2284~~ (June 2004~~March 1998~~): "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~~2~~ (October~~April~~ 2004): " Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP AKA) ~~Authentication~~".

[10] draft-haverinen-pppext-eap-sim-1~~3~~4 (October~~April~~ 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 ~~and selection~~ -05~~1~~ (October~~March~~ 2004): "Identity selection hints for Extensible Authentication Protocol (EAP)~~Network Discovery and Selection within the EAP Framework~~".

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

[14] draft-ietf-ipsec-ikev2-17~~3~~.txt, (October~~March~~ 2004): "Internet Key Exchange (IKEv2) Protocol".

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

Next Change

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 specific 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 (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])

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

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 5.2.2.1, either manually or automatically

selected PLMN: this is the PLMN that has been selected according to clause 5.2.3.3, 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 23.234 [2] apply.

3GPP - WLAN Interworking (WLAN-3GPP IW)
3GPP AAA server
3GPP AAA proxy
Interworking WLAN
W-APN
WLAN UE
WLAN Roaming

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

Decorated NAI
Root NAI

Next Change

4.2.3 Root NAI

This is the NAI format when the WLAN UE authenticates directly to HPLMN (see draft-adrangi-eap-network-discovery ~~and selection~~ [12] and 3GPP TS 23.234 [2]). Root NAI format is specified in 3GPP TS 23.003 [1A]. The usage of Root NAI is specified in clause 5.2.2.

Next Change

8.2.1.1 General

After successful EAP authentication and 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 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~~4~~]) 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 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. See TS 23.003 [1a]. Details on the construction of W-APN in the different roaming scenarios are specified in 3GPP TS 23.234 [2].

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 depende~~a~~nt.

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~~-15~~ [14]). In order to set up an IKE connection between the UE and the PDG, the UE shall initiate the signalling procedure by sending the IKE_SA_INIT request message defined in draft-ietf-ipsec-ikev2~~IKE_v2~~ [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~~IKE_v2~~ [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.

NOTE: The username part of the NAI included in IDi payload may be an IMSI, pseudonym or re-authentication ID. There is no requirement to use full authentication mechanism for the 1st tunnel establishment. 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.

Next Change

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 dependeant.

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]) ~~[15] [AvT22]~~in order to provide secure tunnels between the WLAN UE and the PDG as specified in 3GPP TS 33.234 [5].

Next Change

8.3 Tunnel disconnection procedures

8.3.1 UE procedures

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 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 SA.

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.

8.3.1.1 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 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

PDG shall use the procedures defined in the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [14]) to disconnect an IPSec tunnel to the UE. The PDG shall close the incoming Security Associations associated with the tunnel and instruct the 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 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 UE for the given tunnel in question.

3GPP TSG-CN WG1 Meeting #36 ***N1-042113***

Seoul, Korea. November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **011** ⌘ **rev** **2** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Timers in Scenario 3
Source:	⌘	Nokia
Work item code:	⌘	WLAN
Date:	⌘	18/11/04
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change: ⌘ Timers are listed as an open issue in WLAN-IW. This CR aims to close that gap.

Unlike IKE_v1, IKE_v2 does not define any explicit negotiation of timers between tunnel endpoints. Rather, each end point is required to maintain a timer for each SA. Whichever timer endpoint expires first will determine which entity renegotiates the SA. In WLAN-IW, we have timers associated with the IKE_SA as well as the ESP_SA.

Note also that there will be a timer associated with the UE-3GPP AAA Sever reauthentication. However at present there is no mechanism by which a reauthentication timer can be sent to the UE within IKE_v2. Reauthentication is therefore triggered at rekeying

To simplify timer handling, we propose to recommend the following:

(i) Recommend to use timers as defined in IKE_v2

(ii) Recommend that UE and PDG IKE_v2 users timers of the order of 3 hours.

Summary of change: ⌘ Adds text to describe timers in chapter 8

Consequences if not approved: ⌘ Undefined functionality in 24.234

Clauses affected: ⌘

		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request

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.

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

After successful EAP authentication and 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 DNS procedure as mentioned in clause 8.3.1.2.

The WLAN UE shall support IKEv2 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 [14] 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 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. See TS 23.003 [1a]. Details on the construction of W-APN in the different roaming scenarios are specified in 3GPP TS 23.234 [2].

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 dependant.

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 draft-ietf-ipsec-ikev2-15 [14]. In order to set up an IKE connection between the UE and the PDG, the UE shall initiate the signalling procedure by sending the IKE_SA_INIT request message defined in IKE_v2 [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 in IKE_v2 [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.

NOTE: The username part of the NAI included in IDi payload may be an IMSI, pseudonym or re-authentication ID. There is no requirement to use full authentication mechanism for the 1st tunnel establishment. 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 Subsequent tunnel establishment

Editor's note: From 3GPP TS 23.234: 'In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process (for example, a shorter re-authentication process should be used). This is ffs in Stage 3 work.'

8.2.1.5 Redirection

Editor's note: WLAN UE functionality to support redirection procedure as specified in 3GPP TS 23.234, clause 7.9.1.

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 dependant.

The PDG shall support IPSec tunnelling using IKEv2, in order to establish trusted relationships (i.e. mutual authentication with the WLAN UE).

The PDG shall support IPSec ESP [15] [AvT22]in order to provide secure tunnels between the WLAN UE and the PDG as specified in 3GPP TS 33.234 [5].

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.

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 Subsequent tunnel establishment

Editor's note: From 3GPP TS 23.234: 'In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process (for example, a shorter re-authentication process should be used). This is ffs in Stage 3 work.'

8.2.2.4 Redirection

Editor's note: PDG functionality to support redirection procedure as specified in 3GPP TS 23.234, clause 7.9.1.

8.3 Tunnel disconnection procedures

8.3.1 UE procedures

WLAN UE shall use the procedures defined in IKEv2 [14] to disconnect an IPSec tunnel to the PDG. The 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 SA.

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.

8.3.1.1 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 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

PDG shall use the procedures defined in IKEv2 [14] to disconnect an IPSec tunnel to the UE. The PDG shall close the incoming Security Associations associated with the tunnel and instruct the 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 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 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 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 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 UE; or

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

8.4 Timers and counters for tunnel management

~~Editor's note: it contains timers and counters that are not covered in IETF specifications but that are needed for the purposes of 3GPP IW~~

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 UE-3GPP AAA Server reauthentication procedure. In this way UE-PDG reauthentication, IKE Security Association and IPsec ESP Security Association timers are simultaneously reset.

8.5 Cause codes for tunnel management

Editor's note: it contains causes codes that are not covered in IETF specifications but that are needed for the purposes of 3GPP IW. For example when tunnel establishment failure reason is that the WLAN UE is not allowed to use a visited-PDG to access the given W-APN.