3GPP TSG-CN Meeting #23 10th - 12th March 2004. Phoenix, USA.

NP-040028

Source: TSG CN WG 1

Title: CR to Rel-5 (with mirror CR) on Work Item IMS-CCR towards 24.229,- pack 2

Agenda item: 8.1

Document for: APPROVAL

Introduction:

This document contains 2 CRs, Rel-5 (with mirror CR) on Work Item "IMS-CCR", that have been agreed by TSG CN WG1 in CN1#33 meeting, and are forwarded to TSG CN Plenary meeting #23 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version- Current	Version- New	Doc-2nd- Level
24.229	601	1	Rel-5	Missing statements regarding P-Charging-Function-Addresses	F	5.7.0	5.8.0	N1-040403
24.229	602	1	Rel-6	Missing statements regarding P-Charging-Function-Addresses	Α	6.1.0	6.2.0	N1-040404

CHANGE REQUEST						CR-Form-v7	
æ	24.22	29 CR <mark>601</mark>	∺rev	<u>1</u> - **	Current vers	5.7.0	¥
For <u>HELP</u> on u	ising this	form, see bottom	of this page or	look at th	e pop-up text	tover the ≭ sy	mbols.
Proposed change	affects:	UICC apps第	ME_	Radio A	ccess Netwo	rk Core N	etwork X
Title: ∺	Missin	g statements rega	rding P-Chargi	ng-Functi	on-Addresses	3	
Source: #	Orange	е					
Work item code: ₩	IMS-C	CR			Date: ∺	19/01/2004	
Reason for change Summary of change	F (A (B (C (D	of the following cate correction) corresponds to a condition of feature), functional modification explanations of the lin 3GPP TR 21.900 there are different runction-Addresses consistent. This header has the Register received the value of this I-CSCF shall reddifferent network applies.	prection in an early on of feature) above categories and the statem of	ents in TS ion or rem	e) R96 R97 R98 R99 Rel-4 Rel-5 Rel-6 624.229 regarnoval make the ted that itthe later than 100 me 200 OK when the later than 100 of	the following re (GSM Phase 2) (Release 1996) (Release 1997) (Release 1998) (Release 1999) (Release 4) (Release 5) (Release 6) rding the P-Chae specification 200 OK mess P-CSCF has to	arging- age of costore
Consequences if not approved:	ж <mark>In</mark>	consitent specifica	ation and misal	ignement	with stage 2		
Clauses affected:	光 5.	3.2.1, 5.3.3.1, 5.4.	1.2.2				
Other specs affected:	¥ Y	X Other core specifica X O&M Specifica	tions	Ж			
Other comments:	æ						

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 \(\mathcal{H} \) 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.

5.3.1.2 Normal procedures

When I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

- 1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;
- 2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

- 1) select a S-CSCF that fulfils the indicated mandatory capabilities if more then one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;
- 2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;
- 3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 4) forward the REGISTER request to the selected S-CSCF.

When the I-CSCF receives a 2xx response to a REGISTER request, <u>if this response includes P-Charging-Function-Addresses</u> header and if the I-CSCF is not in the same network as the P-CSCF, the I-CSCF shall remove the P-Charging-Function-Addresses header prior to forwarding the message; otherwise the I-CSCF shall <u>forwardproxy</u> the 2xx response to the P-CSCF.

5.3.3.1 General

The following procedures shall only be applied if topology hiding is required by the network. The network requiring topology hiding is called the hiding network.

NOTE 1: Requests and responses are handled independently therefore no state information is needed for that purpose within an I-CSCF(THIG).

The I-CSCF(THIG) shall apply topology hiding to all headers which reveal topology information, such as Via, Route, Record-Route, Service-Route.

Upon receiving an incoming REGISTER request for which topology hiding has to be applied and which includes a Path header, the I-CSCF(THIG) shall add the routeable SIP URI of an I-CSCF(THIG) to the top of the Path header. The I-CSCF(THIG) may include in the inserted SIP URI an indicator that identifies the direction of subsequent requests received by the I-CSCF i.e., from the S-CSCF towards the P-CSCF, to identify the mobile-terminating case. The I-CSCF(THIG) may encode this indicator in different ways, such as, e.g., a unique parameter in the URI, a character string in the username part of the URI, or a dedicated port number in the URI.

