MultiService
Forum

Implementation Agreement for ISC interface

MSF-IA-SIP.013-FINAL

MultiService Forum
Implementation Agreement

Contribution Number: msf2006.004.04

Document Filename: MSF-IA-SIP.013-FINAL

Working Group: Protocol and Control

Title: Implementation Agreement for ISC Interface

Editors: Stuart Walker
Leapstone Systems Inc
swalker@leapstone.com
IM Leapstone_stuart@msn.com

Working Group Chairperson: Chris Gallon, Fujitsu

Date: 1 November 2006

Abstract: The MultiService Forum (MSF) is responsible for developing Implementation Agreements, Product Specifications or Architectural Frameworks, which can be used by developers and network operators to ensure interoperability between components from different vendors. MSF Implementation Agreements, Product Specifications and Architectural Frameworks are formally ratified via a Straw Ballot and then a Principal Member Ballot. Draft MSF Implementation Agreements, Product Specifications and Architectural Frameworks may be published before formal ratification via Straw or Principal Member Ballot. In order for this to take place, the MSF Technical Committee must formally agree that a draft Implementation Agreement, Product Specifications or Architectural Framework should be progressed through the balloting process. A Draft MSF Implementation Agreement, Product Specification or Architectural Framework is given a document number in the same manner as an Implementation Agreement. Draft Implementation Agreements, Product Specifications or Architectural Frameworks may be revised before or during the full balloting process. The revised document is allocated a new major or minor number and is published. The original Draft Implementation Agreement, Product Specifications or Architectural Framework remains published until the Technical Committee votes to withdraw it. After being ratified by a Principal Member Ballot, the Draft Implementation Agreement, Product Specifications or Architectural Framework becomes final. Earlier Draft Implementation Agreements, Product Specifications or Architectural Frameworks remain published until the Technical Committee votes to withdraw them.

The use of capitalization of the key words “MUST”, “SHALL”, “REQUIRED”, “MUST NOT”, “SHOULD NOT”, “SHOULD”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY” or “OPTIONAL” is as described in section V-B of the MSF Technical Committee Operating Procedures.

The goal of the MSF is to promote multi-vendor interoperability as part of a drive to accelerate the deployment of next generation networks. To this end the MSF looks to adopt pragmatic solutions in order to maximize the chances for early deployment in real world networks.

To date the MSF has defined a number of detailed Implementation Agreements and detailed Test Plans for the signaling protocols between network components and is developing additional Implementation Agreements and Test Plans addressing some of the other technical issues such as QoS and Security to assist vendors and operators in deploying interoperable solutions.

The MSF welcomes feedback and comment and would encourage interested parties to get involved in this work program. Information about the MSF and membership options can be found on the MSF website http://www.msforum.org/

DISCLAIMER

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and the MultiService Forum is not responsible for any errors or omissions. The MultiService Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither the MultiService Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind whether based on theories of tort, contract, strict liability or otherwise, shall be assumed or incurred by the MultiService Forum, its member companies, or the publisher as a result of reliance or use by any party upon any information contained in this publication. All liability for any implied or express warranty of merchantability or fitness for a particular purpose is hereby disclaimed.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

> Any express or implied license or right to or under any MultiService Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor
>
> > Any warranty or representation that any MultiService Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor
> >
> > Any commitment by a MultiService Forum company to purchase or otherwise procure any product(s) and/or service(s) that embody any or all of the ideas, technologies, or concepts contained herein; nor
> >
> > Any form of relationship between any MultiService Forum member companies and the recipient or user of this document.

Implementation or use of specific MultiService Forum Implementation Agreements, Architectural Frameworks or recommendations and MultiService Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in the MultiService Forum.

For addition information contact:

MultiService Forum
39355 California Street, Suite 307
Fremont, CA 94538
USA
Phone: +1 510 608-5922
Fax: +1 510 608-5917
info@msforum.org
http://www.msforum.org

Contents

Figures

1 ISC interface

The Third Generation Partnership Project (3GPP) selected SIP as the protocol to use on the IMS Service Control (ISC) interface. The MSF have adopted the ISC interface for the Service Control interface of the Release 3 architecture. This Implementation Agreement provides details of the ISC interface, as used in the MSF R3 architecture.

2 Applicability and Scope

The scope of the interface described in this IA is shown in the figure below.

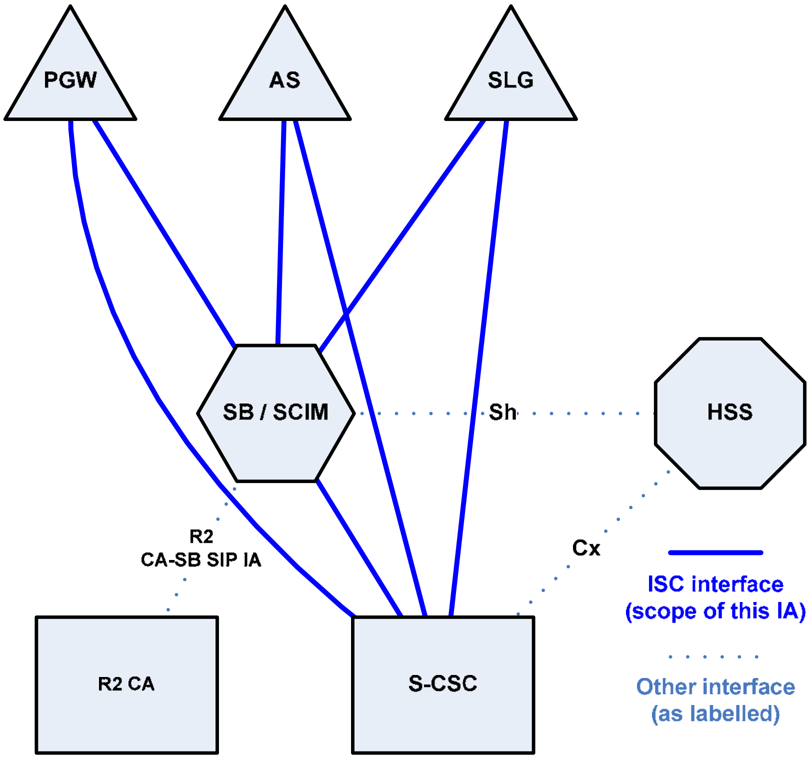


Figure 1 - ISC interface in the MSF R3 architecture

Service Control in the MSF R3 architecture can either be applied between the Serving Call Session Controller (S-CSC) and the application platforms (Parlay / Parlay X Gateway, Application Server, Service Logic Gateway) directly or through the SB/SCIM (Service Broker / Service Capability Interaction Manager).

2.1 Application Invocation without SB/SCIM

Applications can be invoked from the S-CSC directly without engaging the services of the SB/SCIM through the ISC interface described in this IA. The invocation of applications by the S-CSC is based upon the subscriber's service profile which the S-CSC retrieves from the HSS when the subscriber registers (or upon receipt of a SIP INVITE for application invocation for unregistered subscribers). The service profile includes service triggering information presented in the form of a set of prioritized Initial Filter Criteria (iFC). Each iFC contains details of the target application that is to be invoked if the set of triggering conditions (Service Point Triggers) are met; the service is identified as a SIP URL. Service Point Triggers consist of a set of conditional expressions which are either ORed together (Disjunctive Normal Form) or ANDed together (Conjunctive Normal Form). The conditional expressions can include the following elements.

- **Request-URI** – the value of the Request-URI in the SIP message.
- **SIP Method** – this indicates the type of request such as INVITE or NOTIFY.
- **SIP Header** – the conditional expression can be based on the presence or absence of a SIP header or the value of the header contents.
- **Session Case** – Has three possible value Originating, Terminating and Terminating Unregistered
- **Session Description** – the conditional expression can be based any SDP field within the body of the SIP method.

A full description of the subscriber service profile used by the S-CSC can be found in 3GPP TS 29.228.

When the S-CSC receives a SIP message to/from a subscriber it will evaluate iFC in the service profile and, if a match is found forward the SIP message to the application identified in the service profile. The figure below shows a typical application invocation from a SIP INVITE, where the application acts as either a proxy or B2BUA and propagates the SIP INVITE back to the S-CSC.

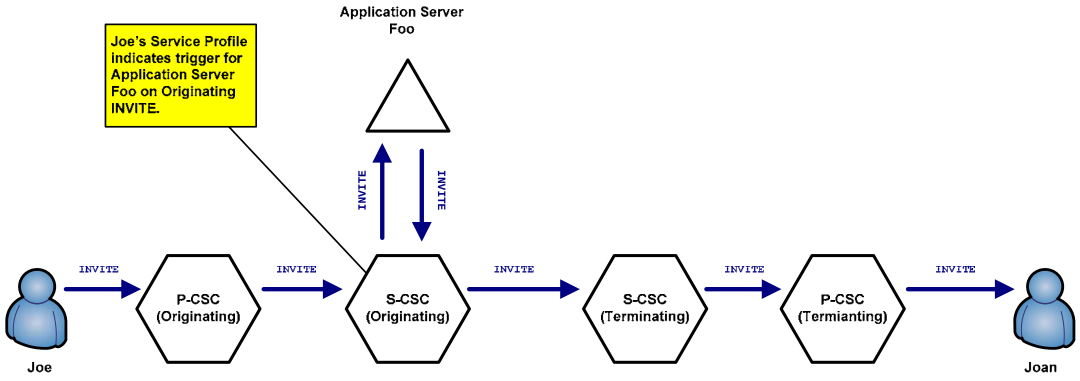


Figure 2 - Invocation of Application from S-CSC directly.

2.2 Application Invocation with SB/SCIM

Applications can also be invoked through the SB/SCIM using the ISC interface described in this IA. In this mode the SB/SCIM itself acts as an Application Server towards the S-CSC, orchestrating the actions of other Applications onto the session. The SB/SCIM also retrieves the subscriber service profile from the HSS, this profile is termed subscriber SCIM service profile (or sometimes just SCIM service profile) in this document and is described in Appendix A.

The circumstances in which it is necessary and appropriate to engage applications via the SB/SCIM rather than directly are:-

a) When the extended filter criteria (described in appendix A) are used to trigger applications. The 3GPP defined iFC are 'static' in that the decision to forward the SIP message to the application is based upon the contents of the message itself. The extended filter criteria permit the use of further context information (for example the subscribers current location) to be used in the filter conditions. Extended filter criteria provides an extensible model to cover a wide variety of context information types. Appendix A in this IA defines two types of context, Basic Call State and Calendar.

b) Where service interactions between applications needs to be resolved, in particular when the interaction involves applications that do not share a common trigger condition (since common trigger interactions may be resolvable in the service profile itself).

c) Where the S-CSC only supports a subset of the iFCs required in order to handle the subscribers service profile, in this case the SB/SCIM is included in the initial session signaling and handles the full set of iFC triggers for the subscriber.

d) The SB/SCIM also supports the (R2) Call Agent to Service Broker SIP IA and can provide access to the IMS service layer from the end-points supported by the R2 Call Agent.

The figure below shows two applications Foo and Bar being invoked for the terminating party via the SB/SCIM. Both of the application servers (acting as either proxies or B2BUA's) propagate the SIP INVITE back to the SB/SCIM.

