

**3rd Generation Partnership Project;
Technical Specification Group Core Network;
IP Multimedia Call Control Protocol based on
Session Initiation Protocol (SIP)
and Session Description Protocol (SDP);
Stage 3
(Release 5)**



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

UMTS, Network, IP, SIP, SDP, multimedia

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

<http://www.3gpp.org>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2003, 3GPP Organizational Partners (ARIB, CCSA, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Foreword	9
1 Scope.....	10
2 References.....	10
3 Definitions and abbreviations	13
3.1 Definitions.....	13
3.2 Abbreviations	14
4 General.....	16
4.1 Conformance of IM CN subsystem entities to SIP, SDP and other protocols.....	16
4.2 URI and address assignments	17
4.2A Transport mechanisms	18
4.3 Routing principles of IM CN subsystem entities	18
4.4 Trust domain	18
4.5 Charging correlation principles for IM CN subsystems	18
4.5.1 Overview	18
4.5.2 IM CN subsystem charging identifier (ICID)	19
4.5.3 Access network charging information.....	19
4.5.3.1 General	19
4.5.3.2 GPRS charging information.....	19
4.5.4 Inter operator identifier (IOI)	19
4.5.5 Charging function addresses	20
5 Application usage of SIP	20
5.1 Procedures at the UE.....	20
5.1.1 Registration and authentication.....	20
5.1.1.1 General	20
5.1.1.1A Parameters contained in the UICC	20
5.1.1.2 Initial registration	21
5.1.1.3 Initial subscription to the registration-state event package	22
5.1.1.4 User-initiated re-registration	23
5.1.1.5 Authentication	24
5.1.1.5.1 General.....	24
5.1.1.5.2 Network-initiated re-authentication.....	25
5.1.1.5.3 Abnormal cases.....	25
5.1.1.5A Change of IP address due to privacy	26
5.1.1.6 Mobile-initiated deregistration	26
5.1.1.7 Network-initiated deregistration	27
5.1.2 Subscription and notification	27
5.1.2.1 Notification about multiple registered public user identities	27
5.1.2.2 General SUBSCRIBE requirements	28
5.1.2A Generic procedures applicable to all methods excluding the REGISTER method.....	28
5.1.2A.1 Mobile-originating case.....	28
5.1.2A.2 Mobile-terminating case.....	29
5.1.3 Call initiation - mobile originating case.....	29
5.1.3.1 Initial INVITE	29
5.1.4 Call initiation - mobile terminating case	30
5.1.4.1 Initial INVITE	30
5.1.5 Call release	30
5.1.6 Emergency service	30
5.1.7 Void.....	30
5.2 Procedures at the P-CSCF.....	30
5.2.1 General	30
5.2.2 Registration	31
5.2.3 Subscription to the user's registration-state event package	34
5.2.4 Registration of multiple public user identities	35
5.2.5 Deregistration	35

5.2.5.1	User-initiated deregistration	35
5.2.5.2	Network-initiated deregistration	35
5.2.6	General treatment for all dialogs and standalone transactions excluding the REGISTER method	36
5.2.6.1	Introduction	36
5.2.6.2	Determination of mobile-originated or mobile-terminated case	36
5.2.6.3	Requests initiated by the UE	36
5.2.6.4	Requests terminated by the UE	39
5.2.7	Initial INVITE	42
5.2.7.1	Introduction	42
5.2.7.2	Mobile-originating case.....	42
5.2.7.3	Mobile-terminating case.....	42
5.2.7.4	Access network charging information.....	43
5.2.8	Call release	43
5.2.8.1	P-CSCF-initiated call release	43
5.2.8.1.1	Cancellation of a session currently being established	43
5.2.8.1.2	Release of an existing session	43
5.2.8.1.3	Abnormal cases.....	44
5.2.8.1.4	Release of the existing dialogs due to registration expiration and deletion of the security association.....	44
5.2.8.2	Call release initiated by any other entity	44
5.2.9	Subsequent requests	44
5.2.9.1	Mobile-originating case.....	44
5.2.9.2	Mobile-terminating case.....	44
5.2.10	Emergency service	44
5.2.11	Void.....	45
5.3	Procedures at the I-CSCF.....	45
5.3.1	Registration procedure	45
5.3.1.1	General	45
5.3.1.2	Normal procedures	45
5.3.1.3	Abnormal cases	46
5.3.2	Initial requests	46
5.3.2.1	Normal procedures	46
5.3.2.2	Abnormal cases	47
5.3.3	THIG functionality in the I-CSCF(THIG)	47
5.3.3.1	General	47
5.3.3.2	Encryption for topology hiding.....	48
5.3.3.3	Decryption for Topology Hiding	48
5.3.4	Void.....	49
5.4	Procedures at the S-CSCF.....	49
5.4.1	Registration and authentication.....	49
5.4.1.1	Introduction	49
5.4.1.2	Initial registration and user-initiated reregistration.....	49
5.4.1.2.1	Unprotected REGISTER	49
5.4.1.2.2	Protected REGISTER.....	50
5.4.1.2.3	Abnormal cases.....	52
5.4.1.3	Authentication and reauthentication.....	53
5.4.1.4	User-initiated deregistration.....	53
5.4.1.5	Network-initiated deregistration	53
5.4.1.6	Network-initiated reauthentication.....	54
5.4.1.7	Notification of Application Servers about registration status	55
5.4.2	Subscription and notification	55
5.4.2.1	Subscriptions to S-CSCF events	55
5.4.2.1.1	Subscription to the event providing registration state	55
5.4.2.1.2	Notification about registration state	56
5.4.3	General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF	57
5.4.3.1	Determination of mobile-originated or mobile-terminated case	57
5.4.3.2	Requests initiated by the served user	57
5.4.3.3	Requests terminated at the served user	59
5.4.3.4	Original dialog identifier.....	61
5.4.3.5	Void	61
5.4.4	Call initiation.....	61
5.4.4.1	Initial INVITE	61

