3GPP TSG-CN Meeting #24 **NP-040189**
2nd – 4th June 2004. Seoul, Korea.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 (with mirror CRs) on Work Item IMS-CCR towards 24.229**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **8** CRs, **Rel-5** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1 in CN1#34 meeting**, and are forwarded to TSG CN Plenary meeting #24 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Doc-2nd-Level
24.229	627	3	Rel-6	Correction of reception of media authorization token	A	6.2.0	N1-040994
24.229	630	1	Rel-5	Missing statements regarding P-Charging-Function-Addresses header	F	5.8.0	N1-040986
24.229	631	1	Rel-6	Missing statements regarding P-Charging-Function-Addresses header	A	6.2.0	N1-040987
24.229	641	3	Rel-5	Syntax of the extension to the P-Charging-Vector header field	F	5.8.0	N1-041099
24.229	642	3	Rel-6	Syntax of the extension to the P-Charging-Vector header field	A	6.2.0	N1-041100
24.229	647	1	Rel-5	Correction of reception of media authorization token	F	5.8.0	N1-040993
24.229	648	1	Rel-5	Revisions due to published version of draft-ietf-sipping-reg-event	F	5.8.0	N1-040991
24.229	649	1	Rel-6	Revisions due to published version of draft-ietf-sipping-reg-event	A	6.2.0	N1-040992

3GPP TSG-CN1 Meeting #34 **Tdoc N1-040994**
Zagreb, Croatia, 10 – 14 May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **627** ⌘**rev** **3** ⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Correction of reception of media authorization token
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	10/05/2004
Category:	⌘	**A**
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:

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:	⌘	According to the RFC 3313, it may be possible to receive the media authorization token in other messages than 200(ok) and 183 (session progress). It is proposed to make the text generic and reference the RFC to get a correct behaviour.
Summary of change:	⌘	Text on media authorization token is corrected and made generic.
Consequences if not approved:	⌘	Stage 3 is not accurate nor according to RFC 3313.

Clauses affected:	⌘	5.2.7.2, B.2.2.5.1A			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

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

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

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

*** First change ***

5.2.7.2 Mobile-originating case

The P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

Upon receiving a response as specified in RFC 3313 [31] ~~(e.g. 183 (Session Progress), 200 (OK))~~ to the initial INVITE request, the P-CSCF shall:

- if a media authorization token is generated by the PDF ~~as specified in RFC 3313 [31]~~ (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE: Typically, the first 183 (Session Progress) response contains an SDP answer including one or more "m=" media descriptions, but it is also possible that the response does not contain an SDP answer or the SDP does not include at least an "m=" media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated. For further details see 3GPP TS 29.207 [12].

When the P-CSCF sends the UPDATE request towards the S-CSCF, the P-CSCF shall also include the access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the access network charging information.

*** Second change ***

B.2.2.5.1A Activation or modification of PDP contexts for media

If the UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), the media stream(s) shall be set up on separate PDP contexts according to the indication of grouping. The UE may freely group media streams to PDP context(s) in case no indication of grouping is received from the P-CSCF.

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. The UE shall, if a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, establish separate PDP context(s) for the media. If a media authorization token is received in subsequent messages for the same SIP session, the UE shall:

- use the existing PDP context(s) for media;
- modify the existing PDP context(s) for media; or
- establish additional PDP context(s) for media.

The UE shall transparently pass the media authorization token received from the P-CSCF in a~~the 200 (OK) response or the 183 (Session Progress)~~ response to an INVITE request at originating setup or in the INVITE request at terminating setup to the GGSN. The UE shall signal it by inserting it within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message.

To identify to the GGSN which flow(s) (identified by m-lines within the SDP) that are transferred within a particular PDP context, the UE shall set the flow identifier(s) within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message. Detailed description of how the flow identifiers are constructed is provided in 3GPP TS 29.207 [12].

Detailed description of how the media authorization token and flow identifiers are carried in the Traffic Flow Template IE is provided in 3GPP TS 24.008 [8].

If the UE receives several media authorization tokens from the P-CSCF within the same SIP request or response, the first instance of the media authorization token shall be sent to the GGSN, and subsequent instances are discarded by the UE.

The UE shall not re-use a PDP context for other SIP sessions when the session has an associated media authorization token. The UE shall deactivate the PDP context when the SIP session that provided the media authorization token is terminated. When no media authorization token is used for a SIP session, the UE may reuse the PDP context between different SIP sessions.

The UE shall not include the IM CN Subsystem Signalling Flag when a PDP context for media is established or modified.

