

# ETSI TS 123 218 V12.3.0 (2014-10)



**Digital cellular telecommunications system (Phase 2+);  
Universal Mobile Telecommunications System (UMTS);  
LTE;  
IP Multimedia (IM) session handling;  
IM call model;  
Stage 2  
(3GPP TS 23.218 version 12.3.0 Release 12)**



---

**Reference**

RTS/TSGC-0123218vc30

---

**Keywords**

GSM,LTE,UMTS

**ETSI**

---

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**

The present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

[http://portal.etsi.org/chaicor/ETSI\\_support.asp](http://portal.etsi.org/chaicor/ETSI_support.asp)

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2014.

All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

---

## Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

---

## Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Contents

Intellectual Property Rights .....	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	6
1 Scope .....	7
2 References .....	7
3 Definitions and abbreviations.....	8
3.1 Definitions .....	8
3.2 Abbreviations .....	9
4 Architecture and information flows for IM multimedia session .....	11
4.0 Introduction .....	11
4.1 Architecture for a UE-originating IP multimedia session .....	11
4.2 Architecture for a UE-terminating IP multimedia session.....	11
4.3 Void.....	12
4.4 Void.....	12
4.5 Void.....	12
5 Functional requirements of network entities .....	12
5.1 Architecture for service provision for IP multimedia subsystem .....	12
5.1.1 General.....	12
5.1.2 Provision of media resources .....	13
5.1.2A Border control concepts for the ISC interface.....	13
5.1.3 Border control concepts for other interfaces.....	14
5.1A IMS communication service identifier (ICSI) .....	15
5.1B IMS Application Reference Identifier (IARI) .....	16
5.2 Service interaction with IP multimedia subsystem.....	16
5.2.1 Service Point Triggers (SPTs) .....	16
5.2.2 Filter Criteria .....	16
5.2.3 S-CSCF Filter Criteria processing .....	17
5.2.4 Transit Invocation Criteria.....	18
5.2.5 Transit Function Transit Invocation Criteria processing.....	18
6 Functional requirements of serving CSCF and Transit Function .....	20
6.1 Modes of operation of the S-CSCF and Transit Function .....	20
6.1.1 General overview of functional models and modes of operation of the S-CSCF .....	20
6.1.2 General overview of functional models and modes of operation of the Transit Function .....	21
6.2 Interfaces defined for S-CSCF and Transit Function .....	22
6.2.1 S-CSCF – CSCF (Mw) interface .....	22
6.2.2 S-CSCF – Application Server (ISC) interface .....	22
6.2.3 S-CSCF – HSS (Cx) interface.....	22
6.2.4 S-CSCF – MRB (ISC) interface .....	22
6.2.5 S-CSCF – MRF (Mr) interface .....	22
6.2.6 Transit Function – Application Server (ISC) interface .....	22
6.3 S-CSCF handling of SIP registration .....	22
6.4 S-CSCF handling of UE-originating requests .....	23
6.4.1 S-CSCF handling of UE-originating requests, registered user .....	23
6.4.2 S-CSCF handling of UE-originating requests, unregistered user.....	24
6.5 S-CSCF handling of UE-terminating requests .....	25
6.5.1 S-CSCF handling of UE-terminating requests, registered user.....	25
6.5.2 S-CSCF handling of UE-terminating requests, unregistered user.....	26
6.5A Transit Function handling of requests .....	27
6.5A.1 Transit Function handling of initial requests and standalone requests.....	27
6.6 S-CSCF and Transit Function handling of IP multimedia session release requests .....	28

6.6.0	Introduction.....	28
6.6.1	S-CSCF and Transit Function proxying release request .....	28
6.6.2	S-CSCF and Transit Function initiating release request .....	28
6.7	S-CSCF handling of subscription and notification .....	29
6.8	S-CSCF handling IMS charging.....	29
6.8A	Transit Function handling IMS charging.....	30
6.9	S-CSCF description of subscriber data.....	31
6.9.1	Application Server subscription information .....	31
6.9.2	Filter Criteria .....	31
6.9.2.0	Introduction.....	31
6.9.2.1	Application Server address .....	31
6.9.2.2	Default handling.....	31
6.9.2.3	Trigger point .....	31
6.9.2.4	iFC Priority .....	31
6.9.2.5	Service Information.....	31
6.9.2.6	Include Register Request.....	32
6.9.2.7	Include Register Response .....	32
6.9.3	Authentication data .....	32
7	Functional requirements of HSS .....	32
7.1	Subscriber data related storage requirements for HSS .....	32
7.2	Interfaces defined for HSS .....	32
7.2.1	HSS – CSCF (Cx) interface .....	32
7.2.2	HSS - Application Server (Sh) interface.....	33
7.2.3	HSS – CSE interface.....	33
7.2.4	HSS – IM-SSF Application Server interface .....	33
7.3	Procedures during IP multimedia registration .....	33
7.4	Procedures during IP multimedia sessions .....	33
8	Functional requirements of the MRFC.....	33
8.1	Functionality of the MRFC .....	33
8.1.1	Overview of MRFC Functionality .....	33
8.1.2	Tones and announcements .....	34
8.1.3	Ad-hoc conferences (multiparty calls).....	34
8.1.4	Transcoding .....	35
8.2	Interfaces defined for MRFC.....	35
8.2.1	MRFC – S-CSCF (Mr) interface.....	35
8.2.2	Application Server – MRFC (Cr) interface.....	35
8.2.3	Application Server – MRFC (Mr') interface .....	36
8.2.4	MRB – MRFC (Mr') interface .....	36
8.2.5	MRB – MRFC (Cr) interface.....	36
9	Generic IP multimedia session handling for SIP Application Servers.....	37
9.1	Architecture .....	37
9.1.0	Introduction.....	37
9.1.1	Modes of operation between Application Server and S-CSCF.....	38
9.1.1.0	Introduction.....	38
9.1.1.1	Application Server acting as terminating UA, or redirect server .....	38
9.1.1.2	Application Server acting as originating UA .....	39
9.1.1.3	Application Server acting as a SIP proxy.....	39
9.1.1.4	Application Server performing third party call control/ B2BUA mode .....	39
9.1.1.5	Application Server not involved or no longer involved .....	41
9.1.2	Modes of operation between Application Server and Transit Function.....	41
9.2	Interfaces defined for a SIP Application Server .....	41
9.2.1	S-CSCF – Application Server (ISC) interface .....	41
9.2.2	Application Server – HSS (Sh) interface .....	41
9.2.3	Application Server – SLF (Dh) interface .....	41
9.2.4	Application Server – MRFC (Cr) interface.....	41
9.2.5	Application Server – MRB interface (Rc) .....	41
9.2.6	Transit Function – Application Server (ISC) interface .....	42
9.3	Description of Application Server related subscriber data .....	42
9.3.1	Application server subscription information.....	42
9.3.1.0	Introduction.....	42

9.3.1.1	Service key .....	42
9.3.1.2	Service platform trigger points (STP) .....	42
9.3.1.3	Service scripts .....	42
9.4	Procedures for multimedia session handling with a SIP based Application Server .....	42
9.4.1	Application Server handling of UE-originating requests .....	42
9.4.2	Application Server handling of UE-terminating requests .....	43
9.4.3	Application Server handling of SIP registration .....	43
9.4.4	Application Server handling of IP multimedia session release requests .....	43
9.4.4.1	Session release request terminated at the Application Server .....	43
9.4.4.2	Session release request proxied by the Application Server .....	44
9.4.4.3	Session release request initiated by the Application Server .....	44
9.4.5	Application server handling of IP multimedia charging .....	45
10	IP multimedia session handling with IM-SSF Application Server .....	45
11	IP multimedia session handling with an OSA-Service Capability Server .....	45
12.	IP multimedia session handling with an Charging Server .....	45
13	Media resource broker (MRB) .....	46
13.0	General .....	46
13.1	MRB Query Mode .....	47
13.2	MRB In-Line Mode .....	48
13.3	MRB knowledge of MRF resources and other information .....	48
<b>Annex A (informative):</b>	<b>Scalability and deployment considerations for IP multimedia service provision .....</b>	<b>49</b>
<b>Annex B (informative):</b>	<b>Information flows for example services .....</b>	<b>51</b>
B.1	Call forwarding example .....	51
B.1.1	Call forwarding through Application Servers .....	51
B.1.1.0	Introduction .....	51
B.1.1.1	Service activation and programming .....	52
B.1.1.2	Service invocation and control .....	52
B.1.2	Assumptions .....	53
B.1.3	UE redirect based call flows .....	53
B.1.4	S-CSCF based redirect call flows .....	54
B.2	Announcement, conferencing and transcoding examples using MRFC .....	56
B.2.1	Example information flow for a UE-originating IP multimedia session that results in playing an announcement .....	56
B.2.2	Example information flow for a UE-originating IP multimedia ad-hoc conferencing session (multiparty call) .....	58
B.2.3	Example information flows for a UE-originating IP multimedia session that requires transcoding .....	60
B.3	Example information flows for a voicemail service .....	64
B.3.1	User out of coverage message recording .....	64
B.3.2	User IMS registers voice mail service plays back messages .....	66
<b>Annex C (informative):</b>	<b>Example for Initial filter criteria triggering .....</b>	<b>69</b>
<b>Annex D (informative):</b>	<b>Change history .....</b>	<b>71</b>
History .....		74

---

# Foreword

This Technical Specification has been produced by the 3<sup>rd</sup> Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

---

# 1 Scope

The present document specifies the IP Multimedia (IM) Call Model for handling of an IP multimedia session origination and termination for an IP Multimedia subscriber.

The present document includes interactions between an Application Server and IP multimedia sessions.

The IP Multimedia (IM) Subsystem stage 2 is specified in 3GPP TS 23.228 [3].

---

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] Void.
- [2] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [3] 3GPP TS 23.228: " IP multimedia subsystem; Stage 2".
- [4] Void.
- [5] 3GPP TS 24.229: "IP multimedia call control protocol based on SIP and SDP; stage 3".
- [6] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [7] 3GPP TR 29.998-4-4 Release 8: "Open Service Access (OSA); Application Programming Interface (API) Mapping for Open Service Access (OSA); Part 4: Call Control Service Mapping; Subpart 4: Multiparty Call Control SIP".
- [8] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx Interface; Signalling flows and message contents".
- [9] 3GPP TS 23.278: "Customised Applications for Mobile network Enhanced Logic (CAMEL); IP Multimedia System (IMS) interworking; Stage 2".
- [10] 3GPP TS 23.008: "Organisation of subscriber data".
- [11] 3GPP TS 33.203: "Access security for IP based services".
- [12] 3GPP TS 29.198: "Open Service Access (OSA); Application programming Interface (API)".
- [13] Void.
- [14] 3GPP TS 29.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3; CAMEL Application Part (CAP) specification".
- [15] IETF RFC 3264: "An Offer/Answer Model with Session Description Protocol".
- [16] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".
- [17] 3GPP TS 29.229: "Cx Interface based on the Diameter protocol".



- [18] 3GPP TS 29.328: "IP Multimedia Subsystem (IMS) Sh Interface; Signalling flows and message contents".
- [19] 3GPP TS 29.329: "Sh Interface based on the Diameter protocol".
- [20] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".
- [21] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".
- [22] IETF RFC 5627 (October 2009): "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)".
- [23] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".
- [24] 3GPP TS 24.247: "Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".
- [25] 3GPP TS 33.328: "IMS Media Plane Security".
- [26] 3GPP TS 29.364: "IP Multimedia Subsystem (IMS) Application Server (AS) service data descriptions for AS interoperability".

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [2] and the following apply:

**Application Server Incoming Leg Control Model (AS-ILCM):** models AS behaviour for handling SIP information for an incoming leg.

**Application Server information (AS-info):** AS-info contains individualized information concerning one particular Application Server entry.

This information contains e.g. Application Server Address (6.9.1.1) and its corresponding Default IP Multimedia Handling information (6.9.1.2).

**Application Server Outgoing Leg Control Model (AS-OLCM):** models AS behaviour for handling SIP information for an outgoing leg.

**Combined ILSM OLSM – Incoming/outgoing Leg State Model:** models the behaviour of an S-CSCF for handling SIP messages on an incoming and outgoing session leg.

**Filter Criteria (FC):** the information which the S-CSCF receives from the HSS or the AS that defines the relevant SPTs for a particular application.

They define the subset of SIP requests received by the S-CSCF that should be sent or proxied to a particular application.

**Incoming Leg Control Model (ILCM):** models the behaviour of an S-CSCF for handling SIP information sent to and received from an AS for an incoming session leg.

**Initial Filter Criteria (iFC):** filter criteria that are stored in the HSS as part of the user profile and are downloaded to the S-CSCF upon user registration.

They represent a provisioned subscription of a user to an application.

**Initial Request:** a SIP request that either initiates the creation of a new dialog or is part of a standalone transaction.

**IP Multimedia Service Switching Function (IM-SSF):** functional entity that interfaces SIP to CAP.

**IP Multimedia CAMEL Subscription Information (IM-CSI):** identifies the subscriber as having IP Multimedia CAMEL services.

**IP Multimedia session:** IP Multimedia session and IP Multimedia call are treated as equivalent in the present document.

**Original Dialog Identifier:** an indication that the S-CSCF includes in a Route header for itself when sending requests to an AS. When the AS returns this indication in a Route header of a message sent to the S-CSCF, the S-CSCF uses it to associate the message with the previous request sent by the S-CSCF (i.e. the original SIP dialog).

**Originating IP Multimedia CAMEL Subscription Information (O-IM-CSI):** identifies the subscriber as having originating IP Multimedia CAMEL services.

**Outgoing Leg Control Model (OLCM):** models the behaviour of an S-CSCF for handling SIP information received from and sent to an AS for an outgoing session leg.

**Private User Identity:** a unique global identity defined by the Home Network Operator, as defined in 3GPP TS 23.228 [3].

**Public User Identity:** the public user identity/identities are used by any user for requesting communications to other users and are in the form of a SIP URL or TEL URL as defined in 3GPP TS 23.228 [3].

**Served User:** The served user is the public user identity, for which the IM CN subsystem handles the call. For an origination call leg the served user is the user for which a UE or AS originates the call for. For a terminating call leg the served user is the user for which a UE or an AS terminates the call for.

**Service Key:** the Service Key identifies to the Application Server the service logic that shall apply. The Service Key is administered by the HPLMN. For CAMEL services, the Service Key is an element of the CAMEL Subscription Information (CSI).

**Service Point Trigger (SPT):** the points in the SIP signalling that may cause the S-CSCF to send/proxy the SIP message to an SIP AS/OSA SCS/IM-SSF.  
The subset of all possible SPTs which are relevant to a particular application are defined by means of Filter Criteria.

**Service Platform Trigger Points (STP):** the points in the SIP signalling that instruct the SIP AS, OSA SCS and IM-SSF to trigger the service logic.  
For the IM-SSF the IP Multimedia Camel Subscriber Information (IM-CSI) defines them.

**Subsequent Filter Criteria (sFC):** filter criteria that are signalled from the SIP AS/OSA SCS/IM-SSF to the S-CSCF. They allow for dynamic definition of the relevant SPTs at application execution time.

**Subsequent Request:** a SIP request which is part of an existing dialog. This also includes target refresh requests as defined in IETF RFC 3261 [6].

**Standalone Transaction:** a SIP transaction that is not part of an existing dialog and does not initiate the creation of a new dialog.