5.4.4.2	Subsequent requests	62
5.4.4.2.1	Mobile-originating case	62
5.4.4.2.2	Mobile-terminating case	62
5.4.5	Call release	62
5.4.5.1	S-CSCF-initiated session release	62
5.4.5.1.1	Cancellation of a session currently being established	62
5.4.5.1.2	Release of an existing session	62
5.4.5.1.2A	Release of the existing dialogs due to registration expiration	63
5.4.5.1.3	Abnormal cases	63
5.4.5.2	Session release initiated by any other entity	63
5.4.6	Call-related requests	64
5.4.6.1	ReINVITE	64
5.4.6.1.1	Determination of served user	64
5.4.6.1.2	Mobile-originating case	64
5.4.6.1.3	Mobile-terminating case	64
5.4.7	MESSAGE support	64
5.5	Procedures at the MGCF	64
5.5.1	General	64
5.5.2	Subscription and notification	64
5.5.3	Call initiation	65
5.5.3.1	Initial INVITE	65
5.5.3.1.1	Calls originated from circuit-switched networks	65
5.5.3.1.2	Calls terminating in circuit-switched networks	65
5.5.3.2	Subsequent requests	65
5.5.3.2.1	Calls originating in circuit-switched networks	65
5.5.3.2.2	Calls terminating in circuit-switched networks	66
5.5.4	Call release	66
5.5.4.1	Call release initiated by a circuit-switched network	66
5.5.4.2	IM CN subsystem initiated call release	66
5.5.4.3	MGW-initiated call release	66
5.5.5	Call-related requests	66
5.5.5.1	ReINVITE	66
5.5.5.1.1	Calls originating from circuit-switched networks	66
5.5.5.1.2	Calls terminating in circuit-switched networks	66
5.5.6	Further initial requests	66
5.6	Procedures at the BGCF	67
5.6.1	General	67
5.6.2	Session initiation transaction	67
5.7	Procedures at the Application Server (AS)	67
5.7.1	Common Application Server (AS) procedures	67
5.7.1.1	Notification about registration status	67
5.7.1.2	Extracting charging correlation information	68
5.7.1.3	Access-Network-Info	68
5.7.2	Application Server (AS) acting as terminating UA, or redirect server	68
5.7.3	Application Server (AS) acting as originating UA	68
5.7.4	Application Server (AS) acting as a SIP proxy	68
5.7.5	Application Server (AS) performing 3rd party call control	69
5.7.5.1	General	69
5.7.5.2	Call initiation	69
5.7.5.2.1	Initial INVITE	69
5.7.5.2.2	Subsequent requests	69
5.7.5.3	Call release	69
5.7.5.4	Call-related requests	69
5.7.5.5	Further initial requests	70
5.7.6	Void	70
5.8	Procedures at the MRFC	70
5.8.1	General	70
5.8.2	Call initiation	70
5.8.2.1	Initial INVITE	70
5.8.2.1.1	MRFC-terminating case	70
5.8.2.1.1.1	Introduction	70
5.8.2.1.2	MRFC-originating case	71

