3GPP TSG CT Meeting #28 **CP-050064**
1st – 3rd June 2005. Quebec, CANADA.

Source: **TSG CT WG1**

Title: **CRs on Rel-6 WI "WLAN" for TSs 24.234 and 24.229**

Agenda item: **9.17**

Document for: **APPROVAL**

This document contains 4 **CRs for Rel-6 WI "WLAN"**, that have been agreed by TSG CT WG1 meeting #38 and forwarded to TSG CT Plenary meeting #28 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Version	WI	Rel
C1-050725	Clarifications to network discovery & selection to enable successful inter-operator AAA	24.234	22	1	F	6.2.0	WLAN	Rel-6
C1-050727	Revision of definitions	24.234	24	1	F	6.2.0	WLAN	Rel-6
C1-050753	Limiting of IPsec SA per IKE SA in scenario 3	24.234	25	1	B	6.2.0	WLAN	Rel-6
C1-050729	I-WLAN information for IMS	24.229	872	2	B	6.6.0	WLAN	Rel-6

3GPP TSG-CT1 Meeting #38 **Tdoc C1-050725**
Cancun, Mexico, 25th to 29th April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘	24.234	CR	22	⌘ rev	1	⌘	Current version:	6.2.0	⌘

*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: ⌘	Clarifications to network discovery & selection to enable successful inter-operator AAA		
Source: ⌘	Vodafone, TeliaSonera		
Work item code: ⌘	WLAN	***Date:*** ⌘	27/04/2005
Category: ⌘	**F**	***Release:*** ⌘	Rel-6

Use <u>one</u> 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 <u>one</u> 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 GRX is the inter-PLMN IP backbone network for PLMNs. It is totally separate from the Internet and as such has it's own, **totally separate** DNS "tree". Please see 3GPP TS 23.003 Annex D for more information on DNS on the GRX.

As such, in order for a 3GPP AAA Proxy (located in the VPLMN) to route AAA messaging to/from the 3GPP AAA Server (located in the HPLMN) an agreed naming convention for NAI realms needs to be agreed. Given that the IETF state that realms must be of the form of a domain name and that domain name must be owned by the organisation using it as a realm, CT4, in collaboration with the GSMA (the standards body in charge of allocation of domain names on the GRX) have defined NAI realms (excluding the Alternative NAI realm – which needs to be unroutable) to be of the form "wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org".

Also, there is some text in clause 4 which duplicates information already mandated in other WLAN related specifications. 3GPP documentation relies on having stage 1, stage 2 and stage 3 and **all stages should be read together** to implement the WLAN WI Therefore, duplication is not necessary.

Summary of change: ⌘

Section 4.1:

- First paragraph removed as this information is already stated in the WLAN stage 2 (3GPP TS 23.234 – section 6).
- Minor textual enhancements to aid readability.

Section 4.2.1:

- NAIs are defined in 3GPP TS 23.003 so re-stating in this specification the format and structure is duplication of specification. Therefore, only a reference to 3GPP TS 23.003 is required here.

Sections 4.2.2, 4.2.3, 4.2.4, 4.2.5:

- Minor textual enhancements to aid readability.

Sections 4.3.1 and 4.3.2:

- Removal of verbiage from the beginning of section headings.
- Minor textual enhancements to aid readability.

Section 4.4.1:

- First paragraph slightly re-worded to describe triggering procedure from the WLAN UE's perspective.
- Minor textual enhancements

Section 4.4.2:

- Minor textual enhancements.

Section 7.7:

- The Supplorted PLMNs list for WLAN access is refined to explicitly state the format of individual realms returned in the "realm-list" of an EAP message (as defined in draft-adrangi-eap-network-discovery-and-selection).

Section 7.8:

- Minor textual corrections.

Consequences if not approved: ⌘ In the WLAN roaming scenario, AAA messaging (both RADIUS and Diameter) will not be routable to the HPLMN, resulting in failure of AAA and consequently failure of WLAN access.

Also, current duplication of specification will eventually lead to divergence of specification which in turns leads to different implementations that do not inter-work.

Clauses affected: ⌘ 4.1, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.3.1, 4.3.2, 4.4.1, 4.4.2, 7.7, 7.8

		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 ******

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.~~

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

~~The Wa and Wd reference points are defined in 3GPP TS 23.234 [2].~~ The WLAN-UE is equipped with a~~n~~ 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.

4.2 WLAN UE Identities

4.2.1 General

WLAN UEs use Network Access Identifier (NAI) as identification towards the 3GPP WLAN AAA server in the EAP Response/Identity message. The NAI is structured according to 3GPP TS 23.003 [1A]~~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 used by the WLAN UE when it attempts to authenticate directly to HPLMN (see draft-adrangi-eap-network-discovery [12] and 3GPP TS 23.234 [2]). The Root NAI format is specified in 3GPP TS 23.003 [1A]. The usage of the Root NAI is specified in clause 5.

