

Source: TSG CN WG1
Title: CR to Rel-6 WI "IMS2" for TS 24.229 and TS 24.247
Agenda item: 9.1
Document for: APPROVAL

This document contains 10 **CRs on Rel-6 Work Item "IMS2"**, that have been agreed by TSG CN WG1 CN#37 meeting and forwarded to TSG CN Plenary meeting #27 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Version	WI	Rel
N1-050348	Addition of IMS-ALG to profile tables	24.229	850	1	F	6.5.1	IMS2	Rel-6
N1-050387	MO - Calls to IPv4 SIP terminals	24.229	788	1	F	6.5.1	IMS2	Rel-6
N1-050390	Alignment between TS 22.340 and on TS 24.247 for "is composing"	24.247	7	2	F	6.0.1	IMS2	Rel-6
N1-050391	Clarifications to TS 24.247 subclause 9.3	24.247	9	2	F	6.0.1	IMS2	Rel-6
N1-050395	Press and im URIs in incoming requests	24.229	851	2	C	6.5.1	IMS2	Rel-6
N1-050412	MESSAGE to multiple recipients	24.247	2	3	F	6.0.1	IMS2	Rel-6
N1-050413	Correction to the Registration procedure	24.229	846	2	F	6.5.1	IMS2	Rel-6
N1-050414	Corrections to subclause 5.5 in TS 24.229	24.229	818	3	F	6.5.1	IMS2	Rel-6
N1-050418	Default handling associated with trigger point (all other requests than REGISTER)	24.229	801	3	F	6.5.1	IMS2	Rel-6
N1-050421	Default handling associated with the trigger for third party registration	24.229	803	4	F	6.5.1	IMS2	Rel-6

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 850** ⌘ rev **1** ⌘ Current version: **6.5.1** ⌘

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:	⌘ Addition of IMS-ALG to profile tables		
Source:	⌘ Lucent Technologies		
Work item code:	⌘ IMS2	Date:	⌘ 07/02/2005
Category:	⌘ F	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Use <u>one</u> of the following releases: 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:	⌘ While the IMS-ALG is defined in the main procedures in clause 5, its behaviour is not defined in the profile tables.		
Summary of change:	⌘ IMS-ALG is added to table A.3A, and appropriate entries for the IMS-ALG are added in the user agent tables.		
Consequences if not approved:	⌘ Incomplete documentation.		

Clauses affected:	⌘ A.1.3, A.2.1.2										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications ⌘ Test specifications ⌘ O&M Specifications ⌘	Y	N	⌘	X	⌘	X	⌘	X		
Y	N										
⌘	X										
⌘	X										
⌘	X										
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.1.3 Roles

Table A.2: Roles

Item	Roles	Reference	RFC status	Profile status
1	User agent	[26]	o.1	o.1
2	Proxy	[26]	o.1	o.1
o.1: It is mandatory to support exactly one of these items.				
NOTE: For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.				

Table A.3: Roles specific to this profile

Item	Roles	Reference	RFC status	Profile status
1	UE	5.1	n/a	o.1
2	P-CSCF	5.2	n/a	o.1
3	I-CSCF	5.3	n/a	o.1
3A	I-CSCF (THIG)	5.3	n/a	c1
4	S-CSCF	5.4	n/a	o.1
5	BGCF	5.6	n/a	o.1
6	MGCF	5.5	n/a	o.1
7	AS	5.7	n/a	o.1
7A	AS acting as terminating UA, or redirect server	5.7.2	n/a	c2
7B	AS acting as originating UA	5.7.3	n/a	c2
7C	AS acting as a SIP proxy	5.7.4	n/a	c2
7D	AS performing 3rd party call control	5.7.5	n/a	c2
8	MRFC	5.8	n/a	o.1
9	IMS-ALG	5.9	n/a	o.1
c1: IF A.3/3 THEN o ELSE x - - I-CSCF.				
c2: IF A.3/7 THEN o.2 ELSE n/a - - AS.				
o.1: It is mandatory to support exactly one of these items.				
o.2: It is mandatory to support at least one of these items.				
NOTE: For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.				

Table A.3A: Roles specific to additional capabilities

Item	Roles	Reference	RFC status	Profile status
1	Presence server	3GPP TS 24.141 [8A]	n/a	c1
2	Presence user agent	3GPP TS 24.141 [8A]	n/a	c2
3	Resource list server	3GPP TS 24.141 [8A]	n/a	c3
4	Watcher	3GPP TS 24.141 [8A]	n/a	c4
11	Conference focus	3GPP TS 24.147 [8B]	n/a	c5
12	Conference participant	3GPP TS 24.147 [8B]	n/a	c6
c1:	IF A.3/7A AND A.3/7B THEN o ELSE n/a - - AS acting as terminating UA, or redirect server and AS acting as originating UA.			
c2:	IF A.3/1 THEN o ELSE n/a - - UE.			
c3:	IF A.3/7A THEN o ELSE n/a - - AS acting as terminating UA, or redirect server.			
c4:	IF A.3/1 OR A.3/7B THEN o ELSE IF A.3/9 THEN m ELSE n/a - - UE or AS acting as originating UA.			
c5:	IF A.3/7D AND A.3/4 AND A.3/8 THEN o ELSE n/a - - AS performing 3rd party call control and S-CSCF and MRFC (note 2).			
c6:	IF A.3/1 OR A.3A/11 THEN o ELSE IF A.3/9 THEN m ELSE n/a - - UE or conference focus.			
NOTE 1:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			
NOTE 2:	The functional split between the MRFC and the conferencing AS is out of scope of this document and they are assumed to be collocated.			

A.2 Profile definition for the Session Initiation Protocol as used in the present document

A.2.1 User agent role

A.2.1.1 Introduction

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for UA implementations:

Prerequisite: A.2/1 - - user agent role.

A.2.1.2 Major capabilities

Table A.4: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
1	client behaviour for registration?	[26] subclause 10.2	o	c3
2	registrar?	[26] subclause 10.3	o	c4
2A	registration of multiple contacts for a single address of record	[26] 10.2.1.2, 16.6	o	o
2B	initiating a session?	[26] subclause 13	o	o
3	client behaviour for INVITE requests?	[26] subclause 13.2	c18	c18
4	server behaviour for INVITE requests?	[26] subclause 13.3	c18	c18
5	session release?	[26] subclause 15.1	c18	c18
6	timestamping of requests?	[26] subclause 8.2.6.1	o	o
7	authentication between UA and UA?	[26] subclause 22.2	c34	c34
8	authentication between UA and registrar?	[26] subclause 22.2	o	n/a
8A	authentication between UA and proxy?	[26] 20.28, 22.3	o	o
9	server handling of merged requests due to forking?	[26] 8.2.2.2	m	m
10	client handling of multiple responses due to forking?	[26] 13.2.2.4	m	m
11	insertion of date in requests and responses?	[26] subclause 20.17	o	o
12	downloading of alerting information?	[26] subclause 20.4	o	o
	Extensions			
13	the SIP INFO method?	[25]	o	n/a
14	reliability of provisional responses in SIP?	[27]	c19	c18
15	the REFER method?	[36]	o	c33
16	integration of resource management and SIP?	[30]	c19	c18
17	the SIP UPDATE method?	[29]	c5	c18
19	SIP extensions for media authorization?	[31]	o	c14
20	SIP specific event notification?	[28]	o	c13
21	the use of NOTIFY to establish a dialog?	[28] 4.2	o	n/a
22	acting as the notifier of event information?	[28]	c2	c15
23	acting as the subscriber to event information?	[28]	c2	c16
24	session initiation protocol extension header field for registering non-adjacent contacts?	[35]	o	c6
25	private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks?	[34]	o	m
26	a privacy mechanism for the Session Initiation Protocol (SIP)?	[33]	o	m
26A	request of privacy by the inclusion of a Privacy header indicating any privacy option?	[33]	c9	c11
26B	application of privacy based on the received Privacy header?	[33]	c9	n/a
26C	passing on of the Privacy header transparently?	[33]	c9	c12
26D	application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured?	[33] 5.1	c10	c27
26E	application of the privacy option "session" such that anonymization for	[33] 5.2	c10	c27

