3GPP TSG-CN1 Meeting #30   ***Tdoc N1-030918Rev1***
San Diego, California, USA,   19 – 23 May 2003

Title:	LS on Security Association Lifetimes
Response to:	
Release:	5
Work Item:	IMS-CCR

Source:	CN1
To:	SA3
Cc:	

Contact Person:
    Name: Kevan Hobbis
    Tel. Number: +44 7782 325252
    E-mail Address: **kevan.hobbis@three.co.uk**

Attachments: N1-030493, N1-030494, N1-030496 and N1-030646917

1. Overall Description:

CN1 would like to inform SA3 of agreed changes to TS 24.229 in regard to the management of security association lifetimes. These changes will appear in the next reference version of TS 24.229

CN1 have agreed changes to enhance the PCSCF behaviour regarding security association lifetimes during authentication and re-authentication. These changes allow the PCSCF to increase or decrease the security association lifetime dependent on the expiry time of still valid registrations.

The four change requests attached to this liaison show the detail of these changes.

CN1 note that this detailed operation is not aligned with 33.203 and ask SA3 to modify 33.203 to align with the agreed operation defined in the CN1 change requests.

2. Actions:

To [SA3] group.

ACTION: CN1 asks SA3 group to make the necessary changes to 33.203 to align with the operation agreed by CN1.

3. Date of Next TSG-CN1 Meetings:

CN1_31	25th – 29th August 2003	Sophia-Antipolis, France
CN1_32	27th – 31st October 2003	???

CR-Form-v7

CHANGE REQUEST

⌘	**24.229** CR **304**	⌘**rev**	**4**	⌘	Current version:	**5.4.0**	⌘

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

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

Title: ⌘	SAs lifetimes in P-CSCF	
Source: ⌘	Lucent Technologies	
Work item code: ⌘	**IMS-CCR**	***Date:*** ⌘ 31/03/2003

Category: ⌘ **F**   ***Release:*** ⌘ **Rel-5**

Use <u>one</u> 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 <u>one</u> 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 SAs between the UE and P-CSCF should be set to the longest registration expiration lifetime. Step 6. incorrectly states "update the SIP level lifetime of the security association with the value found in the Expires header;" since this value may be smaller than the expiration-value of some other previously registered public user identities that are using the same SA.
Summary of change: ⌘	Relevant text added.
Consequences if not approved: ⌘	Incorrect specification.

Clauses affected: ⌘	5.2.2

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

Other comments: ⌘	Revised as requested by the WG.

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.

5.2.2 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 URL 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 URL, a character string in the user part of the URL, or be a port number in the URL;

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 received integrity protected, 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 a temporary lifetime, then the request shall contain a Security-Verify header. If there is no such header, then the P-CSCF shall return a suitable 4xx error code. If there is such header, then compare the content of the Security-Verify header with the local static list. 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 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 came is an 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; 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) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and security association. 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 the Security-Server header in the response, containing the P-CSCF static security list. For further information see 3GPP TS 33.203 [19]; and

3) set up the security association 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 the SIP level lifetime of the security association to be long enough to permit the UE to finalize the registration procedure (longerbigger than 64*T1). The P-CSCF shall set the IPSec level lifetime of the security association to the maximum.

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. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 1: 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) update the SIP level lifetime of the security association. The P-CSCF shall use~~with~~ the value found in the Expires header as the lifetime value for this public user identity, and compare it with all other locally stored registration lifetimes that utilse this security association. The P-CSCF shall select the longest registration lifetime as the SIP level lifetime for this security association;

7) protect the response within the same security association to that in which the associated requestwas protected;

8) delete all earlier security associations and related keys it may have towards the UE, when a message protected within the newly set up security association is received; and

9) delete the new security associations that it was trying to establish with the UE, in case the P-CSCF receives a message from the UE protected with the old security association.

NOTE 2: 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 all public user identities associated with the respective security association have been deregistered, or when~~their~~the SIP level lifetime expires. If there are still active dialogs associated with the user after the security associations were deleted, the P-CSCF shall discard all information pertaining to these dialogs without performing any further SIP transactions with the peer entities of the P-CSCF.

NOTE 3: At the same time, the P-CSCF will also indicate via the Go interface that all resources associated with these dialogs should be released.