3GPP TSG-CN1 Meeting #34 **Tdoc N1-040986**

Zagreb, Croatia 10 – 14 May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **630** ⌘ **rev** **1** ⌘ Current version: **5.8.0** ⌘

*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 **X**

Title:	⌘	Missing statements regarding P-Charging-Function-Addresses header
Source:	⌘	Orange, Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	19/04/2004
Category:	⌘	**F**
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:	⌘	There are different missing statements in TS24.229 regarding the P-Charging-Function-Addresses header inclusion or removal make the specification inconsistent.
Summary of change:	⌘	The following change is made. - This header has to be included by the S-CSCF in the 200 OK message of the Register request if P-CSCF is in the same network as the S-CSCF
Consequences if not approved:	⌘	Inconsitent specification as P-CSF can receive this header (without any statement indicating which entity included it in the message).

Clauses affected:	⌘	5.4.1.2.2

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

Other comments: ⌘

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

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

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

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

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

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx FIRST CHANGE xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

1) check if the user needs to be reauthenticated.

   The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" parameter in the Authorization header set to "yes".

   If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

2) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall proceed beginning with step 6 below.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.

2) stop timer reg-await-auth;

3) check whether an Authorization header is included, containing:

   a) the private user identity of the user in the username field;

   b) the algorithm which is AKAv1-MD5 in the algorithm field; and

   c) the authentication challenge response needed for the authentication procedure in the response field.

   The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

4) check whether the received authentication challenge response and the expected authentication challenge response (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49]) match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;

5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:

   a) the list of public user identities associated to the user, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,

   b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria;

NOTE 1: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same user's subscription may belong to different service profiles.

6) bind to each non-barred registered public user identity all registered contact information and store the related method tag values from the Contact header for future use;

NOTE 2: There might be more then one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

7) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

8) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

9) store the icid parameter received in the P-Charging-Vector header;

10) create a 200 (OK) response for the REGISTER request, including:

a) the list of received Path headers;

b) a P-Associated-URI header containing the list of public user identities that the user is authorized to use. The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;

c) a Service-Route header containing:

- the SIP URI identifying the S-CSCF containing an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) are treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part of the URI or be a port number in the URI; and,

- if network topology hiding is required a SIP URI identifying an I-CSCF(THIG) as the topmost entry; and

d) a P-Charging-Function-Addresses header containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request;

11) send the so created 200 (OK) response to the UE;

12) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event; and,

NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.

13) handle the user as registered for the duration indicated in the Expires header.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxEND of CHANGE xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

3GPP TSG-CN1 Meeting #34 **Tdoc N1-040987**

Zagreb, Croatia 10 – 14 May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **631** ⌘ **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 **X**

Title:	⌘	Missing statements regarding P-Charging-Function-Addresses header
Source:	⌘	Orange, Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	19/04/2004
Category:	⌘	**A**
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:

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:	⌘	There are different missing statements in TS24.229 regarding the P-Charging-Function-Addresses header inclusion or removal make the specification inconsistent.
Summary of change:	⌘	The following change is made. - This header has to be included by the S-CSCF in the 200 OK message of the Register request if P-CSCF is in the same network as the S-CSCF
Consequences if not approved:	⌘	Inconsitent specification as P-CSF can receive this header (without any statement indicating which entity included it in the message).

Clauses affected:	⌘	5.4.1.2.2

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

Other comments: ⌘

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

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

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

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

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

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx FIRST CHANGE xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

1) check if the user needs to be reauthenticated.

   The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" parameter in the Authorization header set to "yes".

   If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

2) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall proceed beginning with step 6 below.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.

2) stop timer reg-await-auth;

3) check whether an Authorization header is included, containing:

   a) the private user identity of the user in the username field;

   b) the algorithm which is AKAv1-MD5 in the algorithm field; and

   c) the authentication challenge response needed for the authentication procedure in the response field.

   The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

4) check whether the received authentication challenge response and the expected authentication challenge response (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49]) match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;

5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:

   a) the list of public user identities associated to the user, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,

   b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria;

NOTE 1: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same user's subscription may belong to different service profiles.

6) bind to each non-barred registered public user identity all registered contact information and store the related method tag values from the Contact header for future use;

NOTE 2: There might be more then one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

7) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

8) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

9) store the icid parameter received in the P-Charging-Vector header;

10) create a 200 (OK) response for the REGISTER request, including:

a) the list of received Path headers;

b) a P-Associated-URI header containing the list of public user identities that the user is authorized to use. The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;

c) a Service-Route header containing:

- the SIP URI identifying the S-CSCF containing an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) are treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part of the URI or be a port number in the URI; and,

- if network topology hiding is required a SIP URI identifying an I-CSCF(THIG) as the topmost entry;

d) a P-Charging-Function-Addresses header containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request;

11) send the so created 200 (OK) response to the UE;

12) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event; and,

NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.