	the session(s) initiated by this message occurs?			
26F	application of the privacy option "user" such that user level privacy functions are provided by the network?	[33] 5.3	c10	c27
26G	application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?	[34] 7	c10	n/a
27	a messaging mechanism for the Session Initiation Protocol (SIP)?	[50]	o	c7
28	session initiation protocol extension header field for service route discovery during registration?	[38]	o	c17
29	compressing the session initiation protocol?	[55]	o	c8
30	private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?	[52]	o	m
31	the P-Associated-URI header extension?	[52] 4.1	c21	c22
32	the P-Called-Party-ID header extension?	[52] 4.2	c21	c23
33	the P-Visited-Network-ID header extension?	[52] 4.3	c21	c24
34	the P-Access-Network-Info header extension?	[52] 4.4	c21	c25
35	the P-Charging-Function-Addresses header extension?	[52] 4.5	c21	c26
36	the P-Charging-Vector header extension?	[52] 4.6	c21	c26
37	security mechanism agreement for the session initiation protocol?	[48]	o	c20
38	the Reason header field for the session initiation protocol?	[34A]	o	o (note 1)
39	an extension to the session initiation protocol for symmetric response routing?	[56A]	o	x
40	caller preferences for the session initiation protocol?	[56B]	C29	c29
40A	the proxy-directive within caller-preferences?	[56B] 9.1	o.5	o.5
40B	the cancel-directive within caller-preferences?	[56B] 9.1	o.5	o.5
40C	the fork-directive within caller-preferences?	[56B] 9.1	o.5	c28
40D	the recurse-directive within caller-preferences?	[56B] 9.1	o.5	o.5
40E	the parallel-directive within caller-preferences?	[56B] 9.1	o.5	c28
40F	the queue-directive within caller-preferences?	[56B] 9.1	o.5	o.5
41	an event state publication extension to the session initiation protocol?	[70]	o	c30
42	SIP session timer?	[58]	c19	c19
43	the SIP Referred-By mechanism?	[59]	o	c33
44	the Session Initiation Protocol (SIP) "Replaces" header?	[60]	c19	c19 (note 1)
45	the Session Initiation Protocol (SIP) "Join" header?	[61]	c19	c19 (note 1)
46	the callee capabilities?	[62]	o	c35

c2:	IF A.4/20 THEN o.1 ELSE n/a - - SIP specific event notification extension.
c3:	IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UE or S-CSCF functional entity.
c4:	IF A.3/4 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - S-CSCF or AS functional entity.
c5:	IF A.4/16 THEN m ELSE o - - integration of resource management and SIP extension.
c6:	IF A.3/4 OR A.3/1 THEN m ELSE n/a. - - S-CSCF or UE.
c7:	IF A.3/1 OR A.3/4 OR A.3/7A OR A.3/7B OR A.3/7D <u>OR A.3/9</u> THEN m ELSE n/a - - UA or S-CSCF or AS acting as terminating UA or AS acting as originating UA or AS performing 3 rd party call control <u>or IMS-ALG</u> .
c8:	IF A.3/1 THEN m ELSE n/a - - UE behaviour.
c9:	IF A.4/26 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10:	IF A.4/26B THEN o.3 ELSE n/a - - application of privacy based on the received Privacy header.
c11:	IF A.3/1 OR A.3/6 THEN o <u>ELSE IF A.3/9 THEN m</u> ELSE n/a - - UE or MGCF, <u>IMS-ALG</u> .
c12:	IF A.3/7D THEN m ELSE n/a - - AS performing 3rd-party call control.
c13:	IF A.3/1 OR A.3/2 OR A.3/4 <u>OR A.3/9</u> THEN m ELSE o - - UE behaviour or S-CSCF <u>or IMS-ALG</u> .
c14:	IF A.3/1 THEN m ELSE IF A.3/2 THEN o ELSE n/a - UE or P-CSCF.
c15:	IF A.4/20 and <u>AND</u> (A.3/4 <u>OR A.3/9</u>) THEN m ELSE o - SIP specific event notification extensions and S-CSCF, <u>IMS-ALG</u> .
c16:	IF A.4/20 and <u>AND</u> (A.3/1 OR A.3/2 <u>OR A.3/9</u>) THEN m ELSE o - - SIP specific event notification extension and UE or P-CSCF <u>or IMS-ALG</u> .
c17:	IF A.3/1 or A.3/4 THEN m ELSE n/a - - UE or S-CSCF.
c18:	IF A.4/2B THEN m ELSE n/a - - initiating sessions.
c19:	IF A.4/2B THEN o ELSE n/a - - initiating sessions.
c20:	IF A.3/1 THEN m ELSE n/a - - UE behaviour.
c21:	IF A.4/30 THEN o.4 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).
c22:	IF A.4/30 AND (A.3/1 OR A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF or UA.
c23:	IF A.4/30 AND A.3/1 THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE.
c24:	IF A.4/30 AND A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF.
c25:	IF A.4/30 AND (A.3/1 OR A.3/4 OR A.3/7A OR A.3/7D <u>OR A.3/9</u>) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE, S-CSCF or AS acting as terminating UA or AS acting as third-party call controller, <u>IMS-ALG</u> .
c26:	IF A.4/30 AND (A.3/6 OR A.3/7A OR A.3/7B or A.3/7D) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and MGCF, AS acting as a terminating UA, or AS acting as an originating UA, or AS acting as third-party call controller.
c27:	IF A.3/7D THEN o ELSE x - - AS performing 3rd party call control.
c28:	IF A.3/1 THEN m ELSE o.5 - - UE.
c29:	IF A.4/40A OR A.4/40B OR A.4/40C OR A.4/40D OR A.4/40E OR A.4/40F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.
c30:	IF A.3A/1 OR A.3A/2 THEN m ELSE IF A.3/1 THEN o ELSE n/a - - presence server, presence user agent, UE, AS.
c33:	IF A.3/11 OR A.3/12 <u>OR A.3/9</u> OR A.4/44 THEN m ELSE o - - conference focus or conference participant <u>or IMS-ALG</u> or the Session Initiation Protocol (SIP) "Replaces" header.
c34:	IF A.4/44 OR A.4/45 <u>OR A.3/9</u> THEN m ELSE n/a - - the Session Initiation Protocol (SIP) "Replaces" header or the Session Initiation Protocol (SIP) "Join" header <u>or IMS-ALG</u> .
c35:	IF A.3/4 <u>OR A.3/9</u> THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7 OR A.3/8) THEN o ELSE n/a - - <u>S-CSCF or IMS-ALG functional entities, UE, or MGCF, or AS, or MRFC or S-CSCF</u> functional entity.
o.1:	At least one of these capabilities is supported.
o.2:	At least one of these capabilities is supported.
o.3:	At least one of these capabilities is supported.
o.4:	At least one of these capabilities is supported.
o.5:	At least one of these capabilities is supported.
NOTE 1:	At the MGCF, the interworking specifications do not support a handling of the header associated with this extension.

Prerequisite A.5/20 - - SIP specific event notification

Table A.4A: Supported event packages

Item	Does the implementation support	Subscriber			Notifier		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	reg event package?	[43]	c1	c3	[43]	c2	c4
2	refer package?	[36] 3	c13	c13	[36] 3	c13	c13
3	presence package?	[74] 6	c1	c5	[74] 6	c2	c6
4	eventlist with underlying presence package?	[75], [74] 6	c1	c7	[75], [74] 6	c2	c8
5	presence.wininfo template-package?	[72] 4	c1	c9	[72] 4	c2	c10
6	xcap-change package?	[77] 2	c1	c11	[77] 2	c2	c12
7	conference package?	[78] 3	c1	c21	[78] 3	c1	c22
c1:	IF A.4/23 THEN o ELSE n/a - - acting as the subscriber to event information.						
c2:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.						
c3:	IF A.3/1 OR A.3/2 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - UE, P-CSCF, AS.						
c4:	IF A.3/4 THEN m ELSE n/a - - S-CSCF.						
c5:	IF A.3A/3 OR A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - resource list server or watcher, acting as the subscriber to event information.						
c6:	IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - watcher, acting as the notifier of event information.						
c7:	IF A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - watcher, acting as the subscriber to event information.						
c8:	IF A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - resource list server, acting as the notifier of event information.						
c9:	IF A.3A/1 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent, acting as the subscriber to event information.						
c10:	IF A.3A/2 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.						
c11:	IF A.3A/2 OR A.3A/4 THEN o ELSE IF A.4/23 THEN o ELSE n/a - - watcher or presence user agent, acting as the subscriber to event information.						
c12:	IF A.3A/1 OR A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server or resource list server, acting as the notifier of event information.						
c13:	IF A.4/15 THEN m ELSE n/a - - the REFER method.						
c21:	IF A.3A/12 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - conference participant or acting as the subscriber to event information.						
c22:	IF A.3A/11 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - conference focus or acting as the notifier of event information.						