5.8.2.2	Subsequent requests	71
5.8.2.2.1	Tones and announcements	71
5.8.3	Call release	71
5.8.3.1	S-CSCF-initiated call release	71
5.8.3.1.1	Tones and announcements	71
5.8.3.2	MRFC-initiated call release	71
5.8.3.2.1	Tones and announcements	71
5.8.2.2.2	Transcoding	72
5.8.4	Call-related requests	72
5.8.4.1	ReINVITE	72
5.8.4.1.1	MRFC-terminating case	72
5.8.4.1.2	MRFC-originating case	72
5.8.4.2	REFER	72
5.8.4.2.1	MRFC-terminating case	72
5.8.4.2.2	MRFC-originating case	72
5.8.4.2.3	REFER initiating a new session	72
5.8.4.2.4	REFER replacing an existing session	72
5.8.4.3	INFO	72
5.8.5	Further initial requests	73
6	Application usage of SDP	73
6.1	Procedures at the UE	73
6.2	Procedures at the P-CSCF	74
6.3	Procedures at the S-CSCF	74
6.4	Procedures at the MGCF	74
6.4.1	Calls originating from circuit-switched networks	74
6.4.2	Calls terminating in circuit-switched networks	75
6.5	Procedures at the MRFC	75
6.6	Procedures at the AS	75
7	Extensions within the present document	76
7.1	SIP methods defined within the present document	76
7.2	SIP headers defined within the present document	76
7.2.0	General	76
7.2.1	Void	76
7.2.2	Void	76
7.2.3	Void	76
7.2.4	Void	76
7.2.5	Void	76
7.2.6	Void	76
7.2.7	Void	76
7.2.8	Void	76
7.2.9	Void	76
7.2.10	Void	76
7.2A	Extensions to SIP headers defined within the present document	76
7.2A.1	Extension to WWW-authenticate header	76
7.2A.1.1	Introduction	76
7.2A.1.2	Syntax	76
7.2A.1.3	Operation	77
7.2A.2	Extension to Authorization header	77
7.2A.2.1	Introduction	77
7.2A.2.2	Syntax	77
7.2A.2.3	Operation	77
7.2A.3	Tokenized-by parameter definition (various headers)	77
7.2A.3.1	Introduction	77
7.2A.3.2	Syntax	77
7.2A.3.3	Operation	78
7.2A.4	P-Access-Network-Info header	78
7.2A.4.1	Introduction	78
7.2A.4.2	Syntax	78
7.2A.4.3	Additional coding rules for P-Access-Network-Info header	78
7.2A.5	P-Charging-Vector header	78

7.2A.5.1	Introduction	78
7.2A.5.2	Syntax	78
7.2A.5.3	Operation	79
7.3	Option-tags defined within the present document	79
7.4	Status-codes defined within the present document	79
7.5	Session description types defined within the present document	79
7.6	3GPP IM CN subsystem XML body, version 1	79
7.6.1	General	79
7.6.2	Document Type Definition	80
7.6.3	DTD description	80
7.7	SIP timers	80
7.8	IM CN subsystem timers	81
8	SIP compression	82
8.1	SIP compression procedures at the UE	82
8.1.1	SIP compression	82
8.1.2	Compression of SIP requests and responses transmitted to the P-CSCF	82
8.1.3	Decompression of SIP requests and responses received from the P-CSCF	82
8.2	SIP compression procedures at the P-CSCF	82
8.2.1	SIP compression	82
8.2.2	Compression of SIP requests and responses transmitted to the UE	82
8.2.3	Decompression of SIP requests and responses received from the UE	82
9	GPRS aspects when connected to the IM CN subsystem	83
9.1	Introduction	83
9.2	Procedures at the UE	83
9.2.1	PDP context activation and P-CSCF discovery	83
9.2.1A	Modification of a PDP context used for SIP signalling	84
9.2.1B	Re-establishment of the PDP context for signalling	84
9.2.2	Session management procedures	85
9.2.3	Mobility management procedures	85
9.2.4	Cell selection and lack of coverage	85
9.2.5	PDP contexts for media	85
9.2.5.1	General requirements	85
9.2.5.1A	Activation or modification of PDP contexts for media	85
9.2.5.2	Special requirements applying to forked responses	86
9.2.5.3	Unsuccessful situations	86
Annex A (normative):	Profiles of IETF RFCs for 3GPP usage	87
A.1	Profiles	87
A.1.1	Relationship to other specifications	87
A.1.2	Introduction to methodology within this profile	87
A.1.3	Roles	88
A.2	Profile definition for the Session Initiation Protocol as used in the present document	89
A.2.1	User agent role	89
A.2.1.1	Introduction	89
A.2.1.2	Major capabilities	90
A.2.1.3	PDU parameters	93
A.2.1.4	PDU parameters	94
A.2.1.4.1	Status-codes	94
A.2.1.4.2	ACK method	95
A.2.1.4.3	BYE method	97
A.2.1.4.4	CANCEL method	102
A.2.1.4.5	COMET method	105
A.2.1.4.6	INFO method	105
A.2.1.4.7	INVITE method	105
A.2.1.4.7A	MESSAGE method	112
A.2.1.4.8	NOTIFY method	118
A.2.1.4.9	OPTIONS method	124
A.2.1.3.10	PRACK method	130
A.2.1.4.11	REFER method	136