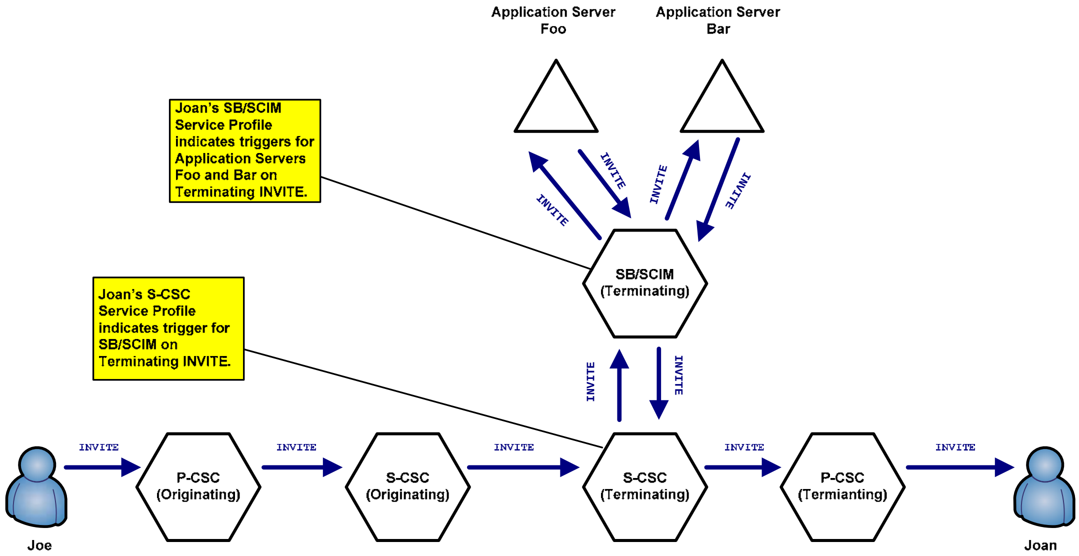


Figure 3 - Invocation of Applications via SB/SCIM

2.3 Application Chaining

One of the key functions of the ISC interface described in this IA is the ability to engage multiple independent applications onto the session. The technique for achieving this is called application chaining and it essentially involves sending the SIP signaling through each 'chained' application in sequence. Although chaining can be achieved both from the S-CSC and the SB/SCIM the 3GPP definitions for the S-CSC function only permit a single application to be invoked from the S-CSC at a time, as shown in Figure 4 below.

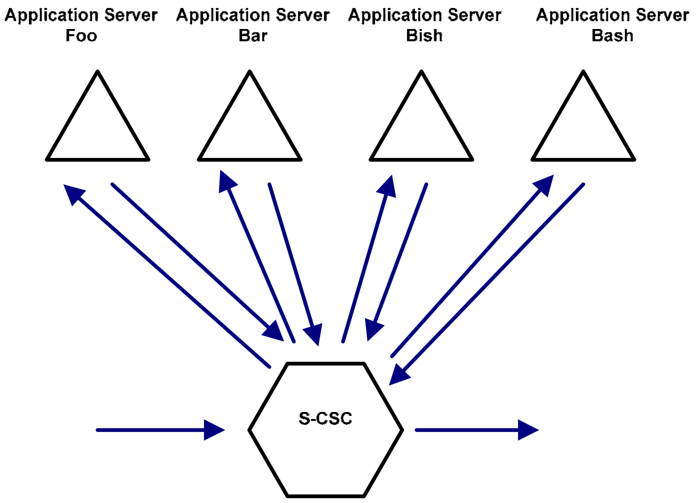


Figure 4 - Application Chaining from S-CSC

The SB//SCIM can operate in the same model as the S-CSC for application chaining but can also support the Application Grouping feature of the MSF Release 2 Service Broker. Application Grouping allows a sequence of applications to be applied atomically to the session which can reduce the number of hops in the signaling path, as shown in Figure 5. Groups of applications will either be applied successfully or fail as a group, the failure of a single application within the group means the group as a whole will not be applied to the session.

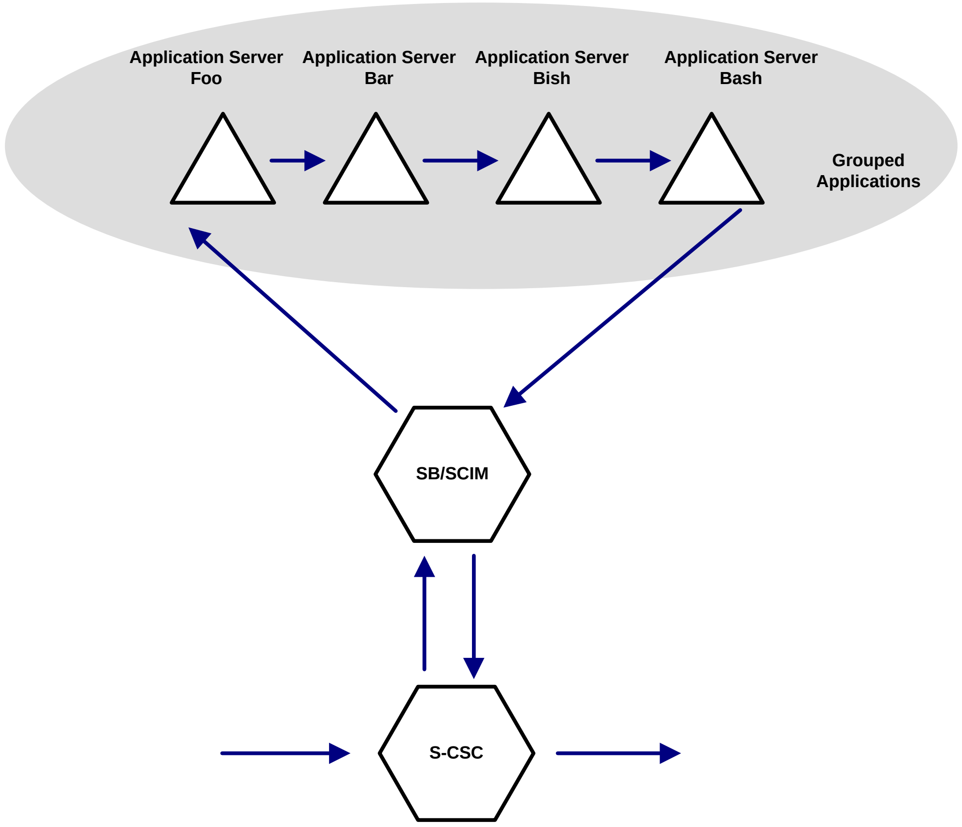


Figure 5 - Application Chaining and Grouping from the SB/SCIM

2.4 Support of Release 2 Call Agents

As was indicated in Figure 1, Release 2 Call Agents are not required to support the ISC interface described in this IA in order to access the Application Platforms. The SB/SCIM supports the Release 2 Call Agent to Service Broker SIP IA and provides interworking between this and the ISC interface, allowing access to the IMS application layer from existing R2 Call Agents.

3 ISC Interface

This Implementation Agreement builds upon the SIP Profile for MSF R3 SIP Server (MSF-IA-SIP.013-FINAL). This IA highlights additional requirements and differences from the R3 SIP Profile and defines the behavior of the S-CSC, the SB/SCIM and the Application Platforms with respect to the SIP interface.

Transport
The ISC interface MUST support UDP as a transport. Other transports (TCP, SCTP) MAY optionally also be supported.

3.1 Registration

The ISC interface supports secondary registration from the S-CSC (which acts as the primary registrar) to the SB/SCIM and Application Platforms.

3.1.1 AS Registration

In order that an Application Server receive a secondary Registration from the S-CSCF then an appropriate entry SHOULD exist in the subscribers service profile. The service profile will contain an iFC (initial Filter Criteria) or shared iFC Set for the Register method, this criteria includes the SIP URI of the Application Server, a default handling (SESSION_CONTINUED or SESSION_TERMINATED) and can optionally contain Service Information to be passed to the Application Server.

3.1.2 SB/SCIM Registration

If the subscriber service profile incorporates the use of the SB/SCIM then a secondary registration for the SB/SCIM SHOULD be generated by the S-CSCF (which is controlled by the subscriber service profile as described above). The SB/SCIM uses the receipt of the REGISTER to retrieve the subscribers service profile (for the SCIM) from the HSS via the Sh interface. This is shown in Figure 6 below. The REGISTER is received by the S-CSC (1) which is used to retrieve the subscribers service profile from the HSS over the Cx (DIAMETER) interface using the Server Assignment Request (SAR) / Server Assignment Answer (SAA) commands (2&3). The subscriber service profile indicates that a secondary REGISTER should be sent to the SB/SCIM (5). The SB/SCIM retrieves the subscriber SCIM service profile from the HSS over the Sh (DIAMETER) interface using the Data Read functions (Sh-Pull 6, Sh-Pull-Response 7). De-registration (indicated with an Expires header value of zero) will cause the SB/SCIM to discard the subscriber SB/SCIM profile.

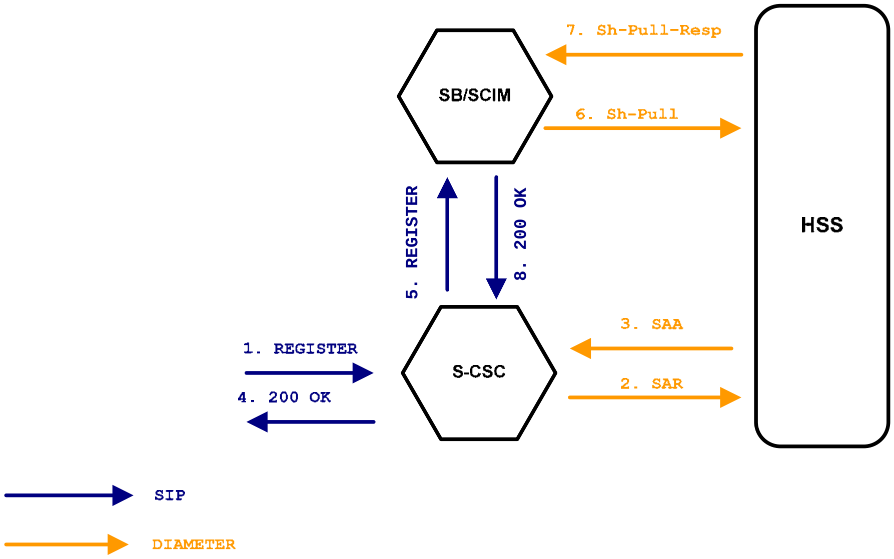


Figure 6 - SB/SCIM Registration

It is recommended (in 3GPP TS 23.218 V7.0.0) that the number of Application Servers receiving secondary REGISTER events should be minimized (in order to reduce the load on the S-CSC). Where multiple Application Servers in a subscribers service profile require notification of Registration then the S-CSC (through the subscriber service profile) generates a single REGISTER towards the SB/SCIM which in turn (based on the subscriber SCIM service profile) generates REGISTER requests to the Application Servers. The 200 response back to the S-CSC is not sent until the REGISTER to all the third party applications has been sent and (in the case of default handling SESSION_TERMINATED) a successful response has returned, this is shown in Figure 7 below.

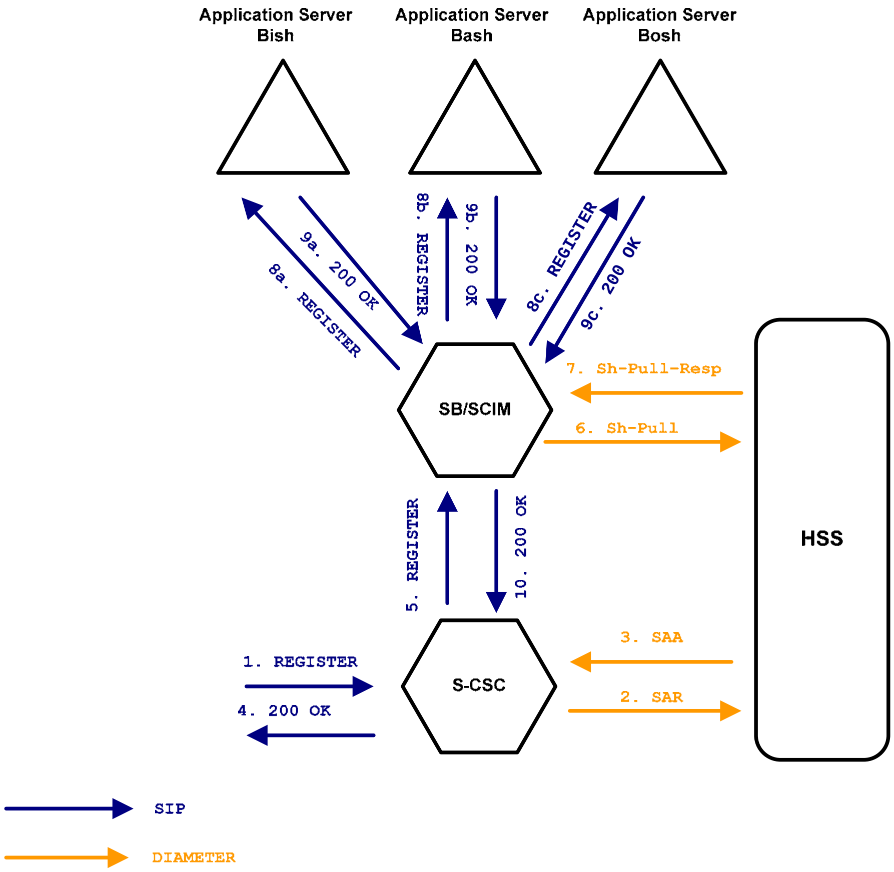


Figure 7 - Registration propagation through SB/SCIM

3.1.3 SIP Header Usage

3.1.3.1 Request-URI

The Request-URI of the REGISTER MUST contain the SIP URI of the AS or SB / SCIM (the S-CSC obtains this from the iFC of the subscribers service profile).

