

**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 to** Work Item "IMS-CCR", that have been agreed by **TSG CN WG1 in CN1#32 meeting**, and are forwarded to TSG CN Plenary meeting #22 for approval.

Approval should be made conditional to corresponding SA3 CR(s) approval.

<b>TDoc #</b>	<b>Tdoc Title</b>	<b>Spec</b>	<b>CR #</b>	<b>Rev</b>	<b>CAT</b>	<b>C_Version</b>	<b>Rel</b>
N1-031711	Correct use of RAND during re-synchronisation failures	24.229	523	2	F	5.6.0	Rel-5
N1-031712	Correct use of RAND during re-synchronisation failures	24.229	524	2	A	6.0.0	Rel-6

CR-Form-v7

## CHANGE REQUEST

⌘ **24.229 CR 523** ⌘ rev **2** ⌘ Current version: **5.6.0** ⌘

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

**Proposed change affects:** UICC apps ⌘  ME  Radio Access Network  Core Network

<b>Title:</b>	⌘ Correct use of RAND during re-synchronisation failures		
<b>Source:</b>	⌘ 3, Nokia, Vodafone		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 13/10/2003
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel 5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	<b>F</b> (correction)		2 (GSM Phase 2)
	<b>A</b> (corresponds to a correction in an earlier release)		R96 (Release 1996)
	<b>B</b> (addition of feature),		R97 (Release 1997)
	<b>C</b> (functional modification of feature)		R98 (Release 1998)
	<b>D</b> (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

<b>Reason for change:</b>	⌘ At a re-synchronisation failure, the RAND sent to the HSS must be the one stored by the S-CSCF and not the RAND passed back to the network by the UE. This needs to be made explicit in the text. This change is in line with the request received in liaison statement from SA3 in S3-030616, and is dependent upon CRs to 33.203 being approved.
<b>Summary of change:</b>	⌘ It is made explicit that S-CSCF store the RAND sent to the UE and uses this RAND if there is a re-synchronisation failure..
<b>Consequences if not approved:</b>	⌘ An implementation not doing the above will allow a replay of re-synchronisation response.

<b>Clauses affected:</b>	⌘ 5.4.1.2.1, 5.4.1.2.3										
<b>Other specs affected:</b>	<table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other core specifications	⌘
Y	N										
<input type="checkbox"/>	<input type="checkbox"/>										
<input checked="" type="checkbox"/>	<input type="checkbox"/>										
<input checked="" type="checkbox"/>	<input type="checkbox"/>										
		Test specifications									
		O&M Specifications									
<b>Other comments:</b>	⌘										

**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 Unprotected REGISTER

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

NOTE 2: A REGISTER with Expires header value equal to zero should always be received protected. However, it is possible that in error conditions a REGISTER with Expires header value equal to zero may be received unprotected. In that instance the procedures below will be applied.

Upon receipt of a REGISTER request with the integrity-protection parameter set to 'no', 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 how many authentications are ongoing for this user. The S-CSCF may – based on local policy – reject the request by sending a 403 (Forbidden) response, if there are a number of ongoing authentications. The response may include a Warning header containing the warn-code 399. If the S-CSCF decides to challenge the user, then proceed as follows;
- 4) 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 3: 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 URI 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) 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 7.2A.1); and
  - ~~the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2A.1);~~

7) store the RAND parameter used in the 401 (Unauthorized) response for future use in case of a resynchronisation. If a stored RAND already exists in the S-CSCF, the S-CSCF shall overwrite the stored RAND with the RAND used in the most recent 401 (Unauthorized) response;

~~Note : the RAND parameter needs to be stored by S-CSCF for future use in case of a synchronisation failure.~~

~~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.~~

If the received REGISTER request indicates that the challenge sent previously by the S-CSCF to the UE was deemed to be invalid by the UE, the S-CSCF shall stop the timer reg-await-auth and proceed as described in the subclause 5.4.1.2.3.

#### 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 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;

- 4) 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;
- 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 than 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;

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.

#### 5.4.1.2.3 Abnormal cases

The S-CSCF need not challenge an unprotected REGISTER request for a private user identity that already has a registration in process, but instead return a 500 (Server Internal Error) response. The response shall contain a Retry-After header with a value indicating a time the UE shall wait before resending the request.

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), the S-CSCF shall:

- send a 403 (Forbidden) response to the UE. The S-CSCF shall consider this authentication attempt as failed. The S-CSCF shall not update the registration time of the subscriber.

NOTE 1: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request, which was supposed to carry the response to the challenge, contains no RES and no AUTS parameters indicating that the MAC parameter was invalid in the challenge, the S-CSCF shall:

- respond with a 403 (Forbidden) response to the UE. The S-CSCF shall not update the registration time of the subscriber.

NOTE 2: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid (contains the AUTS parameter indicating this), the S-CSCF will fetch new authentication vectors from the HSS. ~~In order to indicate a resynchronisation, the S-CSCF shall include the including~~ AUTS ~~received from the UE~~ and ~~the stored RAND, in the request when fetching the new authentication vectors, to~~ ~~indicate a resynchronisation.~~ On receipt of ~~these~~ the new authentication vectors from the HSS, the S-CSCF shall either:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors; or
- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned.

NOTE 3: Since the UE responds only to two consecutive challenges, the S-CSCF will send a 401 (Unauthorized) response that contains a new challenge only twice.

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the AS, the S-CSCF shall not initiate network-initiated deregistration procedure.

In the case that the REGISTER request from the UE contains more than one SIP URIs as Contact header entries, the S-CSCF shall only store the entry with the highest "q" value and include it in the 200 (OK) response.