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR 788** ⌘ rev **1** ⌘ Current version: **6.5.1** ⌘

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:	⌘ MO - Calls to IPv4 SIP terminals				
Source:	⌘ Lucent Technologies				
Work item code:	⌘ IMS2	Date:	⌘ 01/02/2005		
Category:	⌘ F	Release:	⌘ Rel-6		
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:		
	F (correction)		Ph2 (GSM Phase 2)		
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)		
	B (addition of feature),		R97 (Release 1997)		
	C (functional modification of feature)		R98 (Release 1998)		
	D (editorial modification)		R99 (Release 1999)		
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)		
			Rel-5 (Release 5)		
			Rel-6 (Release 6)		
			Rel-7 (Release 7)		

Reason for change:	⌘ The document 24.224 does not specify the handling of outing calls that have been offered to the SIP terminals that supports only IPv4 addressing. [For detail discussion see the companion contribution N1-050072].				
Summary of change:	⌘ The added text specifies the re-routing of the [UE originated] initial INVITE request [by the S-CSCF] to the IMS-ALG.				
Consequences if not approved:	⌘ Failed outgoing calls to SIP terminals that supports only IPv4 addressing				

Clauses affected:	⌘ 5.4.3.2								
Other specs affected:	⌘	<table border="1" style="border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="text-align: center; padding: 2px;"><input type="checkbox"/></td> <td style="text-align: center; padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘	
Y	N								
<input type="checkbox"/>	<input checked="" type="checkbox"/>								
		<table border="1" style="border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="text-align: center; padding: 2px;"><input type="checkbox"/></td> <td style="text-align: center; padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Test specifications		
Y	N								
<input type="checkbox"/>	<input checked="" type="checkbox"/>								
		<table border="1" style="border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="text-align: center; padding: 2px;"><input type="checkbox"/></td> <td style="text-align: center; padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	O&M Specifications		
Y	N								
<input type="checkbox"/>	<input checked="" type="checkbox"/>								
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.

5.4.3.2 Requests initiated by the served user

When the S-CSCF receives from the served user or from a PSI an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

Editor's Note: It needs to be stated, that the S-CSCF will only perform the following steps if the request was received from a trusted entity, e.g. an entity within the trust domain.

- 1) determine whether the request contains a barred public user identity in the P-Asserted-Identity header field of the request or not. In case the said header field contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. The response may include a Warning header containing the warn-code 399. Otherwise, continue with the rest of the steps;

NOTE 1: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

- 2) remove its own SIP URI from the topmost Route header;
- 3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request;
- 4) check whether the initial request matches the next unexecuted initial filter criteria based on a public user identity in the P-Asserted-Identity header in the priority order as described in 3GPP TS 23.218 [5], and if it does, the S-CSCF shall:
 - a) insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4; and
 - b) if the AS is located outside the trust domain then the S-CSCF shall remove the P-Access-Network-Info header field and its values in the request; if the AS is located within the trust domain, then the S-CSCF shall retain the P-Access-Network-Info header field and its values in the request that is forwarded to the AS;

NOTE 2: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request URI.

- 5) if there is no original dialog identifier present in the topmost Route header of the incoming request 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. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;
- 6) if there is no original dialog identifier present in the topmost Route header of the incoming request insert an orig-ioi parameter into the P-Charging-Vector header. The S-CSCF shall set the orig-ioi parameter to a value that identifies the sending network. The S-CSCF shall not include the term-ioi parameter;
- 7) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;
- 8) if there is no original dialog identifier present in the topmost Route header of the incoming request and if the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;
- 9) if the request is not forwarded to an AS and if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see draft-ietf-iptel-rfc2806bis [22]) to a globally routeable SIP URI using an ENUM/DNS translation mechanism with the format specified in RFC 3761 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. If the outgoing Request-URI is a pres URI or an im URI, the S-CSCF shall forward the request as specified in RFC 3861 [63]. In this case, the S-CSCF shall not modify the received Request-URI;

10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. If the destination address is of an IP address type other than the IP address type used in the IM CN subsystem, then the S-CSCF shall forward the request to the IMS-ALG if the IM CN subsystem supports interworking to networks with different IP address type;

11) if network hiding is needed due to local policy, put the address of the I-CSCF (THIG) to the topmost route header;

12) in case of an initial request for a dialog originated from a served user, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or
- if the request is routed elsewhere, create a Record-Route header containing its own SIP URI;

NOTE 3: For requests originated from a PSI the S-CSCF can decide whether to record-route or not.

Editor's Note: It needs to be clarified how the S-CSCF decides whether to put its address into the Record-Route header in the case of handling a request that originates from a PSI. It might be part of the operators policy.

13) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header prior to forwarding the message;

14) route the request based on SIP routing procedures; and

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

When the S-CSCF receives any response to the above request, the S-CSCF may:

- 1) apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header; and
- 2) apply the same privacy mechanism to the P-Access-Network-Info header, if present.

NOTE 4: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 5: The optional procedures above are in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

When the S-CSCF receives any response to the above request containing a term-ioi parameter, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message. The term-ioi parameter and the orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

When the S-CSCF, upon sending an initial INVITE request that includes an IPv6 address in the SDP offer (in "c=" parameter), receives an error response indicating that the IP address type used in the IM CN subsystem is not supported. (e.g., the S-CSCF receives the 488 (Not Acceptable Here) with 301 Warning header indicating "incompatible network address format"), the S-CSCF shall either:

- fork the initial INVITE request to the IMS-ALG; or
- process the error response and forward it using the Via header.

When the S-CSCF receives from the served user a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- 1) remove its own URI from the topmost Route header;
- 2) create a Record-Route header containing its own SIP URI;

- 3) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;
- 4) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header;
- 5) in case the request is routed towards the destination user (Request-URI) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header; and
- 6) route the request based on the topmost Route header.

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

When the S-CSCF receives from the served user a subsequent request other than a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- 1) remove its own URI from the topmost Route header;
- 2) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and
- 3) in case the request is routed towards the destination user (Request-URI) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header; and
- 4) route the request based on the topmost Route header.

5.4.3.3 Requests terminated at the served user

CR-Form-v7.1

CHANGE REQUEST

⌘ **TS 24.247** **CR** **7** ⌘ **rev** **2** ⌘ Current version: **6.0.1** ⌘

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:	⌘ Alignment between TS 22.340 and on TS 24.247 for "is composing"		
Source:	⌘ LM Ericsson		
Work item code:	⌘ IMS2	Date:	⌘ 02/02/2005
Category:	⌘ F	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Use <u>one</u> of the following releases: 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:	⌘ TS 22.340 subclause 7.1 states that it shall be possible for a subscriber in an IMS Messaging session to request and to receive an indication of when user is entering a message ("Is typing").		
Summary of change:	⌘ A reference to RFC 3994 is added in subclause 2. A new term isComposing information is added to subclause 3. Text is added to subclause 5.3 to define how isComposing status message is transported for Immediate messaging. Text is added to subclause 8.3 to show how the isComposing capability is indicated in SDP. Text is added to subclause 9.3 to define how h isComposing status message is transported for session based messaging.		
Consequences if not approved:	⌘ The stage 1 requirement will not be fulfilled, and a commonly used messaging feature will not be supported.		

Clauses affected:	⌘ Subclauses 2, 3, 5.3, 8.3, 9.3 are affected.										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	⌘	X	⌘	X	⌘	X	Other core specifications Test specifications O&M Specifications	⌘
Y	N										
⌘	X										
⌘	X										
⌘	X										
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: "3G Vocabulary".
- [2] 3GPP TS 22.228: "Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1".
- [3] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model; Stage 2".
- [4] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".
- [5] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".
- [6] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".
- [7] RFC 3261 (March 2002): "SIP: Session Initiation Protocol".
- [8] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".
- [9] draft-ietf-simple-message-sessions-096.txt (~~October~~ ~~May~~ 2004): "The Message Session Relay Protocol".

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

- [10] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".
- [11] 3GPP TS 22.340: "IP Multimedia System (IMS) messaging; Stage 1".
- [12] [RFC 3994 \(January 2005\): "Indication of Message Composition for Instant Messaging"](#).

|

NEXT CHANGE

3 Definitions, symbols and abbreviations

3.1 Definitions

IsComposing information [This is a term used to indicate that an indication is sent to the communicating user when a user in entering a new message.](#)

For the purposes of the present document, the following terms and definitions given in TS 22.340 [11] apply:

Immediate messaging

Session based messaging

Session based messaging conferences

For the purposes of the present document, the [following] terms and definitions given in draft-ietf-simple-message-sessions [9] apply:

Host

Page-mode messaging

Session inactivity timer

Session-mode messaging

Session-mode messaging conferences

Visitor

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.147 [10] apply:

Conferencing Application Server

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AS	Application Server
CN	Core Network
DM	Data manipulator
DMS	Data manipulation server
IM	IP Multimedia
IMS	IP Multimedia CN subsystem
IP	Internet Protocol
MRFC	Media Resource Function Controllers
MRFP	Media Resource Function Processors
MSRP	Message Session Relay Protocol
SBLP	Service Based Local Policy
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UE	User Equipment
URL	Uniform Resource Locator

NEXT CHANGE

5.3.1 Participant

5.3.1.1 General

For the purpose of page-mode messaging a participant will send a page-mode message using a SIP MESSAGE request as defined in RFC 3428 [8] to another participant.

