

CSCF ISC 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	3
2.2	Services	4
2.3	Encapsulation and Addressing	4
3	Procedures	5
3.1	Lower-Level Procedures	6
3.2	Invocation of AS at Registration	16
3.3	Invocation of AS, Non-REGISTER	28
3.4	AS Acting as SIP UAC	37
4	Information Model	45
4.1	Supported SIP Methods	45
4.2	SIP Header Information	45
5	Formal Syntax	47
6	Security Considerations	49
6.1	IPsec Tunnel	49
7	Related Standards	51





1 Introduction

This document describes the IMS Service Control (ISC) interface between the Serving Call Session Control Function (S-CSCF) and the Application Server (AS), and the Ma interface between the Interrogating Call Session Control Function (I-CSCF) and the Application Server (AS).

This document is based on the CSCF Mw Interface. It only describes the details that are relevant to the ISC interface and Ma interface. For details that are not mentioned, refer to *CSCF Mw Interface*.

Unless otherwise indicated, SIP headers are handled transparently by the S-CSCF in the ISC interface, and by the I-CSCF in the Ma interface.

For information about the status codes that are generated by the CSCF, refer to *CSCF Fault Codes Catalogue*.





2 Interface Overview

This section describes the ISC interface between the S-CSCF and the AS, and the Ma interface between the I-CSCF and the AS, shown in Figure 1.

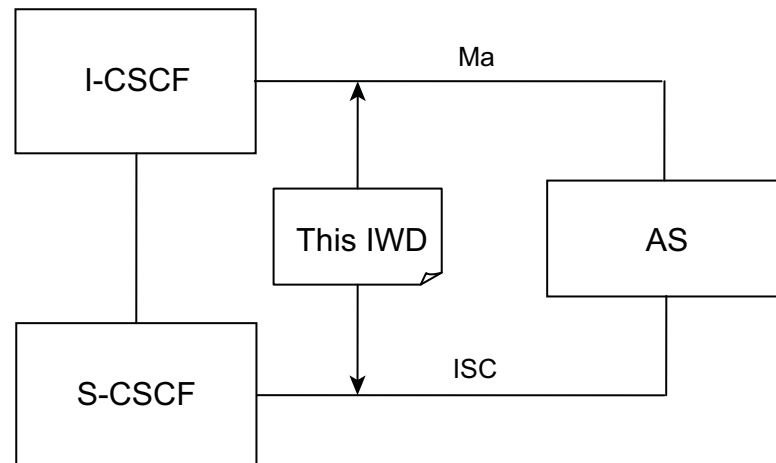


Figure 1 Interface Entities

The SIP protocol is used on the ISC and Ma interfaces.

2.1 Interface Role

This section describes the services that the S-CSCF and I-CSCF offer to the Application Server (AS).

2.1.1 ISC Interface

The ISC interface is used between the S-CSCF and the AS.

In the context of the ISC interface, the following roles exist:

- User Agent Client (UAC)
- User Agent Server (UAS)

2.1.2 Ma Interface

The Ma interface is used between the I-CSCF and the AS.

The I-CSCF sends requests on the Ma interface to the AS for Public Service Identities (PSI) or wildcarded PSIs (wPSI).

The I-CSCF can receive SIP Requests on the Ma interface directly from the AS when the served users S-CSCF is unknown.

2.2 Services

The services offered by the S-CSCF are shown in Table 1.

Table 1 Offered Services by S-CSCF

Offered Service	Description
Registration	The AS is started when the S-CSCF has successfully processed a REGISTER request and the trigger criteria are met.
Invocation of the AS	The AS is started when the trigger criteria are met for a non-REGISTER SIP request. The AS can act as a proxy, a User Agent Server (UAS), or a Back-to-Back User Agent (B2BUA).
AS acting as a SIP UAC	The AS initiates a SIP session or a SIP standalone request.

The services offered by the I-CSCF are shown in Table 2.

Table 2 Offered Services by I-CSCF

Offered Service	Description
Invocation of the AS	When a non-REGISTER SIP request is routed to an AS directly, the AS is started. The AS acts as an UAS.
AS acting as a SIP UAC	The AS initiates a SIP session or a SIP standalone request.

2.3 Encapsulation and Addressing

The CSCF supports IPv4/IPv6 dual stack and SIP on User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). The CSCF terminates a TCP connection after a configurable time of inactivity.

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

In addition, the CSCF supports event notifications and registration event package as defined in the [RFC 3265 Session Initiation Protocol \(SIP\) – Specific Event Notification](#) and [RFC 3680 A Session Initiation Protocol Event Package for Registrations](#) specifications.

3 Procedures

An overview of the overall use between the S-CSCF and the AS is shown in Figure 2.

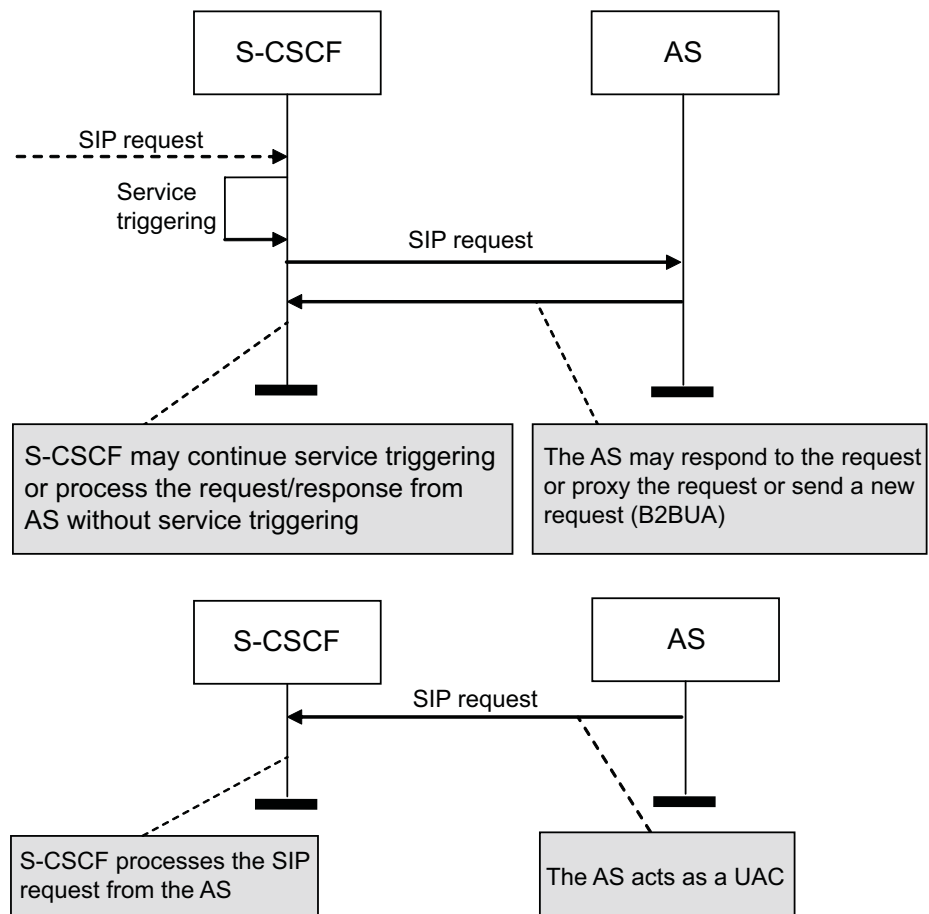


Figure 2 Overall Use Between S-CSCF and AS

After service triggering, the S-CSCF proxies the request to the AS. The AS can act as a UAS, proxy, or B2BUA. The AS can initiate a SIP procedure acting as a User Agent Client (UAC) and send the request to the S-CSCF.

An overview of the overall use between the I-CSCF and the AS is shown in Figure 3.

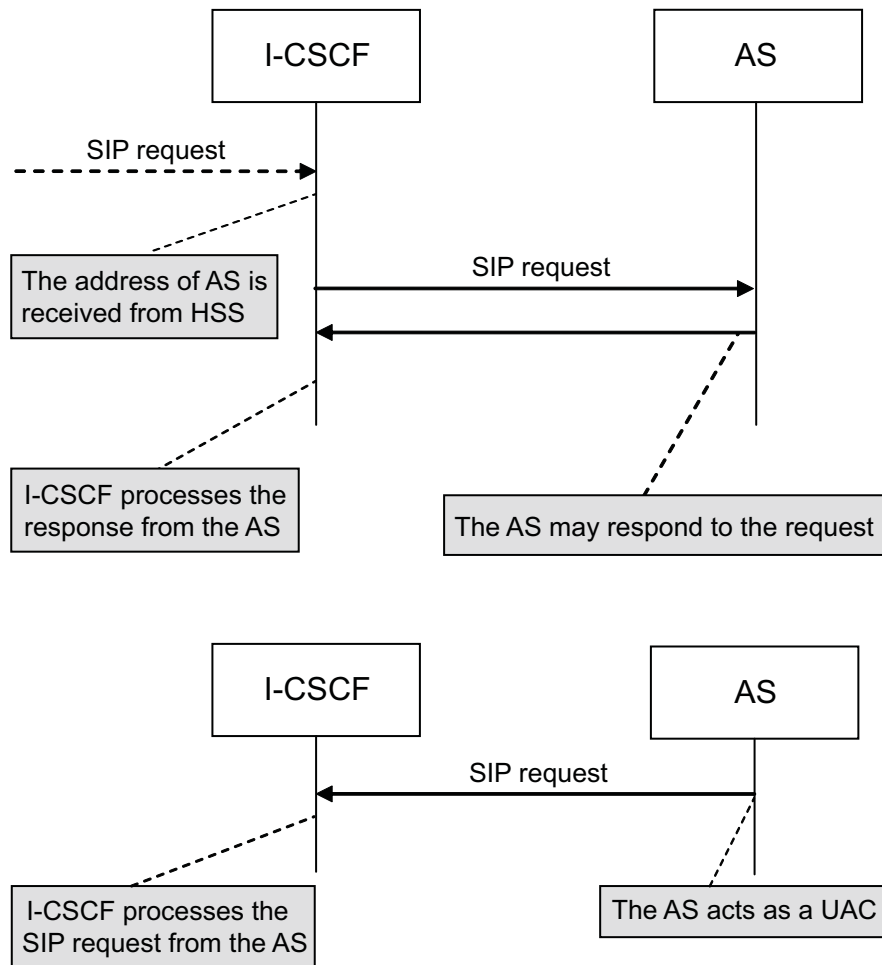


Figure 3 Overall Use Between I-CSCF and AS

After receiving the AS address from the Home Subscriber Server (HSS), the I-CSCF proxies the request to the AS. The AS acts as an UAS. The AS can initiate a SIP procedure acting as an UAC and send the request to the I-CSCF.

3.1 Lower-Level Procedures

3.1.1 Triggering AS

The AS triggering in the S-CSCF relies on the service trigger data downloaded from the Home Subscriber Server (HSS) in the profile of the user. The behavior of the S-CSCF for the evaluation of the trigger criteria for a request depends on if it is the initial evaluation for a request or a subsequent evaluation.



3.1.1.1 Initial AS Trigger Evaluation

For a given initial request, the highest priority trigger (Initial Filter Criteria) is evaluated first. If the criteria are met, the request is routed to the AS that is configured in the trigger. If the criteria are not met, the trigger with the next highest priority is evaluated. This process is repeated until there is either a match or there are no more triggers to evaluate.

