3GPP TSG CN Plenary Meeting #17 **NP-020379**
4th - 6th September 2002. Biarritz, France.

Source: **TSG CN WG 1**

Title: **CR to Rel-5 on Work Item IMS-CCR towards 24.229,- CR153r1**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **1** CR on **Rel-5 to** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #17 for approval.

An alternativ CR153r2 is provided directly to CN#17 in NP-020335.

Spec	CR #	Rev	CAT	Rel	Tdoc Title	Meeting	TDoc #	C_Version
24.229	153	1	F	Rel-5	Registration with intergrity protection	N1-25	N1-021792	5.1.0

3GPP TSG-CN1 Meeting #25
Helsinki, Finland, 29 July – 2 August

Tdoc N1-021759~~5~~2

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **153** ⌘ **rev** **1-** ⌘ Current version: **5.1.0** ⌘

*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:	⌘	Registration with intergrity protection
Source:	⌘	Hutchison 3G UK, Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	25-07-2002
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:	⌘	Current text describing action of S-CSCF does not cover all possible options with regard to the integrity-protected flag. The current wording would mean that a REGISTER for a new public ID would be subjected to authentication every time, regardless of whether it was integrity protected or not, and the case of an uprotected REIGSTER being received when an authentication is ongoing is not specified.
Summary of change:	⌘	Reorganisation of sections so that they cover the integirty-protected = no / yes options rather than trying to define them for initial registration. The text is reorganised to structure it to cover all options, and new behaviour specified to cover the missing behaviour.
Consequences if not approved:	⌘	Unspecified and therefore inconsistent behaviour could cause interoperability problems.

Clauses affected:	⌘	5.4.1.2.1, 5.4.1.2.2

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.

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 ~~Initial registration~~Unprotected REGISTER

NOTE 1: Any REGISTER request sent unprotected by the UE is considered to be an initial registration. A 200 final response to such a request will only be sent back after the S-CSCF receives a correct RES in an integrity protected sent REGISTER.

Upon receipt of a REGISTER request with the integrity-protection ~~field~~parameter set to 'no', ~~by the P-CSCF :for a user that is not registered, and for which also no authentication is currently ongoing (i.e. timer reg-await-auth is not running)~~, the S-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) check the value of the Expires header. The S-CSCF shall only proceed with the following procedures if the Expires header is set to a value greater than zero; if the Expires header is set to a value zero, ~~see subclause 5.4.1.4~~then S-CSCF shall proceed according to subclause 5.4.1.4

4) ~~4)~~ check how many authentications are ongoing for this user. The S-CSCF may – based on local policy – reject the request by sending a 403, if there are a number of ongoing authentications. If the S-CSCF decides to challenge the user, then proceed as follows.

5) select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

   Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-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];

NOTE ~~1~~2: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URL to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

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

6) remove the P-Access-Network-Info header and may act upon the contents accordingly;

7) challenge the user by generating a 401 (Unauthorized) response for the received REGISTER request, including a WWW-Authenticate header which transports:

   - the home network identification in the realm field;
   - the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;
   - the security mechanism, which is AKAv1-MD5, in the algorithm field;
   - the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2.3);
   - optionally the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2.3);

8) send the so generated 401 (Unauthorized) response towards the UE; and,

9) start timer reg-await-auth which guards the receipt of the next REGISTER request.

~~While timer reg-await-auth is running, upon receipt of a REGISTER request, the S-CSCF shall:~~

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

2) stop timer reg-await-auth;

3) check whether the P-CSCF included the Integrity-protection field of the Authorization header set to yes, indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps it the integrity check parameter is included;

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

- the private user identity of the user in the username field;
- the algorithm which is AKAv1-MD5 in the algorithm field; and
- the RES parameter needed for the authentication procedure in the response field.

The S-CSCF shall only proceed with the following steps in this paragraph if the RES parameter was included;

5) check whether the received RES parameter and the XRES parameter 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 RES and XRES are matching;

6) 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:

- 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,
- the user profile of the user including initial Filter Criteria;

7) bind to each non-barred registered public user identity all registered contact information;

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.

8) 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.

9) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may adjust the duration of the registration due to local policy;

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

11)remove the P-Access-Network-Info header and may act upon the contents accordingly;

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

- an expiration time in the Expires header, using one value provided within the S-CSCF, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE; and,
- the list of received Path headers;
- a P-Associated-URI header containing the list of public user identities that the user is authorized to use. Such a collection of public user identities may or may not be implicitly registered by the network. Using information supplied by the HSS, the P-Associated-URI header will indicate the default public user identity to be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header;

Editor's note: The mechanism for indicating this default public user identity is yet to be agreed.

- a P-Service-Route header containing:
  - the SIP URL identifying the S-CSCF; and,
  - an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) shall be treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part or be a port number;
  - if network topology hiding is required a SIP URL identifying an I-CSCF(THIG) as the topmost entry;

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

14) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server 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.

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

5.4.1.2.2 User-initiated reregistrationProtected REGISTER

Upon receipt of a REGISTER request for an already registered userwith the integrity-protection fieldparameter set to ='yes', the S-CSCF shall:

EnsureIn the case that that there is no authentication currently ongoing for this user -(i.e. no timer reg-await-auth is not running) and

1) identify the user by the public user identity as received in the To header and the private user identity as received in the From header of the REGISTER request;

2) check whether the P-CSCF included the Integrity-protection field of the Authorization header set to yes, indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps if the field is set to yes;

23) 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;

34) 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 proceed with the procedures as described for the second REGISTER in subclause 5.4.1.2, beginning with step 7); and

45) remove the P-Access-Network-Info header and may act upon the contents accordingly.

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

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

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

3) stop timer reg-await-auth;

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

- the private user identity of the user in the username field;

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

- the RES parameter needed for the authentication procedure in the response field.

The S-CSCF shall only proceed with the following steps in this paragraph if the RES parameter was included;

54) check whether the received RES parameter and the XRES parameter 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 RES and XRES are matching;

65) 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:

- 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,

- the user profile of the user including initial Filter Criteria;

76) bind to each non-barred registered public user identity all registered contact information;

NOTE 21: There might be more then one contact information available for one public user identity.

NOTE 32: The barred public user identities are not bound to the contact information.

87) 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 43: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

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

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

110) remove the P-Access-Network-Info header and may act upon the contents accordingly;

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

- an expiration time in the Expires header, using one value provided within the S-CSCF, ~~according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE~~; and,

- the list of received Path headers;

- a P-Associated-URI header containing the list of public user identities that the user is authorized to use. Such a collection of public user identities may or may not be implicitly registered by the network. Using information supplied by the HSS, the P-Associated-URI header will indicate the default public user identity to be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header;

Editor's note: The mechanism for indicating this default public user identity is yet to be agreed.

- a P-Service-Route header containing:

  - the SIP URL identifying the S-CSCF; and,

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

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

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

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

NOTE 54: If this registration is a reregistration, the Filter Criteria already exists in the local data.

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