5.3.1.2 Sending of an immediate message

When sending a page-mode message to another participant, the participant shall construct and send a MESSAGE request in accordance with RFC 3428 [8] and subclause 5.1.2A.1 of 3GPP TS 24.229 [5].

The participant may include in a MESSAGE request an isComposing status message as defined in RFC 3994 [12].

The participant shall stop transmitting isComposing status messages if the participant receives a 415 (Unsupported Media Type) status code in a response to a MESSAGE request containing the status indication.

5.3.1.3 Receiving an immediate message

Upon receipt of a MESSAGE request, the participant shall perform the procedures as described in RFC 3428 [8] and subclause 5.1.2A.2 of 3GPP TS 24.229 [5].

NOTE: A MESSAGE request can be used for applications other than immediate messaging (e.g. 3GPP TS 23.228 [6] subclause 5.4.9), and the handling of received MESSAGE requests for such applications is outside the scope of this specification.

NEXT CHANGE

8.3 Role

8.3.1 SDP offerer

When an SDP offerer wants to create a session mode messaging session, the SDP offerer shall populate the SDP as specified in subclause 6.1 in TS 24.229[5]. SDP offerer shall also include:

- a) a media attribute in accordance with draft-ietf-simple-message-sessions [9]; and
- b) the supported MIME types in the accept-types or accept-wrapped-types attributes in accordance with draft-ietf-simple-message-sessions [9]; and
- c) the address of the SDP offerer in the path attribute, in accordance with draft-ietf-simple-message-sessions [9].

The SDP may also include a max-size attribute. The attribute shall be formatted in accordance with draft-ietf-simple-message-sessions [9]

The SDP offerer may want to indicate to the other user(s), that the SDP offerer is prepared to receive isComposing information, then it shall add the MIME type "application/im-iscomposing+xml to the accept type or access-wrapped types attributes.

At the receipt of the SDP answer the SDP offerer shall set up a TCP connection (if not already available) when an IP-CAN bearer with sufficient QoS is available.

8.3.2 SDP answerer

When receiving an SDP offer the SDP answerer shall populate the SDP answer as specified in subclause 6.1 in TS 24.229[5]. In addition the answerer shall include:

- a) a media attribute in accordance with the received media attribute in the SDP offer; and
- b) the supported MIME types in the accept-types or accept-wrapped-types attributes in accordance with draft-ietf-simple-message-sessions [9]; and
- c) the MSRP URI of the SDP answerer in the path attribute in accordance with draft-ietf-simple-message-sessions [9].

The SDP may also include a max-size attribute. The attribute shall be formatted in accordance with draft-ietf-simple-message-sessions [9].

If SDP answerer receives the MIME type “application/im-iscomposing+xml” in the accept-types or accept-wrapped-types attribute and the SDP answerer accepts the exchange of isComposing information the SDP answerer shall add the MIME type “application/im-iscomposing+xml” to the accept-types or access-wrapped types attributes.

8.3.3 Intermediate node

8.3.3.1 Intermediate node Originating case

8.3.3.1.1 Sending of a SDP offer

The intermediate node shall create a SDP offer, which shall include:

- a) a media attribute in accordance with the media attribute received in the received in the SDP offer.; and
- b) the supported MIME types in the accept-types or accept-wrapped-types attributes as provisioned in the intermediate node. The attribute shall be formatted in accordance with draft-ietf-simple-message-sessions [9]; and
- c) a MSRP URI of the Intermediate node in the path attribute to be used when the SDP answerer wants to send a MSRP message to the conference. The attribute shall be formatted in accordance with draft-ietf-simple-message-sessions [9].
- d) the MIME type “application/ im-iscomposing+xml to the accept type or access-wrapped types attributes if it is received from the SDP answerer.

The SDP may also include a max-size attribute. The attribute shall be formatted in accordance with draft-ietf-simple-message-sessions [9].

At the receipt of the SDP answer the Intermediate node shall set up a TCP connection (if not already available) when an IP-CAN bearer with sufficient QoS is available.

8.3.3.2 Intermediate node Terminating case

8.3.3.2.1 Sending of a SDP answer

The intermediate node shall at the receipt of a SDP offer create a SDP answer. The SDP answer shall include:

- a) a media attribute in accordance with the received media attribute in the SDP offer; and
- b) the supported MIME types in the accept-types or accept-wrapped-types attributes in accordance with draft-ietf-simple-message-sessions [9]; and

c) a MSRP URI in the path attribute to be used when the SDP answerer shall send a MSRP message to the conference,. The attribute shall be formatted in accordance with draft-ietf-simple-message-sessions [9].

d) [the MIME type “application/ im-iscomposing+xml to the accept type or access-wrapped types attributes if it is received from the SDP offerer..](#)

The SDP may also include a max-size attribute. The attribute shall be formatted in accordance with draft-ietf-simple-message-sessions [9].

NEXT CHANGE

9.3 Role

9.3.1 MSRP sender

9.3.1.1 MSRP sender sends a message

When a MSRP sender wishes to send a message, the MSRP sender shall ensure that the message length is not longer than the max-size attribute, as received in a SDP offer or a SDP answer. Depending on the message length the message may be included in one SEND request or chunked into a number of SEND requests. The MSRP sender shall follow the procedures and rules as specified in draft-ietf-simple-message-sessions [9], when the MSRP sender fragments a message into a number SEND requests.

The MSRP sender shall create a SEND request in accordance with draft-ietf-simple-message-sessions [9], where the value of To-Path is the MSRP URI shall be set to value of path attribute received in a SDP offer or a SDP answer.

[If it is possible to exchange isComposing information, the MSRP sender may include in a SEND request an isComposing status message as defined in RFC 3994 \[12\].](#)

9.3.2 MSRP receiver

When a MSRP receiver receives a SEND request, the MSRP receiver shall parse the SEND request. The MSRP receiver shall either send a response including:

- a) a 200 (OK) status-code , as specified in draft-ietf-simple-message-sessions [9], for the concerned SEND message if the parsing was successful; or
- b) an appropriate status-code, as specified in draft-ietf-simple-message-sessions [9], for the concerned SEND message if the parsing was unsuccessful.

The MSRP receiver shall send a REPORT request if this is explicit or implicit requested in the SEND request(s) belonging to the message. It shall either be:

- a) a successful REPORT request including status-code 200 (OK) if a complete message is received and the Report-Success header in the SEND request was set to “yes”; or
- b) an unsuccessful REPORT request including status-code other than 200 (OK) as defined in draft-ietf-simple-message-sessions [9] if the MSRP receiver can conclude that a complete message is not received and the Report-Failure header is set to “yes” or not included. The criteria to conclude that a complete message is not received are specified in draft-ietf-simple-message-sessions [9].

9.3.3 Intermediate node

9.3.3.1 Intermediate node terminating case

When an intermediate node receives a SEND request, the intermediate node shall:

- 1) parse the SEND request and either send a response including:

- a) a 200 (OK) status-code, as specified in draft-ietf-simple-message-sessions [9], for the concerned SEND message, if the parsing was successful; or
 - b) an appropriate status-code, as specified in draft-ietf-simple-message-sessions [9], for the concerned SEND message if the parsing was unsuccessful.; and
- 2) determine that a complete message has been received. The following actions in this subclause shall only be performed if a complete message is received.

The MSRP receiver shall send a REPORT request if this is explicit or implicit requested in the SEND request(s) associated to the same message. It shall either be:

- a) a successful REPORT request including status-code 200 (OK) if the intermediate node concludes that all available users on the distribution list has received the complete message or a concerned user has received the complete message and the Report-Success header in the SEND request was set to “yes”; or
- b) an unsuccessful REPORT request including status-code other than 200 (OK) as defined in draft-ietf-simple-message-sessions [9] if the intermediate node conclude that a complete message has not been received or that a complete message has not been able to be delivered to all available users on the distribution list or to a particular member of the distribution list.

9.3.3.2 Intermediate node originating case

When an intermediate node wishes to send a message, the intermediate shall ensure that the message length is not longer than the max-size attribute, as received in a SDP offer or a SDP answer. Depending on the message length the message may be included in one SEND request or chunked into a number of SEND requests. The intermediate shall follow the procedures and rules as specified in draft-ietf-simple-message-sessions [9], when the intermediate node fragments a message into a number SEND requests.

The intermediate shall create a SEND request in accordance with draft-ietf-simple-message-sessions [9] with the following clarifications:

- 1) set the Report-Success header as received in the SEND request;
- 2) set the Report-Failure header as received in the SEND request; and
- 3) depending on the received MSRP URI
 - a) either send the SEND request to all available user of the conference; or
 - b) send the SEND request to one MSRP receiver.