3.1.1.2 Subsequent AS Trigger Evaluation

After triggering, an AS that matched a trigger criteria can route the request back to the S-CSCF either acting as a proxy or as a B2BUA. The S-CSCF continues to trigger evaluation with the next highest priority trigger when it receives the request with the Original Dialog Identifier (ODI).

The following apply:

- An AS acting as a proxy must include the ODI sent by the S-CSCF in the request (the ODI is included in the preloaded `Route` header added by the S-CSCF).
- An AS acting as a B2BUA can send one or several requests to the S-CSCF that includes the ODI, as long as each request has a new call leg, different Call-Id. The AS can choose to set up new call legs even after final responses have been received on previously created legs. For each new call leg, the S-CSCF continues the trigger evaluation with the next highest priority trigger when it receives the request. Triggering evaluation continues from the same trigger priority for every new call leg created by the AS.
- An AS acting as a B2BUA can also send the request back (with a new call leg) to the S-CSCF without the ODI. In this scenario, the S-CSCF treats the request as a request received from an AS acting as UAC, a Call Out Of the Blue (COOB) case, and perform initial trigger evaluation for the received request.

For Terminating, Terminating Unregistered, and After Retargeting Session Cases

If the AS changes the `Request-URI` of the request or adds additional `Route` headers to the request, subsequent terminating trigger evaluation is interrupted. If the user has originating services after retargeting (matching the `Originating_CDIV` session case), the S-CSCF continues to evaluate these triggers as previously described for initial and subsequent triggering. If the user has no originating services after retargeting triggers, then the request is routed based on the contents of the request.

3.1.2 Initial Requests from S-CSCF to AS

When the triggering criteria are met, the S-CSCF routes the request to the AS. This routing is done by using the address of the AS (AS SIP URI) received in the

trigger data. The AS SIP URI can include an optional `as-profile` parameter that indicates that additional services are required for the interworking with the AS. These features are described in Section 3.1.2.1 AS Profile Services on page 9.

An initial request from the S-CSCF to the AS is as follows:

- 1 The S-CSCF adds a `Route` header to the request with the interface of the S-CSCF the request must be proxied to in the form of a SIP URI. This URI can contain tokens in the user portion. This `Route` header can also be used to route requests to the S-CSCF when the AS is acting as a B2BUA.
- 2 If the AS SIP URI has the `lr` parameter defined in [RFC 3261 Session Initiation Protocol](#), the SIP URI is added as the top `Route` header in the request. If the AS SIP URI does not have the `lr` parameter, the S-CSCF rejects the request.
- 3 The S-CSCF also adds a `Record-Route` header containing an interface of the S-CSCF. This is to be used for subsequent requests within the dialog created by the following SIP methods:
 - INVITE
 - SUBSCRIBE (this is configurable)
- 4 S-CSCF adds a `P-Served-User` header, as defined in [RFC 5502 The SIP P-Served-User Private Header \(P-Header\)](#), to any non-register request before sending the request to an AS. S-CSCF populates the `P-Served-User` header by default with the Public ID of the current served user. If the received SIP request matched the registered user, the public ID of the request is used to populate the `P-Served-User` header. If the served user is a wildcard identity, the `P-Served-User` is populated with the non-wildcard identity received in the SIP request. The `P-Served-User` never contains a wildcarded IMPU (no wIMPU, neither wPSI). It is possible to modify the `P-Served-User` information using the AS Profile Services. When adding the `P-Served-User` header, the S-CSCF also adds the session case and the registration state of the user in the `P-Served-User` header according to the Backus-Naur Form (BNF), for example:

```
P-Served-User: <sip:user_a@cscf.com>;sescase=term;reg
state=unreg
```

If the address of the AS has not been cached previously, the address and transport used to route to the AS is determined by using the process defined in [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#) for locating where to send a SIP request based on the AS SIP URI. If the address of the AS has been cached, the SIP request is sent directly to this address. AS-instance caching is described in Section 3.1.2.1.1 AS-Instance Caching on page 9.

The parameter `phone-context` received over the Mw interface in SIP URI or tel URI is to be sent further to the AS. The Mobile Subscriber Integrated Services



Digital Network Number (MSISDN) is to be provisioned in the HSS. The HSS includes it as a parameter in the AS URI when sending the user profile to the S-CSCF. The URI can look like the following example:

`sip:applicationserver.ericsson.com;msisdn=+123456789`

3.1.2.1

AS Profile Services

Several S-CSCF services can be started when including the proprietary parameter `as-profile=<n>` in the AS-URI of the trigger (explicit or shared).

When multiple services are required, the format of the parameter is `as-profile=<m>:<n>`. The values of `m` and `n` can be in any order. Only colon is allowed as a separator between the values.

The values for the parameter are listed in Table 3:

Table 3 Values of as-profile Parameter

as-profile	Service
1	AS-instance caching
2	Mapping of P-Asserted-Identity to P-Served-User

3.1.2.1.1

AS-Instance Caching

The AS-instance caching service, also known as the Application Server Dynamic Allocation feature, enables that a specific AS instance that is selected based on the SIP routing, is stored and reused for subsequent triggering toward the same AS SIP URI during the whole registration lifetime of the user or when the cache is cleared.

When a new AS-instance is going to be cached, S-CSCF adds a URI parameter `initialselection` to the top Route header (AS-URI) before sending the SIP request to the AS: Route: `<...;initialselection>`.

The key to the cached instance is the default IMPU of the user and the hostname of the AS-URI, that is the FQDN excluding user info portion, `transport` parameter, `port` parameter, and all other URI parameters.

The S-CSCF stores the AS instance information that was selected for a specific user and AS SIP URI, for any received SIP response with the following exceptions:

- A 503 trying response, which also clears a cached instance.
- A 305 response to a third-party REGISTER request, which also clears a cached instance.
- A SIP transaction time-out clears a cached instance.

- A cached instance can be cleared by manually configuring parameter `scscfClearAsCache`.

The next time the AS SIP URI is used to trigger an AS for the user, the SIP request is sent directly to the stored AS instance.

The cached AS Instance information consists of the following data:

- The resolved IP address from DNS.
- The resolved port information from the DNS or the default SIP port (5060) if there is no port in AS SIP URI. If there is port in AS SIP URI, the port is not stored in cached AS Instance.

3.1.2.1.2 Mapping of P-Asserted-Identity to P-Served-User

Mapping of P-Asserted-Identity (PAI) to P-Served-User (PSU) service enables the possibility to change the `P-Served-User` information sent to an AS during trigger evaluation.

Mapping of PAI to PSU is applicable during trigger chaining, where the PAI received from the previous AS can be mapped into the PSU sent to the next AS if the service is enabled.

The top PAI header is used when mapping to PSU if multiple PAI headers are received in the SIP request from the previous AS.

3.1.3 SIP Routing Principles

The S-CSCF and the AS follow the provisions for SIP routing specified in the [RFC 3261 Session Initiation Protocol](#) and [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#) specifications with clarifications provided in this section.

The S-CSCF and the AS are behaving as SIP “loose” routers as defined in the [RFC 3261 Session Initiation Protocol](#) specification.

3.1.4 S-CSCF Discovery

This section describes the cases when the AS needs to determine the address of the S-CSCF to use for routing.



3.1.4.1 AS Acting as UAC or B2BUA

When the AS needs to send an initial request to the S-CSCF, it needs to determine the address of the S-CSCF to be used. This address can be obtained from the following:

- Configuration data in the AS or service logic when the AS is acting as a UAC.
- If the AS is acting as a B2BUA, and the AS wants to stop trigger evaluation, the address to the S-CSCF can be obtained from the host port in the `Route` header added by the S-CSCF. If trigger evaluation is to be continued, the AS uses the entire SIP URI from the second `Route` header.

3.1.4.2 AS Acting as UAS

The AS uses the address received in the top `Via` header in the request, to route the response to the S-CSCF.

3.1.4.3 AS Acting as Proxy

The AS uses the address located in the second `Route` header in the request, to proxy the request to the S-CSCF. This address or port, if any, can be different from the address or port the request was sent from by the S-CSCF. The first `Route` header is the address of the AS.

3.1.5 Multiple AS Support

When a request is proxied back from an AS, the S-CSCF evaluates the remaining trigger criteria. If criteria match, the request is proxied to the next AS. This continues until there is no more criteria match.

The responses follow the path established by the `Via` headers added during the processing of the request as specified in the [RFC 3261 Session Initiation Protocol](#) specification.

3.1.6 AS Failover Support

3.1.6.1 AS Failover Support over ISC Interface

The S-CSCF supports multiple nodes of AS deployed in a Network Redundant configuration, see Figure 4. The support is provided by using the mechanisms defined in the [RFC 3261 Session Initiation Protocol](#) and [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#) specifications.

The service triggering data for the user served by the S-CSCF must be populated, including the triggering criteria and the AS address in the form of a SIP URI. This AS hostname must be in the form of a domain name.

The Domain Name System (DNS) Service Record (SRV) entry for the domain name in the AS hostname is configured to resolve to multiple target AS nodes. These targets can have the same priority, in which case the requests from the S-CSCF are distributed across the various targets using the weight parameter. If these targets have different priority values, then the server with the lowest number priority is contacted first as described in the [RFC 2782 A DNS RR for specifying the location of services \(DNS SRV\)](#) specification.

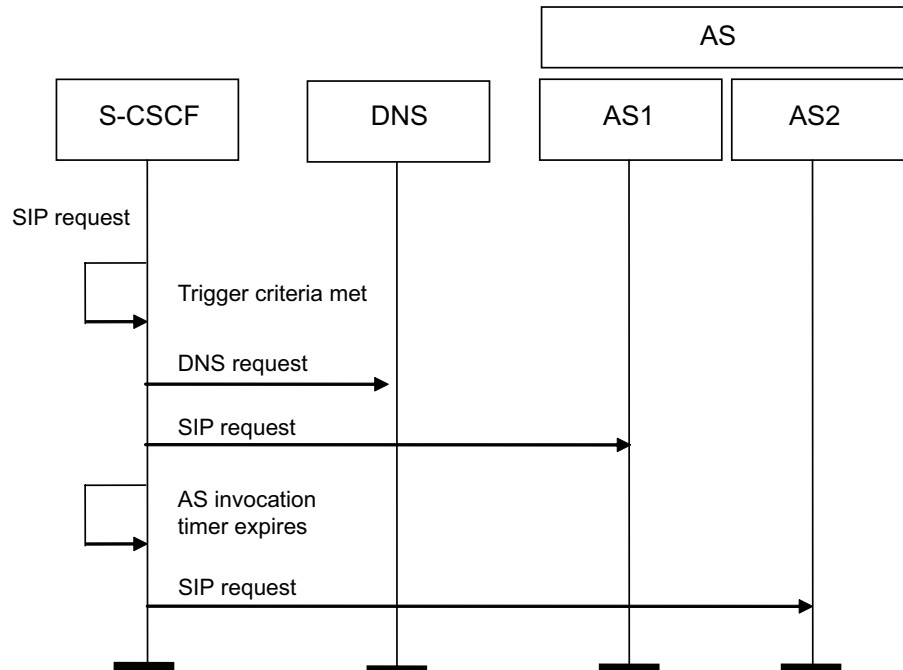


Figure 4 AS Failover on ISC Interface

The procedure for AS failover over ISC interface is as follows:

- 1 After determining that the SIP request received is an initial request, the service triggering criteria are checked. If the triggering criteria are met, the S-CSCF follows the procedure defined in Section 3.1.2 Initial Requests from S-CSCF to AS on page 7 to route the request to the AS domain.
- 2 The S-CSCF uses the procedures defined in [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#) to query DNS to determine to what IP address port and transport to use to send the request to the AS domain.
- 3 The S-CSCF uses the results of the DNS query to route the request to AS1. The S-CSCF sets the SIP layer timers for this transaction based on the configuration data.



