3GPP TSG CT Meeting #28 **CP-050061**
1st – 3rd June 2005. Quebec, CANADA.

Source: **TSG CT WG1**

Title: **CRs on Rel-6 WI “IMS2” for TS 24.229**

Agenda item: **9.1**

Document for: **APPROVAL**

This document contains 20 **CRs for Rel-6 WI “IMS2”**, that have been agreed by TSG CT WG1 meeting #38 and forwarded to TSG CT Plenary meeting #28 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Version	WI	Rel
C1-050571	Completion of status-code tables in SIP profile	24.229	892		F	6.6.0	IMS2	Rel-6
C1-050599	Shared public user identities	24.229	862		F	6.6.0	IMS2	Rel-6
C1-050671	Unsubscribe by P-CSCF	24.229	865	1	F	6.6.0	IMS2	Rel-6
C1-050684	Clarify that S-CSCF shall support Supported and Require headers	24.229	916	1	F	6.6.0	IMS2	Rel-6
C1-050700	S-CSCF redirecting	24.229	858	1	F	6.6.0	IMS2	Rel-6
C1-050701	P-CSCF - routing of REGISTER requests	24.229	860	1	F	6.6.0	IMS2	Rel-6
C1-050708	Protected initial registration	24.229	866	1	F	6.6.0	IMS2	Rel-6
C1-050709	Re-registration failure	24.229	894	1	F	6.6.0	IMS2	Rel-6
C1-050711	Correction of table A.104A	24.229	870	1	F	6.6.0	IMS2	Rel-6
C1-050716	Contact address in REGISTER response	24.229	887	1	F	6.6.0	IMS2	Rel-6
C1-050717	P-CSCF Record-Route processing for target refresh requests/responses	24.229	890	1	F	6.6.0	IMS2	Rel-6
C1-050719	AS originated requests on behalf of PSI	24.229	893	1	F	6.6.0	IMS2	Rel-6
C1-050720	Routing PSI at terminating side	24.229	896	1	F	6.6.0	IMS2	Rel-6
C1-050789	Notification about registration state	24.229	856	2	F	6.6.0	IMS2	Rel-6
C1-050790	Registration failure at UE	24.229	861	3	F	6.6.0	IMS2	Rel-6
C1-050791	Correction of the references for the integration of resource management procedures	24.229	899	2	F	6.6.0	IMS2	Rel-6
C1-050792	Clarification on P-CSCF-intiated call release	24.229	902	2	F	6.6.0	IMS2	Rel-6
C1-050793	Error handling in UE in case of RFC 3524	24.229	863	3	F	6.6.0	IMS2	Rel-6
C1-050794	MT- SDP offer with IPv4 address.	24.229	787	6	F	6.6.0	IMS2	Rel-6
C1-050802	UE registration failure because the selected S-CSCF is unreachable	24.229	895	3	F	6.6.0	IMS2	Rel-6

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050571

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**892**	⌘ **rev**	**-**	⌘	Current version:	**6.6.0** ⌘

*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:	⌘	Completion of status-code tables in SIP profile		
Source:	⌘	Lucent Technologies		
Work item code:	⌘	IMS2	***Date:*** ⌘	14/04/2005
Category:	⌘	**F** *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.	***Release:*** ⌘	Rel-6 *Use one of the following releases:* *Ph2 (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)* *Rel-7 (Release 7)*

Reason for change: ⌘ Tables A.6 and A.164, describing the required support of individual status codes within the SIP profile, are currently substantially empty, and require completion.

Summary of change: ⌘ Many of the empty entries are completed with either mandatory or optional to send, mandatory to receive from a UA, whereas a proxy treats all these transparently. Note that any entity normally acting as a proxy that decides to reject a request acts as a UA in order to perform this function. It is considered inappropriate in most of these cases to define which specific type of IMS functional entities generate these responses, thus leaving flexibility for all IMS S-CSCF, AS acting as proxy, and BGCF to generate such responses for implementation specific reasons, even if not otherwise listed in 24.229.
Exceptions to this are:

- 200: At proxy even though SIP passes on transparently, has been made m to send due to other IMS specific processing, e.g. charging.
- 3xx: UA entries have been left open while we clarify functionality for these responses in other CRs.
- 401: Special support defined for the P-CSCF, as while it handles this as a proxy, has to inspect and modify the contents when received.
- 402: Defined in RFC 3261 for further study, so has been marked n/a.
- 421: Only mandatory to generate at those entities where any extensions support is required, UE, P-CSCF, S-CSCF.
- 484: Treated as optional to send, as overlap sending not supported in IMS.
- 485, 502: Treated as optional to send, as other codes may be used in preference.

Consequences if not approved:	⌘	Incomplete specification.

Clauses affected:	⌘	A.2.1.4.1, A.2.2.4.1				
		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.

A.2.1.4.1 Status-codes

Table A.6: Supported status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	100 (Trying)	[26] 21.1.1	n/a	n/a	[26] 21.1.1	c11	c11
101	1xx response	[26] 21.1	p21	p21	[26] 21.1	p21	p21
2	180 (Ringing)	[26] 21.1.2	c2	c2	[26] 21.1.2	c1	c1
3	181 (Call Is Being Forwarded)	[26] 21.1.3	c2	c2	[26] 21.1.3	c1	c1
4	182 (Queued)	[26] 21.1.4	c2	c2	[26] 21.1.4	c1	c1
5	183 (Session Progress)	[26] 21.1.5	c1	c1	[26] 21.1.5	c1	c1
102	2xx response	[26] 21.2	p22	p22	[26] 21.1	p22	p22
6	200 (OK)	[26] 21.2.1	m	m	[26] 21.2.1	m	m
7	202 (Accepted)	[28] 8.3.1	c3	c3	[28] 8.3.1	c3	c3
103	3xx response	[26] 21.3	p23	p23	[26] 21.1	p23	p23
8	300 (Multiple Choices)	[26] 21.3.1			[26] 21.3.1		
9	301 (Moved Permanently)	[26] 21.3.2			[26] 21.3.2		
10	302 (Moved Temporarily)	[26] 21.3.3			[26] 21.3.3		
11	305 (Use Proxy)	[26] 21.3.4			[26] 21.3.4		
12	380 (Alternative Service)	[26] 21.3.5			[26] 21.3.5		
104	4xx response	[26] 21.4	p24	p24	[26] 21.4	p24	p24
13	400 (Bad Request)	[26] 21.4.1	m	m	[26] 21.4.1	m	m
14	401 (Unauthorized)	[26] 21.4.2	o	c12	[26] 21.4.2	m	m
15	402 (Payment Required)	[26] 21.4.3	n/a	n/a	[26] 21.4.3	n/a	n/a
16	403 (Forbidden)	[26] 21.4.4	m	m	[26] 21.4.4	m	m
17	404 (Not Found)	[26] 21.4.5	m	m	[26] 21.4.5	m	m
18	405 (Method Not Allowed)	[26] 21.4.6	m	m	[26] 21.4.6	m	m
19	406 (Not Acceptable)	[26] 21.4.7	m	m	[26] 21.4.7	m	m
20	407 (Proxy Authentication Required)	[26] 21.4.8	o	o	[26] 21.4.8	m	m
21	408 (Request Timeout)	[26] 21.4.9	m	m	[26] 21.4.9	m	m
22	410 (Gone)	[26] 21.4.10	m	m	[26] 21.4.10	m	m
22A	412 (Conditional Request Failed)	[70] 11.2.1	c20	c20	[70] 11.2.1	c20	c20
23	413 (Request Entity Too Large)	[26] 21.4.11	m	m	[26] 21.4.11	m	m
24	414 (Request-URI Too Large)	[26] 21.4.12	m	m	[26] 21.4.12	m	m
25	415 (Unsupported Media Type)	[26] 21.4.13	m	m	[26] 21.4.13	m	m
26	416 (Unsupported URI Scheme)	[26] 21.4.14	m	m	[26] 21.4.14	m	m
27	420 (Bad Extension)	[26] 21.4.15	m	c13	[26] 21.4.15	m	m
28	421 (Extension Required)	[26] 21.4.16	o		[26] 21.4.16	i	i
28A	422 (Session Interval Too Small)	[58] 6	c7	c7	[58] 6	c7	c7
29	423 (Interval Too Brief)	[26] 21.4.17	c4	c4	[26] 21.4.17	m	m
29A	429 (Provide Referrer Identity)	[59] 5	c8	c8	[59] 5	c9	c9
30	480 (Temporarily Unavailable)	[26] 21.4.18	m	m	[26] 21.4.18	m	m
31	481 (Call/Transaction Does Not Exist)	[26] 21.4.19	m	m	[26] 21.4.19	m	m
32	482 (Loop Detected)	[26] 21.4.20	m	m	[26] 21.4.20	m	m
33	483 (Too Many Hops)	[26] 21.4.21	m	m	[26] 21.4.21	m	m
34	484 (Address Incomplete)	[26] 21.4.22	o	o	[26] 21.4.22	m	m
35	485 (Ambiguous)	[26] 21.4.23	o	o	[26] 21.4.23	m	m
36	486 (Busy Here)	[26] 21.4.24	m	m	[26] 21.4.24	m	m
37	487 (Request Terminated)	[26] 21.4.25	m	m	[26] 21.4.25	m	m
38	488 (Not Acceptable Here)	[26] 21.4.26	m	m	[26] 21.4.26	m	m
39	489 (Bad Event)	[28] 7.3.2	c3	c3	[28] 7.3.2	c3	c3
40	491 (Request Pending)	[26] 21.4.27	m	m	[26] 21.4.27	m	m
41	493 (Undecipherable)	[26] 21.4.28	m	m	[26] 21.4.28	m	m

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
41A	494 (Security Agreement Required)	[48] 2	c5	c5	[48] 2	c6	c6
105	5xx response	[26] 21.5	p25	p25	[26] 21.5	p25	p25
42	500 (Internal Server Error)	[26] 21.5.1	m	m	[26] 21.5.1	m	m
43	501 (Not Implemented)	[26] 21.5.2	m	m	[26] 21.5.2	m	m
44	502 (Bad Gateway)	[26] 21.5.3	o	o	[26] 21.5.3	m	m
45	503 (Service Unavailable)	[26] 21.5.4	m	m	[26] 21.5.4	m	m
46	504 (Server Time-out)	[26] 21.5.5	m	m	[26] 21.5.5	m	m
47	505 (Version not supported)	[26] 21.5.6	m	m	[26] 21.5.6	m	m
48	513 (Message Too Large)	[26] 21.5.7	m	m	[26] 21.5.7	m	m
49	580 (Precondition Failure)	[30] 8			[30] 8		
106	6xx response	[26] 21.6	p26	p26	[26] 21.6	p26	p26
50	600 (Busy Everywhere)	[26] 21.6.1	m	m	[26] 21.6.1	m	m
51	603 (Decline)	[26] 21.6.2	c10	c10	[26] 21.6.2	m	m
52	604 (Does Not Exist Anywhere)	[26] 21.6.3	m	m	[26] 21.6.3	m	m
53	606 (Not Acceptable)	[26] 21.6.4	m	m	[26] 21.6.4	m	m

c1: IF A.5/9 THEN m ELSE n/a - - INVITE response.

c2: IF A.5/9 THEN o ELSE n/a - - INVITE response.

c3: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.

c4: IF A.5/19 OR A.5/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.

c5: IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.

c6: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.

c7: IF A.4/42 AND (A.5/9 OR A.5/23) THEN m ELSE n/a - - the SIP session timer AND (INVITE response OR UPDATE response).

c8: IF A.4/43 AND A.5/17 THEN o ELSE n/a - - the SIP Referred-By mechanism and REFER response.

c9: IF A.4/43 AND A.5/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response.

c10: IF A.4/44 THEN m ELSE o - - the Session Inititation Protocol (SIP) "Replaces" header.

c11: IF A.5/9 THE m ELSE n/a - - INVITE response (note 1).

c12: IF A.3/4 THEN m ELSE o - - S-CSCF.

c13: IF A.3/1 OR A.3/2 OR A.3/4 THEN m ELSE o - - UE, P-CSCF, S-CSCF

c20: IF A.4/41 THEN m ELSE n/a - - an event state publication extension to the session initiation protocol.

p21: A.6/2 OR A.6/3 OR A.6/4 OR A.6/5 - - 1xx response.

p22: A.6/6 OR A.6/7 - - 2xx response.

p23: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/13 - - 3xx response.

p24: A.6/14 OR A.6/15 OR A.6/16 OR A.6/17 OR A.6/18 OR A.6/19 OR A.6/20 OR A.6/21 OR A.6/22 OR A.6/22A OR A.6/23 OR A.6/24 OR A.6/25 OR A.6/26 OR A.6/27 OR A.6/28 OR A.6/28A OR A.6/29 OR A.6/29A OR A.6/30 OR A.6/31 OR A.6/32 OR A.6/33 OR A.6/34 OR A.6/35 OR A.6/36 OR A.6/436 OR A.6/38 OR A.6/39 OR A.6/40 OR A.6/41 OR A.6/41A. - 4xx response.

p25: A.6/42 OR A.6/43 OR A.6/44 OR A.6/45 OR A.6/46 OR A.6/47 OR A.6/48 OR A.6/49 - - 5xx response

p26: A.6/50 OR A.6/51 OR A.6/52 OR A.6/53 - - 6xx response.