13) handle the user as registered for the duration indicated in the Expires header.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxEND of CHANGE xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

3GPP TSG-CN1 Meeting #34 **Tdoc N1-041099**
Zagreb, Croatia 10 – 14 May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **641** ⌘ **rev** **3** ⌘ Current version: **5.8.0** ⌘

*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:	⌘	Syntax of the extension to the P-Charging-Vector header field
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	14/05/2004
Category:	⌘	**F**
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:	⌘	The syntaxt of the extension to the P-Charging-Vector header field that provides GPRS charging information breaks the rules of SIP and staandard SIP parsers. Additionally, the header field is not able to uniquely indicate which GPRS charging information perteins to which flows
Summary of change:	⌘	A new syntax is proposed. This syntax contains several levels of parameters. It is compatible with standard SIP rules for parameters and is able to provide the uniqueness indication of the GPRS charging information
Consequences if not approved:	⌘	The CSCF nodes will not be able to correlate which GPRS charging information applies to which flows, GPRS charging ID, authorization tokens, etc. Consequently the GPRS charging information cannot be applied in IMS.

Clauses affected:	⌘	7.2A.5.2

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

Other comments:	⌘	

7.2A.5 P-Charging-Vector header

7.2A.5.1 Introduction

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

7. 2A.5.2 Syntax

The P-Charging-Vector header field has the syntax described in RFC 3455 [52]. Table 7.3 describes extensions required for 3GPP to that syntax.

Table 7.3: 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-infopdp-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 auth-token *({[SEMI flow-id]})
   pdp-item = "pdp-item" EQUAL DIGIT
   pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
   gcid = "gcid" EQUAL gen-valuetoken1*HEXDIG
   auth-token = "auth-token" EQUAL gen-valuetoken1*HEXDIG
   flow-id = "flow-id" EQUAL gen-value"(" "{" DIGIT COMMA DIGIT "}" *(COMMA "{" DIGIT COMMA DIGIT
"}")")"
   extension-param = token [EQUAL {token | quoted-string}]
```

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 parameters that contains the information for one or more PDP contexts (pdp-info parameter). The pdp-info contains one or more pdp-item values followed by a collection of parameters (pdp-sig, gcid auth token, 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), a media authorization token (auth token parameter) and one or morea flow identifiers (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 and flow-idse parameters are transferred from the GGSN to the P-CSCF (PDF) over the Go interface, see 3GPP TS 29.207 [12].

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.

For a dedicated PDP context for SIP signalling, i.e. no media stream requested for a session, then there is no authorisation activity or information exchange over the Go interface. Since there are no GCID, media authorization token or flow identifiers in this case, the GCID and media authorization token are set to zero and no flow identifier parameters are constructed by the P-CSCF/PDF.

7. 2A.5.3 Operation

The operation of this header is described in subclauses 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

3GPP TSG-CN1 Meeting #34 **Tdoc N1-041100**
Zagreb, Croatia 10 – 14 May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **642** ⌘ **rev** **3** ⌘ 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:	⌘	Syntax of the extension to the P-Charging-Vector header field
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	14/05/2004
Category:	⌘	**A**
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:

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:	⌘	The syntaxt of the extension to the P-Charging-Vector header field that provides GPRS charging information breaks the rules of SIP and staandard SIP parsers. Additionally, the header field is not able to uniquely indicate which GPRS charging information perteins to which flows
Summary of change:	⌘	A new syntax is proposed. This syntax contains several levels of parameters. It is compatible with standard SIP rules for parameters and is able to provide the uniqueness indication of the GPRS charging information
Consequences if not approved:	⌘	The CSCF nodes will not be able to correlate which GPRS charging information applies to which flows, GPRS charging ID, authorization tokens, etc. Consequently the GPRS charging information cannot be applied in IMS.

Clauses affected:	⌘	B.4.1

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

Other comments:	⌘	

B.4 3GPP specific encoding for SIP header extensions

B.4.1 P-Charging-Vector header

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-infopdp-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 auth-token *({[SEMI flow-id]})
   pdp-item = "pdp-item" EQUAL DIGIT
   pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
   gcid = "gcid" EQUAL gen-valuetoken1*HEXDIG
   auth-token = "auth-token" EQUAL gen-valuetoken1*HEXDIG
   flow-id = "flow-id" EQUAL gen-value"(" "{" DIGIT COMMA DIGIT "}" *(COMMA "{" DIGIT COMMA DIGIT
"}")")"
   extension-param = token [EQUAL {token | quoted-string}]
```

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 parameters that contains the information for one or more PDP contexts (pdp-info parameter). The pdp-info contains one or more pdp-item values followed by a collection of parameters (pdp-sig, gcid, auth token, 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), a media authorization token (auth token parameter) and one or morea flow identifiers (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. These gcid 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.

For a dedicated PDP context for SIP signalling, i.e. no media stream requested for a session, then there is no authorisation activity or information exchange over the Go and Gq interfaces. Since there are no GCID, media authorization token or flow identifiers in this case, the GCID and media authorization token are set to zero and no flow identifier parameters are constructed by the PDF.