- 4 If no provisional response is received before the timer expires, AS1 is considered to be unreachable for this request.
- 5 The S-CSCF uses the results of the previous DNS query to determine if there are any other targets for this request. If there is another target, the request is routed to that AS and the timer is reset. If there are no more targets to try, the S-CSCF generates an error response.

Note: A failed-over AS cannot have all information to continue its services, in which case it needs to poll the latest user registration data from S-CSCF, see Section 3.4.1.5 Signaling Parameters for SUBSCRIBE when AS Acts as UAC on page 42. The same case applies to restarted AS.

3.1.6.2

AS Failover Support over Ma Interface

The I-CSCF supports multiple nodes of AS deployed in a Network Redundant configuration, see Figure 5. The support is provided by using the mechanisms defined in [RFC 3261 Session Initiation Protocol](#) and [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#).

The AS address must be in the form of a SIP URI. This AS hostname must be in the form of a domain name.

The DNS SRV entry for the domain name in the AS hostname is configured to resolve to multiple target AS nodes. These targets can have the same priority, in which case the requests from the I-CSCF are distributed across the various targets using the weight parameter as described in [RFC 2782 A DNS RR for specifying the location of services \(DNS SRV\)](#). If these targets have different priority values, then the server with the lowest number priority is contacted first as described in [RFC 2782 A DNS RR for specifying the location of services \(DNS SRV\)](#).

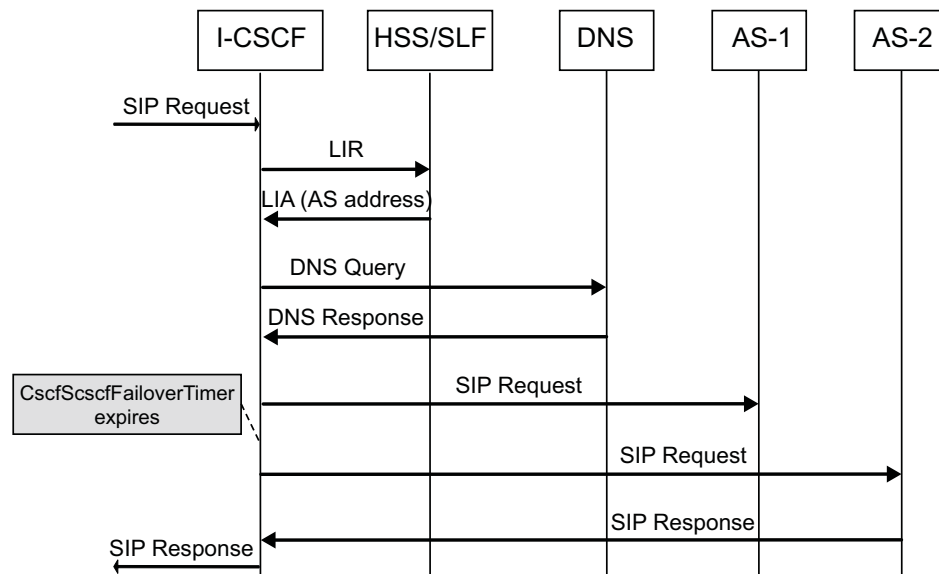


Figure 5 AS Failover on Ma Interface

The procedure for AS failover on Ma interface is as follows:

- 1 After determining the SIP request received is an initial request, a LIR is sent to HSS. An AS address is received from HSS in LIA.
- 2 The I-CSCF uses the procedures defined in [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#) to query DNS to determine what IP address port and transport to use to send the request to the AS domain.
- 3 The I-CSCF uses the results of the DNS query to route the request to AS1. The I-CSCF sets the SIP layer timers (*CscfScscfFailoverTimer*) for this transaction based on the configuration data.
- 4 If no provisional response is received before the timer expires, AS1 is considered to be unreachable for this request.

The I-CSCF uses the results of the previous DNS query to determine if there are any other targets for this request. If there is another target, the request is routed to that AS and the timer is reset. If there are no more targets to try, the I-CSCF generates an error response.

3.1.7

AS Session Case Determination

When requests are sent to the AS by the S-CSCF, the AS or the Value-Added Service running on the AS can need to know the session case, originating registered, originating unregistered, terminating registered, terminating unregistered, or originating services after retargeting, for the request. There are three mechanisms described in the following sections that the AS or service can use to make this determination. The selection of which mechanism is used is outside the scope of this document.



3.1.7.1 Separate Interfaces

The AS could have separate interfaces for receiving originating triggered request and terminating triggered request. Using different AS SIP URI in the trigger data for the different session cases would represent these separate interfaces. The AS SIP URI would be configured with either explicit ports or with different hostnames for each interface.

3.1.7.2 SIP URI Tokens

The AS or service can require a token to be configured in the user portion of the AS SIP URI when the trigger data is provisioned. This SIP URI is as the top most `Route` header in the request forwarded to it by the S-CSCF. If these tokens are unique for each session case, the AS or service can extract the token and use the token to determine the session case.

3.1.7.3 SIP URI Parameters

The AS or service can require a SIP URI parameter to be configured in the AS SIP URI when the trigger data is provisioned. This SIP URI is included as the top most `Route` header in the request forwarded to it by the S-CSCF. If the value of the parameter is unique for each session case, the AS or service can use the value of the parameter to determine the session case.

3.1.8 AS Authorization

When an initial request is received from the AS, the source IP address is compared with a list of authorized UAC AS addresses in the S-CSCF (`CscfTrustedASEntry`). If the address of the AS is not in the list, a `403` (User Agent not authorized) is returned to the AS. If the address of the AS is in the list, then processing continues.

If the received top `Route` header from the AS does not contain an `orig` parameter, there is no check against the list of trusted ASs (`CscfTrustedASEntry`) as the S-CSCF cannot determine if the request was sent from the AS or the originating network.

3.1.9 Security Considerations

There is only minimal security protection for the ISC specified in this document. The S-CSCF and the AS rely on the IP network security to provide a Security Association that allows the S-CSCF and the AS to trust messages sent on the ISC interface, see Section 6 on page 49. The S-CSCF and the AS can use additional Security Associations to other network elements or the User Equipment (UE).

The mechanisms used by the IP network and any additional mechanisms implemented by the S-CSCF or the AS to other network elements are outside the scope of this document.

3.2 Invocation of AS at Registration

3.2.1 Registration Procedure

The triggering on the REGISTER request is handled in a different way compared to other `non-INVITE` requests, refer to the [3GPP TS 23.218 IP Multimedia \(IM\) session handling](#) specification.

If the REGISTER request from the user matches a trigger, the S-CSCF performs a third-party registration to the ASs that are interested in being informed about the user registration event of this Public User Identity, or related Public User Identities in a group of implicitly registered Public User Identities, as shown in Figure 6.

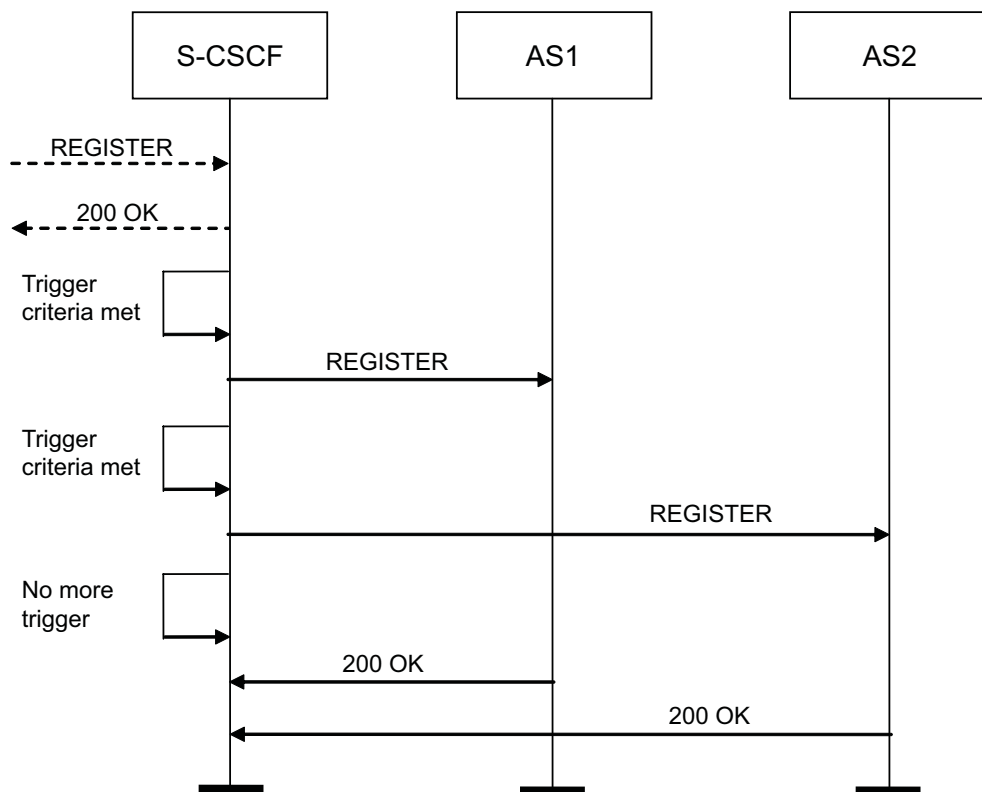


Figure 6 Third-Party Registration

The third-party registration procedure is as follows:



- 1 When a REGISTER request is received, the S-CSCF performs normal REGISTER handling. If the registration is successful, the S-CSCF responds with a 200 OK.
- 2 If the registration is successful, the service triggering criteria are checked.
- 3 If the service triggering criteria are satisfied, the S-CSCF follows the procedure defined in Section 3.1.2 Initial Requests from S-CSCF to AS on page 7 to create and send third-party REGISTER requests to the AS.
- 4 The AS sends a final response.

3.2.1.1

Third-Party Registration Procedure with Redirection

When the application server receives third-party registration requests, it can choose to send back a 305 response to trigger the S-CSCF to redirect the REGISTER request to a new target. The default handling applicable to the IFC that triggered the third-party register request is applied to any redirected request. The redirect sequence is shown in Figure 7.

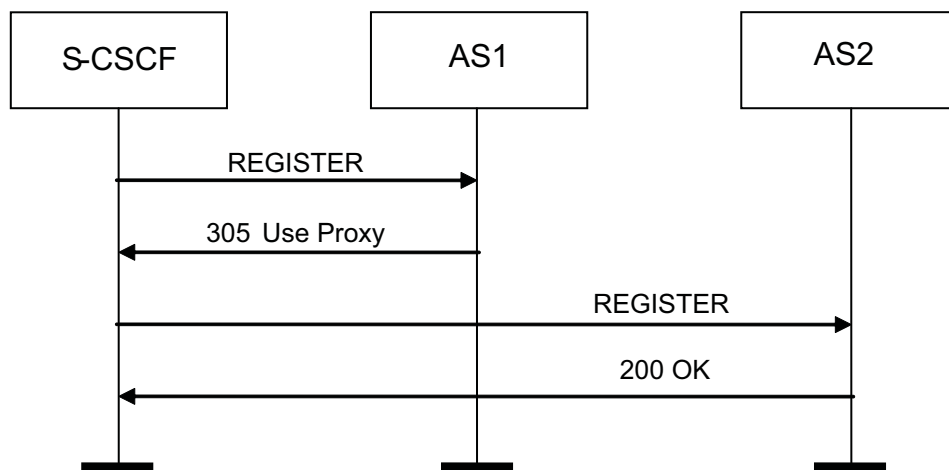


Figure 7 Third-Party Registration Redirection

The third-party registration procedure with redirection is as follows:

- 1 A REGISTER request is sent to AS1 according to steps 1–3 in Section 3.2.1 Registration Procedure on page 16.
- 2 AS1 sends a 305 redirection response.