CR-Form-v7.1

CHANGE REQUEST

⌘ **TS 24.247 CR 9** ⌘ rev **2** ⌘ Current version: **6.0.1** ⌘

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:	⌘ Clarifications to TS 24.247 subclause 9.3		
Source:	⌘ LM Ericsson		
Work item code:	⌘ IMS2	Date:	⌘ 02/02/2005
Category:	⌘ F	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Use <u>one</u> of the following releases: 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:	⌘ Since it is likely that the TCP connections used between the entities are used for several MSRP sessions interruptable SEND requests shall be used for messages longer than 2048 octets. In a 3GPP network it must be possible for the UE to know the message length and therefore they shall also indicate it the SEND request.
Summary of change:	⌘ Clarifications have been added to how MSRP sender and an intermediate node shall code the range end field and total length field.
Consequences if not approved:	⌘ Different interpretation and option may lead to interoperability problem and unnecessary complex implementation

Clauses affected:	⌘ Subclauses 9.3.1.1 and 9.3.3.2						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
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.

9.3.1 MSRP sender

9.3.1.1 MSRP sender sends a message

When a MSRP sender wishes to send a message, the MSRP sender shall ensure that the message length is not longer than the max-size attribute, as received in a SDP offer or a SDP answer. Depending on the message length the message may be included in one SEND request or chunked into a number of SEND requests. The MSRP sender shall follow the procedures and rules as specified in draft-ietf-simple-message-sessions [9], when the MSRP sender fragments a message into a number SEND requests.

The SEND request shall include the Byte-Range header. The MSRP sender shall populate the Byte-Range header fields as follows:

- the range end set to * (interruptable), to make the chunks interruptable, if the SEND request is longer than 2048 octets; and
- the total field set to the total size of the message.

The MSRP sender shall create a SEND request in accordance with draft-ietf-simple-message-sessions [9], where the value of To-Path is the MSRP URI shall be set to value of path attribute received in a SDP offer or a SDP answer.:

9.3.2 MSRP receiver

When a MSRP receiver receives a SEND request, the MSRP receiver shall parse the SEND request. The MSRP receiver shall either send a response including:

- a) a 200 (OK) status-code , as specified in draft-ietf-simple-message-sessions [9], for the concerned SEND message if the parsing was successful; or
- b) an appropriate status-code, as specified in draft-ietf-simple-message-sessions [9], for the concerned SEND message if the parsing was unsuccessful.

The MSRP receiver shall send a REPORT request if this is explicit or implicit requested in the SEND request(s) belonging to the message. It shall either be:

- a) a successful REPORT request including status-code 200 (OK) if a complete message is received and the Report-Success header in the SEND request was set to “yes”; or
- b) an unsuccessful REPORT request including status-code other than 200 (OK) as defined in draft-ietf-simple-message-sessions [9] if the MSRP receiver can conclude that a complete message is not received and the Report-Failure header is set to “yes” or not included. The criteria to conclude that a complete message is not received are specified in draft-ietf-simple-message-sessions [9].

9.3.3 Intermediate node

9.3.3.1 Intermediate node terminating case

When an intermediate node receives a SEND request, the intermediate node shall:

- 1) parse the SEND request and either send a response including:
 - a) a 200 (OK) status-code, as specified in draft-ietf-simple-message-sessions [9], for the concerned SEND message, if the parsing was successful; or
 - b) an appropriate status-code, as specified in draft-ietf-simple-message-sessions [9], for the concerned SEND message if the parsing was unsuccessful.; and
- 2) determine that a complete message has been received. The following actions in this subclause shall only be performed if a complete message is received.

The MSRP receiver shall send a REPORT request if this is explicit or implicit requested in the SEND request(s) associated to the same message. It shall either be:

- a) a successful REPORT request including status-code 200 (OK) if the intermediate node concludes that all available users on the distribution list has received the complete message or a concerned user has received the complete message and the Report-Success header in the SEND request was set to “yes”; or
- b) an unsuccessful REPORT request including status-code other than 200 (OK) as defined in draft-ietf-simple-message-sessions [9] if the intermediate node conclude that a complete message has not been received or that a complete message has not been able to be delivered to all available users on the distribution list or to a particular member of the distribution list.

9.3.3.2 Intermediate node originating case

When an intermediate node wishes to send a message, the intermediate shall ensure that the message length is not longer than the max-size attribute, as received in a SDP offer or a SDP answer. Depending on the message length the message may be included in one SEND request or chunked into a number of SEND requests. The intermediate [node](#) shall follow the procedures and rules as specified in draft-ietf-simple-message-sessions [9], when the intermediate node fragments a message into a number SEND requests.

The SEND request shall include the Byte-Range header. The MSRP sender shall populate the Byte-Range header fields as follows:

- the range-end field set to * (interruptable), to make the chunks interruptable, if the SEND request is longer than 2048 octets; and
- the total field set to the total size of the message.

⌘

The intermediate shall create a SEND request in accordance with draft-ietf-simple-message-sessions [9] with the following clarifications:

- 1) set the Report-Success header as received in the SEND request;
- 2) set the Report-Failure header as received in the SEND request; and
- 3) depending on the received MSRP URI
 - a) either send the SEND request to all available user of the conference; or
 - b) send the SEND request to one MSRP receiver.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 851** ⌘ rev **2** ⌘ Current version: **6.5.1** ⌘

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:	⌘ Pres and im URIs in incoming requests		
Source:	⌘ Nokia		
Work item code:	⌘ IMS2	Date:	⌘ 18/2/2005
Category:	⌘ C	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Use <u>one</u> of the following releases: 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:	⌘ Accotrding to SA2 decision, pres: and im: URIs need to be supported for incoming requests as well.
Summary of change:	⌘ The handling and routing of such URIs in incoming requests is defined.
Consequences if not approved:	⌘ Requirement not fulfilled.

Clauses affected:	⌘ 5.3.2.1						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
	Y	N					
	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
<input checked="" type="checkbox"/>	Test specifications						
<input checked="" type="checkbox"/>	O&M Specifications						
Other comments:	⌘						

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, ~~that does not contain a Route header,~~ 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 azs 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 23: 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.

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, then the THIG functionality in I-CSCF received an outgoing initial request for which topology hiding has to be applied, 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 34: 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.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.247** **CR 002** ⌘ rev **3** ⌘ Current version: **6.0.1** ⌘

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:	⌘ MESSAGE to multiple recipients		
Source:	⌘ Lucent Technologies		
Work item code:	⌘ IMS2	Date:	⌘ 01/02/2005
Category:	⌘ F	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Use <u>one</u> of the following releases: 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 Stage 2 document 23.228 [subclause 5.16.1.2] describes the procedures related to the delivery of immediate messages with multiple recipients. The corresponding Stage 3 text should be added to the document 24.247 to reflect these requirements..
Summary of change:	⌘ The added text specifies two methods of delivery of immediate messages with multiple recipients.
Consequences if not approved:	⌘ Incomplete specification

Clauses affected:	⌘ References, new subclauses added.						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘			
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘			
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
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****

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: "3G Vocabulary".
- [2] 3GPP TS 22.228: " Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1".
- [3] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model; Stage 2".
- [4] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".
- [5] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".
- [6] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".
- [7] RFC 3261 (March 2002): "SIP: Session Initiation Protocol".
- [8] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".
- [9] draft-ietf-simple-message-sessions-06.txt (May 2004): "The Message Session Relay Protocol".

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

- [10] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".
- [11] 3GPP TS 22.340: "IP Multimedia System (IMS) messaging; Stage 1".
- [12] [draft-ietf-sipping-uri-list-message-02 \(November 2004\): "Multiple-Recipient MESSAGE Requests in the Session Initiation Protocol \(SIP\)".](#)

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

****CHANGE****

5.1.1.1 Sending immediate message to multiple recipients

The UE may be able to send a single immediate message to multiple recipients by including in the MESSAGE request the list of URIs (i.e., URI-list) that identify the intended recipients.

The UE shall create a MESSAGE request in accordance with 3GPP TS 24.229 [5], and it shall also include a multipart body in the MESSAGE request. The Request-URI shall be set to the SIP URI of the Application Server that implements the role of the List Server. The multipart body shall contain the body carrying the URI-list (in the XML format) whose Content-Disposition type is 'recipient-list', and the body that contains the immediate message payload as specified in the draft-ietf-sipping-uri-list-message-02 [12].

The handling of the received response shall be in accordance with 3GPP TS 24.229 [5].