**Terminating IP Multimedia CAMEL Subscription Information (T-IM-CSI):** identifies the subscriber as having terminating IP Multimedia CAMEL services.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclause 4.13 apply:

**IMS application reference**  
**IMS communication service**  
**IMS communication service identifier**

## 3.2 Abbreviations

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

AAA	Authentication, Authorization, and Accounting
API	Application Programming Interface
AS	Application Server
AS-ILCM	Application Server Incoming Leg Control Model
AS-OLCM	Application Server Outgoing Leg Control Model

B2BUA	Back-to-Back User Agent
CAMEL	Customized Applications for Mobile network Enhanced Logic
CAP	CAMEL Application Part
CCF	Charging Collection Function
CDR	Charging Data Records
CF	Call Forwarding
CFonCLI	Call Forwarding on Calling Line Identification
CGI	Common Gateway Interface
CPL	Call Processing Language
CLI	Calling Line Identification
CSCF	Call Session Control Function
CSE	CAMEL Service Environment
ECF	Event Charging Function
FC	Filter Criteria
GPRS	General Packet Radio Service
GPRS CID	GPRS Charging Identifiers
GRUU	Globally Routable User agent URI
gsmSCF	gsm Service Control Function
HPLMN	Home PLMN
HSS	Home Subscriber Server
IETF	Internet Engineering Task Force
I-CSCF	Interrogating CSCF
IARI	IMS Application Reference Identifier
ICID	IMS Charging ID
ICSI	IMS Communication Service Identifier
iFC	Initial Filter Criteria
ILCM	Incoming Leg Control Model
IM	IP Multimedia
IM-CSI	IP Multimedia CAMEL Subscription Information
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IM-SSF	IP Multimedia Service Switching Function
IOI	Inter Operator Identifier
IP	Internet Protocol
ISC	IP multimedia Service Control
MAP	Mobile Application Part
MGCF	Media Gateway Control Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
O-IM-CSI	Originating IP Multimedia CAMEL Subscription Information
ODI	Original Dialog Identifier
OLCM	Outgoing Leg Control Model
OSA	Open Service Access
PLMN	Public Land Mobile Network
P-CSCF	Proxy CSCF
RFC	Request For Comments
SCF	Session Charging Function
SCIM	Service Capability Interaction Manager
SCS	Service Capability Server
SDP	Session Description Protocol
sFC	Subsequent Filter Criteria
SIP	Session Initiation Protocol
S-CSCF	Serving CSCF
SPT	Service Point Trigger
STP	Service platform Trigger Points
T-IM-CSI	Terminating IP Multimedia CAMEL Subscription Information
UA	User Agent
UE	User Equipment
URL	Uniform Resource Locator
XML	EXtensible Markup Language
MRB	Media Resource Broker
IVR	Interactive Voice Response

---

## 4 Architecture and information flows for IM multimedia session

### 4.0 Introduction

Subclauses 4.1 and 4.2 show the architecture for handling a basic UE-originating multimedia session and a basic UE-terminating multimedia session. A basic UE-to-UE multimedia session is treated as the concatenation of a UE-originating multimedia session and a UE-terminating multimedia session.

### 4.1 Architecture for a UE-originating IP multimedia session

This is specified in 3GPP TS 23.228 [3].

### 4.2 Architecture for a UE-terminating IP multimedia session

This is specified in 3GPP TS 23.228 [3].

4.3 Void

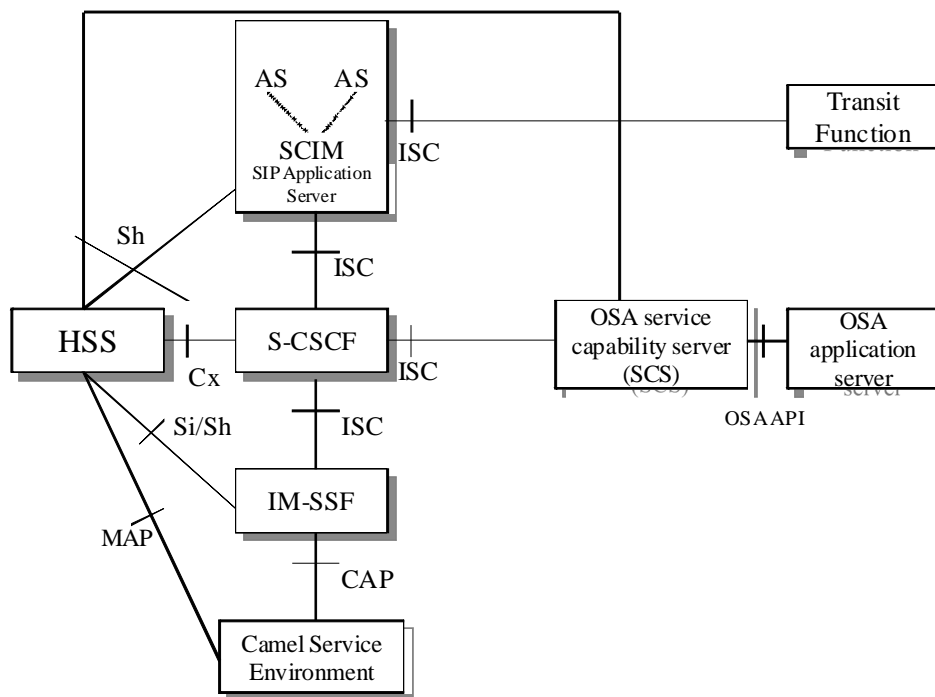
4.4 Void

4.5 Void

## 5 Functional requirements of network entities

### 5.1 Architecture for service provision for IP multimedia subsystem

#### 5.1.1 General



NOTE: Not all interfaces shown are within the scope of this document.

**Figure 5.1.1: Functional architecture for support of service provision for IP multimedia subsystem**

Figure 5.1.1 illustrates the architecture with the S-CSCF communicating to Application Servers via the IP multimedia service control (ISC) interface. The Application Servers can be:

- SIP Application Servers - which may host and execute services. It is intended to allow the SIP Application Server to influence and impact the SIP session on behalf of the services;
- the IM-SSF - which is a particular type of application server the purpose of which is to host the CAMEL network features (i.e. trigger detection points, CAMEL Service Switching Finite State Machine, etc) and to interface to CAP as specified in 3GPP TS 29.078 [14];
- the OSA service capability server (OSA SCS) which interfaces to the OSA framework Application Server and which provides a standardized way for third party secure access to the IM subsystem. The OSA reference architecture defines an OSA Application Server as an entity that provides the service logic execution

environment for client applications using the OSA API as specified in 3GPP TS 29.198 [12]. This definition of Application Server differs from the definition of Application Server in the context of service provisioning for the IM subsystem, i.e. the entity communicating to the S-CSCF via the ISC interface;

- in addition a specialized type of SIP Application Server, the service capability interaction manager (SCIM) which performs the role of interaction management between other application servers.

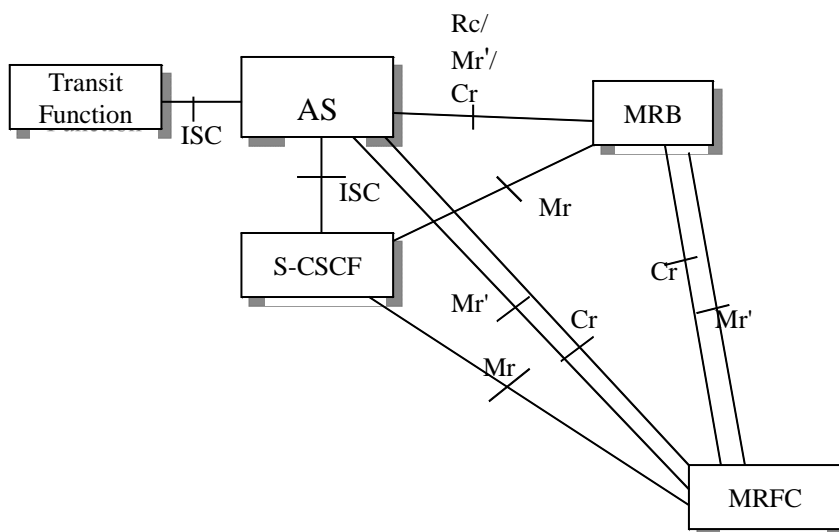
All the Application Servers, (including the IM-SSF and the OSA SCS) behave as SIP application servers on the ISC interface.

## 5.1.2 Provision of media resources

In addition the Application Servers can also interact with the MRFC via the S-CSCF (ISC, Mr), directly via the Mr' interface and via the Cr interface in order to control Multimedia Resource Function processing and can interact with the MRB (Rc interface, or Mr, and Mr' interfaces) in order for appropriate media resources to be assigned to calls (see clause 8 and clause 13). This is shown in figure 5.1.2. The AS can request MRF resources directly based on preconfigured addresses and DNS lookup, or indirectly using an MRB function, which will determine the most suitable resource (see clause 13).

An application server can provide the MRB with information to assist the MRB in determining the most appropriate resource. Aside from information on type of resource required, this can include information on other supporting MRBs in other networks, e.g. the visited network of a roaming user, or more information on the location of the endpoint to which the media is to be delivered, such that this may assist in determining the best location for providing the MRF.

NOTE: In this release direct interaction between an MRFC and a Transit Function has not been specified.



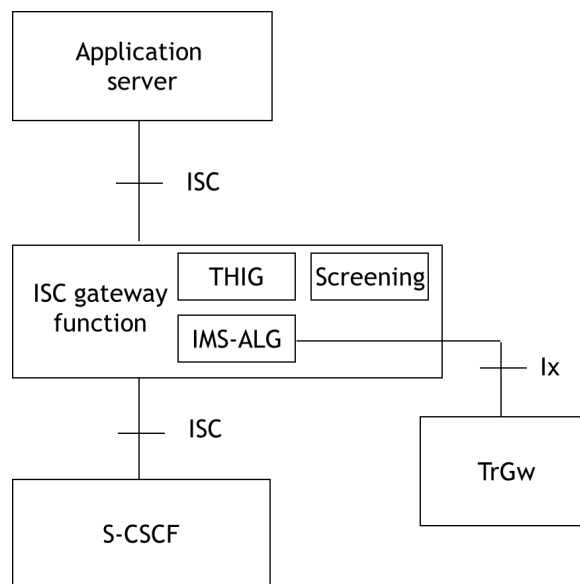
NOTE: An I-CSCF, S-CSCF can also use the resources of the MRF directly, or via an MRB, without going via an AS.

**Figure 5.1.2: Functional architecture for support of media resources for IP multimedia subsystem**

### 5.1.2A Border control concepts for the ISC interface

3GPP TS 23.228 [7] subclause 4.14 identifies the possibility of border control functions between two IM CN subsystems or between an IM CN subsystem and other SIP based multimedia network. Additional functionality may also be required on the ISC interface where an application server provided by a third-party service provider is supported.

An additional functionality called an ISC gateway function is defined as shown in figure 5.1.2A.



**Figure 5.1.2A: ISC gateway function**

The functions of the ISC gateway function are as follows:

- network configuration hiding (as for the IBCF);
- application level gateway (transcoding is not applicable for ISC gateway function);
- transport plane control, i.e. QoS control (as for the IBCF); and
- screening of SIP signalling (as for the IBCF).

NOTE 1: Additional functionality may be determined in later releases of this document. As future functionality could require knowledge of all transactions associated with an AS from the S-CSCF for a particular session / dialog, care is needed to route all such transactions through the same ISC gateway function.

While the ISC gateway function can alter the contents of the protocol on the ISC interface, the information carried should still conform to that required for the ISC interface.

NOTE 2: When this functionality is used, the effect can be to remove information that is required by subsequent AS in the filter criteria chain. Therefore care needs to be exercised both in the order in which AS appear in the filter criteria chain, and in the functionality applies in this functional entity.

NOTE 3: If the ISC gateway function modifies SIP information elements (SIP header fields, SIP message bodies) caution needs to be taken that SIP functionality (e.g. routing, iFC chain and AS application) is not impacted in a way that could create interoperability problems with networks that assume that this information is not modified.

NOTE 4: In this release the ISC gateway function does not have functionalities to save screened information in outgoing message and recover the screened information in incoming message so care is needed both in the order in which the AS appear in the filter criteria chain, and in the functionality applied in the ISC gateway.

### 5.1.3 Border control concepts for other interfaces

3GPP TS 23.228 [7] subclause 4.14 identifies the possibility of border control functions between two IM CN subsystems or between an IM CN subsystem and other SIP based multimedia network. A number of the interfaces identified in the architecture in subclause 5.1.1 and subclause 5.1.2 can be between the networks controlled by different operators, specifically the Mr, Mr' and Cr interfaces (for example between a third-party service provider and the visited network, or between the home network and the visited network).

When used on the Mr, and Mr' interfaces, the IBCF should not be used to duplicate the functions normally performed by the MRF, even if the MRF is being accessed for another unrelated function. Rather, an MRF should be used for supporting those functions.

Both the SIP control package on the Cr interface, and the Mr interface when used in in-line aware MRB mode, can contain information that an operator, for example, would prefer not to exchange with another network operator. For this information, it may be appropriate to use the MRB either in the network of the application server, or the MRB in the network where the MRF is sought, to operate in in-line aware MRB mode and to remove such information.

The IBCF is not used on the Cr interface.

In normal operation, the communication between the application server and the MRF is a communication where those functional entities form the endpoint of the communication. Therefore any information included in the signalling is deemed by one endpoint to be essential to the functionality performed by the other. As such, configuration hiding, screening and privacy functions are not expected to be critical functions on any of these interfaces.

If the network is supporting optimisation of media paths, then the IBCF could well be required on the Mr and Mr' interfaces to support optimal media routing.

For the Mr and Mr' interfaces, the IBCF may be used to support communication between the AS and the MRB, between the AS and the MRFC, between the S-CSCF and the MRB, between the S-CSCF and the MRFC.

Where this occurs, requests to the IBCF are sent over the Mx interface and requests from the IBCF are sent over the Mm interface (see subclause I.2 of 3GPP TS 23.228 [7]). Two IBCFs on either side of an interoperator boundary use the Ici interface (see subclause K.2 of 3GPP TS 23.228 [7]).

The IBCF providing IMS-ALG functions would be supported by TrGW functions using the Ix interface (see subclause I.2 of 3GPP TS 23.228 [7]), so the media from an MRFP may pass through the Izi interface where two TrGWs exist on either side of an interoperator boundary.

For the Rc interface, border control functionality can exist, but the mechanism are not specified. The IBCF is not used. Many techniques exist and are deployed for supporting border functions in HTTP, and any of these can be used on the Rc interface if they meet the needs of the deployer.

**NOTE:** For the Rc interface, the server can be decomposed into a front end https proxy and a back end MRB. The MRB will need to be available both to internal and external clients in different address spaces and with different security requirements. This could be done with a single server but then there will be two interfaces to it (internal and external) rather than one.

## 5.1A IMS communication service identifier (ICSI)

The purpose of identifying IMS communication services is to help triggering to application servers and internal routing in UEs. See 3GPP TS 23.228 [7] for further information on IMS communication services. This clause describes the IMS communication service concept principles.

An initial request for a dialog or a standalone transaction that is used for an IMS communication service can contain an identifier that identifies the IMS communication service related to this request or stand alone transaction. The identifiers for the IMS communication service are included by the originating UE in the initial request for a dialog or standalone transaction but these are unauthenticated. The initial request for a dialog or standalone transaction can also contain identifiers for the IMS communication services supported by the originating UE. The response to an initial request for a dialog or standalone transaction can contain identifiers for the IMS communication services that the responding UE supports. These identifiers are ICSI values. An ICSI value can be used as an SPT by iFC to route the initial requests for a dialog to AS that implement service logic as part of the IMS communication service provided it is first authenticated by the S-CSCF as a subscribed service for that user and that the contents of the request (SDP Media Types etc) are compatible with the IMS communication service identified by the ICSI value. An authenticated ICSI value can be included by the S-CSCF by analyzing the contents of the request (SIP header fields, SDP Media Types etc). The Authenticated ICSI value acts as a summary of the contents of a request. Care should be taken when designing services that for a given subscriber in a given network, the contents of any request (SIP header fields, SDP Media Types etc) correspond to zero or one ICSI so that the network can include the correct Authenticated ICSI value in the request. The ICSI value can be sent to ASes. An AS that is part of the trust domain can include an authenticated ICSI value and an AS that is outside the trust domain can include an unauthenticated ICSI value.



## 5.1B IMS Application Reference Identifier (IARI)

The IARI value identifies the application to be invoked by the terminating UE. When no IARI value is present in a request, the default application is assumed.