- 3 The S-CSCF populates the request that was previously sent to AS1 with the new target in the 305 response. The request is updated with a new top route header and a new `Request-URI`. Also, if the contact header in the 305 response contains SIP URI Header Components, these components can replace the corresponding headers sent in the original REGISTER message or can be inserted or appended in the outgoing REGISTER request towards the new target, refer to *CSCF Mw Interface*.
- 4 The request is sent to AS2.
- 5 The AS sends a successful final response.

3.2.2 Implicit Registration

A SIP REGISTER request referring, through its `To` header, to a Public User Identity that belongs to a group of Public User Identities is called an *Implicit Registration*. All group members are registered within the CSCF.

The triggering evaluation is performed for each service profile within the implicit register set.

3.2.3 Special Kinds of Deregistrations

A user initiated deregistration is a SIP REGISTER request with `expires` value 0. User initiated registrations follow the standard pattern described in Section 3.2.1 Registration Procedure on page 16. There also exist network initiated deregistrations and time-out triggered deregistrations. In both these cases, there is no incoming SIP REGISTER message to use for building the SIP REGISTER request to route to the AS. Instead the requests are built using user and contact information stored in the S-CSCF database.

3.2.4 Signaling Parameters for Registration

The following sections contain the key contents of the REGISTER request, see Section 3.2.4.1 Signaling Parameters for REGISTER Request on page 19, the message body of the request, see Section 3.2.4.2 Message Body of REGISTER Request on page 23, and responses to the request, see Section 3.2.4.3 Response to REGISTER Request on page 26, related to the ISC interface. The syntax of the messages and contents not listed in the table are governed by the [RFC 3261 Session Initiation Protocol](#) specification.

To simplify the reading of this section, the following terms are used:

- Message Embedding

The Message Embedding function is when the Third-Party Registration request in its body contains headers from the REGISTER message received



from UE or headers from 200 OK response sent back to UE, or both. If this function is not active, the message body is empty. Or, if Network Initiated deregistration, when the Third-Party Registration request in its body contains headers from the REGISTER message previously received from UE, see Section 3.2.3 Special Kinds of Deregistrations on page 18.

This function is active when the matched trigger in the users profile contains IncludeRegisterRequest or IncludeRegisterResponse, or both.

- **Contact Transparency**

The Contact Transparency function is when the Contact header used in the Third-Party Registration request contains the original contact received from the UE.

This function is active only when Message Embedding is not active and CscfUseUserContactIn3rdPartyReg is set to **userContact**.

3.2.4.1

Signaling Parameters for REGISTER Request

The headers of REGISTER request sent to the AS from the S-CSCF are listed in Table 4.

Table 4 Headers of REGISTER Request Sent to AS from S-CSCF

Header	Procedure-Specific Values of the Parameter
Request-URI	Contains the SIP URI of the AS. Example: REGISTER sip:134.138.123.123:9997;lr SIP/2.0
To	Contains either the Public User Identity as contained in the REGISTER request received from the UE, or a related implicitly registered Public User Identity. Example: To: sip:user_b0@cscf.com
From	Contains the SIP URI of the S-CSCF plus a tag generated by the S-CSCF. Example: From: sip:scscf.cscf.com:7070;tag=8dfd2426f3fcd5e7aa8dfec37b9cfcd
Call-ID	Generated by the S-CSCF. Example: Call-ID: 792ae-288b9-2cd60@134.138.123.123
CSeq	Generated by the S-CSCF. Example: CSeq: 1 REGISTER
Max-Forwards	Always Max-Forwards: 70



Header	Procedure-Specific Values of the Parameter
Content-Length	If there is no message body in the request, the Content-Length is set to 0. Otherwise, the header contains the total number of bytes of the message body.
Content-Type	<p>If no message body included, the Content-Type header is not present.</p> <p>If the REGISTER contains message body, the Content-Type is set as following:</p> <ul style="list-style-type: none">• If the message body consists of either a SIP REGISTER request or a 200 OK response for the REGISTER request, it is like: Content-Type: message/sip• If the message body consists of a SIP REGISTER request and a 200 OK response for the REGISTER request, it is like: Content-Type: multipart/mixed; boundary=" <boundary value >" <p>The parameter <boundary value> is generated by the S-CSCF (can be random or a constant value).</p>
Route	<p>Contains the SIP URI of the AS.</p> <p>Example: Route: <sip:134.138.123.123:9997;lr></p>



Header	Procedure-Specific Values of the Parameter
Contact	<p>Is always present. There is exactly one instance of this header. So called REGISTER QUERY requests, which lack Contacts, are never forwarded to the AS.</p> <p>There are two main cases, A and B, distinguished by the setting of an S-CSCF configuration parameter and trigger data.</p> <p>A – If Contact Transparency is active, then there are two main subcases to consider, as follows:</p> <ul style="list-style-type: none"> • A1 – If a REGISTER request that is forwarded to an AS does not represent a deregistration, then the Contact: header is an exact copy of the selected Contact, based on q-value, in the REGISTER request received from the UE, with the exception that the expires=xxx parameter is removed. Example: Contact header received from the UE: Contact: <sip:user_b0@134.138.123.123:5058>;q=0.9;expires=360; Contact header forwarded to AS: Contact: <sip:user_b0@134.138.123.123:5058>;q=0.9 • A2 – If a REGISTER request that is forwarded to an AS does represent a deregistration, then there are two subcases, as follows: <ul style="list-style-type: none"> A21 – If the deregistration to the AS is caused by an explicit de-REGISTER message with CONTACT: * from the UE, or the cause is a time-out for the last Contact of a user, or the cause is a network initiated deregistration, then a CONTACT: * header is used to the AS. Example: Contact: * A22 – In all other cases than those listed in A21 the Contact header is an exact copy of the selected Contact: (based on q-value) in the REGISTER request received earlier from the UE (when the Contact was initially registered or later updated), with the exception that the expires=xxx parameter is removed. Example: Contact: <sip:user_b0@134.138.123.123:5058>;q=0.9 <p>B – If Contact Transparency is not active, then the Contact header forwarded to AS only contains that S-CSCF-address. Example: Contact: sip:scscf.cscf.com:7070</p> <p>The parameter expires=xxx is never used. Instead the CSCF uses the Expires header, as in the following example:</p>

Header	Procedure-Specific Values of the Parameter
Expires	<p>Always present. There is exactly one instance of this header.</p> <p>A – For REGISTER requests, forwarded to the AS, that does not represent any deregistration there are the following two subcases to consider:</p> <ul style="list-style-type: none"> • A1 – If the Contact Transparency is active, then the value of this Expires header is derived from the selected, based on q-value, Contact header expires parameter in the REGISTER request received from the UE, or, in absence of such a parameter, from the Expires header of the REGISTER request. • A2 – If the Contact Transparency is not active, then the maximum expire value is calculated over the remaining Contacts, a Contact can have been replaced because of maximum number of allowed contacts, and used as value in the Expires header. Notice that if the S-CSCF deducts that this entire REGISTER request would mean “no change” to what is reported earlier, then it suppresses the sending of the request to the AS. <p>B – For REGISTER requests, forwarded to the AS, that does represent some deregistration there are the following two subcases to consider:</p> <ul style="list-style-type: none"> • B1 – If Contact Transparency is active, then its value is explicitly set to 0, regardless of the cause of the deregistration. • B2 – If Contact Transparency is not active, then there are the following two conditions to consider: <ul style="list-style-type: none"> B21 – If the deregistration implies that the last Contact is removed, then its value is explicitly set to 0, regardless of the cause of the deregistration. B22 – If the deregistration implies that the last Contact is not removed, then the maximum expire value is calculated over the remaining Contacts and used as value in the Expires header. Notice that if the S-CSCF deducts that this entire REGISTER request would mean “no change” to what is reported earlier, then it suppresses the sending of the request to the AS. <p>Example A1: Expires: 360</p> <p>Example B1: Expires: 0</p> <p>Example B22: Expires: 111</p>



Header	Procedure-Specific Values of the Parameter
P-Charging-Vector	<p>Contains the ICID the S-CSCF received in the original REGISTER request.</p> <p>Example: P-Charging-Vector: icid-value=3f9ee890016509e20f8e083</p> <p>The AS can send additional Charging information in the generic param parameter. The S-CSCF forwards the generic param parameter to the next node.</p>
P-Charging-Function-Addresses	<p>Contains the values received from the HSS if the message is forwarded within the S-CSCF home network.</p> <p>Example: P-Charging-Function-Addresses: ccf="aaa://ericsson.se"; ecf="aaa://ericsson.se";</p>
Resource-Priority	<p>If a Resource-Priority is received from incoming request, this header is included by the S-CSCF.</p> <p>Contains:</p> <ul style="list-style-type: none"> ets namespace – The Emergency Telecommunications Service (ETS) namespace is used to indicate that a call is eligible for priority treatment. wps namespace – The Wireless Priority Service (WPS) namespace is used to indicate the priority level of the user.

3.2.4.2 Message Body of REGISTER Request

When Message Embedding is active, the S-CSCF inserts the message body in the third-party REGISTER.

3.2.4.2.1 Message Body with Single Part of REGISTER Request

If Message Embedding includes only indication of register request, the S-CSCF includes a SIP REGISTER request in the message body of the third-party REGISTER request.

If UE initiated registration, the request included in the message body is the REGISTER request which was initiated by the UE and received by the S-CSCF.

If network initiated deregistration, a request containing headers used for REGISTER request is created using user and contact information stored in the S-CSCF database. The included headers and values are shown in Table 5.

Table 5 Headers of REGISTER Request in Message Body if Network Initiated Deregistration

Header	Procedure-Specific Values of the Parameter
Request-URI	Contains the home domain of the served user. Example: REGISTER sip:cscf.com SIP/2.0
To	Contains a public ID associated with the served user. No tag is added. Example: To: sip:user_a@cscf.com
From	Contains a public ID which is associated same as the public ID in To header. Tag is a CSCF generated unique string. Example: From: sip:user_a@cscf.com;tag=8df5e7aa8dfec37b9cfcdb
Call-ID	Contains an S-CSCF generated unique string. Example: Call-ID: 792ae-288b9-2cd60@134.138.123.123
CSeq	Generated by the S-CSCF. Example: CSeq: 1 REGISTER
Max-Forwards	Always Max-Forwards: 70
Contact	Depending on the use case, the Contact header contains different values. A. Complete or partial removal of user state. Contains a "*" Example: Contact: * B. Removal of a single contact. Contains the contact that was deregistered. Example: Contact: <sip:user_a@10.10.10.10:5060>;expires=0



Header	Procedure-Specific Values of the Parameter
Expires	<p>Depending on the use case, the Expires header contains different values.</p> <p>A. Complete or partial removal of user state. Contains a “0” Example: Expires: 0</p> <p>B. Removal of a single contact Expires header is not present in this case.</p>
Via	<p>Contains the address of S-CSCF that generates the message.</p> <p>CSCF generates branch parameter with unique string.</p> <p>Example:</p> <p>Via: SIP/2.0/TCP scscf.cscf99.lab;branch=z9hG4bK42ab8870b8fcc71aa38ada4bef04ad7dg</p>

3.2.4.2.2

Message Body with Single Part of 200 OK Response

If Message Embedding includes only indication of register response, the S-CSCF includes a SIP 200 (OK) response in the message body of the third-party REGISTER request.