3.1.3.2 From

The From header of the REGISTER MUST contain the SIP URI of the S-CSC sending the REGISTER (in the case of REGISTER propagation from SB/SCIM then it will contain the SIP URI of the SB/SCIM).

3.1.3.3 To

The To header of the REGISTER MUST contain a non-barred public user identity (this is either the user identity received in the REGISTER by the S-CSC or one of the implicitly registered public user identities.

3.1.3.4 Contact

The Contact header of the REGISTER MUST contain the SIP URI of the S-CSC sending the REGISTER (in the case of REGISTER propagation by the SB/SCIM then it will contain the SIP URI of the SB/SCIM).

3.1.3.5 Expires

For initial registration and user initiated re-registration the Expires header SHOULD contain the same value that was returned in the 200OK response to the UE initiated REGISTER. For user and network initiated de-registration the Expires header SHOULD contain a value of zero.

3.1.3.6 P-Access-Network-Info

If the Application Server or SB/SCIM is a trusted entity (part of the same trust domain as the S-CSC) then the P-Access-Network-Info header that the S-CSC receives in the REGISTER SHOULD be included in the secondary Registration towards the AS / SB/SCIM. If the Application Server or SB/SCIM is not part of the trust domain then the P-Access-Network-Info header SHOULD NOT be included in the REGISTER sent to them. Where REGISTER propagation by the SB/SCIM occurs then the SB/SCIM is responsible from removing the P-Access-Network-Info header to Application Servers outside of the trust domain (assuming the SB/SCIM is within the trust domain).

3.1.3.7 P-Charging-Vector

For initial registration and user initiated re-registration the P-Charging-Vector header MUST be included in the REGISTER, this will contain the same icid parameter that the S-CSC received in the original REGISTER from the UE.

3.1.3.8 P-Charging-Function-Address

The REGISTER message SHOULD contain the P-Charging-Function-Address with the values retrieved from the HSS provided the recipient (AS or SB/SCIM) is within the home network of the S-CSCF.

3.1.3.9 Content-Type

If Service Information is associated with the Application Server iFC for the REGISTER method then this SHOULD be included as an XML element in the message body of the REGISTER request. In this case then Content-Type header will include the MIME type application/3gpp-ims+xml as defined in section 7.6 in 3GPP TS 24.229 V7.2.0.

3.1.4 Load Balancing

No dynamic load balancing mechanism for distributing REGISTER messages between Application Server instances by the S-CSC is defined by 3GPP. Each Application Server instance would be identified by a unique SIP URI and the subscriber profile would contain an entry for a specific instance of an Application Server. DNS based distribution could be used to perform basic load distribution but this requires the S-CSC to persist the application server instance used for the duration of the subscriber Registration.

The SB/SCIM may provide an intelligent distribution of REGISTERs to Application Servers based on Application Server utilization, network topology and the subscriber and subscriber access at the time of the request. This feature should not impact the interface described in this IA and is left for vendor implementation and innovation.

3.1.5 Application Server Responses

If the REGISTER is received and accepted by the Application Server / SCIM then it MUST return a 200 OK response. The 200 OK response will include the same value in the Expires header as that received in the the REGISTER.

Should no response be received from the Application Server or an error response be returned to the REGISTER then the action of the S-CSC will be dependent upon the default handling defined in the initial filter criteria. If there is no defined default handling or the default handling is SESSION_CONTINUED then no further action is required. If the default handling is defined as SESSION_TERMINATED then the S-CSC will initiate a de-registration for all currently registered public user identities for the user.

Where the Registration is propagated through the SB/SCIM then the SB/SCIM acts in the following way for Application Server Registration failures.

- If no default handling is defined or the default handling defined in the SCIM service profile indicates SESSION_CONTINUED then no action is taken.
- If the default handling defined in the SCIM service profile indicates SESSION_TERMINATED then the SB/SCIM will return an error response to the S-CSC (the same response returned by the failing Application Server, or 408 Request Timeout in the event of the Application Server returning no response) and perform a de-registration against any Application Servers for which the Registration has already been performed. This is shown in the Figure 8 below.

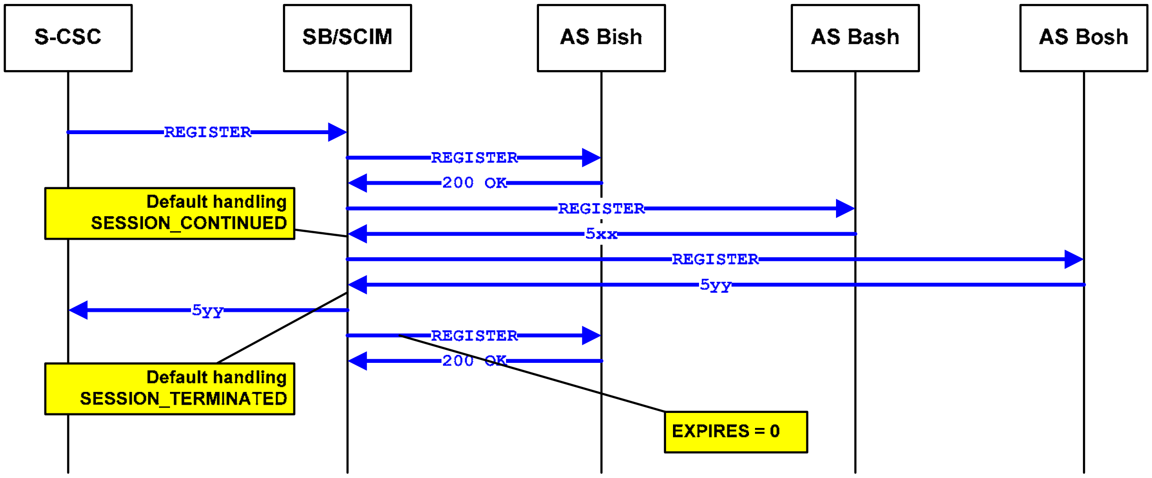


Figure 8 - SB/SCIM propagated Registration failure handling

3.1.6 Registration Event Package

An Application Server or SB/SCIM that receives a secondary Registration may subscribe to the Registration Status event package (described in RFC 3680). In the event of the RESGISTER being propagated through the SB/SCIM the Application Server will subscriber to the SB/SCIM which will in turn subscribe to the S-CSC. Similar to the Registration model, this can help to reduce the load on the S-CSC when multiple Application Servers are subscribing to the registration event package.

3.1.6.1 Registration Event Subscription

The Subscribe sent by the Application Server for the registration event package will have the following headers populated as indicated below.

3.1.6.1.1 Request-URI

The Request-URI is set to the resource that the Application Server is subscribing to, i.e. the public user identity of the user that was received in the To header of the secondary REGISTER.

3.1.6.1.2 From

The From header is set to the SIP URI of the Application Server or SB/SCIM making the subscription request.

3.1.6.1.3 To

The To header is set to the resource that the Application Server or SB / SCIM is subscribing to (same value as the Request-URI).

3.1.6.1.4 Event

The Event header is set to the 'reg' event package (as described in RFC 3680).

3.1.6.1.5 P-Asserted-Identity

The P-Asserted-Identity header is set to the SIP URI of the Application Server or SB/SCIM making the subscription request (same as the From header).

3.1.6.2 Registration Event Notification

The Notification event sent by the S-CSCF (or propagated by the SB/SCIM) will have the following headers populated as indicated below. A NOTIFY response is sent immediately in response to the SUBSCRIBE with additional NOTIFY responses being sent when changes to the registration state occur.

3.1.6.2.1 Request-URI

The Request-URI will contain the SIP URI of the Application Server or SB/SCIM that issued the SUBSCRIBE (the value taken from the From or P-Asserted-Identity header of the SUBSCRIBE).

3.1.6.2.2 Event

The Event header is set to the 'reg' event package (as described in RFC 3680).

3.1.6.2.3 Content-Type

The Content-Type header will contain the value application/registration+xml (from RFC 3680).

The body of the NOTIFY request will contain a registration element for each non-barred public user identity (identified in the aor attribute of each <registration> element).
The <uri> sub-element inside each <contact> sub-element of the <registration> element will contain the contact address provided by the respective UE.

If the public user identity has been de-registered

- The state attribute within the <registered> and <contact> elements is set to 'terminated'.
- The event attribute within each <contact> element to one of 'deactivated','expired','unregistered','rejected; or 'probation' according to RFC3680.

If the deregistration of the public user identity has already been indicated in an earlier NOTIFY and no new registration has occurred then the <registration> element for the deregistered public user identity is not included.

If the public user identity has been registered

- ➢ The state attribute within the <registered> and <contact> elements is set to 'active'.
- ➢ The event attribute within the <contact> element is set to 'registered'

If the public user identity has been automatically registered

- ➢ The state attribute within the <registration> and <contact> elements is set to 'active'.
- ➢ The event attribute within the <contact> element is set to 'created'.

3.2 Service Invocation (INVITE)

The most common SIP method used to trigger applications (and the only one in addition to REGISTER considered in this IA) is the INVITE method used to establish session to and from a subscribers UE. Applications triggered on an INVITE can either act as a terminating User Agent, a redirect server, a proxy or a B2BUA (Back to Back User Agent). These different types of action by the Application Server are shown in Figure 9 below[1].

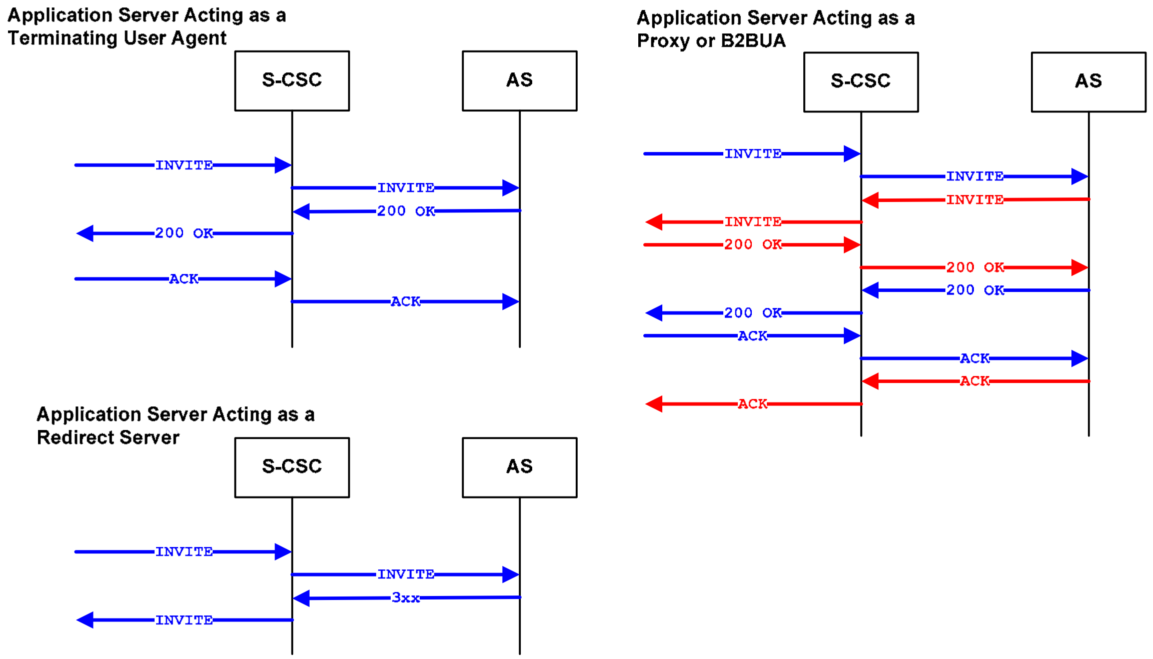

Application Server Acting as a Terminating User Agent
S-CSC
AS
INVITE
INVITE
200 OK
200 OK
ACK
ACK
Application Server Acting as a Proxy or B2BUA
S-CSC
AS
INVITE
INVITE
INVITE
INVITE
200 OK
200 OK
200 OK
200 OK
ACK
ACK
ACK
ACK
Application Server Acting as a Redirect Server
S-CSC
AS
INVITE
INVITE
3xx
INVITE

Figure 9 - Application Server action types

Acting as a Terminating User Agent then the Application Server simply terminates the SIP signaling from the S-CSC. In many cases the Application Server will employ and control a Media Server in order to terminate the media flow. Examples of applications that may act in this manner would be an Information Line service or Voice Mail retrieval.

