3GPP TSG CN Plenary Meeting #19 **NP-030053**
12th - 14th March 2003. Birmingham, U.K.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 on Work Item IMS-CCR towards IMS access with SIM**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **2** CRs, **Rel-5 to** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #19 for approval.

Spec	CR	Rev	Cat	Phase	Subject	Version-Current	Version-New	Meeting-2nd-Level	Doc-2nd-Level
24.228	094	2	C	Rel-5	Allowing IMS access with SIM	5.3.0	5.4.0	N1-28	N1-030257
24.229	299	2	C	Rel-5	Allowing IMS access with SIM	5.3.0	5.4.0	N1-28	N1-030258

3GPP TSG-CN1 Meeting #28 ***draft Tdoc N1-030257***
Dublin, Ireland, 10 – 14 February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.228** **CR** **094** ⌘ **rev** **2** ⌘ Current version: **5.3.0** ⌘

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

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

Title:	⌘	Allowing IMS access with SIM Cards
Source:	⌘	T-Mobile
Work item code:	⌘	IMS-CCR
Date:	⌘	12/02/2003
Category:	⌘	**C**
Release:	⌘	Rel-5

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:

2	*(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)*

Reason for change:	⌘	Inclusion of the SA1 requirement to allow IMS access using a SIM in 3G UEs, following the authentication option selected by SA3#26.
Summary of change:	⌘	The usage of SIM within the UE is introduced. The references to UE behavior are clarified
Consequences if not approved:	⌘	SA1 requirement will not be addressed . The usage of GSM SIM for IMS will not be possible.

Clauses affected:	⌘	2, 3.2, 6.1

	Y	N			
Other specs affected: ⌘	X		Other core specifications	⌘	22.101, 23.228, 24.229, 33.203
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	

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 23.228: "IP multimedia subsystem; Stage 2".

[3] IETF RFC 3261: "SIP: Session Initiation Protocol"

[4] IETF RFC 2782: "A DNS RR for specifying the location of services (DNS SRV)".

[5] IETF RFC 2806: "URLs for Telephone Calls".

[6] IETF RFC 2916: "E.164 number and DNS".

[7] 3GPP TS 33.203: "Access security for IP based services".

[8] 3GPP TS 23.060: "General Packet Radio Service (GPRS) Service description; Stage 2".

[9] 3GPP TS 29.207: "End to end Quality of Service (QoS); stage 3".

[10] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[11] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx Interface; Signalling flows and message contents".

[12] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network Protocols; Stage 3".

[13] IETF RFC 3323: "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[14] IETF RFC 3263: "SIP: Locating SIP Servers"

[15A] draft-ietf-dhc-dhcpv6-23 (February 2002): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"

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

[15B] draft-ietf-sip-dhcpv6-00 (April 2002): "DHCPv6 options for SIP servers".

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

[16] 3GPP TS 24.229: " IP Multimedia Call Control Protocol based on SIP and SDP; Stage3"

[17] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks"

[18] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services ".

NEXT MODIFICATION

3.2 Abbreviations

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

BGCF	Breakout Gateway Control Function
CN	Core Network
COPS	Common Open Policy Service
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FQDN	Fully-Qualified Domain Name
G-MSC	Gateway Mobile Switching Centre
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
HSS	Home Subscriber Server
I-CSCF	Interrogating-CSCF
IM	IP Multimedia
IP	Internet Protocol
IPv6	IP version 6
ISIM	IMS SIM
MEGACO	MEdia GAteway COntrol
MGCF	Media Gateway Control Function
MGW	Media Gateway
P-CSCF	Proxy-CSCF
PDF	Policy Decision Function
PDP	Packet Data Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SBLP	Service-based local policy
S-CSCF	Serving-CSCF
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SS7	Signalling system no. 7
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
URI	Uniform Resource Identifier
UMTS	Universal Mobile Telecommunications System
USIM	User Service Identity Module

NEXT MODIFICATION

6 Signalling flows for REGISTER (non hiding)

6.1 Introduction

In IMS Authentication is performed at registration time. The following sections show examples of SIP registration and ~~UMTS~~ IMS AKA authentication. It is possible for the home to require other types of authentication.

To enable access for subscribers still using a SIM, GSM AKA can be mapped onto IMS AKA.

If the UE is loaded with a SIM card or UICC card that contains a SIM application, the authentication data and key material is generated from the GSM triplet as described in [18]. This conversion takes place in the UE and the HSS. The conversion is transparent to all other network elements.

If the UICC does not contain an ISIM application or if a SIM is used, then the private user identity and the Request-URI used in REGISTER requests are derived from the IMSI on the SIM or USIM as described in 3GPP TS 24.229 [16]. In this case, a temporary public user identity is derived from the IMSI on the SIM or USIM, and is used during initial SIP registration procedures.

The example flows contained in this document are based on the assumption that the UE is loaded with an UICC and an ISIM application is available on the UICC.

In the example below, Digest AKA is used within SIP headers to carry the information related to the authentication-challenge and response.

