3GPP TSG CN Plenary Meeting #22 **NP-030478**
10th - 12th December 2003. Hawaii, USA.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 (with mirror CRs) on Work Item IMS-CCR towards 24.229,- pack 3**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **9** CRs, **Rel-5 with mirrors 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.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Version	Rel
N1-031616	Correction to description or RES/XRES usage	24.229	525	1	F	5.6.0	Rel-5
N1-031617	Correction to description or RES/XRES usage	24.229	526	1	A	6.0.0	Rel-6
N1-031618	Correction of user initiated re-registration	24.229	542	1	F	5.6.0	Rel-5
N1-031619	Correction of user initiated re-registration	24.229	543	1	A	6.0.0	Rel-6
N1-031621	IMS trust domain in Rel 5	24.229	550	1	F	5.6.0	Rel-5
N1-031623	P-CSCF and UE handling of Security Associations	24.229	555	1	F	5.6.0	Rel-5
N1-031624	P-CSCF and UE handling of Security Associations	24.229	556	1	A	6.0.0	Rel-6
N1-031579	Sending challenge	24.229	565		F	5.6.0	Rel-5
N1-031580	Sending challenge	24.229	566		A	6.0.0	Rel-6

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031616**
Bangkok, Thailand, 27 – 31 October 2003 **(Revision of N1-031447)**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **525** ⌘ **rev** **1** ⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Correction to description or RES/XRES usage
Source:	⌘	3, Nokia, Vodafone
Work item code:	⌘	IMS-CCR
Date:	⌘	13/10/2003
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 RES parameter is not sent in an authentication challenge response but is used to calculate the authentication repsonse (along with other parameters). The RES is used as the key for the process of generating the respoinse as defined in RFC3310. RFC3310 states that this is so that the key used for generating the response is not sent in clear text and so avoiding a possible security risk. The CRs also align with the changes agreed by SA3 in S3-030601.
Summary of change:	⌘	Text is changed to say that the response calculated using RES (and other parameters) is sent from the UE to the S-CSCF rather than RES itself. It is also clarified that the response is checked against an expected response calculated from XRES. RES and XRES are replaced with the term 'authentication challenge response' and 'expected challenge response' in a number of places, and the generation of the response and expected response is noted to be as per RFC3310 using RES/XRES in the appropriate places.
Consequences if not approved:	⌘	The text will not be inline with RFC 3310. Implementations may be incorrect as they may include RES rather than the result of the calculation based on RES (and other parameters). The specification will not be aligned with the CRs agreed by SA3 (S3-030601).

Clauses affected:	⌘	5.1.1.5.1, 5.1.1.5.3, 5.4.1.2.1, 5.4.1.2.2, 5.4.1.2.3			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	TS 24.228 (CR 119)
		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.

5.1.1.5.1 General

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

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

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header as described in RFC 3329 [48]. If the header is not present or it does not contain the parameters required for the setup of the security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

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

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up two new pairs of security associations based on the static list and parameters it received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header in the REGISTER request. The UE sets up two pairs of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK as the shared key. The UE shall use the parameters received in the Security-Server header to setup the security associations. The UE shall set a temporary SIP level lifetime for the newly setup security associations to a value which has to be long enough to permit the UE to finalize the registration procedure (longer than 64*T1); and

3) send another REGISTER request using the new security association to protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response ~~(~~calculated by the UE using RES and other parameter~~s)~~, as described in RFC 3310 [49]. The UE shall also insert the Security-Client header that is identical to the Security-Client header that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header into the request, by mirroring in it the content of the Security-Server header received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the integrity protected REGISTER request which carries the authentication challenge response~~RES must shall be~~to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the integrity protected REGISTER request, the UE shall:

- set the security association lifetime to the longest of either the previously existing SA lifetime, or the lifetime of the just completed registration plus 30 seconds;

- send subsequent requests towards the P-CSCF using the new security associations;

- send the responses toward the P-CSCF over the same security association that the associated request was received; and

- receive the responses from the P-CSCF over the same security association that the associated request was sent.

When the first request or response protected with the newly set up security association is received from the P-CSCF, the UE shall delete the old security associations and related keys it may have with the P-CSCF after all SIP transactions that use the old security associations are completed.

Whenever the 200 (OK) response is not received before the temporary SIP level lifetime of the new security associations expires, the UE shall consider the registration to have failed. The UE shall delete the new security associations it was trying to establish, and use the old security associations. The UE should send an unprotected REGISTER message according to the procedure specified in subclause 5.1.1.2 if the UE considers the earlier established security associations to be no longer active at the P-CSCF.

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

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 <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.

5.1.1.5.3 Abnormal cases

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

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no authentication challenge response~~RES~~ and no AUTS parameter;
- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the AUTS parameter and not an authentication challenge response ~~RES parameter~~ (see 3GPP TS 33.102 [18]).

The UE shall send the REGISTER request using an existing security association, if available (see 3GPP TS 33.203 [19]). The REGISTER request shall contain a new Security-Client header, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup.

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

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~~ authentication challenge response 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) send the so generated 401 (Unauthorized) response towards the UE; and,

8) 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 authentication challenge response~~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 authentication challenge response~~RES parameter~~ was included;

4) check whether the received ~~RES parameter~~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])~~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~~the challenage response received from the UE and the expected response calculated by the S-CSCF match ~~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 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;

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 challenge response ~~(RES)~~ from the UE does not match with ~~XRES~~the expected authentication challenge response 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~~authentication challenge response 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 challenge 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, including AUTS and RAND in the request to indicate a resynchronisation. On receipt of these 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.

