

CSCF Mw Interface

Call Session Control Function

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2013–2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
2	Interface Overview	3
2.1	Interface Role	4
2.2	Services	4
2.3	Encapsulation and Addressing	5
3	Procedures	9
3.1	Lower-Level Procedures	12
3.2	Authentication	12
3.3	Registration	25
3.4	Standalone Request Procedures on Originating Side	32
3.5	Standalone Request Procedures on Terminating Side	38
3.6	INVITE Dialog Procedures on Originating Side	43
3.7	INVITE Dialog Procedures on Terminating Side	67
3.8	SUBSCRIBE Dialog	81
3.9	Network Monitoring	89
4	Information Model	91
4.1	Supported SIP Methods	91
4.2	Status Codes Generated by CSCF	92
4.3	Header Information in Requests, Common for Many Services	93
4.4	Header Information in Responses, Common for Many Services	95
4.5	Supported SIP Headers Within SIP Methods	95
5	Formal Syntax	171
6	Security Considerations	173
6.1	IPsec Tunnel	173
7	Related Standards	175
8	Example of XML Document Sent in NOTIFY	179





1 Introduction

This document describes the interface between the Call Session Control Function (CSCF), including the Breakout Gateway Control Function (BGCF), and several SIP-based nodes using the reference points Mg, Mj, Mk, Mm/Mx, Mr, Mw, and I2, see Section 2 on page 3.

Unless otherwise indicated, Session Initiation Protocol (SIP) headers are handled transparently by the CSCF/BGCF in the SIP interfaces outlined by this document.





2 Interface Overview

This section describes the interfaces to the CSCF and a BGCF as shown in Figure 1.

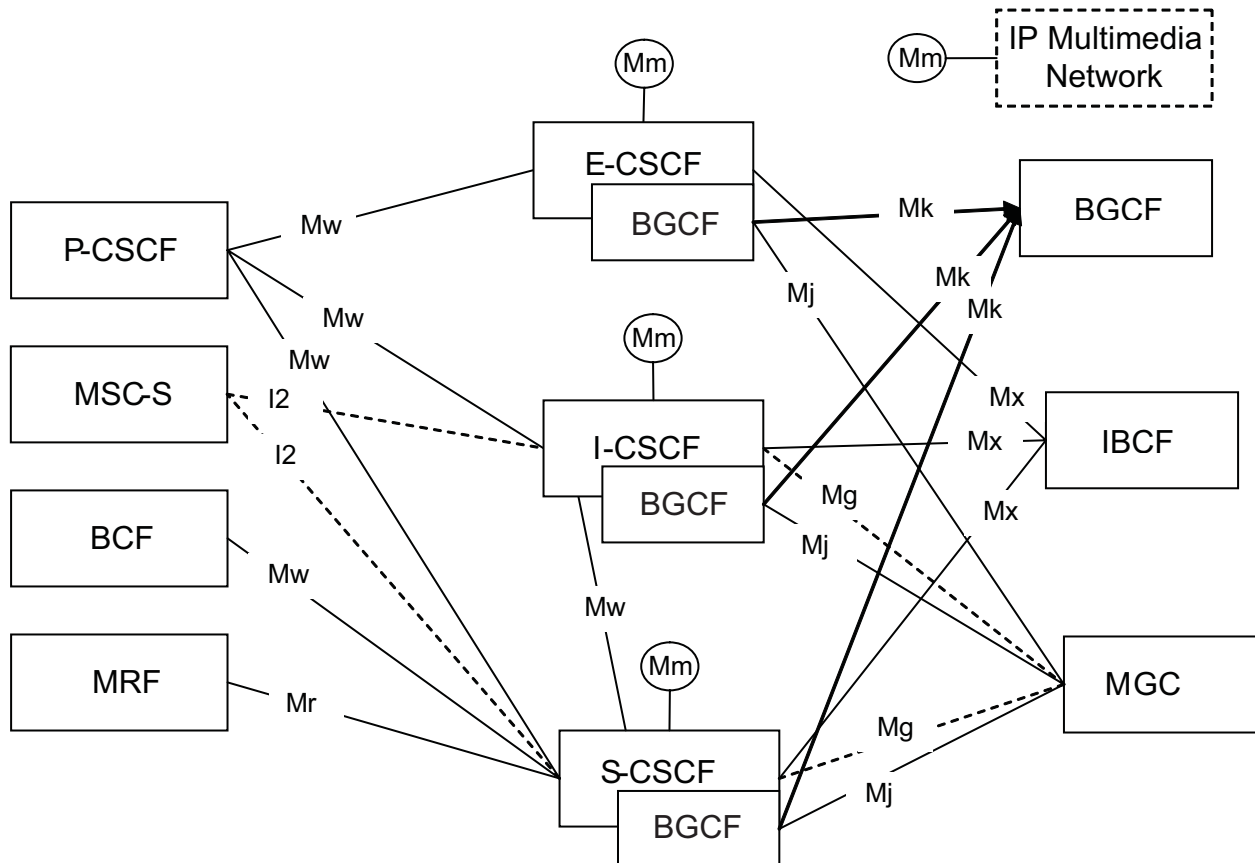


Figure 1 Interface Entities

The Mw interface is between the following nodes:

- P-CSCF and I-CSCF
- P-CSCF and S-CSCF
- P-CSCF and E-CSCF
- I-CSCF and S-CSCF
- BCF and S-CSCF

The Mj interface is between the BGCF and the MGC. The BGCF function is always collocated with the Serving Call Session Control Function (S-CSCF),



Interrogating Call Session Control Function (I-CSCF), or the Emergency Call Session Control Function (E-CSCF). The BGCF is not externally addressable.

The Mk interface is between BGCF and an external BGCF, this means that it is possible to address another BGCF but it is not possible to be addressed as a BGCF.

The Mr interface is between the S-CSCF and the Media Resource Function (MRF).

The Mg interface is between the I- and S-CSCF and the Media Gateway Controller (MGC).

The Mm interface is between E-, I-, and S-CSCF and IP Multimedia Network.

The Mx interface is between E-, I-, and S-CSCF and Interconnection Border Control Function (IBCF).

The I2 interface is between the Mobile Switching Center (MSC) Server and the I-CSCF and S-CSCF.

The protocol used on the interfaces is the SIP protocol.

2.1 Interface Role

The CSCF is a common name for all the interface roles. This document describes the Mg, Mj, Mk, Mm/Mx, Mr, Mw, and the I2 interface for the CSCF.

2.2 Services

This section describes the services the CSCF offers and uses in Mg, Mj, Mk, Mm/Mx, Mr, Mw, and I2.

The services offered by the CSCF are listed in Table 1.

Table 1 Offered Services

Offered Service	Description
Authentication	Authentication is not a standalone service. Authentication is a security mechanism that can be performed in connection to other service uses.
Registration	The CSCF offers registration, reregistration, deregistration, and requesting a list of contacts.



Offered Service	Description
Standalone request procedures on the originating side	The CSCF transfers standalone SIP requests and responses on the originating side.
Standalone request procedures on the terminating side	The CSCF transfers standalone SIP requests and responses on the terminating side.
INVITE dialog procedures on the originating side	The CSCF offers setting up of an INVITE dialog, sending of requests within the dialog, and termination of a dialog on the originating side.
INVITE dialog procedures on the terminating side	The CSCF offers setting up of an INVITE dialog on the terminating side and sending and receiving requests and termination of the dialog.
SUBSCRIBE dialog	The CSCF offers setting up of a SUBSCRIBE dialog and sending requests within the dialog.
Network monitoring	The CSCF offers network monitoring of unreachable SIP interfaces by sending of SIP OPTIONS requests.
Proxy	The CSCF proxies all unknown headers received transparently.
SIP Overload Control	The CSCF offers SIP overload control for communicating overload information between SIP servers and clients so that clients can reduce the amount of traffic sent to overloaded servers.

The user services offered by the Mw/Mj/I2 are listed in Table 2.

Table 2 Used Services

Used Service	Description
Not applicable	

2.3 Encapsulation and Addressing

The Proxy Call Session Control Function (P-CSCF), and Break-in Control Function (BCF) support IPv4 and SIP on User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

The S-CSCF, I-CSCF, E-CSCF, and BGCF support an IPv4/IPv6 dual stack and SIP on UDP and TCP.

The CSCF terminates a TCP connection after a configurable time of inactivity.

The CSCF follows the procedures for SIP routing as specified in [RFC 3261 SIP: Session Initiation Protocol](#) and [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#) with the clarifications given in the following subsections.

The CSCF inserts its address in the `Record-Route` header of the SIP requests for methods initiating a dialog (`SUBSCRIBE` and `INVITE`). The CSCF uses loose routing as defined in [RFC 3261 SIP: Session Initiation Protocol](#).

The S-CSCF can be configured not to `Record-Route` `SUBSCRIBE` requests.

The addresses of the P-CSCF, I-CSCF, and S-CSCF are obtained through Domain Name System Server (DNS) lookups.

DNS NAPTR, SRV, and A Resource Record queries are done according to [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#) as needed by the P-CSCF, I-CSCF, and the S-CSCF.

The P-CSCF uses the route set created for the SIP dialog when sending a SIP request within the dialog.

The P-CSCF uses the route set received in the `Service-Route` header when sending initial or standalone SIP requests to the CSCF.

The S-CSCF uses the route set received in the `Path` header when sending initial or standalone SIP requests to the P-CSCF.

2.3.1 Number Internationalization

The sender of a SIP initial request addresses the destination using dialed information, for example, +46 (8) 719 7378.

The digits are transported as a telephone number in a SIP URI or in a tel URI.

The User Equipment (UE) must include a phone-context parameter if the telephone number is not fully international (global). The phone-context can be set to the home domain name of the user.

```
tel:7197999;phone-context=ims.mnc015.mcc235.3gppnetworks.org
```

If the telephone number is transported in a SIP URI, a user parameter must be included (`user=phone`). The domain name of the SIP URI indicates the home domain name that is responsible to resolve the phone number to a SIP URI that is routable.

```
sip:7197999;phonecontext= =>  
ims.mnc015.mcc235.3gppnetworks.org@ims.mnc015.mcc2 =>  
35.3gppnetworks.org;user=phone
```



It is recommended however that the UE uses tel URIs for telephone numbers.

In either case the format of the dialed information can be as follows:

- The international format, for example, +46(8)7197378
- The national format, for example, 08-7197378
- The local format, for example, 7197378

On reception of dialed information, the CSCF reformats the digits to be in the international format based on configured parameters.

Note: Some special (preconfigured) numbers are not internationalized.

2.3.2 Forking

On reception of an initial or standalone SIP request to be terminated to a served user, and where more than one contact address is registered, the SIP request is sent to all the registered contacts. Each contact is assigned a priority determined by the `q-value` and the `Qa` value. The `q-value` is received during initial registration and reregistration. The `Qa` value is calculated by the Caller Preferences function per initial request as in the [RFC 3261 SIP: Session Initiation Protocol](#) and [RFC 3841 Caller Preferences for the Session Initiation Protocol \(SIP\)](#) specifications.

On reception of a SIP provisional response, except for the SIP 100 (Trying) response, from the remote users, the CSCF forwards the provisional response to the previous hop.

On reception of a SIP 2xx response from the remote users, the response is sent to the previous hop. For non-INVITE requests, only one 2xx is sent to the previous hop.

2.3.3 Illegal Character Handling

According to [RFC 3261 SIP: Session Initiation Protocol](#), the characters “#”, “[”, “]”, “\”, “^”, “{”, “|”, and “}” are considered invalid in the user part of the SIP URI in the SIP request. The CSCF uses, depending on the configuration, one of following mechanisms:

- Rejected. SIP requests containing any of the invalid characters are rejected with status code 400 (Bad Request). This is the default behavior.
- Escaped. Illegal characters are escaped to %HexHex, for example, “#” is replaced by “%23”
- No specific rule. The illegal characters are allowed and can either be escaped or not.



3 Procedures

This section describes the most common signaling sequences.

The sequence for user registration is shown in Figure 2. The dotted arrows are used at digest authentication procedure at initial registration. The sequence without the dotted arrows is valid for initial registration without digest authentication and for successful reregistrations, deregistrations, and reading of registration information.

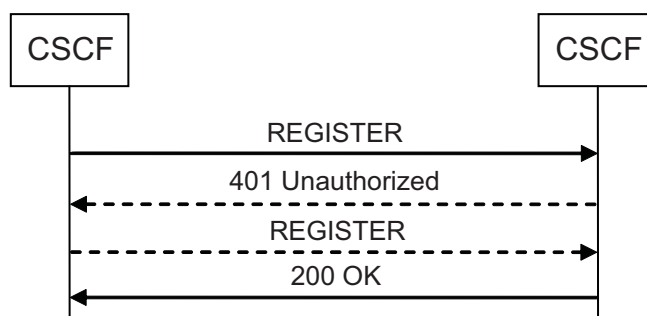


Figure 2 Digest, Challenged NBA, or AKA Authentication Procedure at Registration

The sequence when UE initiates an `INVITE` session is shown in Figure 3. Dotted lines are valid at authentication.

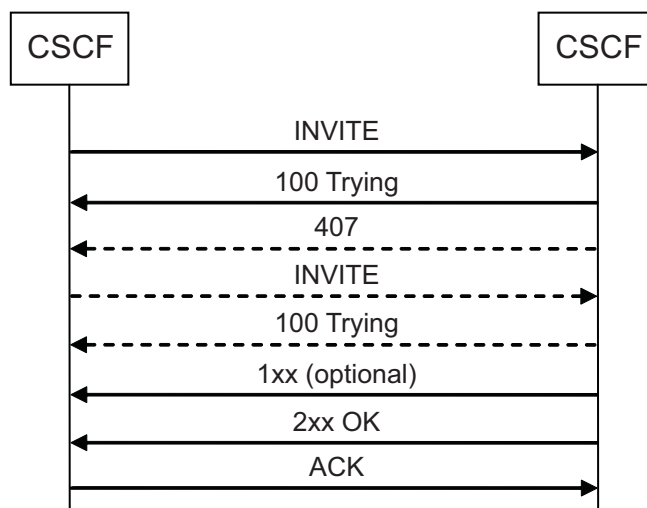


Figure 3 Initiating an `INVITE` Session

The sequence when the CSCF sends or receives a subsequent request within a dialog is shown in Figure 4.

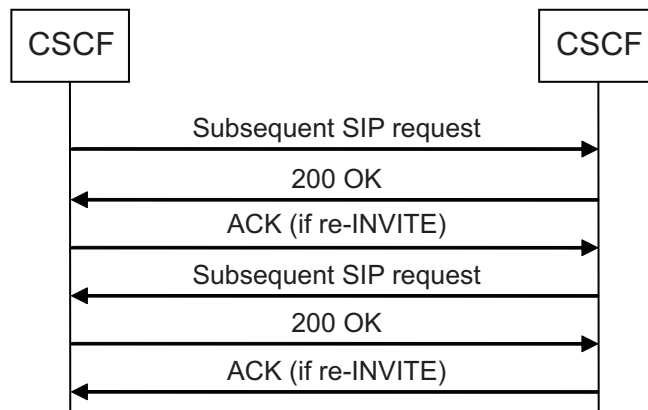


Figure 4 Subsequent Request within an INVITE Dialog

The sequence when the UE initiates a termination of the `INVITE` dialog is shown in Figure 5.

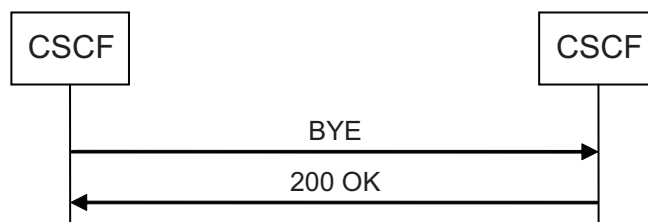


Figure 5 Termination of Session

The sequence when the UE initiates a `SUBSCRIBE` dialog is shown in Figure 6. The sequence is also valid when the UE refreshes the subscription or requests a termination of the `SUBSCRIBE` dialog.

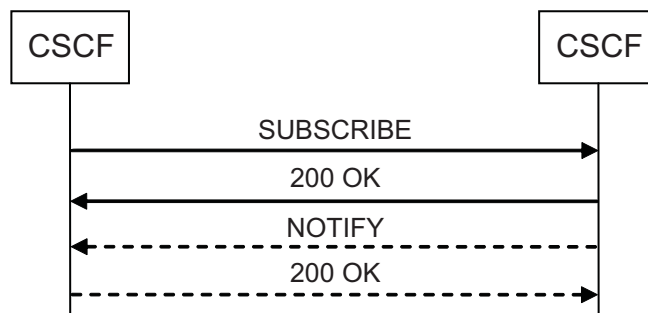


Figure 6 Initiating a SUBSCRIBE Dialog

The sequence when the CSCF sends and receives a standalone request is shown in Figure 7.

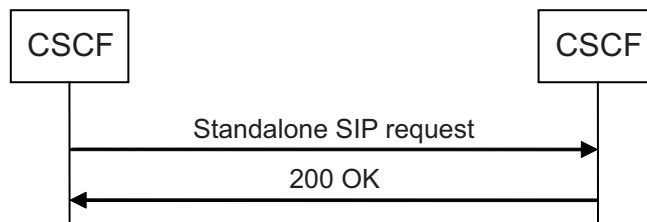


Figure 7 Sending a Standalone SIP Request

The sequence when initiating an `INVITE` session to an External Network is shown in Figure 8.

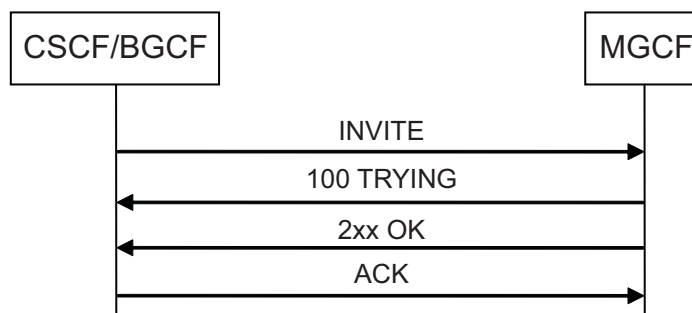


Figure 8 Initiating an `INVITE` Session to an External Network

The sequence when sending a standalone request to an External Network is shown in Figure 9.

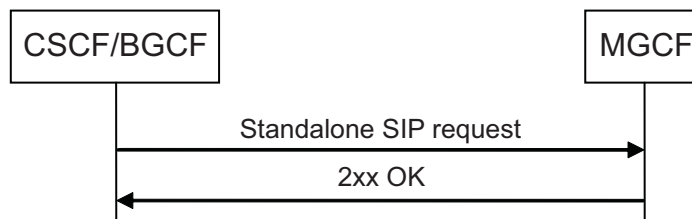


Figure 9 Standalone Request to an External Network

The sequence when I-CSCF/S-CSCF/BGCF redirects a request is shown in Figure 10.

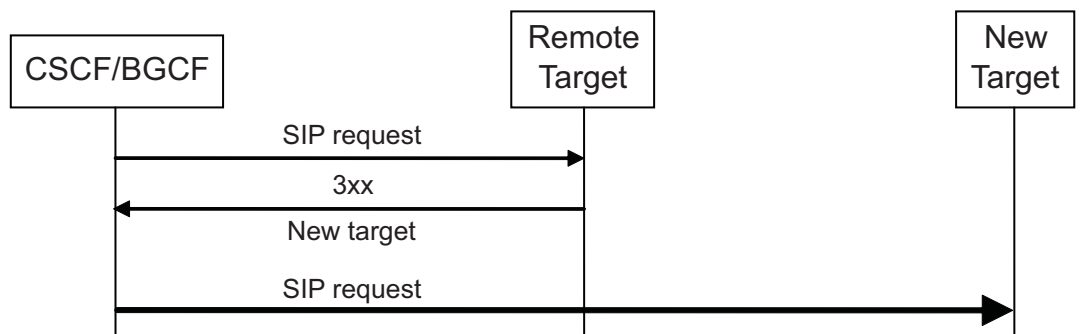


Figure 10 I-CSCF/S-CSCF/BGCF Redirects a Request

3.1 Lower-Level Procedures

3.1.1 Session Timer Procedure

The CSCF supports session timers [RFC 4028 Session Timers in the Session Initiation Protocol \(SIP\)](#) with the following clarifications.

A session is supervised by the CSCF if at least one of the UEs supports session timer.

The CSCF can add a `Session-Expires` header and `Min-SE` header to the message. The CSCF can decrease the value in `Session-Expires` header.

If the `Session-Expires` header is present in the message and the `Session-Expires` value is less than minimum allowed value, the CSCF rejects the `INVITE` by sending 422 response message. The CSCF includes the `Min-SE` header in the response message, which includes the minimum allowed `Session-Expires` value.

3.2 Authentication

The CSCF supports several authentication mechanisms as follows:

- Digest authentication
- GPRS IMS Bundled Authentication (GIBA)
- IMS AKA authentication
- NASS Bundled Authentication (NBA)

With digest authentication, the CSCF requests Home Subscriber Server (HSS) for the Authentication Vectors for digest and uses the vectors to challenge the user with a 401 response.

With GIBA, the S-CSCF compares the UE IP address received in `REGISTER` message to the UE IP address received from the HSS. No challenge is sent to the UE.

With IMS AKA authentication, IPsec is established and no messages other than `REGISTER` are authenticated explicitly, for example, when challenged by 401/407 response.

With NBA authentication, UE is authenticated using information in the `P-Access-Network-Info` header.

The CSCF can authenticate a subsequent SIP request depending on configurable settings within the CSCF. The CSCF can be configured to authenticate any subsequent SIP request except for the `SIP CANCEL` and `ACK` requests. The `SIP CANCEL` and `ACK` request are never authenticated.



3.2.1 Digest

This section describes the Digest procedures between the UE and the CSCF.

3.2.1.1 Initial Registration

At initial registration, the sequence shown in Figure 2 is valid.

3.2.1.1.1 Initial REGISTER

The P-CSCF sends the SIP REGISTER request through I-CSCF to the S-CSCF containing information in the Authorization header as follows:

- 1 username with the Private User Identity
- 2 realm with the home domain name
- 3 nonce with the empty value
- 4 uri with the Request-URI in this SIP REGISTER request
- 5 response with the empty value

3.2.1.1.2 SIP 401 Response

The S-CSCF sends a SIP 401 (Unauthorized) response with the WWW-Authentication header indicating Digest in the authentication scheme token.

- 1 The WWW-Authenticate header includes the following parameters:
 - Digest as the authentication scheme
 - realm with the operator domain name
 - nonce with a value that is stored by the UE
 - qop with the protection value auth
 - domain SIP URI that identifies the protection domain⁽¹⁾
- 2 The WWW-Authenticate header can include the following parameters:
 - opaque
 - stale indicating if the nonce is stale (TRUE) or not (FALSE)
 - algorithm with the value of MD5

(1) The domain parameter is sent as it is received from HSS: empty or populated with configured value in HSS.

3.2.1.1.3 Subsequent Initial REGISTER

The P-CSCF responds to the challenge with a Digest response. The P-CSCF sends the SIP REGISTER request to the CSCF with an Authorization header. The Authorization header must include the following parameters:

- Digest as the authentication scheme
- username with the Private User Identity
- realm with the stored value of the realm field
- nonce with the stored value of the nonce field
- uri with the Request-URI header in the SIP request
- response with the result of the MD5 hash algorithm
- cnonce with a value generated by the UE
- qop with the stored value of the qop field, that is, the selected quality of protection mode from the modes received in the WWW-Authentication header
- nc with an initial value
- Optionally, the stored value of the opaque field, If received earlier in the WWW-Authenticate header
- Optionally, integrity-protected with value ip-assoc-pending when supporting digest authentication as per 3GPP® specification

3.2.1.1.4 Successful SIP Response

The CSCF validates the Authorization header and if the validation is successful, it sends the SIP 200 (OK) response. The SIP 200 (OK) response can include the Authentication-Info header, and if included the header contains the nextnonce parameter.

3.2.1.2 ReRegistration, Deregistration, and Registration Query

At reregistration, deregistration, and registration query, the sequence shown in Figure 2 is valid.

The P-CSCF sends the SIP REGISTER request through the I-CSCF to the S-CSCF with an Authorization header. The Authorization header includes the parameters shown in Section 3.2.1.1.3 Subsequent Initial REGISTER on page 14. In addition, when supporting digest authentication as per 3GPP specification, the integrity-protected parameter is sent with value ip-assoc-yes.



The S-CSCF validates the `Authorization` header and if the validation is successful, then the S-CSCF sends the SIP 200 (OK) response. The SIP 200 (OK) response can include the `Authentication-Info` header, and if included the header contains the `nextnonce` parameter.

3.2.1.3 Other SIP-Related Procedures

The S-CSCF can authenticate the user sending a SIP request depending on configurable settings in the S-CSCF. The S-CSCF can be configured to authenticate any SIP request except for the SIP `CANCEL` and `ACK` requests.

The S-CSCF can, for example, if the `nonce` value is no longer valid, challenge any SIP request, except `CANCEL` and `ACK`, even if the request included valid credentials.

When the P-CSCF sends a SIP request to the S-CSCF, it must include the `Proxy-Authorization` header with the parameters shown in Section 3.2.1.1.3 Subsequent Initial REGISTER on page 14.

If the S-CSCF based on the local policy chooses to authenticate the SIP request, the S-CSCF validates the `Proxy-Authorization` header and if the validation is successful, continue processing as defined in the applicable SIP procedure.

3.2.2 GPRS IMS Bundled Authentication

The GPRS IMS Bundled Authentication (GIBA) is described in this section.

3.2.2.1 Initial Registration

The P-CSCF sends the initial SIP `REGISTER` request through the I-CSCF to the S-CSCF. No `Authorization` header must be included by the UE in the SIP `REGISTER` message.

The S-CSCF uses the `To` header as the Public User Identity.

The S-CSCF validates the received IP address against the UE IP address received from the HSS. If the validation is successful, then the S-CSCF sends the SIP 200 (OK) response.

3.2.2.2 Reregistration, Deregistration, and Other Traffic Procedures

The P-CSCF sends the SIP request to the S-CSCF. No `Authorization` or `Proxy-Authorization` header is included by the UE.

The S-CSCF authenticates all SIP requests related to reregistration, deregistration, and other SIP-related procedures by comparing the received `Via` set against the `Via` set stored at initial registration. The authentication of the user is successful if the `Via` sets match. The authentication of the user is

also successful for a reregistration when the `Via` sets do not match, but the received UE IP address matches the UE IP address stored at initial registration. The S-CSCF sends the SIP 200 (OK) response if the authentication is successful.

3.2.3 IMS AKA Authentication

This section describes the procedure for authenticating users using the IMS AKA authentication described in the following specifications:

- [3GPP TS 33.203 3G security; Access security for IP-based services](#)
- [RFC 2617 HTTP Authentication: Basic and Digest Access Authentication](#)
- [RFC 3310 Hypertext Transfer Protocol \(HTTP\) Digest Authentication Using Authentication and Key Agreement \(AKA\)](#)

With the modifications and clarifications in the following subsections. A SIP REGISTER request can be challenged by the S-CSCF where IMS AKA authentication is used.

3.2.3.1 Initial Registration Procedure Using IMS AKA Authentication

This section describes the IMS AKA-related procedure during initial registration.

Note: This section focuses on the authentication. The initial registration procedure is described in Section 3.3 Registration on page 25 and is shown in Figure 11.