4.2.3 Decorated NAI

This is the NAI format used by the WLAN UE when it attempts to authenticate to HPLMN via VPLMN (see draft-adrangi-eap-network-discovery-and-selection-00 [12]). The Decorated NAI format is specified in 3GPP TS 23.003 [1A]. The usage of the Decorated NAI is specified in clause 5.

4.2.4 Alternative NAI

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

4.2.5 Username

The generation of, and the rules for the use of the username part of an NAI ~~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 the username part of an 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~~For IEEE 802.11 [11] WLANs, the WLAN network name is provided in the SSID information element.

The WLAN UE becomes aware of the supported WSIDs ~~by~~of the WLAN by performing scanning procedures as specified in IEEE 802.11-1999 [11].

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

i) Passive scanning.

ii) Active scanning.

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

In order to assist PLMN selection procedure, the WLAN UE shall create~~s~~ a list of ~~A~~available WSIDs. The list of ~~A~~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 o~~Other WLAN technologies

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

4.4 Network discovery

4.4.1 General

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

If the I-WLAN is unable to route the WLAN UE's EAP authentication signalling to the 3GPP AAA ~~S~~server based on the NAI sent in the initial EAP-Response/Identity message and if the local AAA supports Identity selection hints for EAP procedure as described in draft-adrangi-eap-network-discovery [12], then the I-WLAN sends a subsequent EAP-Request/Identity message to the WLAN UE including the Supported PLMNs list for WLAN access.

If the I-WLAN is unable to route the WLAN UE's EAP authentication signalling to the 3GPP AAA s~~S~~erver based on the NAI sent in the initial EAP-Response/Identity message and if the local AAA does not support Identity selection hints for EAP procedure as described in draft-eap-network-discovery [12], then the I-WLAN sends an EAP-Failure message to the WLAN UE.

4.4.2 UE procedures

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

- Perform PLMN selection according to clause 5.2.

- Use the Decorated NAI as specified in clause 4.2 and using the PLMN ID of the Selected PLMN.

- Attempt to authenticate as specified in clause 6.1.1 and using the NAI determined in the prior step.

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

****** Last Modified Section ******

7 Parameters coding

7.1 General

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

7.2 Pseudonym

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

7.3 Void

7.4 User Controlled PLMN Selector for WLAN access

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

7.5 Operator Controlled PLMN Selector for WLAN access

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

7.6 User Controlled WLAN Specific Identifier list

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

7.6a Operator Controlled WLAN Specific Identifier list

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

7.7 Supported PLMNs list for WLAN access

The "Supported PLMNs list for WLAN access" file contains a list of PLMN codes of roaming partners (i.e. to which the WLAN operator has a direct roaming relationship). This list is per WSID and the WLAN UE ~~may~~ shall store it for further use. The list shall be deleted at WLAN UE switch off. The UE shall structure ~~format of~~ this list as per the "realm-list" ~~is~~ specified in draft-adrangi-eap-network-discovery-and-selection [12] and each "realm" in the "realm-list" shall be of the form of a home network domain name as defined in sub-clause 14.2 of 3GPP TS 23.003 [1A].

7.8 Re-authentication identity

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

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050727

was Tdoc C1-050569

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.234**	**CR**	**24**	⌘**rev**	**1**	⌘	Current version:	**6.2.0**	⌘

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:	⌘	Revision of definitions		
Source:	⌘	Lucent Technologies		
Work item code:	⌘	WLAN	***Date:*** ⌘	14/04/2005
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:	⌘	A number of functional entities rely for their definition on material in 23.234. Since this text was drafted, those functional entities have been defined in the generic 3GPP architecture document, and therefore it is more appropriate to refer to the definitions in 23.002. 23.002 itself refers to 23.234 for additional material and operation, so a link does still exist to 23.234 when this change is made.
Summary of change:	⌘	Definitions of key functional entities are made by reference to 23.002, rather than 23.234. Abbreviation of WAG is removed, as it is not used in 24.234 Final paragraph of scope is removed as it contains an error, and decided that scopes are not really the place to identify what is not in this specification.
Consequences if not approved:	⌘	This change has no technical impact on the WLAN operation.

Clauses affected:	⌘	1, 2, 3.1, 3.3				
		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.

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.

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

PROPOSED 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".

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

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

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

[4] Void

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

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

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

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

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

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

[11] IEEE Std 802.11 (1999): "Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan Area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications".

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

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

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

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

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 (WSID) by for probing it

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

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

EAP AKA: EAP mechanism for authentication and session key distribution using the UMTS AKA authentication mechanism using the Universal Subscriber Identity Module (USIM) (see draft-arkko-pppext-eap-aka [9]).

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

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

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

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

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

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

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

switch on: action of activating a WLAN UE client.

switch off: action of deactivating a WLAN UE client.