****CHANGE****

5.3.2.1 List Server processing the MESSAGE URI-list

Upon receiving the MESSAGE request with the URI-list included in the multipart body, the List Server shall inform the UE that it has received the MESSAGE request by returning the 202 (Accepted) response. Subsequently, the List Server shall create a MESSAGE request for each intended recipient listed in the URI-list, and it shall insert the immediate message payload into the body of each outgoing MESSAGES request.

When creating the outgoing MESSAGE requests destined for each recipient, the List Server shall follow the procedures described in the 3GPP TS 24.229 [5]. The List Server shall populate the header fields of each outgoing MESSAGE request as follows:

- the Request-URI set to the SIP URI of the intended recipient;
- the From header field set to the same value as the From header field that was received in the incoming MESSAGE request;
- the To header set to the SIP URI of the intended recipient; and
- the remaining headers set to the values as specified in 3GPP TS 24.229 [5] subclause 5.7.3.

The List Server shall also compose the multipart body of the outgoing MESSAGE request as specified in the draft-ietf-sipping-uri-list-message-02 [12], and included it in the outgoing MESSAGE request.

When sending the MESSAGE request to each recipient, and processing the respective responses, the List Server shall behave as specified in the 3GPP TS 24.229 [5] subclause 5.7.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 846** ⌘ rev **2** ⌘ Current version: **6.5.1** ⌘

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 to the Registration procedure
Source:	⌘ Huawei
Work item code:	⌘ IMS2
Date:	⌘ 20/01/2005
Category:	⌘ F
	Use <u>one</u> of the following categories:
	F (correction)
	A (corresponds to a correction in an earlier release)
	B (addition of feature),
	C (functional modification of feature)
	D (editorial modification)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .
Release:	⌘ Rel-6
	Use <u>one</u> 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 IMS stage 2 specification, the UE may indicate its capabilities and characteristics during IMS registration, and update its capabilities via re-registration. But this is not reflected in the stage3 specification.
Summary of change:	⌘ Add the description of indicating and updating UE's capabilities and/or characteristics in UE initiated registration.
Consequences if not approved:	⌘ The stage 3 description is missing.

Clauses affected:	⌘ 5.1.1.4									
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	X	X	X	X	X	X	⌘ Other core specifications ⌘ Test specifications ⌘ O&M Specifications
Y	N									
X	X									
X	X									
X	X									
Other comments:	⌘									

How to create CRs using this form:

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

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

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

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

5.1.1.4 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, or when the UE intends to update its capabilities according to RFC 3840 (ref.[62]).

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.

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.

CR-Form-v7.1

CHANGE REQUEST

⌘ **TS 24.229** **CR** **818** ⌘ **rev** **3** ⌘ Current version: **6.5.1** ⌘

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:	⌘ Corrections to subclause 5.5 in TS 24.229		
Source:	⌘ LM Ericsson		
Work item code:	⌘ IMS2	Date:	⌘ 15/01/2005
Category:	⌘ F	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Use <u>one</u> of the following releases: 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:	⌘ TS 24.229 includes a number of misalignment with TS 29.163.
	<ol style="list-style-type: none"> 1) In no calling line identity is not received from the CS network the P-asserted-Identity shall not be included in the INVITE. 2) The TrFO concept is introduced in the interworking which may lead to that no coded is required. 3) The MGCF shall only send an UPDATE if a continuity procedure is carried out in the CS network. 4) The P-Asserted-ID in 200 OK is dependent on if a connected number is received from CS network.
Summary of change:	⌘ . <ol style="list-style-type: none"> 1) The inclusion of P-Asserted Identity is made conditional on whether corresponding information is received from the CS-network 2) The case where TrFO is possible is added. 3) The sending of UPDATE depends on whether a continuity procedure is carried out on the CS side and if an INVITE has been sent.
Consequences if not approved:	⌘ Misalignment between TS 29.163 and TS 24.229, which may lead to incompatible implementations.

Clauses affected:	⌘ 2.5.5.3.1.1, 5.5.3.1.2, 5.5.3.2.1 and 5.5.3.2.2						
Other specs	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> <td style="width: 20px; text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						

Affected:

<input checked="" type="checkbox"/>	Test specifications
<input checked="" type="checkbox"/>	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.

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".
- [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] draft-ietf-iptel-rfc2806bis-09 (June 2004): "The tel URI for Telephone Numbers".

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

- [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)".
- [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 Initiation Protocol (SIP) "Replaces" Header".
- [61] RFC 3911 (October 2004): "The Session Initiation 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".
- [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-simple-xcap-package-01 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Modification Events for the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Managed Documents".

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.

- [80] [3GPP TS 29.163: "Interworking between the IP Multimedia \(IM\) Core Network \(CN\) subsystem and Circuit Switched \(CS\) networks"](#).

5.5 Procedures at the MGCF

5.5.1 General

The MGCF, 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. Therefore table A.4/1 and dependencies on that major capability shall not apply.

The use of the Path and Service-Route headers shall not be supported by the MGCF.

When the MGCF sends any request or response related to a dialog or standalone transaction, the MGCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

5.5.2 Subscription and notification

Void.

5.5.3 Call initiation

5.5.3.1 Initial INVITE

5.5.3.1.1 Calls originated from circuit-switched networks

When the MGCF receives an indication of an incoming call from a circuit-switched network, the MGCF shall:

- generate and send an INVITE request to I-CSCF:
 - set the Request-URI to the "tel" format using an E.164 address;
 - ~~the Supported header to "100rel"~~(see RFC 3312 [30]);~~and~~
 - include an P-Asserted-Identity header, [depending on corresponding information in the circuit switched network](#);
 - create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
 - insert an orig-ioi parameter into the P-Charging-Vector header. The orig-ioi parameter shall be set to a value that identifies the sending network in which the MGCF resides and the term-ioi parameter shall not be included.

5.5.3.1.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request-with Supported header indicating "100rel", the MGCF shall:

- send 100 (Trying) response;
- after a matching codec ~~is~~ found [or no codec is required](#) at the MGW, send 183 "Session Progress" response:
 - set the Require header to the value of "100rel";
 - store the values received in the P-Charging-Function-Addresses header;
 - store the value of the icid parameter received in the P-Charging-Vector header; and
 - insert a term-ioi parameter into the P-Charging-Vector header. The term-ioi parameter shall be set to a value that identifies the network in which the MGCF resides.

~~When~~ [If a codec is required and](#) the MGCF does not find an available matching codec at the MGW for the received initial INVITE request, the MGCF shall:

- send 503 (Service Unavailable) response if the type of codec was acceptable but none were available; or
- send 488 (Not Acceptable Here) response if the type of codec was not supported, and may include SDP in the message body to indicate the codecs supported by the MGCF/MGW.

5.5.3.2 Subsequent requests

5.5.3.2.1 Calls originating in circuit-switched networks

When the MGCF receives 183 response to an INVITE request, the MGCF shall:

- ~~store~~ the values received in the P-Charging-Function-Addresses header.

[The MGCF shall send an UPDATE request when the following conditions are fulfilled;](#)

- [conditions as specified in TS 29.163 \[80\]; and](#)

- ~~When the MGCF receives 200 (OK) response to a PRACK request and notification that bearer setup is complete if the notification is not received in the incoming call information, the MGCF shall:~~
 - ~~—send an UPDATE request.~~

5.5.3.2.2 Calls terminating in circuit-switched networks

When the MGCF receives an indication of a ringing for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 180 Ringing response to the UE.

When the MGCF receives an indication of answer for the called party of outgoing call to a circuit-switched network, the MGCF shall send 200 OK response to the UE. The 200 OK response shall include an P-Asserted-Identity header if corresponding information is received from the circuit switched network.