## 5.2 Service interaction with IP multimedia subsystem

### 5.2.1 Service Point Triggers (SPTs)

Service Point Triggers (SPTs) are those points in the SIP signalling on which Filter Criteria can be set. The following SPTs are defined:

- any initial known or unknown SIP method;
- registration type – indicates if the REGISTER request is initial registration, re-registration, or de-registration;
- presence or absence of any known or unknown header field;
- content of any known or unknown header field or of the Request-URI;

NOTE 1: The presence of a "gruu" parameter in the Request-URI as defined in IETF RFC 5627 [22] indicates that the request is targeted towards a GRUU. Requests targeted towards GRUUs can need different service logic handling to those targeted towards a public user identity. e.g a request targeted towards a GRUU normally would not be routed to voicemail.

- direction of the request with respect to the served user – either UE-originating or UE-terminating to registered user; UE-terminating to unregistered user or UE-originating for unregistered user; see 3GPP TS 29.228 [8] for the details of the direction information in service point trigger;

NOTE 2: REGISTER is considered part of the UE-originating. See 3GPP TS 24.229 [5] for further information about how to determine UE-originating or UE-terminating.

NOTE 3: The S-CSCF shall verify if the end user is barred before checking if any trigger applies for that end user.

- session description information.

### 5.2.2 Filter Criteria

A Filter Criteria triggers one or more SPTs in order to send the related request to one specific application server. The set of Filter Criteria that is stored for a service profile of a specific user is called "Application Server Subscription Information". In order to allow the S-CSCF to handle the different Filter Criteria in the right sequence, a priority shall be assigned to each of them. If the S-CSCF can not reach the specified Application Server, the S-CSCF shall apply the default handling associated with the trigger. This default handling shall be :

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

Therefore a Filter Criteria shall contain the following information:

- address of the Application Server to be contacted;
- priority of the Filter Criteria providing the sequence in which the criteria shall be applied;
- Trigger Point composed by 1 to n instances of the Service Point Triggers (SPTs). The SPTs may be linked by means of logical expressions (AND, OR, NOT, etc.);
- default handling ( as described above);
- optional Service Information that shall be added to the message body before it is sent to the Application Server (as an example this may include the IMSI for the IM-SSF).
- optionally an indication to include the incoming REGISTER request in the third party REGISTER request.

- optionally an indication to include the final response to the incoming REGISTER request in the third party REGISTER request.

The same priority shall not be assigned to more than one initial Filter Criteria for a given served user.

### 5.2.3 S-CSCF Filter Criteria processing

The S-CSCF shall request from the HSS the relevant set of iFCs that applies to the served user (i.e., registered, unregistered, or both). If the S-CSCF has a set of iFCs that is deemed valid (e.g., from a previous request), the S-CSCF need not request a new set.

In the case that multiple Filter Criteria are sent from the HSS to the S-CSCF, the S-CSCF shall check the filter criteria one by one according to their indicated priority when the S-CSCF receives a message via the Mw interface.

On reception of a REGISTER request, the S-CSCF shall send a third-party REGISTER request to each Application Server that matches the Filter Criteria sent from the HSS for the REGISTER request. The S-CSCF shall include in the third-party REGISTER request the incoming REGISTER request if indicated by the Filter Criteria. The S-CSCF shall include in the third-party REGISTER request the final response to the incoming REGISTER request if indicated by the Filter Criteria.

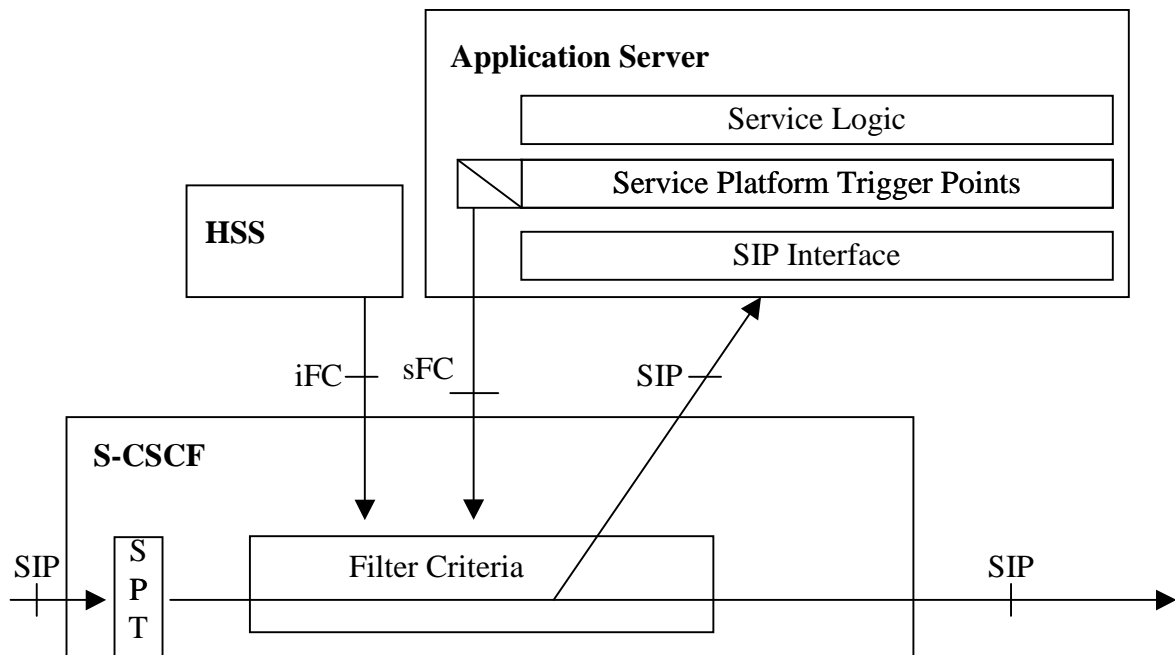
On an event that causes network-initiated deregistration, the S-CSCF shall send a third-party REGISTER request to each Application Server that matches the Filter Criteria sent from the HSS as if a equivalent REGISTER request had been received from the user deregistering that public user identity, or combination of public user identities.

On reception of any other request the S-CSCF shall:

1. set up the list of filter criteria for that request according to their priority – the sequence of the filter criteria shall not be changed until the request finally leaves the S-CSCF via the Mw interface again;
2. parse the received request in order to find out the Service Point Triggers (SPTs) that are included in it;
3. check whether the trigger points of the filter criteria with the next highest priority are matched by the SPTs of the request and
  - a) if it does not match the S-CSCF shall immediately proceed with step 4;
  - b) if it matches the S-CSCF shall:
    - i) add an Original Dialog Identifier (ODI) to the request which will allow the S-CSCF to identify the message on the incoming side, even if its dialog identification has been changed e.g. due to the Application Server performing third party call control;
    - ii) forward the request via the ISC interface to the Application Server indicated in the current filter criteria. The Application Server then performs the service logic, may modify the request and may send the request back to the S-CSCF via the ISC interface;
    - iii) proceed with step 4 if a request with the same ODI is received from the Application Server via the ISC interface;
4. repeat the above steps 2 and 3 for every filter criteria which was initially set up (in step 1) until the last filter criteria has been checked;
5. route the request based on normal SIP routing behaviour.

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

NOTE 4: If AS has service logic whereby it wishes to send a request to the S-CSCF to continue with filter criteria evaluation from where it left off with the final response to the previous request, then a new request must be sent with data that can be used by the S-CSCF to determine where it left off with filter criteria evaluation. For example, a parameter can be included in the request that is also defined in a service point trigger.



**Figure 5.2.1: Application triggering architecture**

Each invoked Application Server/service logic may decide not to be engaged with the invoked session by indicating that during the very first SIP transaction when the Record-Route/Route is generated for subsequent SIP requests. The denial shall mean that subsequent requests shall not be routed to such Application Servers/service logic any more during the lifetime of that session. Any Application Server, which has determined that it will not receive subsequent requests for a session cannot revoke this determination by means of Initial Filter Criteria (iFC).

NOTE 5: Care should be taken in design of the Initial Filter Criteria when designing services to avoid unintended loops being setup, where requests from an Application Server may be sent back to the same Application Server. This does not imply that it is not allowed for requests to be sent back to the same Application Server when that is intended behaviour as part of the design of the service and the Application Server is able to handle this correctly. Special care should be taken for the case when an Application Server may act as an originating UA or B2BUA and may originate an initial request causing evaluation of Initial Filter Criteria.

## 5.2.4 Transit Invocation Criteria

A Transit Invocation Criteria triggers one or more SPTs in order to send the related request to one specific application server. The set of Transit Invocation Criteria is not user specific, but instead is based on e.g. the originating and terminating networks.

The handling of Transit Invocation Criteria is identical to the handling of Filter Criteria, as defined in subclass 5.2.2.

NOTE: The procedures in subclass 5.2.2 associated with the handling of SIP REGISTER request do not apply to the handling of Transit Invocation Criteria.

## 5.2.5 Transit Function Transit Invocation Criteria processing

The Transit Invocation Criteria are locally configured.

In case that multiple Transit Invocation Criteria is configured, the Transit Function shall check the criteria one by one according to their indicated priority when the Transit Function receives a message.

On reception of an initial request, or a standalone request, the Transit Function shall:

1. set up the list of Transit Invocation Criteria for that request according to their priority – the sequence of the criteria shall not be changed until the request finally leaves the Transit Function towards the terminating network;

2. parse the received request in order to find out the Service Point Triggers (SPTs) that are included in it, and in priority order for each Transit Invocation Criteria:
  - a) check whether the trigger points of the Transit Invocation Criteria are matched by the SPTs of the request;
  - b) if it matches the Transit Function shall:
    - i) add an Original Dialog Identifier (ODI) to the request which will allow the Transit Function to identify the message on the incoming side, even if its dialog identification has been changed e.g. due to the Application Server performing third party call control;
    - ii) forward the request via the ISC interface to the Application Server indicated in the current filter criteria. The Application Server then performs the service logic, may modify the request and may send the request back to the Transit Function via the ISC interface;
    - iii) proceed with next Transit Invocation Criteria in a) if a request with the same ODI is received from the Application Server via the ISC interface;
  - c) if it does not match, proceed with next Transit Invocation Criteria in a) for every Transit Invocation Criteria which was initially set up (in step 1) until the last criteria has been checked;
3. route the request based on normal SIP routing behaviour.

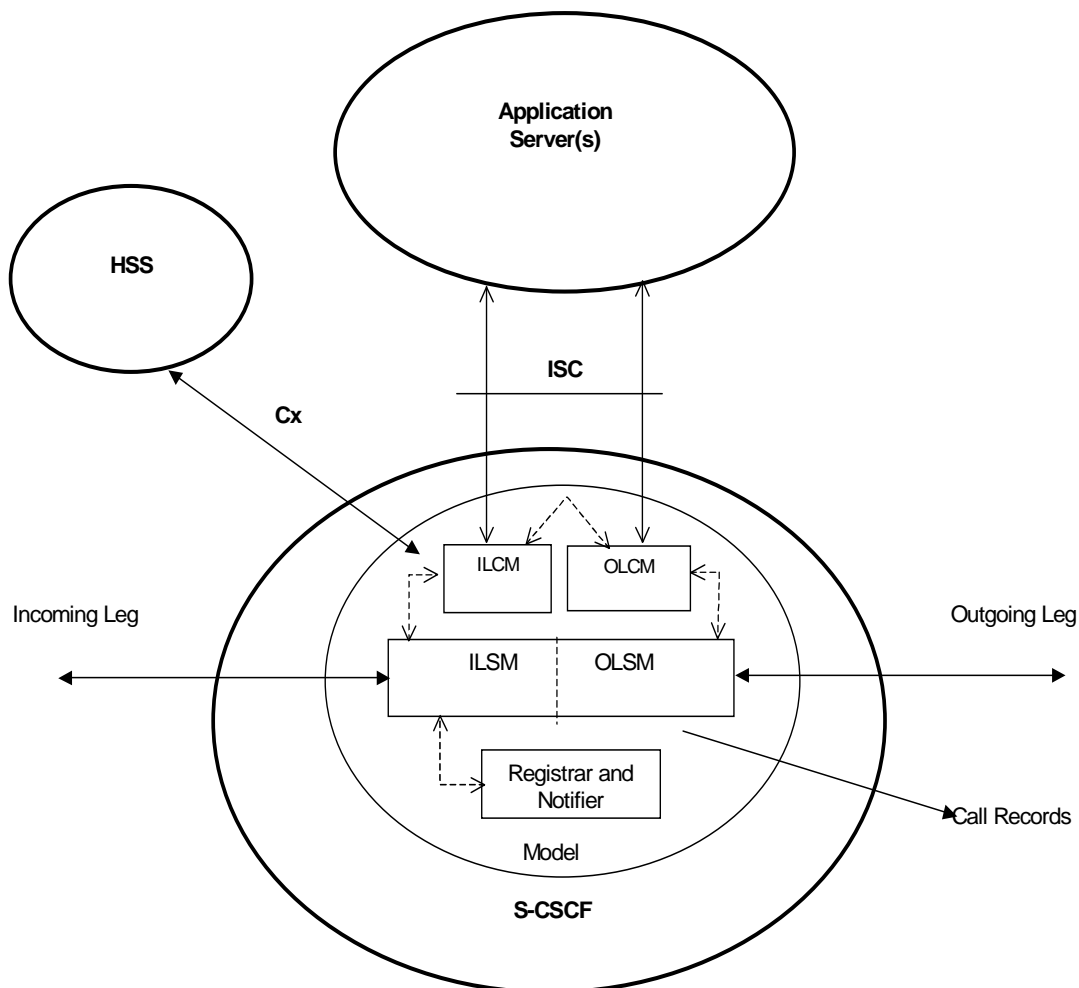
If an Application Server decides to locally terminate a request and sends back a final response for that request via the ISC interface to Transit Function, the Transit Function shall abandon verification of the matching of the triggers of lower priority in the list.

Each invoked Application Server/service logic may decide not to be engaged with the invoked session by indicating that during the very first SIP transaction when the Record-Route/Route is generated for subsequent SIP requests. The denial shall mean that subsequent requests shall not be routed to such Application Servers/service logic any more during the lifetime of that session. Any Application Server, which has determined that it will not receive subsequent requests for a session cannot revoke this determination by means of Transit Invocation Criteria.

## 6 Functional requirements of serving CSCF and Transit Function

### 6.1 Modes of operation of the S-CSCF and Transit Function

#### 6.1.1 General overview of functional models and modes of operation of the S-CSCF



**Figure 6.1.1.1: S-CSCF functional model with incoming leg control and outgoing leg control**

Figure 6.1.1.1 identifies the components of a functional model of the S-CSCF.

**NOTE:** These components are defined only as a model of the expected behaviour of the S-CSCF and are not intended to define or constrain the actual implementation.

The components include the Combined I/OLSM, the ILCM and OLCM and the Registrar and Notifier. There is a single Combined I/OLSM, which shall be able to store session state information. It may act on each leg independently, acting as a SIP Proxy, Redirect Server or User Agent dependant on the information received in the SIP request, the filter conditions specified or the state of the session.