Acting as a Redirect Server then the Application Server returns a 3xx response to the S-CSC which uses the returned address in a new INVITE to the 'redirected' end-point. Examples of applications that may act in this manner are number translation (e.g. 1-800) or short code dialing.

[1] Application Servers can also act as originating User Agents, this is covered in section 3.4.

Acting as a Proxy or B2BUA then the Application Server becomes part of the end-to-end SIP signaling path (although a Proxy could drop out after the propagation of the initial invite if it desired by not including Record-Route and Via headers in the propagated INVITE). The Application Server is free to perform third party call control on the session to provide a variety of services such as three-way calling (with the employment of a Media Server to act as a Multimedia Conferencing Unit).
As was indicated section 2.2, Application Servers can be engaged through the SB/SCIM or from the S-CSC directly. When the SB/SCIM is used to engage Application Servers then it itself will act as a Proxy/B2BUA towards the S-CSC and become part of the end-to-end SIP signaling flow as indicated in Figure 10 below.

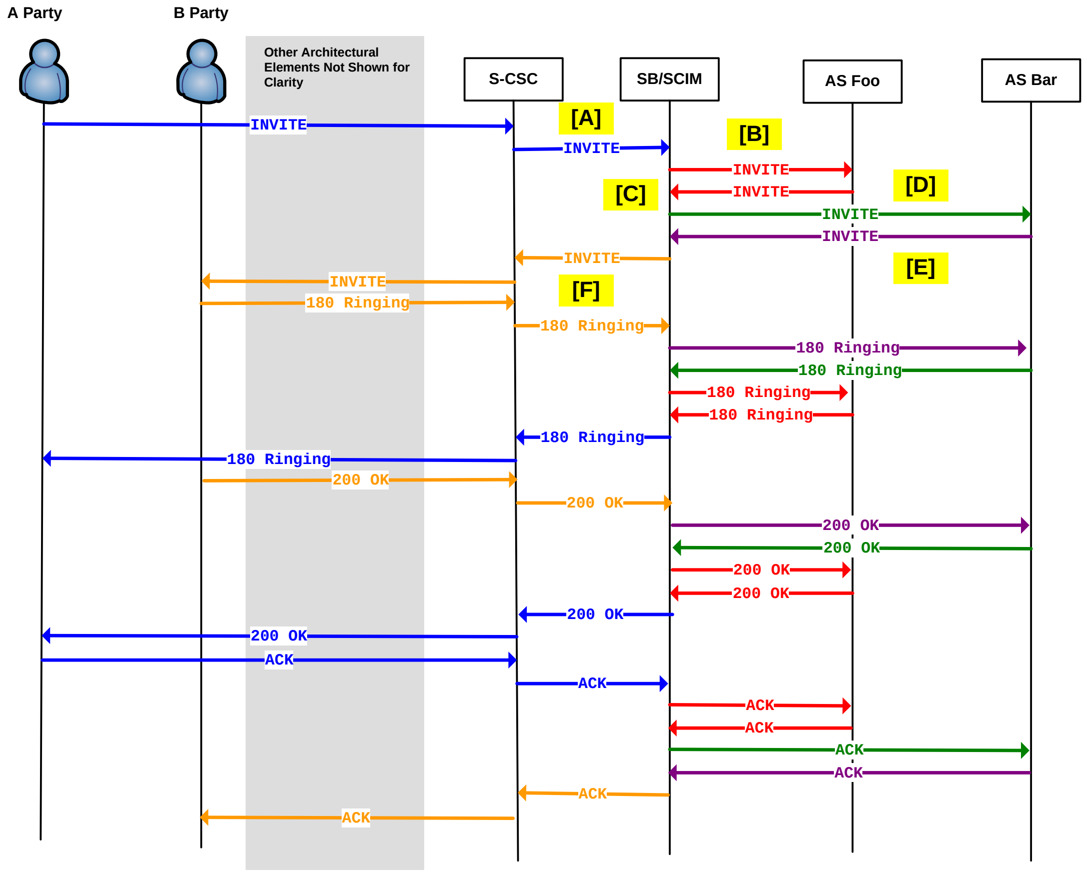


Figure 10 - SB/SCIM as part of end-to-end signaling flow

Figure 10 also illustrates that the Call Id changes during the end-to-end signaling session (in the figure each Call Id is represented as a separate colour). It has been assumed that the S-CSC and Application Server Foo are acting as proxies, the SB/SCIM and Application Server Bar are acting as B2BUA. A reliable mechanism for correlation of the call id's by the S-CSC and SB/SCIM is required as is a mechanism to ensure that appropriate associations of billing records are maintained. These mechanisms are explained in the following section on SIP Header Usage.

3.2.1 SIP Header Usage

The following sections indicate the expected usage of some SIP Headers in the INVITE sent from the S-CSC to the SB/SCIM or Application Server; or from the SB/SCIM to the Application Server.

3.2.1.1 Route

The topmost entry of the Route header SHOULD contain the SIP URI of the entity being invoked (Application Server or SB/SCIM). In order that the Application Server or SB/SCIM is able to distinguish between invocations for the originating and terminating party then a role parameter SHOULD be appended to the SIP URI in the route header; role=orig for originating invocations and role=term for terminating invocations. This role parameter could be included in the Application Server SIP URI of the service profiles read from the HSS.

Where a physical Application Server hosts more than one service and exposes them individually then the RFC 3087 model MAY be used to identify the individual service on the Application Server. The user part of the SIP URI is used to identify the service on the Application Server. For example a Voice Mail Application Server could be invoked in one of three modes, for message retrieval, to leave a message on subscriber busy and to leave a message on subscriber no-answer (similar to busy bit with perhaps a different initial prompt). These could be addressed as, for example:-

retrieve@voicemail.msf.org
deposit-busy@voicemail.msf.org
deposity-rna@voicemail.msf.org

If the Application Grouping Feature of the SB/SCIM is being used (described in section 2.3) then the next entries in the Route header SHOULD contain the SIP URI of the remaining application servers in the group in the order in which they are to be invoked. Thus if the group consists of three application servers (Bish, Bash and Bosh) being invoked for the terminating party then the topmost three entries of the Route header would be.

```
Route:  <sip:serviceFoo@Bish.msf.org; role=term; lr>
        <sip:serviceBar@Bash.msf.org; role=term; lr>
        <sip:serviceBaz@Bosh.msf.org; role=term; lr>
```

After the Application Server entries in the Route header then the S-CSC or SB/SCIM SHOULD include an entry for itself. This entry is used to direct onward signaling from the AS (or SB-SCIM) back through the S-CSC (or SB/SCIM). This Route is also used for correlation purposes (since the Call Id may change), allowing the propagated INVITE to be associated with the sent INVITE. The recommended option for the correlation parameter in the Route header is a character string in the user part of the SIP URI (since the same entity creates and consumes the token then the actual encoding can be left to individual implemention).

For example, with reference to Figure 10 then assuming that Application Server Foo and Bar are invoked for the originating subscriber through the SB SCIM then

The Route header in INVITE [A] will contain

```
Route: <sip:ServiceBroker@sb-scim1.example.com; role=orig; lr>
       <sip:uniquedialogidentifier@s-csc1.example.com; lr>
```

The Route header in INVITE [B] will contain

```
Route: <sip:serviceFoo@Foo.example.com; role=orig; lr>
       <sip:uniquedialogidentifier2@sb-scim1.example.com;lr>
       <sip:uniquedialogidentifier@s-csc1.example.com; lr>
```

The Route header in INVITE [C] will contain

```
Route: <sip:uniquedialogidentifier2@sb-scim1.example.com;lr>
       <sip:uniquedialogidentifier@s-csc1.example.com; lr>
```

The Route header in INVITE [D] will contain

```
Route: <sip:serviceBar@Bar.example.com; role=orig; lr>
```

```
       <sip:uniquedialogidentifier2@sb-scim1.example.com;lr>
       <sip:uniquedialogidentifier@s-csc1.example.com; lr>
```

The Route header in INVITE [E] will contain

```
Route: <sip:uniquedialogidentifier2@sb-scim1.example.com;lr>
       <sip:uniquedialogidentifier@s-csc1.example.com; lr>
```

The Route header in INVITE [F] will contain

```
Route: <sip:uniquedialogidentifier@s-csc1.example.com; lr>
```

3.2.1.2 P-Asserted-Identity

For originating service invocations the P-Asserted-Identity SHOULD contain the SIP URI of the user the service is being invoked for. The Application Server or SB/SCIM will use this value to identify the subscriber to apply the originating service to.

When the S-CSC has knowledge of an associated Tel-URI for the subscriber identified by the SIP-URI in the P-Asserted-Identity header then a second P-Asserted-Identity header MAY be included containing the Tel-URI will be included.

3.2.1.3 P-Access-Network

If the Application Server or SB/SCIM is a trusted entity (part of the same trust domain as the S-CSC) then the P-Access-Network-Info header that the S-CSC receives in the INVITE SHOULD be included in the INVITE propagated to the AS / SB/SCIM. If the Application Server or SB/SCIM is not part of the trust domain then the P-Access-Network-Info header is not included in the INVITE sent to them. Where INVITE propagation by the SB/SCIM occurs then the SB/SCIM is responsible from removing the P-Access-Network-Info header to Application Servers outside of the trust domain (assuming the SB/SCIM is within the trust domain).

3.2.1.4 P-Charging-Vector

The P-Charging-Vector MUST be passed in the INVITE in order to allow the billing records produced by the application entities to be correlated.

3.2.1.5 P-Charging-Function-Address

The INVITE message SHOULD contain the P-Charging-Function-Address with the values retrieved from the HSS provided the recipient (AS or SB/SCIM) is within the home network of the S-CSCF.

3.2.1.6 Record-Route

When the INVITE is crossing a trust domain then it is up to the sending party (S-CSC or SB/SCIM) to determine (based on configuration parameters) whether to Record-Route or not. If the INVITE request is to be Record-Routed then the sending entity shall include a Record-Route header containing its own SIP URI.

3.2.1.7 Request-Disposition

Only the last application in the ‘application chain’ is permitted to perform forking (due to the implications of potentially multiply invoking subsequent applications further down the chain). The SIP INVITE sent towards all Application Servers except the last in the chain (the lowest priority iFC) SHOULD have a Request-Disposition header with a value of ‘no-fork’.

In the case of grouped applications (explained in section 2.3) then all of the applications within the group will receive the same value (‘no-fork’) of Request-Disposition. If the last application in the ‘application chain’ requires the ability to fork it cannot be grouped.

3.2.1.8 Resource-Priority

The SB/SCIM MAY provide special handling, such as priority queuing, for messages that include this header. The SB/SCIM SHOULD be able to trigger to an application server based on the presence of the header. Whether or not it provides any special handling the SB/SCIM MUST pass the Resource-Priority header into the outgoing messages.