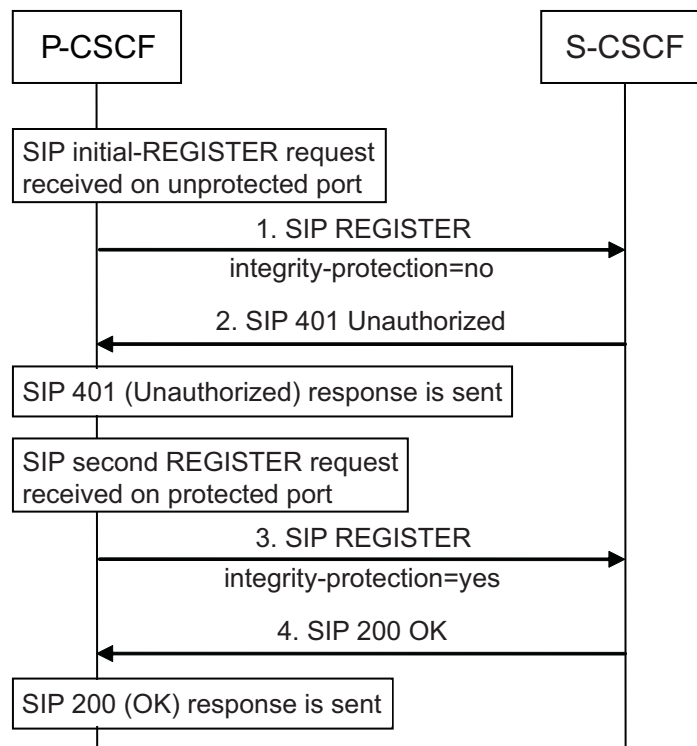


Figure 11 Digest Procedure during Initial Registration

- 1 The P-CSCF sends the REGISTER request from the UE to the S-CSCF through the I-CSCF. The SIP REGISTER request from the UE must include an Authorization header with the following information:
 - username with the Private User Identity
 - realm with the home domain name
 - nonce with the empty value ""
 - uri with the Request-URI in this SIP REGISTER request
 - response with the empty value ""
 - algorithm with value ""(optional)
 - integrity-protected with value no if the request was received at the P-CSCF unprotected
- 2 The AV, except XRES parameter, is sent down to the P-CSCF in 401 (Unauthorized). In IMS AKA, where Digest-AKA is used, the values of the AV are mapped on to the existing parameters of HTTP-Digest Authenticate headers according to specification [RFC 3310 Hypertext Transfer Protocol \(HTTP\) Digest Authentication Using Authentication and Key Agreement \(AKA\)](#).

[RFC 3310 Hypertext Transfer Protocol \(HTTP\) Digest Authentication Using Authentication and Key Agreement \(AKA\)](#) replaces [RFC 2617 HTTP Authentication: Basic and Digest Access Authentication](#) in certain points, concerning IMS AKA. One of these points is the nonce parameter. In IMS AKA nonce is a base64 encoding of concatenation of RAND, AUTN and arbitrary server parameters. No server parameters are currently envisioned to be used.

The keys for IPsec are delivered in the new parameters ik and ck. The algorithm string is assigned the value AKAv1-MD5.

The WWW-Authenticate header includes the following parameters:

- Digest as the authentication scheme
- realm with the operator domain name
- nonce with a base64 encoding to concatenation of RAND and AUTN
- algorithm with value AKAv1-MD5
- qop with the single value of auth

The WWW-Authenticate header can include the following parameters:

- opaque
- ik with Integrity Key, a 128-bit length key. This is to be used for integrity protecting IP packets (password protected CRC). This field is included if integrity protection is required (integrity-protected="no")
- ck with cipher key, an encryption key (length 128 bits). This is used for encrypting payload of IP packets. This field is included if integrity protection is required (integrityprotected="no").



- 3 The UE responds to the challenge with a Digest response and the SIP REGISTER must include an Authorization header. The Authorization header sent by the P-CSCF must include the following parameters:
 - Digest as the authentication scheme
 - username with the Private User Identity
 - realm with the realm value from the WWW-Authenticate header
 - nonce with the nonce value from the WWW-Authenticate header
 - uri with the Request-URI header in the SIP REGISTER request
 - response with the result of the MD5 hash algorithm, presented as a sequence of 32 hexadecimal digits
 - Optionally, the stored value of the opaque field, If received earlier in the WWW-Authenticate header
 - algorithm with value AKAv1-MD5
 - integrity-protected with value yes
 - qop with the value selected from the list sent in WWWAuthenticate, currently auth only
 - cnonce is UE generated quoted random string
 - nc with counter of how many times the nonce has been used
- 4 The S-CSCF validates the Authorization header and if the validation is successful, it sends the SIP 200 (OK) response.

3.2.3.2 Re-Authenticated Reregistration Using IMS AKA Authentication

This use case is the same as the previous one, Initial Registration Procedure using IMS AKA Authentication, except that the authentication is triggered by internal CSCF rules, rather than integrity-protected is being equal to no.

Where authentication is activated despite integrity protection, is shown in Figure 12.

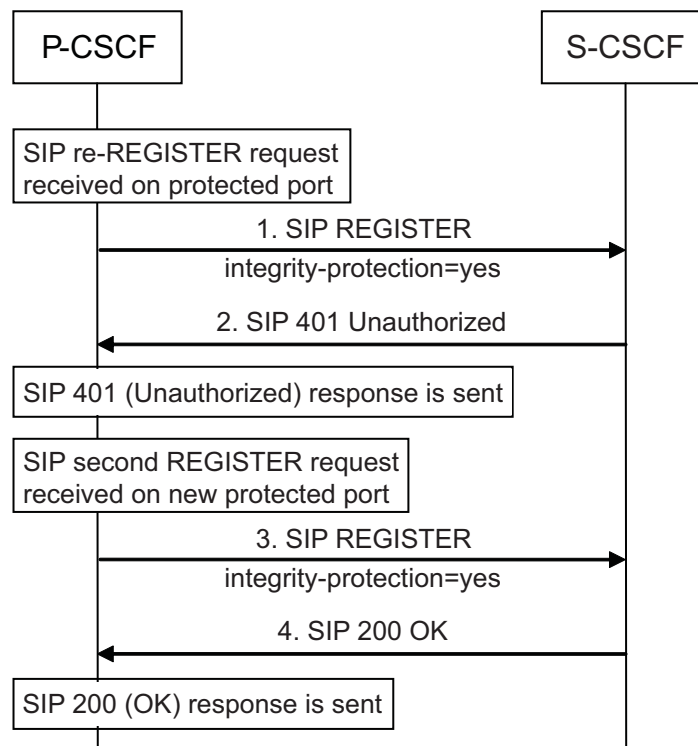


Figure 12 Authenticated Reregistration

3.2.3.3

Resynchronization Using IMS AKA Authentication

If S-CSCF discovers `auts` parameter in `Authorization` header of `REGISTER` whether integrity protected, the S-CSCF abandons the ongoing authentication round and requests a new Authentication Vector (AV). S-CSCF provides the received `auts` value to AuC in the call for the new AV.

The only specific for this use case is the `auts` parameter in `Authorization` header in `REGISTER` in step 3, as shown in Figure 13.

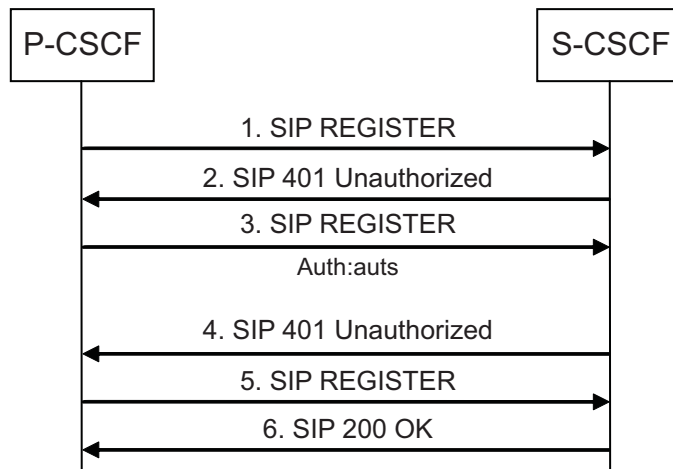


Figure 13 Resynchronization

The `Authorization` header must include the following parameters:

- 1 `Digest` as the authentication scheme
- 2 `username` with the Private User Identity
- 3 `realm` with the `realm` value from the `WWW-Authenticate` header
- 4 `nonce` with the `nonce` value from the `WWW-Authenticate` header
- 5 `uri` with the `Request-URI` header in the `SIP REGISTER` request
- 6 `response` with the result of the MD5 hash algorithm, presented as a sequence of 32 hexadecimal digits. For the resync case, this value is calculated with the empty string as the password.
- 7 `auts` with base64 encoding of the AUTS as defined in TS33.102
- 8 Optionally, the stored value of the `opaque` field, if received earlier in the `WWW-Authenticate` header
- 9 `algorithm` with value `AKAv1-MD5`
- 10 `integrity-protected` with value `yes` or `no`
- 11 `qop` with the value selected from the list sent in `WWWAuthenticate`, currently `auth` only
- 12 `cnonce` is UE generated quoted random string
- 13 `nc` with counter of how many times the nonce has been used

3.2.3.4 Reregistration, Reading Registration Information, and Deregistration Procedure Using IMS AKA Authentication

This section describes the normal IMS AKA-related procedure during reregistration and the deregistration procedures.

Note: This section focuses on authentication. The reregistration and deregistration procedure is described in Section 3.3 Registration on page 25 and is shown in Figure 14.

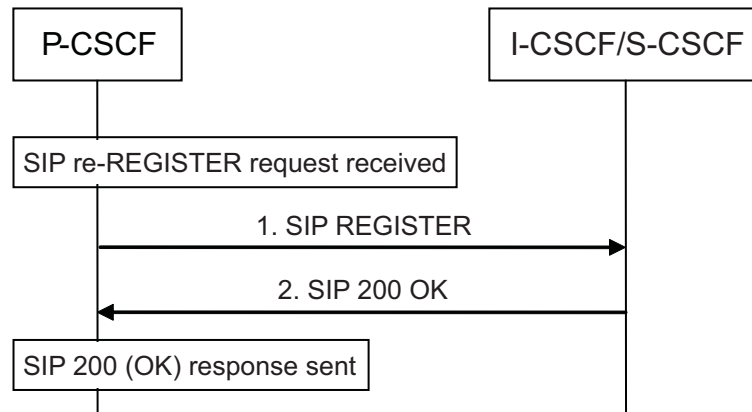


Figure 14 Digest Procedure, Reregistration

The P-CSCF sends the `REGISTER` request from the UE to the S-CSCF. The `SIP REGISTER` request from the UE includes an `Authorization` header with the following information:

- 1 Digest as the authentication scheme
- 2 username with the Private User Identity
- 3 realm with the value of the `realm` field from the latest challenge
- 4 nonce with the value of the `nonce` field from the latest challenge
- 5 uri with the `Request-URI` header in this `SIP REGISTER` request
- 6 response with the result of the MD5 hash algorithm, presented as a sequence of 32 hexadecimal digits
- 7 The stored value of the `opaque` field, If received earlier in the latest challenge
- 8 algorithm with value `AKAv1-MD5`

The S-CSCF validates the `Authorization` header and if the validation is successful, then the CSCF sends the `SIP 200 (OK)` response.

3.2.4 NASS Bundled Authentication

This section describes the NASS Bundled Authentication (NBA) procedures between the UE and the CSCF.

3.2.4.1 Initial Registration

The P-CSCF sends the initial `SIP REGISTER` request through the I-CSCF to the S-CSCF including the `P-Access-Network Info` header. No



`Authorization` header needs to be included. The Public User Identity must be set in the `To` and `From` headers.

The S-CSCF evaluates the `access-type` parameter in the `P-Access-Network-Info` header to find out if NASS Bundled Authentication is applicable.

The S-CSCF evaluates the `dsl-location` parameter in the `P-Access-Network-Info` header and the `Line-identifier` AVP provided by the HSS to authenticate the user.

3.2.4.2 Reregistration, Deregistration, and Other Traffic Procedures

The P-CSCF sends the SIP request to the S-CSCF. No `Authorization` or `Proxy- Authorization` header needs to be included by the UE.

The S-CSCF authenticates all SIP requests related to reregistration, deregistration, and other originating SIP-related procedures by comparing the received contact data (`Via` set, SIP Instance indicator, and Contact URI) to the contact data stored at initial registration. The authentication of the user is successful if the contact data matches.

The S-CSCF continues normal processing of the received SIP procedure after a successful authentication.

3.2.4.3 Challenged NBA

Upon reception of an initial registration request and if Challenged NBA is enabled, a challenge, in the form of a `401 (Unauthorized)`, is sent to the UE after the NBA procedure is successful. The UE is to respond to the challenge by resending the request with the same nonce included in the `Authorization` header.

The challenge is sent with the `WWW-Authenticate` header including the following parameters:

- `Digest` as the authentication scheme
- `realm = value of ScscfSipDigestAuthenticationRealm parameter or ericsson.se`
- `nonce = value generated by the S-CSCF`
- `qop = auth`
- `algorithm = MD5`
- `stale = TRUE`

After the initial registration, if the Challenged NBA is enabled, and after the contact data matching is successful, following procedure is followed.

Upon reception of a REGISTER request with a nonce and a nonce-count included in the Authorization header, if the nonce received matches the nonce stored in the initial registration, and if the nonce-count received equals to or is greater than the nonce-count stored, the challenged NBA authentication is considered successful, and the request is accepted.

Upon reception of an INVITE request with a nonce and a nonce-count included in the Proxy-Authorization header, if the nonce received matches the nonce stored in the initial registration, and if the nonce-count received equals to or is greater than the nonce-count stored, the challenged NBA authentication is considered successful, and the request is accepted.

Upon reception of a nonce, either in the Authorization header from a REGISTER request, or in the Proxy-Authorization header from INVITE request, if the nonce received matches the nonce stored in the initial registration, and if the nonce-count received equals or is greater than the nonce-count stored, but the stored nonce is expired (the expiration time of the stored nonce can be configured in `cscfNbaChallengeAuthenticationNonceTimeLength`), the challenged NBA authentication is considered successful, the request is accepted, a new nonce is generated and sent to the UE in the next nonce directive of Authentication-Info header in the 2xx response.

Upon reception of a request in any other scenarios, including there is no nonce received, or the received nonce does not match the nonce stored, or the received nonce-count is less than the nonce-count stored, a challenge is sent to the UE as follows:

- For a REGISTER request, a challenge is sent to UE in 401 (Unauthorized) response, in which a generated nonce is included in the WWW-Authenticate header.
- For an INVITE request, a challenge is sent to the UE in 407 (Proxy Authentication Required) response, in which a generated nonce is included in the Proxy-Authenticate header.

The UE responds to the challenge by resending the request with the same nonce included in the Authorization header or the Proxy-Authorization header.

The S-CSCF continues normal processing of the received SIP procedure after a successful challenge.

3.2.5

Unsuccessful Cases at Authentication

If the S-CSCF authenticates the SIP request and the authentication fails, the S-CSCF generates a final response with a Status Code and text as defined in the references [RFC 2617 HTTP Authentication: Basic and Digest Access Authentication](#) and [RFC 3261 SIP: Session Initiation Protocol](#). For digest authentication, the UE also checks the `stale` parameter in the



`WWW-Authenticate` header. If the value is `True`, the UE can recalculate the credentials and resubmit the request.

The status codes and reason phrases the S-CSCF can generate as the result of an unsuccessful authentication procedure, are listed in the *CSCF Fault Codes Catalogue*.

3.3 Registration

Registration includes procedures for the following:

- Initial registration
- Reregistration
- Deregistration
- Querying registration information

The security aspect of the registration and deregistration is described in Section 3.2 Authentication on page 12.

The signaling sequence for registration is shown in Figure 2.

The registration is regarded as an initial registration when the Public User Identity is not registered in the CSCF or when a new contact is added.

A registration is regarded as a reregistration when the registration period is refreshed for an already registered contact to the Public User Identity in the CSCF.

At deregistration an `Expires` header, or the `Expires` parameter within the `Contact` header is set to the value of 0. The registered contact is removed from the CSCF.

At querying registration information, the `Contact` header is absent. The CSCF returns the list of currently registered contacts for the user.

The status codes and reason phrases the CSCF can generate, are listed in the *CSCF Fault Codes Catalogue*.

3.3.1 Signaling Parameters

This section shows a Table of Contents of the SIP `REGISTER` requests and SIP responses to the SIP `REGISTER` request. Each table contains a description of the SIP header fields, parameters, and values necessary for the S-CSCF and the P-CSCF to interoperate.

3.3.1.1

SIP REGISTER Request

The SIP REGISTER request must include at least the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include parameters defined by relevant extensions to the RFC as clarified in this section. The SIP REGISTER request sent by the P-CSCF and I-CSCF is listed in Table 3.

Table 3 SIP REGISTER Request Sent by P-CSCF and I-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	SIP URI with the Home domain name
To	M	SIP URI with the Public User Identity
From	M	The same Public User Identity as in the To header.
Call-ID	M	The Call-ID must be the same for a registration cycle (from initial registration to deregistration).
Contact	M	<p>Includes one or more contact addresses. Each contact address:</p> <ul style="list-style-type: none"> • Must include an IP address or hostname⁽¹⁾ of the UE in the form of a SIP URI. • Can include feature tags and parameters as described by RFC 3840 Indicating User Agent Capabilities in the Session Initiation Protocol (SIP). • Can include an expiry value as defined by RFC 3261 SIP: Session Initiation Protocol. • Can include an sos parameter as defined by 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) to indicate emergency registration in the first Contact header. • Can include a URI parameter “bnc” as defined by RFC 6140 Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP). • Can include +sip.instance feature tag as defined by RFC 5626 Managing Client-Initiated Connections in the Session Initiation Protocol (SIP).
Via	M	See Table 58.



Header	Status	Procedure-Specific Values of the Parameter
Route	O	When the Reregistration With HSS Bypass feature is enabled, this header can include the <code>Service-Route</code> to indicate the current stored S-CSCF to the I-CSCF, making it possible to route the <code>re-REGISTER</code> request directly to the S-CSCF when the HSS inquiry fails because of HSS overloaded, no reply or if the inquiry is not sent because of throttling.
Authorization	O	<p>See Table 58.</p> <p>In the AKA case, the field integrity-protected must be included in <code>Authorization</code> header. It assumes the value of <code>no</code> or <code>yes</code>. Indicates whether this <code>REGISTER</code> request was received on protected P-CSCF interface or not.</p> <p>Can include <code>auts</code> parameter. For digest authentication without TLS, as specified in 3GPP Release 8 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), the field integrity-protected is included with the value of “ip-assoc-pending” or “ip-assoc-yes”.</p>
P-Access- -Network- Info	O	<p>For initial registration, S-CSCF uses this header to find out if NASS Bundled Authentication is applicable. If so, this header must include the parameters <code>access-type</code>, <code>network-provided</code>, and <code>dsl-location</code>.</p> <p>For NASS Bundled Authentication verification performed in the S-CSCF, the parameter <code>dsl-location</code> must contain the line-identity subparameter as the first subparameter or prefixed by “line-id=”.</p> <p>Other authentications schemes dependent the <code>PANI</code> header can have different formats for the <code>dsl-location</code>.</p>
Expires	O	See Table 58.
P-Visited- Network-ID	M	Includes a visited network identifier as defined by RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP) .
P-User- Database	O	See Table 58.
P-Charging- Vector	O	Includes the IMS Charging Identifier (ICID). The ICID is a globally unique value.
Resource- Priority ⁽²⁾	O	See Table 58.



Header	Status	Procedure-Specific Values of the Parameter
Require	O/C	<p>Optionally includes a <code>Timer</code> parameter as defined by RFC 4028 Session Timers in the Session Initiation Protocol (SIP).</p> <p>Optionally includes a <code>path</code> parameter as defined by RFC 3327 Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts.</p> <p>Optionally includes a <code>pref</code> parameter as defined by RFC 3840 Indicating User Agent Capabilities in the Session Initiation Protocol (SIP).</p> <p>Optionally includes a <code>gruu</code> parameter as defined by 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).</p> <p>Conditionally includes SIP Option Tag <code>gin</code> when <code>Contact</code> header includes URI parameter <code>bnc</code> to identify the extension that provides registration for Multiple Phone Numbers in SIP as defined by RFC 6140 Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP).</p>
Proxy-Require	O/C	<p>Optionally includes a <code>Timer</code> parameter as defined by RFC 4028 Session Timers in the Session Initiation Protocol (SIP).</p> <p>Optionally includes a <code>path</code> parameter as defined by RFC 3327 Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts.</p> <p>Optionally includes a <code>gruu</code> parameter as defined by 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).</p> <p>Conditionally includes SIP Option Tag <code>gin</code> when <code>Contact</code> header includes URI parameter <code>bnc</code> to identify the extension that provides registration for Multiple Phone Numbers in SIP as defined by RFC 6140 Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP).</p>

(1) It is possible to restrict the use of FQDN, see configuration parameter `ScscfRegistrationContactRestriction`.

(2) TSP-based P-CSCF does not send Resource-Priority.



3.3.1.2 SIP 401 (Unauthorized) Response

The S-CSCF sends this SIP response, to challenge the UE to provide credentials. The S-CSCF does not send this message when GIBA or NBA (non-challenged) is used. The 401 (Unauthorized) response includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and [RFC 2617 HTTP Authentication: Basic and Digest Access Authentication](#) as described in this section. The SIP 401 response is listed in Table 4.

Table 4 SIP 401 Response

Header	Status	Procedure-Specific Values of the Parameter
WWWAuthenticate	M	Includes the challenge as specified in Section 3.2.1 Digest on page 13 for digest authentication or Section 3.2.3 IMS AKA Authentication on page 16 for AKA authentication or Section 3.2.4 NASS Bundled Authentication on page 22 for Challenged NBA.

3.3.1.3 S-CSCF Generating a 305 Redirect Response

The SIP 305 (Use Proxy) response is returned by the S-CSCF when the S-CSCF fails to update the state of a user in the HSS because the HSS already has another serving the CSCF assigned for the user, that is, when the HSS returns the DIAMETER result code DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

The SIP 305 (Use Proxy) response includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and [RFC 2617 HTTP Authentication: Basic and Digest Access Authentication](#) as described in this section. The SIP 305 response is listed in Table 5.

Table 5 SIP 305 Use Proxy Sent by S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Contact	M	Contact header contains the currently assigned S-CSCF returned in the Cx error response from the HSS.

3.3.1.4 SIP 200 (OK) Response

The SIP 200 (OK) response is sent by the S-CSCF to confirm a successful initial registration, a successful reregistration, a successful deregistration, or a successful reading of registration information.

The SIP 200 (OK) response includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and [RFC 2617 HTTP Authentication: Basic and Digest Access Authentication](#) as described in this section. The SIP 200 responses are listed in Table 6.



Table 6 SIP 200 OK (REGISTER) Sent by S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Authentication-Info	O	See Table 59.
Service-Route	C	<p>A route set with addresses to the S-CSCF, containing an <code>orig</code> parameter.</p> <p>Conditionally for emergency registrations, the header is omitted if the configuration parameter <code>scscfEmergencyRegServiceRouteBehavior</code> is set to <code>EXCLUDE</code>.</p>
Contact	M	<p>Contact headers contain the following:</p> <ul style="list-style-type: none">• Currently registered contacts with Expires parameter indicating the contact expiration time for this Public User Identity. A registered contact includes feature tags as described in RFC 3840 Indicating User Agent Capabilities in the Session Initiation Protocol (SIP) if any feature tags have been associated to the contact in an earlier REGISTER request.• Deregistered contacts with Expires parameter value set to zero.• Can contain <code>+sip.instance</code> feature tag as defined by RFC 5626 Managing Client-Initiated Connections in the Session Initiation Protocol (SIP).• Can contain a public GRUU of the current registered contact as defined in RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) when GRUU is supported by CSCF and the REGISTER request includes <code>require="gruu"</code> and <code>+sip.instance</code> feature tag.
P-Associated-URI	O	<p>Includes one or more valid Public User Identities.</p> <p>Can contain one or more Wildcarded Public User Identities and can also contain <code>ServicePriorityLevel</code> per Public User Identity (see Section 4.5.26.14 P-Associated-URI on page 165 for more information on Service Priority Level within the P-Associated-URI).</p> <p>Header not included for Deregistration.</p>
P-Charging-Vector	O	Includes IMS Charging Identifier (ICID) as received from the P-CSCF.



Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Function-Addresses	O	P-Charging-Function-Addresses header transfers the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in the S-CSCF by the HSS.
Resource-Priority	O	See Table 59.

3.3.1.5

SIP REGISTER Request, Querying Registration Information

The P-CSCF sends this SIP REGISTER request when valid credentials are available and when reading register information.

Note: Querying of AKA contact is only allowed protected. Unprotected queries with `sec-agree` option tag in `Require` header are rejected. Unprotected queries without `sec-agree` result in the list of non-AKA contacts.

The SIP REGISTER request includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and relevant extensions to the RFC as described in this section. The SIP REGISTER Request, Querying Registration Information is listed in Table 7.

Table 7 SIP REGISTER Request, Querying Registration Information

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	SIP URI with the Home domain name.
To	M	SIP URI with the Public User Identity.
From	M	The same Public User Identity as in the To header.
Call-ID	M	The <code>Call-ID</code> must be the same as for initial registration.
Via	M	See Table 58.
Route	O	When the Reregistration With HSS Bypass feature is enabled, this header can include the <code>Service-Route</code> to indicate the current stored S-CSCF to the I-CSCF, making it possible to route the <code>re-REGISTER</code> request directly to the S-CSCF when the HSS inquiry fails because of HSS overloaded, no reply or if the inquiry is not sent because of throttling.
Authorization	O	See Table 58.
Expires	O	See Table 58.

Header	Status	Procedure-Specific Values of the Parameter
P-User-Database	O	See Table 58.
P-Charging-Vector	O	Includes the IMS Charging Identifier (ICID). The ICID is a globally unique value.
P-Visited-Network-ID	M	Includes a visited network identifier as defined by RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP) .

3.4 Standalone Request Procedures on Originating Side

This section describes the procedures the UE must use when sending a standalone SIP request.

A standalone SIP request is defined in this document as; a SIP request that does not create a dialog and is sent outside an existing dialog. In this document only the SIP methods MESSAGE, OPTIONS, PUBLISH, and REFER are defined as possible to send as standalone SIP requests but also other SIP methods are possible.

3.4.1 Preconditions

The inviting user is registered.

3.4.2 Send Standalone SIP Request

This section defines the procedure how the user successfully sends a standalone SIP request. For details about the unsuccessful cases, see Section 3.4.3 Unsuccessful Cases at Standalone Requests on page 37.

The procedure is initiated by a UE, as defined in [RFC 3261 SIP: Session Initiation Protocol](#) or other relevant extension to the RFC with the clarifications in this section.

The signaling sequence is shown in Figure 7.

When receiving a standalone SIP request from the UE, the P-CSCF will proxy the request to the S-CSCF and it must include the information listed in Table 8.

When receiving a standalone SIP request from an AS, the I-CSCF will proxy the request to the S-CSCF. If the received request contains a Route header with an orig parameter, the message sent from the I-CSCF must include the information listed in Table 10. If the orig parameter is not included in



the *Route*, see Section 3.5 Standalone Request Procedures on Terminating Side on page 38.

Table 8 *Standalone SIP Request Sent by P-CSCF to S-CSCF*

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI or a tel URI giving the destination of this request.
To	M	A SIP URI or a tel URI giving the destination of this request.
From	M	The registered Public User Identity of the originator. Can be anonymous.
Accept-Contact	O	Included if special capabilities of the target are required.
Reject-Contact	O	Included to prevent the use of targets with certain capabilities supported.
Proxy-Authorization	O	See Table 58.
Route	M	For a standalone SIP request, the <i>Route</i> includes the route set received in the <i>Service-Route</i> during the registration.
P-Charging-Vector	M	Includes the IMS Charging Identifier (ICID). The ICID is a globally unique value.
P-Asserted-Identity	M	The asserted registered Public User Identity indicated by the UE in the <i>P-Preferred-Identity</i> or <i>From</i> header.
Privacy	O	Included if the UE has included the <i>Privacy</i> header.
P-Profile-Key	C	Included if the value of <i>P-Preferred-Identity</i> or <i>From</i> header (if <i>P-Preferred-Identity</i> is not received) matches <i>Wildcarded Identity</i> .
Resource-Priority ⁽¹⁾	O	See Table 58.
P-Access-Network-Info	O	Included if it is received from the UE, or can be asserted if the P-CSCF has the information.

(1) TSP-based P-CSCF does not send *Resource-Priority*.