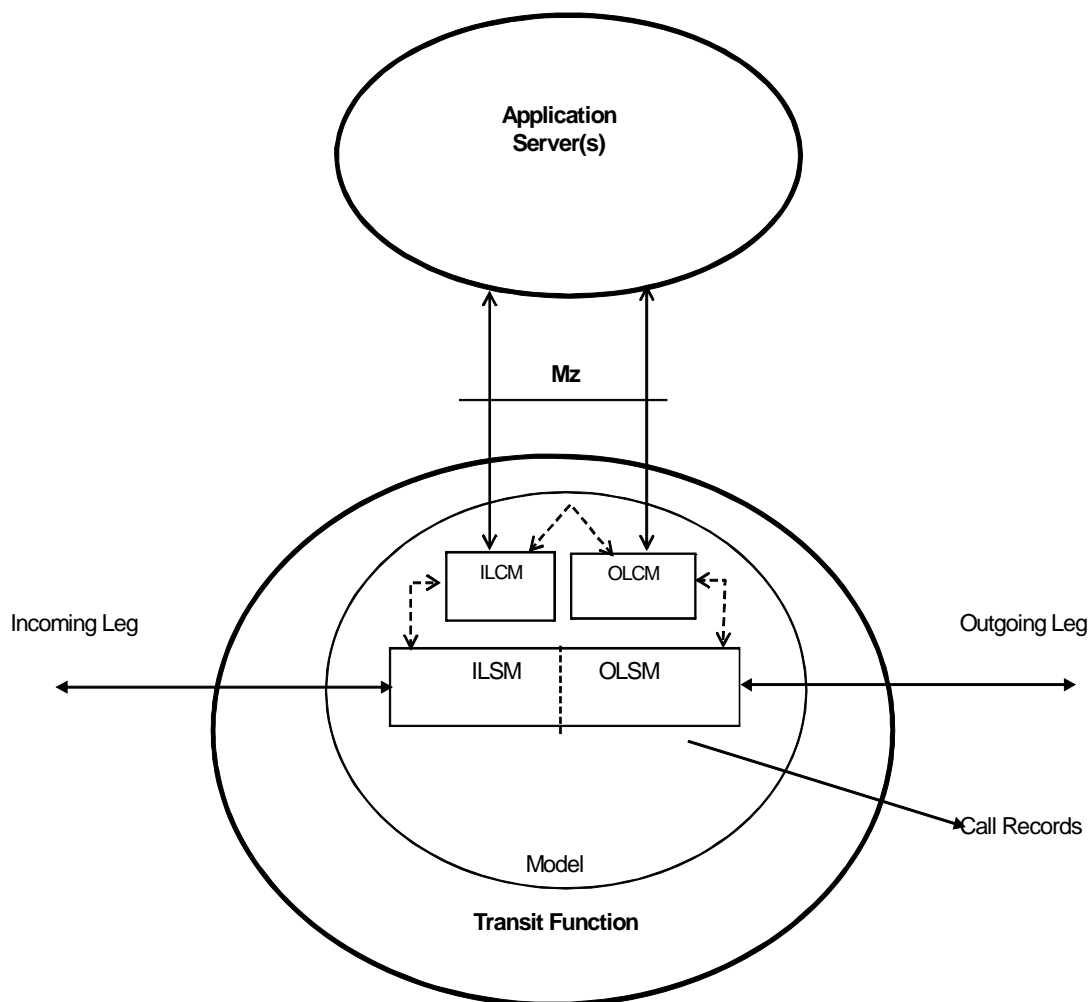
It shall be possible to split the application handling on each leg and treat each endpoint differently.

There is a single ILCM, which shall store transaction state information.

There is a single OLCM, which shall store transaction state information.

The Registrar and Notifier component handles registration and subscription to and notification of registration events.

### 6.1.2 General overview of functional models and modes of operation of the Transit Function



**Figure 6.1.2.1: Transit Function functional model with incoming leg control and outgoing leg control**

Figure 6.1.2.1 identifies the components of a functional model of the Transit Function.

**NOTE:** These components are defined only as a model of the expected behaviour of the Transit Function and are not intended to define or constrain the actual implementation.

The components include the Combined I/OLSM, the ILCM and OLCM. There is a single Combined I/OLSM, which shall be able to store session state information. It may act on each leg independently, acting as a SIP Proxy, Redirect Server or User Agent dependant on the information received in the SIP request, the invocation conditions specified or the state of the session.

It shall be possible to split the application handling on each leg and treat each endpoint differently.

There is a single ILCM, which shall store transaction state information.

There is a single OLCM, which shall store transaction state information.

## 6.2 Interfaces defined for S-CSCF and Transit Function

### 6.2.1 S-CSCF – CSCF (Mw) interface

The protocol used between two CSCFs is also based on Session Initiation Protocol, which is specified in 3GPP TS 24.229 [5].

### 6.2.2 S-CSCF – Application Server (ISC) interface

The protocol used between the S-CSCF and the Application Servers (ISC interface) is also based on Session Initiation Protocol, which is specified in 3GPP TS 24.229 [5].

### 6.2.3 S-CSCF – HSS (Cx) interface

This interface is used to send subscriber data to the S-CSCF; including Filter criteria, which indicates which SIP requests should be proxied to which Application Servers.

The protocol used between the S-CSCF and HSS (Cx Interface) is specified in 3GPP TS 29.228 [8].

### 6.2.4 S-CSCF – MRB (ISC) interface

This interface is used for an MRB operating in In-Line mode when using the capability of the S-CSCF to route to the MRB. The use of this interface is described in subclause 13.2.

### 6.2.5 S-CSCF – MRF (Mr) interface

This interface is used for an MRF when using the capability of the S-CSCF to route to the MRB. The use of this interface is described in subclause 8.2.1.

### 6.2.6 Transit Function – Application Server (ISC) interface

The protocol used between the Transit Function and the Application Servers (ISC interface) is based on Session Initiation Protocol, as defined in 3GPP TS 24.229 [5]. The interface implements the Mf reference point, as defined in 3GPP TS 23.228 [3].

## 6.3 S-CSCF handling of SIP registration

Upon receiving the initial registration request from the served user, the S-CSCF shall authenticate the served user and upon receiving a subsequent registration request containing valid authentication credentials, request the HSS to send the relevant service profile(s) for the served user's subscription. More than one service profile may be sent, depending on configuration options for identifying implicitly registered public user identities. For further detailed information on registration, profile download and authentication procedures see 3GPP TS 24.229 [5], 3GPP TS 33.203 [11], and 3GPP TS 33.328 [25].

The registration request can contain a list of ICSI values and a list of IARI values supported by the UE.

The initial filter criteria (subset of the profile) is stored locally at the S-CSCF, as specified in 3GPP TS 24.229 [5].

The S-CSCF shall verify if the triggers match, from the highest to the lowest priority (see subclause 5.2).

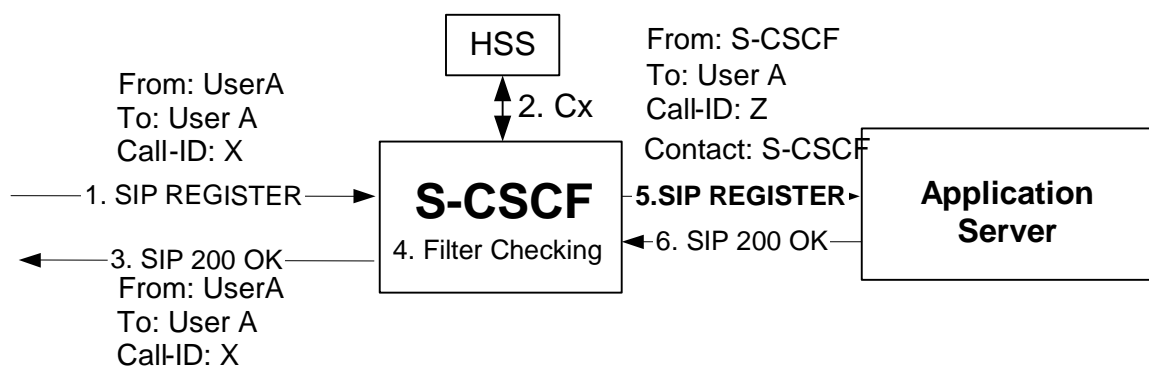
After a successfully authenticated registration, the S-CSCF shall download from the HSS all the implicitly registered public user identities associated with the registered public user identity. The S-CSCF shall then verify, in their order of priority, if the triggers downloaded from the HSS match. For each service profile in the implicit registration set, if the registration request from the served user matches a trigger, the S-CSCF performs a third party registration to the application servers which are interested to be informed about the user registration event of these public user identities. This may trigger services to be executed by an Application Server.

The important information carried in the third party REGISTER request is the public user identity of the served user, the S-CSCF address and the expiration time. It shall be possible based on operator configuration to use one of the implicitly registered public user identities as the public user identity in the To header of the third party REGISTER request sent to the Application Server. Additional application server specific data, which is associated with the Filter Criteria and obtained from the HSS, is added to the REGISTER request body. This data should include the IMSI for an Application Server that supports CAMEL services or the private user identity for other Application Servers as received from the HSS. If indicated by the Filter Criteria the incoming REGISTER request is added to the REGISTER request body. If indicated by the Filter Criteria the final response to the incoming REGISTER request is added to the REGISTER request body.

This third party registration will include an expiration time that is equal to the expiration time sent to the UE by the S-CSCF in the 200 (OK) response to the incoming REGISTER request

On receiving a failure response to one of the REGISTER requests, the S-CSCF shall apply the "default handling" related with the initial Filter Criteria's trigger used (see subclauses 5.2.2, 6.9.2.2).

See figure 6.3.1:



**Figure 6.3.1: S-CSCF handling registration**

Application Servers can in addition subscribe to the S-CSCF reg event package. This provides a mechanism for the Application Server to discover all the implicitly registered public user identities without requiring multiple Register requests to be sent to the Application Server and to obtain the current capabilities of the UE as well as be notified about refresh registrations and de-registrations. The S-CSCF will send NOTIFY requests to the Application Server that has subscribed to the reg event package for the registered public user identity. The reg event package also provides a mechanism for the Application Server to obtain the associated parameters (e.g GRUUs, ICSIs and IARIs) for each contact of every registered public identity.

**NOTE:** When the Application Server maintains a persistent subscription to the reg event package it is not necessary for the Application Server to receive third party registration requests from the S-CSCF in response to refresh and de-registration events as these are communicated to the Application Server in the reg event notifications.

More information on these procedures is contained in 3GPP TS 24.229 [5].

## 6.4 S-CSCF handling of UE-originating requests

### 6.4.1 S-CSCF handling of UE-originating requests, registered user

The served user can be included in different information elements than the calling identity. The S-CSCF shall determine the appropriate identity of the served user from one of these information elements.

The S-CSCF shall verify if the public user identity of the served user is barred. If so, it shall respond with a 4xx error code and stop further processing of the request. A UE-originating initial request may originate from an Application Server via the ISC interface. Originating initial requests from an Application Server via the ISC interface also cause the S-CSCF to look for initial filter criteria.

The S-CSCF only looks for initial filter criteria when receiving an initial request.



The initial filter criteria (subset of the profile) has already been downloaded from the HSS and is stored locally at the S-CSCF, as specified in 3GPP TS 24.229 [5].

When such a request comes in, the S-CSCF shall first check whether this is an UE-originating request or a UE-terminating request in order to perform the matching procedure with SPTs within initial filter criteria. This subclause describes the requirements for the S-CSCF when this request is a UE-originating request. If this request is a UE-originating request, the S-CSCF shall:

- determined the served user;
- check whether the request matches a subscribed service (i.e. SDP and other content matches appropriate SDP and other content for each and any of the subscribed services for served user user). As an operator option, if the contents of the request do not match a subscribed service, the S-CSCF may reject the request;
- check whether any contained unauthenticated ICSI value is part of the set of the subscribed services and is consistent with the contents of the request (i.e. SDP and other content is consistent with the unauthenticated ICSI value) if so that is the IMS communication service related to the request;
- if the request contains an unauthenticated ICSI value then remove the unauthenticated ICSI value;
- if the request does not contain an unauthenticated ICSI value, or the one that is included is not part of the set of the subscribed services, then as an operator option, the S-CSCF may: either reject the request, or proceed without a service identifier or choose one of the others from the subscribed set;
- include an authenticated ICSI value if the contents of the request are related to an IMS communication service based upon the previous checks and use this authenticated ICSI value as the IMS communication service identifier when applying the initial filter criteria in the subsequent steps;
- use the initial Filter Criteria for the UE-originating case tied to the served user;
- check whether this request matches the initial filter criteria with the highest priority for the served user by checking the service profile against the public user identity of the served user, which was used to place this request;
- if this request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server;
- if this request does not match the highest priority initial filter criteria, check for matching of the following filter criteria priorities until one applies;
- if no more (or none) of the initial filter criteria apply, the S-CSCF shall forward this request downstream based on the route decision;
- in any instance, if the contact of the application server fails, the S-CSCF shall use the "default handling" associated with the initial Filter Criteria to determine if it shall either terminate the call or let the call continue based on the information in the filter criteria; if the filter criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the application server, the S-CSCF shall let the call continue as the default behaviour.

#### 6.4.2 S-CSCF handling of UE-originating requests, unregistered user

The served user can be included in different information elements other than calling identity. The S-CSCF shall determine the appropriate identity of the served user from one of these information elements.

The S-CSCF shall verify if the public user identity of the served user is barred. If so, it shall respond with a 4xx error code and stop further processing of the request.

The S-CSCF only looks for initial filter criteria when receiving an initial request. A UE-originating initial request may originate from an Application Server via the ISC interface. Originating initial requests from an Application Server via the ISC interface also cause the S-CSCF to look for initial filter criteria.

When such a request comes in, the S-CSCF shall first check this is an UE-originating request or a UE-terminating request. This subclause describes the requirements for the S-CSCF when this request is an originating request. So, if this request is a UE-originating request, the S-CSCF shall:

- check whether the request matches a subscribed service (i.e. SDP and other content matches appropriate SDP and other content for each and any of the subscribed services for the served user). As an operator option, if the contents of the request do not match a subscribed service, the S-CSCF may reject the request;
- check whether any contained unauthenticated ICSI value is part of the set of the subscribed services and is consistent with the contents of the request (i.e. SDP and other content is consistent with the unauthenticated ICSI value) if so that is the IMS communication service related to the request;
- if the request contains an unauthenticated ICSI value then remove the unauthenticated ICSI value;
- if the request does not contain an unauthenticated ICSI value, or the one that is included is not part of the set of the subscribed services, then as an operator option, the S-CSCF may: either reject the request, or proceed without a service identifier or choose one of the others from the subscribed set;
- include an authenticated ICSI value if the contents of the request are related to an IMS communication service based upon the previous checks and use this authenticated ICSI value as the IMS communication service identifier when applying the initial filter criteria in the subsequent steps;
- if unavailable, download the relevant subscriber profile including the initial filter criteria from the HSS;
- use the initial Filter Criteria for the UE-originating request for unregistered served user;
- check whether this request matches the initial filter criteria with the highest priority for the served user by checking the service profile against the public user identity of the served user, which was used to place this request;
- if this request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server;
- if this request does not match the highest priority initial filter criteria, check for matching of the following filter criteria priorities until one applies;
- if no more (or none) of the initial filter criteria apply, the S-CSCF shall forward this request downstream based on the route decision;
- in any instance, if the contact of the application server fails, the S-CSCF shall use the "default handling" associated with the initial Filter Criteria to determine if it shall either terminate the call or let the call continue based on the information in the filter criteria; if the filter criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the application server, the S-CSCF shall let the call continue as the default behaviour.

## 6.5 S-CSCF handling of UE-terminating requests

### 6.5.1 S-CSCF handling of UE-terminating requests, registered user

The served user can be included in different information elements than the called identity. The S-CSCF shall determine the appropriate identity of the served user from one of those information elements. If the selected information element includes a GRUU associated with a particular public user identity it is the associated public user identity that is the served user for the request and the S-CSCF shall use that served user for the following terminating request handling procedures.

The S-CSCF shall verify if the public user identity is barred of the served user. If so, it shall respond with a 4xx error code and stop further processing of the request.

The S-CSCF only looks for initial filter criteria when receiving an initial request. A UE-terminating initial request may also originate from an Application Server via the ISC interface. Terminating Initial requests from an Application Server via the ISC interface also cause the S-CSCF to look for initial filter criteria.

When such a request comes in, the S-CSCF shall first check whether this is an UE-originating request or a UE-terminating request. For UE-terminating initial requests the S-CSCF shall first perform any routing of the request to Application Server based on matching of initial Filter Criteria before performing other routing procedures towards the terminating UE, (e.g. forking, caller preferences etc). This subclause describes the requirements for the S-CSCF when this request is a UE-terminating request. So, if this request is a UE-terminating request, the S-CSCF shall:

- if the request contains an authenticated ICSI value the S-CSCF shall check whether the IMS communication service identified by the authenticated ICSI value is allowed for the subscribed services for the served user and is consistent with the contents of the request (i.e. SDP and other content is consistent with the unauthenticated ICSI value) and if not remove the authenticated ICSI value otherwise use this as the authenticated ICSI value;
- if the request does not contain an authenticated ICSI value then check whether the request matches a subscribed service (i.e. SDP and other content matches appropriate SDP and other content for each and any of the subscribed services for the served user) As an operator option, if the contents of the request do not match a subscribed service, the S-CSCF may reject the request;
- include an authenticated ICSI value if the contents of the request are related to an IMS communication service based upon the previous checks and use this authenticated ICSI value as the IMS communication service identifier when applying the initial filter criteria in the subsequent steps;
- if unavailable, download the relevant subscriber profile including the initial filter criteria from the HSS;
- use the initial Filter Criteria for the UE-terminating request to registered served user;
- in case the Request-URI changes when visiting an Application Server, terminate the checking of filter criterias, and either:
  - a) route the request, without attempting to verify the barring status of the changed public user identity, based on the changed value of the Request-URI and do not execute the subsequent steps;
  - b) use the initial Filter Criteria for the UE-originating case after retargeting and perform the matching procedure with SPTs within this initial Filter Criteria as described in subclause 6.4.1; or
  - c) continue to use the initial Filter Criteria for the UE terminating case and perform the matching procedure with SPT within the UE terminating UE case.