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031617**
Bangkok, Thailand, 27 – 31 October 2003 **(Revision of N1-031448)**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **526** ⌘ **rev** **1** ⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Correction to description or RES/XRES usage
Source:	⌘	3, Nokia, Vodafone
Work item code:	⌘	IMS-CCR
Date:	⌘	13/10/2003
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 RES parameter is not sent in an authentication challenge response but is used to calculate the authentication repsonse (along with other parameters). The RES is used as the key for the process of generating the respoinse as defined in RFC3310. RFC3310 states that this is so that the key used for generating the response is not sent in clear text and so avoiding a possible security risk. The CRs also align with the changes agreed by SA3 in S3-030601.
Summary of change:	⌘	Text is changed to say that the response calculated using RES (and other parameters) is sent from the UE to the S-CSCF rather than RES itself. It is also clarified that the response is checked against an expected response calculated from XRES. RES and XRES are replaced with the term 'authentication challenge response' and 'expected challenge response' in a number of places, and the generation of the response and expected response is noted to be as per RFC3310 using RES/XRES in the appropriate places.
Consequences if not approved:	⌘	The text will not be inline with RFC 3310. Implementations may be incorrect as they may include RES rather than the result of the calculation based on RES (and other parameters). The specification will not be aligned with the CRs agreed by SA3 (S3-030601).

Clauses affected:	⌘	5.1.1.5.1, 5.1.1.5.3, 5.4.1.2.1, 5.4.1.2.2, 5.4.1.2.3			
Other specs affected:	⌘	**Y** / **N** **X** / ( ) ( ) / **X**	Other core specifications Test specifications	⌘	TS 24.228 (CR 119)

	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.

5.1.1.5.1 General

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

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

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header as described in RFC 3329 [48]. If the header is not present or it does not contain the parameters required for the setup of the security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

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

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up two new pairs of security associations based on the static list and parameters it received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header in the REGISTER request. The UE sets up two pairs of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK as the shared key. The UE shall use the parameters received in the Security-Server header to setup the security associations. The UE shall set a temporary SIP level lifetime for the newly setup security associations to a value which has to be long enough to permit the UE to finalize the registration procedure (longer than 64*T1); and

3) send another REGISTER request using the new security association to protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response ~~(~~calculated by the UE using RES and other parameter~~s)~~, as described in RFC 3310 [49]. The UE shall also insert the Security-Client header that is identical to the Security-Client header that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header into the request, by mirroring in it the content of the Security-Server header received in the 401 (Unauthorized) response. The UE shall set t~~T~~he Call-ID of the integrity protected REGISTER request which carries the authentication challenge response~~RES must shall be~~to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the integrity protected REGISTER request, the UE shall:

- set the security association lifetime to the longest of either the previously existing SA lifetime, or the lifetime of the just completed registration plus 30 seconds;

- send subsequent requests towards the P-CSCF using the new security associations;

- send the responses toward the P-CSCF over the same security association that the associated request was received; and

- receive the responses from the P-CSCF over the same security association that the associated request was sent.

When the first request or response protected with the newly set up security association is received from the P-CSCF, the UE shall delete the old security associations and related keys it may have with the P-CSCF after all SIP transactions that use the old security associations are completed.

Whenever the 200 (OK) response is not received before the temporary SIP level lifetime of the new security associations expires, the UE shall consider the registration to have failed. The UE shall delete the new security associations it was trying to establish, and use the old security associations. The UE should send an unprotected REGISTER message according to the procedure specified in subclause 5.1.1.2 if the UE considers the earlier established security associations to be no longer active at the P-CSCF.

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

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 <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.

5.1.1.5.3 Abnormal cases

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

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no authentication challenge response~~RES~~ and no AUTS parameter;
- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the AUTS parameter and not an authentication challenge response ~~RES parameter~~ (see 3GPP TS 33.102 [18]).

The UE shall send the REGISTER request using an existing security association, if available (see 3GPP TS 33.203 [19]). The REGISTER request shall contain a new Security-Client header, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup.

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

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~~ authentication challenge response 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) send the so generated 401 (Unauthorized) response towards the UE; and,

8) 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 authentication challenge response~~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 authentication challenge response~~RES parameter~~ was included;

4) check whether the received ~~RES parameter~~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])~~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~~the challenage response received from the UE and the expected response calculated by the S-CSCF match~~ 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 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;

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 challenge response ~~(RES)~~ from the UE does not match with ~~XRES~~the expected authentication challenge response 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~~authentication challenge response 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 challenge 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, including AUTS and RAND in the request to indicate a resynchronisation. On receipt of these 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.

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031618**
Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **542** ⌘ **rev** **1** ⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Security-Verify header in Reregistration
Source:	⌘	Siemens, Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	10/10/2003
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:	⌘	During the CN1-SA3 workshop it was clarified that in order to have consistency in the procedures all REGISTER request sent by the UE shall contain a Secrutiy-Verify header.
Summary of change:	⌘	In a reREGISTER request the UE inserts a Secrutiy-Verify header. The P-CSCF shall remove this header in a reREGISTER request before forwarding the request..
Consequences if not approved:	⌘	Incorrect specification

Clauses affected:	⌘	5.1.1.4, 5.2.2

	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.