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

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

WLAN UE

3GPP AAA proxy

3GPP AAA server

Packet Data Gateway (PDG)

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

3GPP - WLAN Interworking (WLAN-3GPP IW)

~~**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

3.3 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

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050729

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**872**	⌘ **rev**	**2**	⌘ Current version:	**6.6.0** ⌘

*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:	⌘	I-WLAN information for IMS		
Source:	⌘	Nokia, Lucent		
Work item code:	⌘	WLAN	***Date:*** ⌘	27/04/2005
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: ⌘

According to the CT plenary exceptions, IMS over WLAN description is a requirement for Rel-6 and we have an extension to get it included.
The purpose of this CR is to accomplish this vis modifications to 3GPP TS 24.229
The technical assumptions behind this proposal are as follows:

- access to IMS is IPv6 only;
- only one WLAN tunnel is available for IMS access, and this tunnel is assumed to be used in the same manner as a general purpose PDP context;
- No specific QoS functionality is available
- P-CSCF discovery is performed using DHCP only;
- media grouping is not available;
- service based local policy and use of the media authorization token is not available;
- there is no WLAN specific coding of the P-Access-Network-ID header beyond identification of the access technology;
- there are no WLAN specific charging parameters carried to IMS.
- only 802.11a and 802.11b are supported in the coding, as these are the currently defined values in RFC 3455

Summary of change: ⌘

A new annex X is created documenting I-WLAN access technology specific procedures. Descriptions of how P-Access-Network-Info and P-Charging-Info headers are treated for the varying access technologies are added back into the main body of the text in sections used in Rel-5 (sections 7.2A.4 & 7.2A.5)), and

		the text aligned where appropriate with the original release 5 text. The GPRS IP CAN case description for these headers that was in Annex B is included there and removed from Annex B. Appropriate references are included in the main body of the text to this new document structure and
Consequences if not approved:	⌘	IMS usage over I-WLAN not described in Rel-6 specifications

Clauses affected:	⌘	2, 3.2, 3.2. 5.1.1.2, 5.1.1.3, 5.1.1.4, 5.1.1.6, 5.1.2A.1, 5.1.2A.2, 7.2A.4, 7.2A5, annex B.4.1, B.3.3.1, annex X added.				
		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 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

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

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".

[6] 3GPP TS 23.221: "Architectural requirements".

[7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[7A] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[8A] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8B] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8C] 3GPP TS 24.234: "3GPP System to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3".

[9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[9A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".

[10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[11A] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".

[11B] 3GPP TS 29.163: "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks".

[11C] 3GPP TS 29.161: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services with Wireless Local Access and Packet Data Networks (PDN "

[12] 3GPP TS 29.207: "Policy control over Go interface".

[13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[13A] 3GPP TS 29.209: "Policy control over Gq interface".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

[16] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[17] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

[18] 3GPP TS 33.102: "3G Security; Security architecture".

[19] 3GPP TS 33.203: "Access security for IP based services".

[19A] 3GPP TS 33.210: "IP Network Layer Security".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[20A] RFC 2401 (November 1998): "Security Architecture for the Internet Protocol".

[20B] RFC 1594 (March 1994): "FYI on Questions and Answers to Commonly asked "New Internet User" Questions".

[20C] RFC 2403 (November 1998) "The Use of HMAC-MD5-96 within ESP and AH".

[20D] RFC 2404 (November 1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[20E] RFC 2462 (November 1998): "IPv6 Address Autoconfiguration".

[21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 3966 (December 2004): "The tel URI for Telephone Numbers".

[23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 3761 (April 2004): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[25] RFC 2976 (October 2000): "The SIP INFO method".

[25A] RFC 3041 (January 2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[26] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[27] RFC 3262 (June 2002): "Reliability of provisional responses in Session Initiation Protocol (SIP)".

[28] RFC 3265 (June 2002): "Session Initiation Protocol (SIP) Specific Event Notification".

[29] RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".

[30] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".

[31] RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".

[32] RFC 3320 (March 2002): "Signaling Compression (SigComp)".

[33] RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[34] RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".

[34A] RFC 3326 (December 2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".

[35] RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method".

[37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag".

[38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[39] draft-ietf-mmusic-sdp-new-13 (May 2003): "SDP: Session Description Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[40] RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[42] RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)".

[43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[51] Void.

[52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[53] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".

[54] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows".

[55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".

[56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[56A] RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[56B] RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)"

[57] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[58] draft-ietf-sip-session-timer-15 (November 2004): "Session Timers in the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[59] RFC 3892 (September 2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".

[60] RFC 3891 (September 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

[61] RFC 3911 (October 2004): "The Session Inititation Protocol (SIP) "Join" Header".

[62] RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

[63] RFC 3861 (August 2004): "Address Resolution for Instant Messaging and Presence".

[64] draft-ietf-sip-rfc3312-update-03 (September 2004): "Update to the Session Initiation Protocol (SIP) Preconditions Framework".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[70] RFC 3903 (October 2004): "An Event State Publication Extension to the Session Initiation Protocol (SIP)".