NOTE: The S-CSCF determines whether to apply a), b) or c) based on information in the initial Filter Criteria.

- the subsequent requirements for the S-CSCF are the same as those for handling UE-originating requests.

Originating UE and terminating UE can share the same S-CSCF and Application Server, therefore the shared application server may interact with the S-CSCF twice in one transaction but in UE-originating and UE-terminating procedures respectively.

## 6.5.2 S-CSCF handling of UE-terminating requests, unregistered user

The Served user can be included in different information elements than the called identity The S-CSCF shall determine the appropriate identity of the served user from one of those information elements. If the selected information element includes a GRUU associated with a particular public user identity it is the associated public user identity that is the served user for the request and the S-CSCF shall use that served user for the following terminating request handling procedures.

The S-CSCF shall verify if the public user identity of the served user is barred. If so, it shall respond with a 4xx error code and stop further processing of the request.

The S-CSCF only looks for initial filter criteria when receiving an initial request. A UE-terminating initial request may also originate from an Application Server via the ISC interface. Terminating initial requests from an Application Server via the ISC interface also cause the S-CSCF to look for initial filter criteria.

When such a request comes in, the S-CSCF shall first check this is an UE-originating request or a UE-terminating request. This subclause describes the requirements for the S-CSCF when this request is a UE-terminating request. So, if this request is a UE-terminating request, the S-CSCF shall:

- if the request contains an authenticated ICSI value the S-CSCF shall check whether the IMS communication service identified by the authenticated ICSI value is allowed for the subscribed services for the served user and is consistent with the contents of the request (i.e. SDP and other content is consistent with the unauthenticated ICSI value) and if not remove the authenticated ICSI value otherwise use this as the authenticated ICSI value;
- if the request does not contain an authenticated ICSI value then check whether the request matches a subscribed service (i.e. SDP and other content matches appropriate SDP and other content for each and any of the subscribed services for the served user user) As an operator option, if the contents of the request do not match a subscribed service, the S-CSCF may reject the request;
- include an authenticated ICSI value if the contents of the request are related to an IMS communication service based upon the previous checks and use this authenticated ICSI value as the IMS communication service identifier when applying the initial filter criteria in the subsequent steps;
- if unavailable, download the relevant subscriber profile including the initial filter criteria from the HSS;
- use the initial Filter Criteria for the UE-terminating request to unregistered served user;
- in case the Request-URI changes when visiting an Application Server, terminate the checking of filter criterias, and either:
  - a) route the request, without attempting to verify the barring status of the changed public user identity, based on the changed value of the Request-URI and do not execute the subsequent steps;
  - b) use the initial Filter Criteria for the UE-originating case after retargeting and perform the matching procedure with SPTs within this initial Filter Criteria as described in subclause 6.4.1; or
  - c) continue to use the initial Filter Criteria for the UE terminating case and perform the matching procedure with SPT within the UE terminating UE case.

NOTE: The S-CSCF determines whether to apply a), b) or c) based on information in the initial Filter Criteria.

- the subsequent requirements for the S-CSCF are the same as those for handling UE-originating requests with one exception: if no more (or none) of the initial filter criteria apply, the S-CSCF shall reject the request.

Originating UE and terminating UE can share the same S-CSCF and Application Server, therefore the shared application server may interact with the S-CSCF twice in one transaction but in UE-originating and UE-terminating procedures respectively.

## 6.5A Transit Function handling of requests

### 6.5A.1 Transit Function handling of initial requests and standalone requests

An initial request or a standalone request may originate from an Application Server via the ISC interface. Originating initial requests and standalone requests from an Application Server via the ISC interface also cause the Transit Function to look for Transit Invocation Criteria.

The Transit Invocation Criteria is locally configured at the Transit Function.

When the Transit Function receives an initial request, or a standalone request, and the request is associated with a transit scenario where IMS application services are provided, in order to perform the matching procedure with SPTs within Transit Invocation Criteria. Then the Transit Function shall:

- check whether the request matches a service configured for the transit scenario. As an operator option, if the contents of the request do not match a configured service, the Transit Function may reject the request;

- use the Transit Invocation Criteria for the transit scenario;
- check whether this request matches the Transit Invocation Criteria with the highest priority configured for the transit scenario;
- if this request matches the Transit Invocation Criteria, the Transit Function shall forward this request to that Application Server, then check for matching of the next following criteria of lower priority, and apply the criteria on the SIP method received from the previously contacted Application Server;
- if this request does not match the highest priority Transit Invocation Criteria, check for matching of the following criteria priorities until one applies;
- if no more (or none) of the Transit Invocation Criteria apply, the Transit Function shall forward this request downstream based on the route decision; and
- in any instance, if the contact of the Application Server fails, the Transit Function shall use the "default handling" associated with the Transit Invocation Criteria to determine if it shall either terminate the call or let the call continue based on the information in the criteria; if the criteria does not contain instruction to the Transit Function regarding the failure of the contact to the Application Server, the Transit Function shall let the call continue as the default behaviour.

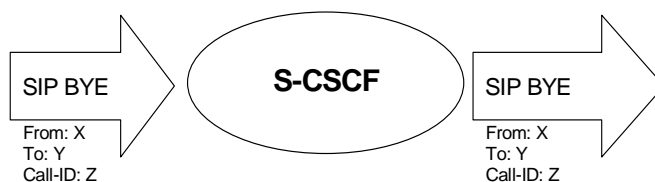
## 6.6 S-CSCF and Transit Function handling of IP multimedia session release requests

### 6.6.0 Introduction

In handling session release, the S-CSCF and the Transit Function may either proxy the release request or initiates a release request.

#### 6.6.1 S-CSCF and Transit Function proxying release request

When the S-CSCF and the Transit Function receives a release request from some entities (etc, application server, user agent) for a dialog, it proxies the release request to the destination according to route information in that release request.



**Figure 6.6.1.1: S-CSCF proxying release request**

#### 6.6.2 S-CSCF and Transit Function initiating release request

For some reason (etc. administration decision of the network), the S-CSCF and the Transit Function may be required to release an ongoing dialog. In this case, the S-CSCF and the Transit Function shall send a release request to all the entities that are involved in this dialog. In a typical AS involved dialog, the S-CSCF and the Transit Function should send the release request to the AS and the UE it is serving as shown in figure 6.6.2.1.

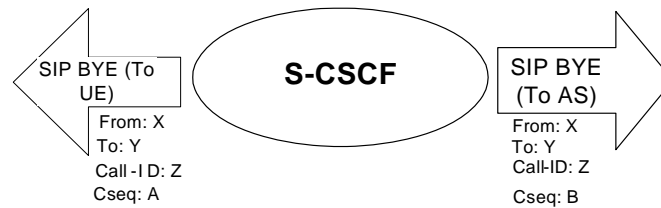


Figure 6.6.2.1: S-CSCF initiating release request

## 6.7 S-CSCF handling of subscription and notification

The S-CSCF supports subscription to and notification of the reg event package by the UE, P-CSCFs and Application Servers. The subscribing entity may subscribe to the registration state of individual public user identities for the purpose of discovering the implicitly registered public user identities and associated parameters (e.g. GRUUs, ICSIs, IARIs) for each registered contact. When notifying a subscribing entity of a change in the registration state of a subscribed to public user identity the S-CSCF shall include in the notification all the implicitly registered public user identities associated with the registered public user identity in addition to the registered public user identity along with the associated parameters of every contact of each registered public user identity.

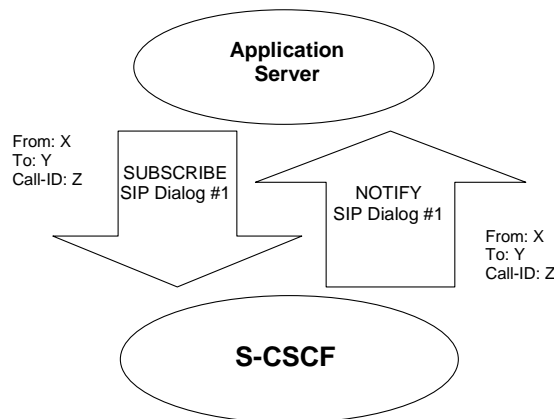


Figure 6.7.1: Application Server – S-CSCF subscribe notify dialog

## 6.8 S-CSCF handling IMS charging

In registration processing, a S-CSCF may send a third party REGISTER to an application server, where the ICID, IOI and charging function addresses are included in the message.

During a session, the S-CSCF shall generate the CDR for charging purposes.

In a session originating case, when receiving an incoming initial request, this request will carry the ICID generated by the upstream P-CSCF, which is serving the originating user; the S-CSCF shall store the ICID for this session and handle this request based on filter criteria. After processing this request the S-CSCF shall include the ICID and the charging function addresses received from the HSS in the outgoing message. The charging function addresses identify on-line, and off-line charging entities in the home network. It is implementation dependent how IMS related entities such as P-CSCF in the visited network get the local CCF or AAA addresses in the case that the P-CSCF is located in the visited network. Charging function addresses may be allocated as locally preconfigured addresses. If this message is sent outside the home network, S-CSCF shall include Inter Operator Identifier (IOI) that identifies the home network into the message. IOI is globally unique identifier for using inter operator accounting purposes. The response to the outgoing message may contain a separate IOI that identifies the home network of the called party. The S-CSCF shall retain either IOI in the message when contacting the Application Servers. The S-CSCF will receive access network (IP-CAN) charging information from subsequent requests and responses, the S-CSCF shall store these parameters and shall remove them from the outgoing message if this message is sent to the terminating UE's home network or the originating UE's visited network. The access network (IP-CAN) charging information may be sent to application servers.

In a session terminating case, when receiving an incoming initial request, this request will carry the ICID generated by the originating UE's P-CSCF; the S-CSCF shall store the ICID for this session and handle this request based on filter criteria. After processing this request the S-CSCF shall include the ICID and the charging function addresses received from the HSS in the outgoing message. The charging function addresses identify on-line and off-line charging entities in the home network. IOI may be received from another network or is inserted by the MGCF to identify the originating PSTN/PLMN. If IOI is received at the S-CSCF, the S-CSCF shall store the IOI value for the network that sent the request. The response to the incoming message may contain a separate IOI that identifies the home network of the S-CSCF. The S-CSCF shall retain either IOI in the message when contacting the Application Servers. Afterwards, the S-CSCF shall remove the IOI of the requesting network from the message before sending the message further within the network. The S-CSCF will receive access network (IP-CAN) charging information from subsequent requests and responses, the S-CSCF shall store these parameters and removes them from the outgoing message if this message is sent to the terminating UE's visited network or the originating UE's home network. The access network (IP-CAN) charging information may be sent to application servers.

For detailed information on transporting charging parameters between IMS entities using SIP, see 3GPP TS 24.229 [5].

## 6.8A Transit Function handling IMS charging

During a session, the Transit Function shall generate a CDR for charging purposes. Charging function addresses are configured in the Transit Function.

Incoming initial SIP requests or a stand-alone SIP requests will carry an ICID generated by an upstream functional entity and an Inter Operator Identifier (IOI) identifying the network sending the request (the home network serving a user or a visited network where the user is connected). The Transit Function shall store the ICID and the IOI for this session.

Incoming SIP requests within an existing dialog will carry the ICID received in the initial SIP request and an IOI identifying the network sending the request (the home network serving a user or a visited network where a user is connected).

When sending SIP requests to Application Servers the Transit Function shall:

- include the ICID received in the incoming initial SIP request or stand-alone SIP request;
- remove the IOI received in the request; and
- include an IOI value identifying the network where the Transit Function resides.

When forwarding the incoming initial request, the stand-alone request or the request received within the existing dialog to a down stream functional entity, i.e. an functional entity that is not an Application Server, the Transit Function shall include the ICID and the IOI received in the incoming request.

Responses to the initial SIP request, the stand-alone SIP request or the SIP request received within the existing dialog will contain the ICID received in the incoming request and an IOI value included by an down stream entity.

When sending responses to Application Servers the Transit Function shall:

- include the ICID value received in the response;
- remove the IOI value received in the response; and
- include an IOI value identifying the network where the Transit Function resides.

The Transit Function shall store any IOI received from an Application Server in requests or responses.

For detailed information on transporting charging parameters between IMS entities using SIP, see 3GPP TS 24.229 [5].

## 6.9 S-CSCF description of subscriber data

### 6.9.1 Application Server subscription information

The Application Server Subscription Information is the set of all Filter Criteria that are stored within the HSS for service profile for a specific user. This information shall be sent by the HSS to the S-CSCF via the Cx Interface during registration. More than one set of Filter Criteria may be sent during registration if implicitly registered public user identities belong to different service profiles. Filter Criteria shall also be sent after registration via the Cx interface when requested, as specified in 3GPP TS 29.228 [8].

### 6.9.2 Filter Criteria

#### 6.9.2.0 Introduction

This subclause defines the contents of the Filter Criteria. This information is part of the Application Server Subscription Information. For further information about the XML modelling see 3GPP TS 29.228 [8].

Filtering is done for initial SIP request messages only.

The S-CSCF shall apply filter criteria to determine the need to forward SIP requests to Application Servers. These filter criteria will be downloaded from the HSS.

Initial Filter Criteria (iFC) are stored in the HSS as part of the user profile and are downloaded to the S-CSCF upon user registration, or upon a terminating initial request for an unregistered user if unavailable, or upon an originating initial request from an Application Server for an unregistered user if unavailable. They represent a provisioned subscription of a user to an application. After downloading the User Profile from the HSS, the S-CSCF assesses the filter criteria. Initial Filter Criteria are valid throughout the registration lifetime of a user or until the User Profile is changed.

Subsequent Filter Criteria (sFC) are not used in this version of this specification.

#### 6.9.2.1 Application Server address

Address to be used to access the Application Server for a particular subscriber.

#### 6.9.2.2 Default handling

The default handling procedure indicates whether to abandon matching of lower priority triggers and to release the dialogue, or to continue the dialogue and trigger matching.

#### 6.9.2.3 Trigger point

Trigger Points are the information the S-CSCF receives from the HSS that defines the relevant SPTs for a particular application. They define the subset of initial SIP requests received by the S-CSCF or headers (eg P-Asserted-Service header) created by S-CSCF that should be sent or proxied to a particular application server. When the S-CSCF receives an initial SIP request, it evaluates the filter criteria one by one. If the initial SIP request matches the filter criteria, the S-CSCF proxies the SIP request to the corresponding SIP AS/IM-SSF/OSA SCS.

#### 6.9.2.4 iFC Priority

If there are multiple initial Filter Criteria assigned for one subscriber, the priority shall describe the order in which the S-CSCF shall assess them, and then contact the Application Servers when the SIP request matches the initial filter criteria. In this case, the S-CSCF shall interact with the application server associated with the initial matching filter criteria, starting from the filter criteria which has the highest priority.

#### 6.9.2.5 Service Information

Service Information is transparent information, and is not processed by the HSS or the S-CSCF. Service Information is optionally part of an initial Filter Criteria. If it is available from the initial Filter Criteria the S-CSCF shall include it into



the body of the SIP request which is sent from the S-CSCF to the AS to which the initial Filter Criteria is pointing to. Service Information is only included by the S-CSCF in REGISTER requests where the S-CSCF acts as a UAC.

### 6.9.2.6 Include Register Request

Include Register Request defines whether the S-CSCF is to include the incoming REGISTER request in the body of the third party REGISTER request.