3GPP TSG-CN1 Meeting #34
Zagreb, Croatia, 10 – 14 May 2004

Tdoc N1-040993

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **647** ⌘ **rev** **1** ⌘ Current version: **5.8.0** ⌘

*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:	⌘	Correction of reception of media authorization token
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	10/05/2004
Category:	⌘	**F**
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:	⌘	According to the RFC 3313, it may be possible to receive the media authorization token in other messages than 200(ok) and 183 (session progress). This is also implied by the text in subclause 5.2.7.2. It is proposed to make the text generic and reference the RFC to get a correct behaviour.
Summary of change:	⌘	Text on media authorization token is corrected and made generic.
Consequences if not approved:	⌘	Clarifications and alignment for forward compatibility

Clauses affected:	⌘	5.2.7.2, 9.2.5.1A			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

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

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

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

*** First change ***

5.2.7.2 Mobile-originating case

The P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

Upon receiving a response as specified in RFC 3313 [31 ~~(e.g. 183 (Session Progress), 200 (OK))~~ to the initial INVITE request, the P-CSCF shall:

- if a media authorization token is generated by the PDF ~~as specified in RFC 3313 [31]~~ (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE: Typically, the first 183 (Session Progress) response contains an SDP answer including one or more "m=" media descriptions, but it is also possible that the response does not contain an SDP answer or the SDP does not include at least an "m=" media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated.

When the P-CSCF sends the UPDATE request towards the S-CSCF, the P-CSCF shall also include the access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the access network charging information.

*** Second change ***

9.2.5.1A Activation or modification of PDP contexts for media

If the UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), the media stream(s) shall be set up on separate PDP contexts according to the indication of grouping. The UE may freely group media streams to PDP context(s) in case no indication of grouping is received from the P-CSCF.

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. The UE shall, if a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, establish separate PDP context(s) for the media. If a media authorization token is received in subsequent messages for the same SIP session, the UE shall:

- use the existing PDP context(s) for media;
- modify the existing PDP context(s) for media; or
- establish additional PDP context(s) for media.

The UE shall transparently pass the media authorization token received from the P-CSCF in a~~the 183 (Session Progress)~~ response to an INVITE request at originating setup or in the INVITE request at terminating setup to the GGSN. The UE shall signal it by inserting it within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message.

To identify to the GGSN which flow(s) (identified by m-lines within the SDP) that are transferred within a particular PDP context, the UE shall set the flow identifier(s) within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message. Detailed description of how the flow identifiers are constructed is provided in 3GPP TS 29.207 [12].

Detailed description of how the media authorization token and flow identifiers are carried in the Traffic Flow Template IE is provided in 3GPP TS 24.008 [8].

If the UE receives several media authorization tokens from the P-CSCF within the same SIP request or response, the first instance of the media authorization token shall be sent to the GGSN, and subsequent instances are discarded by the UE.

The UE shall not re-use a PDP context for other SIP sessions when the session has an associated media authorization token. The UE shall deactivate the PDP context when the SIP session that provided the media authorization token is

terminated. When no media authorization token is used for a SIP session, the UE may reuse the PDP context between different SIP sessions.

The UE shall not include the IM CN Subsystem Signalling Flag when a PDP context for media is established or modified.

3GPP TSG-CN1 Meeting #34 **Tdoc N1-040991**

Zagreb, Croatia 10 – 14 May 2004

Tdoc N1-040936

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **648** ⌘ **rev** **1** ⌘ Current version: **5.8.0** ⌘

*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:	⌘	Revisions due to published version of draft-ietf-sipping-reg-event
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	16/04/2004
Category:	⌘	**F**
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:	⌘	draft-ietf-sipping-reg-event has recently been published as RFC 3680, and as part of the publication process there have been some minor revisions to the XML schema, which result in some minor changes to the procedures text in 24.229, as well as a reference change. This contribution proposes those changes.
Summary of change:	⌘	All references to draft-ietf-sipping-reg-event are replaced by RFC 3680. In the XML document relating to the reg event package, all instances of contact addresses are preceded by a start element <uri> and a end element </uri>.
Consequences if not approved:	⌘	It is inappropriate for 3GPP technical specifications to refer to documents that are no longer generally available. 3GPP implementations will not be compatible with other implementations made according to the RFC, yet the identification of the package (and therefore the normal indicator of compatibility) will be one and the same.
Clauses affected:	⌘	2, 5.1.1.3, 5.1.1.5.2, 5.2.3, 5.4.1.5, 5.4.1.6, 5.4.2.1.1, 5.4.2.1.2, 5.7.1.1

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications	⌘	24.228
			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

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".

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

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

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

[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 32.200: "Telecommunication management; Charging management; Charging principles".

[17] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia subsystem".

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

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

[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 2806 (April 2000): "URLs for Telephone Calls".