*********1.st change*********

5.1.1.4 User-initiated re-registration

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

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less.

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

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be registered;

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

d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;

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

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

e) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network;

g) ~~g)~~a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the new parameter~~s~~ values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

h) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication;

~~h~~i) the Supported header containing the option tag "path"; and

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

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the new expiration time of the registration for this public user identity found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs; and

d) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

******* next change *******

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

1) insert a Path header in the request including an entry containing:

   - the SIP URI identifying the P-CSCF;

   - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

2) insert a Require header containing the option tag "path";

3) for the initial REGISTER request for a public user identity create a new, globally unique value for icid, save it locally and insert it into the icid parameter of the P-Charging-Vector header;

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication response, or it was received on the security association created during the last successful authentication procedure and with no authentication response, otherwise insert the parameter with the value "no";

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'sec-agree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:

   a) check the security association which protected the request. If that has a temporary lifetime, and the REGISTER request was received protected with the new security association, then the request shall contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;

   b) if the security association the REGISTER request was received on, is an already established one, then:

      - ~~a Security-Verify header is not expected to be included. If~~ the P-CSCF shall remove the Security-Verify header if it is present, ~~then the P-CSCF shall remove that header~~ and the "sec-agree" item from the Require header, and the header itself if this is the only entry; ~~together with the 'Require: sec-agree' header;~~

- a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;

- the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and

c) check if the private user identity conveyed in the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and

8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

1) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;

2) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms. The P-CSCF shall support the setup of two pairs of security associations. For further information see 3GPP TS 33.203 [19]; and

3) set up the new security associations with a temporary lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set a temporary SIP level lifetime for the security association which has to be long enough to permit the UE to finalize the registration procedure (bigger than 64*T1).

4) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

2) associate the Service-Route header list with the registered public user identity;

3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;

4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more then one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

5) store the values received in the P-Charging-Function-Addresses header;

6) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds; and

7) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

The P-CSCF shall:

- if new security associations are established and there are no old security associations, start using the new security associations towards the UE after the 200 (OK) has been sent out;
- if a request protected within the newly established security associations is received from a UE which has old security associations, delete the old security associations and related keys when all SIP transactions that use the old security associations are completed;
- if the newly established security associations has not been taken into use by the UE and the UE sends request protected on the old security associations, delete the new security associations; and
- if the newly established security associations are a result of an unprotected REGISTER request being received from the UE, then delete the old security associations which may exist towards the UE.

NOTE 3: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routeing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031619**
Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **543** ⌘**rev** **1** ⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Security-Verify header in Reregistration
Source:	⌘	Siemens, Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	10/10/2003
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:	⌘	During the CN1-SA3 workshop it was clarified that in order to have consistency in the procedures all REGISTER request sent by the UE shall contain a Secrutiy-Verify header.
Summary of change:	⌘	In a reREGISTER request the UE inserts a Secrutiy-Verify header. The P-CSCF shall remove this header in a reREGISTER request before forwarding the request..
Consequences if not approved:	⌘	Incorrect specification

Clauses affected:	⌘	5.1.1.4, 5.2.2

	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.

*********1.st change*********

5.1.1.4 User-initiated re-registration

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

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less.

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

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be registered;

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

d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;

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

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

e) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network;

g) ~~g)~~ a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the new parameter~~s~~ values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

h) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication;

~~h~~i) the Supported header containing the option tag "path"; and

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

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the new expiration time of the registration for this public user identity found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs; and

d) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

******* next change *******

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

1) insert a Path header in the request including an entry containing:

   - the SIP URI identifying the P-CSCF;

   - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

2) insert a Require header containing the option tag "path";

3) for the initial REGISTER request for a public user identity create a new, globally unique value for icid, save it locally and insert it into the icid parameter of the P-Charging-Vector header;

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication response, or it was received on the security association created during the last successful authentication procedure and with no authentication response, otherwise insert the parameter with the value "no";

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'sec-agree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:

   a) check the security association which protected the request. If that has a temporary lifetime, and the REGISTER request was received protected with the new security association, then the request shall contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;

   b) if the security association the REGISTER request was received on, is an already established one, then:

      - ~~a Security-Verify header is not expected to be included. If~~ the P-CSCF shall remove the Security-Verify header if it is present, ~~then the P-CSCF shall remove that header~~ and the "sec-agree" item from the Require header, and the header itself if this is the only entry;~~together with the 'Require: sec-agree' header;~~

- a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;

- the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and

-c) check if the private user identity conveyed in the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and

8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

1) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;

2) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms. The P-CSCF shall support the setup of two pairs of security associations. For further information see 3GPP TS 33.203 [19]; and

3) set up the new security associations with a temporary lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set a temporary SIP level lifetime for the security association which has to be long enough to permit the UE to finalize the registration procedure (bigger than 64*T1).

4) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

2) associate the Service-Route header list with the registered public user identity;

3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;

4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more then one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

5) store the values received in the P-Charging-Function-Addresses header;

6) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds; and

7) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

The P-CSCF shall:

- if new security associations are established and there are no old security associations, start using the new security associations towards the UE after the 200 (OK) has been sent out;
- if a request protected within the newly established security associations is received from a UE which has old security associations, delete the old security associations and related keys when all SIP transactions that use the old security associations are completed;
- if the newly established security associations has not been taken into use by the UE and the UE sends request protected on the old security associations, delete the new security associations; and
- if the newly established security associations are a result of an unprotected REGISTER request being received from the UE, then delete the old security associations which may exist towards the UE.