[71] Void.

[72] RFC 3857 (August 2004): "A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)".

[74] RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[75] draft-ietf-simple-event-list-04 (June 2003): "A Session Initiation Protocol (SIP) Event Notification Extension for Collections".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[77] draft-ietf-sipping-config-framework-05 (October 2004): "A Framework for Session Initiation Protocol User Agent Profile Delivery".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[78] draft-ietf-sipping-conference-package-03 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Conference State"

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[79] draft-ietf-rohc-sigcomp-sip-01 (February 2004): "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

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

-------------------- NEXT CHANGE-----------------

3.1 Definitions

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

Newly established set of security associations: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF after the 200 (OK) response to a REGISTER request was received.

Old set of security associations: Two pairs of IPsec security associations still in existence after another set of security associations has been established due to a successful authentication procedure.

Temporary set of security associations: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF, after an authentication challenge within a 401 (Unauthorized) response to a REGISTER request was received. The SIP level lifetime of such created security associations will be equal to the value of reg-await-auth timer.

Integrity protected: See 3GPP TS 33.203 [19]. Where a requirement exists to send information "integrity protected" the mechanisms specified in 3GPP TS 33.203 [19] are used for sending the information. Where a requirements exists to check that information was received "integrity protected", then the information received is checked for compliance with the procedures as specified in 3GPP TS 33.203 [19].

For the purposes of the present document, the following terms and definitions given in RFC 1594 [20B].

Fully-Qualified Domain Name (FQDN)

For the purposes of the present document, the following terms and definitions given in RFC 3261 [26] apply (unless otherwise specified see clause 6).

Back-to-Back User Agent (B2BUA)
Client
Dialog
Final response
Header
Header field
Loose routeing
Method
Option-tag (see RFC 3261 [26] subclause 19.2)
Provisional response
Proxy, proxy server
Redirect server
Registrar
Request
Response
Server
Session
(SIP) transaction
Stateful proxy
Stateless proxy
Status-code (see RFC 3261 [26] subclause 7.2)
Tag (see RFC 3261 [26] subclause 19.3)
Target Refresh Request
User agent client (UAC)
User agent server (UAS)
User agent (UA)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2] subclause 4.1.1.1 and subclause 4a.7 apply:

Breakout Gateway Control Function (BGCF)
Call Session Control Function (CSCF)
Home Subscriber Server (HSS)
Media Gateway Control Function (MGCF)
Multimedia Resource Function Controller (MRFC)
Multimedia Resource Function Processor (MRFP)
Subscription Locator Function (SLF)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.218 [5] subclause 3.1 apply:

Filter criteria
Initial filter criteria
Initial request
Standalone transaction
Subsequent request

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclauses 3.1, 4.3.3.1, 4.3.6, 4.6 and 5.4.12.1 apply:

Interrogating-CSCF (I-CSCF)
IMS Application Level Gateway (IMS-ALG)
IP-Connectivity Access Network (IP-CAN)
Policy Decision Function (PDF)
Private user identity
Proxy-CSCF (P-CSCF)
Public Service Identity (PSI)
Public user identity
Serving-CSCF (S-CSCF)
Statically pre-configured PSI

For the purposes of the present document, the following terms and definitions given in 3GPP TR 33.203 [19] apply:

IM Subscriber Identity Module (ISIM)
Protected server port
Protected client port

For the purposes of the present document, the following terms and definitions given in 3GPP TR 21.905 [1] apply:

Universal Integrated Circuit Card (UICC)
Universal Subscriber Identity Module (USIM)
User Equipment (UE)

For the purposes of the present document, the following terms and definitions given in RFC 2401 [20A] Appendix A apply:

Security association

NOTE: A number of different security associations exist within the IM CN subsystem. Within this document the term specifically applies to the security association that exists between the UE and the P-CSCF, as this is the only security association that has direct impact on SIP.

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

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

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.234 [7A] apply.

Interworking WLAN

For the purposes of the present document, the following terms and definitions given in ITU-T E.164 [57] apply:

International public telecommunication number

------------------- NEXT CHANGE-----------------

3.2 Abbreviations

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

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AAA	Authentication, Authorization and Accounting
AS	Application Server
APN	Access Point Name
AUTN	Authentication TokeN