NOTE 1: RFC 3261 [26] gives the status of this header for methods other than INVITE as SHOULD NOT.

A.2.2.4.1 Status-codes

Table A.164: Supported-status codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	100 (Trying)	[26] 21.1.1	c1	c1	[26] 21.1.1	c2	c2
101	1xx response	[26] 21.1	p21	p21	[26] 21.1	p21	p21
2	180 (Ringing)	[26] 21.1.2	c3	c3	[26] 21.1.2	c3	c3
3	181 (Call Is Being Forwarded)	[26] 21.1.3	c3	c3	[26] 21.1.3	c3	c3
4	182 (Queued)	[26] 21.1.4	c3	c3	[26] 21.1.4	c3	c3
5	183 (Session Progress)	[26] 21.1.5	c3	c3	[26] 21.1.5	c3	c3
102	2xx response	[26] 21.2	p22	p22	[26] 21.1	p22	p22
6	200 (OK)	[26] 21.2.1	m	m	[26] 21.2.1	i	m
7	202 (Accepted)	[28] 8.3.1	c4	c4	[28] 8.3.1	c4	c4
103	3xx response	[26] 21.3	p23	p23	[26] 21.1	p23	p23
8	300 (Multiple Choices)	[26] 21.3.1	m	m	[26] 21.3.1	i	i
9	301 (Moved Permanently)	[26] 21.3.2	m	m	[26] 21.3.2	i	i
10	302 (Moved Temporarily)	[26] 21.3.3	m	m	[26] 21.3.3	i	i
11	305 (Use Proxy)	[26] 21.3.4	m	m	[26] 21.3.4	i	i
12	380 (Alternative Service)	[26] 21.3.5	m	m	[26] 21.3.5	i	i
104	4xx response	[26] 21.4	p24	p24	[26] 21.4	p24	p24
13	400 (Bad Request)	[26] 21.4.1	m	m	[26] 21.4.1	i	i
14	401 (Unauthorized)	[26] 21.4.2	m	m	[26] 21.4.2	i	c10
15	402 (Payment Required)	[26] 21.4.3	n/a	n/a	[26] 21.4.3	n/a	n/a
16	403 (Forbidden)	[26] 21.4.4	m	m	[26] 21.4.4	i	i
17	404 (Not Found)	[26] 21.4.5	m	m	[26] 21.4.5	i	i
18	405 (Method Not Allowed)	[26] 21.4.6	m	m	[26] 21.4.6	i	i
19	406 (Not Acceptable)	[26] 21.4.7	m	m	[26] 21.4.7	i	i
20	407 (Proxy Authentication Required)	[26] 21.4.8	m	m	[26] 21.4.8	i	i
21	408 (Request Timeout)	[26] 21.4.9	m	m	[26] 21.4.9	i	i
22	410 (Gone)	[26] 21.4.10	m	m	[26] 21.4.10	i	i
22A	412 (Conditional Request Failed)	[70] 11.2.1	c20	c20	[70] 11.2.1	c19~~20~~	c19~~20~~
23	413 (Request Entity Too Large)	[26] 21.4.11	m	m	[26] 21.4.11	i	i
24	414 (Request-URI Too Large)	[26] 21.4.12	m	m	[26] 21.4.12	i	i
25	415 (Unsupported Media Type)	[26] 21.4.13	m	m	[26] 21.4.13	i	i
26	416 (Unsupported URI Scheme)	[26] 21.4.14	m	m	[26] 21.4.14	i	i
27	420 (Bad Extension)	[26] 21.4.15	m	m	[26] 21.4.15	i	i

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
28	421 (Extension Required)	[26] 21.4.16	m	m	[26] 21.4.16	i	i
28A	422 (Session Interval Too Small)	[58] 6	c8	c8	[58] 6	c8	c8
29	423 (Interval Too Brief)	[26] 21.4.17	c5	c5	[26] 21.4.17	c6	c6
29A	429 (Provide Referrer Identity)	[59] 5	c9	c9	[59] 5	c9	c9
30	480 (Temporarily not available)	[26] 21.4.18	m	m	[26] 21.4.18	i	i
31	481 (Call /Transaction Does Not Exist)	[26] 21.4.19	m	m	[26] 21.4.19	i	i
32	482 (Loop Detected)	[26] 21.4.20	m	m	[26] 21.4.20	i	i
33	483 (Too Many Hops)	[26] 21.4.21	m	m	[26] 21.4.21	i	i
34	484 (Address Incomplete)	[26] 21.4.22	m	m	[26] 21.4.22	i	i
35	485 (Ambiguous)	[26] 21.4.23	m	m	[26] 21.4.23	i	i
36	486 (Busy Here)	[26] 21.4.24	m	m	[26] 21.4.24	i	i
37	487 (Request Terminated)	[26] 21.4.25	m	m	[26] 21.4.25	i	i
38	488 (Not Acceptable Here)	[26] 21.4.26	m	m	[26] 21.4.26	i	i
39	489 (Bad Event)	[28] 7.3.2	c4	c4	[28] 7.3.2	c4	c4
40	491 (Request Pending)	[26] 21.4.27	m	m	[26] 21.4.27	i	i
41	493 (Undecipherable)	[26] 21.4.28	m	m	[26] 21.4.28	i	i
41A	494 (Security Agreement Required)	[48] 2	c7	c7	[48] 2	n/a	n/a
105	5xx response	[26] 21.5	p25	p25	[26] 21.5	p25	p25
42	500 (Internal Server Error)	[26] 21.5.1	m	m	[26] 21.5.1	i	i
43	501 (Not Implemented)	[26] 21.5.2	m	m	[26] 21.5.2	i	i
44	502 (Bad Gateway)	[26] 21.5.3	m	m	[26] 21.5.3	i	i
45	503 (Service Unavailable)	[26] 21.5.4	m	m	[26] 21.5.4	i	i
46	504 (Server Time-out)	[26] 21.5.5	m	m	[26] 21.5.5	i	i
47	505 (Version not supported)	[26] 21.5.6	m	m	[26] 21.5.6	i	i
48	513 (Message Too Large)	[26] 21.5.7	m	m	[26] 21.5.7	i	i
49	580 (Precondition Failure)	[30] 8	m	m	[30] 8	i	i
106	6xx response	[26] 21.6	p26	p26	[26] 21.6	p26	p26
50	600 (Busy Everywhere)	[26] 21.6.1	m	m	[26] 21.6.1	i	i
51	603 (Decline)	[26] 21.6.2	m	m	[26] 21.6.2	i	i
52	604 (Does Not Exist Anywhere)	[26] 21.6.3	m	m	[26] 21.6.3	i	i
53	606 (Not Acceptable)	[26] 21.6.4	m	m	[26] 21.6.4	i	i

<table>
<tr><th rowspan="2">Item</th><th rowspan="2">Header</th><th colspan="3">Sending</th><th colspan="3">Receiving</th></tr>
<tr><th>Ref.</th><th>RFC status</th><th>Profile status</th><th>Ref.</th><th>RFC status</th><th>Profile status</th></tr>
<tr><td colspan="8">c1: IF A.163/9 AND A.162/5 THEN m ELSE n/a - - INVITE response, stateful proxy.
c2: IF A.163/9 THEN (IF A.162/5 THEN m ELSE i) ELSE n/a - - INVITE response, stateful proxy.
c3: IF A.163/9 THEN m ELSE n/a - - INVITE response.
c4: IF A.162/27 THEN m ELSE n/a - - SIP specific event notification.
c5: IF A.163/19 OR A.163/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.
c6: IF A.163/19 OR A.163/21 THEN i ELSE n/a - - REGISTER response or SUBSCRIBE response.
c7: IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c8: IF A.162/52 THEN m ELSE n/a - - the SIP session timer.
c9: IF A.162/53 AND A.163/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response.
c10: IF A.3/2 THEN m ELSE i - - P-CSCF.
c19: IF A.162/51 THEN i ELSE n/a - - an event state publication extension to the session initiation protocol.
c20: IF A.1624/51 THEN m ELSE n/a - - an event state publication extension to the session initiation protocol.
p21: A.164/2 OR A.164/3 OR A.164/4 OR A.164/5 - - 1xx response
p22: A.164/6 OR A.164/7 - - 2xx response
p23: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/13 - - 3xx response
p24: A.164/14 OR A.164/15 OR A.164/16 OR A.164/17 OR A.164/18 OR A.164/19 OR A.164/20 OR A.164/21 OR A.164/22 OR A.164/22A OR A.164/23 OR A.164/24 OR A.164/25 OR A.164/26 OR A.164/27 OR A.164/28 OR A.164/28A OR A.164/29 OR A.164/29A OR A.164/30 OR A.164/31 OR A.164/32 OR A.164/33 OR A.164/34 OR A.164/35 OR A.164/36 OR A.164/436 OR A.164/38 OR A.164/39 OR A.164/40 OR A.164/41 OR A.164/41A. - - 4xx response
p25: A.164/42 OR A.164/43 OR A.164/44 OR A.164/45 OR A.164/46 OR A.164/47 OR A.164/48 OR A.164/49 - - 5xx response
p26: A.164/50 OR A.164/51 OR A.164/52 OR A.164/53 - - 6xx response</td></tr>
</table>

3GPP TSG-CT1 Meeting #38 **Tdoc C1-050599**
Cancun, Mexico, 25-29 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	862	⌘**rev**	**-**	⌘	Current version:	**6.6.0**	⌘

*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:	⌘	Shared public user identities		
Source:	⌘	Lucent Technologies		
Work item code:	⌘	IMS2	***Date:*** ⌘	15/04/2005
Category:	⌘	**F**	***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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change: ⌘ If the user shares at least one public user identity with another user through a joint subscription, then all public user identities of both users will be registered with the same S-CSCF, i.e., the registration of all public user identities belonging to the subscription are sent to the same S-CSCF. For example,

- if the public user identities A, B, and X belong to the user#1, and if the public user identities 1, 2, and X belong to the user#2, and the user#1 has registered only the public user identity A with the S-CSCF#1, and subsequently

- if the user#2 sends an initial registration for the public user identity 1, then this registration will be sent to the S-CSCF#1,

in spite of the public user identity X not being registered.

Summary of change: ⌘ Added text clarifies that the registration of all public user identities - not only the shared one - are sent the same S-CSCF.

Consequences if not approved: ⌘ Inaccurate specification.

Clauses affected: ⌘ 5.3.1.2

		Y	**N**		
Other specs	⌘		**X**	Other core specifications	⌘

affected:	☒	Test specifications	
	☒	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.

CHANGE

5.3.1.2 Normal procedures

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

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

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

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

1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;

2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

3) forward the REGISTER request to the indicated S-CSCF.

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

1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more then one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;

2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

4) forward the REGISTER request to the selected S-CSCF.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF.

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050671

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229**	**CR 865**	⌘ **rev**	**1** ⌘	Current version:	**6.6.0** ⌘

*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: ⌘	Unsubscribe by P-CSCF		
Source: ⌘	Lucent Technologies		
Work item code: ⌘	IMS2	***Date:*** ⌘	15/04/2005
Category: ⌘	**F**	***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:* *Ph2 (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)* *Rel-7 (Release 7)*

Reason for change: ⌘	When all public user identities of the subscription have been deregistered, the S-CSCF is not serving this subscription anymore. Hence, the subscribers to the reg event of this subscription can not unsubscribe, since there is no S-CSCF serving this subscription. Therefore, the IMS employs the mechanism where - when all public user identities of the subscription have been deregistered - the S-CSCF unsubscribes all subscribers to reg event by including the Subscription-State header set to "terminated" in the last NOTIFY request. In this case no action from the P-CSCF is necessary.
Summary of change: ⌘	Text added indicating that when the P-CSCF will receive a NOTIFY request with the Subscription-State header set to "terminated", no action from the P-CSCF is necessary.
Consequences if not approved: ⌘	The procedure described in the current text (i.e. the P-CSCF unsubscribeing to reg event) cannot be executed, since upon deregistration of all public user IDs of the subscription, there is no S-CSCF serving this subscription.

Clauses affected: ⌘	5.2.4			
	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.

*** CHANGE***

5.2.4 Registration of multiple public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the P-CSCF shall maintain the generated dialog (identified by the values of the Call-ID, To and From headers).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package of the user, the P-CSCF shall perform the following actions:

1) for each public user identity whose state attribute in the <registration> element is set to "active", i.e. registered; and

    - the state attribute within the <contact> sub-element is set to "active"; and

    - the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and

    - the event attribute of that <contact> sub-element(s) is set to "registered" or "created";

    the P-CSCF shall bind the indicated public user identity as registered to the contact information of the respective user;

2) for each public user identity whose state attribute in the <registration> element is set to "active", i.e. registered: and

    - the state attribute within the <contact> sub-element is set to "terminated";

    - the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and

    - the event attribute of that <contact> sub-element(s) is set to "deactivated", "expired", "probation", "unregistered", or "rejected";

    the P-CSCF shall consider the indicated public user identitiy as deregistered for this user, and shall release all stored information for the public user identity bound to the respective user; and

3) for each public user identity whose state attribute in the <registration> element is set to "terminated", i.e. deregistered; and

    - the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and

    - the event attribute of that <contact> sub-element(s) is set to "deactivated", "expired", "probation", "unregistered", or "rejected";

the P-CSCF shall consider the indicated public user identitiy as deregistered for this UE, and shall release all stored information for these public user identity bound to the respective user.