If UE initiated registration, the response included in the message body is the 200 OK response sent by the S-CSCF for the successful REGISTER request.

If network initiated deregistration, a response containing headers used for REGISTER response is created using user and contact info stored in the S-CSCF database. The included headers and values are shown in Table 6.

Table 6 Headers of REGISTER Response in Message Body if Network Initiated Deregistration

Header	Procedure-Specific Values of the Parameter
Response-Code	<p>Contains the successful response.</p> <p>Example: SIP/2.0 200 OK</p>
To	<p>Contains the To header value described in Table 5 with an extra tag parameter.</p> <p>Example: To: sip:user_a@cscf.com; tag=8df5e7aa8dfec37b9cfcdB</p>
From	<p>Contains the From header value described in Table 5.</p> <p>Example: From: sip:user_a@cscf.com;tag=2df5e7aa8dfxc37b9cfcdf</p>

Header	Procedure-Specific Values of the Parameter
Call-ID	Contains the Call-ID header value from the generated request described in Table 5. Example: Call-ID: 792ae-288b9-2cd60@134.138.123.123
CSeq	Generated by the S-CSCF. Example: CSeq: 1 REGISTER
Contact	Contains the contacts that remain or were deregistered. Example: Contact: <sip:user_a@10.10.10.10:5060>;expires=0 Contact: <sip:user_a@10.50.2.28:5060>;expires=60
Via	Contains the Via header value from the generated request described in Table 5. Example: Via: SIP/2.0/TCP scscf.cscf99.lab;branch=z9hG4bK42ab8870b8fcc71aa38ada4bef04ad7dg

3.2.4.2.3

Message Body with Multipart of REGISTER Request and Response

If Message Embedding includes both indications of include register request and include register response, the S-CSCF creates the message body which contains a REGISTER request, as described in Section 3.2.4.2.1 Message Body with Single Part of REGISTER Request on page 23, and a 200 (OK) response (as described in Section 3.2.4.2.2 Message Body with Single Part of 200 OK Response on page 25) for the third-party REGISTER request.

3.2.4.3

Response to REGISTER Request

3.2.4.3.1

General

There are no important headers to list for third-party registration responses. The CSCF handles non-2xx responses according to Section 3.2.4.3.2 Handling of 305 Responses from a Cached or Non-Cached AS-Instance on page 27 to Section 3.2.4.3.4 Handling of Non-2xx Responses from a Cached AS-Instance on page 27.

A negative final response or no response does not affect the third-party service trigger evaluation.



3.2.4.3.2 Handling of 305 Responses from a Cached or Non-Cached AS-Instance

In case a 305 response is received, the S-CSCF fetches the new target from the 305 response and adds the new target to the `Request-URI` and `Route` header. Also, if the contact header in the 305 response contains SIP URI header components, these components can replace the corresponding headers sent in the original REGISTER message, or can be inserted or appended in the outgoing REGISTER request towards the new target, refer to *CSCF Mw Interface*.

3.2.4.3.3 Handling of Non-2xx Responses from a Non-Cached AS-Instance

If the SIP request is sent to a non-cached AS, based on the received responses, one of the following conditions applies:

- If a 5xx response, or a 408 (Request Timeout) response, or no response is received, the S-CSCF applies default handling to the failed request.
- If extended default handling is enabled and any 5xx or 4xx response is received, the S-CSCF applies default handling to the failed request.

3.2.4.3.4 Handling of Non-2xx Responses from a Cached AS-Instance

If the S-CSCF uses a cached AS-instance, as described in Section 3.1.2.1.1 AS-Instance Caching on page 9 to send a request to an application server, based on the received responses one of the following conditions applies:

- If the request cannot be sent because of transport errors, or a transaction time-out, or the application server responds with 503, the S-CSCF removes the cached AS-instance for the user, and then tries to resend the request using the process defined in [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#).
- If a 5xx response, except 503, or a 408 (Request Timeout) response is received, the S-CSCF applies default handling to the failed request.
- If extended default handling is enabled and any 5xx, except 503, or 4xx response is received, the S-CSCF applies default handling to the failed request.

3.3 Invocation of AS, Non-REGISTER

3.3.1 Initial SIP Request Procedure, Non-REGISTER

3.3.1.1 Invocation of AS for Initial SIP Request from S-CSCF to AS

This section defines the procedures for an initial SIP request from the S-CSCF to AS, see Figure 8.

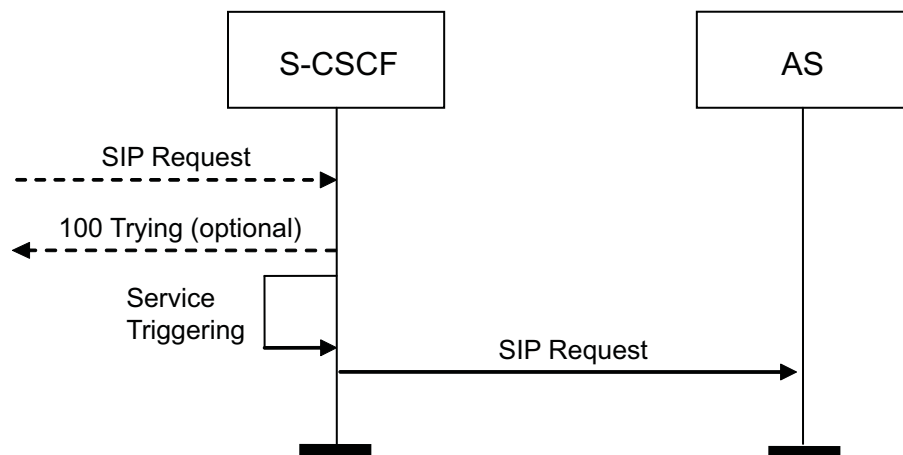


Figure 8 Invocation of AS – Non-REGISTER

The invocation of the AS for an initial SIP request is described in the following procedure:

- 1 After determining the SIP request received as an initial request, 100 Trying is sent if INVITE, the service triggering criteria are checked.
- 2 If the triggering criteria are met, the S-CSCF follows the procedure defined in Section 3.1.2 Initial Requests from S-CSCF to AS on page 7 to route the request to the AS. If the triggering criteria are not met, then the normal S-CSCF processing continues as specified in the *CSCF Gm Interface* and *CSCF Mw Interface* documents.

3.3.1.2 Signaling Parameters for Initial SIP Request from S-CSCF to AS

The syntax of the messages and contents not listed in Table 7 are governed by [RFC 3261 Session Initiation Protocol](#) or other relevant SIP extensions.

Table 7 SIP Request from S-CSCF to AS

Header	Procedure-Specific Values of the Parameter
Route	The SIP URI configured in the trigger data for this service invocation.



Header	Procedure-Specific Values of the Parameter
Route	The address of the S-CSCF interface for the AS to use when acting as a SIP proxy or a B2BUA, that is, the original dialogue identifier. This address can be different from the source IP address of the request or the address contained in the <i>Via</i> header.
P-Charging-Vector	This header is received from the original SIP request, else it is created by the S-CSCF. Additional Charging information can be received from the original SIP request in the generic <i>param</i> parameter. If so, the S-CSCF forwards the generic <i>param</i> parameter to the AS.
P-Charging-Function-Addresses	This header is created and added by the S-CSCF.
P-Served-User	This header is created and added by the S-CSCF.
P-Profile-Key	If a <i>P-Profile-Key</i> is received from incoming request, this header is included by the S-CSCF.
Resource-Priority	This header can be created or modified by the S-CSCF.

Note: The S-CSCF does not add or remove any additional headers or modify the body of the SIP request before routing the SIP Request to the AS.

3.3.2 Redirection Procedure of SIP Request, Non-REGISTER

3.3.2.1 Application Server Replies with 305

An application server can redirect a received request. This section defines the procedures for how a 305 redirect response is handled, see Figure 9. Other redirect responses are proxied upstream by the S-CSCF.

The default handling applicable to the IFC that triggered third-party register request is applied to any redirected request.

Triggering continues after redirection in case the AS receiving the redirected request chooses to act as Proxy or a B2BUA and sends the request back to the S-CSCF.

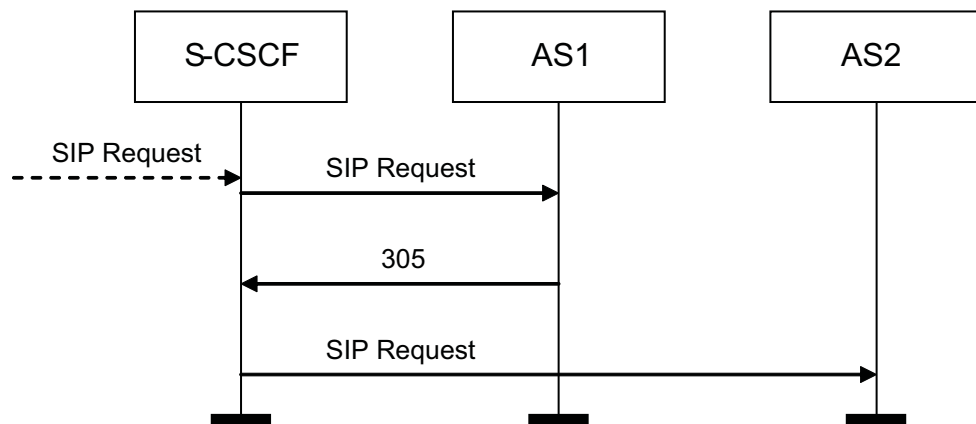


Figure 9 Redirection of SIP Request – Non-REGISTER

How a 305 redirect response is handled is described in the following procedure:

- 1 If the triggering criteria are met, the S-CSCF follows the procedure defined in Section 3.1.2 Initial Requests from S-CSCF to AS on page 7 to route the request to the AS.
- 2 The application server can reply with a redirection response. If this redirection response is a 305 response, the S-CSCF sends the request to the new target found in the *Contact* header in the 305 response. Also, if the *Contact* header in the 305 response contains SIP URI Header Components, these components can replace the corresponding headers sent in the original REGISTER message or can be inserted or appended in the outgoing REGISTER request towards the new target, refer to *CSCF Mw Interface*.

3.3.2.2

Signaling Parameters for Initial SIP Request from S-CSCF to AS

The following table contains the key contents of the SIP request when redirecting the request. The syntax of the messages and contents not listed in the table are governed by the [RFC 3261 Session Initiation Protocol](#) specification or other relevant SIP extensions.

The headers listed in Table 8 overrule Table 7 in Section 3.3.1.2 Signaling Parameters for Initial SIP Request from S-CSCF to AS on page 28. Otherwise the headers defined in Table 7 are applicable.

Table 8 SIP Request from S-CSCF to AS after Redirection

Header	Procedure-Specific Values of the Parameter
Route	The target in the <i>Contact</i> header in the 305 response.
Route	The address of the S-CSCF interface for the AS to use when acting as a SIP proxy or a B2BUA, that is, the original dialogue identifier. This address can be different from the source IP address of the request or the address contained in the <i>Via</i> header.

3.3.3 AS Acting as UAS

3.3.3.1 Initial SIP Request Procedure

This section defines the procedures when the AS is acting as a SIP UAS for an initial SIP request by sending a 2xx–6xx response, see Figure 10. The behavior and responsibilities of a SIP UAS are defined in the [RFC 3261 Session Initiation Protocol](#) specification.