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

[24] RFC 2916 (September 2000): "E.164 number and DNS".

[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".

[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] ~~draft-ietf-sipping-reg-event-00~~ RFC 3680 (~~October 2002~~March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

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

[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".

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

PROPOSED CHANGE

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 users registrar (S-CSCF) as described in ~~draft-ietf-sipping-reg-event-00~~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 initiaial registratioin 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; and

f) a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

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.

PROPOSED CHANGE

5.1.1.5.2 Network-initiated re-authentication

At any time, the UE can receive a NOTIFY request carrying information related to the reg event package (as described in subclause 5.1.1.3). If:

- the state attribute in any of the <registration> elements is set to "active";
- the value of the <uri> sub-element inside the <contact> sub-element is set to the Contact address that the UE registered; and
- the event attribute of that <contact> sub-element(s) is set to "shortened";

the UE shall:

1) use the expiry attribute within the <contact> element to adjust the expiration time for that public user identity; and
2) start the re-authentication procedures at the appropriate time (as a result of the S-CSCF procedure described in subclause 5.4.1.6) by initiating a reregistration as described in subclause 5.1.1.4.

PROPOSED CHANGE

5.2.3 Subscription to the user's registration-state event package

Upon receipt of a 200 (OK) response to the initial REGISTER request of an user, the P-CSCF shall subscribe to the reg event package at the users registrar (S-CSCF) as described in ~~draft-ietf-sipping-reg-event-00~~RFC 3680 [43]. The P-CSCF shall:

1) generate a SUBSCRIBE request with the following elements:
   - a Request-URI set to the resource to which the P-CSCF wants to be subscribed to, i.e. to a SIP URI that contains the default public user identity of the user;
   - a From header set to the P-CSCF's SIP URI;
   - a To header, set to a SIP URI that contains the default public user identity of the user;
   - an Event header set to the "reg" event package;
   - an Expires header set to a value higher then the Expires header indicated in the 200 (OK) response to the REGISTER request;
   - a P-Asserted-Identity header set to the SIP URI of the P-CSCF,which was inserted into the Path header during the registration of the user to whose registration state the P-CSCF subscribes to; and
   - a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17]; and

2) determine the I-CSCF of the home network (e.g., by using DNS services);

before sending the SUBSCRIBE request to that I-CSCF, according to the procedures of RFC 3261 [26].

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

If continued subscription is required the P-CSCF shall automatically refresh the subscription by the reg event package 600 seconds before the expiration time 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.

PROPOSED CHANGE

5.4.1.5 Network-initiated deregistration

Prior to initiating the network-initiated deregistration for the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) while there are still active multimedia sessions belonging to this user, the S-CSCF shall release all multimedia sessions belonging to this user as described in subclause 5.4.5.1.

When a network-initiated deregistration event occurs for one or more public user identity, the S-CSCF shall send a NOTIFY request to the UE on the dialog which was generated by the UE subscribing to the reg event package. When the S-CSCF receives a final response to the NOTIFY request or upon a timeout, the S-CSCF shall release all remaining dialogs related to the public user identity being deregistered and shall generate a NOTIFY request on all remaining dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

4) set the aor attribute within each <registration> element to one public user identity:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;

   b) if the public user identity:

      i) has been deregistered then:

         - set the state attribute within the <registration> element to "terminated";

         - set the state attribute within the <contact> element to "terminated"; and

         - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

      ii) has been kept registered then:

         - set the state attribute within the <registration> element to "active"; and

         - set the state attribute within the <contact> element to "active"; and

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

Also, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event.

On completion of the above procedures in this subclause for one or more public user identities, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities. On completion of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber).

PROPOSED CHANGE

5.4.1.6 Network-initiated reauthentication

The S-CSCF may request a subscriber to reauthenticate at any time, based on a number of possible operator settable triggers as described in subclause 5.4.1.2.

If the S-CSCF is informed that a private user identity needs to be re-authenticated, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;

   b) set the aor attribute within each <registration> element to one public user identity;

   c) set the state attribute within each <registration> element to "active";

   d) set the state attribute within each <contact> element to "active";

   e) set the event attribute within each <contact> element to "shortened"; and

   f) set the expiry attribute within each <contact> element to an operator defined value; and

4) set a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

Afterwards the S-CSCF shall wait for the user to reauthenticate (see subclause 5.4.1.2).

NOTE: Network initiated re-authentication may occur due to internal processing within the S-CSCF.

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

When generating the NOTIFY request, the S-CSCF shall shorten the validity of all registration lifetimes associated with this private user identity to an operator defined value that will allow the user to be re-authenticated.