If all public user identities, that were registered by the user using its private user identity, have been deregistered, the P-CSCF~~,~~ will receive from the S-CSCF a NOTIFY request that may include the Subscription-State header set to "terminated", as described in subclause 5.4.2.1.2. If the Subscription-State header was not set to "terminated", the P-CSCF may either unsubscribe to the reg event package of the user or let the subscription expire.

NOTE 1: Upon receipt of a NOTIFY request with the Subscription-State header set to "terminated", the P-CSCF considers the subscription to the reg event package terminated (i.e. as if the P-CSCF had sent a SUBSCRIBE request with an Expires header containing a value of zero).

NOTE 2: There may be public user identities which are implicitly registered within the registrar (S-CSCF) of the user upon registration of one public user identity. The procedures in this subclause provide a mechanism to inform the P-CSCF about these implicitly registered public user identities.

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050684
(Revision of Tdoc C1-050642)

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**916**	⌘ **rev**	**1**	⌘	Current version:	**6.6.0**	⌘

*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:	⌘	Clarify that S-CSCF shall support Supported and Require headers		
Source:	⌘	Qualcomm Incorporated		
Work item code:	⌘	IMS2	***Date:*** ⌘	28/4/2005
Category:	⌘	**F**	***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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The current text is not clear whether the S-CSCF is required to support Supported and Require headers.
Summary of change:	⌘	Clearly state that the support of these headers is mandatory
Consequences if not approved:	⌘	Incompatible IMS-compliant implementations. Incompatibility between R5 and R6 specifications.

Clauses affected: ⌘ 5.4.1.1

Other specs affected: ⌘

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

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5 Application usage of SIP

[...]

5.4 Procedures at the S-CSCF

5.4.1 Registration and authentication

5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs belonging to the IM CN subsystem and with public user identities.

The S-CSCF shall support the use of the Path and Service-Route header. The S-CSCF shall~~must~~ also support the Require and Supported headers. The Path header is only applicable to the REGISTER request and its 200 (OK) response. The Service-Route header is only applicable to the 200 (OK) response of REGISTER.

The network operator defines minimum and maximum times for each registration. These values are provided within the S-CSCF.

The procedures for notification concerning automatically registered public user identities of a user are described in subclause 5.4.2.1.2.

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050700

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**858**	⌘ **rev**	**1**	⌘	Current version:	**6.6.0**	⌘

*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:	⌘	S-CSCF redirecting			
Source:	⌘	Lucent Technologies			
Work item code:	⌘	IMS2	***Date:***	⌘	15/04/2005
Category:	⌘	**F**	***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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The text in RFC-3261 says: "The 305 (Use Proxy) responses MUST only be generated by UASs". The CR C1-050438 [CR 787] specifies that the S-CSCF will use the 305 (Use Proxy) responses to redirect an incoming call, that originated from a SIP terminal that supports only IPv4 addressing, to the IMS-ALG. If this C1-050438 is approved, then it is necessary to specify that, when sending the 305 (Use Proxy) responses, the S-CSCF shall provide the UA role
Summary of change:	⌘	The added text indicates that, if the S-CSCF redirects the call by returning a 305 (Use Proxy) responses, it acts as a UAS.
Consequences if not approved:	⌘	From the current text in 24229, it is not clear wheteher the CSCFs are allowed to generate the responses directly to requests in situations over and above specific instances in clause 5.

Clauses affected:	⌘	4.1				
		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.

CHANGE

4.1 Conformance of IM CN subsystem entities to SIP, SDP and other protocols

SIP defines a number of roles which entities can implement in order to support capabilities. These roles are defined in annex A.

Each IM CN subsytem functional entity using an interface at the Gm reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point, the Mr reference point and the Mw reference point, and also using the IP multimedia Subsystem Service Control (ISC) Interface, shall implement SIP, as defined by the referenced specifications in Annex A, and in accordance with the constraints and provisions specified in annex A, according to the following roles.

The Gm reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point and the Mw reference point are defined in 3GPP TS 23.002 [2].

The Mr reference point is defined in 3GPP TS 23.228 [7].

The ISC interface is defined in 3GPP TS 23.228 [7] subclause 4.2.4.

- The User Equipment (UE) shall provide the User Agent (UA) role, with the exceptions and additional capabilities to SIP as described in subclause 5.1, with the exceptions and additional capabilities to SDP as described in subclause 6.1, and with the exceptions and additional capabilities to SigComp as described in subclause 8.1. The UE shall also provide the access dependent procedures described in subclause B.2.2.
- The P-CSCF shall provide the proxy role, with the exceptions and additional capabilities to SIP as described in subclause 5.2, with the exceptions and additional capabilities to SDP as described in subclause 6.2, and with the exceptions and additional capabilities to SigComp as described in subclause 8.2. Under certain circumstances as described in subclause 5.2, the P-CSCF shall provide the UA role with the additional capabilities, as follows:

  a) when acting as a subscriber to or the recipient of event information; and

  b) when performing P-CSCF initiated dialog-release the P-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.
- The I-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.3.
- The S-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.4, and with the exceptions and additional capabilities to SDP as described in subclause 6.3. Under certain circumstances as described in subclause 5.4, the S-CSCF shall provide the UA role with the additional capabilities, as follows:

  a) the S-CSCF shall also act as a registrar. When acting as a registrar, or for the purposes of executing a third-party registration, the S-CSCF shall provide the UA role;

  b) as the notifier of event information the S-CSCF shall provide the UA role;

  c) when providing a messaging mechanism by sending the MESSAGE method, the S-CSCF shall provide the UA role; and

  d) when performing S-CSCF initiated dialog release the S-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.
- The MGCF shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.4.
- The BGCF shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.6.

- The AS, acting as terminating UA, or redirect server (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.1), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.2, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

- The AS, acting as originating UA (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.2), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.3, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

- The AS, acting as a SIP proxy (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.3), shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.7.4.

- The AS, performing 3rd party call control (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.4), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

NOTE 1: Subclause 5.7 and its subclauses define only the requirements on the AS that relate to SIP. Other requirements are defined in 3GPP TS 23.218 [5].

- The AS, receiving third-party registration requests, shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.

- The MRFC shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8, and with the exceptions and additional capabilities to SDP as described in subclause 6.5.

- The IMS-ALG shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.9, and with the exceptions and additional capabilities to SDP as described in subclause 6.5.

In addition to the roles specified above, the P-CSCF, the I-CSCF, the S-CSCF, the BGCF can act as a UA when providing server functionality to return a final response for any of the reasons specified in RFC 3261 [26].

NOTE 2: Annex A can change the status of requirements in referenced specifications. Particular attention is drawn to table A.4 and table A.162 for capabilities within referenced SIP specifications, and to table A.317 and table A.328 for capabilities within referenced SDP specifications. The remaining tables build on these initial tables.

NOTE 3: The allocated roles defined in this clause are the starting point of the requirements from the IETF SIP specifications, and are then the basis for the description of further requirements. Some of these extra requirements formally change the proxy role into a B2BUA. In all other respects other than those more completely described in subclause 5.2a P-CSCF implements proxy requirements. Despite being a B2BUA a P-CSCF does not implement UA requirements from the IETF RFCs, except as indicated in this specification, e.g., relating to registration event subscription.

3GPP TSG-CT1 Meeting #38 **Tdoc C1-050701**
Cancun, Mexico, 25-29 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **860** ⌘**rev** **1** ⌘ Current version: **6.6.0** ⌘

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: ⌘	P-CSCF - routing of REGISTER requests		
Source: ⌘	Lucent Technologies		
Work item code: ⌘	IMS2	***Date:*** ⌘	15/04/2005
Category: ⌘	**F**	***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:* *Ph2 (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)* *Rel-7 (Release 7)*

Reason for change: ⌘	The document 24.229-660 [Rel-6] subclause 5.3.1.3 specifies the procedure that the I-CSCF follows when - upon receiving a REGISTER request - fail to forward the request to the "next hop" [i.e., S-CSCF]. In addition, subclause 5.1.1.4 also specifies the procedure that the UE follows when it fails to forward the REGISTER request to the "next hop" [i.e., P-CSCF] - "the case when the timer F expires". The same procedure is not described for the P-CSCF.
Summary of change: ⌘	Text added describing the P-CSCF's procedure when it fails to forward the REGISTER request.
Consequences if not approved: ⌘	Unnecessary failure of registration in spite of resources needed for registration being available.

Clauses affected: ⌘	References and 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 *****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".

[6] 3GPP TS 23.221: "Architectural requirements".

[7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[8A] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8B] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[9A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".

[10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[11A] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".

[11B] 3GPP TS 29.163: "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks".

[12] 3GPP TS 29.207: "Policy control over Go interface".

[13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[13A] 3GPP TS 29.209: "Policy control over Gq interface".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

[16] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[17] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

[18] 3GPP TS 33.102: "3G Security; Security architecture".

[19] 3GPP TS 33.203: "Access security for IP based services".

[19A] 3GPP TS 33.210: "IP Network Layer Security".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[20A] RFC 2401 (November 1998): "Security Architecture for the Internet Protocol".

[20B] RFC 1594 (March 1994): "FYI on Questions and Answers to Commonly asked "New Internet User" Questions".

[20C] RFC 2403 (November 1998) "The Use of HMAC-MD5-96 within ESP and AH".

[20D] RFC 2404 (November 1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[20E] RFC 2462 (November 1998): "IPv6 Address Autoconfiguration".

[21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 3966 (December 2004): "The tel URI for Telephone Numbers".

[23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 3761 (April 2004): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[25] RFC 2976 (October 2000): "The SIP INFO method".

[25A] RFC 3041 (January 2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[26] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[27] RFC 3262 (June 2002): "Reliability of provisional responses in Session Initiation Protocol (SIP)".

[27A] RFC 3263 (June 2002): " Session Initiation Protocol (SIP): Locating SIP Servers".

[28] RFC 3265 (June 2002): "Session Initiation Protocol (SIP) Specific Event Notification".

[29] RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".

[30] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".

[31] RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".

[32] RFC 3320 (March 2002): "Signaling Compression (SigComp)".

[33] RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[34] RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".

[34A] RFC 3326 (December 2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".

[35] RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method".

[37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag".

[38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[39] draft-ietf-mmusic-sdp-new-13 (May 2003): "SDP: Session Description Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[40] RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[42] RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)".

[43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[51] Void.

[52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[53] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".

[54] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows".

[55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".

[56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[56A] RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[56B] RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)"

[57] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[58] draft-ietf-sip-session-timer-15 (November 2004): "Session Timers in the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[59] RFC 3892 (September 2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".

[60] RFC 3891 (September 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

[61] RFC 3911 (October 2004): "The Session Inititation Protocol (SIP) "Join" Header".

[62] RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

[63] RFC 3861 (August 2004): "Address Resolution for Instant Messaging and Presence".

[64] draft-ietf-sip-rfc3312-update-03 (September 2004): "Update to the Session Initiation Protocol (SIP) Preconditions Framework".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[70] RFC 3903 (October 2004): "An Event State Publication Extension to the Session Initiation Protocol (SIP)".

[71] Void.

[72] RFC 3857 (August 2004): "A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)".

[74] RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[75] draft-ietf-simple-event-list-04 (June 2003): "A Session Initiation Protocol (SIP) Event Notification Extension for Collections".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[77] draft-ietf-sipping-config-framework-05 (October 2004): "A Framework for Session Initiation Protocol User Agent Profile Delivery".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[78] draft-ietf-sipping-conference-package-03 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Conference State"

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[79] draft-ietf-rohc-sigcomp-sip-01 (February 2004): "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

***** 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) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];

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 challenge response (i.e. RES parameter), or it was received on the security association created during the last successful

authentication procedure and with no authentication challenge response (i.e. no RES parameter), 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. 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 the security association is a temporary one, then the request 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;

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

      - the P-CSCF shall remove the Security-Verify header if it is present;

      - 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 Authorization header of 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.

   If the selected I-CSCF:

   - does not respond to the REGISTER request and its retransmissions by the P-CSCF; or

   - sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

   the P-CSCF shall select a new I-CSCF and forward the original REGISTER request.

NOTE 1: The list of the I-CSCFs may be either obtained as specified in RFC 3263 [27A] or provisioned in the P-CSCF.

   If the P-CSCF fails to forward the REGISTER request to any I-CSCF, the P-CSCF shall send back a 408 (Request Timeout) response or 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26].

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) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and 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) 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;

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 the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and

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 2~~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 3~~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) if a temporary set of 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 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.

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 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 4~~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 5~~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 other set 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 6~~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-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050708

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**866**	⌘**rev**	**1**	⌘	Current version:	**6.6.0** ⌘

*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:	⌘	Protected initial registration		
Source:	⌘	Lucent Technologies		
Work item code:	⌘	IMS2	***Date:*** ⌘	15/04/2005
Category:	⌘	**F**	***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:*	*Ph2 (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)* *Rel-7 (Release 7)*

Reason for change:	⌘	The registration is considered to be "initial" if it is the first public user identity being registered by the UE using its private user identity [i.e. at that stage all public user identities have been deregistered]. The document 33.203 subclause 7.4.1a entitled "Management of security associations in the UE" clearly states: " The UE shall delete all SAs it holds once all the IMPUs are de-registered". Hence, the UE has no SAs when it starts the initial registration.
Summary of change:	⌘	Text removed.
Consequences if not approved:	⌘	Risk of registration failure.