NOTE: When the AS is outside the trust domain for any header field that is permitted in the REGISTER request received from the UE, including an Include Register Request indication in the initial Filter Criteria would cause the incoming REGISTER request contents to be delivered to the AS revealing information that AS is not trusted to obtain. Include Register Request indication is therefore not included in the initial Filter Criteria for an AS that exists outside the trust domain for any such header field.

### 6.9.2.7 Include Register Response

Include Register Response defines whether the S-CSCF is to include the final response to the incoming REGISTER request in the body of the third party REGISTER request.

NOTE: When the AS is outside the trust domain for any header field that is permitted in the final response to the REGISTER request received from the UE, including an Include Register Response indication in the initial Filter Criteria would cause the final response to the incoming REGISTER request contents to be delivered to the AS revealing information that AS is not trusted to obtain. Include Register Response indication is therefore not included in the initial Filter Criteria for an AS that exists outside the trust domain for any such header field.

## 6.9.3 Authentication data

This subclause defines the Authentication Data. This data shall be sent by the HSS to the S-CSCF via the Cx Interface during registration.

For definition of authentication data see specification 3GPP TS 23.008 [10]. For the handling of authentication data, see 3GPP TS 33.203 [11].

---

# 7 Functional requirements of HSS

## 7.1 Subscriber data related storage requirements for HSS

HSS stores information required by:

- S-CSCFs (downloaded via Cx interface). Data model and abstract syntax notation are described in 3GPP TS 29.228 [8];
- IM-SSF Application Servers (downloaded via Si or Sh interface);
- Application Servers (downloaded via Sh interface).

The service related data shall be transparent to HSS, this requires the HSS has some means to differentiate the source of the request for the data, therefore, the HSS can respond with the data the request asks for.

## 7.2 Interfaces defined for HSS

### 7.2.1 HSS – CSCF (Cx) interface

This interface is used to send subscriber data to the S-CSCF, including Filter Criteria (and their priority); which indicates which SIP requests should be proxied to which Application Servers.

The protocol used between the HSS and CSCF (Cx Interface) is specified in 3GPP TS 29.228 [8] and 3GPP TS 29.229 [17].

## 7.2.2 HSS - Application Server (Sh) interface

The Sh interface is between the HSS and the SIP Application Servers and the OSA SCS and may be used for transferring User Profile information such as user service related information or user location information or charging function addresses. Requirements for the Sh interface are specified in 3GPP TS 23.228 [3].

The Sh interface also supports mechanisms that allow Application Servers to activate/deactivate their own existing initial filter criteria stored in the HSS on a per subscriber basis.

The protocol used between the HSS and AS (Sh Interface) is specified in 3GPP TS 29.328 [18] and 3GPP TS 29.329 [19].

## 7.2.3 HSS – CSE interface

The protocol used on the interface between the HSS and the CAMEL Service Environment (CSE) is the MAP protocol [16].

## 7.2.4 HSS – IM-SSF Application Server interface

The interfaces between the HSS and the IM-SSF Application Server are:

- the Si interface when the MAP protocol as specified in 3GPP TS 23.278 [9] and 3GPP TS 29.002 [16] is used
- the Sh interface when the Diameter based protocol as specified in 3GPP TS 29.328 [18], 3GPP TS 29.329 [19] and 3GPP TS 29 364 [26] is used

The Si and the Sh interfaces between HSS and the IM-SSF Application Server are used for transferring IMS CAMEL specific information.

## 7.3 Procedures during IP multimedia registration

These procedures are described in 3GPP TS 29.228 [8].

## 7.4 Procedures during IP multimedia sessions

These procedures are described in 3GPP TS 29.228 [8].

---

# 8 Functional requirements of the MRFC

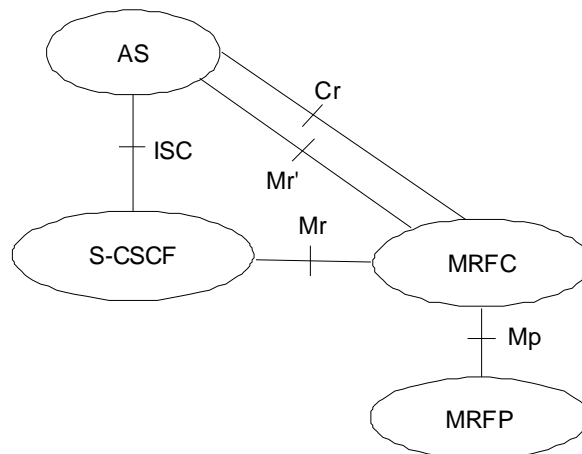
## 8.1 Functionality of the MRFC

### 8.1.1 Overview of MRFC Functionality

The functionality of the MRFC is defined in 3GPP TS 23.228 [3]. These subclauses describe how an Application Server may interact with a MRFC. In some cases a UE may interact directly with the MRFC, however these cases are outside the scope of this specification and only the cases of Application Server control for service provision are considered here. In all cases of Application Server control, all session control requests that are passed between the Application Server and the MRFC may be either exchanged directly via the Mr' interface or sent via the S-CSCF using the ISC interface and the interface of the Mr reference point. In addition to the session control requests, media control related commands and resources may be passed between the Application Server and the MRFC using the Cr interface.

MRFC addresses are made known via peer-to-peer arrangements within the IM CN subsystem.

Figure 8.1.1.1 describes the relationship of the Application Server with the S-CSCF and MRFC.



**Figure 8.1.1.1: Relationship of MRFC and MRFP with S-CSCF, and Application Servers**

## 8.1.2 Tones and announcements

An Application Server is in control of the tone/announcement selection and is aware of MRFC capabilities.

The MRFC accepts INVITE requests sent from an Application Server, either directly using the Mr' interface or via the S-CSCF using the ISC interface, for the purpose of applying tones and announcements. The INVITE request sent to the MRFC will contain sufficient information to play the appropriate tone or announcement or sufficient information for the request to be linked to a media control command passed between the Application Server and MRFC using the Cr interface that will contain that information.

Any additional resources required (for example announcement files) may be fetched from the Application Server via the Cr interface.

The MRFC shall support both the offer/answer as defined in IETF RFC 3264 [15] and the offer/answer with preconditions models for SDP negotiation with the AS. However, the offer/answer model for SDP negotiation between the AS and the MRFC is sufficient for applying tones and announcements. The MRFC should always grant the requests from the AS (unless there is a resource problem). The receipt of the ACK request or media control command at the MRFC triggers the playing of the tone or announcement.

The tone or announcement should end when a BYE request is received. Alternatively, an expiration time may have been specified from the AS within the SDP of the INVITE request or a media control command. In this case, the MRFC may terminate the media on its own and generate a BYE request towards the AS. A tone or announcement may also have a pre-determined play time (e.g., confirmation tone), and so there may not be a need for the AS to send a request to stop it or to include the play time in the request.

See annex B for a call flow example of playing an announcement for a UE-originating call.

## 8.1.3 Ad-hoc conferences (multiparty calls)

An Application Server can control an Ad-Hoc conference (multiparty call) and is aware of MRFC capabilities.

The MRFC accepts INVITE requests sent from an Application Server, either directly using the Mr' interface or via the S-CSCF using the ISC interface, for the purpose of managing ad hoc conferences. The INVITE request sent to the MRFC shall contain sufficient information to initiate, add and remove parties from the conference. ReINVITE requests can also be sent for managing floor control and for parties to leave and rejoin the media path.

Media control commands to control the conference (for example conference gain) may be sent between the Application Server and the MRFC via the Cr interface.

The MRFC shall support both the offer/answer as defined in IETF RFC 3264 [15] and the offer/answer with preconditions models for SDP negotiation with the AS. However, the offer/answer model for SDP negotiation between the AS and the MRFC is sufficient for managing ad hoc conferences. The MRFC should always grant the requests from the AS (unless there is a resource problem). The MRFC will reserve the requested local resources and return the appropriate resource identifiers in the 200 (OK) response.

See annex B for a call flow example of an Ad Hoc Conference (Multiparty Call).

## 8.1.4 Transcoding

An Application Server can control a transcoding session and is aware of MRFC capabilities.

The MRFC accepts INVITE requests sent from an Application Server, either directly using the Mr' interface or via the S-CSCF using the ISC interface, for the purpose of transcoding. The INVITE request sent to the MRFC shall contain sufficient information to associate the two sessions that require transcoding.

The MRFC shall support both the offer/answer as defined in IETF RFC 3264 [15] and the offer/answer with preconditions models for SDP negotiation with the AS. Either may be necessary for SDP negotiation between the AS/S-CSCF and the MRFC. The MRFC should always grant the requests from the AS (unless there is a resource problem).

For the offer/answer model, the MRFC responds to the INVITE request with a 200 (OK) response indicating the selected media in the SDP. The MRFC will also reserve the requested local resources at that time and return the appropriate resource identifiers in the 200 (OK) response.

For the offer/answer with preconditions model, the MRFC responds to the INVITE request with a 183 (Session Progress) response indicating the list of codecs supported by the MRFC. When the PRACK request is received indicating the selected media in the SDP, the MRFC will reserve the requested local resources at that time and return the appropriate resource identifiers in the 200 (OK) response.

See annex B for call flow examples of providing transcoding.

## 8.2 Interfaces defined for MRFC

### 8.2.1 MRFC – S-CSCF (Mr) interface

The protocol used between MRFC and S-CSCF is based on Session Initiation Protocol, which is specified in 3GPP TS 24.229 [5].

The interface is used where it is wished to use the services of the S-CSCF to route to the MRF.

The interface is also used to support the establishment of a media control channel with the MRF, or between the MRF and the MRB.

The interface is also used where the S-CSCF, I-CSCF or UE wishes to address the MRF directly. These entities can also use an MRB (using this interface) to support selection of the appropriate MRF. Such usage is however limited to In-Line mode (see subclause 13.2).

### 8.2.2 Application Server – MRFC (Cr) interface

The Cr interface allows interaction between an Application Server and an MRFC.

The Cr interface enables the MRFC to fetch and cache documents and resources from an Application Server and to return data to an Application server.

The Cr interface enables media control protocol requests, responses and notifications to be sent between the MRFC and an Application Server.

The establishment and management of the media control protocol is done via SIP messages sent between the Application Server and the MRFC (either directly using the Mr' interface or via the S-CSCF using the ISC interface) and is specified in 3GPP TS 24.229 [5].

The protocols which use this interface are specified in 3GPP TS 24.229 [5], 3GPP TS 24.147 [23] and 3GPP TS 24.247 [24].

### 8.2.3 Application Server – MRFC (Mr') interface

Mr' interface allows an Application Server and an MRFC to exchange session control messages without passing through an S-CSCF.

The protocol used between Application Server and MRFC over Mr' interface is based on Session Initiation Protocol, which is specified in 3GPP TS 24.229 [5].

### 8.2.4 MRB – MRFC (Mr') interface

This interface is used for an MRB operating in In-Line mode. The use of this interface is described in subclause 13.2.

This interface can also be used by the MRFC to establish a media control channel between the MRB and the MRFC to allow the publication of resource information, see subclause 13.3.

Mr' interface allows an MRB and an MRFC to exchange session control messages without passing through an S-CSCF.

The protocol used between MRB and MRFC over Mr' interface is based on Session Initiation Protocol, which is specified in 3GPP TS 24.229 [5].

### 8.2.5 MRB – MRFC (Cr) interface

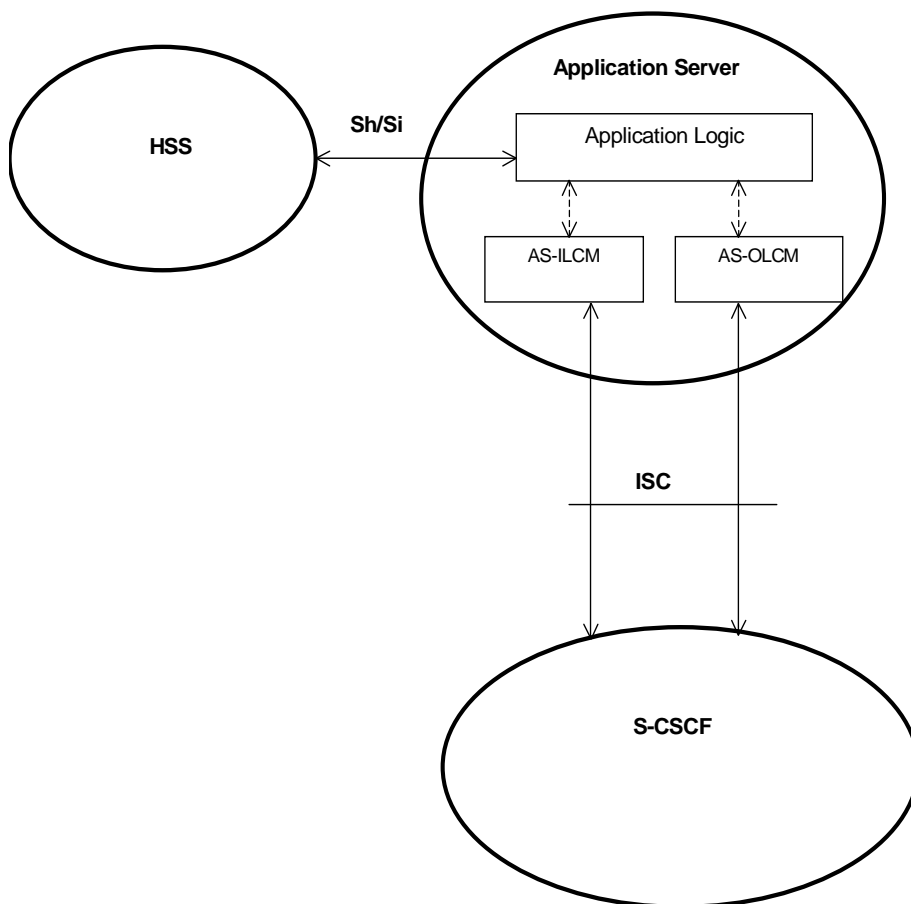
This interface is used for an MRFC to publish information to the MRB. The use of this interface is described in subclause 13.3.

## 9 Generic IP multimedia session handling for SIP Application Servers

### 9.1 Architecture

#### 9.1.0 Introduction

This subclause describes the functional architecture needed to support interactions between the S-CSCF in the IP Multimedia Subsystem and the Application Server(s). This subclause relates to the generic behaviour of SIP Application Servers, which since SIP is the ISC interface protocol shall be considered to apply to all application servers, (which also includes the SIP behaviour of the OSA SCS and IM-SSF). The detailed models for service provision are described in the subclauses below. These models shall apply to the SIP behaviour of the OSA SCS and IM-SSF and all the Application Servers.



**Figure 9.1.1: Application Server functional model**

Figure 9.1.1 identifies the components of a functional model of the AS.

**NOTE:** These components are defined only as a model of the expected behaviour of the AS on the ISC interface and are not intended to define or constrain the actual implementation.

The components include the AS-ILCM, the AS-OLCM and the Application Logic. The AS-ILCM shall store transaction state, and may optionally store session state depending on the specific service being executed. The AS-ILCM interfaces to the S-CSCF (ILCM) for an incoming leg.

The AS-OLCM shall store transaction state, and may optionally store session state depending on the specific service being executed. The AS-OLCM interfaces to the S-CSCF (OLCM) for an outgoing leg.

The Application Logic provides the service(s) and interacts between the AS-ILCM and AS-OLCM.

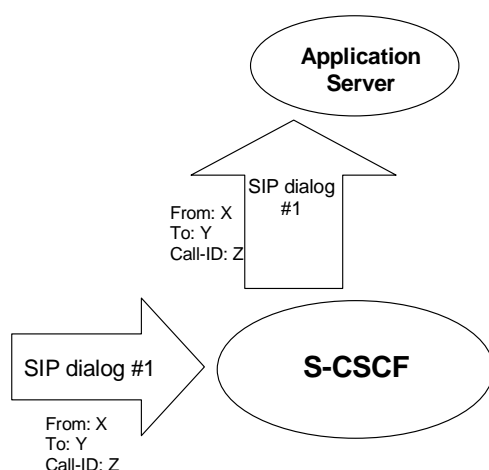
The Application Server can access the HSS via the Sh or Si interface to access subscriber related data specific to the service or application including the address of the S-CSCF.