Application servers SHOULD be able to communicate the information contained in the header to associated application code.

3.2.2 Load Balancing

No dynamic load balancing mechanism for distributing INVITE messages between Application Server instances by the S-CSC is defined by 3GPP. Each Application Server instance would be identified by a unique SIP URI and the subscriber profile would contain an entry for a specific instance of an Application Server. In many cases the ‘pinning’ of a subscriber to a specific Application Server instance is necessary (since the Application Server may host subscriber specific data) in other cases then DNS based distribution could be used to perform basic load distribution amongst equivalent Application Server instances.

The SB/SCIM may provide an intelligent distribution of INVITEs to Application Servers based on Application Server utilization, network topology and the subscriber and subscriber access at the time of the request. This feature should not impact the interface described in this IA and is left for vendor implementation and innovation.

3.2.3 Retries

According to RFC3261 then if an unreliable protocol (such as UDP) is used as the transport for SIP then an INVITE must be retried a number of times before the destination is considered unreachable; the default timings are for six retries to be attempted at 0.5s, 1.5s, 3.5s, 7.5s, 15.5s, 31.5s with the destination being declared unreachable after 32 seconds. 32 seconds is too great a time period to wait for an unavailable Application Server.
The following is suggested.

For Application Servers with a default handling in the filter criteria of SESSION_CONTINUED then a maximum of two retries will be performed (at 500ms and 1.5s) and the Application Server considered unreachable after 2 seconds.

For Application Servers with a default handling in the filter criteria of SESSION_TERMINATED then a maximum of three retries will be performed (at 500ms, 1.5s and 3.5s) and the Application Server considered unreachable after 4 seconds.

3.2.4 Application Server Responses

Where the Application Server acts as a proxy or B2BUA then the session will continue with an INVITE being sent back from the Application Server to the S-CSC (or SB/SCIM). The actions taken on responses to the INVITE sent to the Application Server are described below.

3.2.4.1 100 Trying

The Application Server (or SB/SCIM) should return a 100 Trying response to the S-CSC or SB/SCIM Broker immediately upon receipt of the INVITE to prevent un-necessary resends of the INVITE.

3.2.4.2 3xx Redirect

An Application Server acting as a Redirect server may return a 3xx response to the INVITE.

If a 3xx response is returned to the SB/SCIM then it will be passed back along the Application chain (should one exist) and then returned to the S-CSC (no further applications will be invoked by the SB/SCIM).

If a 3xx response is returned to the S-CSC then no further applications are invoked and the S-CSC will propagate the INVITE to the destination indicated in the 3xx response. Should that destination be currently registered on the S-CSC that receives the 3xx then it will check the service profile and engage any applications (or the SB/SCIM) as indicated in the filter criteria of the profile. If the destination is not registered on the S-CSC then it performs originating side session routing and forwards the INVITE on to the S-CSC handling the registration of the subscriber identified in the destination address, or in the case of the subscriber not being registered an appropriate S-CSC

3.2.4.3 Error Responses

If the Application Server returns an error response to the INVITE (or no response is received at all) then the action taken depends upon the default handling specified in the filter criteria for the application.

If the default handling indicates SESSION_CONTINUED then the failed application is ignored and the next application (if any) is invoked by sending an INVITE to it. If no further applications are to be invoked then call processing continues.
If the default handling indicates SESSION_TERMINATED then the receiving entity (SB/SCIM or S-CSC) removes any already engaged application from the chain (by returning the error response received from the failed application to each of the propagated INVITES from the application. This error is then returned to the INVITE received by the triggering entity (in the case of the SB/SCIM then back to the S-CSC, in the case of the S-CSC then back to the P-CSC).

Failures detected through no-response from the Application Server are reported as a 503 ‘Service Unavailable’ to entities earlier in the SIP chain.

3.2.5 Session Continuation

Where the Application Server acts as a proxy or B2BUA then the session will continue with an INVITE being sent back from the Application Server to the S-CSC (or SB/SCIM). Generally the INVITE returned from the Application Server will form the input INVITE to the next entity. Should the Application Server modify the Request-URI however then different action may be taken as described in the section below.

3.2.5.1 Request-URI

The Request-URI in the SIP INVITE returned/ propagated back from the Application Server will contain the destination party address. The Application Server may, as part of the service it is providing, have modified this destination party address.

If the propagated INVITE contains a different destination address than the INVITE sent to the Application Server, and the Application Server was invoked for terminating services then.

- If the propagated INVITE is received by the SB/SCIM it will not engage any further applications for the original terminating user and will immediately propagate the INVITE with the new destination party address back to the S-CSC.

- If the propagated INVITE is received by the S-CSC then it will not engage any further applications for the original terminating user.
  - If the new destination address is registered on the S-CSC then it will check the service profile to determine if any terminating services need to be invoked for the subscriber identified by new destination address.
  - If the new destination address is not registered on the S-CSC then it performs originating side session routing and forwards the INVITE on to the S-CSC handling the registration of the subscriber identified in the new destination address, or in the case of the subscriber not being registered an appropriate S-CSC.

3.3 Service Invocation (other SIP Methods)

This version of the IA only details the invocation of applications based on the REGISTER and INVITE SIP Methods. Applications that need to take action based on other SIP Methods or messages within the session should be invoked with the initial INVITE and act as a proxy or B2BUA, becoming part of the end-to-end SIP signaling path in order to monitor the SIP messages and take appropriate action.

Details of service triggering on other SIP methods may be added in future versions of this IA.

3.4 Application Initiated Sessions

Figure 11 below shows the basic SIP flow for an Application Server initiated session between two parties (for example a click to dial application). The recommendation for such both two party calls is flow IV of RFC3725. The Application Server issues an INVITE to the initial (A) party including an SDP with no media (no m lines -< implying the media makeup of the session will be established later). The party answers the call and responds with 200 OK containing an SDP with no media.

The Application Server sends n INVITE to the second (B) party, this time with no SDP. The second (B) party returns an offer SDP in the 200 OK which the Application Server uses in a re-INVITE to the initial (A) party. The SDP returned from the initial (A) party in the 200 OK is sued to answer the offer in ACK to the second (B) party.

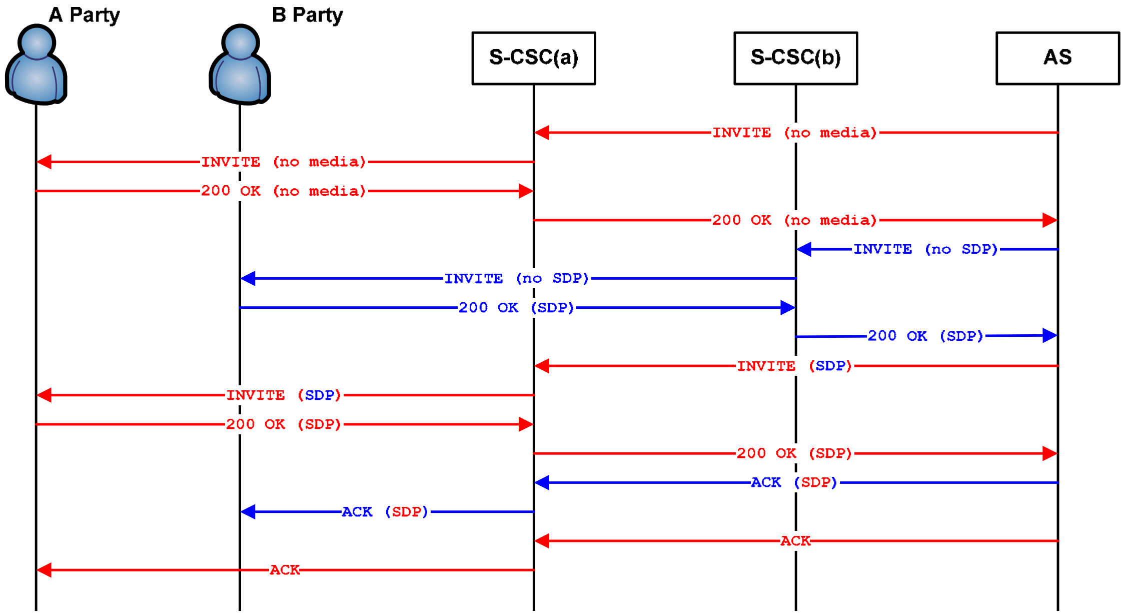


Figure 11 - 3PCC from an Application Server

It is the responsibility of the Application Server to determine the S-CSC to send the INVITE to, this can be achieved through

- Monitoring the Registration state of the subscribers it is serving (although this is likely to only provide information for one of the two destinations in the general case).
- Querying the HSS (via the Sh interface)
- Static configuration.

The Application Server Initiating the Session must handle the following headers as specified.

3.4.1 P-Charging-Vector

The same value of P-Charging-Vector must be used on both call legs in order that the billing records for them can subsequently be correlated.

3.4.2 P-Asserted-Identity

When the Application Server is acting on behalf of a subscriber then the subscribers public identity will be included in the P-Asserted-Identity of the INVITEs.

3.4.3 Route

The Application Server will include a Route header entry (the topmost) for the S-CSC where the destination public identity is registered or hosted (unregistered case). Where the destination and the P-Asserted-Identity are the same (Application Server acting on behalf of a subscriber and initiating a call leg to them) then the role=orig parameter will be appended to the SIP-URI of the S-CSC in the Route header.

3.4.4 Off-Net Subscribers

In some cases one or more of the target destinations for an application initiated session are not destinations handled by the same network that is hosting the Application Server. Where one destination of the session is handled through an S-CSC of the same network as the Application Server then any INVITE for 'off network' destinations will also be sent through the same S-CSC instance. Where none of the destinations of the session are handled through an S-CSC of the same network then the Application Server then the S-CSC instance to send the INVITEs to will be configured in the Application Server.

3.5 Conditional Service Invocation

One of the primary functions of the SB/SCIM is to enable Conditional Service Invocation. The service profiles of the S-CSC are essentially static in nature. The filtering decision about whether a SIP Request is to be forwarded to an Application Server or not is based purely on the contents (headers, header values and SDP) of the SIP Request. Conditional Service Invocation extends the decision criteria in order to take account of state information, this can be state information associated with the session itself or external state information (for example location).

Conditional Service Invocation is included in the SCIM service profile definition described in Appendix A. The model is intended to be extensible to a wide variety of context state types.
Conditional Service Invocation is only performed by the SB/SCIM.

This IA describes two context state types, Basic Call State Model and Calendar. Future versions of this IA may include additional context state types.

3.5.1 Basic Call State Model

The Basic Call State Model context state type allows the definition of service triggering based on four call trigger points for both the originating and terminating call half. The service can be triggered on:-

- Call Attempt (INVITE)
- Busy (486 Busy Here)
- No Answer (internal timer)
- Hang-Up (BYE)

Invocation of Applications based on Call Attempt is identical to the invocation of applications on an INVITE described earlier in the IA.

The invocation of an Application Server based on a busy condition is shown in Figure 12 below. When a Busy condition is detected by the SB/SCIM then it completes the SIP transaction to the busy leg of the call (sending an ACK) and initiates a new SIP INVITE towards the Application Server.

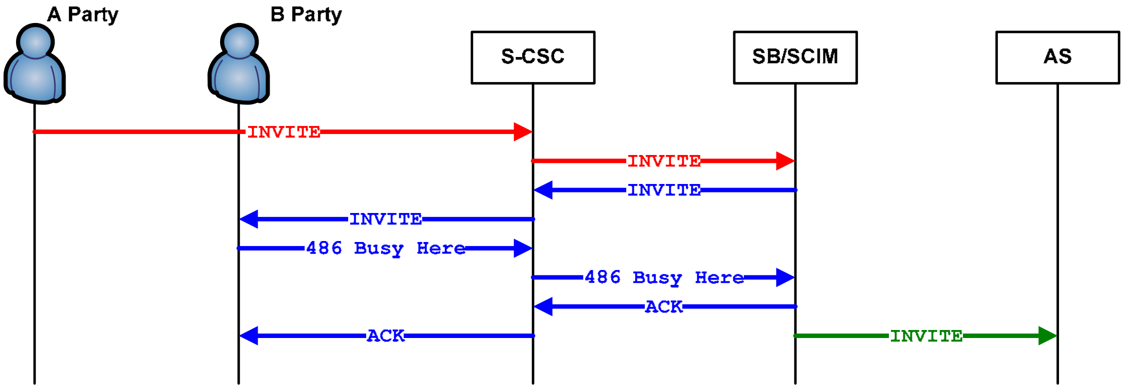


Figure 12 - Invocation of Application Server upon Busy

The invocation of an Application Server based on a No Answer condition is shown in Figure 13 below. When the no-answer timer expires on the SB/SCIM then the INVITE on the terminating call half is cancelled and a new INVITE sent to engage the Application.