NOTE 3: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routeing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031621**

was N1-031541

Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **550** ⌘ **rev** **1** ⌘ 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 ☒

Title:	⌘	IMS trust domain in Rel 5
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	27/10/2003
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 concept of the IMS trust domain has been recently discussed in a joint SA3-CN1 session. This CR clarifies that Release 5 is a closed network and there are no requirements on removal of the P-Asserted-Identity
Summary of change:	⌘	Release 5 is a closed network. Nodes need no take an action on the removal of the P-Asserted-Identity
Consequences if not approved:	⌘	It is not clear whether a node need to remove the P-Asserted-Identity or not. On the absence of such text, some IMS nodes may remove the P-Asserted-Identity and it might not be possible to identify the originator of a session attempt.

Clauses affected:	⌘	4.4

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

Other comments:	⌘	

4.4 Trust domain

RFC 3325 [34] provides for the existence and trust of an asserted identity within a trust domain. For the IM CN subsystem, this trust domain consists of the P-CSCF, the I-CSCF, the S-CSCF, the BGCF. the MGCF, the MRFC, and all ASs that are not provided by third-party service providers. ASs provided by third-party service providers are outside the trust domain. Except when communicating with the UE, functional entities within the trust domain can safely consider that there are no requirements to take an action on the removal of the P-Asserted-Identity header, unless otherwise explicitly stated.

For the purpose of the P-Access-Network-Info header, a trust domain also applies. This trust domain is identical to that of the P-Asserted-Identity. For the P-Access-Network-Info header, subclause 5.4 also identifies additional cases for the removal of the header.

NOTE: In addition to the procedures specified in clause 5, procedures of RFC 3325 [34] in relation to transmission of P-Asserted-Identity headers and their contents outside the trust domain also apply.

3GPP TSG-CN1 Meeting #32
Bangkok, Thailand, 27 – 31 October 2003

Tdoc N1-031623~~547~~

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **555** ⌘ **rev** **-1** ⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	P-CSCF and UE handling of Security Associations
Source:	⌘	Nokia, 3, Siemens, Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	08/10/2003
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 description of handling of Security Associations in 24.229 is not completely in-line with the procedures described in 33.203
Summary of change:	⌘	Handling of SAs is aligned.
Consequences if not approved:	⌘	SA3 and CN1 documents are not in-line.

Clauses affected:	⌘	3.1, 5.1.1.5.1, 5.1.1.5.3, 5.2.2

	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.

First Change

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Newly established set of security associations: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF after the 200(OK) response to a REGISTER request was received.

Old set of security associations: Two pairs of IPsec security associations after another set of security associations has been established due to a successful authentication procedure.

Temporary set of security associations: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF, after an authentication challenge within a 401 (Unauthorized) response to a REGISTER request was received. The SIP level lifetime of such created security associations will be equal to the value of reg-await-auth timer.

For the purposes of the present document, the following terms and definitions given in RFC 1594 [20B].

Fully-Qualified Domain Name (FQDN)

For the purposes of the present document, the following terms and definitions given in RFC 3261 [26] apply (unless otherwise specified see clause 6).

Back-to-Back User Agent (B2BUA)
Client
Dialog
Final response
Header
Header field
Loose routeing
Method
Option-tag (see RFC 3261 [26] subclause 19.2)
Provisional response
Proxy, proxy server
Redirect server
Registrar
Request
Response
Server
Session
(SIP) transaction
Stateful proxy
Stateless proxy
Status-code (see RFC 3261 [26] subclause 7.2)
Tag (see RFC 3261 [26] subclause 19.3)
Target Refresh Request
User agent client (UAC)
User agent server (UAS)
User agent (UA)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2] subclause 4.1.1.1 and subclause 4a.7 apply:

Breakout Gateway Control Function (BGCF)
Call Session Control Function (CSCF)
Home Subscriber Server (HSS)
Media Gateway Control Function (MGCF)
Media Resource Function Controller (MRFC)
Subscription Locator Function (SLF)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.218 [5] subclause 3.1 apply:

Filter criteria
Initial filter criteria
Initial request
Standalone transaction
Subsequent request

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclause 4.3.3.1 and subclause 4.6 apply:

Interrogating-CSCF (I-CSCF)
Policy Decision Function (PDF)
Private user identity
Proxy-CSCF (P-CSCF)
Public user identity
Serving-CSCF (S-CSCF)

For the purposes of the present document, the following terms and definitions given in 3GPP TR 33.203 [19] apply:

Protected Server Port
Protected Client Port

For the purposes of the present document, the following terms and definitions given in 3GPP TR 21.905 [1] apply:

User Equipment (UE)

For the purposes of the present document, the following terms and definitions given in RFC 2401 [20A] Appendix A apply:

Security association

NOTE: A number of different security associations exist within the IM CN subsystem. Within this document the term specifically applies to the security association that exists between the UE and the P-CSCF, as this is the only security association that has direct impact on SIP.