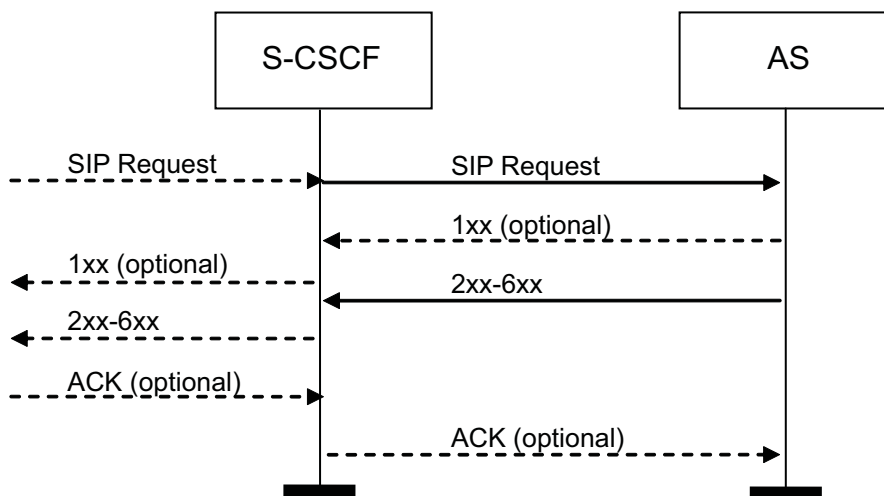


Figure 10 AS Acting as UAS for Initial SIP Request

Note: A 305 response can trigger redirection of the request according to Section 3.3.2 Redirection Procedure of SIP Request, Non-REGISTER on page 29.

The procedure in Section 3.3.1 Initial SIP Request Procedure, Non-REGISTER on page 28 must have been performed before the following procedure:

- 1 The AS can send zero or more provisional responses. The construction and uses of provisional responses as governed by [RFC 3261 Session Initiation Protocol](#). The S-CSCF proxies the provisional responses based on the `Via` headers except 100 Trying, as described by in [RFC 3261 Session Initiation Protocol](#).
- 2 The AS sends one final response. The construction and uses of final responses as governed by [RFC 3261 Session Initiation Protocol](#). The S-CSCF proxies the final response based on the `Via` headers, unless default handling applies.

The S-CSCF stops evaluating triggering criteria for the request when the final response is received from the AS, unless default handling applies. When default handling applies, service triggering continues.

- 3 In case the SIP request is an `INVITE`, the S-CSCF forwards the received `ACK` to the AS using the established route set for this dialogue.

3.3.3.2 Signaling Parameters for SIP Request Responses from AS Acting as UAS

The syntax of the messages and contents are governed by the [RFC 3261 Session Initiation Protocol](#) specification or other relevant SIP extensions.

3.3.4 AS Acting As Proxy

3.3.4.1 Initial SIP Request Procedure

This section defines the procedures when the AS is acting as a SIP proxy for an initial SIP request by proxying the SIP request to the S-CSCF, see Figure 11.

The behavior and responsibilities of a SIP proxy are defined in the [RFC 3261 Session Initiation Protocol](#) specification.

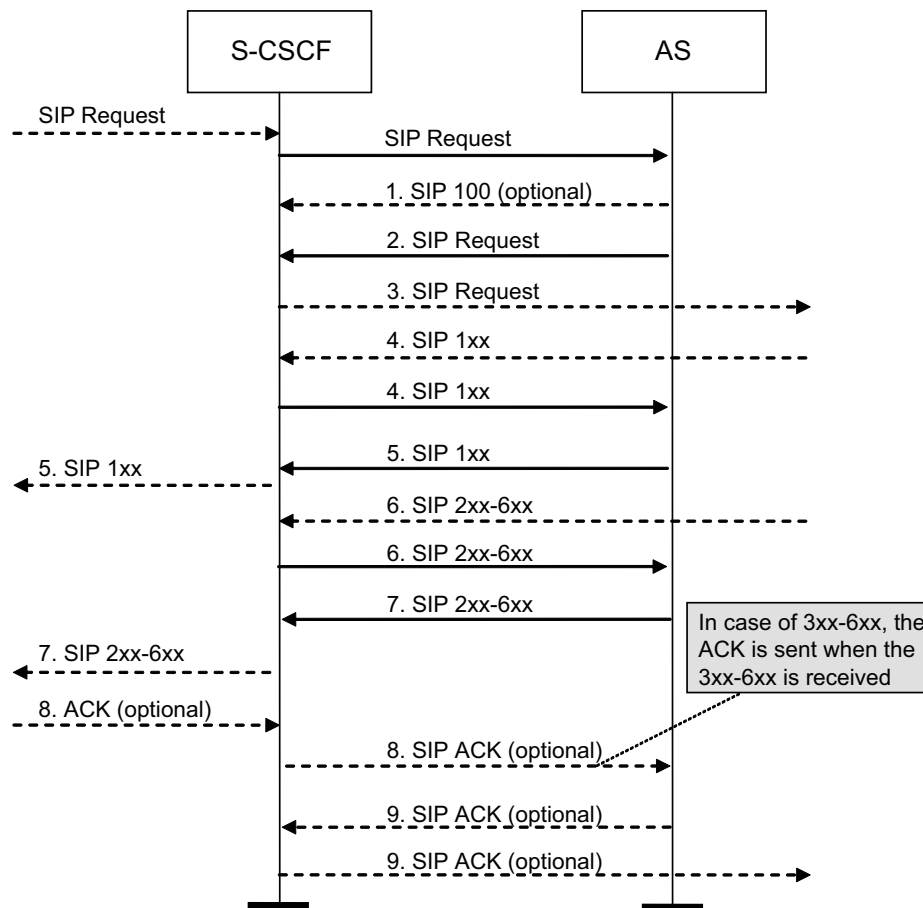


Figure 11 AS Acting as Proxy for Initial INVITE Request

Note: A 305 response can trigger redirection of the request according to Section 3.3.2 Redirection Procedure of SIP Request, Non-REGISTER on page 29.



The procedure in Section 3.3.1 Initial SIP Request Procedure, Non-REGISTER on page 28 must have been performed before the following procedure:

- 1 If INVITE, the AS sends a 100 (Trying) response to the S-CSCF using the Via header the S-CSCF put in the INVITE request.
- 2 Based on service logic the AS proxies the request back to the S-CSCF using the Route header added by the S-CSCF in the message as governed by [RFC 3261 Session Initiation Protocol](#).
- 3 The S-CSCF evaluates the remaining trigger criteria. If subsequent trigger criteria match, the request is proxied to the next AS, repeating previous steps. If no subsequent trigger criteria match, the S-CSCF executes the request processing as defined in Section 3.1.3 SIP Routing Principles on page 10.
- 4 Any provisional responses received by the S-CSCF in response to this request are sent to the AS using the Via headers in the response.
- 5 Any provisional responses sent by the AS to the S-CSCF are sent using the Via headers in the response.
- 6 Any final responses received by the S-CSCF in response to this request are sent to the AS using the Via headers in the response.
- 7 Any final responses sent by the AS to the S-CSCF are sent using the Via headers in the response. All final responses that the AS receives for the request must be proxied back to the S-CSCF.
- 8 If SIP INVITE: When the ACK is received, the S-CSCF routes the ACK request to the AS only if the AS inserted a Record-Route header in the initial INVITE request.
- 9 If SIP INVITE: The AS proxies the ACK request back to the S-CSCF using the route set in the request.

3.3.4.2

Signaling Parameters for SIP Requests from AS Acting as Proxy

Key contents of the SIP request from an AS acting as a proxy are listed in Table 9.

Depending on the functionality executed in the AS functionality, the Request-URI can include additional routing parameters as per the [RFC 4694 Number Portability Parameters for the “tel” URI](#) and [DAI Parameter for the “tel” URI](#) specifications.

Table 9 SIP Request from AS Acting as Proxy

Header	Procedure-Specific Values of the Parameter
Request-URI	If the AS has inserted additional routing parameters as per RFC 4694 Number Portability Parameters for the “tel” URI or DAI Draft, the S-CSCF uses the information for routing or Charging purposes.

Header	Procedure-Specific Values of the Parameter
Route	The address of the S-CSCF interface for the AS to use when acting as a SIP proxy. This address can be different from the source IP address of the request or the address contained in the <code>Via</code> header.
P-Charging-Vector	The S-CSCF ignores the ICID and O-IOI received. For additional subsequent AS invocations, the S-CSCF uses the stored <code>P-Charging-Vector</code> from the forwarded request to the AS. The AS can send additional Charging information in the generic <code>param</code> parameter. The S-CSCF forwards the generic <code>param</code> parameter to the next node.
P-Charging-Function-Addresses	The S-CSCF ignores the <code>P-Charging-Function-Addresses</code> header received. For additional subsequent AS invocations, the S-CSCF uses the stored <code>P-Charging-Function-Addresses</code> header from the forwarded request to the AS.
Resource-Priority	The S-CSCF prioritizes the SIP request according to <code>Resource-Priority</code> values. The S-CSCF forwards the <code>Resource-Priority</code> header to the next node.

3.3.5 AS Acting as B2BUA

When the AS is acting as a SIP B2BUA, the procedures defined in Section 3.3.3 AS Acting as UAS on page 31 for the UAS transaction and in Section 3.4 AS Acting as SIP UAC on page 37 for the UAC transaction are followed. The AS must include the `Route` header with the address of the S-CSCF interface in the request.

3.3.6 Subsequent Requests from S-CSCF to AS

3.3.6.1 Routing of Subsequent Requests

The trigger data is only checked during the processing of the initial request. The S-CSCF routes all subsequent requests based on the route set established by the initial request as defined in the [RFC 3261 Session Initiation Protocol](#) specification.

3.3.6.2 Signaling Parameters for Subsequent Requests

Key contents of the subsequent requests are listed in Table 10 and Table 11.



Table 10 Subsequent Request to AS from S-CSCF

Header	Procedure-Specific Values of the Parameter
Route	The address the AS put in the Record-Route header of the request that established this SIP dialog.
	The address the S-CSCF put in the Record-Route header of the request that established this SIP dialog.

Table 11 Subsequent Request to S-CSCF from AS

Header	Procedure-Specific Values of the Parameter
Route	The address the S-CSCF put in the Record-Route header of the request that established this SIP dialog.

3.3.7 Response to Non-REGISTER Request

3.3.7.1 General

There are no important headers to list non-REGISTER responses. The CSCF handles non-2xx responses according to Section 3.3.7.2 Handling of Non-2xx Responses from a Non-Cached AS-Instance on page 35 to Section 3.3.7.3 Handling of Non-2xx Responses from a Cached AS-Instance on page 35.

3.3.7.2 Handling of Non-2xx Responses from a Non-Cached AS-Instance

If the SIP request is sent to a non-cached AS, based on the received responses, one of the following conditions applies:

- If the S-CSCF fails to receive a SIP response, or receives a 408 (Request Timeout) response, or a 5xx response is received, the S-CSCF applies default handling to the failed request.
- If extended default handling is enabled and the S-CSCF fails to receive a SIP response, or receives a 4xx response or a 5xx response, the S-CSCF applies default handling to the failed request.

3.3.7.3 Handling of Non-2xx Responses from a Cached AS-Instance

If the S-CSCF uses a cached AS-instance, as described in Section 3.1.2.1.1 AS-Instance Caching on page 9, to send a request to an application server, based on the received responses one of the following conditions applies:

- If the SIP request cannot be sent because of transport errors, or a transaction time-out or the application server responds with 503, the S-CSCF removes the cached AS-instance for the user, and then tries to resend the request using the process defined in [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#).