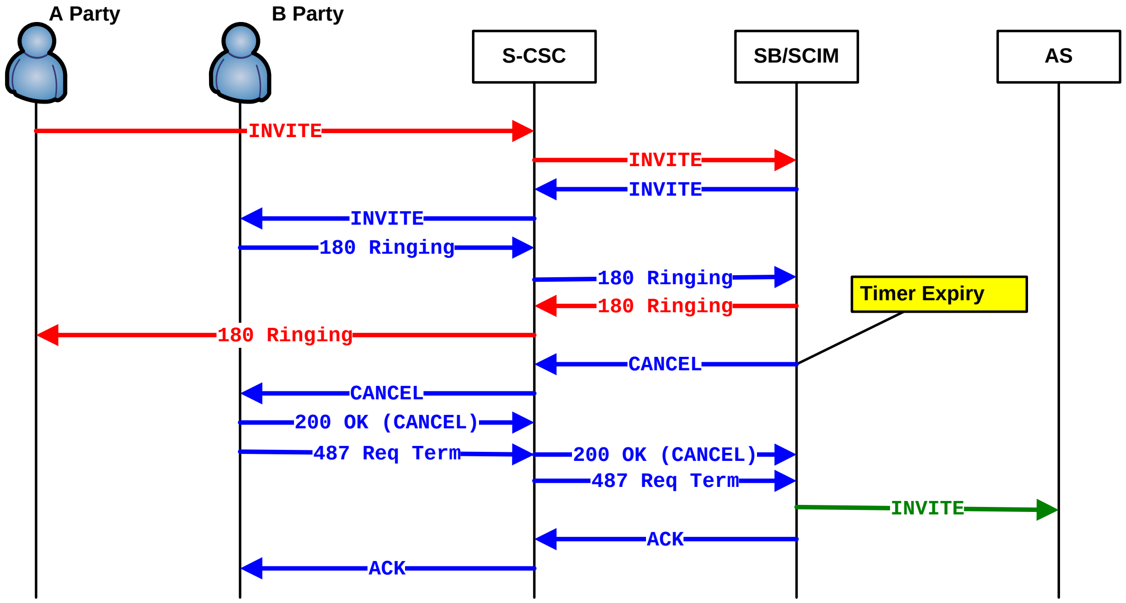


Figure 13 - Invocation of Application upon No Answer

The invocation of an Application Server based on a Hang-up condition is shown in Figure 14 below. When the destination (B) party hangs-up the SB/SCIM receives a BYE which triggers a new INVITE to an Application Server. During the invocation of the new Application Server the remaining party (originating (A) party in this example) is put on hold and subsequently re-INVITED with the SDP returned from the newly invoked Application Server.

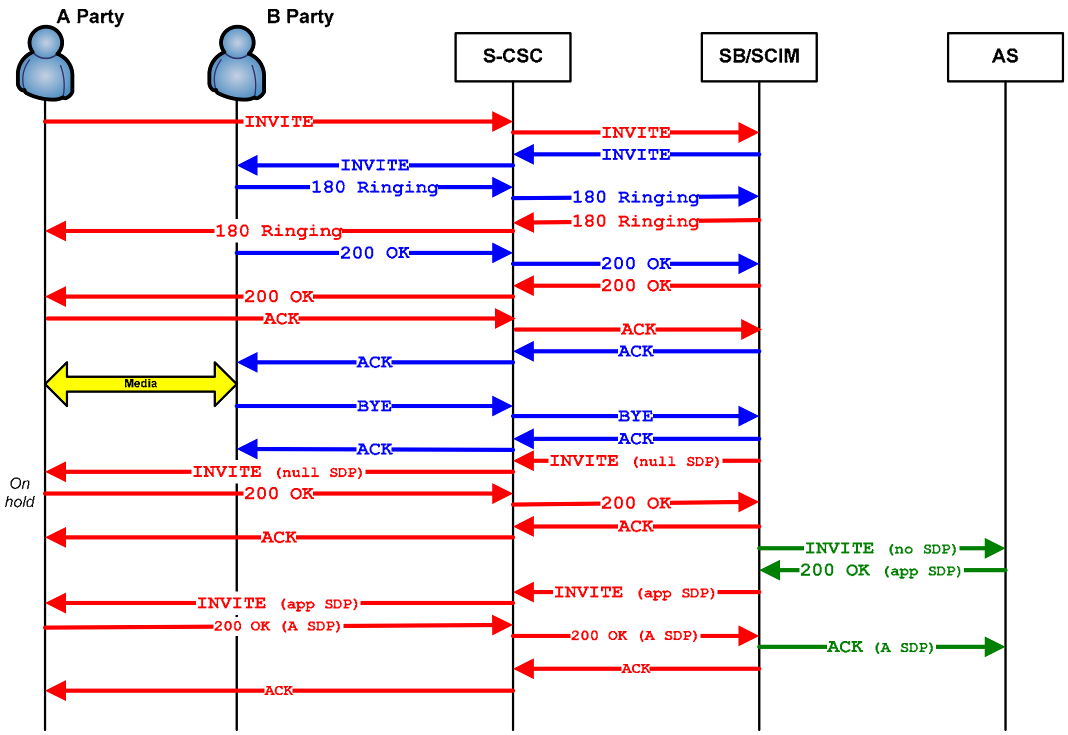


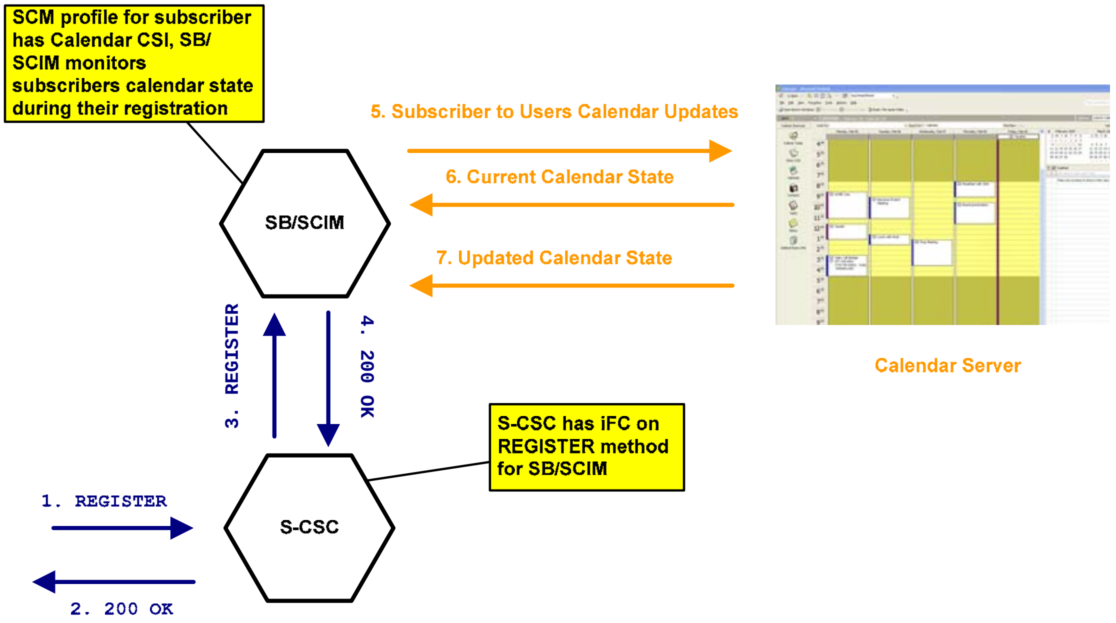
Figure 14 - Invocation of Application upon Hangup

3.5.2 Calendar

The Calendar context state type allows the definition of further conditions on filter criteria or Basic Call State Model triggers. The Calendar state for a subscriber can take the values of ‘FREE’, BUSY’, ‘BUSY-UNAVAILABLE’, ‘BUSY-TENTATIVE’ (these states are taken from the iCalendar definitions in RFC 2445) along with ‘UNOBTAINABLE’ which indicates the subscribers calendar information is not currently available.

The Filter Criteria of the Subscriber SCIM service profile can include conditions on this state, for example a trigger on a terminating INVITE for the Voice Mail application if the subscribers calendar state is BUSY-UNAVAILABLE.

It is envisaged that the SB/SCIM will obtain a subscribers current calendar state upon registration and be notified of changes to the state. The SB/SCIM is always aware of the calendar state for registered subscribers (that make use of Calendar based Conditional Service Invocation) such that it does not have to query an external data source in order to evaluate any calendar conditional statements (reducing the transit delay for the SIP messages). This is shown in Figure 15 - Calendar Conditional Service Invocation below.


5. Subscriber to Users Calendar Updates
6. Current Calendar State
7. Updated Calendar State
SB/SCIM
3. REGISTER
4. 200 OK
S-CSC
1. REGISTER
2. 200 OK
Calendar Server

SCM profile for subscriber has Calendar CSI, SB/ SCIM monitors subscribers calendar state during their registration

S-CSC has iFC on REGISTER method for SB/SCIM

Figure 15 - Calendar Conditional Service Invocation

The mechanism for obtaining and monitoring the subscribers calendar state is not within the scope of this IA.

4 NAT and Firewall traversal

Should NAT functions be performed between the S-CSC, the SB/SCIM and the Application Servers then the Route headers still need to remain sufficiently intact for the correlation functions described earlier in this IA to be performed.

5 QoS aspects

There are no specific QoS aspects to the ISC interface but as it does form part of the overall end-to-end call set-up signaling then any end-to-end messaging associated with QoS establishment (such as the precondition offer/answer model described in RFC 3312) will be preserved on the ISC interface.

6 Security aspects

This IA assumes that encrypted SIP signaling will not be used on the ISC interface.

7 Redundancy and resilience

Stateful components (S-CSC, SB/SCIM and some Application Servers) are required to meet accepted network reliability levels. Typically five nines 99.999% reliability with no single point of failure. Components should perform failover processing themselves without reliance on any external stimulus and with the minimum of impact on any component they interface with (sole reliance on clients resending to an alternate IP address is not a robust mechanism for providing resilience).

Mechanism for disaster recovery may also be required in order to cater for larger scale failures (such as loss of a complete site). External intervention to affect DR level switchover is acceptable.

8 References

Issuer	Reference	Title
IETF	RFC3261	SIP: Session Initiation Protocol
IETF	RFC3725	Best current practices for third party call control (3pcc) in SIP.
IETF	RFC3680	SIP Event Package for Registration.
IETF	RFC3087	Control of service context using SIP Request-URI.
IETF	RFC3312	Integration of Resource Management and SIP.
IETF	RFC2445	Internet Calendaring and Scheduling Core Object Specification (iCalendar).
3GPP	TS 23.218 v 7.0.0	IMS IM Call Model.
3GPP	TS 24.229 v 7.2.0	IP Multimedia call control based on SIP and SDP.
3GPP	TS 29.228 v 7.0.0	IMS Cx and Dx interfaces; Signaling flows and message contents.
3GPP	TS 29.229 v 7.0.0	Cx and Dx interface based on the Diameter protocol.
3GPP	TS 29.328 v 7.0.0	IMS Sh interface; Signaling flows and message contents.
MSF	MSF-IA-SIP.012-FINAL	SIP profile for an MSF R3 SIP Server.
MSF	MSF-IA-DIAMETER.002-FINAL	Implementation Agreement for the d2 and d3 interfaces for GMI 2006.
MSF	MSF-IA-DIAMETER.003-FINAL	Implementation Agreement for the d4,d5,d6 and d7 interfaces for GMI 2006.
MSF	MSF-ARCH-003.00-FINAL	MSF Release 3 Architecture.
MSF	MSF-IA-SIP.005-FINAL	Implementation Agreement for SIP interface between Call Agent and Service Broker.