B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
c	conditional
CCF	Charging Collection Function
CDR	Charging Data Record
CK	Ciphering Key
CN	Core Network
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTD	Document Type Definition
ECF	Event Charging Function
FQDN	Fully Qualified Domain Name
GCID	GPRS Charging Identifier
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
HSS	Home Subscriber Server
i	irrelevant
I-CSCF	Interrogating CSCF
ICID	IM CN subsystem Charging Identifier
IK	Integrity Key
IM	IP Multimedia
IMS	IP Multimedia core network Subsystem
IMS-ALG	IMS Application Level Gateway
IMSI	International Mobile Subscriber Identity
IOI	Inter Operator Identifier
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC	IP Multimedia Subsystem Service Control
ISIM	IM Subscriber Identity Module
I-WLAN	Interworking – WLAN
m	mandatory
MAC	Message Authentication Code
MCC	Mobile Country Code
MGCF	Media Gateway Control Function
MGW	Media Gateway
MNC	Mobile Network Code
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
PDG	Packet Data Gateway
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
n/a	not applicable
NAI	Netework Access Identifier
o	optional
P-CSCF	Proxy CSCF
PDU	Protocol Data Unit
PSI	Public Service Identity
QoS	Quality of Service
RAND	RANDom challenge
RES	RESponse
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SQN	SeQuence Number

UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UDVM	Universal Decompressor Virtual Machine
USIM	Universal Subscriber Identity Module
WLAN	Wireless Local Area Network
x	prohibited
XMAC	expected MAC
XML	eXtensible Markup Language

-------------------- NEXT CHANGE------------------

3A Interoperability with different IP-CAN

The IM CN subsystem can be accessed by UEs resident in different types of IP-CAN. The main body of this document, and annex A, are general to UEs and IM CN subsystems that are accessed using any type of IP-CAN. Requirements that are dependent on the type of IP-CAN are covered in annexes B and X~~,~~ or in separate specifications.

-------------------- NEXT CHANGE------------------

5.1.1.2 Initial registration

The UE can register a public user identity with its contact address at any time after it has aquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

A REGISTER request may be protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field, set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be registered;

c) a To header set to the SIP URI that contains the public user identity to be registered;

d) a Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) an Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Security-Client header field set to specify the security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];

i) the Supported header containing the option tag "path"; and

j) if a security association exists, a P-Access-Network-Info header set as specified for the access network technology ~~(for GPRS see subclause B.3).~~ (see subclause 7.2A.4).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;

d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;

e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

f) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

5.1.1.3 Initial subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680 [43].

The UE shall use the default public user identiy for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initial registration is not barred.

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header set to a SIP URI that contains the public user identity used for subscription;

c) a To header set to a SIP URI that contains the public user identity used for subscription;

d) an Event header set to the "reg" event package;

e) an Expires header set to 600 000 seconds as the value desired for the duration of the subscription

f) a P-Access-Network-Info header set as specified for the access network technology ~~(for GPRS see subclause B.3)~~(see subclause 7.2A.4); and

g) a Contact header set to contain the same IP address or FQDN, and with the protected server port value as in the initial registration.

Upon receipt of a 2xx response to the SUBSCRIBE request, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header of the received response.

If continued subscription is required, the UE shall automatically refresh the subscription by the reg event package, for a previously registered public user identity, either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less.

5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity with its contact address at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 [62].

The UE shall protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if IK is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be registered;

c) a To header set to the SIP URI that contains the public user identity to be registered;

d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

i) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication;

j) the Supported header containing the option tag "path"; and

k) the P-Access-Network-Info header set as specified for the access network technology ~~(for GPRS see subclause B).~~(see subclause 7.2A.4)

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the new expiration time of the registration for this public user identity found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

d) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

When the timer F expires at the UE, the UE shall:

1) stop processing of all ongoing dialogs and transactions and silently discard them locally; and

2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2, the UE may:

   a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1;

   b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1; and

   c) perform the procedures for initial registration as described in subclause 5.1.1.2.

NOTE 4: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

After a maximum of 5 consecutive initial registration attempts, the UE shall not automatically attempt any further initial registration for an implementation dependant time of at least 30 minutes.

-------------------- NEXT CHANGE------------------

5.1.1.6 User-initiated deregistration

The UE can deregister a public user identity that it has previously registered with its contact address at any time.

The UE shall integrity protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if one is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field, set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be deregistered;

c) a To header set to the SIP URI that contains the public user identity to be deregistered;

d) a Contact header set to either the value of "*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and the protected server port value bound to the security association;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

f) an Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;

g) a Request-URI set to the SIP URI of the domain name of the home network; and

h) a P-Access-Network-Info header set as specified for the access network technology ~~(for GPRS see subclause B.3~~ (see subclause 7.2A.4~~see subclause X.1~~).

On receiving the 200 (OK) response to the REGISTER request, the UE shall remove all registration details relating to this public user identity.

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the IM CN subsystem.

If all public user identities are deregistered and the security association is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

NOTE: When the UE has received the 200 (OK) response for the REGISTER request of the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered), the UE removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

-------------------- NEXT CHANGE------------------

5.1.2A.1 Mobile-originating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request, the UE shall:

- include the protected server port in the Via header entry relating to the UE; and
- include the protected server port in any Contact header that is otherwise included.

