3GPP TSG CN Meeting #27 **NP-050079**
9th - 11th March 2005. Tokyo, Japan.

Source: **TSG CN WG1**

Title: **CRs to Rel-6 WI "WLAN" for TS 24.234**

Agenda item: **9.17**

Document for: **APPROVAL**

This document contains 2 **CRs on Rel-6 Work Item "WLAN"**, that have been agreed by TSG CN WG1 CN#37 meeting and forwarded to TSG CN Plenary meeting #27 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Ver	WI	Rel
N1-050352	PLMN selection for WLAN	24.234	19	1	B	6.1.1	WLAN	Rel-6
N1-050353	Correction of Abbreviation Usage	24.234	21	1	D	6.1.1	WLAN	Rel-6

3GPP TSG-CN1 Meeting #37
Sydney, Australia, 14-18 February 2005

Tdoc N1-050352
Revision of N1-50200

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **019** ⌘ **rev** **1** ⌘ Current version: **6.1.1** ⌘

*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:	⌘	PLMN selection for WLAN
Source:	⌘	Research In Motion
Work item code:	⌘	WLAN
Date:	⌘	16/2/2005
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:	⌘	In order to obtain the Supported PLMNs list for WLAN access for manual network selection the definition of an 'Alternative NAI' should be used.
Summary of change:	⌘	Addition of 'Alternative NAI' to enable WLAN UE to obtain list of Supported PLMNs list for WLAN access for manual network selection. In the clauses 4 revision of definition of NAI with addition of 'Alternative NAI' and the related usage of such different NAI types. In subclause 6 addition of Network discovery procedure for PLMN selection both automatic and manual, i.e. the capability to send to the WLAN UE the list of PLMN by WLAN when an 'Alternative NAI' is received.
Consequences if not approved:	⌘	The manual network selection will not work.

Clauses affected:	⌘	4.2 and 6.1.1

		Y	N			
Other specs affected:	⌘	Y		Other core specifications	⌘	CR 93 against TS 23.003
			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 Changes

4 General

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.

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 Root NAI

This is the NAI format ~~when~~ used by the WLAN UE when it attempts to authenticate~~s~~ directly to HPLMN (see draft-adrangi-eap-network-discovery [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.

4.2.3 Decorated NAI

This is the NAI format ~~when~~ used by the WLAN when it attempts to authenticate~~s~~ 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.

4.2.4 Alternative NAI

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

4.2.54 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].

End of First Changes

Second Changes

6 UE to 3GPP Network protocols

6.1 UE to 3GPP AAA Server protocols

6.1.1 WLAN Access Authentication and Authorization protocols

6.1.1.1 General

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

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

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

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

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

6.1.1.2 UE procedures

6.1.1.2.1 Identity management

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

The WLAN UE shall always use the leading digits notation when building the username part of NAI from IMSI, as specified in TS 23.003 [1A]. draft-arkko-pppext-eap-aka [9] and draft-haverinen-pppext-eap-sim [10] each define the leading digits to identify their particular authentication mechanism.

In the first EAP-Response/Identity message the WLAN UE shall include a NAI which username is derived from IMSI. The format of such username is defined in 3GPP TS 23.003 [1A]. The WLAN UE shall include the Root NAI or

Decorated NAI for authentication purposes. The WLAN UE shall include the Alternative NAI for manual network selection procedure.

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

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

6.1.1.2.2 User Identity Privacy

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

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

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

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

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

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

- if the temporary identity is a re-authentication identity, the WLAN UE shall store it in the "Re-authentication identity", data file in the USIM together with new Master Key, Transient EAP Keys and Counter value. If the "Re-authentication identity" data file is not available in the USIM, the WLAN UE shall store the re-authentication identity in the ME together with new Master Key, Transient EAP Key and Counter value.