For the purposes of the present document, the following terms and definitions given in ITU-T E.164 [57] apply:

International public telecommunication number

Second Change

5.1.1.5 Authentication

5.1.1.5.1 General

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

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

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header as described in RFC 3329 [48]. If the header is not present or it does not contain the parameters required for the setup of the ~~security associations~~set of security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

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

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up ~~two new pairs of security associations~~a temporary set of security associations based on the static list and parameters it received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header in the REGISTER request. The UE sets up ~~two pairs of security associations~~the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK as the shared key. The UE shall use the parameters received in the Security-Server header to setup the ~~security associations.~~temporary set of security associations. The UE shall set a temporary SIP level lifetime for the ~~newly setup security associations to a value which has to be long enough to permit the UE to finalize the registration procedure (longer than 64*T1);~~temporary set of security associations to the value of reg-await-auth timer; and

3) send another REGISTER request using the ~~new security association~~temporary set of security associations to protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response (RES parameter), as described in RFC 3310 [49]. The UE shall also insert the Security-Client header that is identical to the Security-Client header that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header into the request, by mirroring in it the content of the Security-Server header received in the 401 (Unauthorized) response. The Call-ID of the integrity protected REGISTER request which carries RES must be the same as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the integrity protected REGISTER request, the UE shall:

- ~~set the security association~~change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing ~~SA~~set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

- ~~send subsequent requests towards the P-CSCF using the new security associations;~~

~~send the responses toward the P-CSCF over the same security association that the associated request was received; and~~

~~receive the responses from the P-CSCF over the same security association that the associated request was sent.~~use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

NOTE: In this case, the UE will send requests towards the P-CSCF over the newly established set of security associations. Responses towards the P-CSCF that are sent via UDP will be sent over the newly established set of security associations. Responses towards the P-CSCF that are sent via TCP will be sent over the same set of security associations that the related request was received on.

When the first request or response protected with the newly ~~set up security association~~established set of security associations is received from the P-CSCF, the UE shall delete the old ~~security associations~~set of security associations and related keys it may have with the P-CSCF after all SIP transactions that use the old ~~security associations~~set of security associations are completed.

Whenever the 200 (OK) response is not received before the temporary SIP level lifetime of the ~~new security associations~~temporary set of security associations expires or a 403 (Forbidden) response is received, the UE shall consider the registration to have failed. The UE shall delete the ~~new security associations~~temporary set of security

associations it was trying to establish, and use the old ~~security associations.~~set of security associations. The UE should send an unprotected REGISTER message according to the procedure specified in subclause 5.1.1.2 if the UE considers the ~~earlier established security associations~~old set of security associations to be no longer active at the P-CSCF.

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

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 <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.

5.1.1.5.3 Abnormal cases

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

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

~~The~~Whenever the UE detects any of the above cases, the UE shall:

- send the REGISTER request using an existing ~~security association,~~set of security associations, if available (see 3GPP TS 33.203 [19]);
- ~~3GPP TS 33.203 [19]). The REGISTER request shall contain~~ populate a new Security-Client header within the REGISTER request, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association ~~setup.~~setup; and
- not create a temporary set of security associations.

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

Third Change

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

1) insert a Path header in the request including an entry containing:
   - the SIP URI identifying the P-CSCF;

- an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

2) insert a Require header containing the option tag "path";

3) for the initial REGISTER request for a public user identity create a new, globally unique value for icid, save it locally and insert it into the icid parameter of the P-Charging-Vector header;

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication response, or it was received on the security association created during the last successful authentication procedure and with no authentication response, otherwise insert the parameter with the value "no";

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'sec-agree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:

- check the security association which protected the request. If ~~that has~~the security association is a temporary ~~lifetime, and the REGISTER request was received protected with the new security association,~~one, then the request ~~shall~~is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;

- if the security association the REGISTER request was received on, is an already established one, then:

  - a Security-Verify header is not expected to be included. If the Security-Verify header is present, then the P-CSCF shall remove that header together with the 'Require: sec-agree' header;

  - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;

  - the P-CSCF shall remove the Security-Client header before forwarding the request to the S-CSCF; and

- check if the private user identity conveyed in the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and

8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

1) delete any temporary set of security associations established towards the UE;

2~~1~~) ~~-~~remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and ~~security associations~~to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;

3~~2~~) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer ~~algorithms. The P-~~

~~CSCF shall support the setup of two pairs of security associations. For further information see 3GPP TS 33.203 [19]; and~~algorithms;

4) ~~3) set up the new security associations~~ set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set ~~a~~the temporary SIP level lifetime for the ~~security association which has to be long enough to permit the UE to finalize the registration procedure (bigger~~ temporary set of security associations to the value of reg-await-auth timer; and

~~than 64*T1).~~

~~4)~~5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

2) associate the Service-Route header list with the registered public user identity;

3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;

4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more then one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

5) store the values received in the P-Charging-Function-Addresses header;

6) ~~set the security association~~if a set of temporary security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing ~~security association~~set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

7) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

~~The P-CSCF shall:~~

- ~~if new security associations are established and there are no old security associations, start using the new security associations towards the UE after the 200 (OK) has been sent out;~~
- ~~if a request protected within the newly established security associations is received from a UE which has old security associations, delete the old security associations and related keys when all SIP transactions that use the old security associations are completed;~~
- ~~if the newly established security associations has not been taken into use by the UE and the UE sends request protected on the old security associations, delete the new security associations; and~~
- ~~if the newly established security associations are a result of an unprotected REGISTER request being received from the UE, then delete the old security associations which may exist~~

When receiving a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

1) reduce the SIP level lifetime lifetime of the old set of security associations towards the same UE to 64*T1 (if currently longer than 64*T1) ; and

2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e. take the newly established set of security associations into use).