Clauses affected:	⌘	5.1.1.2				
		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.

*** CHANGE***

5.1.1.2 Initial registration

The UE can register a public user identity with its contact address at any time after it has aquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. 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 protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.~~

The UE shall extract or derive 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. 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) 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) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via 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 association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) an 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 3: 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.

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

h) 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. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];

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

j) if a security association exists, a P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3).

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

a) store the expiration time of the registration for the public user identities 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 as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;

d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;

e) 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 standalone transactions; and

f) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), 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) 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.

3GPP TSG-CT1 Meeting #38 **Tdoc C1-050709**
Cancun, Mexico, 25-29 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**894**	⌘ **rev**	**1**	⌘	Current version:	**6.6.0**	⌘

*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: ⌘	Re-registration failure			
Source: ⌘	Orange			
Work item code: ⌘	IMS2		***Date:*** ⌘	25/04/05
Category: ⌘	**F**		***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:* *Ph2 (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)* *Rel-7 (Release 7)*

Reason for change: ⌘	In the context of multiple UEs sharing the same public user identity, it can occur a re-register reaches a new S-CSCF. The following case shows an example where a re-register can reach a new S-CSCF: When the HSS is informed by the I-CSCF that the currently assigned S-CSCF is unreachable by the I-CSCF, deregistration by the HSS with the reason "SERVER_CHANGE" can be used to deregister all the UEs sharing the same public user identity and force them to perform an initial registration in order that all the UEs have the same new S-CSCF assigned. If the deregistration procedure initiated by the HSS with the reason "SERVER_CHANGE" can not be done correctly (e.g. because the S-CSCF is unreachable for the HSS or there is a link failure in the network preventing from reaching the UEs that are currently registered) there will be UEs that try to re-register towards the new assigned S-CSCF ; this new S-CSCF has been assigned to one of UEs among those sharing the same public user identities that performed an initial registration. This case should be covered in the specification TS 24.229. When re-register messages reaches a new S-CSCF, the new S-CSCF should send a 500 (Server Internal Error) error response to these re-register messages and the UEs should initiate an initial registration procedure.
Summary of change: ⌘	In section 5.4.1.2.3dealing with abnormal cases for the registration procedure at the S-CSCF, it is added that when receiving a re-register message that does not

		correspond to a registered user in the S-CSCF, the S-CSCF shall send the 500 (Server Internal Error) error message.
Consequences if not approved:	⌘	A possible failure case of re-registration when several UEs are sharing the same public user identity is not covered by the specification .

Clauses affected:	⌘	5.4.1.2.3				
		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.

*** BEGINNING OF THE FIRST MODIFICATION ***

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 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 without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", for an already registered public user identity linked to the same private user identity but with a new contact information (e.g. a user roams to a different network without de-registering the previous one), the S-CSCF shall:

1) perform the procedure for receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no"', for the received public user identity; and

2) if the authentication has been successful and if the previous registration has not expired, the S-CSCF shall perform the network initiated deregistration procedure only for the previous contact information as described in subclause 5.4.1.5.

Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", which is not for an already registered public user identity linked to the same private user identity, 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) 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 29.228 [14], 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 used by the HSS to direct all subsequent incoming initial requests for a dialog or standalone transactions destined for this user to this S-CSCF.

NOTE 4: When passing its SIP URI to the HSS, the S-CSCF may include in its SIP URI the transport protocol and the port number where it wants to be contacted.

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

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);

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

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-protected" 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 REGISTER requests received without the "integrity-protected" parameter in the Authorization header set to "yes".

   If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

2) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall proceed beginning with step 6 below.

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

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

2) stop timer reg-await-auth;

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

   a) the private user identity of the user in the username field;

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

   c) the authentication challenge response needed for the authentication procedure in the response field.

   The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

4) check whether the received authentication challenge response and the expected authentication challenge response (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49]) match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;

5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228 [14], 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(the initial Filter Criteria for the Registered and common parts is stored and the unregisterd part is retained for possible use later - in the case of the S-CSCF is retained if the user becomes unregistered);

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 including all header parameters contained in the Contact header and all associated URI parameters and store information for future use;

NOTE 2: There might be more then one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

7) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

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

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

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

a) the list of received Path headers;

b) a P-Associated-URI header containing the list of public user identities that the user is authorized to use. The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;

c) a Service-Route header containing:

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

d) a P-Charging-Function-Addresses header containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request; and

e) a Contact header listing all contact addresses for this public user identity.

NOTE 5: There might be other contact addresses available, that other UEs have registered for the same public user identity.

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 6: 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

In the case that the REGISTER request, that contains the authentication challenge response from the UE does not match with the expected REGISTER request (e.g. wrong Call-Id or authentication challenge response) and the request has the "integrity-protected" parameter in the Authorization header set to "yes", 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 state 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 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 state 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. In order to indicate a resynchronisation, the S-CSCF shall include the AUTS received from the UE and the stored RAND, when fetching the new authentication vectors. On receipt of the new authentication vectors from the HSS, the S-CSCF shall either:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors; or

- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned. The S-CSCF shall not update the registration state of the subscriber.

NOTE 3: If the UE was registered before, it stays registered until the registration expiration time expires.

NOTE 4: Since the UE responds only to two consecutive invalid 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 5: 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].

In the case that the S-CSCF receives a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", for which the public user identity received in the To header and the private user identity received in the Authorization header of the REGISTER request do not match to any registered user at this S-CSCF, the S-CSCF shall:

- respond with a 500 (Server Internal Error) response to the UE.

*** END OF THE FIRST MODIFICATION ***

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, April 25th – April 29th, 2005

Tdoc ⌘C1-050711

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**870**	⌘**rev**	**1**	⌘	Current version:	**6.6.0**	⌘

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: ⌘	Correction of table A.104A		
Source: ⌘	Ericsson		
Work item code: ⌘	IMS2	***Date:*** ⌘	12/04/2005
Category: ⌘	**F**	***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:* *Ph2 (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)* *Rel-7 (Release 7)*

Reason for change: ⌘	The table A.104A is incorrect for the header field Accept-Contact. The table also incorrectly refer to the major capabilities table for the P-CSCF instead of the corresponding table for the UE.
Summary of change: ⌘	The table A.104A is corrected
Consequences if not approved: ⌘	Incorrect implementation of the callers preferences may cause sessions to fail.

Clauses affected: ⌘	A.2.1.4.10A				
	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.

A.2.1.4.10A PUBLISH method

Prerequisite A.5/15A – PUBLISH request

Table A.104A: Supported headers within the PUBLISH request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Contact	[56B] 9.2	c224	c224	[56B] 9.2	n/a	n/a
2	Allow	[26] 20.5	o	o	[26] 20.5	m	m
3	Allow-Events	[26] 7.2.2	c1	c1	[26] 7.2.2	c2	c2
4	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
5	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
7	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
8	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
9	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
14	Event	[70] 4, 6	m	m	[70] 4, 6	m	m
15	Expires	[26] 20.19, [70] 4, 5, 6	o	o	[26] 20.19, [70] 4, 5, 6	m	m
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	In-Reply-To	[26] 20.21	o	o	[26] 20.21	o	o
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
19	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
20	Organization	[26] 20.25	o	o	[26] 20.25	o	o
21	P-Access-Network-Info	[52] 4.4	c15	c16	[52] 4.4	c15	c17
22	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c11	c11
23	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c13	c13
24	P-Charging-Function-Addresses	[52] 4.5	c20	c21	[52] 4.5	c20	c21
25	P-Charging-Vector	[52] 4.6	c18	c19	[52] 4.6	c18	c19
26	P-Preferred-Identity	[34] 9.2	c11	c7	[34] 9.2	n/a	n/a
27	P-Visited-Network-ID	[52] 4.3	x (note 3)	x	[52] 4.3	c14	n/a
28	Priorità	[26] 20.26	o	o	[26] 20.26	o	o
29	Privacy	[33] 4.2	c12	c12	[33] 4.2	c12	c12
30	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
31	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
32	Reason	[34A] 2	c8	c8	[34A] 2	c8	c8
33	Reject-Contact	[56B] 9.2	c22	c22	[56B] 9.2	n/a	n/a
33A	Referred-By	[59] 3	c25	c25	[59] 3	c26	c26
34	Request-Disposition	[56B] 9.1	c22	c22	[56B] 9.1	n/a	n/a
35	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
36	Require	[26] 20.32	o	o	[26] 20.32	m	m
37	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
38	Security-Client	[48] 2.3.1	c9	c9	[48] 2.3.1	n/a	n/a
39	Security-Verify	[48] 2.3.1	c10	c10	[48] 2.3.1	n/a	n/a
40	SIP-If-Match	[70] 11.3.2	o	o	[70] 11.3.2	m	m
41	Subject	[26] 20.36	o	o	[26] 20.36	o	o
42	Supported	[26] 20.37, [26] 7.1	o	o	[26] 20.37, [26] 7.1	m	m
43	Timestamp	[26] 20.38	c6	c6	[26] 20.38	m	m
44	To	[26] 20.39	m	m	[26] 20.39	m	m
45	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
46	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1: IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.
c2: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c3: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5: IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c7: IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c8: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c9: IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 1).
c10: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c11: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c12: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c13: IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c14: IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c15: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c16: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c17: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c18: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c19: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c20: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c21: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c22: IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
~~c24: IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.~~
c25: IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c26: IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.

NOTE 1: Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented.
NOTE 2: The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.

………….

Remaining part of subclause not shown

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050716

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**887**	⌘**rev**	**1**	⌘	Current version:	**6.6.0** ⌘

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:	⌘	Contact address in REGISTER response		
Source:	⌘	LM Ericsson		
Work item code:	⌘	IMS2	***Date:*** ⌘	14/04/2005
Category:	⌘	**F**	***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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Section 5.4.1.2.3 describes which contact address the S-CSCF shall include in the contact header in the 200 OK when multiple SIP URIs were included in the contact header in REGISTER request. However it only describes the case when one of the contact addresses has a higher "q" value than the other contact addresses.
Summary of change:	⌘	Two more cases are added.
Consequences if not approved:	⌘	The specification is incomplete.

Clauses affected:	⌘	5.4.1.2.3			
		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.

5.4.1.2.3 Abnormal cases

In the case that the REGISTER request, that contains the authentication challenge response from the UE does not match with the expected REGISTER request (e.g. wrong Call-Id or authentication challenge response) and the request has the "integrity-protected" parameter in the Authorization header set to "yes", 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 state 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 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 state 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. In order to indicate a resynchronisation, the S-CSCF shall include the AUTS received from the UE and the stored RAND, when fetching the new authentication vectors. On receipt of the new authentication vectors from the HSS, the S-CSCF shall either:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors; or

- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned. The S-CSCF shall not update the registration state of the subscriber.

NOTE 3: If the UE was registered before, it stays registered until the registration expiration time expires.

NOTE 4: Since the UE responds only to two consecutive invalid 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~~ ;or

- the entry in the contact header with the highest “q”; or

- an entry decided by the S-CSCF based on local policy

and include it in the 200 (OK) response.

NOTE 5: 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].

5.4.1.3 Authentication and reauthentication

Authentication and reauthentication is performed by the registration procedures as described in subclause 5.4.1.2.

5.4.1.4 User-initiated deregistration

When S-CSCF receives a REGISTER request with the Expires header field containing the value zero, the S-CSCF shall:

- check whether the "integrity-protected" parameter in the Authorization header field set to "yes", indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps if the "integrity-protected" parameter is set to "yes";
- release each multimedia session that includes this user, where the session was initiated by this UE with the public user identity found in the P-Asserted-Identity header field or with one of the implicitly registered public used identities by applying the steps listed in subclause 5.4.5.1.2;
- if this public used identity was registered only by this UE, deregister the public user identity found in the To header field together with the implicitly registered public user identities. Otherwise, the S-CSCF will only remove the contact address that was registered by this UE;
- 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
- if this is a deregistration request for the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) and there are still active multimedia sessions that includes this user, where the session was initiated with the public user identity currently registered or with one of the implicitly registered public used identities, release each of these multimedia sessions by applying the steps listed in subclause 5.4.5.1.2.

If all public user identities of the UE are deregistered, then the S-CSCF may consider the UE and P-CSCF subscriptions 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).

If the Authorization header of the REGISTER request did not contain an "integrity-protected" parameter, or the "integrity-protected" parameter was set to the value "no", the S-CSCF shall apply the procedures described in subclause 5.4.1.2.1.

On completion of the above procedures in this subclause and of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228 [14], for one or more public user identities, the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber).

3GPP TSG-CT1 Meeting #38 **Tdoc C1-050717**
Cancun, Mexico, 25-29 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **TS 24.229** **CR** **890** ⌘**rev** **1** ⌘ Current version: **6.6.0** ⌘

*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:	⌘	P-CSCF Record-Route processing for target refresh requests/responses
Source:	⌘	LM Ericsson
Work item code:	⌘	IMS2
Date:	⌘	12/04/2005
Category:	⌘	**F**
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change: ⌘ The route-set cannot be updated during a session, even if Record-Route headers are added to the request. Only the remote target can be updated. RFC3261 does, however, say that a proxy SHOULD add a Record-Route when forwarding a target refresh request.