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

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

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

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

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

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

End of Second Changes

3GPP TSG-CN1 Meeting #37
Sydney, Australia, 14-18 February 2004

Tdoc N1-050353

was Tdoc N1-050224

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **021** ⌘ **rev** **1** ⌘ Current version: **6.1.1** ⌘

*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:	⌘	Correction of Abbreviation Usage
Source:	⌘	Lucent Technologies
Work item code:	⌘	WLAN
Date:	⌘	17/01/2005
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:	⌘	A number of abbreviations are included in the main text of the specification, yet not included in the abbreviations list. Additionally, in many case of first usage, the abbreviation is not expanded.
Summary of change:	⌘	This CR corrects abbreviation listing and expansion of first usage consistently throughout the specification. The opportunity has also been taken to remove a number of hanging paragraphs, precluded by the drafting rules.
Consequences if not approved:	⌘	Less clarity in specification.

Clauses affected:	⌘	1, 3.1, 3.2, 3.3, 4.1, 4.3.1, 8.1, 8.2.1.1, 8.2.1.2, 8.2.2.1, 8.3.1, 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.

PROPOSED CHANGE

1 Scope

The present document specifies the network selection, including Authentication and Access Authorization using Authentication, Authorization and Accounting (AAA) procedures used for the interworking of the 3GPP System and WLANs. In addition to these, the present document also specifies the Tunnel management procedures used for establishing an end-to-end tunnel from the WLAN UE to the 3GPP network via the Wu reference point.

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

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

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. Packet Data Gateway (PDG), 3GPP AAA server and Wireless Access Gateway (WAG)) are covered in 3GPP TS 29.234 [3].

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 WLAN Specific Identifier ~~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 using the Universal Subscriber Identity Module (USIM) (see draft-arkko-pppext-eap-aka [9]).

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

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

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

Public Land Mobile Network (PLMN) selection: procedure for the selection of a PLMN, via a WLAN, either manually or automatically.

selected WSID: this is the WSID that has been selected according to clause 5.1, either manually or automatically.

selected PLMN: this is the PLMN that has been selected according to clause 5.2, either manually or automatically.

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

switch on: action of activating a WLAN UE client.

switch off: action of deactivating a WLAN UE client.

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

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.234 [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 [12] apply.

Decorated NAI
Root NAI

PROPOSED CHANGE

3.2 Symbols

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

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

PROPOSED CHANGE

3.3 Abbreviations

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

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

USIM	Universal Subscriber Identity Module
W-APN	WLAN - APN
WAG	Wireless Access Gateway
WLAN	Wireless Local Area Network
WSID	WLAN Specific Identifier

PROPOSED CHANGE

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 Universal Integrated Circuit Card (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.

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.

PROPOSED CHANGE

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 Available WSIDs. The list of Available WSIDs consists of all WSIDs found in passive scanning and all WSIDs received as a result of active scanning.

PROPOSED CHANGE

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~~ IPsec and IKEv2 are specified in 3GPP TS 33.234 [5].

PROPOSED 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 Domain Name System (DNS) procedure as mentioned in the subclause 8.3.1.2.

The WLAN UE shall support the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [14]) for ~~IPSec~~ 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~~ IPsec ESP (see draft-ietf-ipsec-esp-v3 [15]) in order to provide secure tunnels between the WLAN UE and the PDG as specified in 3GPP TS 33.234 [5].

PROPOSED CHANGE

8.2.1.2 Selection of remote tunnel endpoint

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

When performing W-APN resolution (i.e. building an Fully Qualified Domain Name (FQDN) for the DNS request), the WLAN UE shall include both W-APN Network Identifier (NI) and W-APN Operator Identifier (OI). If the user did not provide a value for W-APN OI, then the WLAN UE shall use the HPLMN ID or VPLMN ID as the W-APN OI, depending on internal configuration. 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 dependent.

PROPOSED 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 dependent.

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

PROPOSED CHANGE

8.3.1 UE procedures

8.3.1.1 General

WLAN UE shall use the procedures defined in the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [14]) to disconnect an ~~IPSec~~ 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.

8.3.1.2~~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.

PROPOSED CHANGE

8.3.2 PDG procedures

8.3.2.1 General

PDG shall use the procedures defined in the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [14]) to disconnect an IPSec tunnel to the 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.

8.3.2.21 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.