NOTE 4: If the timer reg-await-auth expires, the S-CSCF will consider the authentication to have failed. If the public user identity was already registered, the S-CSCF will leave it as registered described in 3GPP TS 33.203 [19]. The operator's policy will specify when will, upon authentication failure, the currently registered public user identity or the user be de-registered by the S-CSCF.

CR-Form-v7

## CHANGE REQUEST

⌘ **24.229 CR 524** ⌘ rev **2** ⌘ Current version: **6.0.0** ⌘

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

<b>Title:</b>	⌘ Correct use of RAND during re-synchronisation failures		
<b>Source:</b>	⌘ 3, Nokia, Vodafone		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 13/10/2003
<b>Category:</b>	⌘ <b>A</b>	<b>Release:</b>	⌘ Rel 6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	<b>F</b> (correction)	<b>2</b>	(GSM Phase 2)
	<b>A</b> (corresponds to a correction in an earlier release)	<b>R96</b>	(Release 1996)
	<b>B</b> (addition of feature),	<b>R97</b>	(Release 1997)
	<b>C</b> (functional modification of feature)	<b>R98</b>	(Release 1998)
	<b>D</b> (editorial modification)	<b>R99</b>	(Release 1999)
	Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<b>Rel-4</b> (Release 4)
			<b>Rel-5</b> (Release 5)
			<b>Rel-6</b> (Release 6)

<b>Reason for change:</b>	⌘ At a re-synchronisation failure, the RAND sent to the HSS must be the one stored by the S-CSCF and not the RAND passed back to the network by the UE. This needs to be made explicit in the text. This change is in line with the request received in liaison statement from SA3 in S3-030616, and is dependent upon CRs to 33.203 being approved.
<b>Summary of change:</b>	⌘ It is made explicit that S-CSCF store the RAND sent to the UE and uses this RAND if there is a re-synchronisation failure..
<b>Consequences if not approved:</b>	⌘ An implementation not doing the above will allow a replay of re-synchronisation response.

<b>Clauses affected:</b>	⌘ 5.4.1.2.1, 5.4.1.2.3										
<b>Other specs affected:</b>	<table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other core specifications	⌘
Y	N										
<input type="checkbox"/>	<input type="checkbox"/>										
<input checked="" type="checkbox"/>	<input type="checkbox"/>										
<input checked="" type="checkbox"/>	<input type="checkbox"/>										
		Test specifications									
		O&M Specifications									
<b>Other comments:</b>	⌘										

### 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 Unprotected REGISTER

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

NOTE 2: A REGISTER with Expires header value equal to zero should always be received protected. However, it is possible that in error conditions a REGISTER with Expires header value equal to zero may be received unprotected. In that instance the procedures below will be applied.

Upon receipt of a REGISTER request with the integrity-protection parameter set to 'no', 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 how many authentications are ongoing for this user. The S-CSCF may – based on local policy – reject the request by sending a 403 (Forbidden) response, if there are a number of ongoing authentications. The response may include a Warning header containing the warn-code 399. If the S-CSCF decides to challenge the user, then proceed as follows;
- 4) 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 3: 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 URI 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) 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 7.2A.1); and
  - ~~the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2A.1);~~
- 7) store the RAND parameter used in the 401 (Unauthorized) response for future use in case of a resynchronisation. If a stored RAND already exists in the S-CSCF, the S-CSCF shall overwrite the stored RAND with the RAND used in the most recent 401 (Unauthorized) response;

~~Note : the RAND parameter needs to be stored by S-CSCF for future use in case of a synchronisation failure.~~

~~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.

If the received REGISTER request indicates that the challenge sent previously by the S-CSCF to the UE was deemed to be invalid by the UE, the S-CSCF shall stop the timer reg-await-auth and proceed as described in the subclause 5.4.1.2.3.

#### 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 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;

- 4) 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;
- 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 than 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;

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.

#### 5.4.1.2.3 Abnormal cases

The S-CSCF need not challenge an unprotected REGISTER request for a private user identity that already has a registration in process, but instead return a 500 (Server Internal Error) response. The response shall contain a Retry-After header with a value indicating a time the UE shall wait before resending the request.

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), the S-CSCF shall:

- send a 403 (Forbidden) response to the UE. The S-CSCF shall consider this authentication attempt as failed. The S-CSCF shall not update the registration time of the subscriber.

NOTE 1: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request, which was supposed to carry the response to the challenge, contains no RES and no AUTS parameters indicating that the MAC parameter was invalid in the challenge, the S-CSCF shall:

- respond with a 403 (Forbidden) response to the UE. The S-CSCF shall not update the registration time of the subscriber.

NOTE 2: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid (contains the AUTS parameter indicating this), the S-CSCF will fetch new authentication vectors from the HSS. ~~In order to indicate a resynchronisation, the S-CSCF shall include the including AUTS received from the UE and the stored RAND, in the request when fetching the new authentication vectors. to indicate a resynchronisation.~~ On receipt of ~~these~~ the new authentication vectors from the HSS, the S-CSCF shall either:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors; or
- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned.

NOTE 3: Since the UE responds only to two consecutive challenges, the S-CSCF will send a 401 (Unauthorized) response that contains a new challenge only twice.

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the AS, the S-CSCF shall not initiate network-initiated deregistration procedure.

In the case that the REGISTER request from the UE contains more than one SIP URIs as Contact header entries, the S-CSCF shall only store the entry with the highest "q" value and include it in the 200 (OK) response.

NOTE 4: If the timer reg-await-auth expires, the S-CSCF will consider the authentication to have failed. If the public user identity was already registered, the S-CSCF will leave it as registered described in 3GPP TS 33.203 [19]. The operator's policy will specify when will, upon authentication failure, the currently registered public user identity or the user be de-registered by the S-CSCF.