However, since the route-set cannot be updated the P-CSCF does not need to, when the target refresh response is received, store the Record-Route headers for the purpose of possible session release. Also, since all proxies may not insert a Record-Route in the target refresh request the new route-set may be incorrect.

See chapters 12.2 and 16.6 in RFC3261 for detailed information.

Summary of change: ⌘ The P-CSCF does not store (in order to be able to release the session) the Record-Route entities received in the target refresh response.

Consequences if not approved: ⌘ The P-CSCF performs tasks that can lead to the wrong route-set to be stored.

Clauses affected: ⌘ 5.2.6.3, 5.2.6.4

Other specs affected: ⌘

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

Other comments:	⌘	There is another CR that corrects the text on when the Record-Route header values are stored by the P-CSCF for the purpose of P-CSCF initiated session release.

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 MODIFICATION ******

5.2.6.3 Requests initiated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more then one default public user identity available, the P-CSCF shall randomly select one of them.

NOTE 1: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCFshall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

   b) replace the preloaded Route header value in the request with the value of the Service-Route header received during the last 200 (OK) response for a registration or reregistration;

2) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC3261 [26], and either:

   a) the P-CSCF FQDN that resolves to the IP address, or

   b) the P-CSCF IP address;

3) when adding its own SIP URI to the top of the Record-Route header, build the ~~. The~~ P-CSCF SIP URI ~~is built~~ in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

   a) the P-CSCF FQDN that resolves to the IP address; or

   b) the P-CSCF IP address;

4) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]; and

6) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

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

2) store the list of Record-Route headers from the received response;

3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;

4) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 2: The P-CSCF 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 values see 3GPP TS 33.203 [19].

5) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE a target refresh request for a dialog, the P-CSCF shall:

1) verify if the request relates to a dialog in which the originator of the request is involved:

   a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;

   b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

   b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog;

3) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF where it awaits the responses to come, and either:

   a) the P-CSCF FQDN that resolves to the IP address, or

   b) the P-CSCF IP address;

4) when adding its own SIP URI to the top of Record-Route header~~.~~, build ~~T~~the P-CSCF SIP URI ~~is built~~ in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

   a) the P-CSCF FQDN that resolves to the IP address; or

   b) the P-CSCF IP address; and

5) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

~~1) store the list of Record-Route headers from the received response;~~

1~~2~~) rewrite the port number of its own Record Route entry to the same value as for the response to the initial request for the dialog~~to its own protected server port number negotiated with the calling UE~~, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

~~NOTE 3: The P-CSCF 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].~~

2~~3~~) if the response corresponds to an INVITE request, save the Contact ~~and Record-Route~~ header ~~field~~ value~~s~~ received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for a standalone transaction, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

   b) replace the preloaded Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response;

2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and

3) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

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

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall:

1) verify if the request relates to a dialog in which the originator of the request is involved:

   a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;

   b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

   b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog; and

3) for dialogs that are not INVITE dialogs, add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];

before forwarding the request, (based on the topmost Route header,) in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for an unknown method (that does not relate to an existing dialog), and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) is included, preserving the same order, as a subset of the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

   b) replace the Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response; and

2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

****** SECOND MODIFICATION ******

5.2.6.4 Requests terminated by the UE

When the P-CSCF receives, destined for the UE, an initial request for a dialog, prior to forwarding the request, the P-CSCF shall:

1) convert the list of Record-Route header values into a list of Route header values and save this list of Route headers;

2) if the request is an INVITE request, save a copy of the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

3) when adding its own SIP URI to the top of the list of Record-Route headers and save the list~~.~~, build ~~T~~the P-CSCF SIP URI ~~is built~~ in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

4) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 1: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

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

6) remove and store the icid parameter received in the P-Charging-Vector header; and

7) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

1) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with the value saved from the P-Called-Party-ID header that was received in the request;

2) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

3) verify that the list of URIs received in the Record-Route header of the request corresponding to the same dialog is included, preserving the same order, as a subset of the Record-Route header list of this response. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Record-Route header values with those received in the request, rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter.

   If the verification is successful, the P-CSCF shall rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

4) store the dialog ID and associate it with the private user identity and public user identity involved in the session; and

5) if the response corresponds to an INVITE request, save the Contact and Record-Route header field value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a target refresh request for a dialog, prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

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

2) when adding its own SIP URI to the top of the list of Record-Route headers and save the list, build the P-CSCF SIP URI in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

3~~2~~) if the request is an INVITE request, save the Contact and~~,~~ Cseq ~~and Record-Route~~ header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

2) rewrite the port number of its own Record-Route entry to the same value as for the response to the initial request for the dialog~~to the port number where it awaits subsequent requests from the calling party~~ and remove the comp parameter; and

3) if the response corresponds to an INVITE request, save the Contact~~ and Record-Route~~ header field value~~s~~ received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a request for a standalone transaction, or a request for an unknown method (that does not relate to an existing dialog), prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 3: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

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

3) remove and store the icid parameter received in the P-Charging-Vector header; and

4) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request; and

2) remove the P-Preferred-Identity header, if present, and insert an P-Asserted-Identity header with the value saved from the P-Called-Party-ID header of the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request (including requests relating to an existing dialog where the method is unknown), prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

NOTE 4: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

2) remove and store the icid parameter from P-Charging-Vector header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050719

was Tdoc C1-050572

CR-Form-v7.1

CHANGE REQUEST

⌘	**TS 24.229**	**CR**	**893**	⌘ **rev**	**1**	⌘ Current version:	**6.6.0** ⌘

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:	⌘	AS originated requests on behalf of PSI
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	15/04/2005
Category:	⌘	**F**
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	3GPP TS 23.228 has requirements for an AS to originate requests on behalf of a PUID or a PSI. This requires that the S-CSCF recognize the request for origination processing rather than termination processing. 3GPP TS 24.229 currently describes the originating AS behavior for originating on behalf of PUID by including “orig” parameter with the S-CSCF URI in the Route header. The corresponding description for AS originating on behalf of PSI does not include the “orig” parameter. The S-CSCF processing decision to do origination versus termination processing depends on the “orig” parameter when receiving requests from an AS. Since the “orig” parameter is missing for PSI, the S-CSCF cannot make the correct decision. With the change, the S-CSCF will be able to perform the correct origination processing. It remains a S-CSCF implementation issue for how it recognizes a PSI.
Summary of change:	⌘	In clause 5.7.3, a statement is added such that the “orig” parameter is added to the S-CSCF URI in the Route header when the AS originates a request on behalf of a PSI owned by the AS.
Consequences if not approved:	⌘	In clause 5.4.3.1, the decision to perform mobile-originating procedures depends upon information in the Route header: either a match of information from Service-Route header from registration or the presence of the “orig” parameter. Without this change, an AS originated request sent on behalf of a PSI without the “orig” parameter can only fall into the mobile-terminating procedures, which results in incorrect processing and failed requests. For example, if AS wishes to

		originate an INVITE to a PSTN destination on behalf of PSI, it won’t work with the current specification because the termination procedures expect an IMS subscriber in the Request-URI.

Clauses affected:	⌘	5.7.3				
		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.

5.7.3 Application Server (AS) acting as originating UA

When acting as an originating UA the AS shall behave as defined for a UE in subclause 5.1.3, with the exceptions identified in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

When an AS acting as an originating UA generates an initial request for a dialog or a request for a standalone transaction, the AS shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]. The AS may retrieve CCF and/or ECF addresses from HSS on Sh interface.

When an AS acting as an originating UA generates a subsequent request that does not relate to an INVITE dialog, the AS shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

The AS shall extract charging function addresses from any P-Charging-Function-Addresses header that is received in any 1xx or 2xx responses to the requests.

The AS may also indicate that the proxies should not fork the INVITE request by including a "no-fork" directive within the Request-Disposition header in the initial INVITE request as described in RFC 3841 [56B].

When sending an initial request on behalf of a PSI that is hosted by the AS, the AS shall insert a Route header pointing to an S-CSCF of the home network of the PSI, if:

- the AS is not able to resolve the next hop address by itself; or
- the operator policy requires it.

NOTE 1: The address of the S-CSCF may be obtained by querying the HSS on the Sh interface or from static configuration.

When sending an initial request on behalf of a public user identity, the AS shall insert a Route header pointing to the S-CSCF where the public user identity on whose behalf the request is generated is registered or hosted (unregistered case).

NOTE 2: The address of the S-CSCF may be obtained either from a previous request terminated by the AS, by querying the HSS on the Sh interface or from static configuration.

For the use of the P-Asserted-Identity by the AS, at least two cases exist:

a) any initial request for a dialog or request for a standalone transaction is generated as if it was originated by the UE on whose behalf the request is generated. In this case the AS shall insert a P-Asserted-Identity representing a public user identity of that UE. The AS shall append the "orig" parameter to the URI of the S-CSCF; and

b) any initial request for a dialog or request for a standalone transaction is generated by an AS supporting a service identified by a PSI. In this case the AS shall insert a P-Asserted-Identity containing the PSI of the AS. Also, the AS shall append the "orig" parameter to the URI of the S-CSCF.

Editor's Note: It needs to be specified that the AS can only add the P-Asserted-Identity when the AS is within the trust domain.

The AS can indicate privacy of the P-Asserted-Identity in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the AS shall set the From header to "Anonymous".

NOTE 3: The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the AS indication of privacy or by network subscription or network policy. Therefore the AS should include the value "Anonymous" whenever privacy is explicitly required.

Editor's note: Is there a need to specify any conditions for the AS choosing to indicate privacy that are generic to all originating AS, or all conditions service specific, and therefore out of the scope of 24.229.

3GPP TSG–CT1 Meeting #38
Cancun, Mexico, 25th to 29th April 2005

***Tdoc* ⌘C1-050720**

CR-Form-v7

CHANGE REQUEST

⌘	**TS 24.229**	**CR**	**896**	⌘**rev**	**1**	⌘	Current version:	**6.6.0** ⌘

*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:	⌘	Routing of PSI at the terminating side			
Source:	⌘	Orange			
Work item code:	⌘	IMS2	***Date:***	⌘	18/04/05
Category:	⌘	**F**	***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: ⌘ In TS 23.228 section 5.4.12.2 about PSIs on the terminating side, it is stated:

The Application Server hosting the PSI may be invoked as a terminating Application Server via information stored in the HSS.

For both the distinct PSIs and wildcarded PSIs, there are two ways to route towards the AS hosting the PSI:

a) The HSS maintains the assigned S-CSCF information and ISC Filter Criteria information for the "PSI user" to route to the AS hosting the PSI according to IMS routing principles. In this case, the I-CSCF receives SIP requests at the terminating side, queries the HSS and directs the request to the S-CSCF assigned to the "PSI user". The S-CSCF forwards the session to the Application Server hosting the PSI according to the terminating ISC Filter Criteria.

b) The HSS maintains the address information of the AS hosting the PSI for the "PSI user". In this case, the AS address information for the PSI is returned to the I-CSCF in the location query response, in which case the I-CSCF will forward the request directly to the AS hosting the PSI.

Thus, the I-CSCF may obtain the AS address (direct routing case) or the S-CSCF address (indirect routing case) when querying the HSS for user location. In TS 23.228 section 5.4.12.3 about Subdomain based PSIs, it is stated:

Subdomain based PSIs are globally routable and can be made available to users within and outside the operator domain.

In this case, there are two ways to route towards the AS hosting the PSI:

a) When the subdomain name is defined in the global DNS, then the originating S-CSCF receives the IP address of the AS hosting the PSI, when it queries DNS. The principles defined in RFC 3263 [44] may be used. For example, a NAPTR query

		and then a SRV query may be used to get the IP address of the AS. b) The PSI is resolved by the global DNS to an I-CSCF address in the domain where the AS hosting the PSI is located. The I-CSCF recognises the subdomain (and thus does not query the HSS). It resolves the same PSI to the address of the actual destination AS hosting the PSI using an internal DNS mechanism, and forwards the requests directly to the AS. Thus, the I-CSCF may not query the HSS for user location when the Request-URI can be resolved into the IP address of an AS hosting a PSI.
Summary of change:	⌘	In section 5.3.2.1 for the I-CSCF behaviour, it is added that the I-CSCF may obtain an AS IP address by internal DNS mechanism and in that case will not do the user location query procedure.
Consequences if not approved:		Incomplete specifications: PSI routing is partially treated at the I-CSCF.

Clauses affected:	⌘	5.3.2.1				
		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 co

*** FIRST MODIFICATION ***

5.3.2.1 Normal procedures

The I-CSCF may behave as a stateful proxy for initial requests.

The I-CSCF shall verify for all requests whether they arrived from a trusted domain or not. If the request arrived from a non trusted domain, then the I-CSCF shall:

1) respond with 403 (Forbidden) response if the request is a REGISTER request;

2) remove all P-Asserted-Identity headers, all P-Access-Network-Info headers, all P-Charging-Vector headers and all P-Charging-Function-Addresses headers the request may contain, if the request is other than REGISTER request; and

3) continue with the procedures below.