PROPOSED CHANGE

5.4.2.1 Subscriptions to S-CSCF events

5.4.2.1.1 Subscription to the event providing registration state

When an incoming SUBSCRIBE request addressed to S-CSCF arrives containing the Event header with the reg event package, the S-CSCF shall:

1) check if, based on the local policy, the request was generated by a subscriber who is authorised to subscribe to the registration state of this particular user. The authorized subscribers include:

   - all public user identities this particular user owns, that the S-CSCF is aware of, and which are not-barred;
   - all the entities identified by the Path header (i.e. the P-CSCF to which this user is attached to); and
   - all the ASs listed in the initial filter criteria and not belonging to third-party providers.

NOTE: The S-CSCF finds the identity of the originator of the SUBSCRIBE request in the P-Asserted-Identity header.

2) generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the authorised subscription was successful as described in ~~draft-ietf-sipping-reg-event-00~~RFC 3680 [43]. The S-CSCF shall populate the header fields as follows:

   - an Expires header, set to either the same or a decreased value as the Expires header in SUBSCRIBE request; and
   - a Contact header, set to is an identifier generated within the S-CSCF that will help to correlate refreshes for the SUBSCRIBE.

Afterwards the S-CSCF shall perform the procedures for notification about registration state as described in subclause 5.4.2.1.2.

5.4.2.1.2 Notification about registration state

For each NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;
2) set the Event header to the "reg" value;
3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;
4) set the aor attribute within each <registration> element to one public user identity:
   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE; and
   b) if the public user identity:
      I) has been deregistered then:
         - set the state attribute within the <registration> element to "terminated";
         - set the state attribute within the <contact> element to "terminated"; and
         - set the event attribute within the <contact> element to "deactivated", "expired", "unregistered" or "probation" according ~~draft-ietf-sipping-reg-event-00~~RFC 3680 [43]; or
      II) has been registered then:
         - set the state attribute within the <registration> element to "active";
         - set the state attribute within the <contact> element to "active"; and
         - set the event attribute within the <contact> element to "registered"; or
      III) has been automatically registered:
         - set the state attribute within the <registration> element to "active";
         - set the state attribute within the <contact> element to "active"; and