3GPP TSG-CN1 Meeting #37
Sydney, Australia, 14th to 18th February 2005

Tdoc #N1-050418

CR-Form-v7

CHANGE REQUEST

⌘ **24.229 CR 801** ⌘ rev **3** ⌘ Current version: **6.5.1** ⌘

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:	⌘ Default handling associated with trigger point (all other requests than REGISTER)																
Source:	⌘ Orange																
Work item code:	⌘ IMS2 Date: ⌘ 17/02/2005																
Category:	⌘ F Release: ⌘ REL-6																
Use <u>one</u> of the following categories:																	
<table border="0"> <tr> <td>F (correction)</td> <td>2 (GSM Phase 2)</td> </tr> <tr> <td>A (corresponds to a correction in an earlier release)</td> <td>R96 (Release 1996)</td> </tr> <tr> <td>B (addition of feature),</td> <td>R97 (Release 1997)</td> </tr> <tr> <td>C (functional modification of feature)</td> <td>R98 (Release 1998)</td> </tr> <tr> <td>D (editorial modification)</td> <td>R99 (Release 1999)</td> </tr> <tr> <td>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</td> <td>Rel-4 (Release 4)</td> </tr> <tr> <td></td> <td>Rel-5 (Release 5)</td> </tr> <tr> <td></td> <td>Rel-6 (Release 6)</td> </tr> </table>		F (correction)	2 (GSM Phase 2)	A (corresponds to a correction in an earlier release)	R96 (Release 1996)	B (addition of feature),	R97 (Release 1997)	C (functional modification of feature)	R98 (Release 1998)	D (editorial modification)	R99 (Release 1999)	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .	Rel-4 (Release 4)		Rel-5 (Release 5)		Rel-6 (Release 6)
F (correction)	2 (GSM Phase 2)																
A (corresponds to a correction in an earlier release)	R96 (Release 1996)																
B (addition of feature),	R97 (Release 1997)																
C (functional modification of feature)	R98 (Release 1998)																
D (editorial modification)	R99 (Release 1999)																
Detailed explanations of the above categories can be found in 3GPP TR 21.900 .	Rel-4 (Release 4)																
	Rel-5 (Release 5)																
	Rel-6 (Release 6)																
Use <u>one</u> of the following releases:																	

Reason for change:⌘ In TS 23.218 section 5.2 about Service interaction, it is stated:

"If the S-CSCF can not reach the Application Server, the S-CSCF shall apply the default handling associated with the trigger. This default handling shall be :

- to continue verifying if the triggers of lower priority in the list match; or
- to abandon verification of matching of the triggers of lower priority in the list; and to release the dialogue."

Also, it is stated:

"If an Application Server decides to locally terminate a request and sends back a final response for that request via the ISC interface to the S-CSCF, the S-CSCF shall abandon verification of the matching of the triggers of lower priority in the list."

In TS 23.218 section 6.4 about Handling of mobile originating requests, it is stated (same requirement for section 6.5 for terminating requests):

In any instance, if the contact of the application server fails, the S-CSCF shall use the "default handling" associated with the initial Filter Criteria to determine if it shall either terminate the call or let the call continue 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 application server, the S-CSCF shall let the call continue as the default behaviour.

In TS 29.228 in the normative annex E that describes the XML schema for the Cx interface user profile about Service profile:

Default Handling is of type enumerated and can take the values: SESSION_CONTINUED or SESSION_TERMINATED.

Consequently, default handling should be taken into account in all stage 3

	specifications.
Summary of change: ⌘	In sections 5.4.3.2 and 5.4.3.3 about S-CSCF handling when receiving an initial request for a dialog or a request for a standalone transaction on originating part/terminating part, it is added what behaviour the S-CSCF shall apply according to the default handling associated with the trigger if the S-CSCF can not reach the AS or when the S-CSCF receives a final response from the AS.
Consequences if not approved:	Incomplete procedure: the treatment at the S-CSCF is not determined: <ul style="list-style-type: none"> - when the S-CSCF can not reach the AS the default handling stored in the Service profile is not used; - when the S-CSCF receives a final response from the AS.

Clauses affected: ⌘	5.4.3.2, 5.4.3.3										
Other specs affected:	<table border="1"><tr><td>Y</td><td>N</td></tr><tr><td>X</td><td></td></tr><tr><td></td><td>X</td></tr><tr><td></td><td>X</td></tr></table>	Y	N	X			X		X	Other core specifications	⌘ TS 23.218 (CR 74)
	Y	N									
	X										
	X										
	X										
	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 co

*** FIRST MODIFICATION ***

5.4.3.2 Requests initiated by the served user

When the S-CSCF receives from the served user or from a PSI an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

Editor's Note: It needs to be stated, that the S-CSCF will only perform the following steps if the request was received from a trusted entity, e.g. an entity within the trust domain.

- 1) determine whether the request contains a barred public user identity in the P-Asserted-Identity header field of the request or not. In case the said header field contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. The response may include a Warning header containing the warn-code 399. Otherwise, continue with the rest of the steps;

NOTE 1: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

- 2) remove its own SIP URI from the topmost Route header;
- 3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request;
- 4) check whether the initial request matches the next unexecuted initial filter criteria based on a public user identity in the P-Asserted-Identity header in the priority order as described in 3GPP TS 23.218 [5], and if it does, the S-CSCF shall:
 - a) insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4; and
 - b) if the AS is located outside the trust domain then the S-CSCF shall remove the P-Access-Network-Info header field and its values in the request; if the AS is located within the trust domain, then the S-CSCF shall retain the P-Access-Network-Info header field and its values in the request that is forwarded to the AS;

NOTE 2: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request URI.

- 5) if there is no original dialog identifier present in the topmost Route header of the incoming request 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. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;
- 6) if there is no original dialog identifier present in the topmost Route header of the incoming request insert an orig-ioi parameter into the P-Charging-Vector header. The S-CSCF shall set the orig-ioi parameter to a value that identifies the sending network. The S-CSCF shall not include the term-ioi parameter;
- 7) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;
- 8) if there is no original dialog identifier present in the topmost Route header of the incoming request and if the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;
- 9) if the request is not forwarded to an AS and if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see draft-ietf-iptel-rfc2806bis [22]) to a globally routeable SIP URI using an ENUM/DNS translation mechanism with the format specified in RFC 3761 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. If the outgoing Request-URI is a pres URI or an im URI, the S-CSCF shall forward the request as specified in RFC 3861 [63]. In this case, the S-CSCF shall not modify the received Request-URI;

- 10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. If the destination address is of an IP address type other than the IP address type used in the IM CN subsystem, then the S-CSCF shall forward the request to the IMS-ALG if the IM CN subsystem supports interworking to networks with different IP address type;
- 11) if network hiding is needed due to local policy, put the address of the I-CSCF (THIG) to the topmost route header;
- 12) in case of an initial request for a dialog originated from a served user, either:
- if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or
 - if the request is routed elsewhere, create a Record-Route header containing its own SIP URI;

NOTE 3: For requests originated from a PSI the S-CSCF can decide whether to record-route or not.

Editor's Note: It needs to be clarified how the S-CSCF decides whether to put its address into the Record-Route header in the case of handling a request that originates from a PSI. It might be part of the operators policy.

- 13) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header prior to forwarding the message;
- 14) route the request based on SIP routing procedures; and
- 15) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed.

If the S-CSCF fails to receive a SIP response or receives a 408 Request Timeout response or a 5xx response from the AS, the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION_CONTINUE" as specified in TS 29.228 [14] or no default handling is indicated, execute the procedure from step 4; and
- if the default handling defined in the filter criteria indicates the value "SESSION_TERMINATED" as specified in TS 29.228 [14], either forward the received response or send a 408 Request Timeout response or a 5xx response towards the served UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CSCF receives any final response from the AS, it shall forward the response towards the served UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CSCF receives any response to the above request, the S-CSCF may:

- 1) apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header; and
- 2) apply the same privacy mechanism to the P-Access-Network-Info header, if present.

NOTE 4: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 5: The optional procedures above are in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

When the S-CSCF receives any response to the above request containing a term-ioi parameter, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message. The term-ioi parameter and the orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

When the S-CSCF receives from the served user a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- 1) remove its own URI from the topmost Route header;
- 2) create a Record-Route header containing its own SIP URI;
- 3) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;
- 4) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header;
- 5) in case the request is routed towards the destination user (Request-URI) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header; and
- 6) route the request based on the topmost Route header.

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

When the S-CSCF receives from the served user a subsequent request other than a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- 1) remove its own URI from the topmost Route header;
- 2) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and
- 3) in case the request is routed towards the destination user (Request-URI) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header; and
- 4) route the request based on the topmost Route header.

*** NEXT MODIFICATION ***

5.4.3.3 Requests terminated at the served user

When the S-CSCF receives, destined for a statically pre-configured PSI or a registered served user, an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

- 1) determine whether the request contains a barred public user identity in the Request-URI of the request or not. In case the Request URI contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 404 (Not Found) response. Otherwise, continue with the rest of the steps;
- 2) remove its own URI from the topmost Route header;
- 3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.
 - If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.
 - If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case the S-CSCF shall save the Request-URI from the request;
- 4) check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 1: Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.