If the request arrived from a trusted domain, the I-CSCF shall perform the procedures below.

NOTE 1: The I-CSCF may find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

When the I-CSCF receives an initial request for a dialog or standalone transaction the I-CSCF shall:

1) if the Request-URI includes a pres: or an im: URI, then translate the pres: or im: URI to a public user identity and replace the Request-URI of the incoming request with that public user identity; and

NOTE 2: SRV records have to be advertised in DNS pointing to the I-CSCF for pres: and im: queries.

2) if the request does not contain a Route header, then check if the domain name of the Request-URI matches with one of the PSI subdomains configured in the I-CSCF. If the match is successful, the I-CSCF resolves the Request-URI by an internal DNS mechanism into the IP address of the AS hosting the PSI and does not start the user location query procedure. Otherwise, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the called user, indicated in the Request-URI. Prior to performing the user location query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

When the I-CSCF receives an INVITE request, the I-CSCF may require the periodic refreshment of the session to avoid hung states in the I-CSCF. If the I-CSCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer [58] clause 8.

NOTE 3: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

In case the I-CSCF is able to resolve the Request-URI into the IP address of the AS hosting the PSI, then it shall:

1) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. If no icid parameter was found, then create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

3) forward the request directly to the AS hosting the PSI.

Upon successful user location query, when the response contains the URI of the assigned S-CSCF, the I-CSCF shall:

1) insert the URI received from the HSS as the topmost Route header;

2) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. If no icid parameter was found, then create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

4) forward the request based on the topmost Route header.

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, the I-CSCF shall:

1) select a S-CSCF according to the method described in 3GPP TS 29.228 [14];

2) insert the URI of the selected S-CSCF as the topmost Route header field value;

3) execute the procedure described in step 2 and 3 in the above paragraph (upon successful user location query, when the response contains the URI of the assigned S-CSCF); and

4) forward the request to the selected S-CSCF.

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network.

Upon an unsuccessful user location query when the response from the HSS indicates that the user is not registered and no services are provided for such a user, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

When the I-CSCF receives an initial request for a dialog or standalone transaction, that contains a single Route header pointing to itself, the I-CSCF shall determine from the entry in the Route header whether it needs to do HSS query or hiding. In case HSS query is needed, then the I-CSCF shall perform the procedures described for the case when there is no Route header present. If the I-CSCF determines that hiding must be performed for an outgoing request, and the I-CSCF shall:

1) remove its own SIP URI from the topmost Route header;

2) perform the procedures described in subclause 5.3.3; and

3) route the request based on the Request-URI header field.

When the I-CSCF receives an initial request for a dialog or standalone transaction containing more than one Route header, the I-CSCF shall:

1) remove its own SIP URI from the topmost Route header;

2) apply the procedures as described in subclause 5.3.3; and

3) forward the request based on the topmost Route header.

NOTE 4: In accordance with SIP the I-CSCF can add its own routeable SIP URI to the top of the Record-Route header to any request, independently of whether it is an initial request, or whether topology hiding is performed. The P-CSCF will ignore any Record-Route header that is not in the initial request of a dialog.

When the I-CSCF receives a response to an initial request (e.g. 183 or 2xx), the I-CSCF shall store the values from the P-Charging-Function-Addresses header, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

*** END OF MODIFICATION ***

3GPP TSG-CT1 Meeting #38 **Tdoc C1-050789**
Cancun, Mexico, 25-29 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **856** ⌘**rev** **2** ⌘ Current version: **6.6.0** ⌘

*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: ⌘	Notification about registration state			
Source: ⌘	Lucent Technologies			
Work item code: ⌘	IMS2		***Date:*** ⌘	15/04/2005
Category: ⌘	**F**		***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:* *Ph2 (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)* *Rel-7 (Release 7)*

Reason for change: ⌘	With respect to shared public user identities, curently the document 24229 does not explicitly state whether the NOTIFY request includes only the public user identities belonging to a single user or to the public user identities belonging to the subscription. Furthermore, if an entity [e.g. P-CSCF, AS] subscribes to the reg-event of shared public user identity, it is not clear which user the subscription pertains to. In addition, the RFC-3680 specifies that if there are no contacts registered for a given address-of-record [aor], i.e. the state of the respective aor is "init", the NOTIFY request would still contain the state attribute within the <registration> element set to "init" for this aor. In IMS the information pertaining to the public user identities [i.e. aors] that have no contacts assigned to them [i.e. state attribute within the <registration> element set to "init"], are not included in the NOTIFY request.
Summary of change: ⌘	Added unambiguous text that specifies that the the public user identities that belong to the subscription will be included in the NOTIFY request. In addition, indicate that in IMS the status of public user identities that have no contacts assigned to them [i.e. state attribute within the <registration> element set to "init"], are not included in the NOTIFY request.
Consequences if not approved: ⌘	The IMS implementations will not interwork.

Clauses affected: ⌘	5.4.2.1.2

		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.

CHANGE

5.4.2.1.2 Notification about registration state

For each NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

4) set the aor attribute within each <registration> element to one public user identity:

    a) set the <uri> sub-element inside each <contact> sub-element of the <registration> element to the contact address provided by the respective UE; and

    b) if the public user identity:

        I) has been deregistered (i.e. no active contact left) then:

        - set the state attribute within the <registration> element to "terminated";

        - set the state attribute within each <contact> element to "terminated"; and

        - set the event attribute within each <contact> element to "deactivated", "expired", "unregistered", "rejected" or "probation" according to RFC 3680 [43].~~; or~~

        If the public user identity has been deregistered and the deregistration has already been indicated in the NOTIFY request, and no new registration has occurred, its <registration> element shall not be included in the subsequent NOTIFY requests; or

        II) has been registered then:

        - set the <unknown-param> element to any additional header parameters contained in the contact header of the REGISTER request according to RFC 3680 [43];

        - set the state attribute within the <registration> element to "active", if not already set to "active", otherwise leave it unchanged; and either:

        - for the contact address to be registered: set the state attribute within the <contact> element to "active"; and set the event attribute within the <contact> element to "registered"; or

        - for the contact address which remain unchanged, if any, leave the <contact> element unmodified; or

        III) has been automatically registered, and have not been previously automatically registered:

        - set the <unknown-param> element to any additional header parameters contained in the contact header of the originsl REGISTER request according to RFC 3680 [43];

        - set the state attribute within the <registration> element to "active";