- set the event attribute within the <contact> element to "created"; and

5) set the P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

EXAMPLE: If sip:user1_public1@home1.net is registered, the public user identity sip:user1_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
             version="0" state="full">
  <registration aor="sip:user1_public1@home1.net" id="as9"
                state="active">
    <contact id="76" state="active" event="registered">
          <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    </contact>
  </registration>
  <registration aor="sip:user1_public2@home1.net" id="as10"
                state="active">
    <contact id="86" state="active" event="created">
          <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    </contact>
  </registration>
</reginfo>
```

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities have been deregistered or expired), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header to the value of "terminated".

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

PROPOSED CHANGE

5.7.1.1 Notification about registration status

The AS may support the REGISTER method in order to discover the registration status of the user. If a REGISTER request arrives containing information about the user's registration status and the AS supports the REGISTER method, the AS shall store the Expires parameter from the request and generate a 200 (OK) response or an appropriate failure response. For the success case, the 200 (OK) response shall contain Expires value equal to the value received in the REGISTER request. The AS shall store the values received in P-Charging-Function-Addresses header. Also, the AS shall store the values of the icid parameter in the P-Charging-Vector header from the REGISTER request.

Upon receipt of a third-party REGISTER request, the AS may subscribe to the reg event package for the public user identity registered at the users registrar (S-CSCF) as described in ~~draft-ietf-sipping-reg-event-00~~RFC 3680 -[43].

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

a) a Request URI set to the resource to which the AS wants to be subscribed to, i.e. to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;

b) a From header field set to the AS's SIP URI;

c) a To header field, set to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;

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

e) a P-Asserted-Identity header field set to the SIP URI of the AS; and

NOTE 1: The S-CSCF expects the SIP URI used in the P-Asserted-Identity header to correspond to the SIP URI, which identified this AS in the initial filter criteria of the user to whose registration state the AS subscribes to.

f) a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

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

NOTE 2: Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header set to "terminated", the AS considers the subscription to the reg event package terminated, i.e. as if the AS had sent a SUBSCRIBE request with an Expires header containing a value of zero.

3GPP TSG-CN1 Meeting #34 **Tdoc N1-040992**

Zagreb, Croatia 10 – 14 May 2004

was Tdoc N1-040937

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **649** ⌘ **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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Revisions due to published version of draft-ietf-sipping-reg-event
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	16/04/2004
Category:	⌘	**A**
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:

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:	⌘	draft-ietf-sipping-reg-event has recently been published as RFC 3680, and as part of the publication process there have been some minor revisions to the XML schema, which result in some minor changes to the procedures text in 24.229, as well as a reference change. This contribution proposes those changes.
Summary of change:	⌘	All references to draft-ietf-sipping-reg-event are replaced by RFC 3680. In the XML document relating to the reg event package, all instances of contact addresses are preceded by a start element <uri> and a end element </uri>.
Consequences if not approved:	⌘	It is inappropriate for 3GPP technical specifications to refer to documents that are no longer generally available. 3GPP implementations will not be compatible with other implementations made according to the RFC, yet the identification of the package (and therefore the normal indicator of compatibility) will be one and the same.

Clauses affected:	⌘	2, 5.1.1.3, 5.1.1.5.2, 5.2.3, 5.4.1.5, 5.4.1.6, 5.4.2.1.1, 5.4.2.1.2, 5.7.1.1

	Y	N			
Other specs affected: ⌘	X		Other core specifications	⌘	24.228
		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

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".

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

[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 2806 (April 2000): "URLs for Telephone Calls".

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

[24] RFC 2916 (September 2000): "E.164 number and DNS".

[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] ~~draft-ietf-sipping-reg-event-00~~ RFC 3680 (~~October 2002~~March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

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

[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] draft-ietf-sip-callerprefs-10 (October 2003): "Caller Preferences for the Session Initiation Protocol (SIP)"

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

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

PROPOSED CHANGE

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 users registrar (S-CSCF) as described in ~~draft-ietf-sipping-reg-event-00~~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 initiaial registratioin 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; and

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

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.

PROPOSED CHANGE

5.1.1.5.2 Network-initiated re-authentication

At any time, the UE can receive a NOTIFY request carrying information related to the reg event package (as described in subclause 5.1.1.3). If:

- the state attribute in any of the <registration> elements is set to "active";
- the value of the <uri> sub-element inside the <contact> sub-element is set to the Contact address that the UE registered; and
- the event attribute of that <contact> sub-element(s) is set to "shortened";

the UE shall:

1) use the expiry attribute within the <contact> element to adjust the expiration time for that public user identity; and

2) start the re-authentication procedures at the appropriate time (as a result of the S-CSCF procedure described in subclause 5.4.1.6) by initiating a reregistration as described in subclause 5.1.1.4.

PROPOSED CHANGE

5.2.3 Subscription to the user's registration-state event package

Upon receipt of a 200 (OK) response to the initial REGISTER request of an user, the P-CSCF shall subscribe to the reg event package at the users registrar (S-CSCF) as described in ~~draft-ietf-sipping-reg-event-00~~RFC 3680 [43]. The P-CSCF shall:

1) generate a SUBSCRIBE request with the following elements:

   - a Request-URI set to the resource to which the P-CSCF wants to be subscribed to, i.e. to a SIP URI that contains the default public user identity of the user;
   - a From header set to the P-CSCF's SIP URI;

- a To header, set to a SIP URI that contains the default public user identity of the user;
- an Event header set to the "reg" event package;
- an Expires header set to a value higher then the Expires header indicated in the 200 (OK) response to the REGISTER request;
- a P-Asserted-Identity header set to the SIP URI of the P-CSCF,which was inserted into the Path header during the registration of the user to whose registration state the P-CSCF subscribes to; and
- a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]; and

2) determine the I-CSCF of the home network (e.g., by using DNS services);

before sending the SUBSCRIBE request to that I-CSCF, according to the procedures of RFC 3261 [26].

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

If continued subscription is required the P-CSCF shall automatically refresh the subscription by the reg event package 600 seconds before the expiration time 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.

PROPOSED CHANGE

5.4.1.5 Network-initiated deregistration

Prior to initiating the network-initiated deregistration for the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) while there are still active multimedia sessions belonging to this user, the S-CSCF shall release all multimedia sessions belonging to this user as described in subclause 5.4.5.1.

When a network-initiated deregistration event occurs for one or more public user identity, the S-CSCF shall send a NOTIFY request to the UE on the dialog which was generated by the UE subscribing to the reg event package. When the S-CSCF receives a final response to the NOTIFY request or upon a timeout, the S-CSCF shall release all remaining dialogs related to the public user identity being deregistered and shall generate a NOTIFY request on all remaining dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;
2) set the Event header to the "reg" value;
3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;
4) set the aor attribute within each <registration> element to one public user identity:
   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;
   b) if the public user identity:
      i) has been deregistered then:
         - set the state attribute within the <registration> element to "terminated";
         - set the state attribute within the <contact> element to "terminated"; and
         - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

ii) has been kept registered then:

- set the state attribute within the <registration> element to "active";
- set the state attribute within the <contact> element to "active"; and

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

Also, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event.

On completion of the above procedures for one or more public user identities, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities. On completion of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber).

PROPOSED CHANGE

5.4.1.6 Network-initiated reauthentication

The S-CSCF may request a subscriber to reauthenticate at any time, based on a number of possible operator settable triggers as described in subclause 5.4.1.2.

If the S-CSCF is informed that a private user identity needs to be re-authenticated, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;

   b) set the aor attribute within each <registration> element to one public user identity;

   c) set the state attribute within each <registration> element to "active";

   d) set the state attribute within each <contact> element to "active";

   e) set the event attribute within each <contact> element to "shortened"; and

   f) set the expiry attribute within each <contact> element to an operator defined value; and

4) set a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

Afterwards the S-CSCF shall wait for the user to reauthenticate (see subclause 5.4.1.2).

NOTE: Network initiated re-authentication may occur due to internal processing within the S-CSCF.

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

When generating the NOTIFY request, the S-CSCF shall shorten the validity of all registration lifetimes associated with this private user identity to an operator defined value that will allow the user to be re-authenticated.

PROPOSED CHANGE

5.4.2.1 Subscriptions to S-CSCF events

5.4.2.1.1 Subscription to the event providing registration state

When an incoming SUBSCRIBE request addressed to S-CSCF arrives containing the Event header with the reg event package, the S-CSCF shall:

1) check if, based on the local policy, the request was generated by a subscriber who is authorised to subscribe to the registration state of this particular user. The authorized subscribers include:

   - all public user identities this particular user owns, that the S-CSCF is aware of, and which are not-barred;
   - all the entities identified by the Path header (i.e. the P-CSCF to which this user is attached to); and
   - all the ASs listed in the initial filter criteria and not belonging to third-party providers.

   NOTE: The S-CSCF finds the identity of the originator of the SUBSCRIBE request in the P-Asserted-Identity header.

2) generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the authorised subscription was successful as described in ~~draft ietf sipping reg event 00~~RFC 3680 [43]. The S-CSCF shall populate the header fields as follows:

   - an Expires header, set to either the same or a decreased value as the Expires header in SUBSCRIBE request; and
   - a Contact header, set to is an identifier generated within the S-CSCF that will help to correlate refreshes for the SUBSCRIBE.

Afterwards the S-CSCF shall perform the procedures for notification about registration state as described in subclause 5.4.2.1.2.

5.4.2.1.2 Notification about registration state

For each NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;
2) set the Event header to the "reg" value;
3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;
4) set the aor attribute within each <registration> element to one public user identity:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE; and

   b) if the public user identity:

      I) has been deregistered then:

         - set the state attribute within the <registration> element to "terminated";
         - set the state attribute within the <contact> element to "terminated"; and
         - set the event attribute within the <contact> element to "deactivated", "expired", "unregistered" or "probation" according ~~draft ietf sipping reg event 00~~ RFC 3680 [43]; or

      II) has been registered then:

- set the state attribute within the <registration> element to "active";
- set the state attribute within the <contact> element to "active"; and
- set the event attribute within the <contact> element to "registered"; or

III) has been automatically registered:

- set the state attribute within the <registration> element to "active";
- set the state attribute within the <contact> element to "active"; and
- set the event attribute within the <contact> element to "created"; and

5) set the P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

EXAMPLE: If sip:user1_public1@home1.net is registered, the public user identity sip:user1_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
             version="0" state="full">
  <registration aor="sip:user1_public1@home1.net" id="as9"
                state="active">
    <contact id="76" state="active" event="registered">
          <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    </contact>
  </registration>
  <registration aor="sip:user1_public2@home1.net" id="as10"
                state="active">
    <contact id="86" state="active" event="created">
          <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    </contact>
  </registration>
</reginfo>
```