NOTE 3: In this case, the P-CSCF will send requests towards the UE over the newly established set of security associations. Responses towards the UE that are sent via UDP will be sent over the newly established set of security associations. Responses towards the UE that are sent via TCP will be sent over the same set of security associations that the related request was received on.

NOTE 4: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorter than 64*T1 and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly estabslihed set of security associations for further messages towards the UE as appropriate (see Note 3).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;

2) keep the newly established set of security associations created during this authentication;

3) delete, if existing, any other set of security associations towards this UE immediately; and,

4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

When sending the 200 (OK) respone for a REGISTER request that concludes an initial authentication, i.e. the initial REGISTER request was received unprotected, the P-CSCF shall:

1) keep the newly established set of security associations created during this authentication;

2) delete, if existing, any otherset of security associations towards this UE immediately; and,

3) use the kept newly established set of security associations for further messages sent towards the UE.

~~NOTE 3:~~NOTE 5: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routeing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

The handling of the security associations at the P-CSCF is summarized in table 5.2.2.-1.

Table 5.2.2-1: Handling of security associations at the P-CSCF

	Temporary set of security associations	Newly established set of security associations	Old set of security associations
SIP message received over newly established set of security associations that have not yet been taken into use	No action	Take into use	Reduce SIP level lifetime to 64*T1, if lifetime is larger than 64*T1
SIP message received over old set of security associations	No action	No action	No action
Old set of security associations currently in use will expire in 64*T1	No action	Take into use	No action
Sending an authorization challenge within a 401 (Unauthorized) response for a REGISTER request	Create Remove any previously existing temporary set of security associations	No action	No action
Sending 200 (OK) response for REGISTER request that concludes re-authentication	Change to a newly established set of security associations	Convert to and treat as old set of security associations (see next column)	Continue using the old set of security associations over which the REGISTER request, that initiated the re-authentication was received. Delete all other old sets of security associations immediately
Sending 200 (OK) response for REGISTER request that concludes initial authentication	Change to a newly established set of security associations and take into use immediately	Convert to old set of security associations, i.e. delete	Delete

3GPP TSG-CN1 Meeting #32
Bangkok, Thailand, 27 – 31 October 2003

Tdoc N1-031624~~548~~

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **556** ⌘ **rev** **1-** ⌘ 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 ☒

Title:	⌘	P-CSCF and UE handling of Security Associations
Source:	⌘	Nokia, 3, Siemens, Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	08/10/2003
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 description of handling of Security Associations in 24.229 is not completely in-line with the procedures described in 33.203
Summary of change:	⌘	Handling of SAs is aligned.
Consequences if not approved:	⌘	SA3 and CN1 documents are not in-line.

Clauses affected:	⌘	3.1, 5.1.1.5.1, 5.1.1.5.3, 5.2.2			
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.

First Change

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Newly established set of security associations: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF after the 200(OK) response to a REGISTER request was received.

Old set of security associations: Two pairs of IPsec security associations after another set of security associations has been established due to a successful authentication procedure.

Temporary set of security associations: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF, after an authentication challenge within a 401 (Unauthorized) response to a REGISTER request was received. The SIP level lifetime of such created security associations will be equal to the value of reg-await-auth timer.

For the purposes of the present document, the following terms and definitions given in RFC 1594 [20B].

Fully-Qualified Domain Name (FQDN)

For the purposes of the present document, the following terms and definitions given in RFC 3261 [26] apply (unless otherwise specified see clause 6).

Back-to-Back User Agent (B2BUA)
Client
Dialog
Final response
Header
Header field
Loose routeing
Method
Option-tag (see RFC 3261 [26] subclause 19.2)
Provisional response
Proxy, proxy server
Redirect server
Registrar
Request
Response
Server
Session
(SIP) transaction
Stateful proxy
Stateless proxy
Status-code (see RFC 3261 [26] subclause 7.2)
Tag (see RFC 3261 [26] subclause 19.3)
Target Refresh Request
User agent client (UAC)
User agent server (UAS)
User agent (UA)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2] subclause 4.1.1.1 and subclause 4a.7 apply:

Breakout Gateway Control Function (BGCF)
Call Session Control Function (CSCF)
Home Subscriber Server (HSS)
Media Gateway Control Function (MGCF)
Media Resource Function Controller (MRFC)
Subscription Locator Function (SLF)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.218 [5] subclause 3.1 apply:

Filter criteria
Initial filter criteria
Initial request
Standalone transaction
Subsequent request

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclause 4.3.3.1 and subclause 4.6 apply:

Interrogating-CSCF (I-CSCF)
Policy Decision Function (PDF)
Private user identity
Proxy-CSCF (P-CSCF)
Public user identity
Serving-CSCF (S-CSCF)

For the purposes of the present document, the following terms and definitions given in 3GPP TR 33.203 [19] apply:

Protected Server Port
Protected Client Port

For the purposes of the present document, the following terms and definitions given in 3GPP TR 21.905 [1] apply:

User Equipment (UE)

For the purposes of the present document, the following terms and definitions given in RFC 2401 [20A] Appendix A apply:

Security association

NOTE: A number of different security associations exist within the IM CN subsystem. Within this document the term specifically applies to the security association that exists between the UE and the P-CSCF, as this is the only security association that has direct impact on SIP.