The UE shall discard any SIP response that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

In accordance with RFC 3325 [34] the UE may insert a P-Preferred-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity within the IM CN subsystem. The UE may include any of the following in the P-Preferred-Identity header:

- a public user identity which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration that was not subsequently deregistered or has expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 1: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header.

NOTE 2: Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header.

NOTE 3: A number of headers can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other headers that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of headers.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set the From header to "Anonymous".

NOTE 4: The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user should include the value "Anonymous" whenever privacy is explicitly required. As the user may well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header from the public user identity or other values stored in or derived from the UICC. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header other than Anonymous.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

The UE shall insert a P-Access-Network-Info header into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method. The UE shall populate the P-Access-Network-Info header with the current point of attachment to the IP-CAN as specified for the access network technology (~~for GPRS see subclause B.~~ see subclause 7.2A.4~~3~~).

NOTE 5: During the dialog, the points of attachment to the IP-CAN of the UE may change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected server port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 6: It is an implementation option whether these actions are also triggered by other means.

5.1.2A.2 Mobile-terminating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any response, the UE shall:

- include the protected server port in any Contact header that is otherwise included.

The UE shall discard any SIP request that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

NOTE 1: In the mobile-terminating case, this version of the document makes no provision for the UE to provide an P-Preferred-Identity in the form of a hint.

NOTE 2: A number of headers can reveal information about the identity of the user. Where, privacy is required, implementers should also give consideration to other headers that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of headers.

The UE shall insert a P-Access-Network-Info header into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method. The UE shall populate the P-Access-Network-Info header with its current point of attachment to the IP-CAN as specified for the access network technology (~~for GPRS see subclause B.~~ see subclause 7.2A.4~~3~~).

-------------------- NEXT CHANGE------------------

7.2A.4 ~~Void~~ P-Access-Network-Info header

7.2A4.1 Introduction

The P-Access-Network-Info header is extended to include specific information relating to particular access technologies.

7.2A4.2 Syntax

The syntax of the P-Access-Network-Info header is described in RFC 3455 [52].

7.2A4.3 Additional coding rules for P-Access-Network-Info header

The UE shall populate the P-Access-Network-Info header, where use is specified in subclause 5.1, with the following contents:

1) the access-type field set to one of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-CDMA2000", "IEEE-802.11a" or "IEEE-802.11b" as appropriate to the radio access technology in use.

2) if the access type field is set to "3GPP-GERAN", a cgi-3gpp parameter set to the Cell Global Identity obtained from lower layers of the UE. The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "cgi-3gpp" parameter is therefore coded as a text string as follows:

   Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation);

3) if the access type field is equal to "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and UMTS Cell Identity (fixed length code of 28 bits).

4) if the access-type field set to one of "IEEE-802.11a" or "IEEE-WLAN-802.11b" the access info parameter is set to a null value. This release of this specification does not define values for use in this parameter

-------------------- NEXT CHANGE------------------

7.2A.5 P-Charging-Vector header

7.2A.5.1 Introduction

The P-Charging-Vector header field is extended to include specific charging correlation information needed for IM CN subsystem functional entities.

7.2A.5.2 Syntax

7.2A5.2.1 General

The syntax of the P-Charging-Vector header field is described in RFC 3455 [52]. There may be additional coding rules for this header depending on the type of IP-CAN, according to access technology specific descriptions.

Table 7.3 describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52].

Table 7.3: Syntax of extensions to P-Charging-Vector header

```
   access-network-charging-info = (gprs-charging-info / i-wlan-charging-info / generic-param)
   gprs-charging-info = ggsn SEMI auth-token [SEMI pdp-info-hierarchy] *(SEMI extension-param)
   ggsn = "ggsn" EQUAL gen-value
   pdp-info-hierarchy = "pdp-info" EQUAL LDQUOT pdp-info *(COMMA pdp-info) RDQUOT
   pdp-info = pdp-item SEMI pdp-sig SEMI gcid [SEMI flow-id]
   pdp-item = "pdp-item" EQUAL DIGIT
   pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
   gcid = "gcid" 1*HEXDIG
   auth-token = "auth-token" EQUAL 1*HEXDIG
   flow-id = "flow-id" EQUAL "(" "{" 1*DIGIT COMMA 1*DIGIT "}" *(COMMA "{" 1*DIGIT COMMA 1*DIGIT
        "}")")"
   extension-param = token [EQUAL token]
   i-wlan-charging-info = "pdg"
```

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.

The access-network-charging-info parameter includes alternative definitions for different types access networks. The description of these parameters are given in the subsequent subclauses.

The access network charging information is not included in the P-Charging-Vector for SIP signalling that is not associated with a session.