The S-CSCF performs checks of the request and authenticates the end user as described in Section 3.2.1 Digest on page 13 or in Section 3.2 Authentication on page 12, and if not successful, the CSCF returns an error response according to Section 3.4.3.2 CSCF Rejects Standalone SIP Request on page 37.

The S-CSCF inserts a `P-Charging-Vector` with an ICID if the header is missing in the message and inserts the own domain name as the value of the `orig-ioi` parameter.

If applicable, the S-CSCF adds additional routing parameters to the `Request-URI`; for example: NPDI, RN, CIC as described in [RFC 4694 Number Portability Parameters for the “tel” URI](#) and DAI as described in [draft-yu-tel-dai-05 DAI Parameter for the “tel” URI](#).

The S-CSCF can forward the request to an External Network through the BGCF as shown in Figure 9. Alternatively, the request is forwarded to the remote side from the S-CSCF as shown in Figure 7.

When the node sends the standalone SIP request to the remote side, it includes the information listed in Table 9.

Table 9 Standalone SIP Request Sent by S-CSCF/BGCF to Remote Side

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI or tel URI giving the destination of this request.
To	M	A SIP URI or a tel URI giving the destination of this request.
From	M	A registered Public User Identity.
Accept-Contact	O	Included if special capabilities of the target are required.
Reject-Contact	O	Included to prevent the use of targets with certain capabilities supported.
P-Charging-Vector	M	Includes the following: <ul style="list-style-type: none"> IMS Charging Identifier (ICID) as received from the P-CSCF Originating Inter Operator Identifier (<code>orig-ioi</code>) generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).
P-Charging-Function-Addresses	O	Includes the following, if <code>CscfTrustedNetwork</code> is TRUE : <ul style="list-style-type: none"> <code>P-Charging-Function-Addresses</code> header transfers the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in the S-CSCF by the HSS, to the next IMS CN node handling the SIP request.



Header	Status	Procedure-Specific Values of the Parameter
P-Asserted-Identity	M ⁽¹⁾	The asserted registered Public User Identity.
P-Asserted-Identity	O	A second asserted identity including a tel URI or SIP URI.
Privacy	O	Included if the UE has included the <code>Privacy</code> header.
Resource-Priority	O	See Table 58. If S-CSCF is the authorizing node for prioritization, the <code>Resource-Priority</code> includes the priority received in the profile of the user.
P-Access-Network-Info	O	When <code>RoamingAwarenessInfo</code> , including <code>SgsnMccMnc</code> and <code>GPRSRoamingStatus</code> , is in the profile of the user, it is added as a new <code>PANI</code> header or it replaces the network-provided <code>PANI</code> header that is selected.

(1) A second P-Asserted-Identity header is included either with a tel URI when a tel URI is provisioned for the user and the first P-Asserted-Identity contains a SIP URI or with a SIP URI when a SIP URI is provisioned for the user and the first P-Asserted-Identity contains a tel URI.

The SIP request is listed in Table 10.

Table 10 SIP Request from I-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI or a tel URI giving the destination of the request.
To	M	A SIP URI or a tel URI giving the destination of the request.
From	M	The Public User Identity of the originator. Can be anonymous.
Accept-Contact	O	Included if special capabilities of the target are required.
Reject-Contact	O	Included to prevent the use of targets with certain capabilities supported.
Route	M	For a standalone SIP request the Route must include the location of the S-CSCF and an <code>orig</code> parameter.
P-Asserted-Identity	O	The asserted registered Public User Identity.

Header	Status	Procedure-Specific Values of the Parameter
Privacy	O	Included if the AS has included the <code>Privacy</code> header.
P-Charging-Vector	M	Includes the IMS Charging Identifier (ICID). The ICID is a globally unique value.
P-Served-User-Identity	O	The served registered Public User Identity.
P-Profile-Key	C	Included if the I-CSCF receives Wildcarded Identity in Location Information Answer (LIA) from the HSS.
Resource-Priority	O	See Table 58.

When a confirmation is received, the remote side must send the SIP 2xx response to the S-CSCF and it includes the information listed in Table 11.

Table 11 SIP 2xx Response Sent by Remote Side to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	M	Includes the following: <ul style="list-style-type: none"> IMS Charging Identifier (ICID) as received from the remote side. The Originating Inter-Operator Identifier (<code>orig-ioi</code>) is generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP). Terminating Inter-Operator Identifier (<code>term-ioi</code>)
P-Asserted-Identity	M	Must include the value of the <code>Request-URI</code> in the request that generated this response.

On reception of the SIP 2xx response, the S-CSCF performs checks and if successful continues with next step.

The S-CSCF removes optionally, defined by configuration, the `term-ioi` parameter if the parameter is included in the `P-Charging-Vector` header; and removes the `orig-ioi` parameter if the parameter is included in the `P-Charging-Vector` header.

The S-CSCF sends the SIP 2xx response to the P-CSCF and it includes the information listed in Table 12.



Table 12 SIP 2xx Response Sent by S-CSCF to P-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Authentication-Info	O	See Table 59.
P-Charging-Vector	M ⁽¹⁾	Includes the IMS Charging Identifier (ICID) as received from the remote side.
P-Charging-Function-Addresses	O	Includes the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in S-CSCF by HSS, to the next IMS CN node handling the SIP request.
Resource-Priority	O	See Table 59.
P-Asserted-Identity	M	Must include the value of the Request-URI in the request that generated this response.

(1) The S-CSCF removes the term-voi and orig-voi parameters.

3.4.3 Unsuccessful Cases at Standalone Requests

For protocol errors or errors outside the scope of this document, refer to [RFC 3261 SIP: Session Initiation Protocol](#) and other relevant extensions to the RFC.

3.4.3.1 CSCF Receives Redirect Response for Standalone SIP Request

The CSCF/BGCF can redirect the request on a received 3xx response. The important header in the redirect response is given in Table 13.

Table 13 SIP 3xx Response

Header	Status	Procedure-Specific Values of the Parameter
Contact	M	Contact header contains the new target to where the request is to be redirected. Also, the Contact header can also contain SIP URI header components associated with the SIP URI of the returned new target, refer to RFC 3261 SIP: Session Initiation Protocol . Some or all these SIP URI header components can be included as headers in the outgoing redirected SIP request to the new target destination.

3.4.3.2 CSCF Rejects Standalone SIP Request

This section describes the procedure when the CSCF rejects the standalone SIP request.

The sending of the standalone SIP request is initiated as shown in Section 3.4.2 Send Standalone SIP Request on page 32.

The S-CSCF sends the SIP final non-2xx response to the P-CSCF and it includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and other relevant extensions to the RFC.

If a standalone request is received by the E-CSCF, the E-CSCF rejects the message by sending a failure response 501 (Not Implemented), which includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and other relevant extensions to the RFC.

The status codes and reason phrases the CSCF can generate, are listed in the *CSCF Fault Codes Catalogue*.

3.5 Standalone Request Procedures on Terminating Side

This section describes the procedures the CSCF uses when delivering a standalone SIP request to terminating UE.

A standalone SIP request is defined in this document as; a SIP request that does not create a dialog and is sent outside an existing dialog. In this document only the SIP methods, MESSAGE, OPTIONS, PUBLISH, and REFER are defined as possible to send as standalone SIP requests.

3.5.1 Preconditions

The UE must be registered.

3.5.2 Deliver Standalone SIP Requests

This section describes the successful delivery of a standalone SIP request. The unsuccessful cases are described in Section 3.5.3 Unsuccessful Cases at Standalone Requests on page 42.

The signaling sequence is shown in Figure 15.

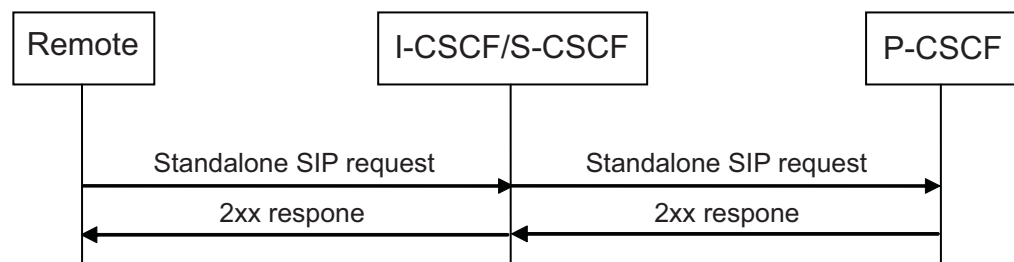


Figure 15 Delivering Standalone SIP Request



When the I-CSCF has received a standalone SIP request from the remote side, the SIP request must include the information listed in Table 14.

The Request-URI can include routing parameters, for example NPDI, RN, CIC, as described in [RFC 4694 Number Portability Parameters for the “tel” URI](#) or DAI as described in [draft-yu-tel-dai-05 DAI Parameter for the “tel” URI](#).

Once the I-CSCF has determined that the user is served by the S-CSCF, it forwards the request to the S-CSCF. If the I-CSCF has determined that the user is in an External Network, the I-CSCF can add routing parameters, for example NPDI, RN, CIC, as described in [RFC 4694 Number Portability Parameters for the “tel” URI](#) and DAI as described in [draft-yu-tel-dai-05 DAI Parameter for the “tel” URI](#). The I-CSCF forwards the request to the BGCF which then forwards the request to the External Network. The signaling is as shown in Figure 9. The request includes the same information as listed in Table 14 with the addition of the new routing parameters in the Request-URI.

Table 14 Standalone SIP Request Sent by Remote Side to I-CSCF/S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	The Public User Identity of the invited user in the format of a SIP URI.
To	M	A SIP URI or a tel URI giving the identity of the receiving user as received from the sender.
From	M	The registered Public User Identity of the sender.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
P-Charging-Vector	M	Includes the following: <ul style="list-style-type: none"> • An IMS Charging Identifier (ICID) generated by the remote side • An Originating Inter-Operator Identifier (orig-ioi) inserted by the remote side
P-Asserted-Identity	M	Includes the asserted Public User Identity of the inviting user.
P-Asserted-Identity	O ⁽¹⁾	A second asserted identity including a tel URI.

Header	Status	Procedure-Specific Values of the Parameter
Privacy	O	See Table 58.
Resource-Priority	O	See Table 58.

(1) A second P-Asserted-Identity header is included with a tel URI where the remote network has provided a tel URI for the inviting user and the first P-Asserted-Identity contains a SIP URI.

The S-CSCF sends the SIP request to each registered user using the address received during registration, and it includes the information listed in Table 15.

Table 15 Standalone SIP Request Sent by S-CSCF to P-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	The registered contact address of the invited user; or it is kept unchanged if loose routing is required.
To	M	A SIP URI or a tel URI giving the identity of the receiving user as received from the sender.
From	M	The registered Public User Identity of the sender.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
Route	M	The values of Path header stored at registration, and the registered contact address is included in the last route header if loose routing is required.
P-Charging-Vector	M	Includes the IMS Charging Identifier (ICID) as received from the remote side.
P-Charging-Function-Addresses	O	Includes the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in S-CSCF by HSS, to the next IMS CN node handling the SIP request.
Resource-Priority	O	See Table 58.
P-Called-Party-ID	M	Includes a copy of the value of the Request-URI in the received INVITE request. The P-Called-Party-ID header is defined in RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP) and its use is further defined in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) .



Header	Status	Procedure-Specific Values of the Parameter
P-Asserted-Identity	O ⁽¹⁾	Includes the asserted Public User Identity of the inviting user.
P-Asserted-Identity	O ⁽¹⁾	A second asserted identity including a tel URI.

(1) The P-Asserted-Identity header is removed by the P-CSCF where the request in Table 14 included a Privacy header.

If more than one registered contact of the called user fulfilling the implicit and explicit caller preferences of the caller, through a P-CSCF the S-CSCF forks the SIP request to each qualified registered contact according to their priorities determined by the caller preferences function, refer to [RFC 3841 Caller Preferences for the Session Initiation Protocol \(SIP\)](#) and [RFC 3261 SIP: Session Initiation Protocol](#).

If only one registered P-CSCF fulfills the implicit and explicit requirements of the caller, that is, if explicit requirements are received in the `Accept-Contact` header, the S-CSCF sends the standalone SIP request to the P-CSCF.

The P-CSCF, when receiving a 2xx response, sends a SIP 2xx response and it must include the parameters listed in Table 16.

Table 16 SIP 2xx Response Sent by P-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
P-Asserted-Identity	M	Includes the stored value from the P-Called-Party-ID header received in Table 15.
P-Charging-Vector	O	Includes the stored IMS Charging Identifier (ICID) value.

On reception of the SIP 2xx response, the S-CSCF performs checks and if successful continues with the following:

- Removes `IOI` parameters and `ICID` parameter in existing `P-Charging-Vector` header
- Adds the `term-ioi` parameter with the configured value to the existing `P-Charging-Vector` header
- Adds the `orig-ioi` parameter with the stored value to the existing `P-Charging-Vector` header
- Adds the `icid-value` parameter with the stored `ICID` value to the existing `P-Charging-Vector` header

The S-CSCF sends the SIP 2xx response to the remote side through the I-CSCF and it includes the information listed in Table 17.

Table 17 SIP 2xx Response Sent by S-CSCF to Remote Side

Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	M ⁽¹⁾	Includes the following: <ul style="list-style-type: none"> • The stored IMS Charging Identifier (ICID) value • The stored orig-ioi value • The configured term-ioi value
P-Charging-Function-Addresses	O	Includes the following, if CscfTrustedNetwork is TRUE : P-Charging-Function-Addresses header transfers the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in the S-CSCF by the HSS, to the next IMS CN node handling the SIP request.
P-Asserted-Identity	M	Includes the value from the P-CSCF.
Resource-Priority	O	See Table 59.

(1) The P-Charging-Vector is mandatory if the SIP 2xx response is the response to the initial SIP request.

The S-CSCF discards responses received from other users, if the SIP request was sent to more than one user.

3.5.3 Unsuccessful Cases at Standalone Requests

For protocol errors or errors outside the scope of this document, refer to [RFC 3261 SIP: Session Initiation Protocol](#) and other relevant extensions to the RFC.

The S-CSCF can reject the delivery of the standalone SIP request.

The status codes and reason phrases the CSCF can generate are listed in the *CSCF Fault Codes Catalogue*.

3.5.3.1 CSCF Redirects Standalone SIP Request

The SIP 305 (Use Proxy) response is returned by the S-CSCF when the S-CSCF fails to update the state of a user in the HSS because the HSS already has another S-CSCF assigned for the user, that is, when the HSS returns the DIAMETER result code DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.



The SIP 305 (Use Proxy) response includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) with the clarifications in this section. See Table 18.

Table 18 SIP 305 Use Proxy Sent by S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Contact	M	Contact header contains the currently assigned the S-CSCF returned in the Cx error response from the HSS.

3.5.3.2

CSCF Receives Redirect Response for Standalone SIP Request

The CSCF/BGCF can redirect the request on a received 3xx response. The important header in the redirect response, is listed in Table 19.

Table 19 SIP 3xx Response

Header	Status	Procedure-Specific Values of the Parameter
Contact	M	Contact header contains the new target to where the request is to be redirected. Also, the Contact header can also contain SIP URI header components associated with the SIP URI of the returned new target, refer to RFC 3261 SIP: Session Initiation Protocol . Some or all these SIP URI header components can be included as headers in the outgoing redirected SIP request to the new target destination.

3.5.3.3

CSCF Rejects Standalone SIP Request

This section describes the procedure when the CSCF rejects the standalone SIP request.

The sending of the standalone SIP request is initiated as shown in Section 3.5.2 Deliver Standalone SIP Requests on page 38.

The S-CSCF sends the SIP final non-2xx response to the originating network and includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and other relevant extensions to the RFC.

The status codes and reason phrases the CSCF can generate are listed in the *CSCF Fault Codes Catalogue*.

3.6

INVITE Dialog Procedures on Originating Side

This section describes the INVITE Dialog Procedures on the Originating Side.

3.6.1 Preconditions

For S-CSCF, the inviting user must be registered.

For E-CSCF, the inviting user can or can not be registered.

3.6.2 Create INVITE Dialog

This section defines the successful creation of an `INVITE` dialog. For details about the unsuccessful cases, see Section 3.6.7 Unsuccessful Cases at `INVITE` on page 64.

The procedure is initiated by the UE, as defined in [RFC 3261 SIP: Session Initiation Protocol](#) with the clarifications in this section.

The SIP `INVITE` dialog is valid until the UE terminates the dialog, see Section 3.6.4 Terminate `INVITE` Dialog on page 60, or until the S-CSCF terminates the dialog, see Section 3.7.4 Termination of Dialog on page 77.

The UE or P-CSCF can cancel the `INVITE` as described in Section 3.6.5 Cancel SIP `INVITE` Request on page 61 and Section 3.7.5 Cancel of SIP `INVITE` Request on page 78.

The status codes and reason phrases the CSCF can generate are listed in the *CSCF Fault Codes Catalogue*.

The message flow for the scenario is shown in Figure 3 .

When a SIP `INVITE` request is received from a UE, the P-CSCF sends a SIP `INVITE` request to the S-CSCF and it must include the information listed in Table 20. The P-CSCF removes the Number Portability parameters RN and NPDI, as defined in [RFC 4694 Number Portability Parameters for the “tel” URI](#) , from the `Request-URI` before forwarding the request to the S-CSCF.

Table 20 SIP `INVITE` Request from P-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI or a tel URI giving the destination of the <code>INVITE</code> request.
To	M	A SIP URI or a tel URI giving the destination of the <code>INVITE</code> request.
From	M	The registered Public User Identity of the originator. Can be anonymous.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.



Header	Status	Procedure-Specific Values of the Parameter
Route	M	For an initial SIP INVITE request, the Route includes the route set received in the Service-Route during the registration. For re-INVITE request, see Section 3.6.3 Sending of a Request Within INVITE Dialog on page 58.
Session-Expires	M	Includes a “refresh value”.
Proxy-Authorization	O	See Table 58.
Supported	O	Must include timer, if session Timer is supported.
Contact	M	Includes a UE address in the form of a SIP URI or a public GRUU as described by RFC 5627 Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP) . Can include feature tags and parameters as described by RFC 3840 Indicating User Agent Capabilities in the Session Initiation Protocol (SIP) .
P-Charging-Vector	M	Includes the IMS Charging Identifier (ICID). The ICID is a globally unique value.
P-Asserted-Identity	M	The asserted registered Public User Identity indicated by the UE in the P-Preferred-Identity or From header.
Priority	O	Can include emergency for an emergency call.
Privacy	O	Included if the UE has included the Privacy header.
Record-Route	M	Recorded the P-CSCF routes.
P-Profile-Key	C	Included if the value of P-Preferred-Identity or From header (if P-Preferred-Identity is not received) matches Wildcarded Identity.
Resource-Priority ⁽¹⁾	O	See Table 58.
P-Access-Network-Info	O	Included if it is received from the UE, or can be asserted if the P-CSCF has the information.

(1) TSP-based P-CSCF does not send Resource-Priority.

When an emergency call SIP INVITE request is received from a UE, the P-CSCF can send a SIP INVITE request to the E-CSCF and it must include the information listed in Table 21.

Table 21 SIP INVITE Request from P-CSCF to E-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI, a tel URI, or an emergency service URN RFC 5031 A Uniform Resource Name (URN) for Emergency and Other Well-Known Services giving the destination of the INVITE request.
To	M	A SIP URI, a tel URI, or an emergency service URN RFC 5031 A Uniform Resource Name (URN) for Emergency and Other Well-Known Services giving the destination of the INVITE request.
From	M	The Public User Identity of the originator. Can be anonymous.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
Route	O	For an initial SIP INVITE request, the Route must include the configured E-CSCF address.
Session-Expires	O	Includes a “refresh value”.
Supported	O	Includes timer, if session Timer is supported.
Contact	O	Includes a UE address in the form of a SIP URI or a public GRUU as described by RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) . Can include feature tags and parameters as described by RFC 3840 Indicating User Agent Capabilities in the Session Initiation Protocol (SIP) .
P-Charging-Vector	O	Includes the IMS Charging Identifier (ICID). The ICID is a globally unique value.
P-Asserted-Identity	O	For a registered user: Can include the asserted registered Public User Identity indicated by the UE in the P-Preferred-Identity or From header. For an unregistered user: This header is not present.
P-Preferred-Identity	O	For a registered user: This header is not present. For an unregistered user: Can have the unaltered P-Preferred-Identity from the UE included.
Priority	O	Can include emergency for an emergency call.
Privacy	O	Included if the UE has included the Privacy header.



Header	Status	Procedure-Specific Values of the Parameter
Record-Route	O	Recorded the P-CSCF routes.
P-Access- -Network- Info	O	Included if it is received from UE, or can be included if the P-CSCF has the information.

When a SIP `INVITE` request is received from a gateway, the BCF sends a SIP `INVITE` request to the S-CSCF and it must include the information listed in Table 22. The BCF removes the Number Portability parameters RN and NPDI, as defined in [RFC 4694 Number Portability Parameters for the “tel” URI](#), from the `Request-URI` before forwarding the request to the S-CSCF.

Table 22 SIP INVITE Request from BCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI or a tel URI giving the destination of the <code>INVITE</code> request.
To	M	A SIP URI or a tel URI giving the destination of the <code>INVITE</code> request.
From	M	The registered Public User Identity of the originator. Can be anonymous.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
Route	M	For an initial SIP <code>INVITE</code> request, the Route must include the address of the S-CSCF, and an <code>orig</code> parameter. For <code>re-INVITE</code> request, see Section 3.6.3 Sending of a Request Within <code>INVITE</code> Dialog on page 58.
Session-Expires	O	Includes a “refresh value”.
Supported	O	Must include <code>timer</code> , if session Timer is supported.
Contact	M	Includes a registered UE address in the form of a SIP URI. Can include feature tags and parameters as described by RFC 3840 Indicating User Agent Capabilities in the Session Initiation Protocol (SIP) .
P-Asserted-Identity	M	The asserted registered Public User Identity indicated by the UE in the <code>P-Preferred-Identity</code> or <code>From</code> header.

Header	Status	Procedure-Specific Values of the Parameter
Privacy	O	Included if the gateway has included the <code>Privacy</code> header.
Resource-Priority	O	See Table 58.

When a SIP `INVITE` request is received from an AS, the I-CSCF will proxy the request to the S-CSCF. If the received request contains a `Route` header with an `orig` parameter, the `INVITE` sent from the I-CSCF includes the information listed in Table 23, if the `orig` parameter is not included in the `Route`, see Section 3.7 `INVITE` Dialog Procedures on Terminating Side on page 67.

Table 23 SIP `INVITE` Request from I-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI or a tel URI, or a public GRUU as described by RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) giving the destination of the <code>INVITE</code> request.
To	M	A SIP URI or a tel URI giving the destination of the <code>INVITE</code> request.
From	M	The registered Public User Identity of the originator. Can be anonymous.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
Route	M	For an initial SIP <code>INVITE</code> request, the <code>Route</code> includes the address of the S-CSCF, and an <code>orig</code> parameter. For <code>re-INVITE</code> request, see Section 3.6.3 Sending of a Request Within <code>INVITE</code> Dialog on page 58.
Session-Expires	O	Includes a “refresh value”.
Supported	O	Must include “timer”, if session Timer is supported.
Contact	M	Includes the AS address in the form of a SIP URI. Can include feature tags and parameters as described by RFC 3840 Indicating User Agent Capabilities in the Session Initiation Protocol (SIP) .
P-Asserted-Identity	O	The asserted registered Public User Identity.



Header	Status	Procedure-Specific Values of the Parameter
Privacy	O	Included if the gateway has included the <code>Privacy</code> header.
P-Charging-Vector	M	Includes the IMS Charging Identifier (ICID). The ICID is a globally unique value.
P-Served-User-Id entity	O	The served registered Public User Identity.
P-Profile-Key	C	Included if I-CSCF receives Wildcarded Identity in Location Information Answer (LIA) from the HSS.
Resource-Priority	O	See Table 58.

On reception of a SIP `INVITE` request outside a dialog, the S-CSCF or the E-CSCF performs checks and if unsuccessful S-CSCF or E-CSCF returns an error response.

The S-CSCF or the E-CSCF sends the SIP `100 (Trying)` response to the P-CSCF and it includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#).

If authentication is required, the S-CSCF authenticates the end user as described in Section 3.2 Authentication on page 12.

The S-CSCF adds a P-Charging-Vector if it is missing in the SIP message; and inserts the own domain name as the value of the `orig-ioi` parameter in the P-Charging-Vector header.

If applicable, the S-CSCF can add additional routing parameters to the `Request-URI`; for example NPDI, RN, CIC as described in [RFC 4694 Number Portability Parameters for the “tel” URI](#) and DAI as described in [draft-yu-tel-dai-05 DAI Parameter for the “tel” URI](#).

The S-CSCF or E-CSCF can forward the request to an External Network through the BGCF as shown in Figure 8. Otherwise the request is forwarded to the remote side from the S-CSCF as shown in Figure 3.

The S-CSCF/BGCF translates the `Request-URI` to an IP address according to the principles described in Section 2.3.1 Number Internationalization on page 6 and sends the SIP `INVITE` request to the remote side and it includes the information listed in Table 24.

Table 24 SIP INVITE Request from S-CSCF/BGCF to Remote Side

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI (or tel URI for BGCF) or a public GRUU as described by RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) giving the destination of the INVITE request.
To	M	A SIP URI or a tel URI giving the destination of the INVITE request.
From	M	The registered Public User Identity of the originator. Can be anonymous.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
Session-Expires	M	Includes a “refresh value”.
Supported	O	Can include <code>timer</code> if Session Timer is supported.
Contact	M	Includes a registered UE address in the form of a SIP URI or a public GRUU as described by RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) . Can include feature tags and parameters as described by RFC 3840 Indicating User Agent Capabilities in the Session Initiation Protocol (SIP) .
P-Charging-Vector	M	Includes the following: <ul style="list-style-type: none"> IMS Charging Identifier (ICID) as received from the P-CSCF Originating Inter-Operator Identifier (<code>orig-iei</code>) generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).
P-Charging-Function-Addresses	O	Includes the following, if <code>CscfTrustedNetwork</code> is TRUE : P-Charging-Function-Addresses header transfers the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in S-CSCF by HSS, to the next IMS CN node handling the SIP request.



Header	Status	Procedure-Specific Values of the Parameter
P-Asserted-Identity	M	The asserted registered Public User Identity.
P-Asserted-Identity	O	<p>A second asserted identity including a tel URI.</p> <p>A second P-Asserted-Identity header is included either with a tel URI where a tel URI is provisioned for the user and the first P-Asserted-Identity contains a SIP URI or with a SIP URI where a SIP URI is provisioned for the user and the first P-Asserted-Identity contains a tel URI.</p>
Priority	O	Can include emergency for an emergency call.
Privacy	O	Included if the UE has included the Privacy header.
Route	O	Included if sent from the BGCF
Record-Route	M	Includes recorded the P-CSCF and the S-CSCF routes.
Resource-Priority	O	<p>See Table 58.</p> <p>If the S-CSCF is the authorizing node for prioritization, the Resource-Priority includes the priority received in the profile of the user.</p>
P-Access-Network-Info	O	When RoamingAwarenessInfo, including SgsnMccMnc and GPRSRoamingStatus, is in the profile of the user, it is added as a new PANI header or it replaces the network-provided PANI header that is selected.

Note: Any Proxy-Authorization header received from the P-CSCF is removed by the S-CSCF.

A second P-Asserted-Identity header is included either with a tel URI where a tel URI is provisioned for the user and the first P-Asserted-Identity contains a SIP URI or with a SIP URI where a SIP URI is provisioned for the user and the first P-Asserted-Identity contains a tel URI.

When an originating user matches a Wildcarded Public User Identity, S-CSCF inserts a second P-Asserted-Identity only if user is a registered Distinct IMPU, and if such second identity is available in the S-CSCF database. A Wildcarded Public User Identity is not inserted.

The E-CSCF/BGCF sends the SIP INVITE request to the remote side in Public Switched Telephone Network (PSTN) and it includes the information listed in Table 25.