- If a 5xx response, except 503, or a 408 (Request Timeout) response is received, the S-CSCF applies default handling to the failed request.
- If extended default handling is enabled and any 5xx, except 503, or 4xx response is received, the S-CSCF applies default handling to the failed request.

3.3.8 Invocation of AS from I-CSCF, Non-REGISTER

This section describes the invocation of the AS Non-REGISTER from the I-CSCF over the Ma interface.

3.3.8.1 Invocation of AS from I-CSCF

The invocation of the AS from the I-CSCF for a non-REGISTER initial request is shown in Figure 12.

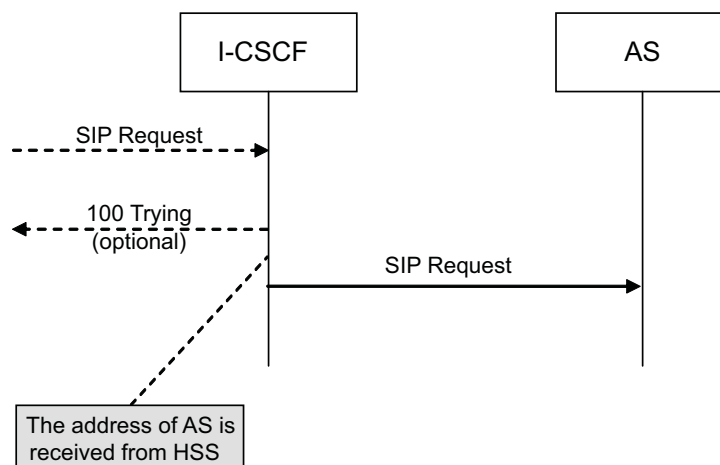


Figure 12 Invocation of the AS (Non-REGISTER) from I-CSCF

The procedure is as follows:

- 1 After determining the SIP request received is an initial request, the 100 (Trying) can be sent in the case of INVITE.
- 2 After the address of AS is received from the HSS, the request is sent to the AS directly through the Ma interface.

3.3.8.2 Signaling Parameters for SIP Request from I-CSCF to AS

This section describes the key contents of the SIP request. The syntax of the message and the contents not listed in Table 12 are governed by [RFC 3261 Session Initiation Protocol](#) or other relevant SIP extensions.

Table 12 SIP Request from I-CSCF to AS

Header	Procedure-Specific Values of the Parameter
Route	The address of the AS received from the HSS.

3.4 AS Acting as SIP UAC

3.4.1 Initial SIP Request Procedure

3.4.1.1 AS Acting as UAC with Initial SIP Request Sent to S-CSCF

This section defines the procedure when the AS is acting as a SIP UAC sending an initial SIP request to S-CSCF, see Figure 13. The behavior and responsibilities of a SIP UAC are defined in the [RFC 3261 Session Initiation Protocol](#) specification.

At reception of the initial request, the S-CSCF authorizes the AS as described in Section 3.1.8 AS Authorization on page 15.

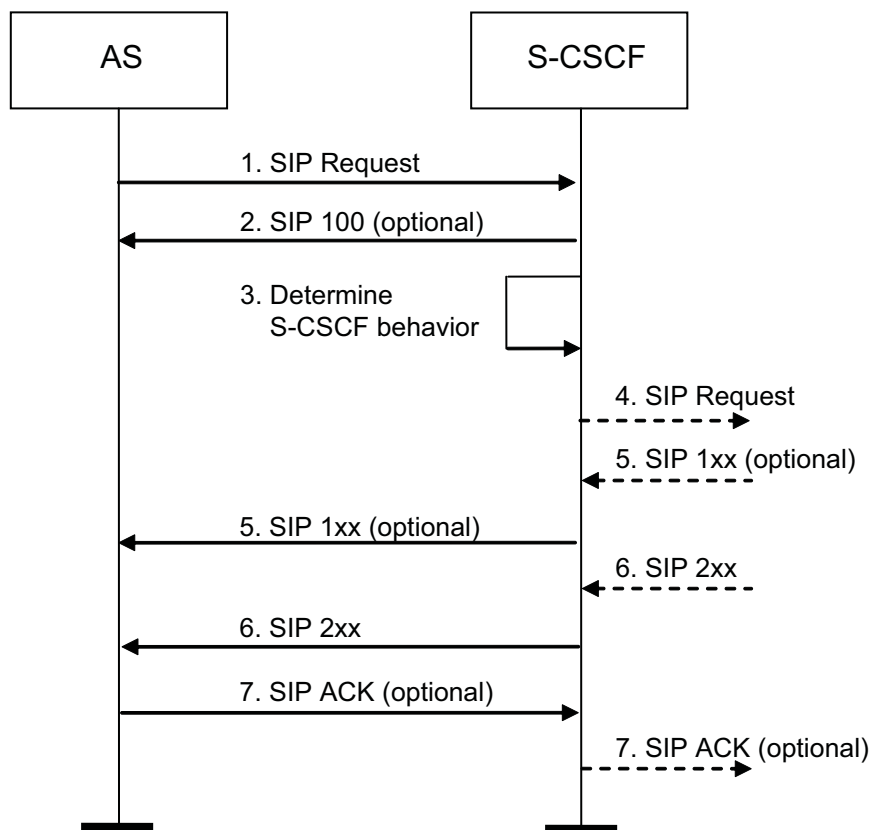


Figure 13 AS Acting as UAC with Initial SIP Request Sent to S-CSCF

The AS acting as a UAC with initial SIP request sent to S-CSCF is described in the following procedure:

- 1 The AS builds a SIP request and sends the message to the S-CSCF. The address of the S-CSCF is determined by the procedure in Section 3.1.4.1 AS Acting as UAC or B2BUA on page 11.

Depending on the functionality executed in the AS functionality, the Request-URI can include additional routing parameters as per the [RFC 4694 Number Portability Parameters for the “tel” URI](#) and [DAI Parameter for the “tel” URI](#) specifications.

- 2 If SIP INVITE, the S-CSCF sends a 100 (Trying) response to the AS using the Via header the AS put in the INVITE request.
- 3 The S-CSCF behavior is determined by the following factors:

If the received top Route from the AS contains an orig parameter, the Calling user identity is fetched from the P-Served-User header in the SIP message. If no P-Served-User header is present in the message, then the P-Served-User-Identity is used. If the P-Served-User-Identity header is not present, the P-Asserted-Identity header is used. If neither of the headers is present, then the From header is used.

- If the calling user is registered in the S-CSCF, then originating behavior and service trigger evaluation are performed.
- In case the user is not registered, the S-CSCF downloads the user profile from the HSS and stores it in the database in unregistered state. In case the download fails, the S-CSCF rejects the request with a negative response unless the HSS returns DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED and the Server-Assignment-Answer (SAA) contains a server name where the S-CSCF instead returns a 305 with a Contact header representing the server name received in the SAA. Originating behavior and service trigger evaluation are performed. Any P-Served-User or P-Served-User-Identity header is removed before the message is forwarded to the terminating network.

If the received top Route from the AS does not contain an orig parameter. The called user identity is fetched from the Request-URI.

- If the called user is registered in the S-CSCF, terminating behavior and service trigger evaluation are performed.
- If the called user is not registered in the S-CSCF, and the IP address in the top Via header is configured in the CscfTrustedASEntry, originating behavior is performed, but no user trigger evaluation is performed.
- If none of the two previous conditions apply, terminating behavior is performed.



- 4 If trigger matching is to be performed, the S-CSCF executes the procedure in Section 3.3.1 Initial SIP Request Procedure, Non-REGISTER on page 28, otherwise the request is routed according to Section 3.1.3 SIP Routing Principles on page 10.
- 5 Any provisional responses received by the S-CSCF in response to this request are sent to the AS using the `Via` headers in the response.
- 6 Any final responses received by the S-CSCF in response to this request are sent to the AS using the `Via` headers in the response. If this response establishes a SIP dialog, the route set must be stored by the AS and used for subsequent requests as defined in the [RFC 3261 Session Initiation Protocol](#) specification.
- 7 If SIP `INVITE`, the AS sends an `ACK` for the final responses received as defined in [RFC 3261 Session Initiation Protocol](#).

3.4.1.2

Signaling Parameters for INVITE Sent to S-CSCF When AS Acts as UAC

Key contents of the SIP request sent to S-CSCF from the AS acting as a UAC are listed in Table 13.

Table 13 SIP Request Sent to S-CSCF from AS Acting as UAC

Header	Procedure-Specific Values of the Parameter
Request-URI	If the AS has inserted additional routing parameters as per RFC 4694 Number Portability Parameters for the “tel” URI or DAI Draft, the S-CSCF uses the information for routing or Charging purposes.
P-Charging-Vector	If a P-Charging-Vector header is received in the S-CSCF, the S-CSCF uses this header. If no P-Charging-Vector header is received, the S-CSCF adds a P-Charging-Vector header. The AS can send additional Charging information in the generic <code>param</code> parameter. The S-CSCF forwards the generic <code>param</code> parameter to the next node.
P-Charging-Function-Addresses	This header is ignored.
From	This header contains the AS SIP URI.
P-Served-User	This header can be created and added by the AS.
P-Asserted-Identity	This header can be created and added by the AS.

Header	Procedure-Specific Values of the Parameter
P-Profile-Key	This header can be created and added by the AS.
Resource-Priority	If a Resource-Priority header is received in the S-CSCF, the S-CSCF prioritizes the SIP request according to Resource-Priority values. This header can be created or modified by the S-CSCF.

3.4.1.3

AS Acting as UAC with Initial SIP Request Sent to I-CSCF

This section defines the procedures when the AS is acting as a SIP UAC sending an initial SIP request to the Interrogating CSCF (I-CSCF) over the Ma interface, see Figure 14. The behavior and responsibilities of a SIP UAC are defined in the [RFC 3261 Session Initiation Protocol](#) specification.

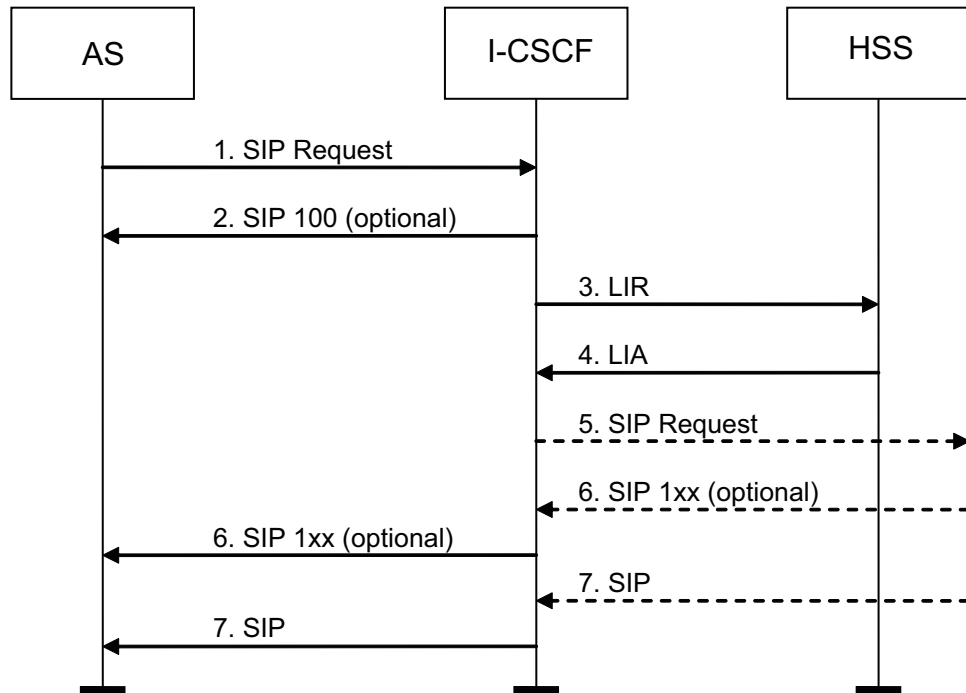


Figure 14 AS Acting as UAC with Initial SIP Request Sent to I-CSCF

The AS acting as a UAC with initial SIP request sent to I-CSCF is described in the following procedure:

- 1 The AS builds a SIP request and sends the message to the I-CSCF.
- 2 If SIP INVITE, the I-CSCF sends a 100 (Trying) response to the AS using the Via header the AS put in the INVITE request.