When the access network charging information is included in the P-Charging-Vector and necessary information is not available from the Go/Gq interface reference points then null or zero values are included

7.2A5.2.2 GPRS as IP-CAN

GPRS is the initially supported access network (gprs-charging-info parameter). For GPRS there are the following components to track: GGSN address (ggsn parameter), media authorization token (auth token parameter), and a pdp-info parameter that contains the information for one or more PDP contexts. The pdp-info contains one or more pdp-item values followed by a collection of parameters (pdp-sig, gcid, and flow-id). The value of the pdp-item is a unique number that identifies each of the PDP-related charging information within the P-Charging-Vector header. Each PDP context has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig parameter), an associated GPRS Charging Identifier (gcid parameter), and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the PDP context charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.207 [12] Annex C. The gcid, ggsn address and flow-id parameters are transferred from the GGSN to the P-CSCF via the PDF over the Go interface (see 3GPP TS 29.207 [12]) and Gq interface (see 3GPP TS 29.209 [13A]).

The gcid value is received in binary format at the P-CSCF (see 3GPP TS 29.207 [12]). The P-CSCF shall encode it in hexadecimal format before include it into the gcid parameter. On receipt of this header, a node receiving a gcid shall decode from hexadecimal into binary format.

The access network charging information is not included in the P-Charging-Vector for SIP signalling may not be available for sessions that use a general purpose PDP context (for both SIP signalling and media) or that do not require media authorisation.

7.2A5.2.3 I-WLAN as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.

This version of the specification defines the use of "pdg" for inclusion in the P-Charging-Vector header. No other extensions are defined for use in I-WLAN in this version of the specification.

-------------------- NEXT CHANGE------------------

9.2.2 Handling of the IP-CAN

The UE shall ensure that appropriate resources are available for the media flow(s) on the IP-CAN(s) related to a SIP-session. The means to ensure this is dependant on the characteristics for each IP-CAN, and is described separately for each IP-CAN in question.

GPRS is described in annex B. I-WLAN is described in annex X.

-------------------- NEXT CHANGE------------------

B.3.1.1 ~~Additional coding rules for P-Access-Network-Info header~~Void

.~~The UE shall populate the P-Access-Network-Info header, where use is specified in subclause 5.1, with the following contents:~~

1) ~~the access-type field set to one of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000" as appropriate to the radio access technology in use;~~

2) ~~if the access type field is set to "3GPP-GERAN", a cgi-3gpp parameter set to the Cell Global Identity obtained from lower layers of the UE. The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "cgi-3gpp" parameter is therefore coded as a text string as follows:~~

   ~~Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation);~~

3) ~~if the access type field is equal to "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:~~

   ~~Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and UMTS Cell Identity (fixed length code of 28 bits).~~

-------------------- NEXT CHANGE------------------

B.4.1 ~~P-Charging-Vector header~~Void

~~The access network charging information is populated in the P-Charging-Vector using the gprs-charging-info parameter. Table B.1 describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52]~~.

~~Table B.1: Syntax of extensions to P-Charging-Vector header~~

```
~~   access-network-charging-info = (gprs-charging-info / generic-param)~~
~~   gprs-charging-info = ggsn SEMI auth-token [SEMI pdp-info-hierarchy] *(SEMI extension-param)~~
~~   ggsn = "ggsn" EQUAL gen-value~~
~~   pdp-info-hierarchy = "pdp-info" EQUAL LDQUOT pdp-info *(COMMA pdp-info) RDQUOT~~
~~   pdp-info = pdp-item SEMI pdp-sig SEMI gcid [SEMI flow-id]~~
~~   pdp-item = "pdp-item" EQUAL DIGIT~~
~~   pdp-sig = "pdp-sig" EQUAL ("yes" / "no")~~
~~   gcid = "gcid" 1*HEXDIG~~
~~   auth-token = "auth-token" EQUAL 1*HEXDIG~~
~~   flow-id = "flow-id" EQUAL "(" "{" 1*DIGIT COMMA 1*DIGIT "}" *(COMMA "{" 1*DIGIT COMMA 1*DIGIT~~
~~        "}")")"~~
~~   extension-param = token [EQUAL token]~~
```

~~The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.~~

~~The access-network-charging-info parameter includes alternative definitions for different types access networks.~~

~~GPRS is the initially supported access network (gprs-charging-info parameter). For GPRS there are the following components to track: GGSN address (ggsn parameter), media authorization token (auth token parameter), and a pdp-info parameter that contains the information for one or more PDP contexts. The pdp-info contains one or more pdp-item values followed by a collection of parameters (pdp-sig, gcid, and flow-id). The value of the pdp-item is a unique number that identifies each of the PDP-related charging information within the P-Charging-Vector header. Each PDP context has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig parameter), an associated GPRS Charging Identifier (gcid parameter), and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the PDP context charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.207 [12] Annex C. The gcid, ggsn address and flow-id parameters are transferred from the GGSN to the P-CSCF via the PDF over the Go interface (see 3GPP TS 29.207 [12]) and Gq interface (see 3GPP TS 29.209 [13A]).~~

~~The gcid value is received in binary format at the P-CSCF (see 3GPP TS 29.207 [12]). The P-CSCF shall encode it in hexadecimal format before include it into the gcid parameter. On receipt of this header, a node receiving a gcid shall decode from hexadecimal into binary format.~~

~~The access network charging information is not included in the P-Charging-Vector for SIP signalling that is not associated with a session, and may not be available for sessions that use a general purpose PDP context (for both SIP signalling and media) or that do not require media authorisation.~~

~~When the access network charging information is included in the P-Charging-Vector and necessary information is not available from the Go/Gq interface reference points then null or zero values are included.~~

-------------------- NEXT CHANGE------------------

Annex X (normative): IP-Connectivity Access Network specific concepts when using I-WLAN to access IM CN subsystem

X.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is Wireless LAN Interworking (I-WLAN).