Table 25 *SIP INVITE Request from E-CSCF/BGCF to Remote Side in PSTN*

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	An international telephone number in tel URI either from LRF or from default number configured.
To	M	A SIP URI or a tel URI including a dialed string, or emergency service URN.
From	M	The Public User Identity of the originator. Can be anonymous.
Session-Expires	M	Includes a “refresh value”.
Supported	O	Can include “timer” if Session Timer is supported.
P-Charging-Vector	M	Includes the following: <ul style="list-style-type: none"> IMS Charging Identifier (ICID) as received from the P-CSCF. Originating Inter-Operator Identifier (orig-ioi) generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).
P-Charging-Function-Addresses	O	Included if the value of CscfTrustedNetwork is TRUE .
P-Asserted-Identity	O	PAI value received from LRF, PAI value received from P-CSCF, if no PAI received from LRF, or PAI created by E-CSCF, if no PAI received from both LRF and P-CSCF.
Priority	O	Included with “emergency”.
Route	O	Included with next hop address.
Record-Route	M	Includes recorded the P-CSCF and the E-CSCF routes.
P-Access-Network-Info	O	Included if it is received from the P-CSCF as a SIP header, or from LRF, or both, as a SIP URI header component.

The E-CSCF sends the SIP `INVITE` request to Public Safety Answering Point (PSAP) in IP Multimedia Network directly or through IBCF, and it includes the information listed in Table 26.



Table 26 *SIP INVITE Request from E-CSCF to PSAP in IP Multimedia Network Directly (Mm) or Through IBCF (Mx)*

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI or a tel URI including a dialed string, or emergency service URN.
To	M	A SIP URI or a tel URI including a dialed string, or emergency service URN.
From	M	The Public User Identity of the originator. Can be anonymous.
Session-Expires	M	Includes a “refresh value”.
Supported	O	Can include “timer” if Session Timer is supported.
P-Charging-Vector	M	Includes the following: <ul style="list-style-type: none"> IMS Charging Identifier (ICID) as received from the P-CSCF. Originating Inter-Operator Identifier (orig-ioi) generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).
P-Charging-Function-Addresses	O	Included if the value of <code>CscfTrustedNetwork</code> is TRUE .
P-Asserted-Identity	O	The PAI value received from LRF, PAI value received from the P-CSCF (if no PAI received from LRF), or PAI created by the E-CSCF (if no PAI received from both the LRF and the P-CSCF).
Priority	O	Included with “emergency”.
Route	M	A SIP URI containing a non-telephone number, which is received from LRF
Record-Route	M	Includes recorded the P-CSCF and the E-CSCF routes.
P-Access-Network-Info	O	Included if it is received from the P-CSCF as a SIP header, or from LRF, or both, as a SIP URI header component.

The remote side can send the SIP 100 (Trying) response to the S-CSCF or E-CSCF and it must include the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#).

Optionally, when call progress information is received, the remote side sends a SIP provisional response (for example, a 180 (Ringing response)) to the S-CSCF or E-CSCF and it must include the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC and according to Table 27.

Table 27 SIP 1xx (except 100) Response

Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	O	Includes the following: <ul style="list-style-type: none"> IMS Charging Identifier (ICID) as received from the remote side Originating Inter-Operator Identifier (<code>orig-ioi</code>) generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP). Terminating Inter-Operator Identifier (<code>term-ioi</code>) generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).
P-Asserted-Identity	M	Includes the value of the Request-URI in the request that generated this response.

Note: The P-Charging-Vector is mandatory in the first SIP provisional response. The S-CSCF removes the `orig-ioi` and `term-ioi` parameters before the response is sent to the P-CSCF.

On reception of the SIP provisional response, the S-CSCF sends the SIP provisional response to the P-CSCF and it includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC and according to Table 27.

The S-CSCF can remove, as defined by configuration, the `term-ioi` parameter if the parameter is included in the P-Charging-Vector header and can remove the `orig-ioi` parameter if the parameter is included in the P-Charging-Vector header.

If it is an emergency call, the E-CSCF sends the SIP provisional response to the P-CSCF and it includes the information listed in Table 28.



Table 28 SIP 1xx (Except 100) Response from E-CSCF to P-CSCF

Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	O ⁽¹⁾	Includes the IMS Charging Identifier (ICID) as received in the request from the P-CSCF.
P-Asserted-Identity	O	<p>If the original Request-URI received is an emergency service URN, the E-CSCF adds P-Asserted-Identity with a tel URI number, that is preconfigured in the E-CSCF.</p> <p>If the original Request-URI received is a dialed string (either in tel URI or SIP URI), the E-CSCF adds P-Asserted-Identity with the dialed string (either in tel URI or SIP URI) that the E-CSCF has saved from the original request received.</p>

(1) The P-Charging-Vector is mandatory in the first SIP provisional response. The E-CSCF removes the orig-ioi and term-ioi parameters before the response is sent to the P-CSCF.

The P-CSCF sends the SIP provisional response to the UE.

When the remote side has received an answer indication, the remote side sends a SIP 2xx (INVITE) response to the S-CSCF and it must include the information listed in Table 29.

Table 29 SIP 2xx Response from Remote Side to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	O ⁽¹⁾	<p>Includes the following:</p> <ul style="list-style-type: none"> IMS Charging Identifier (ICID) as received from the remote side Originating Inter-Operator Identifier (orig-ioi) generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP). Terminating Inter-Operator Identifier (term-ioi) generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).
P-Asserted-Identity	O ⁽¹⁾	Includes the value of the Request-URI in the request that generated this response.

Header	Status	Procedure-Specific Values of the Parameter
P-Asserted-Identity	O	A second asserted identity including a tel URI.
Session-Expires	O ⁽²⁾	See Section 3.1.1 Session Timer Procedure on page 12.
Record-Route	O ⁽³⁾	Includes the recorded route set according to RFC 3261 SIP: Session Initiation Protocol .

(1) Mandatory if the SIP 2xx response is the first response to an initial INVITE request.

(2) Mandatory if response to the SIP INVITE request or the SIP UPDATE request.

(3) Mandatory if response to the SIP initial-INVITE request.

On reception of the SIP 2xx response, the S-CSCF removes the `term-ioi` parameter if the parameter is included in the P-Charging-Vector header; and removes the `orig-ioi` parameter if the parameter is included in the P-Charging-Vector (configurable).

The S-CSCF sends the SIP 2xx response to the P-CSCF and it includes the information listed in Table 30.

Table 30 SIP 2xx Response from S-CSCF to P-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Authentication-Info	O	See Table 59.
P-Charging-Vector	O ⁽¹⁾	Includes the IMS Charging Identifier (ICID) as received from the remote side.
P-Charging-Function-Addresses	O	Includes the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in the S-CSCF by the HSS, to the next IMS CN node handling the SIP request.
Session-Expires	O ⁽²⁾	See Section 3.1.1 Session Timer Procedure on page 12.
P-Asserted-Identity	O ⁽³⁾	Includes the value of the Request-URI in the request that generated this response.
P-Asserted-Identity	O	A second asserted identity including a tel URI.



Header	Status	Procedure-Specific Values of the Parameter
Record-Route	O ⁽⁴⁾	Includes the recorded route set according to RFC 3261 SIP: Session Initiation Protocol .
Resource-Priority	O	See Table 59.

(1) Mandatory if the SIP 2xx response is the first response to an initial INVITE request. The S-CSCF removes the *term-ioi* and *orig-ioi* parameters.

(2) Mandatory if response to the SIP INVITE request or the SIP UPDATE request.

(3) Mandatory if response to the SIP initial INVITE request.

(4) Mandatory if response to the SIP initial INVITE request.

The E-CSCF sends the SIP 2xx response to the P-CSCF if it is and emergency call and it includes the information listed in Table 31.

Table 31 SIP 2xx Response from E-CSCF to P-CSCF

Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	O ⁽¹⁾	Includes IMS Charging Identifier (ICID) as received in the request from the P-CSCF.
P-Asserted-Identity	O	If the original Request-URI received is an emergency service URN, the E-CSCF adds P-Asserted-Identity with a tel URI number, that is preconfigured in the E-CSCF. If the original Request-URI received is a dialed string (either in tel URI or in SIP URI), the E-CSCF adds P-Asserted-Identity with the dialed string (either in tel URI or in SIP URI) that the E-CSCF has saved from the original request received.
Session-Expires	O ⁽²⁾	See Section 3.1.1 Session Timer Procedure on page 12.
Record-Route	O ⁽³⁾	Includes the recorded route set according to RFC 3261 SIP: Session Initiation Protocol .
Resource-Priority	O	See Table 59.

(1) Mandatory if the SIP 2xx response is the first response to an initial INVITE request. The E-CSCF removes the *term-ioi* and *orig-ioi* parameters.

(2) Mandatory if response to the SIP INVITE request or the SIP UPDATE request.

(3) Mandatory if response to the SIP initial INVITE request.

The P-CSCF sends the 2xx response to the UE.

When a SIP ACK request is received from the UE, the P-CSCF sends the SIP ACK request to the S-CSCF or E-CSCF, and it must include the mandatory

parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC.

On reception of the SIP ACK request, the S-CSCF or E-CSCF sends the SIP ACK request to the remote side.

3.6.3 Sending of a Request Within INVITE Dialog

This section defines the procedures how to send a SIP request successfully within a dialog. For details about the unsuccessful cases, see Section 3.6.7 Unsuccessful Cases at INVITE on page 64.

The procedure for sending a SIP BYE request is described in Section 3.6.4 Terminate INVITE Dialog on page 60.

The signaling sequence is shown in Figure 4.

Note: The SIP ACK is only sent when the SIP request is a SIP re-INVITE request.

When receiving a SIP request from the UE, the P-CSCF sends the SIP request to the S-CSCF or E-CSCF within the existing SIP dialog for a dialog and it must include the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC and information listed in Table 32.

Table 32 SIP Request Sent from P-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Proxy-Authorization	O	See Table 58.
Route	M	The Route must include the route set received in the SIP 200 (OK) for the initial SIP INVITE request.
P-Charging-Vector	O	Includes the stored IMS Charging Identifier (ICID) value.

On reception of the SIP request, the S-CSCF or E-CSCF performs checks and if unsuccessful, the S-CSCF or E-CSCF returns an error response according to the *CSCF Fault Codes Catalogue*.

The S-CSCF authenticates the user if necessary.

If the SIP request is a SIP re-INVITE request or a SIP UPDATE request, the SIP session timer is checked as described in Section 3.1.1 Session Timer Procedure on page 12.



The S-CSCF or E-CSCF sends the SIP request to the remote side using the dialog route and it includes the information listed in Table 33.

Table 33 SIP Request Sent from S-CSCF/BGCF or E-CSCF/BGCF to Remote Side

Header	Status	Procedure-Specific Values of the Parameter
Route	M	The <code>Route</code> must include the route set received in the SIP 200 (OK) for the initial SIP INVITE request.
P-Charging-Vector	O	Includes the following: <ul style="list-style-type: none"> • The stored IMS Charging Identifier (ICID) value • The stored <code>orig-ioi</code> value • The stored <code>term-ioi</code> value
Resource-Priority	O	See Table 58 (only for S-CSCF/BGCF).

Note:

The `Proxy-Authorization` header received from the P-CSCF is removed by the S-CSCF.

When the request to transfer information is confirmed by the remote side, the remote side sends a SIP 2xx response to the S-CSCF or E-CSCF and it must include the information listed in Table 29.

The S-CSCF or E-CSCF sends the SIP 2xx response to the P-CSCF and it includes the information listed in Table 30.

The P-CSCF sends the SIP 2xx response to the UE.

If the SIP request was a SIP `re-INVITE` request, the following applies:

- When the P-CSCF receives a SIP `ACK` request from the UE, the P-CSCF sends a SIP `ACK` request to the S-CSCF or E-CSCF and it must include the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC.
- On reception of the SIP `ACK` request, the S-CSCF or E-CSCF performs checks and if successful sends it to the remote side and it includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC.

3.6.4 Terminate INVITE Dialog

This section defines how to terminate a dialog successfully. For details about the unsuccessful cases, see Section 3.6.7 Unsuccessful Cases at INVITE on page 64.

The UE usually initiates this procedure but the P-CSCF can initiate this procedure by an internal event as defined in [RFC 3261 SIP: Session Initiation Protocol](#) with the clarifications in this section.

The signaling sequence is shown in Figure 5.

Note: The UE in the figure can be the inviting or invited user.

When receiving a SIP BYE request from the UE, or because of a P-CSCF internal event, the P-CSCF sends a SIP BYE request to the S-CSCF or E-CSCF and it must include the information listed in Table 34.

Table 34 SIP BYE Request from P-CSCF to S-CSCF or E-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Proxy-Authorization	O	See Table 58, unless the P-CSCF generates the request.
Reason	O	The reason for disconnecting the session, refer to RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP) for details, normally not when the UE generates the request.
P-Charging-Vector	O	Includes the stored IMS Charging Identifier (ICID) value.

On reception of the SIP BYE request, the S-CSCF or E-CSCF performs checks and the S-CSCF authenticates the end user if necessary.

The S-CSCF or E-CSCF sends the SIP BYE request to the remote side and it includes the information listed in Table 35.

Table 35 SIP BYE Request from S-CSCF/BGCF or E-CSCF/BGCF to Remote Side

Header	Status	Procedure-Specific Values of the Parameter
Proxy-Authorization	-	The header received from the P-CSCF is removed by the CSCF.



Header	Status	Procedure-Specific Values of the Parameter
Reason	O	The reason for disconnecting the session, refer to RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP) for details.
P-Charging-Vector	O	Includes the following: <ul style="list-style-type: none"> • The stored IMS Charging Identifier (ICID) value • The stored <code>orig-ioi</code> value • The stored <code>term-ioi</code> value

Note: The `Proxy-Authorization` header received from the P-CSCF is removed by the CSCF.

When the remote user is disconnected, the remote side sends a SIP 200 (OK) response to the S-CSCF or E-CSCF and it includes the information listed in Table 29.

On reception of the SIP 200 (OK) response, the S-CSCF or E-CSCF sends the SIP 200 (OK) response to the P-CSCF and it includes the information listed in Table 30.

3.6.5 Cancel SIP INVITE Request

This section defines how to cancel a SIP INVITE request successfully. For details about the unsuccessful cases, see Section 3.6.7 Unsuccessful Cases at INVITE on page 64.

The UE can cancel the SIP INVITE request as described in [RFC 3261 SIP: Session Initiation Protocol](#).

The status codes and reason phrases the CSCF can generate as the result of an unsuccessful authentication procedure are listed in the *CSCF Fault Codes Catalogue*.

The process for canceling a SIP INVITE request process is shown in Figure 16.

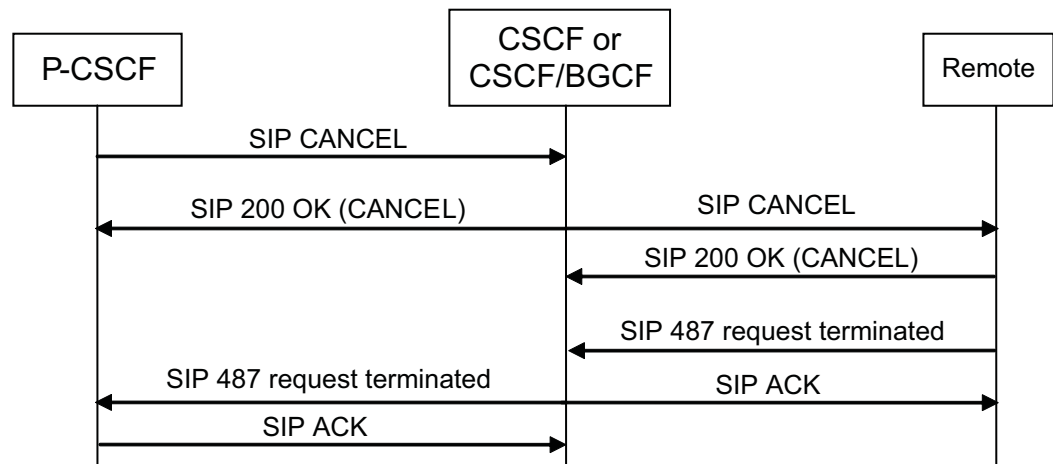


Figure 16 Canceling a SIP INVITE Request

The CSCF in the figure is applicable to both the S-CSCF and E-CSCF

The P-CSCF sends the SIP `CANCEL` request to the CSCF and it includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and relevant extensions to the RFCs.

The CSCF performs checks and if unsuccessful CSCF returns an error response according to the *CSCF Fault Codes Catalogue*.

The CSCF sends the SIP `200 (OK)` response and it includes the information listed in Table 30.

The CSCF sends the SIP `CANCEL` request to the remote side. The remote side sends the SIP `200 (OK)` response to the CSCF and it includes the information listed in Table 29.

The terminating UE has not sent any final response and then terminates the `INVITE` request and send the SIP `487 (Request terminated)` response to the CSCF. The response includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and relevant extensions to the RFCs.

On reception of the SIP `487 (Request terminated)` response, the CSCF sends the SIP `ACK` request to the remote side and it includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC.

The CSCF sends the SIP `487 (Request terminated)` response to the P-CSCF.

The P-CSCF sends the SIP `ACK` request to the CSCF and it must include the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC.

3.6.6 Rejection of Cancel

This section defines the cancellation of a SIP `INVITE` when the terminating UE has already generated a `200 (OK)` response for the dialogue establishment, but the inviting user has not received the `200 (OK)`. For details about the unsuccessful cases, see Section 3.6.7 Unsuccessful Cases at `INVITE` on page 64.

The UE can cancel a SIP `INVITE` request as described in the reference [RFC 3261 SIP: Session Initiation Protocol](#).

The status codes and reason phrases the CSCF can generate are listed in the *CSCF Fault Codes Catalogue*.

The rejection of a cancel process is shown in Figure 17.

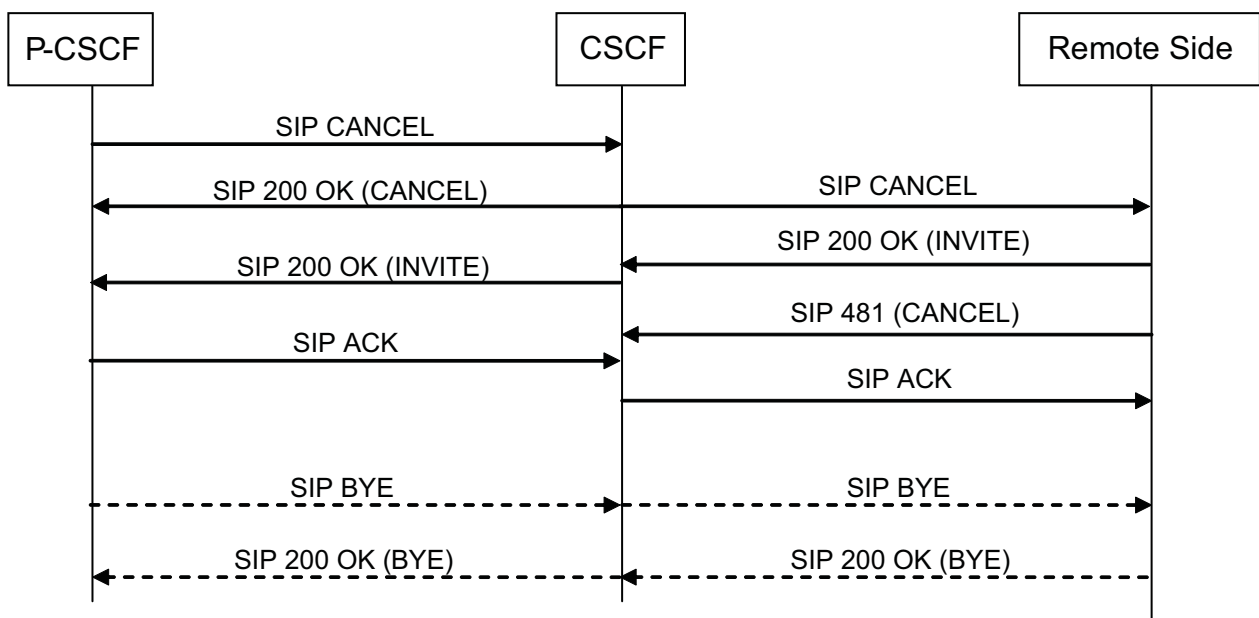


Figure 17 Rejection of Cancel of SIP `INVITE` Request

The CSCF in the figure is applicable to both the S-CSCF and E-CSCF.

The P-CSCF sends the SIP `CANCEL` request to the CSCF and it must include the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and relevant extensions to the RFCs.

The CSCF performs checks and sends the SIP `200 (OK)` response and it must include the information listed in Table 30.

The CSCF sends the SIP `CANCEL` request to the remote side and it includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and relevant extensions to the RFCs.

The remote side sends a 200 (OK) response for the INVITE request. CSCF includes the information listed in Table 29.

The CSCF proxies the 200 (OK) response to the P-CSCF

The remote side sends a SIP 481 (Call/Transaction Does Not Exist) response for the CANCEL request to the S-CSCF.

The CSCF sends an ACK request to the remote side.

The P-CSCF sends an ACK request to the CSCF

The inviting UE can keep the dialog or terminate the dialog by sending a BYE request to the CSCF through the P-CSCF.

3.6.7 Unsuccessful Cases at INVITE

For protocol errors or errors outside the scope of this document, refer to the [RFC 3261 SIP: Session Initiation Protocol](#) or relevant extensions to the RFC.

3.6.7.1 INVITE Redirected by Network

The SIP 305 (Use Proxy) response is returned by the S-CSCF when the S-CSCF fails to update the state of a user in the HSS because the HSS already has another S-CSCF assigned for the user, that is, when the HSS returns the DIAMETER result code DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

The SIP 305 (Use Proxy) response includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and [RFC 2617 HTTP Authentication: Basic and Digest Access Authentication](#) and described in this section. The SIP 305 (Use Proxy) response is listed in Table 36.

Table 36 SIP 305 Use Proxy Sent by S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Contact	M	The Contact header contains the currently assigned S-CSCF returned in the Cx error response from the HSS.

3.6.7.2 INVITE Rejected by Network

The CSCF can reject the SIP INVITE request as the result of an unsuccessful procedure.

The status codes and reason phrases the CSCF can generate are listed in the *CSCF Fault Codes Catalogue*.

The reject the SIP INVITE request process is shown in Figure 18.

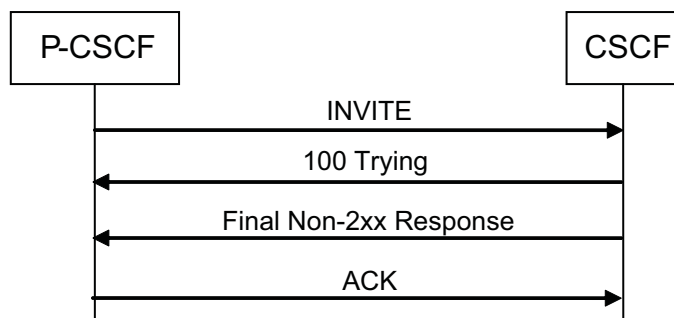


Figure 18 CSCF Rejects INVITE

The CSCF in the figure is applicable to both the S-CSCF and E-CSCF.

The procedure is initiated as described in Section 3.7.2 Create INVITE Dialog on page 67.

The CSCF sends a SIP final non-2xx response and includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC.

The P-CSCF sends a SIP ACK request to the CSCF includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC.

3.6.7.3 INVITE Redirected by Remote Side

The CSCF/BGCF can redirect the request on a received 3xx response. Table 37 lists the important header in the redirect response.

Table 37 SIP 3xx Response

Header	Status	Procedure-Specific Values of the Parameter
Contact	M	The Contact header contains the new target to where the request is to be redirected. Also, the contact header can also contain SIP URI header components associated with the SIP URI of the returned new target, refer to RFC 3261 SIP: Session Initiation Protocol . Some or all these SIP URI header components can be included as headers in the outgoing redirected SIP request to the new target destination.

3.6.7.4 INVITE Rejected by Remote Side

This section describes the procedure when the remote side rejects the SIP INVITE request.

The status codes and reason phrases the CSCF can generate are listed in the *CSCF Fault Codes Catalogue*.

The message flow for the scenario is shown in Figure 19.

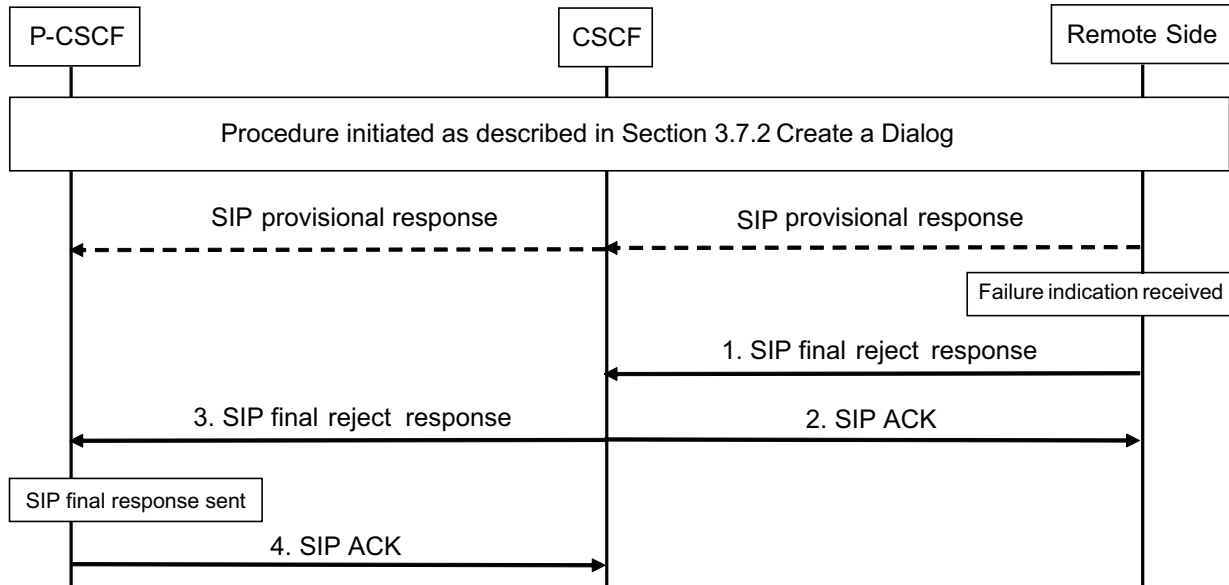


Figure 19 INVITE Rejected by Remote Side

Note: One or more SIP provisional responses can be sent before the procedure fails.

The CSCF in this figure is applicable to both S-CSCF and E-CSCF.

The procedure is initiated as described in Section 3.6.2 Create INVITE Dialog on page 44.

When a failure indication is received, the remote side sends a SIP final reject response to the CSCF and it includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include other parameters defined by relevant extensions to the RFC.

On reception of the SIP final reject response, the CSCF sends a SIP ACK request to the remote side.

The CSCF sends a SIP final reject response to the P-CSCF.

The P-CSCF sends a SIP ACK request to the CSCF.

3.6.7.5 CSCF Rejects SIP Request Within Dialog

This section describes the procedure when the S-CSCF rejects the SIP request sent by the UE within a dialog.

The message flow for the scenario is shown in Figure 20.

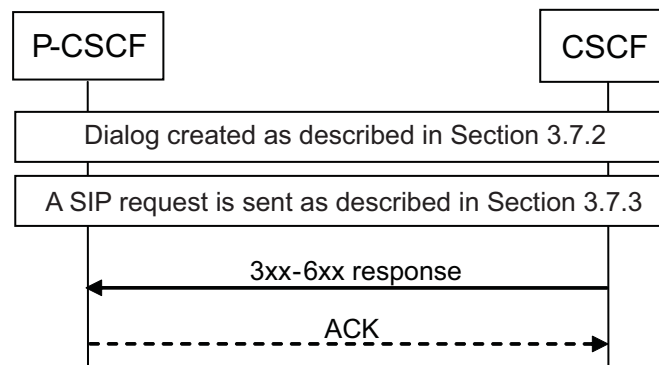


Figure 20 CSCF Rejects SIP Request within Dialog

The CSCF in the figure is applicable to both the S-CSCF and E-CSCF.