## 9.1.1 Modes of operation between Application Server and S-CSCF

### 9.1.1.0 Introduction

An Application Server can utilize five basic modes of operation for processing SIP Requests. Services can be built using combinations of these five modes of operation between the Application Server and the S-CSCF. An application Server can transition from one mode of operation to another during the lifetime of a multimedia session it is managing.

#### 9.1.1.1 Application Server acting as terminating UA, or redirect server



**Figure 9.1.1.1.1: Application Server acting as terminating UA, or redirect server**

In this mode of operation the incoming SIP Request is proxied by the S-CSCF to the Application Server, which then acts as either a UA or Redirect Server as specified in IETF RFC 3261 [6].

9.1.1.2 Application Server acting as originating UA

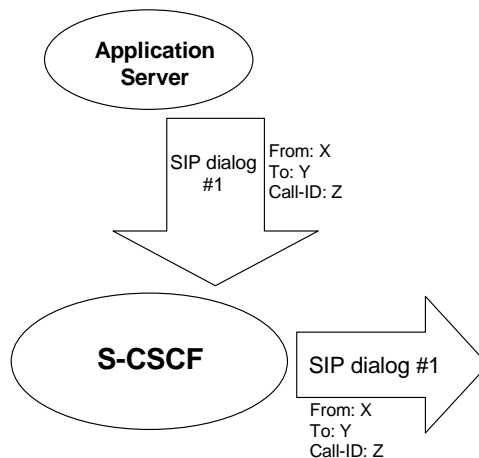


Figure 9.1.1.2.1: Application Server acting as originating UA

In this mode of operation the Application Server acts as a UA as specified in IETF RFC 3261 [6] and generates a SIP Request which it sends to the S-CSCF which then proxies it towards the destination.

9.1.1.3 Application Server acting as a SIP proxy

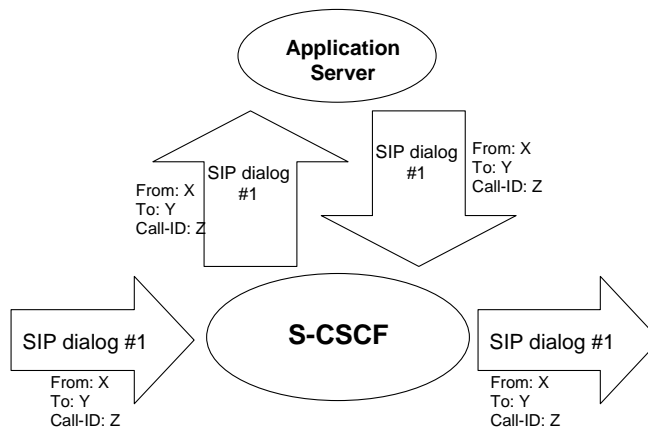


Figure 9.1.1.3.1: Application Server acting as a SIP proxy

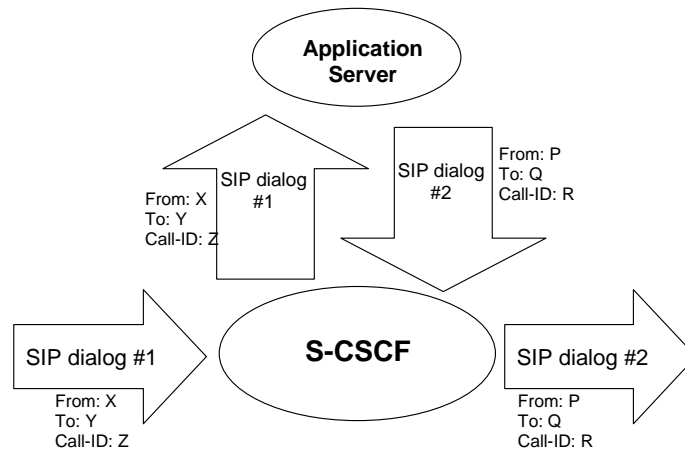
In this mode of operation the incoming SIP Request is proxied by the S-CSCF to the Application Server which then acts as a proxy as specified in IETF RFC 3261 [6] proxying the request back to the S-CSCF which then proxies it towards the destination. During the proxy operation the Application Server can add, remove or modify the header contents contained in the SIP request according to the Proxy rules specified in IETF RFC 3261 [6].

9.1.1.4 Application Server performing third party call control/ B2BUA mode

The AS performing 3rd party call control acts as a B2BUA. There are several kinds of 3rd party call control, for example:

- Routing B2BUA: an AS receives a request from the S-CSCF, terminates it and generates a new request, which is based on the received request.

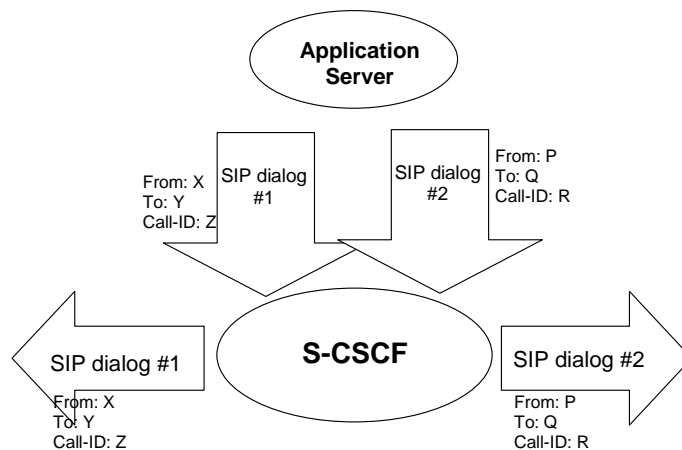




**Figure 9.1.1.4.1: Application Server performing third party call control acting as a routing B2BUA**

In this mode of operation the incoming SIP Request is proxied by the S-CSCF to the Application Server which then generates a new SIP request for a different SIP dialog which it sends to the S-CSCF which then proxies it towards the destination. In this mode the Application Server behaves as a B2BUA for the multiple SIP dialogs as specified in IETF RFC 3261 [6].

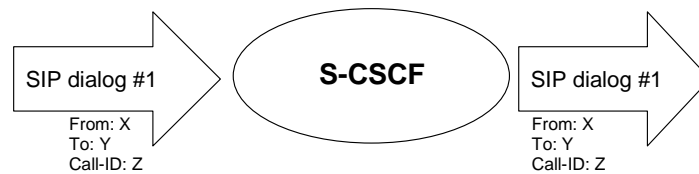
- Initiating B2BUA: an AS initiates two requests, which are logically connected together at the AS.



**Figure 9.1.1.4.2: Application Server performing third party call control acting as an initiating B2BUA**

In this mode of operation the Application Server initiates two requests with different SIP dialogs. The Application Server is responsible for correlating the two dialogs. These requests are proxied through the S-CSCF which then proxies them towards the destination. In this mode the Application Server behaves as a B2BUA for the multiple SIP dialogs as specified in IETF RFC 3261 [6].

### 9.1.1.5 Application Server not involved or no longer involved



**Figure 9.1.1.5.1: A SIP leg is passed through the S-CSCF without Application Server involvement**

In this mode of operation the Application Server was either never involved in the SIP session signalling or has determined to be no longer involved. The incoming SIP Request is proxied by the S-CSCF towards the destination. The Application Server can maintain itself in the SIP session signalling path by inserting itself in a Record-Route Header as specified in IETF RFC 3261 [6]. If the Application Server does not insert itself in a Record Route header then this mode of operation shall be used for all subsequent requests related to this SIP dialog.

## 9.1.2 Modes of operation between Application Server and Transit Function

The modes of operation between the Application Server and the Transit Function are identical to the modes of operation between the Application Server and the S-CSCF, as specified in subclause 9.1.1.

## 9.2 Interfaces defined for a SIP Application Server

### 9.2.1 S-CSCF – Application Server (ISC) interface

This interface can be used by the Application Server to control an IP Multimedia session via a S-CSCF. Transactions between the S-CSCF and the Application Server on this interface are initiated either as a result of the S-CSCF proxying a SIP request to the Application Server or by the Application Server initiating by generating and sending a SIP request to the S-CSCF. This interface is based on SIP.

### 9.2.2 Application Server – HSS (Sh) interface

The Sh interface is between the HSS and the SIP Application Servers and the OSA SCS and may be used for transferring User Profile information.

The Sh interface also supports mechanisms that allow Application Servers to activate/deactivate their own existing initial filter criteria stored in the HSS on a per subscriber basis.

### 9.2.3 Application Server – SLF (Dh) interface

The Dh interface is between the SLF and the SIP Application Servers, the OSA SCS, and the IM-SSF and may be used for retrieving the address of the HSS which holds the User Profile information for a given user.

### 9.2.4 Application Server – MRFC (Cr) interface

The Cr interface allows interaction between an Application Server and an MRFC and is described further in subclause 8.2.2.

### 9.2.5 Application Server – MRB interface (Rc)

The Rc interface is used by the AS to request that media resources be assigned to a call when utilizing MRB in Query mode. See clause 13.

## 9.2.6 Transit Function – Application Server (ISC) interface

This interface can be used by the Application Server to control an IP Multimedia session via a transit function. Transactions between the transit function and the Application Server on this interface are initiated as a result of the transit proxying a SIP request to the Application Server. This interface is based on SIP. The interface implements the Mf reference point, as defined in 3GPP TS 23.228 [3].

## 9.3 Description of Application Server related subscriber data

### 9.3.1 Application server subscription information

#### 9.3.1.0 Introduction

This subclause defines the general contents of the Subscription Information that may be required by the Application Server. The AS shall obtain this information from the HSS via the Sh interface or by other operator defined methods. The subscription information may be retrieved during registration or at any other time dependent on AS and service requirements.

#### 9.3.1.1 Service key

The Service Key identifies to the Application Server the service logic that shall apply.

#### 9.3.1.2 Service platform trigger points (STP)

Service Platform Trigger Points (STP) are the points in the SIP signalling that instruct the Application Server to trigger the service logic.

#### 9.3.1.3 Service scripts

The Application Server can utilize a call processing script (e.g. in CGI, CPL, Java® Servlets, or another proprietary language), which may be obtained from the HSS via the Sh interface or by other operator defined methods.

**NOTE:** Java® is the trade name of a product supplied by Sun Microsystems. This information is given for the convenience of users of the present document and does not constitute an endorsement by 3GPP of the product named. Equivalent products may be used if they can be shown to lead to the same results.

## 9.4 Procedures for multimedia session handling with a SIP based Application Server

### 9.4.1 Application Server handling of UE-originating requests

The functional mode of application server is shown in figure 9.1.1.

For an UE-originating request, the AS-ILCM may interact with the application logic reporting call state information. Depending on the service that is being provided, the application logic may instruct the AS-OLCM to modify the request if needed (e.g. by inserting itself in the Record-Route etc). After processing the request the AS-OLCM may send this request back to the S-CSCF.

When the AS acts as a B2BUA, the application server shall maintain and correlate the multiple dialogues that it creates. It shall be responsible for correlating the dialogue identifiers and shall decide when to translate a message from one dialog to the other, or when to perform other functions based on the instruction from the application logic.

If an AS that supports a IMS communication service is acting as an initiating B2BUA and it receives an initial request or standalone transaction without an ICSI, it can insert an ICSI appropriate to the service it is performing on other legs and can also insert an ICSI appropriate to the service it is performing on the originating leg in appropriate SIP response messages on the originating leg.

NOTE: Whether to insert an ICSI on a leg and whether the ICSIs inserted on the legs are the same or not depend on the services being performed.

An AS that supports a IMS communication service that is acting as an originating UA can insert an ICSI appropriate to the service in the request and can also insert an ICSI appropriate to the service it is performing in appropriate SIP response messages.

An AS that acts as a SIP proxy or routeing B2BUA can include in the SIP request and response an indication that it is on the route of the SIP signalling and indicate the capabilities that it supports (including the ICSI) and if required can also indicate the associated address that can be used to send related requests.

## 9.4.2 Application Server handling of UE-terminating requests

The handling of UE-terminating requests is similar with the handling of UE-originating requests as defined in subclause 9.4.1.

## 9.4.3 Application Server handling of SIP registration

When the user is registered with the network and has been assigned a S-CSCF, the application servers, which are interested to know about the user registration events, should get a third party registration request generated by the S-CSCF. When the application server receives the request, the Application Server may perform a service triggered by a REGISTER. If the application server doesn't support this mechanism, it shall send back an error response to the S-CSCF. If the application server supports this mechanism, it shall treat this request as a notification from the network about the user's registration event and extract the important information from this request.

The application server may, depending on the Filter Criteria receive REGISTER requests indicating reregistration or deregistration events from the S-CSCF, so that the application server can update or release user's registration information.

The important information carried in the third party registration request are, the public user identity, the S-CSCF address, and the expiration time.

The application server can also extract user specific data from the REGISTER request, e.g. the IMSI for an Application Server that supports CAMEL services and information from the original REGISTER request included in the body.

Application Servers can also subscribe to the S-CSCF Registration Event Package after receiving the third party registration request. After subscribing to the event package with the S-CSCF, the application will expect to receive the notifications from the S-CSCF, which may carry the user's implicitly registered public user identities, the user's terminal current capabilities and the user's registration event information.

The application server can also obtain the user's implicitly registered public identities by accessing the HSS via Sh or Si interface.

An application server will require knowledge of a user's IMS subscription information if they are to correctly apply services. This information can be provided to the application server in two ways, either:

- a) Manually by provisioning. This is outside of the scope of this specification.
- b) Automatically from the HSS via the Sh and Si interfaces.

More information on these procedures is contained in 3GPP TS 24.229 [5].

## 9.4.4 Application Server handling of IP multimedia session release requests

### 9.4.4.1 Session release request terminated at the Application Server

When the application server receives a session release request, if the application server is acting as a user agent or a B2BUA, it shall send a 200 (OK) response to the entity that initiated the session release request.

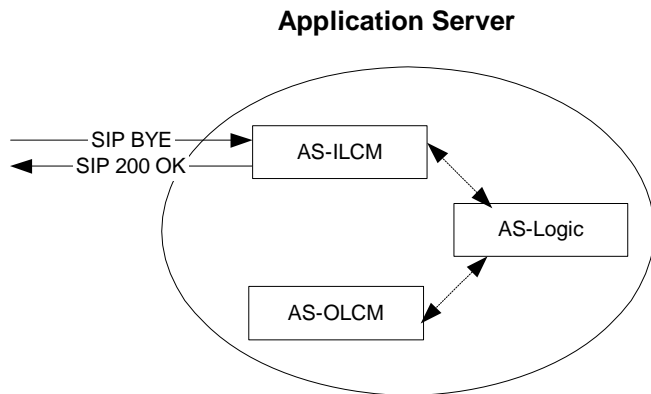


Figure 9.4.4.1.1: Release request terminated at the Application Server

9.4.4.2 Session release request proxied by the Application Server

When receiving a session release request, the application server may proxy the release request based on the route information in that request. This handling is typically used when the application server is in proxy mode.

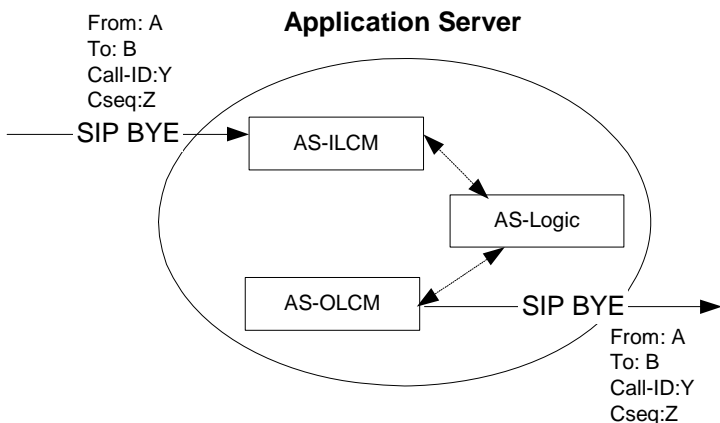


Figure 9.4.4.2.1: Release request proxied by the Application Server

9.4.4.3 Session release request initiated by the Application Server

If needed, the application server may initiate release requests to the entities involved in the dialogs the application server manages. Application servers may initiate release requests in either user agent or B2BUA mode.