Appendix A – SCIM HSS Profile

The following picture gives an outline UML model of the SCIM Service Profile Class:

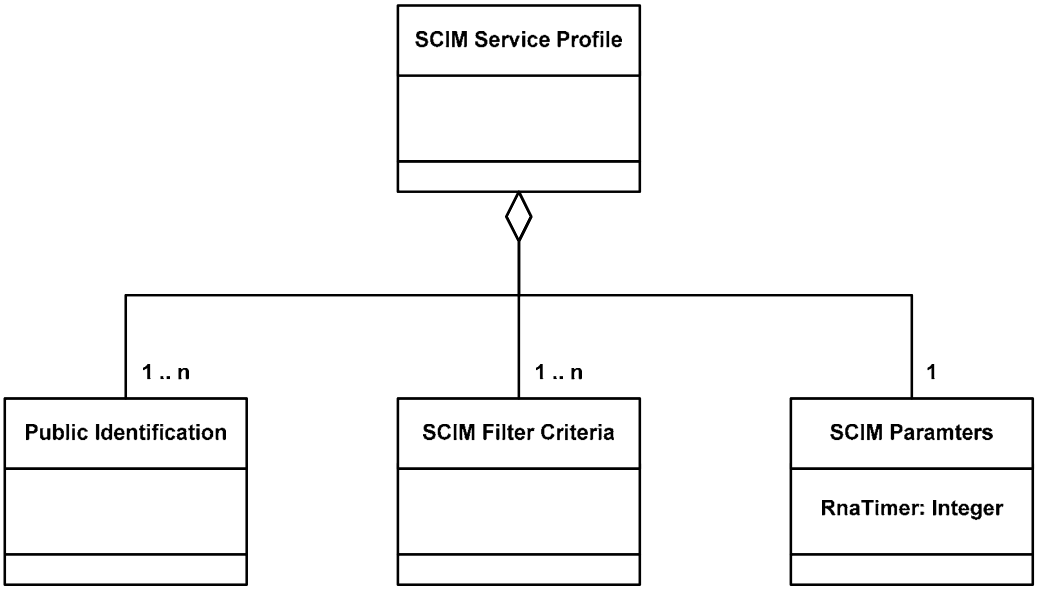


Figure 16 - SCIM Service Profile Class

Each instance of the SCIM Service Profile consists on one or several instances of the class Public Identification. This class is defined for the base User Profile for the subscriber in Annex B of 3GPP TS 29.228 V7.0.0. The information in the SCIM Filter Criteria and SCIM Parameters classes apply to all Public Identification Instances. Each instance of the SCIM Service Profile class contains 1 or more instances of the SCIM Filter Criteria class and one instance of the SCIM Parameters Class.

The SCIM Parameters class contains a single attribute, RnaTimer. This is the an integer value that represents the timeout value to be used to trigger 'no-answer' service invocation. The RnaTimer is in units of 0.1 seconds, a value of 120 = 12 seconds.

The SCIM Filter Criteria class is shown in Figure 17. The Application Server, Trigger Point and Service Information Classes are identical to those of the base User Profile for the subscriber. The two differences being SCIM Service Point Trigger class replaces the Service Point Trigger class and that multiple applications can be associated with a SCIM Filter Criteria instances to enable Application Grouping (see Figure 5).

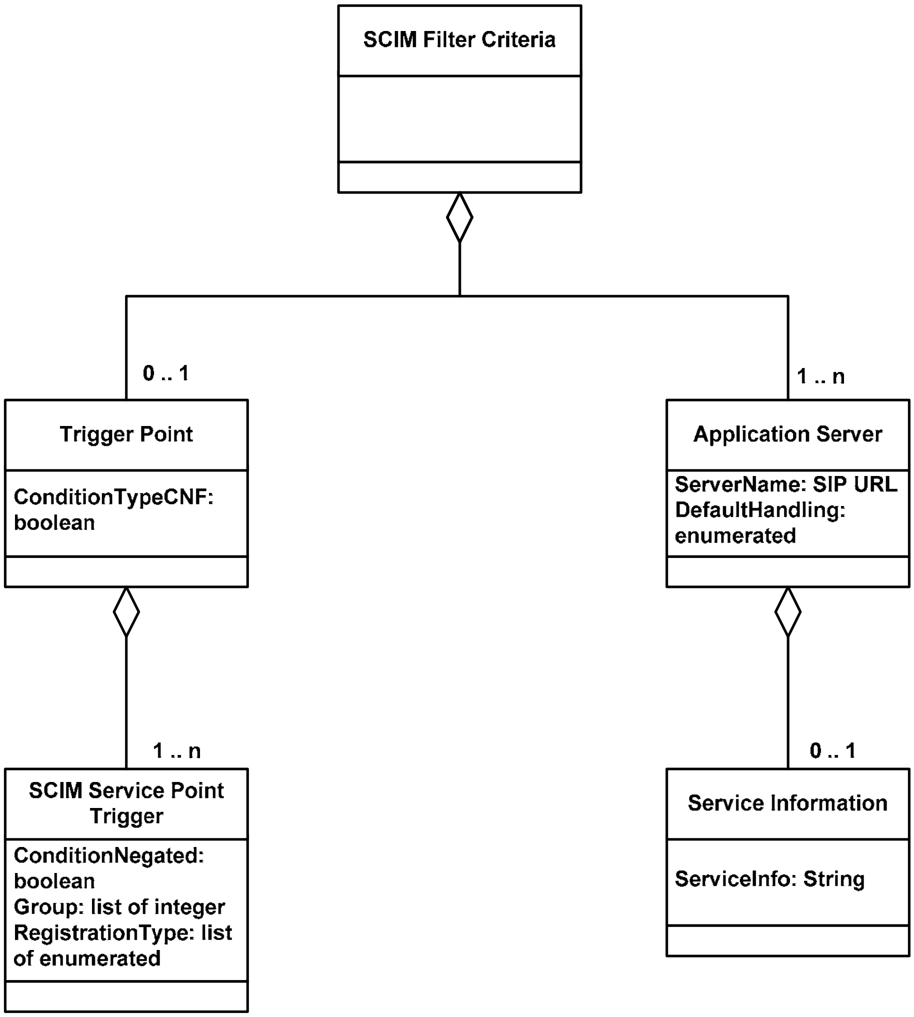


Figure 17 - SCIM Filter Criteria Class

Figure 18 below shows the SCIM Service Point Trigger class. This is an extension to the Service Point Trigger class of the base User Profile for the subscriber. The additional classes within the SCIM Service Point Trigger class are shown in red in the figure.

The Basic Call State class defines SCIM Service Point Triggers on the basic calls state. The CallState attribute can take one of the following values ‘Call Attempt’, ‘Busy’,’No Answer’,Hang Up’. If an instance of the Basic Call State class exists within the SCIM Service Point Trigger then the only other classes allowed are Session Case and Calendar. Conversely if any of the Request-URI, SIP Method, SIP Header or Session Description classes are present then the Basic Call State class may not be present in the SCIM Filter Criteria class instance.

The Calendar class defines SCIM Service Point Triggers on the subscribers calendar state. The CalendarState attribute can take one of the following values ‘FREE’,’BUSY’,’BUSY-UNAVAILABLE’,’BUSY-TENTATIVE’ and ‘UNOBTAINABLE’.

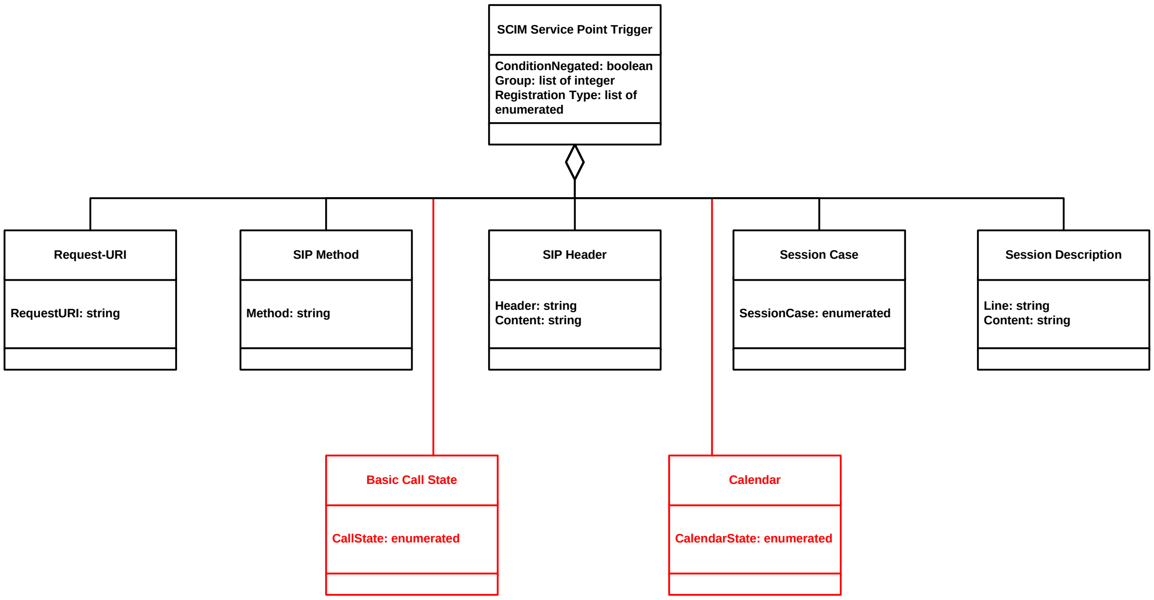


Figure 18 - SCIM Service Point Trigger Class

Appendix B – Sample Call Flows

B.1 Registration

This example shows the propagation of a registration to application server Foo during the registration of subscriber Major Clanger.

1) REGISTER (authenticated) FROM I-CSC to S-CSC

```
REGISTER sip:blueplanet.com SIP/2.0
Via: SIP/2.0/UDP icsc.blueplanet.com;branch=z9hG4bK77ef4c12345.2
Via: SIP/2.0/UDP pcsc.blueplanet.com;branch=z9hG4bK77ef4c2312983.2
;received=192.168.1.44
Via: SIP/2.0/UDP 89.0.224.34;branch=z9hG4bKnashds8;received=147.29.80.136
Max-Forwards: 68
To: Major Clanger <sip:mclanger@blueplanet.com>
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301775
Call-ID: a84b4c76e66711
Supported: path
Path: <sip:MajorClanger@pcsc.blueplanet.com;lr>
CSeq: 2 REGISTER
Contact: <sip:mclanger@89.0.224.34>
Authorization: Digest realm="blueplanet.com",
nonce="6b9fe2f50fcad6eb134d952fe3a07160",
opaque="42e063c9b26f9b189c83cd5a596aa35a",qop=auth,username="9723542109",uri="s
ip:coventry.com, algorithm=MD5,
response="a3aa339fa168a357e2792d0a30e2f6b1",cnonce="4aafe4f95bfda97181fc90bf31b
d981a", nc=00000001
Content-Length: 0
```

2) 200 OK response from S-CSC to I-CSC

```
SIP/2.0 OK
Via: SIP/2.0/UDP icsc.blueplanet.com;branch=z9hG4bK77ef4c12345.2
Via: SIP/2.0/UDP pcsc.blueplanet.com;branch=z9hG4bK77ef4c2312983.2
;received=192.168.1.44
Via: SIP/2.0/UDP 89.0.224.34;branch=z9hG4bKnashds9;received=147.29.80.136
Path: <sip:mclanger@pcsc.blueplanet.com;lr>
Service-Route: <sip:mclanger@scsc.blueplanet.com;lr>
To: Major Clanger <sip:mclanger@blueplanet.com>;tag=12345679
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301775
Contact: <sip:mclanger@89.0.224.34>
Call-ID: a84b4c76e66711
CSeq: 2 REGISTER
Content-Length: 0
```

3) Secondary REGISTER propagated to Application Server Foo (based on the iFC of the service profile of Major Clanger). The Secondary REGISTER includes Service Information from the HSS.

```
REGISTER sip:foo.blueplanet.com SIP/2.0
Via: SIP/2.0/UDP scsc.blueplanet.com; brancj=z9hG4bK3434343434
Max-Forwards: 70
To: Major Clanger <sip:mclanger@blueplanet.com>
From: sip:scsc@blueplanet.com>;tag=1928307656
Call-ID: abc123456def
CSeq: 1 REGISTER
```

```
Contact: <sip:scsc.blueplanet.com>
Content-Length: x
Content-Type: application/3gpp-ims+xml
```

24) 00 OK response from Application Server Foo to the S-CSC

```
SIP/2.0 OK
Via: SIP/2.0/UDP scsc.blueplanet.com;branch=z9hG4bK3434343434
To: Major Clanger <sip:mclanger@blueplanet.com>;tag=12345679
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301775
Contact: <sip:scsc.blueplaner.com>
Call-ID: abc123456def
CSeq: 1 REGISTER
Content-Length: 0
```

B.2 Application Invocation

Application Server Foo is invoked for an originating INVITE from Major Clanger. In this example Major Clanger is initiating a session to Tiny Clanger.