The sending of the SIP request is initiated as described in sections Section 3.6.3 Sending of a Request Within INVITE Dialog on page 58, Section 3.6.4 Terminate INVITE Dialog on page 60, or Section 3.6.5 Cancel SIP INVITE Request on page 61.

The CSCF sends the SIP reject response to the P-CSCF.

The P-CSCF sends a SIP ACK request to the CSCF if the request was an INVITE.

The status codes and reason phrases the CSCF can generate are listed in the *CSCF Fault Codes Catalogue*.

3.7 INVITE Dialog Procedures on Terminating Side

This section describes the INVITE Dialog Procedures on the Terminating Side.

3.7.1 Preconditions

The terminating user that is going to be invited must be registered.

3.7.2 Create INVITE Dialog

This section defines the procedure for creating a successful terminating INVITE dialog. For details about the unsuccessful cases, see Section 3.7.6 Unsuccessful Cases at INVITE on page 79.

The SIP INVITE dialog is valid until the inviting user or the P-CSCF terminates the dialog, see Section 3.6.4 Terminate INVITE Dialog on page 60, or until the S-CSCF terminates the dialog (see Section 3.7.4 Termination of Dialog on page 77).

The signaling sequence is shown in Figure 21.

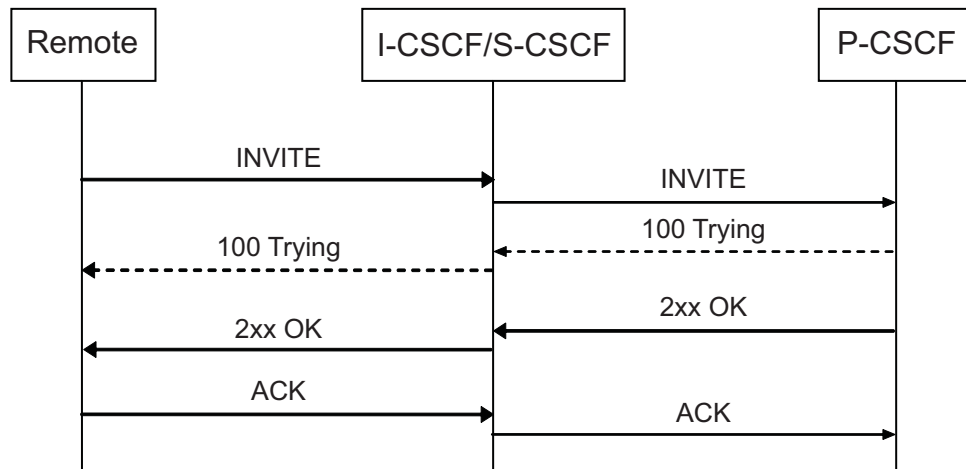


Figure 21 INVITE Dialog Procedure on Terminating Side

When the I-CSCF has received a SIP `INVITE` request to invite a user from the remote side, the `INVITE` request must include the information listed in Table 38. The `Request-URI` can include routing information (NPDI, RN, CIC) as described in [RFC 4694 Number Portability Parameters for the “tel” URI](#) and DAI as described in [draft-yu-tel-dai-05 DAI Parameter for the “tel” URI](#). If the received request contains a `P-Profile-Key` header, the I-CSCF discards it.

Table 38 SIP `INVITE` Request Sent by Remote Side to I-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	The Public User Identity of the invited user in the format of a SIP URI, tel URI, or a public GRUU as described by RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) .
To	M	A SIP URI or a tel URI giving the identity of the invited user as received from the originator.
From	M	The registered Public User Identity of the originator.
Session-Expires	O	A SIP session expire value can be included by the remote side and modified by the CSCF.
Supported	O	timer, if Session Timer is supported.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.



Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	M	Includes the following: <ul style="list-style-type: none"> • An IMS Charging Identifier (ICID) as generated by the remote side • An Originating Inter-Operator Identifier (<code>orig-ioi</code>) inserted by the remote side.
P-Asserted-Identity	M	Includes the asserted Public User Identity of the inviting user.
P-Asserted-Identity	O	A second asserted identity, as received from the remote side.
Priority	O	Can include <code>emergency</code> for an emergency call as defined in RFC 3261 SIP: Session Initiation Protocol .
Privacy	O	See Table 58.
Resource-Priority	O	See Table 58.

Note: A second `P-Asserted-Identity` header must be included with a `tel` URI where the remote network has provided a `tel` URI for the inviting user and the first `P-Asserted-Identity` contains a SIP URI.

If the originating user matches a Wildcarded Public User Identity, the S-CSCF inserts a second `P-Asserted-Identity` only if user is a registered Distinct IMPU, and if such second identity is available in the S-CSCF database. A Wildcarded Public User Identity is not inserted.

The `INVITE` is forwarded to the S-CSCF once it has determined that the user is served by the S-CSCF. If the I-CSCF at reception of the Location Information Answer found that the message included a wildcarded identity, then the content of the wildcarded identity (Wildcarded PSI or Wildcarded Public User Identity) is included in the SIP `INVITE` in a `P-Profile-Key` header.

If the I-CSCF has determined that the user is in an External Network, the I-CSCF can add routing parameters to the `Request-URI`. For example, NPDI, RN, CIC as described in [RFC 4694 Number Portability Parameters for the “tel” URI](#) and DAI as described in [draft-yu-tel-dai-05 DAI Parameter for the “tel” URI](#). The I-CSCF forwards the request to the BGCF which forwards the request to the External Network. The signaling is as shown in Figure 8. The request includes the information listed in Table 39 with the addition of the new routing parameters in the `Request-URI`.

Table 39 SIP INVITE Request Sent by I-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	The Public User Identity of the invited user in the format of a SIP URI, tel URI, or a public GRUU as described by RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) .
To	M	A SIP URI or a tel URI giving the identity of the invited user as received from the originator.
From	M	The registered Public User Identity of the originator.
Session-Expires	O	A SIP session expire value can be included by the remote side and modified by the CSCF.
Supported	O	timer, if Session Timer is supported.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
P-Charging-Vector	M	Includes the following: <ul style="list-style-type: none"> • An IMS Charging Identifier (ICID) as generated by the remote side • An Originating Inter-Operator Identifier (orig-ioi) inserted by the remote side
P-Asserted-Identity	M	Includes the asserted Public User Identity of the inviting user as received from the originating network.
P-Asserted-Identity	O	A second asserted identity as received from the originating network.
P-Profile-Key	C	Included if the I-CSCF receives Wildcarded Identity in Location Information Answer (LIA) from the HSS.
Priority	O	Can include emergency for an emergency call as defined in RFC 3261 SIP: Session Initiation Protocol .
Privacy	O	See Table 58.
Resource-Priority	O	See Table 58.

The S-CSCF sends the SIP 100 (Trying) response to the remote side and it includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation](#)



[Protocol](#) but can also include parameters defined in other relevant extensions to the RFC.

The S-CSCF removes the `term-ioi` parameter if the parameter is included in the `P-Charging-Vector` header; and removes the `orig-ioi` parameter if the parameter is included in the `P-Charging-Vector` header (not done if a configuration parameter instructs the S-CSCF to keep the `ioi` in the header) and depending on a configuration parameter, replaces the `Request-URI` with the default public identity (SIP URI).

When forwarding SIP request to next SIP entity after service invocation, the S-CSCF removes the `P-Profile-Key` parameter if the parameter was received in the INVITE message.

The S-CSCF inserts in the `P-Called-Party-ID` the canonical form of the `Request-URI`.

The S-CSCF inserts the registered contact address of the invited user into `Request-URI`, or the S-CSCF keeps `Request-URI` unchanged if loose routing is required.

The S-CSCF inserts the values of `Path` header stored at registration in `Route` header; and the S-CSCF builds the last `Route` header with the registered contact information if loose routing is required.

The request includes the information listed in Table 40.

Table 40 SIP INVITE Request Sent by S-CSCF to P-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	The registered contact address of the invited user; or it is kept unchanged as received if loose routing is required.
To	M	A SIP URI or a tel URI giving the identity of the invited user as received from the originator.
From	M	The registered Public User Identity of the originator. Can be anonymous.
Record-Route	O	Includes recorded P-CSCF and S-CSCF routes.
Route	M	The values of <code>Path</code> header stored at registration; and the registered contact address is included in the last route header if loose routing is required.
Session-Expires	M	A SIP session expire value can be included by the remote side and modified by the CSCF.
Supported	O	<code>timer</code> , if Session Timer is supported.

Header	Status	Procedure-Specific Values of the Parameter
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
P-Charging-Vector	M ⁽¹⁾	Includes an IMS Charging Identifier (ICID) as generated by the remote side.
P-Charging-Function-Addresses	O	Includes the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in the S-CSCF by the HSS, to the next IMS CN node handling the SIP request.
P-Called-Party-ID	M	Must include a copy of the value of the Request-URI. The P-Called-Party-ID header is defined in RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP) and its use is further defined in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) .
P-Asserted-Identity	O ⁽²⁾	Includes the asserted Public User Identity of the inviting user.
P-Asserted-Identity	O ⁽²⁾	A second asserted identity
Priority	O	Can include emergency for an emergency call as defined in RFC 3261 SIP: Session Initiation Protocol .
Privacy	O	See Table 58.
Resource-Priority	O	See Table 58.

(1) The S-CSCF removes the *orig-voi* parameter.

(2) The P-Asserted-Identity header or headers must be removed by P-CSCF where the INVITE request in Table 39 included a Privacy header.

If more than one registered contact of the called user fulfilling the implicit and explicit caller preferences of the caller, through a P-CSCF, the S-CSCF forks the SIP request to each qualified registered contact according to their priorities determined by the caller preferences function, refer to [RFC 3841 Caller Preferences for the Session Initiation Protocol \(SIP\)](#) and [RFC 3261 SIP: Session Initiation Protocol](#).

If only one registered contact fulfills the implicit and explicit requirements of the caller, the S-CSCF sends the standalone SIP request to the P-CSCF.

The P-CSCF must send a SIP 100 (Trying) response to the S-CSCF.



On reception of the SIP 100 (Trying) response, the S-CSCF performs checks and if successful continues with next step.

Optionally, the P-CSCF can send one or more provisional responses, except for the SIP 100 (Trying) response, to the S-CSCF, and it must include the information listed in Table 41.

Table 41 SIP Provisional Response Sent by P-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
P-Asserted-Identity	M	Includes the stored value from the P-Called-Party-ID header received in Table 40.
P-Charging-Vector	O	Includes the stored IMS Charging Identifier (ICID).

Note: The P-Charging-Vector is mandatory if the SIP provisional response is the first provisional response.

On reception of a SIP provisional response, the S-CSCF performs checks and if successful continues in next step.

The S-CSCF removes IOI parameters and ICID parameter in existing P-Charging-Vector header and adds the following:

- The term-ioi parameter with the configured value to the existing P-Charging-Vector header
- The orig-ioi parameter with the stored value to the existing P-Charging-Vector header
- The icid-value parameter with the stored ICID value to the existing P-Charging-Vector header

The S-CSCF sends the SIP provisional response is sent to the remote side through the I-CSCF and it must include the information listed in Table 42.

Table 42 SIP Provisional Response Sent by S-CSCF to Remote Side

Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	M ⁽¹⁾	Includes the following: <ul style="list-style-type: none"> • The stored IMS Charging Identifier (ICID) value • The stored orig-ioi value • The configured term-ioi value

Header	Status	Procedure-Specific Values of the Parameter
P-Asserted-Identity	M	Includes the value from the P-CSCF.
P-Asserted-Identity	O ⁽²⁾	A second asserted identity including a tel URI.
Resource-Priority	O	See Table 59.

(1) The P-Charging-Vector is always included if the SIP provisional response is the first provisional response.

(2) A second P-Asserted-Identity header must be included either with a tel URI in the case a tel URI is provisioned for the user and the first P-Asserted-Identity contains a SIP URI or with a SIP URI in the case a SIP URI is provisioned for the user and the first P-Asserted-Identity contains a tel URI.

Note: When a terminating user matches a Wildcarded Public User Identity, S-CSCF inserts a second P-Asserted-Identity only if user is a registered Distinct IMPU, and if such second identity is available in the S-CSCF database. A Wildcarded Public User Identity is not inserted.

The P-CSCF, when receiving a 2xx response, sends a SIP 2xx response to the S-CSCF and it includes the information listed in Table 43.

Table 43 SIP 2xx Response Sent by P-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
P-Asserted-Identity	M	Must include the stored value from the P-Called-Party-ID header received in Table 40.
P-Charging-Vector	O	Includes the stored IMS Charging Identifier (ICID).

On reception of a SIP 2xx response the S-CSCF performs checks and if successful continues with the following steps:

- Removes IOI parameters and ICID in existing P-Charging-Vector header
- Adds the term-ioi parameter with the configured value to the existing P-Charging-Vector header
- Adds the orig-ioi parameter with the stored value to the existing P-Charging-Vector header
- Adds the icid-value parameter with the stored ICID value to the existing P-Charging-Vector header



The S-CSCF sends the SIP 2xx response through the I-CSCF to the remote side and it includes the information listed in Table 44.

Table 44 *SIP 2xx Response Sent by S-CSCF to Remote Side*

Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	O ⁽¹⁾	Includes the following: <ul style="list-style-type: none"> • The stored IMS Charging Identifier (ICID) value • The stored <code>orig-ioi</code> value • The configured <code>term-ioi</code> value
P-Charging-Function-Addresses	O	Includes if <code>CscfTrustedNetwork</code> is TRUE; P-Charging-Function-Addresses header transfers the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in the S-CSCF by the HSS, to the next IMS CN node handling the SIP request.
P-Asserted-Identity	M	Includes the value from the P-CSCF.
P-Asserted-Identity	O ⁽²⁾	A second asserted identity, if available for the called user.
Resource-Priority	O	See Table 59.

(1) The P-Charging-Vector is mandatory if the SIP 2xx response is the first response to the initial SIP INVITE request.

(2) A second P-Asserted-Identity header must be included either with a tel URI where a tel URI is provisioned for the user and the first P-Asserted-Identity contains a SIP URI or with a SIP URI where a SIP URI is provisioned for the user and the first P-Asserted-Identity contains a tel URI.

Note: When a terminating user matches a Wildcarded Public User Identity, the S-CSCF inserts a second P-Asserted-Identity only if user is a registered Distinct IMPU, and if such second identity is available in the S-CSCF database. A Wildcarded Public User Identity is not inserted.

If the SIP INVITE request was sent to more than one P-CSCF, the CSCF cancels the SIP INVITE request as described in the Section 3.7.5 Cancel of SIP INVITE Request on page 78.

The remote side sends a SIP ACK request to the S-CSCF.

The S-CSCF sends a SIP ACK to the P-CSCF.

The CSCF starts the SIP session timer as described in Section 3.1.1 Session Timer Procedure on page 12.

3.7.3 Deliver a SIP Request Within INVITE Dialog

This section defines the procedure for a successful delivery of a SIP request within a dialog. For details about the unsuccessful cases, see Section 3.7.6 Unsuccessful Cases at INVITE on page 79.

The signaling sequence is shown in Figure 4.

The remote side sends a SIP request to the S-CSCF within a dialog and the request must include the information listed in Table 45.

Table 45 SIP Request within Dialog

Header	Status	Procedure-Specific Values of the Parameter
Session-Expires	O ⁽¹⁾	A SIP session expires value that can be modified by the CSCF.
P-Charging-Vector	O	Includes the following: <ul style="list-style-type: none"> • The IMS Charging Identifier (ICID) value • The orig-ioi value • The term-ioi value

(1) Only applicable when the SIP request is a SIP re-INVITE request or a SIP UPDATE request.

The S-CSCF performs checks and if successful processing continues in next step.

The S-CSCF sends the SIP request to the P-CSCF and it includes the information listed in Table 40.

The P-CSCF sends the SIP request to the UE.

The P-CSCF, when receiving a 2xx response, sends a SIP 2xx response to the S-CSCF and it must include the information listed in Table 46.

Table 46 SIP 2xx Response Sent by P-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Session-Expires	O ⁽¹⁾	A SIP session expires value that can be modified by the CSCF.
P-Charging-Vector	O	Includes the stored IMS Charging Identifier (ICID) value.

(1) Only applicable when the SIP request is a SIP re-INVITE request or a SIP UPDATE request.

On reception of the SIP 2xx response, the S-CSCF performs checks and if successful continues with next step.



The S-CSCF sends the SIP 2xx response to the remote side and it must include the information listed in Table 47.

Table 47 SIP 2xx Response Sent by S-CSCF to Remote Side

Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	O ⁽¹⁾	Includes the following: <ul style="list-style-type: none"> • The stored IMS Charging Identifier (ICID) value • The stored <code>orig-ioi</code> value • The stored <code>term-ioi</code> value
P-Asserted-Identity	M	Includes the value from the P-CSCF.
Resource-Priority	O	See Table 59.

(1) The P-Charging-Vector is mandatory if the SIP 2xx response is the first response to the initial SIP INVITE request.

If the SIP request was a SIP `re-INVITE`, request the following applies:

- When an acknowledgment is received, the remote side sends a SIP `ACK` request to the S-CSCF.
- The S-CSCF sends the SIP `ACK` request to the P-CSCF.

3.7.4 Termination of Dialog

This section describes the procedure for the successful termination of a dialog. For details about the unsuccessful cases, see Section 3.7.6 Unsuccessful Cases at INVITE on page 79.

The sequence is shown in Figure 5.

The remote side sends a SIP `BYE` request to the S-CSCF to terminate a dialog.

The S-CSCF performs checks and if successful continues with next step.

The S-CSCF sends the SIP `BYE` request to the P-CSCF.

The P-CSCF, when receiving a 2xx response, sends a SIP `200 (OK)` response to the S-CSCF.

On reception of the SIP `200 (OK)` response, the S-CSCF performs checks and if successful continues with next step.

The S-CSCF sends the SIP `200 (OK)` response is sent to the remote end.

3.7.5 Cancel of SIP INVITE Request

This section describes a successful cancelation of an `INVITE` request. For details about the unsuccessful cases, see Section 3.7.6 Unsuccessful Cases at `INVITE` on page 79.

The S-CSCF initiates the following:

- When receiving a cancel request from the originating side.
- When receiving a `SIP 200 (OK)` response from one P-CSCF and the S-CSCF needs to cancel the `SIP INVITE` request sent to other UEs (if forking).

The sequence is shown in Figure 22.

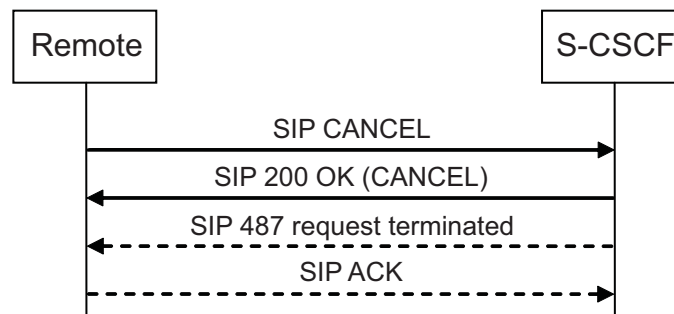


Figure 22 Canceling `INVITE` Request on Terminating Side

When the S-CSCF receives a `SIP CANCEL` request from the remote side, the `SIP CANCEL` request must include the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and relevant extensions to the RFC.

The S-CSCF performs checks and if the successful continues with next step.

The S-CSCF sends the `SIP 200 (OK)` response to the remote side.

For each registered UE that the S-CSCF has invited, the S-CSCF sends the `SIP CANCEL` request to the P-CSCF.

For each sent `SIP CANCEL` request, the P-CSCF sends the `SIP 200 (OK)` response to the S-CSCF.

If the S-CSCF receives a `SIP 487 (Request Terminated)` reject response, the S-CSCF performs checks and if the successful continues with next step.

The S-CSCF sends a `SIP ACK` request to P-CSCF.

If this is the first `SIP 487 (Request Terminated)` reject response, the CSCF sends the `SIP 487 (Request Terminated)` reject response to the remote side.



If the remote side receives a SIP 487 (Request Terminated) reject response, the remote side must send a SIP ACK request to the S-CSCF.

3.7.6 Unsuccessful Cases at INVITE

For protocol errors or errors outside the scope of this document, refer to [RFC 3261 SIP: Session Initiation Protocol](#) and other relevant extensions to the RFC.

3.7.6.1 Terminating S-CSCF Redirects INVITE

The SIP 305 (Use Proxy) response is returned by the S-CSCF if the S-CSCF fails to update the state of a user in the HSS because the HSS already has another S-CSCF assigned for the user, that is, when the HSS returns the DIAMETER result code DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

The SIP 305 (Use Proxy) response includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and [RFC 2617 HTTP Authentication: Basic and Digest Access Authentication](#) described in this section and listed in Table 48.

Table 48 SIP 305 Use Proxy Sent by S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Contact	M	The Contact header contains the currently assigned S-CSCF returned in the Cx error response from the HSS.

3.7.6.2 Terminating CSCF Rejects INVITE

The S-CSCF can reject the creation of a dialog according to the following:

- When receiving the invitation from the originating side
- When no SIP 2xx final response is received from any of the invited UEs.

If more than one SIP final reject response is received the CSCF selects the SIP final response with the highest priority as defined in [RFC 3261 SIP: Session Initiation Protocol](#).

- When no response is received from the invited UEs.
- When the request contains more than 20 rules specified in its Accept-Contact and Reject-Contact headers together.

3.7.6.3 Remote Side Redirects INVITE

The CSCF/BGCF can redirect the request on a received 3xx response. The important header in the redirect response is listed in Table 49.

Table 49 SIP 3xx Response

Header	Status	Procedure-Specific Values of the Parameter
Contact	M	The <code>Contact</code> header contains the new target to where the request is to be redirected. Also, the contact header can also contain SIP URI header components associated with the SIP URI of the returned new target, refer to RFC 3261 SIP: Session Initiation Protocol . Some or all these SIP URI header components can be included as headers in the outgoing redirected SIP request to the new target destination.

3.7.6.4 Terminating P-CSCF Rejects INVITE

This section describes the procedures when the terminating P-CSCF rejects the `INVITE` request.

The sequence is shown in Figure 23.

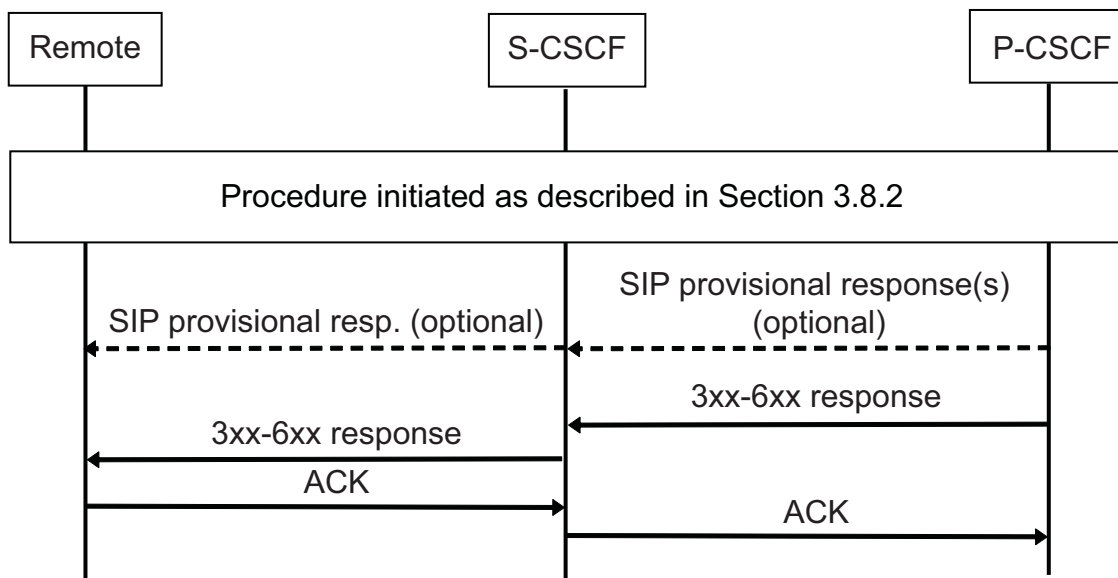


Figure 23 Terminating P-CSCF Rejects INVITE

Note: The P-CSCF can have returned none, one, or more SIP provisional responses before sending the SIP final reject response.

The `INVITE` is sent as described in Section 3.7.2 Create `INVITE` Dialog on page 67.

The P-CSCF can send a SIP final non-2xx response to the S-CSCF and must include the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) but can also include parameters defined in other relevant extensions to the RFC.



The S-CSCF performs checks and if successful the SIP final non-2xx response is sent to the remote end.

The S-CSCF sends the SIP `ACK` request to the P-CSCF.

3.8 SUBSCRIBE Dialog

3.8.1 Preconditions

The subscribing user is registered or the subscribing AS is trusted.

3.8.2 Create SUBSCRIBE Dialog

This section defines how the subscriber (UE, P-CSCF, or AS) successfully creates a `SUBSCRIBE` initiated dialog. For details about the unsuccessful cases, see Section 3.8.4 Unsuccessful Cases at `SUBSCRIBE` on page 87.

The procedure is initiated by the subscriber, as defined in [RFC 3261 SIP: Session Initiation Protocol](#) and [RFC 3265 Session Initiation Protocol \(SIP\)-Specific Event Notification](#) with the clarifications in this section. Specific RFCs are also followed for specific events. For example, [RFC 3680 A Session Initiation Protocol \(SIP\) Event Package for Registrations](#) specifies the Reg-Event subscribe procedure.

The SIP `SUBSCRIBE` dialog is valid until the subscriber terminates the dialog explicitly or until the dialog expires or the notifier explicitly terminates the dialog.

The signaling sequence is shown in Figure 6.

When receiving an SIP request from the UE, the P-CSCF sends a SIP request to the S-CSCF and it must include the information listed in Table 50.

Table 50 SIP SUBSCRIBE Sent by P-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI, a tel URI, or a public GRUU as described by RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) giving the destination of this request.
To	M	A SIP URI or a tel URI giving the destination of this request.
From	M	A registered Public User Identity.
Contact	M	UE, a public GRUU associated with UE or P-CSCF SIP URI.

Header	Status	Procedure-Specific Values of the Parameter
Event	O ⁽¹⁾	When P-CSCF subscribes to reg-event, the value is set to reg .
Expires	O	Optional for requests initiated by UE. Mandatory for requests initiated by the P-CSCF. For Reg_Event subscriptions, the header is equal to the value of the Expires Header returned in the 200 OK (REGISTER) + 161. For subscription termination, the value is set to 0.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
Proxy-Authorization	O	See Table 58.
Route	M	For an initial SIP request, the Route includes the route set received in the Service-Route during the registration. SIP requests, within the created SIP dialog, include the recorded route set.
Record-Route	M ⁽²⁾	Must be included in the initial SIP request with the route set to be used within the created SIP dialog.
P-Charging-Vector	M	Includes the IMS Charging Identifier (ICID). The ICID is a globally unique value.
P-Asserted-Identity	M	The asserted registered Public User Identity indicated by the UE in the P-Preferred-Identity or From header. For SUBSCRIBES initiated by the P-CSCF, the value is set to the P-CSCF SIP URI.
P-Profile-Key	C	Included if the value of P-Preferred-Identity or From header, if P-Preferred-Identity is not received, matches the Wildcarded Identity.
Privacy	O	Included if the UE has included the Privacy header.

(1) The **Event** header is mandatory if P-CSCF subscribes to reg-event otherwise the P-CSCF forwards unaltered any value it received from the UE.

(2) The **Record-Route** is conditional and must be included when the **SUBSCRIBE** dialog is established by the initial **SUBSCRIBE** request and must be included otherwise.

When a **SUBSCRIBE** is received from an AS, the I-CSCF will proxy the request to the S-CSCF. If the received request contains a **Route** header with an **orig**



parameter, the `SUBSCRIBE` sent from I-CSCF must include the information listed in Table 51.