X.2 I-WLAN aspects when connected to the IM CN subsystem

X.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by I-WLAN to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause. Requirements for the PDG in support of this communication are specified in 3GPP TS 29.161 [11C]. When using the I-WLAN, the IP-CAN bearer is provided by an I-WLAN tunnel.

X.2.2 Procedures at the UE

X.2.2.1 I-WLAN tunnel activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

a) Perform I-WLAN network selection i.e. gaining 3GPP Direct access as described in 3GPP TS 24.234 [8C] in the access dependent case;

b) Establish an I-WLAN tunnel with the PDG according to the W-APN and PDG selection criteria described in 3GPP TS 24.234 [8C]. The I-WLAN tunnel shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration.;

The I-WLAN tunnel shall carry both signalling and media i.e. it shall be a general-purpose. I-WLAN tunnel.

Note: Only one I-WLAN tunnel is available therefore no dedicated I-WLAN tunnel for signalling is possible.

c) Acquire a P-CSCF address(es).

The method for P-CSCF discovery is:

Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] as described in subclause 9.2.1.

If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

The UE may request a DNS Server IPv6 address(es) via RFC 3315 [40]

X.2.2.2 I-WLAN tunnel procedures

X.2.2.2.1 General requirements

The UE can establish media streams that belong to different SIP sessions on the same I-WLAN tunnel.

X.2.2.2.2 Usage of I-WLAN tunnel for media

The UE may freely group media streams to the existing I-WLAN tunnel in case no indication of grouping of media streams is received from the P-CSCF.

If the UE receives media grouping attributes in accordance with RFC 3524[54] that it cannot provide within a single I-WLAN tunnel, then the UE shall handle such SDP offers in accordance with RFC 3388[53].

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, the UE shall reuse the existing I-WLAN tunnel and ignore the media authorization token.

X.2.2.2.3 Special requirements applying to forked responses

Since the UE is unable to perform bearer modification, forked responses place no special requirements on the UE.

.------------------- NEXT CHANGE------------------

3GPP TSG-CT1 Meeting #38 **Tdoc C1-050753**
Cancun, Mexico, 25-29 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234**	**CR** **25**	⌘**rev**	**1**	⌘	Current version:	**6.2.0** ⌘

*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:	⌘	Limiting of IPsec SA per IKE SA in scenario 3		
Source:	⌘	Nokia		
Work item code:	⌘	WLAN	***Date:*** ⌘	22/04/2005
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:	⌘	SA3 have mandated that only one IPSec SA is allowed per IKE SA. In the 3GPP IP Access Scenario. This CR seeks to build that limitation into the specification without losing the optional inband rekeying permitted in the IKE_v2 spec. It is necessary to specify how the stage 2 requirement for one IPSec SA per IKE SA is built into the spec.
Summary of change:	⌘	Added text to section 8.2.2.1
Consequences if not approved:	⌘	Spec does not disallow multiple IPSec SA per IKE SA which is not permitted by stage 2

Clauses affected:	⌘	8.2.2.1				
		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 CHANGE------------------

8 Tunnel management procedures

8.1 General

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

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

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

8.2 Tunnel establishment procedures

8.2.1 UE procedures

8.2.1.1 General

Before initiation of tunnel establishment the WLAN UE shall offer the possibility to the subscriber to select between direct access to external IP network from the WLAN or access through the PLMN. In case the user selects to access through the PLMN, the WLAN UE shall initiate the Tunnel Establishment procedure after selecting a remote tunnel endpoint using Domain Name System (DNS) procedure as mentioned in the subclause 8.3.1.2.

The WLAN UE shall support the IKEv2 protocol (see draft-ietf-ipsec-ikev2 [14]) for IPsec tunnel negotiation as specified in 3GPP TS 33.234 [5], in order to establish trusted relationships (i.e. mutual authentication with the PDG).

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

8.2.1.2 Selection of remote tunnel endpoint

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

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

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].

As specified in draft-ietf-ipsec-ikev2 [14], the PDG should support in place rekeying of SA. Multiple IPSec ESP tunnels per IKE connection shall not be supported.

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

8.3.1.1 General

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

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.

8.3.2.2 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

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