NOTE 2: Any subsequent request that includes the direction indicator (in the Route header) or arrives at the dedicated port number, indicates that the request was sent by the S-CSCF towards the P-CSCF.

Upon receiving an incoming initial request for which topology hiding has to be applied and which includes a Record-Route header, the I-CSCF(THIG) shall add its own routeable SIP URI to the top of the Record-Route header.

Upon receiving an outgoing initial request <u>or response</u> for which topology hiding has to be applied and which includes P-Charging-Function-Addresses header, the I-CSCF(THIG) shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the integrity-protection 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 registration requests received without integrity protection by the P-CSCF. The information that a REGISTER request was received integrity protected at the P-CSCF may be used as part of the decision to challenge the user.

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;
- 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.

CHANGE REQUEST					
*	24.229 CR 602				
For <u>HELP</u> on t	sing this form, see bottom of this page or look at the pop-up text over the 策 symbols.				
Proposed change	ME Radio Access Network Core Network X				
Title:	Missing statements regarding P-Charging-Function-Addresses				
Source:	Orange				
Work item code: ₩	IMS-CCR Date: 第 26/01/2004				
Reason for chang	Function-Addresses header inclusion or removal make the specification inconsistent.				
Consequences if not approved:	光 Inconsitent specification and misalignement with stage 2				
Clauses affected: Other specs affected: Other comments:	# 5.3.2.1, 5.3.3.1, 5.4.1.2.2 Y N X Other core specifications # X Test specifications O&M Specifications # X O&M Specifications #				

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 \(\mathcal{H} \) 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.

5.3.1.2 Normal procedures

When I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

NOTE: Different UEs, each with its own private user identity, may register the same public user identity. Registrations for the same shared public user identity are directed to the same S-CSCF as described in 3GPP TS 29.228 [14].

Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

- 1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;
- 2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

- 1) select a S-CSCF that fulfils the indicated mandatory capabilities if more then one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;
- 2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;
- 3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 4) forward the REGISTER request to the selected S-CSCF.

When the I-CSCF receives a 2xx response to a REGISTER request, <u>if this response includes P-Charging-Function-Addresses header and if the I-CSCF is not in the same network as the P-CSCF, the I-CSCF shall remove the P-Charging-Function-Addresses header prior to forwarding the message; otherwise the I-CSCF shall <u>forwardproxy</u> the 2xx response to the P-CSCF.</u>

5.3.3.1 General

The following procedures shall only be applied if topology hiding is required by the network. The network requiring topology hiding is called the hiding network.

NOTE 1: Requests and responses are handled independently therefore no state information is needed for that purpose within an I-CSCF(THIG).

The I-CSCF(THIG) shall apply topology hiding to all headers which reveal topology information, such as Via, Route, Record-Route, Service-Route.

Upon receiving an incoming REGISTER request for which topology hiding has to be applied and which includes a Path header, the I-CSCF(THIG) shall add the routeable SIP URI of an I-CSCF(THIG) to the top of the Path header. The I-CSCF(THIG) may include in the inserted SIP URI an indicator that identifies the direction of subsequent requests received by the I-CSCF i.e., from the S-CSCF towards the P-CSCF, to identify the mobile-terminating case. The I-

CSCF(THIG) may encode this indicator in different ways, such as, e.g., a unique parameter in the URI, a character string in the username part of the URI, or a dedicated port number in the URI.

NOTE 2: Any subsequent request that includes the direction indicator (in the Route header) or arrives at the dedicated port number, indicates that the request was sent by the S-CSCF towards the P-CSCF.

Upon receiving an incoming initial request for which topology hiding has to be applied and which includes a Record-Route header, the I-CSCF(THIG) shall add its own routeable SIP URI to the top of the Record-Route header.

Upon receiving an outgoing initial request <u>or response</u> for which topology hiding has to be applied and which includes P-Charging-Function-Addresses header, the I-CSCF(THIG) shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

xxxxxxxxxxxxxxxxxxxxxxxxxxxx NEXT CHANGES xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the integrity-protection 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 registration requests received without integrity protection by the P-CSCF. The information that a REGISTER request was received integrity protected at the P-CSCF may be used as part of the decision to challenge the user.

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;
- 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.