Table 51 SUBSCRIBE Sent by I-CSCF to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI, a tel URI, or a public GRUU as described by RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) giving the destination of this request.
To	M	A SIP URI or a tel URI giving the destination of this request.
From	M	A registered Public User Identity.
Contact	M	AS SIP URI
Event	O	Event type
Expires	O	Optional for requests initiated by AS. If subscription termination, the value is set to 0.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
Route	M	For an initial SIP request, the Route includes the route set received in the <code>Service-Route</code> during the registration. SIP requests, within the created SIP dialog, include the recorded route set.
P-Charging-Vector	M	Includes the IMS Charging Identifier (ICID). The ICID is a globally unique value.
P-Asserted-Identity	O	The asserted registered Public User Identity.
P-Profile-Key	C	Included if the I-CSCF receives a Wildcarded Identity in a Location Information Answer (LIA) from the HSS.
Privacy	O	Included if the AS has included the <code>Privacy</code> header.
P-Served-User-Identity	O	The served registered Public User Identity.
Resource-Priority	O	See Table 58.

The S-CSCF performs checks and if successful continues with next step.

If authentication is required, it authenticates the end user, and if authentication is successful or not used, continues with next step.

The S-CSCF inserts the own domain name as the value of the `orig-ioi` parameter in the `P-Charging-Vector` header if there is such a header; and depending on a configuration parameter record its route in the `Record-Route` header or does not record its route.

If applicable, the S-CSCF can add additional routing parameters to the `Request-URI`; for example NPDI, RN, CIC as described in [RFC 4694 Number Portability Parameters for the “tel” URI](#) and DAI as described in [draft-yu-tel-dai-05 DAI Parameter for the “tel” URI](#).

The S-CSCF sends the SIP request to the remote side or alternatively to an External Network through the BGCF and it includes the information listed in Table 52.

Table 52 SUBSCRIBE Request Sent by S-CSCF /BGCF to Remote Side

Header	Status	Procedure-Specific Values of the Parameter
Request-URI	M	A SIP URI, a tel URI, or a public GRUU as described by RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) giving the destination of this request. For a SIP request within a SIP dialog: The contact address received in the 2xx response when the SIP dialog was established.
To	M	A SIP URI or a tel URI giving the destination of this request.
From	M	A registered Public User Identity.
Contact	M	UE, a public GRUU associated with UE or P-CSCF SIP URI.
Event	O	The value is set to any value other than <code>reg</code> and is transferred unaltered.
Expires	O	Can be included if received by the S-CSCF.
Accept-Contact	O	Can be included if target with special capabilities is requested.
Reject-Contact	O	Can be included to prevent the use of targets with certain capabilities supported.
Record-Route	M ⁽¹⁾	Included in the initial SIP request with the route set to be used within the created SIP dialog.
Route	O ⁽²⁾	The route set recorded during the establishment of the SIP dialog minus those consumed by remote side and the CSCF.



Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	M	Includes the following: <ul style="list-style-type: none"> IMS Charging Identifier (ICID) as received from the P-CSCF Originating Inter-Operator Identifier (<code>orig-ioi</code>) is generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) if the request is sent outside a dialog. The <code>orig-ioi</code> parameter is not included if the request is sent within a dialog.
P-Charging-Function-Addresses	O	Includes the following, if <code>CscfTrustedNetwork</code> is TRUE: <ul style="list-style-type: none"> <code>P-Charging-Function-Addresses</code> header transfers the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in the S-CSCF by the HSS, to the next IMS CN node handling the SIP request.
P-Asserted-Identity	M	The asserted registered Public User Identity.
P-Asserted-Identity	O ⁽³⁾	A second asserted identity including a tel URI.
Privacy	O	Included if the UE has included the <code>Privacy</code> header.
Resource-Priority	O	See Table 58.

(1) The *Record-Route* is conditional for P-CSCF and must be included when the *SUBSCRIBE* dialog is established by the initial *SUBSCRIBE* request and must be included otherwise. The *Record-Route* for S-CSCF depends on a configuration parameter in the S-CSCF and the S-CSCF can not record its route.

(2) Mandatory for an initial SIP request.

(3) A second *P-Asserted-Identity* header must be included with a tel URI where a tel URI is provisioned for the user and the first *P-Asserted-Identity* contains a SIP URI.

When a confirmation is received, the remote side must send a SIP 2xx response to the S-CSCF and it includes the information listed in Table 53.

Table 53 SIP 2xx Response Sent by Remote Side to S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
P-Charging-Vector	O	Includes the following: <ul style="list-style-type: none"> IMS Charging Identifier (ICID) as received from the P-CSCF Originating Inter-Operator Identifier (<i>orig-ioi</i>) generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Terminating Inter-Operator Identifier (<i>term-ioi</i>) generated as described in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)
P-Asserted-Identity	M	Includes the value of the Request-URI in the request that generated this response.

Note: The P-Charging-Vector is only mandatory in the response to the initial SIP request.

The S-CSCF performs checks and if successful continues with next step.

The S-CSCF removes optionally, as defined by configuration, the *term-ioi* parameter if the parameter is included in the P-Charging-Vector header and the *orig-ioi* parameter if the parameter is included in the P-Charging-Vector header.

The S-CSCF sends the SIP 2xx response to the P-CSCF and it includes the information listed in Table 54.

Table 54 SIP 2xx Response Sent by S-CSCF to P-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Authentication-Info	O	See Table 59.
P-Charging-Vector	O ⁽¹⁾	Includes IMS Charging Identifier (ICID) as received from the P-CSCF.
P-Charging-Function-Addresses	O	Includes the addresses of the CDF (offline) and OCF (online) Charging functions, as populated in S-CSCF by HSS, to the next IMS CN node handling the SIP request.



Header	Status	Procedure-Specific Values of the Parameter
P-Asserted-Identity	M	Includes the value of the Request-URI in the request that generated this response.
Resource-Priority	O	See Table 59.

(1) The P-Charging-Vector is only mandatory in the response to the initial SIP request. The S-CSCF removes the *term-ioi* and *orig-ioi* parameters.

3.8.3 Originating Request Using SUBSCRIBE Dialog

The procedure in this section is only valid if the S-CSCF has included itself in the route set by adding a Record-Route header as described in the previous section.

This section defines the originating procedure for sending requests within a SUBSCRIBE dialog.

The requests that are typically sent within a SUBSCRIBE dialog are as follows:

- SUBSCRIBE request to refresh the dialog before it expires.
- SUBSCRIBE request to request termination of the dialog. This SUBSCRIBE request has an Expires header with the value zero.
- NOTIFY request to send the current state information to the user that initiated the SUBSCRIBE dialog.

The handling is identical to the description in Section 3.8.2 Create SUBSCRIBE Dialog on page 81.

3.8.4 Unsuccessful Cases at SUBSCRIBE

For protocol errors or errors outside the scope of this document, refer to [RFC 3261 SIP: Session Initiation Protocol](#) and [RFC 3265 Session Initiation Protocol \(SIP\)-Specific Event Notification](#) or relevant extensions to the RFC.

3.8.4.1 SUBSCRIBE Redirected by Network

The SIP 305 (User Proxy) response is returned by the S-CSCF if the S-CSCF fails to update the state of a user in the HSS because the HSS already has another serving the CSCF assigned for the user, that is, when the HSS returns the DIAMETER result code DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

The SIP 305 (User Proxy) response includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and [RFC 2617 HTTP](#)

[Authentication: Basic and Digest Access Authentication](#) described in this section and listed in Table 55.

Table 55 SIP 305 Use Proxy Sent by S-CSCF

Header	Status	Procedure-Specific Values of the Parameter
Contact	M	The <code>Contact</code> header contains the currently assigned S-CSCF returned in the Cx error response from the HSS.

3.8.4.2 SUBSCRIBE Rejected by Network

The CSCF can reject the SIP `SUBSCRIBE` request as the result of an unsuccessful procedure described in Section 3.8.2 Create `SUBSCRIBE` Dialog on page 81.

The status codes and reason phrases the CSCF can generate are listed in the *CSCF Fault Codes Catalogue*.

The procedure is initiated as described in Section 3.8.2 Create `SUBSCRIBE` Dialog on page 81.

If a `SUBSCRIBE` request is received by the E-CSCF, the E-CSCF rejects the message by sending a failure response 501 (Not Implemented), which includes the mandatory parameters defined in [RFC 3261 SIP: Session Initiation Protocol](#) and other relevant extensions to the RFC.

3.8.4.3 SUBSCRIBE Redirected by Remote Side

The CSCF/BGCF can redirect the request on a received 3xx response. Table 56 lists the important header in the redirect response.

Table 56 SIP 3xx Response

Header	Status	Procedure-Specific Values of the Parameter
Contact	M	The <code>Contact</code> header contains the new target to where the request must be redirected. Also, the <code>Contact</code> header can also contain SIP URI header components associated with the SIP URI of the returned new target, refer to RFC 3261 SIP: Session Initiation Protocol . Some or all these SIP URI header components can be included as headers in the outgoing redirected SIP request to the new target destination.



3.9 Network Monitoring

Network monitoring of the unreachable adjacent SIP nodes is possible by sending SIP `OPTIONS` requests. An interface can be regarded as unreachable because of various reasons, for example, time-out, ICMP failure, transport failure, or overload.

SIP `OPTIONS` requests are sent either according to the `Retry-After` header that can exist in the SIP error response SIP 503, or according to a configurable monitoring frequency until the node is considered reachable, that is, a SIP `OPTIONS` response other than SIP 503 is received.

The monitored interface is defined as specific combination of a source transport address together with a destination transport address. Network monitoring is configurable.





4 Information Model

This section describes supported SIP methods, status codes generated by the CSCF, and SIP requests and responses. Each table contains a description of the SIP header fields and their status. The status codes and notes describe the static behavior (whether the header field needs to present or not) that is required for the CSCF and the UE to interoperate.

Each header field has also a dynamic behavior, that is the actual format of the header field during use, described in a relevant RFC that is referenced.

4.1 Supported SIP Methods

The SIP methods are listed in Table 57 and [3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol \(SIP\) and Session Description Protocol \(SDP\)](#) as supported methods and are considered within this document.

Table 57 Supported SIP Methods

SIP Method	Sending	Receiving	Reference
ACK request	Supported	Supported	RFC 3261 SIP: Session Initiation Protocol
BYE request	Supported	Supported	RFC 3261 SIP: Session Initiation Protocol
CANCEL request	Supported	Supported	RFC 3261 SIP: Session Initiation Protocol
INVITE request	Supported	Supported	RFC 3261 SIP: Session Initiation Protocol
MESSAGE request	Supported	Supported	RFC 3428 Session Initiation Protocol (SIP) Extension for Instant Messaging
NOTIFY request	Supported	Supported	RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification



SIP Method	Sending	Receiving	Reference
OPTIONS request	Supported	Supported	RFC 3261 SIP: Session Initiation Protocol
PRACK request	Supported	Supported	RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
PUBLISH request	Supported	Supported	RFC 3903 Session Initiation Protocol (SIP) Extension for Event State Publication
REFER request	Supported	Supported	RFC 3515 The Session Initiation Protocol (SIP) Refer Method
REGISTER request	Supported	Supported	RFC 3261 SIP: Session Initiation Protocol
SUBSCRIBE request	Supported	Supported	RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification
UPDATE request	Supported	Supported	RFC 3311 The Session Initiation Protocol (SIP) UPDATE Method

4.2 Status Codes Generated by CSCF

Status codes generated by the CSCF are listed in the *CSCF Fault Codes Catalogue*.

The CSCF can also transfer status codes generated by other nodes.

Some generated reason phrases include a trailing hexadecimal code. These codes provide extra information to help identify the situation that triggered the response. For details of the hexadecimal code, refer to *CSCF SIP Hexadecimal Error Codes*.



4.3 Header Information in Requests, Common for Many Services

Header information in requests which are common for many services is listed in Table 58.

Table 58 Header Information in Requests

Header	Status	Procedure-Specific Values of the Parameter
Authorization	O	Included in this header is the <code>username</code> field, set to the value of the private user identity, see Section 3.2.1.1.1 Initial REGISTER on page 13. If the UE has valid credentials, then this information must also be included in the Authorization header (see Section 3.2.1.2 ReRegistration, Deregistration, and Registration Query on page 14). If GIBA is used, then this header must not be used. Included for Digest, AKA authentication, and Challenged NBA authentication.
Expires	O	Can include an expiry value valid for all contacts as defined by RFC 3261 SIP: Session Initiation Protocol .
P-Access- -Network- Info	O	For initial registration and NASS Bundled Authentication this header is mandatory and must include the following parameters: <code>access-type</code> , <code>network-provided</code> , and <code>dsl-location</code> . The parameter <code>dsl-location</code> must contain the line-identity as the first subparameter or prefixed by "line-id=". Other authentications schemes dependent the PANI header can have different formats for the <code>dsl-location</code> .
P-User- Database	O	Contains the HSS name. Defined by RFC 4457 The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-Header) .
Privacy	O	An optional parameter to indicate privacy of the P-Asserted-Identity. This element is included if the inviting user wants to be anonymous. This element is defined in RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks and its use is further specified in 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) .

Header	Status	Procedure-Specific Values of the Parameter
Proxy-Authorization	O	<p>Includes the following parameters:</p> <ul style="list-style-type: none"> • Digest as the authentication scheme • username=The user's Private User Identity • realm • nonce • uri with the Request-URI header in the SIP REGISTER request • response • cnonce • qop • nc <p>Can include the following parameter:</p> <ul style="list-style-type: none"> • opaque <p>The Proxy-Authorization header can only be included if the digest authentication procedure or Challenged NBA authentication is used.</p>
Via	M	<p>The Via header field indicates the transport used for the transaction and identifies the location where the response is to be sent.</p> <p>A Via header that includes the optional oc parameters in the received SIP request as described in RFC 7339 Session Initiation Protocol (SIP) Overload Control.</p> <p>If the Reacting Role for SIP Overload Control is enabled, the CSCF adds the oc and oc-algo parameters in the top Via header.</p>
Resource-Priority	O	<p>Includes the following:</p> <ul style="list-style-type: none"> • ets namespace – The ETS namespace is used to indicate that a call is eligible for priority treatment. • wps namespace – The WPS namespace is used to indicate the user's priority level.

Note: 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 the UE has to ensure that the given FQDN resolves to the IP address that is bound to the UE.



4.4 Header Information in Responses, Common for Many Services

Header information in responses which are common for many services is listed in Table 59.

Table 59 Header Information in Responses

Header	Status	Procedure-Specific Values of the Parameter
Authentication-Info	O	<p>Can include the following parameters:</p> <ul style="list-style-type: none"> • Digest as authentication scheme • nextnonce <p>If the header is included, the UE stores the value of the nextnonce as the new nonce value. The Authentication-Info header can be present for digest authentication or Challenged NBA authentication. The header must not be sent in an AKA case.</p>
Resource-Priority	O	<p>Includes the following:</p> <ul style="list-style-type: none"> • ets namespace – The ETS namespace is used to indicate that a call is eligible for priority treatment. • wps namespace – The WPS namespace is used to indicate the priority level of the user.
Via	M	<p>The Via header field indicates the transport used for the transaction and identifies the location where the response is to be sent.</p> <p>If the Reporting Role for SIP Overload Control is enabled and the oc parameter is present in the top via header, the CSCF modifies oc, oc-algo, adds oc-validity and oc-seq parameters according to RFC 7339 Session Initiation Protocol (SIP) Overload Control.</p>

4.5 Supported SIP Headers Within SIP Methods

All headers that are supported according to [3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol \(SIP\) and Session Description Protocol \(SDP\)](#) are listed in Table 60. A reference to the relevant RFC is indicated.

Table 60 Supported SIP Headers

Headers	Reference
Accept	RFC 3261 SIP: Session Initiation Protocol
Accept-Contact	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Accept-Encoding	RFC 3261 SIP: Session Initiation Protocol
Accept-Language	RFC 3261 SIP: Session Initiation Protocol
Alert-Info	RFC 3261 SIP: Session Initiation Protocol
Allow	RFC 3261 SIP: Session Initiation Protocol
Allow-Events	RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification
Answer-Mode	draft-willis-sip-answeralert-01 Requesting Answering and Alerting Modes for the Session Initiation Protocol (SIP)
Authorization	RFC 3261 SIP: Session Initiation Protocol RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
Call-ID	RFC 3261 SIP: Session Initiation Protocol
Call-Info	RFC 3261 SIP: Session Initiation Protocol
Contact	RFC 3261 SIP: Session Initiation Protocol
Content-Disposition	RFC 3261 SIP: Session Initiation Protocol
Content-Encoding	RFC 3261 SIP: Session Initiation Protocol
Content-Language	RFC 3261 SIP: Session Initiation Protocol
Content-Length	RFC 3261 SIP: Session Initiation Protocol
Content-Type	RFC 3261 SIP: Session Initiation Protocol



Headers	Reference
Cseq	RFC 3261 SIP: Session Initiation Protocol
Date	RFC 3261 SIP: Session Initiation Protocol
Error-info	RFC 3261 SIP: Session Initiation Protocol
Event	RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification
Expires	RFC 3261 SIP: Session Initiation Protocol
From	RFC 3261 SIP: Session Initiation Protocol
History-Info	RFC 4244 An Extension to the Session Initiation Protocol (SIP) for Request History Information⁽¹⁾
In-Reply-To	RFC 3261 SIP: Session Initiation Protocol
Join	RFC 3911 The Session Initiation Protocol (SIP) “Join” Header
Max-Breadth	draft-ietf-sip-fork-loop-fix-08 Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies
Max-Forwards	RFC 3261 SIP: Session Initiation Protocol
MIME-Version	RFC 3261 SIP: Session Initiation Protocol
Min-Expires	RFC 3261 SIP: Session Initiation Protocol
Min-SE	RFC 4028 Session Timers in the Session Initiation Protocol (SIP)
Organization	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)

Headers	Reference
P-Answer-State	draft-allen-sipping-poc-p-answer-stateheader-01 The P-Answer-State Header Extension to the Session Initiation Protocol (SIP) for the Open Mobile Alliance (OMA) Push to talk over Cellular (PoC)
P-Asserted-Identity	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Asserted-Service	draft-drage-sipping-service-identification A Session Initiation Protocol (SIP) Extension for the Identification of Services
P-Called-Party-ID	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Media-Authorization	RFC 3313 Private Session Initiation Protocol (SIP) Extensions for Media Authorization
P-Preferred-Identity	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Preferred-Service	draft-drage-sipping-service-identification A Session Initiation Protocol (SIP) Extension for the Identification of Services
P-Profile-Key	RFC 5002 The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)
P-User-Database	RFC 4457 The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-Header)



Headers	Reference
P-Visited-Network-ID	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Path	RFC 3327 Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
Priority	RFC 3261 SIP: Session Initiation Protocol
Priv-Answer-Mode	draft-willis-sip-answeralert-01 Requesting Answering and Alerting Modes for the Session Initiation Protocol (SIP)
Privacy	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Proxy-Authenticate	RFC 3261 SIP: Session Initiation Protocol
Proxy-Authorization	RFC 3261 SIP: Session Initiation Protocol
Proxy-Require	RFC 3261 SIP: Session Initiation Protocol
Rack	RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
Reason	RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
Record-Route	RFC 3261 SIP: Session Initiation Protocol
Referred-By	RFC 3892 The Session Initiation Protocol (SIP) Referred-By Mechanism
Refer-Sub	draft-ietf-sip-refer-with-norefersub-04 Suppression of Session Initiation Protocol REFER Method Implicit Subscription
Reject-Contact	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Replaces	RFC 3891 The Session Initiation Protocol (SIP) "Replaces" Header



Headers	Reference
Reply-To	RFC 3261 SIP: Session Initiation Protocol
Request-Disposition	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Require	RFC 3261 SIP: Session Initiation Protocol
Resource-Priority	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Retry-After	RFC 3261 SIP: Session Initiation Protocol
Route	RFC 3261 SIP: Session Initiation Protocol
Rseq	RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
Security-Client	RFC 3329 Security Mechanism Agreement for the Session Initiation Protocol (SIP)
Security-Server	RFC 3329 Security Mechanism Agreement for the Session Initiation Protocol (SIP)
Security-Verify	RFC 3329 Security Mechanism Agreement for the Session Initiation Protocol (SIP)
Server	RFC 3261 SIP: Session Initiation Protocol
Session-Expires	RFC 4028 Session Timers in the Session Initiation Protocol (SIP)
SIP-If-Match	RFC 3903 Session Initiation Protocol (SIP) Extension for Event State Publication
Subject	RFC 3261 SIP: Session Initiation Protocol
Supported	RFC 3261 SIP: Session Initiation Protocol
Timestamp	RFC 3261 SIP: Session Initiation Protocol
To	RFC 3261 SIP: Session Initiation Protocol



Headers	Reference
Unsupported	RFC 3261 SIP: Session Initiation Protocol
User-Agent	RFC 3261 SIP: Session Initiation Protocol
Via	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control
Warning	RFC 3261 SIP: Session Initiation Protocol
WWW-Authenticate	RFC 3261 SIP: Session Initiation Protocol

(1) Diversion header (RFC 5806) is also supported, although it is not required by TS24.229.

The different status codes used in the tables within this section are listed in Table 61.

Any headers that are received but not listed in this section are ignored.

Table 61 Key to Status Codes

Status Code	Meaning
m	Mandatory. The header is mandatory in the SIP message according to the present profile.
n/a	Not applicable. No relevant traffic case exists where the header could be present.
t	Transparent. This header is not generated by the CSCF. If this header is inserted by a remote end point, then this header is transported transparently by the CSCF. Depending on the services used, the interworking node can need to interpret and understand the header according to the relevant RFC.
x	Prohibited (excluded). The header is not allowed in the SIP message according to this profile. The header is removed by the CSCF if present.

The following tables list the methods that are to be supported according to [3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol \(SIP\) and Session Description Protocol \(SDP\)](#). Only the headers that are mandatory or that need a special comment are listed per SIP method.

4.5.1 Supported Headers Within ACK Request

Supported headers within ACK requests are listed in Table 62.

Table 62 ACK Request

Headers	Sending	Receiving	Reference
Accept-Contact	See Section 4.5.26.6 Contact (2) in 200 OK Responses on page 162	See Section 4.5.26.6 Contact (2) in 200 OK Responses on page 162	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.30 Reject-Contact on page 167	See Section 4.5.26.30 Reject-Contact on page 167	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)



Headers	Sending	Receiving	Reference
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.2 Supported Headers Within BYE Request

Supported headers within BYE requests are listed in Table 63.

Table 63 BYE Request

Headers	Sending	Receiving	Reference
Accept-Contact	See Section 4.5.26.6 Contact (2) in 200 OK Responses on page 162	See Section 4.5.26.6 Contact (2) in 200 OK Responses on page 162	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	See Section 4.5.26.16 P-Charging-Vector on page 165	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authorization	See Section 4.5.26.25 Proxy-Authorization on page 167	See Section 4.5.26.25 Proxy-Authorization on page 167	RFC 3261 SIP: Session Initiation Protocol
Record-Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.8 Content-Type on page 162	See Section 4.5.26.8 Content-Type on page 162	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)



Headers	Sending	Receiving	Reference
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol
User-Agent	See Section 4.5.26.39 User-Agent on page 170	See Section 4.5.26.39 User-Agent on page 170	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.3

Supported Headers Within BYE Response

Supported headers within BYE responses are listed in Table 64.

Table 64 BYE Response

Headers	Sending	Receiving	Reference
Authentication-Info	See Section 4.5.26.3 Authentication-Info on page 161	See Section 4.5.26.3 Authentication-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol

Headers	Sending	Receiving	Reference
From	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3261 SIP: Session Initiation Protocol
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3261 SIP: Session Initiation Protocol
P-Charging-Vector	See Section 4.5.26.16 P-Charging-Vector on page 165	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authenticate	See Section 4.5.26.24 Proxy-Authenticate on page 166	See Section 4.5.26.24 Proxy-Authenticate on page 166	RFC 3261 SIP: Session Initiation Protocol
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
To	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.4 Supported Headers Within CANCEL Request

Supported headers within CANCEL requests are listed in Table 65.

Table 65 Cancel Request

Headers	Sending	Receiving	Reference
Accept-Contact	See Section 4.5.26.6 Contact (2) in 200 OK Responses on page 162	See Section 4.5.26.6 Contact (2) in 200 OK Responses on page 162	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Reason	See Section 4.5.26.27 Reason on page 167	t	RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
Record-Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.8 Content-Type on page 162	See Section 4.5.26.8 Content-Type on page 162	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.5

Supported Headers Within CANCEL Response

Supported headers within CANCEL responses are listed in Table 66.

Table 66 Cancel Response

Headers	Sending	Receiving	Reference
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.6 Supported Headers Within INVITE Request

Supported headers within `INVITE` requests are listed in Table 67.

Table 67 *INVITE Request*

Headers	Sending	Receiving	Reference
Accept-Contact	See Section 4.5.26.2 Accept-Contact on page 161	See Section 4.5.26.2 Accept-Contact on page 161	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Contact	m	m	RFC 3261 SIP: Session Initiation Protocol

Headers	Sending	Receiving	Reference
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol
Min-SE	m	See Section 4.5.26.11 Min-SE on page 163	RFC 4028 Session Timers in the Session Initiation Protocol (SIP)
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Asserted-Identity	m	m	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Called-Party-ID	m	m	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)



Headers	Sending	Receiving	Reference
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Preferred-Identity	n/a	See Section 4.5.26.17 P-Preferred-Identity on page 165	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Profile-Key	See Section 4.5.26.18 P-Profile-Key on page 165	See Section 4.5.26.18 P-Profile-Key on page 165	RFC 5002 The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)
P-User-Database	See Section 4.5.26.19 P-User-Database on page 166	See Section 4.5.26.19 P-User-Database on page 166	RFC 4457 The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-Header)
Priority	See Section 4.5.26.22 Priority on page 166	See Section 4.5.26.22 Priority on page 166	RFC 3261 SIP: Session Initiation Protocol
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)



Headers	Sending	Receiving	Reference
Proxy-Authorization	See Section 4.5.26.25 Proxy-Authorization on page 167	See Section 4.5.26.25 Proxy-Authorization on page 167	RFC 3261 SIP: Session Initiation Protocol
Proxy-Require	See Section 4.5.26.26 Proxy-Require on page 167	See Section 4.5.26.26 Proxy-Require on page 167	RFC 3261 SIP: Session Initiation Protocol
Record-Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.30 Reject-Contact on page 167	See Section 4.5.26.30 Reject-Contact on page 167	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Session-Expires	m	See Section 4.5.26.34 Session-Expires on page 169	RFC 4028 Session Timers in the Session Initiation Protocol (SIP)
Supported	See Section 4.5.26.35 Supported (1) on page 169	See Section 4.5.26.35 Supported (1) on page 169	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
User-Agent	See Section 4.5.26.39 User-Agent on page 170	See Section 4.5.26.39 User-Agent on page 170	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.7 Supported Headers Within INVITE Response

Supported headers within `INVITE` responses are listed in Table 68.

Table 68 *INVITE Response*

Headers	Sending	Receiving	Reference
Authentication-Info	See Section 4.5.26.3 Authentication-Info on page 161	See Section 4.5.26.3 Authentication-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Contact	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol

Headers	Sending	Receiving	Reference
Min-SE	m	See Section 4.5.26.11 Min-SE on page 163	RFC 4028 Session Timers in the Session Initiation Protocol (SIP)
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Asserted-Identity	m	m	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Preferred-Identity	n/a	See Section 4.5.26.17 P-Preferred-Identity on page 165	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks



Headers	Sending	Receiving	Reference
Proxy-Authenticate	See Section 4.5.26.24 Proxy-Authenticate on page 166	See Section 4.5.26.24 Proxy-Authenticate on page 166	RFC 3261 SIP: Session Initiation Protocol
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Record-Route	See Section 4.5.26.29 Record-Route (2) on page 167	See Section 4.5.26.29 Record-Route (2) on page 167	RFC 3261 SIP: Session Initiation Protocol
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Session-Expires	m	See Section 4.5.26.34 Session-Expires on page 169	RFC 4028 Session Timers in the Session Initiation Protocol (SIP)
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.8 Supported Headers Within MESSAGE Request

Supported headers within MESSAGE requests are listed in Table 69.