INVITE from P-CSC to S-CSC to which Major Clanger is registered.

```
INVITE sip:tclanger@blueplanet.com SIP/2.0
Route: <sip:scsc.blueplanet.com;lr>
Record-Route: <sip:mclanger@pcsc.blueplanet.com;lr>
Via: SIP/2.0/UDP pcsc.blueplanet.com;branch=z9hG4bK77ef4c2312983.1
Via: SIP/2.0/UDP 89.0.224.34;branch=z9hG4bKnashds8;received=147.29.80.136
Max-Forwards: 69
To: Tiny Clanger <sip:tclanger@blueplanet.com>
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Route:<sip:mclanger@scsc.blueplanet.com;lr>
Supported: 100rel, timer, precondition
Session-Expires: 180; refreshor=uac
Min-SE: 120
Allow: INVITE, ACK, CANCEL, BYE, PRACK, REFER, UPDATE
Contact: <sip:sessionxx@pcsc.blueplanet.com>
P-Asserted-Id: Major Clanger <sip:mclanger@blueplanet.com>
P-Charging-Vector: icid-value=”123456”
Require: precondition, 100rel
Content-Type: application/sdp
Content-Length: XX
```

INVITE from S-CSC to Application Server Foo.

```
INVITE sip:tclanger@blueplanet.com SIP/2.0
Route: <sip: service1@foo.blueplanet.com;role=orig;lr>
Route: <sip:12345678@scs.blueplanet.com;lr>
Record-Route: <sip:mclanger@scsc.blueplanet.com;lr>
Record-Route: <sip:mclanger@pcsc.blueplanet.com;lr>
Via: SIP/2.0/UDP scsc.blueplanet.com;branch=z9hG4bK77ef4c7765432
Via: SIP/2.0/UDP pcsc.blueplanet.com;branch=z9hG4bK77ef4c2312983.1
Via: SIP/2.0/UDP 89.0.224.34;branch=z9hG4bKnashds8;received=147.29.80.136
Max-Forwards: 68
To: Tiny Clanger <sip:tclanger@blueplanet.com>
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Supported: 100rel, timer, precondition
Session-Expires: 180; refreshor=uac
Min-SE: 120
Allow: INVITE, ACK, CANCEL, BYE, PRACK, REFER, UPDATE
Contact: <sip:sessionxx@pcsc.blueplanet.com>
P-Asserted-Id: Major Clanger <sip:mclanger@blueplanet.com>
P-Charging-Vector: icid-value=”123456”
Require: precondition, 100rel
Content-Type: application/sdp
Content-Length: XX
```

Propagated INVITE from Application Server Foo (a B2BUA) to S-CSC

```
INVITE sip:tclanger@blueplanet.com SIP/2.0
Route: <sip:12345678@scsc.blueplanet.com;lr>
Record-Route: <sip:session1234@foo.blueplanet.com;lr>
Via: SIP/2.0/UDP foo.blueplanet.com;branch=z9hG4bK77ef4c6534262
Max-Forwards: 67
To: Tiny Clanger <sip:tclanger@blueplanet.com>
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301774
Call-ID: fb123e45d3
CSeq: 1 INVITE
Supported: 100rel, timer, precondition
Session-Expires: 180; refreshor=uac
Min-SE: 120
Allow: INVITE, ACK, CANCEL, BYE, PRACK, REFER, UPDATE
Contact: <sip:sessionxx@pcsc.blueplanet.com>
P-Asserted-Id: Major Clanger <sip:mclanger@blueplanet.com>
P-Charging-Vector: icid-value=”123456”
Require: precondition, 100rel
Content-Type: application/sdp
Content-Length: XX
```

B.3 Application Invocation via SB/SCIM

Tiny Clanger is registered to the same S-CSC instance, Tiny Clangers service profile includes a SCIM for a terminating INVITE which in turn will engage application servers bar (acting as a proxy) and baz (acting as a B2BUA).

INVITE from S-CSC to SCIM

```
INVITE sip:tclanger@blueplanet.com SIP/2.0
Route: <sip: sb@scim.blueplanet.com;role=term;lr>
Route: <sip:12345679@scsc.blueplanet.com;lr>
Record-Route: <sip:tclanger1@scsc.blueplanet.com;lr>
Record-Route: <sip:session1234@foo.blueplanet.com;lr>
Via: SIP/2.0/UDP foo.blueplanet.com;branch=z9hG4bK77ef4c6534262
Via: SIP/2.0/USP scsc.blueplanet.com;branch=z9hG4bK7ef4c1234567
Max-Forwards: 66
To: Tiny Clanger <sip:tclanger@blueplanet.com>
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301774
Call-ID: fb123e45d3
CSeq: 1 INVITE
Supported: 100rel, timer, precondition
Session-Expires: 180; refreshor=uac
Min-SE: 120
Allow: INVITE, ACK, CANCEL, BYE, PRACK, REFER, UPDATE
Contact: <sip:sessionxx@pcsc.blueplanet.com>
P-Asserted-Id: Major Clanger <sip:mclanger@blueplanet.com>
P-Charging-Vector: icid-value=”123456”
Require: precondition, 100rel
Content-Type: application/sdp
Content-Length: XX
```

INVITE from SCIM to Application Server Bar

```
INVITE sip:tclanger@blueplanet.com SIP/2.0
Route: <sip: service1@bar.blueplanet.com;role=term;lr>
Route: <sip:2233445566@scim.blueplanet.com;lr>
Record-Route: <sip:sessionabcd@scim.blueplanet.com;lr>
Via: SIP/2.0/USP scim.blueplanet.com;branch=z9hG4bK7ef4c23456
Max-Forwards: 64
To: Tiny Clanger <sip:tclanger@blueplanet.com>
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301774
Call-ID: ef4567ef
CSeq: 1 INVITE
Supported: 100rel, timer, precondition
Session-Expires: 180; refreshor=uac
Min-SE: 120
Request-Disposition no-fork
Allow: INVITE, ACK, CANCEL, BYE, PRACK, REFER, UPDATE
Contact: <sip:mclanger@pcsc.blueplanet.com>
P-Asserted-Id: Major Clanger <sip:mclanger@blueplanet.com>
P-Charging-Vector: icid-value=”123456”
Require: precondition, 100rel
Content-Type: application/sdp
Content-Length: XX
```

Propagated INVITE from Application Server Bar to SCIM

```
INVITE sip:tclanger@blueplanet.com SIP/2.0
Route: <sip:2233445566@scim.blueplanet.com;lr>
Record-Route: <sip:session9999@bar.blueplaner.com;lr>
Record-Route: <sip:sessionabcd@scim.blueplanet.com;lr>
Via: SIP/2.0/USP bar.blueplanet.com;branch=z9hG4bK7ef4c23986
Via: SIP/2.0/USP scim.blueplanet.com;branch=z9hG4bK7ef4c23456
Max-Forwards: 63
To: Tiny Clanger <sip:tclanger@blueplanet.com>
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301774
Call-ID: ef4567ef
CSeq: 1 INVITE
Supported: 100rel, timer, precondition
Session-Expires: 180; refreshor=uac
Min-SE: 120
Request-Disposition no-fork
Allow: INVITE, ACK, CANCEL, BYE, PRACK, REFER, UPDATE
Contact: <sip:sessionxx@pcsc.blueplanet.com>
P-Asserted-Id: Major Clanger <sip:mclanger@blueplanet.com>
P-Charging-Vector: icid-value=”123456”
Require: precondition, 100rel
Content-Type: application/sdp
Content-Length: XX
```

INVITE from SCIM to Application Server Baz

```
INVITE sip:tclanger@blueplanet.com SIP/2.0
Route: <sip: service1@baz.blueplanet.com;role=term;lr>
Route: <sip:2233445567@scim.blueplanet.com;lr>
Record-Route: <sip:sessionabce@scim.blueplanet.com;lr>
Via: SIP/2.0/USP scim.blueplanet.com;branch=z9hG4bK7ef4c23456
Max-Forwards: 62
To: Tiny Clanger <sip:tclanger@blueplanet.com>
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301774
Call-ID: ef4569da
CSeq: 1 INVITE
Supported: 100rel, timer, precondition
Session-Expires: 180; refreshor=uac
Min-SE: 120
Allow: INVITE, ACK, CANCEL, BYE, PRACK, REFER, UPDATE
Contact: <sip:sessionxxx@pcsc.blueplanet.com>
P-Asserted-Id: Major Clanger <sip:mclanger@blueplanet.com>
P-Charging-Vector: icid-value=”123456”
Require: precondition, 100rel
Content-Type: application/sdp
Content-Length: XX
```

Propagated INVITE from Application Server Baz to SCIM

```
INVITE sip:tclanger@blueplanet.com SIP/2.0
Route: <sip:2233445567@scim.blueplanet.com;lr>
Record-Route: <sip:session8888@baz.blueplaner.com;lr>
Via: SIP/2.0/USP baz.blueplanet.com;branch=z9hG4bK7ef4c23976
Max-Forwards: 61
To: Tiny Clanger <sip:tclanger@blueplanet.com>
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301774
Call-ID: dfdfac23456
CSeq: 1 INVITE
Supported: 100rel, timer, precondition
Session-Expires: 180; refreshor=uac
Min-SE: 120
```

```
Allow: INVITE, ACK, CANCEL, BYE, PRACK, REFER, UPDATE
Contact: <sip:sessionxx@pcsc.blueplanet.com>
P-Asserted-Id: Major Clanger <sip:mclanger@blueplanet.com>
P-Charging-Vector: icid-value=”123456”
Require: precondition, 100rel
Content-Type: application/sdp
Content-Length: XX
```

INVITE from SCIM back to S-CSC

```
INVITE sip:tclanger@blueplanet.com SIP/2.0
Route: <sip:12345679@scsc.blueplanet.com;lr>
Record-Route: <sip:session9999@scim.blueplanet.com;lr>
Via: SIP/2.0/UDP scim.blueplanet.com;branch=z9hG4bK77ef4c6533527
Max-Forwards: 60
To: Tiny Clanger <sip:tclanger@blueplanet.com>
From: Major Clanger <sip:mclanger@blueplanet.com>;tag=1928301774
Call-ID: ef4593dc
CSeq: 1 INVITE
Supported: 100rel, timer, precondition
Session-Expires: 180; refreshor=uac
Min-SE: 120
Allow: INVITE, ACK, CANCEL, BYE, PRACK, REFER, UPDATE
Contact: <sip:sessionxx@pcsc.blueplanet.com>
P-Asserted-Id: Major Clanger <sip:mclanger@blueplanet.com>
P-Charging-Vector: icid-value=”123456”
Require: precondition, 100rel
Content-Type: application/sdp
Content-Length: XX
```