3GPP TSG-CN1 Meeting #28 ***draft Tdoc N1-030258***
Dublin, Ireland, 10 – 14 February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **299** ⌘ **rev** **2** ⌘ Current version: **5.3.0** ⌘

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

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

Title:	⌘	Allowing IMS access with SIM Cards
Source:	⌘	T-Mobile
Work item code:	⌘	IMS-CCR
Date:	⌘	12/02/2003
Category:	⌘	**C**
Release:	⌘	Rel-5

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:

2	*(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)*

Reason for change:	⌘	Inclusion of the SA1 requirement to allow IMS access using a SIM in 3G UEs, following the authentication option selected by SA3#26.
Summary of change:	⌘	The usage of SIM within the UE is introduced. The references to UE behavior are clarified.
Consequences if not approved:	⌘	SA1 requirement will not be addressed . The usage of GSM SIM for IMS will not be possible.

Clauses affected:	⌘	3.2, 4.2, 5.1.1.1A, 5.1.1.2, 5.1.1.4, 5.1.1.5.1, 5.1.1.5.3, 5.1.1.6, 5.1.2A.1

Other specs affected:	Y	N			
⌘	X		Other core specifications	⌘	22.101, 23.228, 24.228, 33.203
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	

FIRST MODIFICATION

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
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
GCID	GPRS Charging Identifier
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
i	irrelevant
I-CSCF	Interrogating CSCF
ICID	IM CN subsystem Charging Identifier
IK	Integrity Key
IM	IP Multimedia
IMS	IP Multimedia core network Subsystem
IMSI	International Mobile Subscriber Identity
IOI	Inter Operator Identifier
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC	IP multimedia Subsystem Service Control
ISIM	IMS Suscriber Identity Module
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
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
RAND	RANDom challenge

RES	RESponse
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
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	Universal Resource Identifier
URL	Universal Resource Locator
USIM	UMTS Subscriber Identity Module
x	prohibited
XML	eXtensible Markup Language

NEXT MODIFICATION

4.2 URL and address assignments

In order for SIP and SDP to operate, the following preconditions apply:

1) I-CSCFs used in registration are allocated SIP URLs. Other IM CN subsystem entities may be allocated SIP URLs. For example sip:pcscf.home1.net and sip:<impl-specific-info>@pcscf.home1.net are valid SIP URLs. If the user part exists, it is an essential part of the address and shall not be omitted when copying or moving the address. How these addresses are assigned to the logical entities is up to the network operator. For example, a single SIP URL may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or separate SIP URLs may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.

2) All IM CN subsystem entities are allocated IPv6 addresses in accordance with the constraints specified in 3GPP TS 23.221 [6] subclause 5.1.

3) The subscriber is allocated a private user identity by the home network operator, and this is contained within the ISIM application, if present, on the UICC. Where no ISIM application is present, the private user identity is derived from the IMSI, which is contained on the USIM or SIM (see 3GPP TS 23.003 [3]). This private user identity is available to the SIP application within the UE.

NOTE: The SIP URLs may be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

4) The subscriber is allocated one or more public user identities by the home network operator. At least one of these is contained within the ISIM application, if present, on the UICC. Where no ISIM application is present, the UE shall derive a temporary public user identity from the IMSI contained on the USIM or SIM (see 3GPP TS 23.003 [3]). All registered public user identities are available to the SIP application within the UE, after registration.

5) For the purpose of access to the IM CN subsystem, UEs are assigned IPv6 prefixes in accordance with the constraints specified in 3GPP TS 23.221 [6] subclause 5.1 (see subclause 9.2.1 for the assignment procedures).

NEXT MODIFICATION

5 Application usage of SIP

5.1.1.1A Parameters contained in the UICC or SIM

In case the UE is loaded with a UICC that contains the ISIM application, it will be preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

- the private user identity;
- one ore more public user identities; and
- the home network domain name used to address the SIP REGISTER request

In case the UE is loaded with a SIM card or a UICC that does not contain the ISIM application, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to.

All these three parameters are derived from the IMSI parameter in the USIM or SIM, according to the procedures described in 3GPP TS 23.003 [3]. If the UICC does not contain the ISIM application or if a SIM is used, the UE shall derive new values every time the UICC or SIM is changed, and shall discard existing values if the UICC or SIM is removed.

The temporary public user identity is only used in REGISTER requests. After a successful registration, the UE will get the associated public user identities, and the UE may use any of them in subsequent non-REGISTER messages.

As the temporary public user identity may be barred, the UE shall not reveal the temporary public user identity to the user.

NEXT MODIFICATION

5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. 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 integrity protected using IK, see 3GPP TS 33.203 [19], derived as a result of an earlier registration.

The public user identity to be registered can be extracted or derived ~~either from the ISIM application, if present, on the UICC or derived from the USIM~~, 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) the username field carried in the Authorization header, shall contain the private user identity;

b) the From header shall contain the public user identity to be registered;

c) the To header shall contain the public user identity to be registered;

d) the Expires header, or the expires parameter within the Contact header, shall contain 600 000 seconds as the value desired for the duration of the registration;

e) a Request-URI that contains the SIP URI of the domain name of the home network; and

f) the Security-Client header field by specifying the security mechanism it supports, the IPSec layer algorithms it supports and the parameters needed for the security association setup. For further details see 3GPP TS 33.203 [19] and draft-ietf-sip-sec-agree [48].