Table 69 MESSAGE Request

Headers	Sending	Receiving	Reference
Accept-Contact	See Section 4.5.26.2 Accept-Contact on page 161	See Section 4.5.26.2 Accept-Contact on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3261 SIP: Session Initiation Protocol
P-Asserted-Identity	See Section 4.5.26.13 P-Asserted-Identity on page 164	See Section 4.5.26.13 P-Asserted-Identity on page 164	RFC 3261 SIP: Session Initiation Protocol
P-Called-Party-ID	m	m	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)



Headers	Sending	Receiving	Reference
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Profile-Key	See Section 4.5.26.18 P-Profile-Key on page 165	See Section 4.5.26.18 P-Profile-Key on page 165	RFC 5002 The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)
P-User-Database	See Section 4.5.26.19 P-User-Database on page 166	See Section 4.5.26.19 P-User-Database on page 166	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Proxy-Authorization	See Section 4.5.26.25 Proxy-Authorization on page 167	See Section 4.5.26.25 Proxy-Authorization on page 167	RFC 3261 SIP: Session Initiation Protocol
Proxy-Require	See Section 4.5.26.26 Proxy-Require on page 167	See Section 4.5.26.26 Proxy-Require on page 167	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Record-Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.30 Reject-Contact on page 167	See Section 4.5.26.30 Reject-Contact on page 167	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Supported	t	t	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol
User-Agent	See Section 4.5.26.39 User-Agent on page 170	See Section 4.5.26.39 User-Agent on page 170	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.9

Supported Headers Within MESSAGE Response

Supported headers within MESSAGE responses are listed in Table 70.



Table 70 MESSAGE Response

Headers	Sending	Receiving	Reference
Authentication-Info	See Section 4.5.26.3 Authentication-Info on page 161	See Section 4.5.26.3 Authentication-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Asserted-Identity	See Section 4.5.26.13 P-Asserted-Identity on page 164	See Section 4.5.26.13 P-Asserted-Identity on page 164	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)



Headers	Sending	Receiving	Reference
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authenticate	See Section 4.5.26.24 Proxy-Authenticate on page 166	See Section 4.5.26.24 Proxy-Authenticate on page 166	RFC 3261 SIP: Session Initiation Protocol
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control
WWW-Authenticate	n/a	n/a	RFC 3261 SIP: Session Initiation Protocol

4.5.10 Supported Headers Within NOTIFY Request

Supported headers within NOTIFY requests are listed in Table 71.



Table 71 NOTIFY Request

Headers	Sending	Receiving ⁽¹⁾	Reference
Accept-Contact	See Section 4.5.26.2 Accept-Contact on page 161	See Section 4.5.26.2 Accept-Contact on page 161	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Contact	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Content-Type	See Section 4.5.26.8 Content-Type on page 162	See Section 4.5.26.8 Content-Type on page 162	RFC 3261 SIP: Session Initiation Protocol RFC 3680 A Session Initiation Protocol (SIP) Event Package for Registrations
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)

Headers	Sending	Receiving ⁽¹⁾	Reference
P-Charging-Vector	See Section 4.5.26.16 P-Charging-Vector on page 165	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authorization	See Section 4.5.26.25 Proxy-Authorization on page 167	See Section 4.5.26.25 Proxy-Authorization on page 167	RFC 3261 SIP: Session Initiation Protocol
Proxy-Require	See Section 4.5.26.26 Proxy-Require on page 167	See Section 4.5.26.26 Proxy-Require on page 167	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.8 Content-Type on page 162	See Section 4.5.26.8 Content-Type on page 162	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Supported	t	t	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving ⁽¹⁾	Reference
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

(1) Normally the *NOTIFY* request is not sent by a UE, instead the request originates in an AS or S-CSCF. The CSCF does not, however, exclude the possibility to subscribe to events that are generated by a UE.

NOTIFY request can also carry Registration Event XML[®] file in the message body, when requested in *SUBSCRIBE* request message through event type for Reg-Event. For an example of Registration Event XML file, refer to Section 8 on page 179.

4.5.11

Supported Headers Within NOTIFY Response

Supported headers within *NOTIFY* responses are listed in Table 72.

Table 72 *NOTIFY Response*

Headers	Sending	Receiving	Reference
Authentication-Info	See Section 4.5.26.3 Authentication-Info on page 161	See Section 4.5.26.3 Authentication-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol

Headers	Sending	Receiving	Reference
From	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	See Section 4.5.26.16 P-Charging-Vector on page 165	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Proxy-Authenticate	See Section 4.5.26.24 Proxy-Authenticate on page 166	See Section 4.5.26.24 Proxy-Authenticate on page 166	RFC 3261 SIP: Session Initiation Protocol
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
To	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.12 Supported Headers Within OPTIONS Request

Supported headers within OPTIONS requests are listed in Table 73.

Table 73 *OPTIONS Request*

Headers	Sending	Receiving	Reference
Accept-Contact	See Section 4.5.26.2 Accept-Contact on page 161	See Section 4.5.26.2 Accept-Contact on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol

Headers	Sending	Receiving	Reference
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Asserted-Identity	See Section 4.5.26.13 P-Asserted-Identity on page 164	See Section 4.5.26.13 P-Asserted-Identity on page 164	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Called-Party-ID	m	m	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)



Headers	Sending	Receiving	Reference
Proxy-Authorization	See Section 4.5.26.25 Proxy-Authorization on page 167	See Section 4.5.26.25 Proxy-Authorization on page 167	RFC 3261 SIP: Session Initiation Protocol
Proxy-Require	See Section 4.5.26.26 Proxy-Require on page 167	See Section 4.5.26.26 Proxy-Require on page 167	RFC 3261 SIP: Session Initiation Protocol
Record-Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.30 Reject-Contact on page 167	See Section 4.5.26.30 Reject-Contact on page 167	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Supported	t	t	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol
User-Agent	See Section 4.5.26.39 User-Agent on page 170	See Section 4.5.26.39 User-Agent on page 170	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.13 Supported Headers Within OPTIONS Response

Supported headers within OPTIONS responses are listed in Table 74.

Table 74 OPTIONS Response

Headers	Sending	Receiving	Reference
Authentication-Info	See Section 4.5.26.3 Authentication-Info on page 161	See Section 4.5.26.3 Authentication-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Asserted-Identity	See Section 4.5.26.13 P-Asserted-Identity on page 164	See Section 4.5.26.13 P-Asserted-Identity on page 164	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks



Headers	Sending	Receiving	Reference
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authenticate	See Section 4.5.26.24 Proxy-Authenticate on page 166	See Section 4.5.26.24 Proxy-Authenticate on page 166	RFC 3261 SIP: Session Initiation Protocol
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Supported	See Section 4.5.26.37 Supported (3) on page 169	t	RFC 3261 SIP: Session Initiation Protocol RFC 6140 Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)
To	m	m	RFC 3261 SIP: Session Initiation Protocol

Headers	Sending	Receiving	Reference
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.14 Supported Headers Within PRACK Request

Supported headers within PRACK requests are listed in Table 75.

Table 75 PRACK Request

Headers	Sending	Receiving	Reference
Accept-Contact	See Section 4.5.26.2 Accept-Contact on page 161	See Section 4.5.26.2 Accept-Contact on page 161	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	See Section 4.5.26.16 P-Charging-Vector on page 165	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authorization	See Section 4.5.26.25 Proxy-Authorization on page 167	See Section 4.5.26.25 Proxy-Authorization on page 167	RFC 3261 SIP: Session Initiation Protocol
Proxy-Require	See Section 4.5.26.26 Proxy-Require on page 167	See Section 4.5.26.26 Proxy-Require on page 167	RFC 3261 SIP: Session Initiation Protocol
Rack	m	m	RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
Record-Route	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Reject-Contact	See Section 4.5.26.30 Reject-Contact on page 167	See Section 4.5.26.30 Reject-Contact on page 167	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.15 Supported Headers Within PRACK Response

Supported headers within `PRACK` responses are listed in Table 76.

Table 76 *PRACK Response*

Headers	Sending	Receiving	Reference
Authentication-Info	See Section 4.5.26.3 Authenticat ion-Info on page 161	See Section 4.5.26.3 Authenticat ion-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Contact	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	See Section 4.5.26.16 P-Charging-Vector on page 165	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authenticate	See Section 4.5.26.24 Proxy-Authenticate on page 166	See Section 4.5.26.24 Proxy-Authenticate on page 166	RFC 3261 SIP: Session Initiation Protocol
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)

Headers	Sending	Receiving	Reference
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.16 Supported Headers Within PUBLISH Request

Supported headers within PUBLISH requests are listed in Table 77.

Table 77 PUBLISH Request

Headers	Sending ⁽¹⁾	Receiving	Reference
Accept-Contact	See Section 4.5.26.2 Accept-Contact on page 161	See Section 4.5.26.2 Accept-Contact on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending ⁽¹⁾	Receiving	Reference
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Asserted-Identity	m	m	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Called-Party-ID	m	x	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)

Headers	Sending ⁽¹⁾	Receiving	Reference
P-Profile-Key	See Section 4.5.26.18 P-Profile-Key on page 165	See Section 4.5.26.18 P-Profile-Key on page 165	RFC 5002 The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)
P-User-Database	See Section 4.5.26.19 P-User-Database on page 166	See Section 4.5.26.19 P-User-Database on page 166	RFC 4457 The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-Header)
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Proxy-Authorization	See Section 4.5.26.25 Proxy-Authorization on page 167	See Section 4.5.26.25 Proxy-Authorization on page 167	RFC 3261 SIP: Session Initiation Protocol
Proxy-Require	See Section 4.5.26.26 Proxy-Require on page 167	See Section 4.5.26.26 Proxy-Require on page 167	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.30 Reject-Contact on page 167	See Section 4.5.26.30 Reject-Contact on page 167	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Supported	t	t	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending ⁽¹⁾	Receiving	Reference
User-Agent	See Section 4.5.26.39 User-Agent on page 170	See Section 4.5.26.39 User-Agent on page 170	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

(1) Normally the *PUBLISH* request is not routed to the terminating UE, instead the request is terminated in an AS. The CSCF does not however exclude the possibility for an UE to publish event state to another UE.

4.5.17

Supported Headers Within PUBLISH Response

Supported headers within *PUBLISH* responses are listed in Table 78.

Table 78 *PUBLISH Response*

Headers	Sending	Receiving ⁽¹⁾	Reference
Authentication-Info	See Section 4.5.26.3 Authentication-Info on page 161	See Section 4.5.26.3 Authentication-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol

Headers	Sending	Receiving ⁽¹⁾	Reference
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Asserted-Identity	m	m	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authenticate	See Section 4.5.26.24 Proxy-Authenticate on page 166	See Section 4.5.26.24 Proxy-Authenticate on page 166	RFC 3261 SIP: Session Initiation Protocol
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)



Headers	Sending	Receiving ⁽¹⁾	Reference
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

(1) Normally the *PUBLISH* request is not routed to the terminating UE, instead the request is terminated in an AS. The CSCF does not however exclude the possibility for an UE to publish event state to another UE.

4.5.18 Supported Headers Within REFER Request

Supported headers within *REFER* requests are listed in Table 79.

Table 79 *REFER* Request

Headers	Sending	Receiving	Reference
Accept-Contact	See Section 4.5.26.2 Accept-Contact on page 161	See Section 4.5.26.2 Accept-Contact on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Contact	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Called-Party-ID	m	m	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Profile-Key	See Section 4.5.26.18 P-Profile-Key on page 165	See Section 4.5.26.18 P-Profile-Key on page 165	RFC 5002 The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)



Headers	Sending	Receiving	Reference
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Proxy-Authorization	See Section 4.5.26.25 Proxy-Auth orization on page 167	See Section 4.5.26.25 Proxy-Auth orization on page 167	RFC 3261 SIP: Session Initiation Protocol
Proxy-Require	See Section 4.5.26.26 Proxy-Req uire on page 167	See Section 4.5.26.26 Proxy-Req uire on page 167	RFC 3261 SIP: Session Initiation Protocol
Record-Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.30 Reject-Con tact on page 167	See Section 4.5.26.30 Reject-Con tact on page 167	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Pri ority on page 168	See Section 4.5.26.32 Resource-Pri ority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Supported	t	t	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
User-Agent	See Section 4.5.26.39 User-Agent on page 170	See Section 4.5.26.39 User-Agent on page 170	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.19 Supported Headers Within REFER Response

Supported headers within `REFER` responses are listed in Table 80.

Table 80 *REFER Response*

Headers	Sending	Receiving	Reference
Authentication-Info	See Section 4.5.26.3 Authentication-Info on page 161	See Section 4.5.26.3 Authentication-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Contact	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authenticate	See Section 4.5.26.24 Proxy-Authenticate on page 166	See Section 4.5.26.24 Proxy-Authenticate on page 166	RFC 3261 SIP: Session Initiation Protocol
Privacy	See Section 4.5.26.23 Privacy on page 166	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Record-Route	See Section 4.5.26.29 Record-Route (2) on page 167	See Section 4.5.26.29 Record-Route (2) on page 167	RFC 3261 SIP: Session Initiation Protocol
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)



Headers	Sending	Receiving	Reference
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.20 Supported Headers Within REGISTER Request

Supported headers within REGISTER requests are listed in Table 81.

Table 81 REGISTER Request

Headers	Sending	Receiving	Reference
Authorization	See Section 4.5.26.4 Authorization on page 161	See Section 4.5.26.4 Authorization on page 161	RFC 3261 SIP: Session Initiation Protocol RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Contact	See Section 4.5.26.5 Contact (1) in Register Requests on page 162	See Section 4.5.26.5 Contact (1) in Register Requests on page 162	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
Expires	See Section 4.5.26.9.1 Expires in REGISTER on page 163	See Section 4.5.26.9.1 Expires in REGISTER on page 163	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Called-Party-Id	o	o	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)



Headers	Sending	Receiving	Reference
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-User-Database	See Section 4.5.26.19 P-User-Database on page 166	See Section 4.5.26.19 P-User-Database on page 166	RFC 4457 The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-Header)
P-Visited-Network-ID	See Section 4.5.26.20 P-Visited-Network-ID on page 166	See Section 4.5.26.20 P-Visited-Network-ID on page 166	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Path	See Section 4.5.26.21 Path on page 166	See Section 4.5.26.21 Path on page 166	RFC 3327 Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
Proxy-Authorization	See Section 4.5.26.25 Proxy-Authorization on page 167	See Section 4.5.26.25 Proxy-Authorization on page 167	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Require	See Section 4.5.26.31 Require on page 168	See Section 4.5.26.31 Require on page 168	RFC 3261 SIP: Session Initiation Protocol RFC 3840 Indicating User Agent Capabilities in the Session Initiation Protocol (SIP) RFC 4028 Session Timers in the Session Initiation Protocol (SIP) RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP) RFC 6140 Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Supported	See Section 4.5.26.35 Supported (1) on page 169	See Section 4.5.26.35 Supported (1) on page 169	RFC 3261 SIP: Session Initiation Protocol RFC 4028 Session Timers in the Session Initiation Protocol (SIP) RFC 5627 Obtaining and Using Globally Routable User agent URIs (GRUUs) in the Session Initiation Protocol (SIP)
To	m	m	RFC 3261 SIP: Session Initiation Protocol
User-Agent	See Section 4.5.26.39 User-Agent on page 170	See Section 4.5.26.39 User-Agent on page 170	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.21

Supported Headers Within REGISTER Response

Supported headers within REGISTER responses are listed in Table 82.

Table 82 REGISTER Response

Headers	Sending	Receiving	Reference
Authentication-Info	See Section 4.5.26.3 Authentication-Info on page 161	See Section 4.5.26.3 Authentication-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Contact	See Section 4.5.26.6 Contact (2) in 200 OK Responses on page 162	See Section 4.5.26.6 Contact (2) in 200 OK Responses on page 162	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Min-Expires	See Section 4.5.26.10 Min-Expires on page 163	See Section 4.5.26.10 Min-Expires on page 163	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Associated-URI	See Section 4.5.26.14 P-Associated-URI on page 165	See Section 4.5.26.14 P-Associated-URI on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)

Headers	Sending	Receiving	Reference
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Path	See Section 4.5.26.21 Path on page 166	See Section 4.5.26.21 Path on page 166	RFC 3327 Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
Service-Route	See Section 4.5.26.33 Service-Route on page 169	See Section 4.5.26.33 Service-Route on page 169	RFC 3608 Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control
WWW-Authenticate	See Section 4.5.26.40 WWW-Authenticate on page 170	See Section 4.5.26.40 WWW-Authenticate on page 170	RFC 3261 SIP: Session Initiation Protocol



4.5.22

Supported Headers Within SUBSCRIBE Request

Supported headers within SUBSCRIBE Requests are listed in Table 83.

Table 83 SUBSCRIBE Request

Headers	Sending ⁽¹⁾	Receiving	Reference
Accept	See Section 4.5.26.1 Accept on page 161	See Section 4.5.26.1 Accept on page 161	RFC 3261 SIP: Session Initiation Protocol
Accept-Contact	See Section 4.5.26.2 Accept-Contact on page 161	See Section 4.5.26.2 Accept-Contact on page 161	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Contact	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
Event	m	m	RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification RFC 3680 A Session Initiation Protocol (SIP) Event Package for Registrations
Expires	o See Section 4.5.26.9.2 Expires in SUBSCRIBE on page 163	o	RFC 3261 SIP: Session Initiation Protocol RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification

Headers	Sending ⁽¹⁾	Receiving	Reference
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Asserted-Identity	See Section 4.5.26.13 P-Asserted-Identity on page 164	See Section 4.5.26.13 P-Asserted-Identity on page 164	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Preferred-Identity	n/a	See Section 4.5.26.17 P-Preferred-Identity on page 165	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks



Headers	Sending ⁽¹⁾	Receiving	Reference
P-Profile-Key	See Section 4.5.26.18 P-Profile-Key on page 165	See Section 4.5.26.18 P-Profile-Key on page 165	RFC 5002 The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)
P-User-Database	See Section 4.5.26.19 P-User-Database on page 166	See Section 4.5.26.19 P-User-Database on page 166	RFC 4457 The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-Header)
Privacy	n/a	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Proxy-Authorization	See Section 4.5.26.25 Proxy-Authorization on page 167	See Section 4.5.26.25 Proxy-Authorization on page 167	RFC 3261 SIP: Session Initiation Protocol
Proxy-Require	See Section 4.5.26.26 Proxy-Require on page 167	See Section 4.5.26.26 Proxy-Require on page 167	RFC 3261 SIP: Session Initiation Protocol
Record-Route	See Section 4.5.26.28 Record-Route (1) on page 167	See Section 4.5.26.28 Record-Route (1) on page 167	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.30 Reject-Contact on page 167	See Section 4.5.26.30 Reject-Contact on page 167	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol

Headers	Sending ⁽¹⁾	Receiving	Reference
Supported	t	t	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

(1) Normally the *SUBSCRIBE* request is routed to an AS. If the event-type is reg-event, the *SUBSCRIBE* request is not routed to an AS.

4.5.23

Supported Headers Within SUBSCRIBE Response

Supported headers within *SUBSCRIBE* responses are listed in Table 84.

Table 84 *SUBSCRIBE* Response

Headers	Sending	Receiving	Reference
Authentication-Info	See Section 4.5.26.3 Authentication-Info on page 161	See Section 4.5.26.3 Authentication-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Contact	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Min-Expires	See Section 4.5.26.10 Min-Expires on page 163	See Section 4.5.26.10 Min-Expires on page 163	RFC 3261 SIP: Session Initiation Protocol
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Asserted-Identity	See Section 4.5.26.13 P-Asserted-Identity on page 164	See Section 4.5.26.13 P-Asserted-Identity on page 164	RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authenticate	See Section 4.5.26.24 Proxy-Authenticate on page 166	See Section 4.5.26.24 Proxy-Authenticate on page 166	RFC 3261 SIP: Session Initiation Protocol

Headers	Sending	Receiving	Reference
Privacy	t	See Section 4.5.26.23 Privacy on page 166	RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
Record-Route	See Section 4.5.26.29 Record-Route (2) on page 167	See Section 4.5.26.29 Record-Route (2) on page 167	RFC 3261 SIP: Session Initiation Protocol
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.24 Supported Headers Within UPDATE Request

Supported headers within UPDATE requests are listed in Table 85.

Table 85 UPDATE Request

Headers	Sending	Receiving	Reference
Accept-Contact	See Section 4.5.26.2 Accept-Contact on page 161	See Section 4.5.26.2 Accept-Contact on page 161	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
Contact	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol
Max-Forwards	m	m	RFC 3261 SIP: Session Initiation Protocol
Min-SE	m	See Section 4.5.26.11 Min-SE on page 163	RFC 4028 Session Timers in the Session Initiation Protocol (SIP)
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	m	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)



Headers	Sending	Receiving	Reference
Proxy-Authorization	See Section 4.5.26.25 Proxy-Authorization on page 167	See Section 4.5.26.25 Proxy-Authorization on page 167	RFC 3261 SIP: Session Initiation Protocol
Proxy-Require	See Section 4.5.26.26 Proxy-Require on page 167	See Section 4.5.26.26 Proxy-Require on page 167	RFC 3261 SIP: Session Initiation Protocol
Record-Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Reject-Contact	See Section 4.5.26.30 Reject-Contact on page 167	See Section 4.5.26.30 Reject-Contact on page 167	RFC 3841 Caller Preferences for the Session Initiation Protocol (SIP)
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Route	m	m	RFC 3261 SIP: Session Initiation Protocol
Session-Expires	m	See Section 4.5.26.34 Session-Expires on page 169	RFC 3261 SIP: Session Initiation Protocol
Supported	t	t	RFC 3261 SIP: Session Initiation Protocol
To	m	m	RFC 3261 SIP: Session Initiation Protocol



Headers	Sending	Receiving	Reference
User-Agent	See Section 4.5.26.39 User-Agent on page 170	See Section 4.5.26.39 User-Agent on page 170	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.25

Supported Headers Within UPDATE Response

Supported headers within UPDATE requests are listed in Table 86.

Table 86 UPDATE Response

Headers	Sending	Receiving	Reference
Authentication-Info	See Section 4.5.26.3 Authentication-Info on page 161	See Section 4.5.26.3 Authentication-Info on page 161	RFC 3261 SIP: Session Initiation Protocol
Call-ID	m	m	RFC 3261 SIP: Session Initiation Protocol
Contact	m	m	RFC 3261 SIP: Session Initiation Protocol
Content-Length	m	See Section 4.5.26.7 Content-Length on page 162	RFC 3261 SIP: Session Initiation Protocol
Cseq	m	m	RFC 3261 SIP: Session Initiation Protocol
From	m	m	RFC 3261 SIP: Session Initiation Protocol

Headers	Sending	Receiving	Reference
Min-SE	m	See Section 4.5.26.11 Min-SE on page 163	RFC 4028 Session Timers in the Session Initiation Protocol (SIP)
P-Access-Network-Info	See Section 4.5.26.12 P-Access-Network-Info on page 163	See Section 4.5.26.12 P-Access-Network-Info on page 163	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Function-Addresses	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	See Section 4.5.26.15 P-Charging-Function-Addresses on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
P-Charging-Vector	See Section 4.5.26.16 P-Charging-Vector on page 165	See Section 4.5.26.16 P-Charging-Vector on page 165	RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
Proxy-Authenticate	See Section 4.5.26.24 Proxy-Authenticate on page 166	See Section 4.5.26.24 Proxy-Authenticate on page 166	RFC 3261 SIP: Session Initiation Protocol
Resource-Priority	See Section 4.5.26.32 Resource-Priority on page 168	See Section 4.5.26.32 Resource-Priority on page 168	RFC 4412 Communications Resource Priority for the Session Initiation Protocol (SIP)
Session-Expires	m	See Section 4.5.26.34 Session-Expires on page 169	RFC 4028 Session Timers in the Session Initiation Protocol (SIP)



Headers	Sending	Receiving	Reference
To	m	m	RFC 3261 SIP: Session Initiation Protocol
Unsupported	See Section 4.5.26.38 Unsupported on page 169	See Section 4.5.26.38 Unsupported on page 169	RFC 3261 SIP: Session Initiation Protocol
Via	m	m	RFC 3261 SIP: Session Initiation Protocol RFC 7339 Session Initiation Protocol (SIP) Overload Control

4.5.26 Header Notes

4.5.26.1 Accept

The `Accept` header can be included by the subscriber when subscribing to an event. The header specifies the format of the body type in the `NOTIFY` request.

4.5.26.2 Accept-Contact

The `Accept-Contact` header can be included by the originating UE when requesting support for certain capabilities by the terminating UE (contact). The terminating S-CSCF only routes the request to terminating UE's (contacts) that matches the capabilities requested. Only `Accept-Contact` headers of the initial request are considered. `Accept-Contact` headers in the requests within an established dialog are not considered

4.5.26.3 Authentication-Info

If digest authentication or Challenged NBA authentication is used, then the `Authentication-Info` header can be included in SIP 2xx responses. If the header is included, it contains the `nextnonce` parameter that must be used by the UE as the new `nonce` value, and `Digest` as authentication scheme.

The `Authentication-Info` header is not sent in NBA, GIBA, or AKA case.

4.5.26.4 Authorization

If digest authentication is used, then the `Authorization` header is to be present in the request message. Some UEs do not send the SIP

`Authorization` header in the first `REGISTER`, and S-CSCF supports it with Digest Authentication for UEs not sending SIP Authorization header in the first `REGISTER`.

If user authentication is active in S-CSCF, then it is recommended that a pre-emptive authorization header is sent in the request message.

If GIBA authentication is used, then the `Authorization` header must not be present in the request message. If NBA authentication is used, then the `Authorization` header is optional. In both cases where the SIP Authorization header is missing, the private user identity is derived from the `To` header.

If Challenged NBA authentication is used, then the `Authorization` header is expected to be present in the request message. It is not necessary to send the SIP Authorization header in the first `REGISTER`.

4.5.26.5 Contact (1) in Register Requests

The `Contact` header is mandatory except when a `REGISTER` request message is sent to request the total list of contacts for a Public User Identity.

4.5.26.6 Contact (2) in 200 OK Responses

The `Contact` header is present with the `Expire` parameter containing the contact expiration time in SIP 2xx responses when the user has one or more contacts currently registered in the CSCF.

The `Contact` header is present with the `Expire` parameter set to value zero in SIP 2xx responses for all contacts that have been deregistered in the CSCF.

The `Contact` header can contain the public GRUU (`pub-gruu`) parameter of the registered contact which is generated by the S-CSCF as part of the registration process when GRUU is requested by UE and CSCF supports GRUU.

4.5.26.7 Content-Length

The `Content-Length` header is mandatory if TCP is used as transport. The CSCF always includes a `Content-Length` in SIP requests sent to the UE independent of transport.

4.5.26.8 Content-Type

The `SUBSCRIBE` request can contain an `Accept` header field. If the header field is present, the `NOTIFY` must include the `Content-Type` header field and it must include “application/reginfo+xml” for subscriptions for `Reg-Event`.



4.5.26.9 Expires

This section describes Expires in REGISTER and Expires in SUBSCRIBE.

4.5.26.9.1 Expires in REGISTER

An expiration time received in the Contact header is valid for that contact only. An expiration time received in the Expires header is valid for all contacts without defined expiration times.

4.5.26.9.2 Expires in SUBSCRIBE

If no Expires header is present in SUBSCRIBE request, the implied default is defined by the event package being used.

If subscriber sends SUBSCRIBE with Expires of value 0 while initiating the SUBSCRIBE dialog, that is, at initial subscription, it implies that an immediate fetch of state without a continuous subscription is in effect, that is, exercises polling of registration state.

The SUBSCRIBE request with an Expires header of value 0 for already established subscription, constitutes a request to unsubscribe from an event. It also causes a fetch of state.

4.5.26.10 Min-Expires

The Min-Expires header is present in the SIP response 423 (Interval Too Brief). This indicates that the expiry time is too short.