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities have been deregistered or expired), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header to the value of "terminated".

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

PROPOSED CHANGE

5.7.1.1 Notification about registration status

The AS may support the REGISTER method in order to discover the registration status of the user. If a REGISTER request arrives containing information about the user's registration status and the AS supports the REGISTER method, the AS shall store the Expires parameter from the request and generate a 200 (OK) response or an appropriate failure response. For the success case, the 200 (OK) response shall contain Expires value equal to the value received in the REGISTER request. The AS shall store the values received in P-Charging-Function-Addresses header. Also, the AS shall store the values of the icid parameter in the P-Charging-Vector header from the REGISTER request.

Upon receipt of a third-party REGISTER request, the AS may subscribe to the reg event package for the public user identity registered at the users registrar (S-CSCF) as described in ~~draft-ietf-sipping-reg-event-00~~ RFC 3680 [43].

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

a) a Request URI set to the resource to which the AS wants to be subscribed to, i.e. to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;

b) a From header field set to the AS's SIP URI;

c) a To header field, set to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;

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

e) a P-Asserted-Identity header field set to the SIP URI of the AS; and

NOTE 1: The S-CSCF expects the SIP URI used in the P-Asserted-Identity header to correspond to the SIP URI, which identified this AS in the initial filter criteria of the user to whose registration state the AS subscribes to.

f) a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

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

NOTE 2: Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header set to "terminated", the AS considers the subscription to the reg event package terminated, i.e. as if the AS had sent a SUBSCRIBE request with an Expires header containing a value of zero.