3GPP TSG CN Meeting #27 **NP-050080**
9th - 11th March 2005. Tokyo, Japan.

Source:	**TSG CN WG1**
Title:	**CR to Rel-6 WI “WLAN-IW” for TS 24.234**
Agenda item:	**9.17**
Document for:	**APPROVAL**

This document contains **CR on Rel-6 Work Item “WLAN-IW”**, that has 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
N1-050356	On 3GPP IP access independence	24.234	17	3	F	6.1.1	WLAN-IW

3GPP TSG-CN1 Meeting #37 **Tdoc N1-050356**
Sydney, Australia, 14-18 February 2004

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.234**	**CR**	17	⌘**rev**	**3**	⌘	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 ☒ Radio Access Network □ Core Network ☒

Title:	⌘	On 3GPP IP access independence		
Source:	⌘	Nokia		
Work item code:	⌘	WLAN-IW	***Date:*** ⌘	16/02/2005
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 independence of 3GPP IP Access is not explicit in the specification. It is the intention of this CR to remedy that
Summary of change:	⌘	Seperation of WLAN 3GPP IP Access from WLAN IP Direct Access in the specification.
Consequences if not approved:	⌘	Independence of WLAN 3GPP IP access from WLAN IP Direct Access is not explicit in the spec

Clauses affected:	⌘	Section 1, 8.1, 8.2.1.1 and 8.2.1.3				
		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.

**** Start of change #1 ****

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.

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

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].

**** End of change #1 ****

**** Start of change #2 ****

8 Tunnel management procedures

8.1 General

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

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

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

8.2 Tunnel establishment procedures

8.2.1 UE procedures

8.2.1.1 General

~~After successful EAP authentication and ~~B~~b~~efore 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]) 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 dependent.

8.2.1.3 UE initiated tunnel establishment

In order to request the establishment of a tunnel to a certain W-APN, the WLAN UE shall comply with IKE_v2 protocol definitions as defined in the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [14]). In order to set up an IKE connection between the 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 [14] to the PDG. On receipt of an IKE_SA_INIT response, the WLAN UE shall send a tunnel establishment request (IKE_AUTH request message defined in draft-ietf-ipsec-ikev2 [14]) to the selected PDG (see clause 8.2.1.2) including the W-APN and the NAI. The WLAN UE shall include in IDr payload the W-APN that was used in the DNS query and in the IDi payload the NAI.

NOTE1: The username part of the NAI included in IDi payload may be an IMSI, pseudonym or re-authentication ID. ~~There is no requirement to use full authentication mechanism for the 1st tunnel establishment.~~

NOTE2: Fast re-authentication mechanism is optional, and therefore is an implementation option in the WLAN UE and operator configuration issue (i.e. it also depends on whether the AAA server sent an re-authentication ID during previous EAP authentication) whether to use it during tunnel establishment.

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

- select a new PDG from the list received from the DNS server during remote tunnel endpoint selection (see clause 8.2.1.2) and initiate a new tunnel establishment using this newly selected PDG; or

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

- - stop the tunnel establishment attempt and release the Security Association (SA) with the PDG.

8.2.1.4 Void

8.2.1.5 Void

8.2.2 PDG procedures

8.2.2.1 General

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

The PDG shall support IPSec tunnelling using the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [14]), in order to establish trusted relationships (i.e. mutual authentication with the WLAN UE).

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

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 Void

8.2.2.4 Void

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.

8.3.2.1 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

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 Void

**** End of change #2 ****