        - set the state attribute within the <contact> element to "active"; and

        - set the event attribute within the <contact> element to "created"; and

5) set the P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

EXAMPLE: If sip:user1_public1@home1.net is registered, the public user identity sip:user1_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
             version="0" state="full">
  <registration aor="sip:user1_public1@home1.net" id="as9"
                state="active">
    <contact id="76" state="active" event="registered">
           <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
           <unknown-param name="audio"/>
    </contact>
  </registration>
  <registration aor="sip:user1_public2@home1.net" id="as10"
                state="active">
    <contact id="86" state="active" event="created">
           <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
           <unknown-param name="audio"/>
    </contact>
  </registration>
</reginfo>
```

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities have been deregistered or expired), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header to the value of "terminated".

When all UE's contact addresses have been deregistered (i.e.there is no <contact> element set to "active" for this UE), the S-CSCF shall consider subscription to the reg event package belonging to the UE cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

3GPP TSG-CT1 Meeting #38 **Tdoc C1-050790**
Cancun, Mexico, 25-29 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**861**	⌘ **rev**	**3**	⌘ Current version:	**6.6.0** ⌘

*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:	⌘	Registration failure at UE		
Source:	⌘	Lucent Technologies		
Work item code:	⌘	IMS2	***Date:*** ⌘	15/04/2005
Category:	⌘	**F**	***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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change: ⌘ The subclause 5.3.1.3 specifies that if the I-CSCF, upon receiving the REGISTER request that was integrity protected [i.e. it indicates that this is not an initial registration], fail to forward the request to the assigned S-CSCF, it will return the 408 (Request Timeout) response or 504 (Server Time-Out) response. Obviously, if all I-CSCFs have failed then the 504 (Server Time-Out) response was generated by the P-CSCF.

In either case the UE should - the 408 (Request Timeout) response or 504 (Server Time-Out) response - initiate a new initial registration and subscription to reg event to find out what are its valid registrations, and obtain a new Service-Route to the new S-CSCF. If all I-CSCFs have failed then the new initial registration will fail again.

The document 24229 660 does not specify the procedure at the UE when it receives the 408 (Request Timeout) response or 504 (Server Time-Out) response to the REGISTER request.

Summary of change: ⌘ Text added indicating that the UE - upon receiving the 408 (Request Timeout) response or 504 (Server Time-Out) response - may initiate a new initial registration and subscription to reg event to find out what are its valid registrations, and obtain a new Service-Route to the new S-CSCF. In addition, the UE may re-register the public user identities that were registered with the failed S-CSCF.

Consequences if not approved: ⌘ Incomplete specification, i.e., the UE doesn't know how to proceed. It will never be able to register with the new S-CSCF. Since it follows the current procedure, and sends the re-register requests that are integrity protected, each registeration request will be rejected with the error code. It must send the initial unprotected registration to be able to register

		with the new S-CSCF.

Clauses affected:	⌘	5.1.1.4			
		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.

*** CHANGE ***

5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity with its contact address 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 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;

e) a Via header containing the IP address or FQDN of the UE in the sent-by field and the 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 and in the sent-by field in the Via 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].

f) 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 3: 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.

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

h) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the new parameter 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];

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

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

k) the P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3).

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 standalone transactions; 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.

On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) response for a reregistration, the UE shall perform the procedures for initial registration as described in subclause 5.1.1.2.

When the timer F expires at the UE, the UE shall:

1) stop processing of all ongoing dialogs and transactions and silently discard them locally; and

2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2, the UE may:

   a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1;

   b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1; and

c) perform the procedures for initial registration as described in subclause 5.1.1.2.NOTE 4: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

After a maximum of 5 consecutive initial registration attempts, the UE shall not automatically attempt any further initial registration for an implementation dependant time of at least 30 minutes.

3GPP TSG–CT1 Meeting #38
Cancun, Mexico, 25th to 29th April 2005

Tdoc **⌘C1-050791**

CR-Form-v7

CHANGE REQUEST

⌘	**24.229**	**CR**	**899**	⌘ **rev**	**2**	⌘ Current version:	**6.6.0** ⌘

*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:	⌘	Correction of the references for integration of resource management procedures		
Source:	⌘	Orange		
Work item code:	⌘	IMS2	***Date:*** ⌘	25/04/05
Category:	⌘	**F**	***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: ⌘	In TS 24.229, reference is made to subclause 5.1.3.2 in section 5.1.3.1.2 and to subsclause 9.2.5 in section 5.1.3.1.3 whereas these subclauses do not exist.
Summary of change: ⌘	In section 3.1, the terms "resource reservation" are defined. In section 5.1.3.1.2, the reference is corrected from subclause 5.1.3.2 to 5.1.3.1.3. Minor correction in section 5.1.3.1.2. In section 5.1.3.1.3, the reference to 9.2.5 is removed.
Consequences if not approved:	Inconsistent specifications

Clauses affected:	⌘	3.1, 5.1.3.1			
		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 co

*** FIRST MODIFICATION ***

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 still in existence 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.

Integrity protected: See 3GPP TS 33.203 [19]. Where a requirement exists to send information "integrity protected" the mechanisms specified in 3GPP TS 33.203 [19] are used for sending the information. Where a requirements exists to check that information was received "integrity protected", then the information received is checked for compliance with the procedures as specified in 3GPP TS 33.203 [19].

Resource reservation: Mechanism for reserving bearer resources that is required for certain access technologies.

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)
Multimedia Resource Function Controller (MRFC)
Multimedia Resource Function Processor (MRFP)
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] subclauses 3.1, 4.3.3.1, 4.3.6, 4.6 and 5.4.12.1 apply:

Interrogating-CSCF (I-CSCF)
IMS Application Level Gateway (IMS-ALG)
IP-Connectivity Access Network (IP-CAN)
Policy Decision Function (PDF)
Private user identity
Proxy-CSCF (P-CSCF)
Public Service Identity (PSI)
Public user identity
Serving-CSCF (S-CSCF)
Statically pre-configured PSI

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

IM Subscriber Identity Module (ISIM)
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:

Universal Integrated Circuit Card (UICC)
Universal Subscriber Identity Module (USIM)
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

*** END OF MODIFICATION ***

*** SECOND MODIFICATION ***

5.1.3.1 Initial INVITE request

5.1.3.1.1 General

Subclause 5.1.3.1 describe the procedures when the initial INVITE is sent by the originating UE. The default behaviour using the "integration of resource management and SIP" extension (herafter in this subclause known as the SIP precondition mechanism and defined in RFC 3312 [30] as updated by draft-ietf-sip-rfc3312-update [64], and with the request for such a mechanism known as a precondition) is described in subclause 5.1.3.1.2.1. Session without preconditions may be initiated:

- when the remote node does not support the precondition mechanism, as discovered in subclause 5.1.3.1.3; or
- when the specific service does not require the precondition mechanism, as described in subclause 5.1.3.1.4.

Editor's Note: The detailed criteria when to use the non-precondition procedures / resource reservation should be either derived from stage 2 or should be included as a reference to 3GPP TS 23.228.

The UE may indicate that proxies should not fork the INVITE request by including a "no-fork" directive within the Request-Disposition header in the initial INVITE request as described in RFC 3841 [56B].

NOTE 1: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and

2) send a BYE request to this dialog in order to terminate it.

If the UA receives a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

If the UE receives a 488 (Not Acceptable Here) response to an initial INVITE request, the UE should send a new INVITE request containing SDP according to the procedures defined in subclause 6.1.

NOTE 2: An example of where a new request would not be sent is where knowledge exists within the UE, or interaction occurs with the user, such that it is known that the resulting SDP would describe a session that did not meet the user requirements

5.1.3.1.2 "Integration of resource management and SIP" required by originating UE

Upon generating an initial INVITE request using preconditions, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;
- indicate the requirement for the preconditions mechanism and specify it using the Require header mechanism.

When the initial INVITE has been created and forwarded the forthcoming procedures are identical to the procedures described in subclause 5.1.3.1.1.

If the UE receives a 420 (Bad Extension) response to an initial INVITE request with "precondition" option-tag in the Unsupported header field, the UE shall either:

a) abort the session attempt and shall not resend this INVITE request with~~out~~ "precondition" option-tag in the Require header, or

b) try to complete the session by relaxing the requirement on the usage of the precondition mechanism and proceed with the procedures described in subclause 5.1.3.~~2~~1.3 and subclause 6.1.

5.1.3.1.3 "Integration of resource management and SIP" required by originating UE and not supported by terminating UE

This procedure is initiated upon the reception of a 420 (Bad Extension) response to an initial INVITE request, the response containing the "precondition" option-tag in the Unsupported header field value.

The UE may create a new INVITE request addressed to the same destination as initial INVITE. When creating the new INVITE request, the UE shall:

1) populate the From, To, Call-ID headers and the Request-URI as per the initial INVITE request;

2) include the "precondition" option-tag in the Supported header;

3) set each of the media streams in inactive mode in SDP as described in subclause 6.1 in this specification in order to prevent the terminating end to send media whereas the resource reservation is not done at the originating side; and

4) forward the INVITE request as per regular procedures.

Upon receiving a provisional response or final response containing the remote SDP, the UE shall:

1) if required by the regular SIP procedures defined in RFC 3261 [26] and RFC 3262 [27], acknowledge, the SIP response; and

2) initiate the regular resource reservation mechanism~~, as described in subclause 9.2.5~~.

When the above INVITE transaction is successfully completed, and the local resource reservation procedure is complete, the UE shall create and forward a re-INVITE request including:

1) the From, To, Call-ID headers as per a re-INVITE request; and

2) SDP in which the media streams previously set in inactive mode are set to active (sendrecv, sendonly or recvonly) mode, according to the procedures described in subclause 6.1 in this specification.

5.1.3.1.4 "Integration of resource management and SIP" not required by originating UE

This procedure is initiated when the precondition mechanism is not required for a session by the origination UE.

Upon generating the initial INVITE the UE may indicate the support of the precondition mechanism by including the "precondition" option-tag in the Supported header.

When the initial INVITE has been created and forwarded the forthcoming procedures are identical to the procedures described in subclause 5.1.3.1.1.

*** END OF MODIFICATION ***

3GPP TSG-CT1 Meeting #38 **Tdoc C1-050792**
Cancun, Mexico, 25-29 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**902**	⌘**rev**	**2**	⌘	Current version:	**6.6.0** ⌘

*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:	⌘	Clarification on P-CSCF-initiated call release		
Source:	⌘	Nokia		
Work item code:	⌘	IMS2	***Date:*** ⌘	29/04/2005
Category:	⌘	**F**	***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:* *Ph2 (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)* *Rel-7 (Release 7)*

Reason for change:	⌘	Radio coverage loss at a multimedia session of a served user does not mean that all dialogs of the user need to be released.
Summary of change:	⌘	Coverage loss is indicated for multimedia sessions instead of served users. Erroneous note corrected.
Consequences if not approved:	⌘	Incorrect specification

Clauses affected:	⌘	5.2.8.1				
		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.

5.2.8.1 P-CSCF-initiated call release

5.2.8.1.1 Cancellation of a session currently being established

Upon receipt of an indication that radio coverage is no longer available for a ~~served user, for whom one ore more ongoing~~ multimedia session ~~are~~ currently being established (e.g. abort session request from PDF), the P-CSCF shall cancel ~~the related~~that dialog~~s~~ by sending out a CANCEL request according to the procedures described in RFC 3261 [26].

5.2.8.1.2 Release of an existing session

Upon receipt of an indication that the radio interface resources are no longer available for a ~~served user, for whom one or more ongoing~~ session (e.g. abort session request from PDF)~~exists~~, the P-CSCF shall release ~~each of the related~~ that dialog~~s~~ by applying the following steps:

1) if the P-CSCF serves the calling user of ~~a~~ the session it shall generate a BYE request based on the information saved for the related dialog, including:

   - a Request-URI, set to the stored Contact header provided by the called user;
   - a To header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;
   - a From header, set to the From header value as received in the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
   - a Route header, set to the routeing information towards the called user as stored for the dialog;
   - further headers, based on local policy or the requested session release reason.

2) If the P-CSCF serves the called user of ~~a~~ the session it shall generate a BYE request based on the information saved for the related dialog, including:

   - a Request-URI, set to the stored Contact header provided by the calling user;
   - a To header, set to the From header value as received in the initial INVITE request;
   - a From header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;
   - a Route header, set to the routeing information towards the calling user as stored for the dialog;
   - further headers, based on local policy or the requested session release reason.

3) send the so generated BYE request towards the indicated user.

4) upon receipt of the 2xx responses for the BYE request, shall delete all information related to the dialog and the related multimedia session.

5.2.8.1.3 Abnormal cases

Upon receipt of a request on a dialog for which the P-CSCF initiated session release, the P-CSCF shall terminate this received request and answer it with a 481 (Call/Transaction Does Not Exist) response.

5.2.8.1.4 Release of the existing dialogs due to registration expiration and deletion of the security association

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: At the same time, the P-CSCF will also indicate via the ~~Go~~ Gq interface that the session has been terminated~~all resources associated with these dialogs should be released~~.

Cancun, Mexico, 25-29 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**863**	⌘**rev**	**3**	⌘	Current version:	**6.6.0**	⌘

*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:	⌘	Error handling in UE in case of RFC 3524		
Source:	⌘	Ericsson		
Work item code:	⌘	IMS2	***Date:*** ⌘	06/04/2005
Category:	⌘	**F**	***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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	In case the P-CSCF supports RFC 3524, the P-CSCF may require more contexts than the UE can or is willing to use for the session. As the P-CSCF may indicate that particular streams shall be using different PDP contexts (according to RFC 3524), an error case apply if the UE doesn't support as many contects as the P-CSCF requires. In this situation, the UE shall do another offer-answer and remove the media component that the P-CSCF requested on a separate stream.
Summary of change:	⌘	It is specified how the UE shall behave in case the P-CASCF requests more separate streams than the UE supports.
Consequences if not approved:	⌘	The functionality in the UE (in case the P-CSCF requests more PDP contexts than available within the UE) remains unspecified and can cause misoperation.

Clauses affected:	⌘	2, B.2.2.5.1A				
		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.

*** FIRST CHANGE ***

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".

[6] 3GPP TS 23.221: "Architectural requirements".

[7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[8A] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8B] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[9A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".

[10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[11A] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".

[11B] 3GPP TS 29.163: "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks".

[12] 3GPP TS 29.207: "Policy control over Go interface".

[13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[13A] 3GPP TS 29.209: "Policy control over Gq interface".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

[16] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[17] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

[18] 3GPP TS 33.102: "3G Security; Security architecture".

[19] 3GPP TS 33.203: "Access security for IP based services".

[19A] 3GPP TS 33.210: "IP Network Layer Security".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[20A] RFC 2401 (November 1998): "Security Architecture for the Internet Protocol".

[20B] RFC 1594 (March 1994): "FYI on Questions and Answers to Commonly asked "New Internet User" Questions".

[20C] RFC 2403 (November 1998) "The Use of HMAC-MD5-96 within ESP and AH".

[20D] RFC 2404 (November 1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[20E] RFC 2462 (November 1998): "IPv6 Address Autoconfiguration".

[21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 3966 (December 2004): "The tel URI for Telephone Numbers".

[23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 3761 (April 2004): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[25] RFC 2976 (October 2000): "The SIP INFO method".

[25A] RFC 3041 (January 2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[26] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[27] RFC 3262 (June 2002): "Reliability of provisional responses in Session Initiation Protocol (SIP)".

[27A] RFC 3264 (June 2002): "An Offer/Answer Model with Session Description Protocol (SDP)".

[28] RFC 3265 (June 2002): "Session Initiation Protocol (SIP) Specific Event Notification".

[29] RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".

[30] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".

[31] RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".

[32] RFC 3320 (March 2002): "Signaling Compression (SigComp)".

[33] RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[34] RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".

[34A] RFC 3326 (December 2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".

[35] RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method".

[37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag".

[38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[39] draft-ietf-mmusic-sdp-new-13 (May 2003): "SDP: Session Description Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[40] RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[42] RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)".

[43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[51] Void.

[52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[53] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".

[54] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows".

[55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".

[56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[56A] RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[56B] RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)"

[57] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[58] draft-ietf-sip-session-timer-15 (November 2004): "Session Timers in the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[59] RFC 3892 (September 2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".

[60] RFC 3891 (September 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

[61] RFC 3911 (October 2004): "The Session Inititation Protocol (SIP) "Join" Header".

[62] RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