A.2.1.4.12	REGISTER method	142
A.2.1.4.13	SUBSCRIBE method	149
A.2.1.4.14	UPDATE method	156
A.2.2	Proxy role	161
A.2.2.1	Introduction	161
A.2.2.2	Major capabilities	162
A.2.2.3	PDU's	166
A.2.2.4	PDU parameters	167
A.2.2.4.1	Status-codes	167
A.2.2.4.2	ACK method	169
A.2.2.4.3	BYE method	170
A.2.2.4.4	CANCEL method	176
A.2.2.4.5	COMET method	179
A.2.2.4.6	INFO method	179
A.2.2.4.7	INVITE method	179
A.2.2.4.7A	MESSAGE method	187
A.2.2.4.8	NOTIFY method	193
A.2.2.4.9	OPTIONS method	199
A.2.2.4.10	PRACK method	206
A.2.2.4.11	REFER method	212
A.2.2.4.12	REGISTER method	219
A.2.2.4.13	SUBSCRIBE method	226
A.2.2.4.14	UPDATE method	233
A.3	Profile definition for the Session Description Protocol as used in the present document	238
A.3.1	Introduction	238
A.3.2	User agent role	238
A.3.2.1	Major capabilities	239
A.3.2.2	SDP types	239
A.3.2.3	SDP types parameters	240
A.3.2.4	SDP types parameters within attribute lines	242
A.3.3	Proxy role	242
A.3.3.1	Major capabilities	243
A.3.3.2	SDP types	243
A.3.3.3	SDP types parameters	244
A.3.3.4	SDP types parameters within attribute lines	246
A.4	Profile definition for other message bodies as used in the present document	246
Annex B (informative):	Change history	247

- 3) use as encrypted string the user part of the NAI which follows the sent-protocol (for Via Headers, e.g. "SIP/2.0/UDP") or the URI scheme (for Route and Record-Route Headers, e.g. "sip:");
- 4) replace all content of the received header which carries encrypted information with the entries resulting from decryption.

EXAMPLE: An encrypted entry to a Via header that looks like:

```
Via: SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net;lr,
SIP/2.0/UDP pcscf1.home1.net;lr)@home1.net;tokenized-by=home1.net
```

will be replaced with the following entries:

```
Via: SIP/2.0/UDP scscf1.home1.net;lr, SIP/2.0/UDP pcscf1.home1.net;lr
```

NOTE: Motivations for these decryption procedures are e.g. to allow the correct routing of a response through the hiding network, to enable loop avoidance within the hiding network, or to allow the entities of the hiding network to change their entries within e.g. the Record-Route header.

5.3.4 Void

5.4 Procedures at the S-CSCF

5.4.1 Registration and authentication

5.4.1.1 Introduction

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

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

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

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

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Unprotected REGISTER

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

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

Upon receipt of a REGISTER request with the integrity-protection parameter set to 'no', the S-CSCF shall:

- 1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;
- 2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;
- 3) select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14];

NOTE 3: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

- 4) store the icid parameter received in the P-Charging-Vector header;
- 5) challenge the user by generating a 401 (Unauthorized) response for the received REGISTER request, including a WWW-Authenticate header which transports:
 - the home network identification in the realm field;
 - the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;
 - the security mechanism, which is AKAv1-MD5, in the algorithm field;
 - the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2A.1); and
 - the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2A.1);
- 6) store the RAND parameter used in the 401 (Unauthorized) response for future use in case of a resynchronisation. If a stored RAND already exists in the S-CSCF, the S-CSCF shall overwrite the stored RAND with the RAND used in the most recent 401 (Unauthorized) response;
- 7) send the so generated 401 (Unauthorized) response towards the UE; and,
- 8) start timer reg-await-auth which guards the receipt of the next REGISTER request.

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

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the integrity-protection parameter in the Authorization header set to 'yes', the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

- 1) check if the user needs to be reauthenticated.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for registration requests received without integrity protection by the P-CSCF. The information that a REGISTER request was received integrity protected at the P-CSCF may be used as part of the decision to challenge the user.

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

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

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

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