CR-Form-v7

CHANGE REQUEST

⌘	**24.229** CR **344**	⌘ **rev**	**1**	⌘	Current version:	**5.4.0**	⌘

*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 ☐

Title: ⌘	Setting the SA lifetime at UE upon registration	
Source: ⌘	Lucent Technologies	
Work item code: ⌘	**IMS-CCR**	***Date:*** ⌘ 31/03/2003
Category: ⌘	**F**	***Release:*** ⌘ **Rel-5**

Use <u>one</u> 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 <u>one</u> 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 SA lifetime in the UE should be set to the longest registration-expiration lifetime. Currently, the document 24.229 does not explicitly specify when the UE sets the SA lifetime and its value.
Summary of change: ⌘	Relevant text added.
Consequences if not approved: ⌘	Incomplete specification.

Clauses affected: ⌘	5.1.1.2 and 5.1.1.4

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

Other comments: ⌘	Revised as requested by the WG.

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.

5.1.1.2   Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

A REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [19], derived as a result of an earlier registration.

The public user identity to be registered can be extracted either from the ISIM application, if present, on the UICC or derived from the USIM, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

On sending a REGISTER request, the UE shall populate the header fields as follows:

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

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

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

d) the Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the protected port value that is bound to the security association is known by the UE, that shall be also included in the hostport parameter;

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.

e) the Expires header, or the expires parameter within the Contact header, set to the value of 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) the Security-Client header field set to specify the security mechanism the UE supports, the IPSec layer algorithms the UE supports and the parameters needed for the security association setup. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

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

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

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 receiving the 200 (OK) response to the REGISTER request, the UE shall store the expiration time of the registration for the public user identities found in the To header value. The UE shall also 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. The list contains also the identity under registration, unless this identity is barred. In order to build a proper preloaded Route header value for new dialogs, the UE shall also store the list of Service Route headers contained in the Service-Route header.

The UE shall use the registration expiration time received in the 200 (OK) response and compare it with all other locally stored registration lifetimes. The UE shall select the longest registration lifetime as the SIP level lifetime for its security association with the P-CSCF.

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) 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.

5.1.1.4   User-initiated re-registration

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

The UE shall reregister the public user identity 600 seconds before the expiration time of a previous registration, unless either the user or the application within the UE has determined that a continued registration is not required. If the registration period indicated from the S-CSCF is less than 600 seconds, the UE shall reregister when half of the registration period has expired.

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

On sending a REGISTER request, 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 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.

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) a Security-Client header field, set to specify the security mechanism it supports, the IPSec layer algorithms it supports and the parameters needed for the security association setup. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

NOTE 3: The 401 (Unauthorized) challenge 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 the security association with the UE during the same registration procedure.

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

i) 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).

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 receiving the 200 (OK) response to the REGISTER request, the UE shall store the new expiration time of the registration for this public user identity found in the To header value. The UE shall also 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.

The UE shall use the registration expiration time received in the 200 (OK) response and compare it with all other locally stored registration lifetimes. The UE shall select the longest registration lifetime as the SIP level lifetime for its security association with the P-CSCF.

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.

CR-Form-v7

CHANGE REQUEST

⌘	**24.229** CR **346**	⌘**rev**	**1-**	⌘	Current version:	**5.4.0**	⌘

*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: ⌘	SA liftime upon network initiated de-registration	
Source: ⌘	Lucent Technologies	
Work item code: ⌘	**IMS-CCR**	***Date:*** ⌘ 31/03/2003
Category: ⌘ **F**		***Release:*** ⌘ **Rel-5**

Use <u>one</u> 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 <u>one</u> 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: ⌘	When the network de-registers a given public user identity, and if there are other remaining public user identities registered, the UE and P-CSCF should update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities. Currently, the document 24.229 does not explicitly specify this procedure.
Summary of change: ⌘	Relevant text added.
Consequences if ⌘ ***not approved:***	Incomplete specification.

Clauses affected: ⌘	5.1.1.7 and 5.2.5.2

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

Other comments: ⌘	Revised as requested by the Nokia.

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.

5.1.1.7 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) with the state attribute set to "terminated" and the event attribute set to "rejected" or "deactivated", the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the reregistration procedure as described in subclause 5.1.1.4.

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the P-CSCF.

If there are other remaining public user identities registered, the UE shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities.

Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header contains the value of "terminated", the UE shall remove the security associations towards the P-CSCF after the server transaction (as defined in RFC 3261 [26]) pertaining to the NOTIFY request terminates.

NOTE 1: If the security association towards the P-CSCF is removed, then the UE considers the subscription to the registration event package terminated (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero, or a NOTIFY request was received with Subscription-State header containing the value of "terminated").

NOTE 2: When the P-CSCF has removed the security association established between the P-CSCF and the UE, further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

5.2.5.2 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.2.3, including one or more <registration> element(s) with the state attribute set to "terminated" the P-CSCF shall remove all stored information for these public user identities.

If there are no more public user identities registered, the P-CSCF shall delete the security associations and related keys it may have towards the UE.

If there are other remaining public user identities registered, the P-CSCF shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities that utilse this security association.

Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered), the P-CSCF shall remove the security associations towards the UE.

NOTE: When the P-CSCF has removed the security association established between the P-CSCF and the UE, further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

CR-Form-v7

CHANGE REQUEST

| ⌘ | **24.229** CR **398** | ⌘**rev** | ⌘ | Current version: | **5.4.0** | ⌘ |

*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:	⌘	Combined CRs: N1-030495 (Lucent), N1-030558 (Nokia), and N1-030559(Nokia)
Source:	⌘	Nokia, Lucent Technologies
Work item code: ⌘	**IMS-CCR**	**Date:** ⌘ 12/05/2003

Category:	⌘	**F**	**Release:** ⌘	**Rel-5**

Use <u>one</u> 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 <u>one</u> 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 CRs N1-030495, N1-030558, and N1-030559 were addressing different issues in the subclause 5.2.5.1 of the document TS 24.229. To facilitate the inclusion of the respective CRs into the document TS 24.229, this CR combines all three CRs into a single CR.
Summary of change: ⌘		The text in the CRs N1-030495, N1-030558, and N1-030559 were combined together.
Consequences if not approved:	⌘	The editor will have to incorporate each individual CR into the 24.229 document.

Clauses affected:	⌘	5.1.1.6 and 5.2.5.1

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

Other comments:	⌘	Revised as requested by Nokia.

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.

5.1.1.6   Mobile-initiated deregistration

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

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

On sending a REGISTER request, the UE shall populate the header fields as follows:

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

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

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

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

   e) the Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;

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

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

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 receiving the 200 (OK) response to the REGISTER request, the UE shall remove all registration details relating to this public user identity.

The UE shall release all dialogs prior to deregistering the last registered public user identity.

If there are other remaining public user identities registered, the UE shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities.

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the P-CSCF. If there are other remaining public user identities registered, the UE shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities.

If all public user identities are deregistered and the security association is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

   NOTE: When the UE has received the 200 (OK) for the REGISTER request of the last registered public user identity, the UE removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

5.2.5.1   User-initiated deregistration

When the P-CSCF receives a 200 (OK) response to a REGISTER request (sent according to subclause 5.2.2), it shall check the value of the Expires header field and/or expires parameter in the Contact header field. When the value of the Expires header field or expires parameter equals zero, then the P-CSCF shall:

   1) remove the public user identity found in the To header field, and all the associated public user identities, from the registered public user identities list and all related stored information; and

   2) check if the user has left any other registered public user identity. Due to that, the P-CSCF shall:

- iIf there are other remaining public user identities registered, the P-CSCF shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities; or

- iIf When all of the public user identities of a user are deregistered, the P-CSCF shall,

    remove the security associations towards that user after the server transaction (as defined in RFC 3261 [26]) pertaining to this deregistration terminates.; and

    - if the subscription to the reg event package for that user is still alive, terminate the subscription to the reg event package for that user by sending a SUBSCRIBE request with an Expires header containing a value of zero. The P-CSCF shall also remove the security associations towards that user after the server transaction (as defined in RFC 3261 [26]) pertaining to this deregistration terminates.

NOTE 1: Deleting a security association is an internal procedure of the P-CSCF and does not involve any SIP procedures.

NOTE 21:There is no requirement to distinguish a REGISTER request relating to a registration from that relating to a deregistration. For administration reasons the P-CSCF may distinguish such requests, however this has no impact on the SIP procedures.

NOTE 32:When the P-CSCF has sent the 200 (OK) for the REGISTER request of the last registered public user identity, the P-CSCF removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.