4.5.26.11 Min-SE

The Min-SE header can be present in the request if session timers are requested and the UE or the CSCF request a minimum session interval higher than the default.

4.5.26.12 P-Access-Network-Info

The P-Access-Network-Info is mandatory within the home network. It is not sent outside the trusted domain.

For NASS Bundled Authentication, this header must include a networkprovided parameter, an access-type parameter, and a dsl-location parameter in the initial REGISTER request.

The P-Access-Network-Info is asserted by the P-CSCF before forwarding to the next node. The assertion ensures that the access network type in the PANI header is coherent with the IP address of the sender. PANI Header assertion is an optional feature which can be enabled by configuration.

When `RoamingAwarenessInfo`, including `SgsnMccMnc` and `GPRSRoamingStatus`, is available in the user profile, a new `PANI` header is generated by S-CSCF as follows:

- The access-type is created with value `3GPP-GERAN`
- The access-info is created with the following parameter values:
 - `Cgi-3gpp` = the value of `SgsnMccMnc` received from the HSS
 - The network-provided is added
 - `x-roaming-status` = the value of `GPRSRoamingStatus` received from the HSS

When there is no `PANI` header received, or there is no network-provided `PANI` header received, this created `PANI` header is added in the outgoing request. When there is a network-provided `PANI` header received, this created `PANI` header is added to replace the received network-provided `PANI` header.

When a `PANI` header is received from the P-CSCF as a SIP header, or a `PANI` header is received from LRF as a SIP URI header component, or both, the E-CSCF sends the `PANI` to a remote side.

4.5.26.13

P-Asserted-Identity

The `P-Asserted-identity` is mandatory outside a dialog. It is not sent within a dialog.

The E-CSCF adds `P-Asserted-Identity` in the request to PSAP directly, through BGCF or through IBCF as follows:

- If there is any PAI received in 3xx from LRF, the whole PAI value received is proxied to PSAP.
- If there is no PAI received in 3xx from LRF, and there are PAIs received from P-CSCF, the PAI received from P-CSCF is proxied to PSAP.
- If there is no PAI received either from LRF or P-CSCF, and a PAI has been successfully created by E-CSCF from available PPI header information, the PAI created is sent to PSAP.

The E-CSCF adds `P-Asserted-Identity` in the 1xx or 2xx response to P-CSCF as follows:

- If the original `Req-URI` received is an Emergency Service URN, add `P-Asserted-Identity` with the preconfigured tel URI emergency number.
- If the original `Req-URI` received is a dialed string (either in tel URI or SIP URI), add `P-Asserted-Identity` with the dialed string (either in tel URI or SIP URI) that the E-CSCF has saved from the original request received.



4.5.26.14 **P-Associated-URI**

The P-Associated-URI is present in SIP 2xx responses when the user has an Implicit Registration Set with additional associated public user identities with the Public User Identity that is being registered.

The P-Associated-URI is present in SIP 2xx responses if user is a Distinct IMPU and has an Implicit Registration Set with one or more Wildcarded Public User Identities, if identities are not barred.

For de-REGISTRATION requests, the S-CSCF does not include the P-Associated-URI header in the 200 (OK) response.

The S-CSCF can add the ServicePriorityLevel value in the P-Associated-URI header to the P-CSCF (for example, P-Associated-URI: <sip:u0000000000@cscf.com>; service-priority=3). The S-CSCF receives the XML data type ServicePriorityLevel (one ServicePriorityLevel per IMPU) in the SAA message during initial registration and stores it within the user's profile.

4.5.26.15 **P-Charging-Function-Addresses**

The P-Charging-Function-Addresses are mandatory within the home network. It is sent to other networks based on configuration.

4.5.26.16 **P-Charging-Vector**

The P-Charging-Vector header must be present but absence of the P-Charging-Vector header is also accepted.

4.5.26.17 **P-Preferred-Identity**

The P-Preferred-Identity (PPI) header can be removed by the P-CSCF, ignored by I-CSCF and S-CSCF.

If a PPI is received from P-CSCF or LRF, the PPI is not proxied by the E-CSCF to the PSAP.

The P-Preferred-Identity is removed by the E-CSCF in 1xx or 2xx response to the P-CSCF.

4.5.26.18 **P-Profile-Key**

If the identity of a served user in the request, which was taken from P-Preferred-Identity header or From header, if P-Preferred-Identity header is not received, matches a registered wildcarded identity, originating P-CSCF includes the wildcarded identity value in the P-Profile-Key header field as defined in [RFC 5002 The Session Initiation Protocol \(SIP\) P-Profile-Key Private Header \(P-Header\)](#) and sends the request to the S-CSCF.

If a Wildcarded Identity, in either Wildcarded-Public-Identity AVP (634) or Wildcarded-Public-User-Identity AVP (636), is received from the HSS in a Location Information Answer (LIA), the I-CSCF includes the received Wildcarded Identity in the `P-Profile-Key` header as defined in [RFC 5002 The Session Initiation Protocol \(SIP\) P-Profile-Key Private Header \(P-Header\)](#) and sends the request to the S-CSCF or the AS.

The I-CSCF removes the `P-Profile-Key` header field, if the I-CSCF receives the `P-Profile-Key` header field in a SIP request or response.

An AS can include `P-Profile-Key` in a request to the S-CSCF or the I-CSCF.

The S-CSCF removes the `P-Profile-Key` when forwarding the SIP request to the next SIP entity after service invocation.

4.5.26.19 P-User-Database

The `P-User-Database` header is included by the I-CSCF.

4.5.26.20 P-Visited-Network-ID

The `P-Visited-Network-ID` header is included by the P-CSCF and is checked by the I-CSCF.

4.5.26.21 Path

The `Path` header is not normally to be included by the UE. There can however be cases where a SIP proxy is deployed in the path between the UE and the P-CSCF, the `Path` header can be used in such cases.

4.5.26.22 Priority

The `Priority` header can be present in emergency calls.

4.5.26.23 Privacy

The `Privacy` header must be present in the request/response if privacy is requested by originating/terminating UE.

4.5.26.24 Proxy-Authenticate

If digest authentication or Challenged NBA authentication is used, then the `Proxy-Authenticate` header is present in a SIP 407 (Proxy Authentication required) response indicating Digest in the authentication scheme token.



4.5.26.25 Proxy-Authorization

If digest authentication is used, then the `Proxy-Authorization` header is to be present in the request message. The `Proxy-Authorization` header is sent from the P-CSCF to the S-CSCF and is removed before sending to the terminating network.

If GIBA is active for the user, then the `Proxy-Authorization` header is not used.

If Challenged NBA authentication is used, the `Proxy-Authorization` header in `INVITE` request can include a nonce and a nonce-count.

4.5.26.26 Proxy-Require

The `Proxy-Require` header can be included by the originating UE when requiring support for certain capabilities or procedures by the CSCF, or both. If the requested capability is not supported by CSCF, the CSCF rejects the request.

4.5.26.27 Reason

If the `Reason` header is present in a received `CANCEL` request, the CSCF copies the `Reason` header to the outgoing `CANCEL` request.

When the CSCF generates a `CANCEL` request a `Reason` header with protocol SIP, cause and text are included.

4.5.26.28 Record-Route (1)

The S-CSCF adds `Record-Route` based on configuration. The P-CSCF always adds `Record-Route`.

4.5.26.29 Record-Route (2)

The `Record-Route` header must be present in SIP 1xx and 2xx responses that are part of a dialog establishment.

4.5.26.30 Reject-Contact

The `Reject-Contact` header can be included by the originating UE for requesting to exclude terminating UEs which support certain capabilities. The CSCF does not route the request to those excluded terminating UEs (contacts). Only `Reject-Contact` headers of the initial request are considered. `Reject-Contact` headers in the requests within an established dialog are not considered.

4.5.26.31 **Require**

The UE can include a `Require` header field with the value “pref” that indicates that the CSCF must store feature parameters included in the `Contact` header. The CSCF stores feature parameters even if the “pref” is missing.

The UE can include a `Require` header field with the value “gin” that indicates that the CSCF must support registration of a “bnc” contact.

The UE can include a `Require` header field containing the option tag “gruu” to indicate that GRUU has to be provided by S-CSCF as part of registration process.

All other `Require` header field values included in the Register request are rejected with 420 (`Bad Extension`).

4.5.26.32 **Resource-Priority**

The `Resource-Priority` header can be included to prioritize the request within the IMS Core. The CSCF prioritizes the request using the `Resource-Priority` values (`ets`, `wps`) and includes `Resource-Priority` in the outgoing SIP request.

The `ets` namespace is used to indicate that a call is eligible for priority treatment (also referred to as priority indicator) and it is set or reset when a call is identified as an NGN GETS call. The `ets` namespace has five values designated as `ets.0` through `ets.4`. The `ets.0` is used for NGN GETS voice. Other `ets.x` values are reserved for future use (for example, for NGN GETS data, video).

The `wps` namespace is used to indicate the user’s priority level and it is set when the user is authenticated and authorized for NGN GETS calling privileges. The `WPS` namespace value indicates the five priority levels where `wps.0` is the highest priority and `wps.4` is the lowest priority.

If the priority feature is enabled in the CSCF node, the following rules are applied to `Resource-Priority` values. The CSCF supports `Resource-Priority` with values `ets.0`, `wps.0-4`. The `ets.0` is mandatory, and no multiple namespaces are allowed. A SIP 400 (`Bad Request`) response with a 417 code in the `Reason` header field is returned if:

- If multiple `ets` or `wps` values are defined (for example, `ets.0`, `wps.3`, `wps.4`).
- The `ets.0` is not present (for example, `wps.4`) or `ets` value is non-zero.

If `wps` is not in the range of 0–4, then it is ignored and the call is treated as a normal call.

When the incoming SIP Response is received, the CSCF proxies the received `Resource-Priority` header in the SIP Response to the next hop.



4.5.26.33 Service-Route

The S-CSCF always include `Service-Route` header in 200 (OK) SIP response for non-emergency registrations. If there is an emergency registration, if the configuration parameter `scscfEmergencyRegServiceRouteBehavior` is set to EXCLUDE, `Service-Route` header is omitted from 200 (OK) response.

4.5.26.34 Session-Expires

`Session-Expires` header into the SIP request message or response. The recommendation in this profile is that the Originating and Terminating UE must support session timers according to [RFC 4028 Session Timers in the Session Initiation Protocol \(SIP\)](#) and must therefore include a `Session-Expires` header in the request and corresponding response.

4.5.26.35 Supported (1)

If the UE supports certain capabilities or procedures, the UE can indicate this by including a `Supported` header into the SIP message.

The CSCF checks that the `Supported` header includes `Timer`, to enable time supervisions or not.

4.5.26.36 Supported (2)

The UE can include `Supported` header containing the option tag `path`. If the header is not present, then the P-CSCF inserts the header before forwarding the request. The S-CSCF requires that the option tag `path` is received.

The UE can include a `Supported` header containing the option tag “gruu” to indicate that the GRUU needs to be provided as part of registration process if GRUU is supported by S-CSCF.

4.5.26.37 Supported (3)

The CSCF (P-, I-, S-, and E-) and BCF include following supported capabilities when its capabilities are requested; `Timer`, `Path`, `Pref`, `100rel`, `Precondition`, `gin`, `gruu`. When CSCF/BCF proxies a 200 OK, the `Supported` header is transparent.

4.5.26.38 Unsupported

The `Unsupported` header is included in the response if the request contained a `Require` or `Proxy-Require` header field listing a feature not supported by either the CSCF (`Proxy-Require`) or the terminating UE (`Require`).



4.5.26.39 User-Agent

If `User-Agent` restriction is defined in the CSCF and is activated, then the `User-Agent` header is mandatory. If `User-Agent` restriction is not defined, then the `User-Agent` header is ignored and sent transparently to the other end point (or ignored for a `REGISTER` request).

4.5.26.40 WWW-Authenticate

If digest authentication, IMS AKA authentication or Challenged NBA authentication is present in SIP 401 (Unauthorized) response indicating Digest in the authentication scheme token.



5 Formal Syntax

Not applicable.





6 Security Considerations

6.1 IPsec Tunnel

The communication over the Mg, Mj, Mk, Mm/Mx, Mr, Mw, and I2 interfaces can be secured using IPsec (Zb interface) on the IP transport layer, refer to [3GPP TS 33.210 3G security; Network Domain Security \(NDS\); IP network layer security](#).

IPsec tunnels can be defined between the two nodes. IKEv1 performs mutual authentication between the two nodes and establishes an IKE Security Association that includes shared secret information used to establish IPsec SAs. Different forms of authentication and encryptions can be selected when defining the IPsec tunnels. For the native CSCF, refer to *Security Management User Guide*, and for the virtual CSCF, refer to *eVIP Management Guide*.





7 Related Standards

The CSCF is compliant to standards [3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol \(SIP\) and Session Description Protocol \(SDP\)](#) and [RFC 3261 SIP: Session Initiation Protocol](#).

The main deviations from the standards are as follows:

- The P-CSCF, E-CSCF, and BCF nodes only support IPv4 interfaces. They support the handling of IPv6 addresses in SIP headers but cannot route a message based on an IPv6 address. When IPv6 addresses are present, a means to route the message to the next hop using an IPv4 address, for example, Record-Route, Path, Via, must be available.
- The Service-Route header is not sent to the UE.
- TLS is not supported.

The following standards are also applicable:

- [draft-allen-sipping-poc-p-answer-stateheader-01 The P-Answer-State Header Extension to the Session Initiation Protocol \(SIP\) for the Open Mobile Alliance \(OMA\) Push to talk over Cellular \(PoC\)](#)
- [draft-drage-sipping-service-identification A Session Initiation Protocol \(SIP\) Extension for the Identification of Services](#)
- [draft-ietf-sip-fork-loop-fix-08 Addressing an Amplification Vulnerability in Session Initiation Protocol \(SIP\) Forking Proxies](#)
- [draft-ietf-sip-refer-with-norefersub-04 Suppression of Session Initiation Protocol REFER Method Implicit Subscription](#)
- [draft-willis-sip-answeralert-01 Requesting Answering and Alerting Modes for the Session Initiation Protocol \(SIP\)](#)
- [RFC 2543 SIP: Session Initiation Protocol \(1999\)](#)
- [RFC 2617 HTTP Authentication: Basic and Digest Access Authentication](#)
- [RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol \(SIP\)](#)
- [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#)
- [RFC 3265 Session Initiation Protocol \(SIP\)-Specific Event Notification](#)
- [RFC 3310 Hypertext Transfer Protocol \(HTTP\) Digest Authentication Using Authentication and Key Agreement \(AKA\)](#)
- [RFC 3311 The Session Initiation Protocol \(SIP\) UPDATE Method](#)

- [RFC 3313 Private Session Initiation Protocol \(SIP\) Extensions for Media Authorization](#)
- [RFC 3323 A Privacy Mechanism for the Session Initiation Protocol \(SIP\)](#)
- [RFC 3325 Private Extensions to the Session Initiation Protocol \(SIP\) for Asserted Identity within Trusted Networks](#)
- [RFC 3326 The Reason Header Field for the Session Initiation Protocol \(SIP\)](#)
- [RFC 3327 Session Initiation Protocol \(SIP\) Extension Header Field for Registering Non-Adjacent Contacts](#)
- [RFC 3329 Security Mechanism Agreement for the Session Initiation Protocol \(SIP\)](#)
- [RFC 3428 Session Initiation Protocol \(SIP\) Extension for Instant Messaging](#)
- [RFC 3455 Private Header \(P-Header\) Extensions to the Session Initiation Protocol \(SIP\) for the 3rd-Generation Partnership Project \(3GPP\)](#)
- [RFC 3515 The Session Initiation Protocol \(SIP\) Refer Method](#)
- [RFC 3608 Session Initiation Protocol \(SIP\) Extension Header Field for Service Route Discovery During Registration](#)
- [RFC 3680 A Session Initiation Protocol \(SIP\) Event Package for Registrations](#)
- [RFC 3840 Indicating User Agent Capabilities in the Session Initiation Protocol \(SIP\)](#)
- [RFC 3841 Caller Preferences for the Session Initiation Protocol \(SIP\)](#)
- [RFC 3891 The Session Initiation Protocol \(SIP\) “Replaces” Header](#)
- [RFC 3892 The Session Initiation Protocol \(SIP\) Referred-By Mechanism](#)
- [RFC 3903 Session Initiation Protocol \(SIP\) Extension for Event State Publication](#)
- [RFC 4028 Session Timers in the Session Initiation Protocol \(SIP\)](#)
- [RFC 4119 A Presence-based GEOPRIV Location Object Format](#)
- [RFC 4244 An Extension to the Session Initiation Protocol \(SIP\) for Request History Information](#)
- [RFC 4412 Communications Resource Priority for the Session Initiation Protocol \(SIP\)](#)
- [RFC 4457 The Session Initiation Protocol \(SIP\) P-User-Database Private-Header \(P-Header\)](#)
- [RFC 4694 Number Portability Parameters for the “tel” URI](#)



- [draft-yu-tel-dai-05 DAI Parameter for the “tel” URI](#)
- [RFC 5002 The Session Initiation Protocol \(SIP\) P-Profile-Key Private Header \(P-Header\)](#)
- [RFC 5031 A Uniform Resource Name \(URN\) for Emergency and Other Well-Known Services](#)
- [RFC 5502 The SIP P-Served-User Private-Header \(P-Header\) for the 3GPP IP Multimedia \(IM\) Core Network \(CN\) Subsystem](#)
- [RFC 5626 Managing Client-Initiated Connections in the Session Initiation Protocol \(SIP\)](#)
- [RFC 5627 Obtaining and Using Globally Routable User agent URIs \(GRUUs\) in the Session Initiation Protocol \(SIP\)](#)
- [RFC 5628 Registration Event Package Extension for Session Initiation Protocol \(SIP\) Globally Routable User agent URIs \(GRUUs\)](#)
- [RFC 6140 Registration for Multiple Phone Numbers in the Session Initiation Protocol \(SIP\)](#)
- [RFC 7339 Session Initiation Protocol \(SIP\) Overload Control](#)
- [3GPP TS 23.003 Numbering, addressing and identification](#)
- [3GPP TS 24.292 IP Multimedia \(IM\) Core Network \(CN\) subsystem Centralized Services \(ICS\); Stage 3](#)
- [3GPP TS 33.203 3G security; Access security for IP-based services](#)
- [3GPP TS 33.210 3G security; Network Domain Security \(NDS\); IP network layer security](#)





8 Example of XML Document Sent in NOTIFY

During subscription to RegEvent, the notifier (S-CSCF) sends NOTIFY request whenever a state changes for a registration with the current registration state of the user. Whenever the registration state is changed, a new NOTIFY request is sent to the subscriber. The notification message contains an XML document with registration information, such as the new state and the event that triggered the state change. All subscribers must support the `application/reginfo+xml` format for the XML registration information, as described in [RFC 3680 A Session Initiation Protocol \(SIP\) Event Package for Registrations](#).

The principle layout of the XML document is shown in Figure 24.

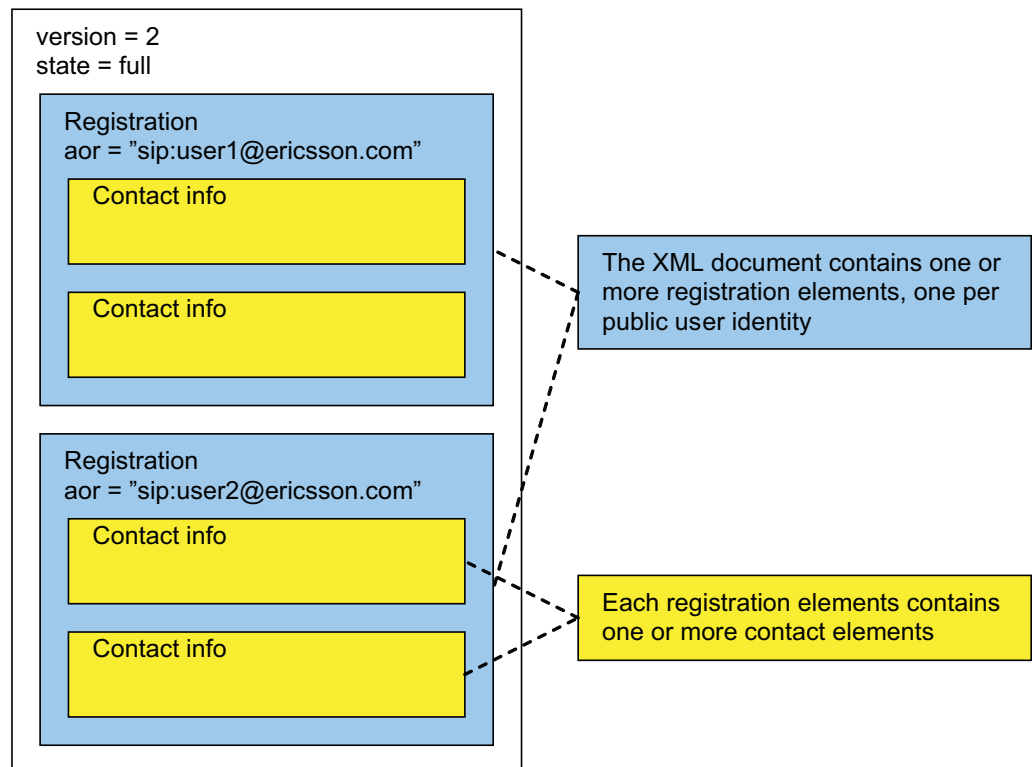


Figure 24 Principle Layout XML Document

The complete XML schema for `reginfo` is defined in [RFC 3680 A Session Initiation Protocol \(SIP\) Event Package for Registrations](#).

An example of a registration information document is shown in Figure 25.

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema" instance
  version="2" state="full">
  <registration aor="sip:+468121000005@cscf21.lab" id="199861061"
    state="active">
    <contact id="2285698402" state="active" event="registered">
      <uri>sip:u000005@10.50.215.127:5065</uri>
      <unknown-param name="+g.poc.talkburst"></unknown-param>
    </contact>
  </registration>
  <registration aor="tel:+468121000005" id="3977664237" state="active">
    <contact id="2285698402" state="active" event="registered">
      <uri>sip:u000005@10.50.215.127:5065</uri>
      <unknown-param name="+g.poc.talkburst"></unknown-param>
    </contact>
  </registration>
</reginfo>
```

Figure 25 Example Registration Information Document

The XML document makes use of XML namespaces for identifying registration information documents and document fragments. [RFC 3680 A Session Initiation Protocol \(SIP\) Event Package for Registrations](#) defines the namespace URI to use:

```
urn:ietf:params:xml:ns:reginfo
```

The registration information document begins with the root element tag `reginfo`. The `reginfo` element has the following two attributes that must be present:

- `version`: Starts at 0 and increments with one for each new generated document.
- `state`: Indicates whether the document contains the full registration state (`full`) or whether it contains only information on those registrations which have currently been changed (`partial`). The state value is controlled by the configurable parameter `Full State Notification`.

The `reginfo` element can contain any number of registration subelements each of which contains the registration state for a particular Address Of Record. The `registration` element contains the following three attributes that must be present:

- `aor`: Contains the URI which is the Address Of Record (Public User Identity) this registration refers to.
- `id`: Identifies this registration, it must be unique among all other id attributes present in the `registration` elements. A hashed value of the `aor` is used.



- `state`: Indicates the state of the registration for this Public User Identity. The S-CSCF supports the state `active` (at least one contact registered) and `terminated` (the last contact was currently unregistered). The defined state `init` (no contact registered) is not supported.

The `registration` element can contain any number of `contact` subelements. The `contact` element must contain the following three attributes:

- `id`: Identifies this contact, it must be unique among all other `id` attributes present in the `contact` elements. The `id` is unique, except when the same contact URI is shared by multiple contacts, and those contacts have the same `id`. Therefore, the optional SIP Instance indicator must be provided by the contacts in this case as the differentiator. The `id` is a hashed value of the contact URI.
- `state`: Indicates the state of the contact, valid states are `active` and `terminated`.
- `event`: Indicates the event which caused the contact to go into its current state.

The following additional attributes are optional in the `contact` element:

- Duration-registered
- Expires
- Q-value
- Call-ID
- CSeq

The following additional subelement are in the `contact` element:

- URI
- Display-Name (optional)
- Unknown-param (Multiple elements can be included containing additional contact-header parameters besides the once included in the `contact` element attributes)
- Pub-gruu (public GRUU received from registration when GRUU is required by UE)

Other parameters found in the `Contact` header which are not specified in [RFC 3261 SIP: Session Initiation Protocol](#) are stored in the `unknown-param` subelement of the `contact` element. An example of information stored in the `unknown-param` attribute is the SIP Instance indicator which is used to differentiate contacts which have the same contact URI.

All Public User Identities belonging to the same private user identity are added in separate registration subelements.

The notifier (S-CSCF) can also include some proprietary elements, as feature-caps-header element (carrying Access Transfer Control Function (ATCF) information), impi element (carrying IMPI information), P-Visited-Network-ID header element (carrying PVNI information), and P-Access-Network-Info header element (carrying PANI information).

Inclusion of the elements is configurable.

The following is an example of XML file with included public GRUU and proprietary elements.

```
<?xml version="1.0" encoding="utf-8"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo" xmlns:xsi="http://www.w3.org/2001/XMLSchema" \=>
  version="0" state="full">
    <registration aor="sip:user@example.com" id="as9" state="active">
      <contact id="76" state="active" event="registered" duration-registered="7322" q="0.8">
        <uri>sip:user@pc887.example.com</uri>
        <unknown-param name="+sip.instance">
          "<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6">" </unknown-param>
        <pub-gruu xmlns="urn:ietf:params:xml:ns:gruuinfo">
          "sip:user@example.com;gr= urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6"</pub-gruu>
        <feature-caps-header xmlns="urn:com:ericsson:schema:xml:ims:feature-caps-header-\=>
          regevent-extension">
            *;+g.3gpp.atcf-mgmt="<urn:atcf.visited2.net>";+g.3gpp.atcf-path="<urn:sip:\=>
              termsdgfdwe@atcf.visited2.net>";+g.3gpp.mid-call;+g.3gpp.srvcc-alerting
          </feature-caps-header>
        <feature-caps-header xmlns="urn:com:ericsson:schema:xml:ims:feature-caps-header-\=>
          regevent-extension">
            *;+g.3gpp.atcf="<urn:tel:+1-237-888-9999>";
          </feature-caps-header>
        <impi xmlns="urn:com:ericsson:schema:xml:ims:impi-regevent-extension\=>
          ">alice@ericsson.com</impi>
        <pani xmlns="urn:com:ericsson:schema:xml:ims:pani-regevent-extension">
          3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=31122512001b20701;network-provided
        </pani>
        <pvni xmlns="urn:com:ericsson:schema:xml:ims:pvni-regevent-extension">
          ims.groupb.uscellular.com
        </pvni>
      </contact>
      <contact id="77" state="terminated" event="expired" duration-registered="3600" q="0.5">
        <uri>sip:user@university.edu</uri>
        <feature-caps-header xmlns="urn:com:ericsson:schema:xml:ims:feature-caps-header-\=>
          regevent-extension">
            *;+g.3gpp.atcf-mgmt="<urn:sip:atcf.visited2.net>";+g.3gpp.atcf-path="<urn:sip:\=>
              termsdgfdwe@atcf.visited2.net>";+g.3gpp.mid-call;+g.3gpp.srvcc-alerting
          </feature-caps-header>
        <feature-caps-header xmlns="urn:com:ericsson:schema:xml:ims:feature-caps-header-\=>
          regevent-extension">
            *;+g.3gpp.atcf="<urn:tel:+1-237-888-9999>";
          </feature-caps-header>
        <impi xmlns="urn:com:ericsson:schema:xml:ims:impi-regevent-extension\=>
          ">alice@ericsson.com</impi>
        <pani xmlns="urn:com:ericsson:schema:xml:ims:pani-regevent-extension">
          3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=31122512001b20701;network-provided
        </pani>
        <pvni xmlns="urn:com:ericsson:schema:xml:ims:pvni-regevent-extension">
          ims.groupb.uscellular.com
        </pvni>
      </contact>
    </registration>
  </reginfo>
```