- 3 A LIR is sent to the HSS, containing the public Id selected according to the following substeps, requesting the location of the home S-CSCF of the user.

The I-CSCF selects a public Id for the LIR according to the following steps:

- If the received top Route from the AS contains an orig parameter, originating logic is applied. The Calling user identity is fetched from the P-Served-User header in the SIP message. If no P-Served-User header is present in the message, then the P-Asserted-Identity header is used. If neither of the headers is present, then the From header is used. The LIR is populated with the Originating-Request AVP to indicate to the HSS that this is an originating use case.
 - If the received top Route from the AS does not contain an orig parameter terminating logic is applied, the Called user identity is fetched from the Request-URI header in the SIP message.
- 4 A LIA is returned from the HSS. The I-CSCF behavior is determined by the following factors:
 - If the HSS returns one or more server names, the I-CSCF proxies the request towards the received destinations.
 - If the HSS returns capabilities, the I-CSCF uses the Resource Broker list to find S-CSCF nodes that matches the received capabilities.
 - 5 The request is proxied to the server selected in the previous step.
 - 6 Any provisional responses received by the I-CSCF in response to this request are sent to the AS using the Via headers in the response.
 - 7 Any final responses received by the I-CSCF in response to this request are sent to the AS using the Via headers in the response.

3.4.1.4

Signaling Parameters for INVITE Sent to I-CSCF When AS Acts as UAC

Key contents of the SIP request sent to the I-CSCF from the AS acting as a UAC are listed in Table 14.

Table 14 SIP Request Sent to I-CSCF from AS Acting as UAC

Header	Procedure-Specific Values of the Parameter
Request-URI	Used by the I-CSCF as served user for terminating request.
Route	A Route header can be present and can contain an orig parameter indicating that originating logic is to be applied.
P-Charging-Vector	This header is passed on by the I-CSCF as received; except if no ICID is received, the I-CSCF adds the ICID parameter.

Header	Procedure-Specific Values of the Parameter
P-Charging-Function-Addresses	This header is ignored.
From	This header contains the AS SIP URI.
P-Served-User	This header is used by the I-CSCF as served user for originating request.
P-Served-User-Identity	This header is used by the I-CSCF as served user for originating request.
P-Asserted-Identity	This header is used by the I-CSCF as served user for originating request.
P-Profile-Key	This header received is removed by the I-CSCF.
Resource-Priority	If a Resource-Priority header is received in the I-CSCF, the I-CSCF prioritizes the SIP request according to Resource-Priority values. The I-CSCF forwards the Resource-Priority header to the next node.

3.4.1.5 Signaling Parameters for SUBSCRIBE when AS Acts as UAC

An overview of subscription procedure is shown in the Figure 15.

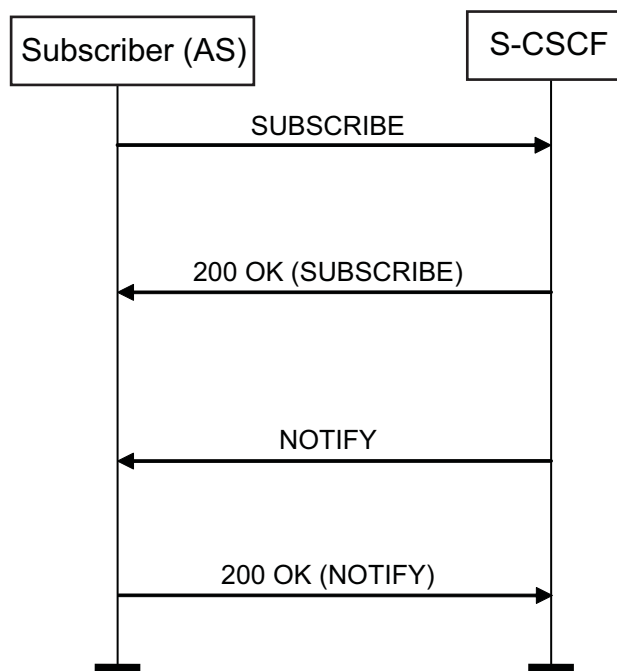


Figure 15 Initiating SUBSCRIBE Dialog

The case of Polling resource state by the AS during SUBSCRIBE Dialog initialization is shown in Figure 16.

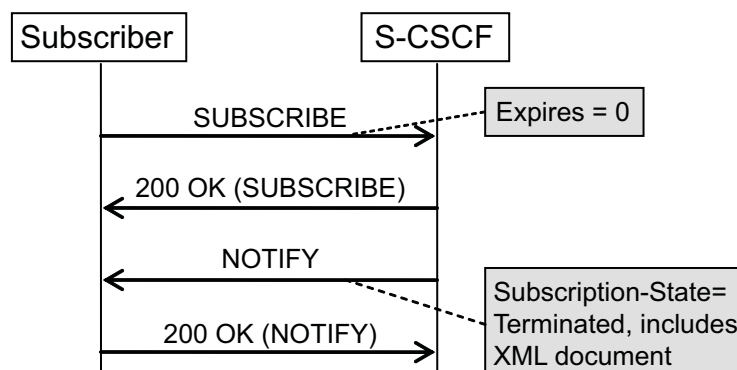


Figure 16 Polling at SUBSCRIBE Initialization

3.4.1.5.1 Subscription Request

When a SIP SUBSCRIBE is received from AS in the S-CSCF, the important information expected is listed in Table 15.

Table 15 *SIP Request from AS Acting as UAC to S-CSCF*

Header	Procedure-Specific Values of the Parameter
To	Resource for which subscription applies, for which notifications are requested.
Contact	AS SIP URI.
Expires	Optional header. Subscription expiry time, see Section 4.2.2 Expires on page 46.
Accept	Optional header, see Section 4.2.1 Accept on page 45.

Information presented in the table applies to Initial Subscription Request, Subscription Refresh Request, and Subscription Termination Request.

3.4.1.6 Signaling Parameters for NOTIFY when AS Acts as UAC

Besides NOTIFY Request header parameters, the message can carry Registration Event XML[®] file in the message body, `application/reginfo+xml`, when requested in SUBSCRIBE request message through event type for Reg-Event, Event field of value `reg`, refer to *CSCF Mw Interface*.

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 proprietary elements is configurable.

3.4.2 Subsequent Requests from AS to S-CSCF

The trigger data is only checked during the processing of the initial request. The S-CSCF routes all subsequent requests based on the route set established by the initial request as defined in the [RFC 3261 Session Initiation Protocol](#) specification.

Any provisional and final responses received by the S-CSCF in response to this request are sent to the AS using the `Via` headers in the response.



4 Information Model

4.1 Supported SIP Methods

The following SIP methods, see Table 16, are listed in TS 24.229 as supported methods, and are considered within this document. Other SIP methods are handled according to RFC 3261. Refer to the [3GPP TS 24.229 IP Multimedia call control protocol based on SIP and SDP](#) and [RFC 3261 Session Initiation Protocol](#) specifications.

Table 16 Supported SIP Methods

SIP Method	CSCF -> AS	AS -> CSCF	Reference
ACK request	Supported	Supported	RFC 3261
BYE request	Supported	Supported	RFC 3261
CANCEL request	Supported	Supported	RFC 3261
INVITE request	Supported	Supported	RFC 3261
MESSAGE request	Supported	Supported	RFC 3428
NOTIFY request	Supported	Supported	RFC 3265
OPTIONS request	Supported	Supported	RFC 3261
PRACK request	Supported	Supported	RFC 3262
PUBLISH request	Supported	Supported	RFC 3903
REFER request	Supported	Supported	RFC 3515
REGISTER request	Supported	Not applicable	RFC 3261
SUBSCRIBE request	Supported	Supported	RFC 3265
UPDATE request	Supported	Supported	RFC 3311

4.2 SIP Header Information

4.2.1 Accept

If no Accept header is present in SUBSCRIBE request sent by AS, a default value `application/reginfo+xml` is used.

Both Subscriber and Notifier must be able to support this format.

4.2.2 Expires

If no `Expires` header is present in `SUBSCRIBE` request, the implied default is defined by the event package being used, for example, the S-CSCF uses default of Reg-Event package when the AS subscribes to Reg-Event event type.

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

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

4.2.3 Route

The S-CSCF adds two `Route` headers in the request sent to the AS. The top `Route` header contains the SIP URI of the AS as defined in trigger data. The second `Route` header contains the S-CSCF address and is used when the AS acts as a proxy or a B2BUA. When acting as a UAC, the AS can include the `orig` parameter to control the further processing of the request as described in Section 3.4.1.1 AS Acting as UAC with Initial SIP Request Sent to S-CSCF on page 37.

4.2.4 P-Profile-Key

If a `P-Profile-Key` is received by the S-CSCF, it is sent to an AS over the ISC interface. If a `P-Profile-Key` is received by the I-CSCF, it is removed. Refer to the [RFC5002 The SIP P-Profile-Key Private Header \(P-Header\)](#) specification.

Note: The I-CSCF can also send `P-Profile-Key` to an AS over the Ma interface.



5 Formal Syntax

Not applicable.





6 Security Considerations

6.1 IPsec Tunnel

The communication between the S-CSCF and an AS can be secured using IP Security (IPsec), Zb interface, on the IP transport layer, refer to the [3GPP TS 33.210 3G security; Network Domain Security \(NDS\); IP network layer](#) specification.

IPsec tunnels can be defined between the two nodes. Internet Key Exchange version 1 (IKEv1) performs mutual authentication between the two nodes and establishes an IKE Security Association that includes shared secret information used to establish IPsec Security Associations (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

This section states the related standards and explains any deviations from them.

The related standards are mainly the [3GPP TS 24.229 IP Multimedia call control protocol based on SIP and SDP](#) and [RFC 3261 Session Initiation Protocol](#) specifications.

The following standards are also applicable:

- [RFC 2782 A DNS RR for specifying the location of services \(DNS SRV\)](#)
- [RFC 3263 Session Initiation Protocol \(SIP\): Locating SIP Servers](#)
- [RFC 3265 Session Initiation Protocol \(SIP\) – Specific Event Notification](#)
- [RFC 3680 A Session Initiation Protocol Event Package for Registrations](#)
- [RFC 4694 Number Portability Parameters for the “tel” URI](#)
- [RFC 5002 The SIP P-Profile-Key Private Header \(P-Header\)](#)
- [RFC 5502 The SIP P-Served-User Private Header \(P-Header\)](#)
- [DAI Parameter for the “tel” URI](#)
- [3GPP TS 23.218 IP Multimedia \(IM\) session handling; IM call model; Stage 2](#)
- [3GPP TS 33.210 3G security; Network Domain Security \(NDS\); IP network layer security](#)

The following are the main deviations from the standards:

- SIPS URI is not supported.
- TLS is not supported.