For the purposes of the present document, the following terms and definitions given in ITU-T E.164 [57] apply:

International public telecommunication number

Second Change

5.1.1.5 Authentication

5.1.1.5.1 General

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

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

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header as described in RFC 3329 [48]. If the header is not present or it does not contain the parameters required for the setup of the ~~security associations~~set of security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

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

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up ~~two new pairs of security associations~~a temporary set of security associations based on the static list and parameters it received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header in the REGISTER request. The UE sets up ~~two pairs of security associations~~the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK as the shared key. The UE shall use the parameters received in the Security-Server header to setup the ~~security associations.~~temporary set of security associations. The UE shall set a temporary SIP level lifetime for the ~~newly setup security associations to a value which has to be long enough to permit the UE to finalize the registration procedure (longer than 64*T1);~~temporary set of security associations to the value of reg-await-auth timer; and

3) send another REGISTER request using the ~~new security association~~temporary set of security associations to protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response (RES parameter), as described in RFC 3310 [49]. The UE shall also insert the Security-Client header that is identical to the Security-Client header that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header into the request, by mirroring in it the content of the Security-Server header received in the 401 (Unauthorized) response. The Call-ID of the integrity protected REGISTER request which carries RES must be the same as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the integrity protected REGISTER request, the UE shall:

- ~~set the security association~~change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing ~~SA~~set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

- ~~send subsequent requests towards the P-CSCF using the new security associations;~~

~~send the responses toward the P-CSCF over the same security association that the associated request was received; and~~

~~receive the responses from the P-CSCF over the same security association that the associated request was sent.~~use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

NOTE 1: In this case, the UE will send requests towards the P-CSCF over the newly established set of security associations. Responses towards the P-CSCF that are sent via UDP will be sent over the newly established set of security associations. Responses towards the P-CSCF that are sent via TCP will be sent over the same set of security associations that the related request was received on.

When the first request or response protected with the newly ~~set up security association~~established set of security associations is received from the P-CSCF, the UE shall delete the old ~~security associations~~set of security associations and related keys it may have with the P-CSCF after all SIP transactions that use the old ~~security associations~~set of security associations are completed.

Whenever the 200 (OK) response is not received before the temporary SIP level lifetime of the ~~new security associations~~temporary set of security associations expires or a 403 (Forbidden) response is received, the UE shall consider the registration to have failed. The UE shall delete the ~~new security associations~~temporary set of security

associations it was trying to establish, and use the old ~~security associations.~~set of security associations. The UE should send an unprotected REGISTER message according to the procedure specified in subclause 5.1.1.2 if the UE considers the ~~earlier established security associations~~old set of security associations to be no longer active at the P-CSCF.

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

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 <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.

5.1.1.5.3 Abnormal cases

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

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

~~The~~Whenever the UE detects any of the above cases, the UE shall:

- send the REGISTER request using an existing ~~security association,~~set of security associations, if available (see 3GPP TS 33.203 [19]);
- ~~3GPP TS 33.203 [19]). The REGISTER request shall contain~~ populate a new Security-Client header within the REGISTER request, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association ~~setup.~~setup; and
- not create a temporary set of security associations.

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

Third Change

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

1) insert a Path header in the request including an entry containing:
   - the SIP URI identifying the P-CSCF;

- an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

2) insert a Require header containing the option tag "path";

3) for the initial REGISTER request for a public user identity create a new, globally unique value for icid, save it locally and insert it into the icid parameter of the P-Charging-Vector header;

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication response, or it was received on the security association created during the last successful authentication procedure and with no authentication response, otherwise insert the parameter with the value "no";

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'sec-agree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:

- check the security association which protected the request. If ~~that has~~the security association is a temporary ~~lifetime, and the REGISTER request was received protected with the new security association,~~one, then the request ~~shall~~is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Security-Verify and the Security-Client header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;

- if the security association the REGISTER request was received on, is an already established one, then:

  - a Security-Verify header is not expected to be included. If the Security-Verify header is present, then the P-CSCF shall remove that header together with the 'Require: sec-agree' header;

  - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;

  - the P-CSCF shall remove the Security-Client header before forwarding the request to the S-CSCF; and

- check if the private user identity conveyed in the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and

8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

1) delete any temporary set of security associations established towards the UE;

2~~1~~) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and ~~security associations~~to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;

3~~2~~) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer ~~algorithms. The P-~~

~~CSCF shall support the setup of two pairs of security associations. For further information see 3GPP TS 33.203 [19]; and~~algorithms;

~~3) set up the new security associations~~4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set ~~a~~the temporary SIP level lifetime for the ~~security association which has to be long enough to permit the UE to finalize the registration procedure (bigger~~ temporary set of security associations to the value of reg-await-auth timer; and

~~than 64*T1).~~

~~4)~~5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

2) associate the Service-Route header list with the registered public user identity;

3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;

4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more then one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

5) store the values received in the P-Charging-Function-Addresses header;

6) ~~set the security association~~if a set of temporary security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing ~~security association~~set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

7) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

~~The P-CSCF shall:~~

- ~~if new security associations are established and there are no old security associations, start using the new security associations towards the UE after the 200 (OK) has been sent out;~~
- ~~if a request protected within the newly established security associations is received from a UE which has old security associations, delete the old security associations and related keys when all SIP transactions that use the old security associations are completed;~~
- ~~if the newly established security associations has not been taken into use by the UE and the UE sends request protected on the old security associations, delete the new security associations; and~~
- ~~if the newly established security associations are a result of an unprotected REGISTER request being received from the UE, then delete the old security associations which may exist~~

When receiving a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

1) reduce the SIP level lifetime lifetime of the old set of security associations towards the same UE to 64*T1 (if currently longer than 64*T1) ; and

2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e. take the newly established set of security associations into use).