[63] RFC 3861 (August 2004): "Address Resolution for Instant Messaging and Presence".

[64] draft-ietf-sip-rfc3312-update-03 (September 2004): "Update to the Session Initiation Protocol (SIP) Preconditions Framework".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[70] RFC 3903 (October 2004): "An Event State Publication Extension to the Session Initiation Protocol (SIP)".

[71] Void.

[72] RFC 3857 (August 2004): "A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)".

[74] RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[75] draft-ietf-simple-event-list-04 (June 2003): "A Session Initiation Protocol (SIP) Event Notification Extension for Collections".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[77] draft-ietf-sipping-config-framework-05 (October 2004): "A Framework for Session Initiation Protocol User Agent Profile Delivery".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[78] draft-ietf-sipping-conference-package-03 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Conference State"

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[79] draft-ietf-rohc-sigcomp-sip-01 (February 2004): "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

*** SECOND CHANGE ***

B.2.2.5 PDP contexts for media

B.2.2.5.1 General requirements

The UE can establish media streams that belong to different SIP sessions on the same PDP context.

During establishment of a session, the UE establishes data streams(s) for media related to the session. Such data stream(s) may result in activation of additional PDP context(s). Such additional PDP context(s) shall be established as secondary PDP contexts associated to the PDP context used for signalling.

When the UE has to allocate bandwidth for RTP and RTCP in a PDP context, the UE shall use the rules outlined in 3GPP TS 29.208 [13].

B.2.2.5.1A Activation or modification of PDP contexts for media

If the UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), the media stream(s) shall be set up on separate PDP contexts according to the indication of grouping of media streams. The

UE may freely group media streams to PDP context(s) in case no indication of grouping of media streams is received from the P-CSCF.

If the capabilities of the originating UE prevents it from establishment of additional PDP contexts according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the UE will not establish such grouping of media streams. Instead, the originating UE shall negotiate media parameters for the session according to RFC 3264 [27A].

If the capabilities of the terminating UE prevents it from establishment of additional PDP contexts according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the UE will not establish such grouping of media streams. Instead, the terminating UE shall the UE shall handle such SDP offers in accordance with RFC 3388 [53].

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, the UE shall:

- either use existing PDP context(s) where another media authorization token is already in use and no indication of grouping of media streams is required; or
- establish separate PDP context(s) for the media; or
- use an existing PDP context where media authorization token is not in use and no indication of grouping of media streams is required.

When a UE modifies a PDP context to indicate a new media authorization token:

- either as a result of establishment of an additional SIP session; or
- modification of media streams for an ongoing SIP session;

the UE shall include all media authorization tokens and all flow identifiers for all ongoing SIP sessions that use this particular PDP context.

If a media authorization token is received in subsequent messages for the same SIP session, the UE shall:

- use the existing PDP context(s) for media;
- modify the existing PDP context(s) for media; or
- establish additional PDP context(s) for media.

If either background or interactive QoS class is needed for the media, then the UE does not need to use the authorization token even if it receives one. In this case the UE may reuse an existing PDP context and it does not need to request PDP context modification unless it needs to modify the QoS.

If existing PDP context(s) where another media authorization token is already in use is re-used for the media, or separate PDP context(s) is established for the media, the UE shall proceed as follows:

- when a SIP session is terminated, the media authorization token is no longer valid and the UE shall not include it in future GPRS session management messages. The UE shall send a MODIFY PDP CONTEXT REQUEST message updating the binding information by deleting the media authorization token and the corresponding flow identifiers that are no longer valid. If a SIP session is terminated and no other SIP sessions are using the PDP context, the UE shall either update the binding information as described above or deactivate the PDP context;
- the UE shall transparently pass the media authorization token received from the P-CSCF in a response to an INVITE request at originating setup or in the INVITE request at terminating setup to the GGSN. The UE shall signal it by inserting it within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message;
- to identify to the GGSN which flow(s) (identified by m-lines within the SDP) that are transferred within a particular PDP context, the UE shall set the flow identifier(s) within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message. Detailed description of how the flow identifiers are constructed is provided in 3GPP TS 29.207 [12];

- if the UE receives several media authorization tokens from the P-CSCF within the same SIP request or response, the first instance of the media authorization token shall be sent to the GGSN, and subsequent instances are discarded by the UE; and

- the UE shall not include the IM CN Subsystem Signalling Flag when a PDP context for media is established or modified.

The encoding of the media authorization token and the flow identifiers within the Traffic Flow Template IE is described in 3GPP TS 24.008 [8].

3GPP TSG-CT1 Meeting #38
Cancun, Mexico, 25-29 April 2005

Tdoc C1-050794

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229**	**CR**	**787**	⌘**rev**	**6**	⌘	Current version:	**6.6.0**	⌘

*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: ⌘	MT - SDP offer with IPv4 address			
Source: ⌘	Lucent Technologies			
Work item code: ⌘	IMS2		***Date:*** ⌘	15/04/2005
Category: ⌘	**F**		***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:* *Ph2 (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)* *Rel-7 (Release 7)*	

Reason for change: ⌘	The document 24.229 does not specify the handling of an incoming call that originated from a SIP terminal that supports only IPv4 addressing.
Summary of change: ⌘	The added text specifies the routing of an incoming initial INVITE request with SDP offer containing the IPv4 address.
Consequences if not approved: ⌘	Failed incoming calls from SIP terminals that supports only IPv4 addressing.

Clauses affected: ⌘	5.4.4.1, 5.3.2.1, and 6.1				
	Y	**N**			
Other specs affected: ⌘		**X**	Other core specifications	⌘	
		X	Test specifications		
		X	O&M Specifications		
Other comments: ⌘	This is a postponed CR from the CN1#37 meeting in Sydney, Australia. The companion CR, pertaining to MO calls, was accepted.				

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

5.4.4.1 Initial INVITE

When the S-CSCF receives an INVITE request, either from the served user or destined to the served user, the S-CSCF may require the periodic refreshment of the session to avoid hung states in the S-CSCF. If the S-CSCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

When the S-CSCF receives an initial INVITE request destined for the served user, it shall either:

a) examine the SDP offer (the "c=" parameter) to detect if it contains an IP address type that is not supported by the IM CN subsystem; or

b) process the initial INVITE request without examining the SDP.

NOTE 2: If the SDP offer contained an IP address type that is not supported by the IM CN subsystem, the S-CSCF will receive the 488 (Not Acceptable Here) response with 301 Warning header indicating "incompatible network address format".

Subsequently, when the S-CSCF detects that the SDP offer contained an IP address type that is not supported by the IM CN subsystem (i.e., either case a) or b)), the S-CSCF shall either:

- return a 305 (Use Proxy) response to the I-CSCF with the Contact field containing the SIP URI of the IMS-ALG, or

- forward the initial INVITE request to the IMS-ALG. When forwarding the initial INVITE request, the S-CSCF shall not insert its SIP URI into the Record-Route header.

NEXT CHANGE

5.3.2 Initial requests

5.3.2.1 Normal procedures

The I-CSCF may behave as a stateful proxy for initial requests.

The I-CSCF shall verify for all requests whether they arrived from a trusted domain or not. If the request arrived from a non trusted domain, then the I-CSCF shall:

1) respond with 403 (Forbidden) response if the request is a REGISTER request;

2) remove all P-Asserted-Identity headers, all P-Access-Network-Info headers, all P-Charging-Vector headers and all P-Charging-Function-Addresses headers the request may contain, if the request is other than REGISTER request; and

3) continue with the procedures below.

If the request arrived from a trusted domain, the I-CSCF shall perform the procedures below.

NOTE 1: The I-CSCF may find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

When the I-CSCF receives an initial request for a dialog or standalone transaction the I-CSCF shall:

1) if the Request-URI includes a pres: or an im: URI, then translate the pres: or im: URI to a public user identity and replace the Request-URI of the incoming request with that public user identity; and

NOTE 2: SRV records have to be advertised in DNS pointing to the I-CSCF for pres: and im: queries.

2) if the request does not contain a Route header, then start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the called user, indicated in the Request-URI. Prior to performing the user location query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

When the I-CSCF receives an INVITE request, the I-CSCF may require the periodic refreshment of the session to avoid hung states in the I-CSCF. If the I-CSCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer [58] clause 8.

NOTE 3: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

Upon successful user location query, when the response contains the URI of the assigned S-CSCF, the I-CSCF shall:

1) insert the URI received from the HSS as the topmost Route header;

2) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. If no icid parameter was found, then create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

4) forward the request based on the topmost Route header.

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, the I-CSCF shall:

1) select a S-CSCF according to the method described in 3GPP TS 29.228 [14];

2) insert the URI of the selected S-CSCF as the topmost Route header field value;

3) execute the procedure described in step 2 and 3 in the above paragraph (upon successful user location query, when the response contains the URI of the assigned S-CSCF); and

4) forward the request to the selected S-CSCF.

~~When the I-CSCF, upon sending an initial INVITE request to the S-CSCF, receives a 305 (Use Proxy) response from the S-CSCF, it shall forward the initial INVITE request to the SIP URI indicated in the Contact field of the 305 (Use Proxy) response, as specified in RFC3261 [26].~~

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network.

Upon an unsuccessful user location query when the response from the HSS indicates that the user is not registered and no services are provided for such a user, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

When the I-CSCF receives an initial request for a dialog or standalone transaction, that contains a single Route header pointing to itself, the I-CSCF shall determine from the entry in the Route header whether it needs to do HSS query or hiding. In case HSS query is needed, then the I-CSCF shall perform the procedures described for the case when there is no Route header present. If the I-CSCF determines that hiding must be performed for an outgoing request, and the I-CSCF shall:

1) remove its own SIP URI from the topmost Route header;

2) perform the procedures described in subclause 5.3.3; and

3) route the request based on the Request-URI header field.

When the I-CSCF receives an initial request for a dialog or standalone transaction containing more than one Route header, the I-CSCF shall:

1) remove its own SIP URI from the topmost Route header;

2) apply the procedures as described in subclause 5.3.3; and

3) forward the request based on the topmost Route header.

NOTE 4: In accordance with SIP the I-CSCF can add its own routeable SIP URI to the top of the Record-Route header to any request, independently of whether it is an initial request, or whether topology hiding is performed. The P-CSCF will ignore any Record-Route header that is not in the initial request of a dialog.

When the I-CSCF receives a response to an initial request (e.g. 183 or 2xx), the I-CSCF shall store the values from the P-Charging-Function-Addresses header, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

When the I-CSCF, upon sending an initial INVITE request to the S-CSCF, receives a 305 (Use Proxy) response from the S-CSCF, it shall forward the initial INVITE request to the SIP URI indicated in the Contact field of the 305 (Use Proxy) response, as specified in RFC3261 [26].

*****NEXT CHANGE*****

6.1 Procedures at the UE

Usage of SDP by the UE:

1. In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

2. An INVITE request generated by a UE shall contain SDP payload. The SDP payload shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP payload with the most preferred codec listed first.

3. If the SIP request includes a "precondition" option-tag in the Require header (indicating the requirement for "Integration of resource management and SIP" and hereafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30]), the calling user shall indicate the desired QoS for the session, using the segmented status type. In an initial INVITE request the UE shall indicate that it mandates local QoS and that this precondition is not yet satisfied, i.e. the UE shall include the following preconditions:

   a=des: qos mandatory local sendrecv

   a=curr: qos local none

   If the SIP request does not include the "precondition" option-tag in the Require header, the UE shall not indicate that it mandates local QoS. The UE may indicate its desire for optional local QoS, by including the following preconditions:

   a=des:qos optional local sendrecv

   In the case described in subclause 5.1.3.1.3 in the first SDP offer the UE sends, the UE shall set each media stream in inactive mode by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39].

NOTE 1: When setting the media streams in the inactive mode, the UE may include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

4. Providing that the INVITE request received by the UE contains an SDP offer including one or more "m=" media descriptions, and the precondition mechanism is used as described in subclause 5.1.4.1.2, the first 183 (Session

Progress) provisional response that the UE sends, shall contain the answer for the SDP received in the INVITE. The said SDP answer shall reflect the called user's terminal capabilities and user preferences.

In the case described in subclause 5.1.4.1.5 no specific SDP procedures for integration of resource reservation have to be performed.

In the case described in subclause 5.1.4.1.4 in the first SDP answer the UE sends, the UE shall set each media streams in inactive mode by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39].

If the UE is setting one or more media streams in active mode, it shall apply the procedures described in draft-ietf-mmusic-sdp-new [39] with respect to setting the direction of media streams.

5. When the UE sends a 183 (Session Progress) response with SDP payload including one or more "m=" media descriptions, if the precondition mechanism is supported by the calling UE, the called UE shall request confirmation for the result of the resource reservation at the originating end point.

6. During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261[26].

7. For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

   If the media line in the SDP indicates the usage of RTP/RTCP, in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 [56] to specify the required bandwidth allocation for RTCP.

   For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208 [13].

NOTE 2: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifer will typically get the value of zero.

8. The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 2833 [23].

9. The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 [54] and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

10. If an IP-CAN bearer is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 [26] and RFC 3311 [29].

11. If the UE builds SDP for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE may be attempting a session establishment through multiple networks with different policies and potentially may need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

12. When the UE receives an initial INVITE request, that includes the SDP offer containing an IP address type (in the "c=" parameter) that is not supported by the UE, it shall respond with the 488 (Not Acceptable Here) response with 301 Warning header indicating "incompatible network address format".

3GPP TSG-CT1 Meeting #38 **Tdoc C1-050802**
Cancun, Mexico, 25-29 April 2005

CR-Form-v7.1

CHANGE REQUEST

⌘	**TS 24.229**	**CR**	**895**	⌘**rev**	**3**	⌘ Current version:	**6.6.0** ⌘

*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:	⌘	UE registration failure because the selected S-CSCF is unreachable		
Source:	⌘	Orange		
Work item code:	⌘	IMS2	***Date:*** ⌘	25/04/05
Category:	⌘	**F**	***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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change: ⌘ In the current specification for the abnormal case of an unreachable S-CSCF at initial register, it is not considered that there can be a S-CSCF already assigned for the public user identity because this public user identity is shared among multiple UEs.

Summary of change: ⌘ The proposal is the following:

Modification of the procedure at the I-CSCF (section 5.3.1.3) in case of failure of the initial registration because the selected S-CSCF is unreachable, two cases are considered:

- case 1: the I-CSCF has received the list of capabilities from the HSS, the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS.

- case 2: the I-CSCF has received a valid SIP URI from the HSS because the S-CSCF is already assigned to other UEs sharing the same public user identity, it shall request the list of capabilities from the HSS and select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS.

Consequences if not approved: ⌘ The case where the S-CSCF is already assigned for the public user identity because this public user identity is shared among multiple UEs is missing in the I-CSCF procedure when the S-CSCF is unreachable.

Clauses affected:	⌘	5.3.1.3				
		Y	N			
Other specs	⌘		X	Other core specifications	⌘	
Affected:			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.

*** BEGINNING OF THE MODIFICATION ***

5.3 Procedures at the I-CSCF

5.3.1 Registration procedure

5.3.1.1 General

During the registration procedure the I-CSCF shall behave as a stateful proxy.

5.3.1.2 Normal procedures

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

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

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

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

1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;

2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

3) forward the REGISTER request to the indicated S-CSCF.

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

1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more then one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;

2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

4) forward the REGISTER request to the selected S-CSCF.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF.

5.3.1.3 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 403 (Forbidden) response to the UE. The response may include a Warning header containing the warn-code 399.

If the HSS sends a negative response to the user registration status query request, the I-CSCF shall send back a 403 (Forbidden) response. The response may include a Warning header containing the warn-code 399.

If the the user registration status query procedure cannot be completed, e.g. due to time-out or incorrect information from the HSS, the I-CSCF shall send back a 480 (Temporarily Unavailable) response to the UE.

If a selected S-CSCF:

- does not respond to the REGISTER request and its retransmissions by the I-CSCF; or

- sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

and:

- the REGISTER request did not include an "integrity-protected" parameter in the Authorization header; or
- did include an "integrity-protected" parameter with a value different from "yes" in the Authorization header;

then:

- if the I-CSCF has received the list of capabilities from the HSS, the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.
- if the I-CSCF has received a valid SIP URI from the HSS because the S-CSCF is already assigned to other UEs sharing the same public user identity, it will request the list of capabilities from the HSS and, on receiving these capabilities, the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.

If a selected S-CSCF does not respond to a REGISTER request and its retransmissions by the I-CSCF and the REGISTER request did include an Authorization header with the "integrity-protected" parameter set to "yes", the I-CSCF shall send back a 408 (Request Timeout) response or 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26].

If the I-CSCF cannot select a S-CSCF which fulfils the mandatory capabilities indicated by the HSS, the I-CSCF shall send back a 600 (Busy Everywhere) response to the user.

*** END OF THE MODIFICATION ***