NOTE: 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.

The UE shall extract or derive ~~or derive from the UICC~~ 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.

The UE shall include a Supported header containing the option tag "path".

The UE shall also include the P-Access-Network-Info header in the REGISTER request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

On receiving the 200 (OK) response to the REGISTER request, the UE shall store the expiration time of the registration for the public user identities found in the To header value. The UE shall also 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. In order to build a proper preloaded Route header value for new dialogs, the UE shall also store the list of Service Route headers contained in the Service-Route header.

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.

NEXT MODIFICATION

5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity at any time.

The UE shall reregister the public user identity 600 seconds before the expiration time of a previous registration, unless either the user or the application within the UE has determined that a continued registration is not required. If the registration period indicated from the S-CSCF is less than 600 seconds, the UE shall reregister when half of the registration period has expired.

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

On sending a REGISTER request, the UE shall include the following elements:

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 URL that contains the public user identity to be registered;

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

d) a Contact header set to a SIP URL that contains in the hostport parameter the IP address and protected port values that are bound to the security association.

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

e) 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;

f) a Request-URI that contains the SIP URI of the domain name of the home network; and

g) a Security-Client header field, specifying the security mechanism it supports, the IPSec layer algorithms it supports and the parameters needed for the security association setup. For further details see 3GPP TS 33.203 [19] and draft-ietf-sip-sec-agree [48].

NOTE 2: 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.

NOTE 3: The 401 (Unauthorized) challenge sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up the security association with the UE during the same registration procedure.

The UE shall extract or derive ~~from the UICC~~ 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.

The UE shall also include the P-Access-Network-Info header in the REGISTER request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

On receiving the 200 (OK) response to the REGISTER request, the UE shall store the new expiration time of the registration for this public user identity found in the To header value. The UE shall also 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.

The UE shall include a Supported header containing the option tag "path".

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.

NEXT MODIFICATION

5.1.1.5.1 General

Authentication is achieved via the registration and re-registration procedures. When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

- <u>if the UE is loaded with a UICC containing either an ISIM or USIM application,</u> check the validity of a received authentication challenge, as described in 3GPP TS 33.102 [18] i.e. the locally calculated MAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

- check the existence of the Security-Server header as described in draft-sip-sec-agree [48]. If the header is not present, the UE shall send a new REGISTER request.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

- extract the RAND and AUTN parameters, and derive the keys CK and IK;

- set up the security association based on the static list it received in the 401 (Unauthorized) and its capabilities sent in the Security-Client header in the REGISTER request. The UE shall set up the security association using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using CK and IK as shared keys; and

- send another REGISTER request using the derived IK to integrity protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header

containing the private user identity and the authentication challenge response (RES parameter). Instead of the Security-Client header the UE shall insert the Security-Verify header into the request, by mirroring in it the content of the Security-Server header received in the 401 (Unauthorized) response. The Call-ID of the integrity protected REGISTER request which carries RES must be the same as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) for the integrity protected REGISTER request, the UE shall start using the security association the 200 (OK) was protected with.

Whenever the 200 (OK) response is not received after a time-out, the UE shall consider the registration to have failed. The UE shall delete the new security associations it was trying to establish, and use the old security association.

In the case that the 401 (Unauthorized) response is deemed to be invalid then the UE shall behave as defined in subclause 5.1.1.5.3.

NEXT MODIFICATION

5.1.1.5.3 Abnormal cases

If the UE is loaded with a UICC containing either an ISIM or USIM application,and ~~If,~~ in a 401 (Unauthorized) response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no response parameter (e.g. no RES or AUTS);
- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the AUTS parameter (see 3GPP TS 33.102 [18]).

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time. The REGISTER request shall be protected with the existing keys (CK and IK) if available, see 3GPP TS 33.203 [19].

NEXT MODIFICATION

5.1.1.6 Mobile-initiated deregistration

The UE can deregister a previously registered public user identity at any time.

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

a) the username field carried in the Authorization header, shall contain the private user identity;

b) the From header shall contain the public user identity to be deregistered;

c) the To header shall contain the public user identity to be deregistered;

d) the Expires header, or the expires parameter of the Contact header, shall contain a value of zero, appropriate to the deregistration requirements of the user; and

e) a Request-URI that contains the SIP URI of the domain name of the home network.

The UE shall extract or derive ~~from the UICC~~ 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.

The UE shall also include the P-Access-Network-Info header in the REGISTER request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

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

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 P-CSCF.

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).

NEXT MODIFICATION

5.1.2A.1 Mobile-originating case

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 ~~stored in the USIM~~ 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.

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 2: The contents of the From header are 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 not 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 <u>extracted or derived from the UICC or SIM</u>~~stored in the USIM~~ <u></u>. 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-Preferred-Identity 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 or response within a dialog or any request for a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

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 (learnt through the P-CSCF discovery procedures) and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.