NOTE 3: In this case, the P-CSCF will send requests towards the UE over the newly established set of security associations. Responses towards the UE that are sent via UDP will be sent over the newly established set of security associations. Responses towards the UE that are sent via TCP will be sent over the same set of security associations that the related request was received on.

NOTE 4: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorther than 64*T1 and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly estabslihed set of security associations for further messages towards the UE as appropriate (see Note 3).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;

2) keep the newly established set of security associations created during this authentication;

3) delete, if existing, any other set of security associations towards this UE immediately; and,

4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

When sending the 200 (OK) respone for a REGISTER request that concludes an initial authentication, i.e. the initial REGISTER request was received unprotected, the P-CSCF shall:

1) keep the newly established set of security associations created during this authentication;

2) delete, if existing, any otherset of security associations towards this UE immediately; and,

3) use the kept newly established set of security associations for further messages sent towards the UE.

~~NOTE 3:~~NOTE 5: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routeing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

The handling of the security associations at the P-CSCF is summarized in table 5.2.2.-1.

Table 5.2.2-1: Handling of security associations at the P-CSCF

	Temporary set of security associations	Newly established set of security associations	Old set of security associations
SIP message received over newly established set of security associations that have not yet been taken into use	No action	Take into use	Reduce SIP level lifetime to 64*T1, if lifetime is larger than 64*T1
SIP message received over old set of security associations	No action	No action	No action
Old set of security associations currently in use will expire in 64*T1	No action	Take into use	No action
Sending an authorization challenge within a 401 (Unauthorized) response for a REGISTER request	Create Remove any previously existing temporary set of security associations	No action	No action
Sending 200 (OK) response for REGISTER request that concludes re-authentication	Change to a newly established set of security associations	Convert to and treat as old set of security associations (see next column)	Continue using the old set of security associations over which the REGISTER request, that initiated the re-authentication was received. Delete all other old sets of security associations immediately
Sending 200 (OK) response for REGISTER request that concludes initial authentication	Change to a newly established set of security associations and take into use immediately	Convert to old set of security associations, i.e. delete	Delete

3GPP TSG-CN1 Meeting #32
Bangkok, Thailand, 27-31 October 2003

Tdoc ⌘N1-031579

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **565** ⌘ **rev** **-** ⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Sending challenge
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	18/10/2003
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 outcome of the CN1-SA3 joint session was, that the P-CSCF always deletes a set of temporary SAs when a new set is to be set up. This means that while there is an ongoing authentication and the user requests again to be authenticated, then the previously sent challenge is ignored by the S-CSCF, and a new challenge is always sent to the user. As the P-CSCF deletes all 'old temporary SAs' when setting up a new set of SAs towards the user, the user will not be able to respond to the previous challenge anyhow.
Summary of change:	⌘	It has been removed the condition on when to send a challenge to the user. A challenge will always be sent once an unprotected REGISTER is received.
Consequences if not approved:	⌘	The user may end up not being able to connect to REGISTER. There will be different behaviours of the P-CSCF and S-CSCF which results in incosistent way of handling the registration procedure.

Clauses affected:	⌘	5.4.1.2.1

		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.

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~~3) 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~~4) store the icid parameter received in the P-Charging-Vector header;

~~6~~5) 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~~6) send the so generated 401 (Unauthorized) response towards the UE; and,

~~8~~7) 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.

3GPP TSG-CN1 Meeting #32
Bangkok, Thailand, 27-31 October 2003

Tdoc ⌘N1-031580

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **566** ⌘ **rev** **-** ⌘ 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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Sending challenge
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	18/10/2003
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 outcome of the CN1-SA3 joint session was, that the P-CSCF always deletes a set of temporary SAs when a new set is to be set up. This means that while there is an ongoing authentication and the user requests again to be authenticated, then the previously sent challenge is ignored by the S-CSCF, and a new challenge is always sent to the user. As the P-CSCF deletes all 'old temporary SAs' when setting up a new set of SAs towards the user, the user will not be able to respond to the previous challenge anyhow.
Summary of change:	⌘	It has been removed the condition on when to send a challenge to the user. A challenge will always be sent once an unprotected REGISTER is received.
Consequences if not approved:	⌘	The user may end up not being able to connect to REGISTER. There will be different behaviours of the P-CSCF and S-CSCF which results in incosistent way of handling the registration procedure.

Clauses affected:	⌘	5.4.1.2.1

		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.

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~~3) 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~~4) store the icid parameter received in the P-Charging-Vector header;

~~6~~5) 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~~6) send the so generated 401 (Unauthorized) response towards the UE; and,

~~8~~7) 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.