- 5) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header field, if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

- 6) if there is no original dialog identifier present in the topmost Route header of the incoming request 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;
- 7) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;
- 8) check whether the Request-URI equals to the saved value of the Request-URI. If there is no match, then:
 - a) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed; and
 - b) forward the request based on the Request-URI and skip the following steps;If there is a match, then continue with the further steps;

- 9) if necessary perform the caller preferences to callee capabilities matching according to RFC 3841 [56B];

- 10) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2. Furthermore, the S-CSCF shall:

- a) build the Route header field with the values determined in the previous step;
- b) determine, from the destination public user identity, the saved Contact URI where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2. If there is more than one contact address saved for the destination public user identity, the S-CSCF shall:
 - if the fork directive in the Request Disposition header was set to "no-fork", the contact with the highest qvalue parameter shall be used when building the Request-URI. In case no qvalue parameters were provided, the S-CSCF shall decide locally what contact address to be used when building the Request-URI; otherwise
 - fork the request or perform sequential search based on the relative preference indicated by the qvalue parameter of the Contact header in the original REGISTER request, as described in RFC3261 [26]. In case no qvalue parameters were provided, then the S-CSCF determine the contact address to be used when building the Request-URI as directed by the Request Disposition header as described in RFC 3841 [56B]. If the Request-Disposition header is not present, the S-CSCF shall decide locally whether to fork or perform sequential search among the contact addresses;
- c) build a Request-URI with the contents of the saved Contact URI determined in the previous step; and
- d) insert a P-Called-Party-ID SIP header field including the Request-URI received in the request;

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

- 12) optionally, apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header and apply the same privacy mechanism to the P-Access-Network-Info header;

NOTE 2: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

- 13) in case of an initial request for a dialog, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or
- if the request is routed elsewhere, create a Record-Route header containing its own SIP URI; and

- 14) forward the request based on the topmost Route header.

If the S-CSCF fails to receive a SIP response or receives a 408 Request Timeout response or a 5xx response from the AS, the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION_CONTINUED" as specified in TS 29.228 [14] or no default handling is indicated, execute the procedure from step 4; and
- if the default handling defined in the filter criteria indicates the value "SESSION_TERMINATED" as specified in TS 29.228 [14], either forward the received response or send a 408 Request Timeout response or a 5xx response towards the served UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CSCF receives any final response from the AS, it shall forward the response towards the served UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CSCF receives, destined for an unregistered user, an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall:

- 1) if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14];
- 2) execute the procedures described in the steps 1, 2 and 3 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction); and
- 3) execute the procedure described in step 4, 5, 6, 7, 8, 10, 12 and 13 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

In case that no AS needs to be contacted, then S-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures.

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

- 1) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed;
- 2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi;
- 3) in the case where the S-CSCF has knowledge of an associated tel-URL for a SIP URI contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URL;
- 4) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header; and
- 5) in case the response is sent towards the originating user, the S-CSCF may remove the P-Access-Network-Info header based on local policy rules and the destination user (Request-URI).

When the S-CSCF receives a response to a request for a standalone transaction (whether the user is registered or not), in the case where the S-CSCF has knowledge of an associated tel-URL for a SIP URI contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URL. In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the terminating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, the S-CSCF shall:

- 1) insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards an AS; and

- 2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

When the S-CSCF receives, destined for a served user, a target refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

- 1) remove its own URI from the topmost Route header;
- 2) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;
- 3) create a Record-Route header containing its own SIP URI; and
- 4) forward the request based on the topmost Route header.

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

- 1) if the response corresponds to an INVITE request, save the Record-Route and Contact header field values in the response such that the S-CSCF is able to release the session if needed; and
- 2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the originating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

When the S-CSCF receives, destined for the served user, a subsequent request other than target refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

- 1) remove its own URI from the topmost Route header; and
- 2) forward the request based on the topmost Route header.

When the S-CSCF receives a response to a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the terminating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

*** END OF MODIFICATION ***

3GPP TSG-CN1 Meeting #37
 Sydney, Australia, 14th to 18th February 2005

Tdoc #N1-050421

CR-Form-v7
CHANGE REQUEST
⌘ 24.229 CR 803 ⌘ rev 4 ⌘ Current version: 6.5.1 ⌘

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:	⌘ Default handling associated with the trigger for third party registration		
Source:	⌘ Orange		
Work item code:	⌘ IMS2 Date: ⌘ 17/02/2005		
Category:	⌘ F Release: ⌘ REL-6 Use <u>one</u> of the following categories: <table style="width: 100%; margin-top: 5px;"> <tr> <td style="width: 50%; vertical-align: top;"> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) </td> <td style="width: 50%; vertical-align: top;"> Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) </td> </tr> </table> Detailed explanations of the above categories can be found in 3GPP TR 21.900 .	F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)	Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)
F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)	Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)		

Reason for change:	⌘ In TS 23.218 section 5.2 about Service interaction, it is stated: If the S-CSCF can not reach the Application Server, the S-CSCF shall apply the default handling associated with the trigger. This default handling shall be : - to continue verifying if the triggers of lower priority in the list match; or - to abandon verification of matching of the triggers of lower priority in the list; and to release the dialogue. In TS 23.218 section 6.3 about Handling of SIP registration, it is stated: On receiving a failure response to one of the REGISTER requests, the S-CSCF shall apply the "default handling" related with the initial Filter Criteria's trigger used. In TS 24.229 section 5.4.1.2.3 about abnormal cases for registration, it is stated that: "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." Consequently, the text in section 5.4.1.7 "Notification of Application Servers about registration status" should be aligned in order to describe the default handling on failure of third-party registration.
Summary of change:	⌘ In section 5.4.1.7 about 3 rd -party registration, it is added what behaviour the S-CSCF shall apply according to the default handling associated with the trigger

when a 3rd-party registration fails.

If the S-CSCF receives a failure response to a 3rd-party REGISTER, the S-CSCF shall apply the default handling associated with the trigger:

- if the default handling indicates the value "SESSION_CONTINUED" as specified in TS 29.228 [14] or no default handling is indicated, the S-CSCF shall continue trigger matching and execute the procedure by sending a third-party REGISTER request to the AS associated to the next unexecuted trigger if any.
- if the default handling indicates the value "SESSION_TERMINATED" as specified in TS 29.228 [14], the S-CSCF shall initiate the network-initiated deregistration as described in section 5.4.1.5.

Consequences if not approved: Incomplete procedure in section 5.4.1.7: the treatment at the S-CSCF is not determined when the S-CSCF receives a failure response to a 3rd-party REGISTER.

Clauses affected: ⌘ 5.4.1.7

Other specs affected:	⌘	<table border="1"><tr><td>Y</td><td>N</td></tr><tr><td>X</td><td></td></tr><tr><td></td><td>X</td></tr></table>	Y	N	X			X	Other core specifications	⌘	TS 23.218 (CR 74)
		Y	N								
		X									
	X										
<table border="1"><tr><td></td><td>X</td></tr><tr><td></td><td>X</td></tr></table>		X		X	Test specifications						
	X										
	X										
<table border="1"><tr><td></td><td>X</td></tr></table>		X	O&M Specifications								
	X										

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 ***

5.4.1.7 Notification of Application Servers about registration status

During registration, the S-CSCF shall include a P-Access-Network-Info header (as received in the REGISTER request from the UE) in the 3rd-party REGISTER sent towards the ASs, if the AS is part of the trust domain. If the AS is not part of the trust domain, the S-CSCF shall not include any P-Access-Network-Info header. The S-CSCF shall not include a P-Access-Network-Info header in any responses to the REGISTER request.

If the registration procedure described in subclauses 5.4.1.2, 5.4.1.4 or 5.4.1.5 (as appropriate) was successful, the S-CSCF shall send a third-party REGISTER request to each AS with the following information:

- a) the Request-URI, which shall contain the AS's SIP URI;
- b) the From header, which shall contain the S-CSCF's SIP URI;
- c) the To header, which shall contain either the public user identity as contained in the REGISTER request received from the UE or one of the implicitly registered public user identities, as configured by the operator;
- d) the Contact header, which shall contain the S-CSCF's SIP URI;
- e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header, which shall contain the same value that the S-CSCF returned in the 200 (OK) response for the REGISTER request received from the UE;
- f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the Expires header, which shall contain the value zero;
- g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body, if there is Filter Criteria indicating the need to include HSS provided data for the REGISTER event (e.g. HSS may provide AS specific data to be included in the third-party REGISTER). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [14]), then the S-CSCF shall include it in the message body of the REGISTER request within the <service-info> XML element as described in subclause 7.6. For the messages including the IM CN subsystem XML body, the S-CSCF shall set the value of the Content-Type header to include the MIME type specified in subclause 7.6;
- h) for initial registration and user-initiated reregistration, the P-Charging-Vector header, which shall contain the same icid parameter that the S-CSCF received in the original REGISTER request from the UE;
- i) for initial registration and user-initiated reregistration, a P-Charging-Function-Addresses header, which shall contain the values received from the HSS if the message is forwarded within the S-CSCF home network.

If the S-CSCF fails to receive a SIP response or receives a 408 Request Timeout response or a 5xx response to a 3rd-party REGISTER, the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION CONTINUED" as specified in TS 29.228 [14] or no default handling is indicated, no further action is needed; and

- if the default handling defined in the filter criteria indicates the value "SESSION TERMINATED" as specified in TS 29.228 [14], the S-CSCF shall initiate the network-initiated deregistration as described in subclause 5.4.1.5.

*** END OF MODIFICATION ***