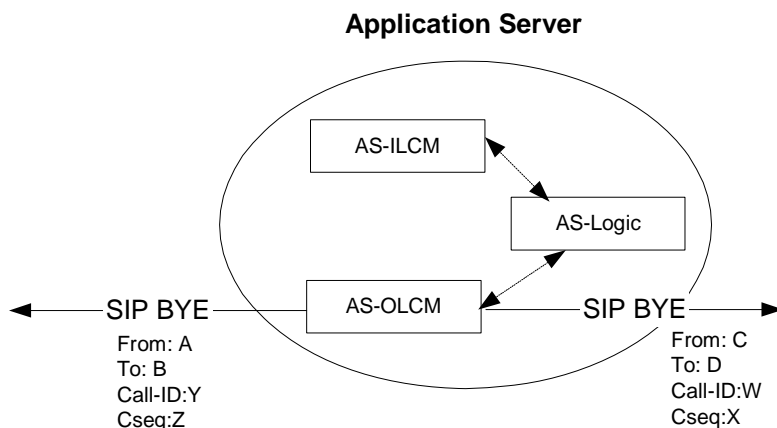


Figure 9.4.4.3.1: Release request initiated by the Application Server

### 9.4.5 Application server handling of IP multimedia charging

If an application server receives a third party REGISTER from the S-CSCF carrying the ICID, IOI and charging function addresses, the application server may store these parameters for charging purposes.

In an originating case, when processing an incoming initial request carrying the ICID, IOI, access network (IP-CAN) charging information and charging function addresses for this session, the application server shall pass these parameters in the outgoing message and may store the parameters for charging purposes.

In a terminating case, when processing an incoming initial request carrying the ICID, IOI, access network (IP-CAN) charging information and charging function addresses for this session, the application server shall pass these parameters in the outgoing message and may store the parameters for charging purposes.

When the application server is acting as an originating user agent as described in subclause 9.1.1.2 and initiates a session or a standalone transaction, it shall generate ICID itself. Charging function addresses may be allocated as locally preconfigured addresses. The application server may retrieve the charging addresses on Sh interface.

When the conflict occurs between the charging function address(es) received over the ISC interface and those received over the Sh interface, the address(es) received over the ISC interface should take precedence.

**NOTE:** The use of the Sh interface to retrieve charging function addresses is not intended as a general-purpose alternative to receiving charging function addresses from the ISC interfaces. Rather, it is meant to address a special case where the AS needs to interact with the charging system before initiating a request to a user when the AS has not received the third party REGISTER for that user.

For detailed information on transporting charging parameters between IMS entities using SIP, see 3GPP TS 24.229 [5].

---

## 10 IP multimedia session handling with IM-SSF Application Server

This subclause describes the functional architecture needed to support CAMEL interactions with the S-CSCF and the Transit Function in the IP Multimedia Subsystem. The IM-SSF is a SIP Application Server that interfaces SIP to CAP. The generic SIP Application Server behaviour of the IM-SSF is specified in clause 9 of the present document.

The detailed CAMEL procedures for IM-SSF Application Server are specified in 3GPP TS 23.278 [9].

---

## 11 IP multimedia session handling with an OSA-Service Capability Server

This subclause describes the functional architecture needed to support interactions with the S-CSCF and the Transit Function in the IP Multimedia Subsystem and the OSA-SCS. The OSA-Service Capability Server is a SIP Application Server which interfaces SIP to the OSA framework. The generic SIP Application Server behaviour of the OSC-SCS is specified in clause 9 of the present document.

The detailed OSA-SCS procedures for IMS Application Server are specified in 3GPP TR 29.998 [7].

---

## 12. IP multimedia session handling with an Charging Server

This clause describes the functional architecture needed to support interactions with the S-CSCF in the IP Multimedia Subsystem and Charging Server. The Charging Server is a specific SIP Application Server that performs the role of online charging mechanism for the Event Charging Function (ECF) and Session Charging Function (SCF).

The detailed procedures for Charging Server are specified in 3GPP TS 32.240 [20] and 3GPP TS 32.260 [21].

---

## 13 Media resource broker (MRB)

### 13.0 General

The Media Resource Broker (MRB) is a functional entity that is responsible for both collection of appropriate published MRF information and supplying of appropriate MRF information to consuming entities such as the AS. Therefore, the MRB is responsible for supporting the identification and selection of appropriate MRF resources.

The MRB supports the sharing of a pool of heterogeneous MRF resources by multiple heterogeneous applications. MRB assigns (and later releases) specific suitable MRF resources to calls as requested by the consuming applications, based on MRF attributes specified by the applications as well as other criteria.

The MRB may take the following kinds of information into account when assigning MRF resources to an application:

- the specific characteristics of the media resources required for the call or calls;
- the identity of the application;
- rules for allocating MRF resources across different applications;
- per-application or per-subscriber SLA or QoS criteria;
- capacity models of particular MRF resources; and
- if it can use the services of another (visited network) MRB.

There are two modes in which MRB can be utilized – Query and In-Line, as explained below. An instance of an MRB may simultaneously operate in both modes. Likewise, a given AS/application could employ Query mode on some calls and In-Line mode on others.

Query and In-Line modes of MRB have the following in common:

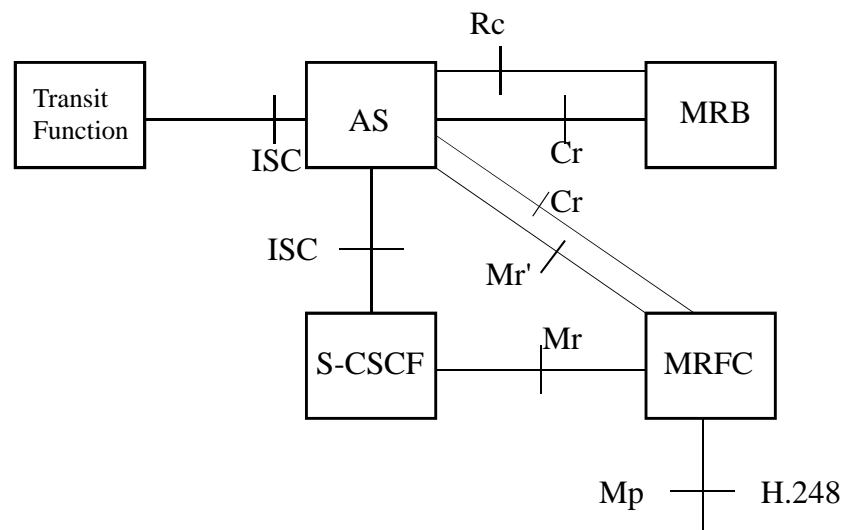
- the role of MRB is the same – assignment of MRF resources to calls as requested by applications;
- an application server provides the same kind of information to MRB on MRF attributes needed for a given call; and
- the way MRB acquires knowledge of MRF resources and other information needed to perform its role is the same (see subclause 13.3).

Query mode allows the application to:

- be the entity that determines when an MRF resource can be released;
- request and be assigned MRF resources for multiple calls in advance; and do that in a single request/response; and
- incrementally request more MRF resources or release resources that it determines aren't in fact needed.

An MRB can use the services of another MRB, either in In-Line mode or in Query mode, using the Mr, Mr' and Rc interfaces appropriately.

## 13.1 MRB Query Mode



**Figure 13.1.1: Query Mode**

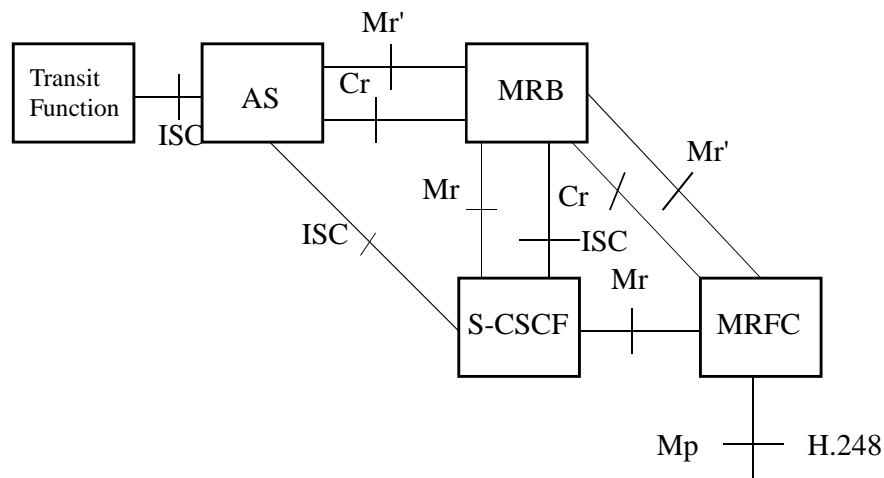
With Query mode, the AS queries the MRB with a request for media resources with certain attributes using the Rc interface. The MRB selects suitable MRF Resources, assigns them to that AS/application, and responds to the AS with the addresses of the selected MRF resources.

Once the AS receives the response from MRB, it sets up the call or calls to the MRFC either through the S-CSCF (ISC and Mr interface) or directly to the MRFC (Mr' interface), using the MRF address information supplied by MRB. Control packages are supported over the Cr interface.

When the AS/application is done using a MRF resource, it sends another message to MRB indicating so, and MRB returns that resource to the idle pool and acknowledges to the AS/application.



## 13.2 MRB In-Line Mode



**Figure 13.2.1: In-Line Mode**

With In-Line mode, the MRB is between the AS and the MRFC. The AS sends a request to establish a dialog to the MRB (using the Mr' interface, or via the S-CSCF using the ISC and Mr interface). The request can contain information relating to the kind of MRF required to handle that particular call. The MRB selects an appropriate MRF resource and sends the request along to the MRF (using the Mr' interface, or via the S-CSCF using the ISC and Mr interface). Subsequent messages in the same dialog between the AS and MRFC traverse the MRB (as well as the S-CSCF if that was in the path between the AS and the MRB, or between the MRB and the MRFC).

Control packages are supported over the Cr interface directly between AS and MRFC.

The MRB infers that the media resource is no longer needed when it sees a session release request from either the AS or MRFC.

## 13.3 MRB knowledge of MRF resources and other information

In order to perform its function, MRB may need the following kinds of information (this is not necessarily an exhaustive list):

- available MRF resources and their attributes; current and future. This may take into account planned and unplanned downtime and the scheduled addition/deletion or availability of MRF resources;
- rules for fair-share allocation across applications;
- capacity models for particular MRF resources; and
- reservations for future use of media resources (for example, for conferencing, or for anticipated traffic spikes for other applications such as a FreePhone application).

The above information can all be acquired by MRB through operations interfaces. However, it the MRB can also learn of available MRF resources and their characteristics via a direct MRB-MRF interface.

## Annex A (informative): Scalability and deployment considerations for IP multimedia service provision

This Annex is intended to guide the reader in deployment and real life issues.

This specification has provided a set of tools for the application developer and the application integrator to utilize in order to develop and deploy applications and provide services for the IP multimedia core network subsystem. However, practical deployments will need to consider certain scalability issues with the use or misuse of some of the tools specified in this specification.

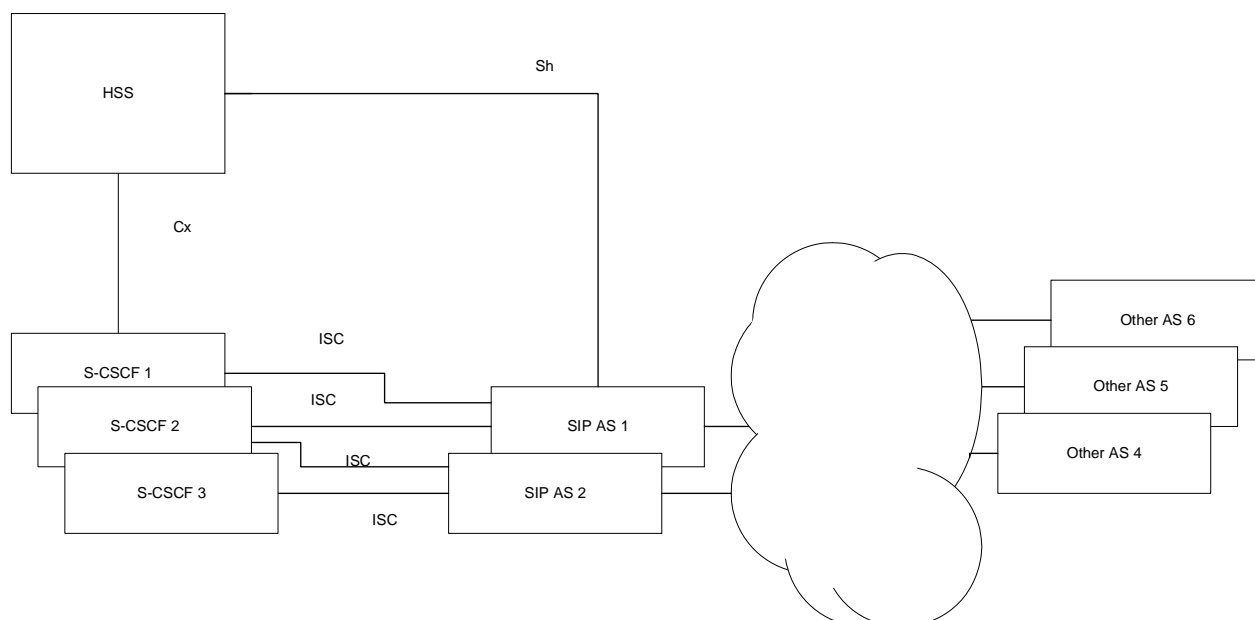
The architecture allows for any number of Application Servers to be connected to any number of S-CSCFs and Transit Functions, and any number of Application Servers to be involved in the initiation of a multimedia session. A scalability issue may arise if there are a large number of S-CSCF, Transit Functions and AS in a network.

Consideration should be given to the signalling propagation delays introduced when many Application Servers add themselves to the route to provide originating and terminating services for the calling and called parties.

A SIP Application Server may act as gateway function by forwarding an incoming request to external ASs beyond the IM CN subsystem. An external ASs will also send responses to IM CN subsystem via a SIP AS gateway. These other Application Servers can be located externally to the home network, and use the SIP Application Server as a gateway to the ISC interface. The interface between the SIP Application Server acting as a gateway, and other Application Servers is outside the scope of the present document.

There is another case where the external AS is connected with S-CSCF (or I-CSCF) via public ISP networks depending on the operators desire for network configuration hiding. S-CSCF or entities outside the S-CSCF may perform the interworking function.

Care must also be taken to the priority and order of contact of multiple Application Servers during a session in order to account for feature interaction issues.



**Figure A.1: Example hierarchical architecture for Application Servers**

Figure A.1 depicts a possible solution that shows how a S-CSCF (S-CSCF1 S-CSCF3) could be connected to a single AS (SIP AS1), while another (S-CSCF2) could be connected to more than one, in this case it is two (SIP AS1, SIP AS2). All S-CSCF will be connected to the HSS via Cx. A SIP AS may be connected to the HSS via Sh. SIP ASs may be connected to the IP network, which could allow them to contact Application Servers (e.g., either SIP ASs, or Other ASs).

Care should be taken to the transaction delays resulting of a high number of S-CSCF, Transit Functions and ASs on the session signalling path.

A possible application of this architecture is described below (see figure A.2).

While some applications need to discover the registration of a user on an event driven basis, many applications do not. For many applications an access to the HSS or other database to obtain the address of the S-CSCF that serves a user is sufficient to contact and initiate a session to that user, and others (such as basic call feature servers) do not require to be informed of the registration state or necessarily even need to know the identity of the user. It is therefore possible that the filter criteria are set in such a way that S-CSCF3 does not forward or notify SIP AS 3 of REGISTER requests. SIP AS3 would then need to determine registration status via other means (i.e. via IP network) not specified.

The number of Application Servers receiving REGISTER requests (i.e., SIP AS3) from an individual S-CSCF should be minimized.

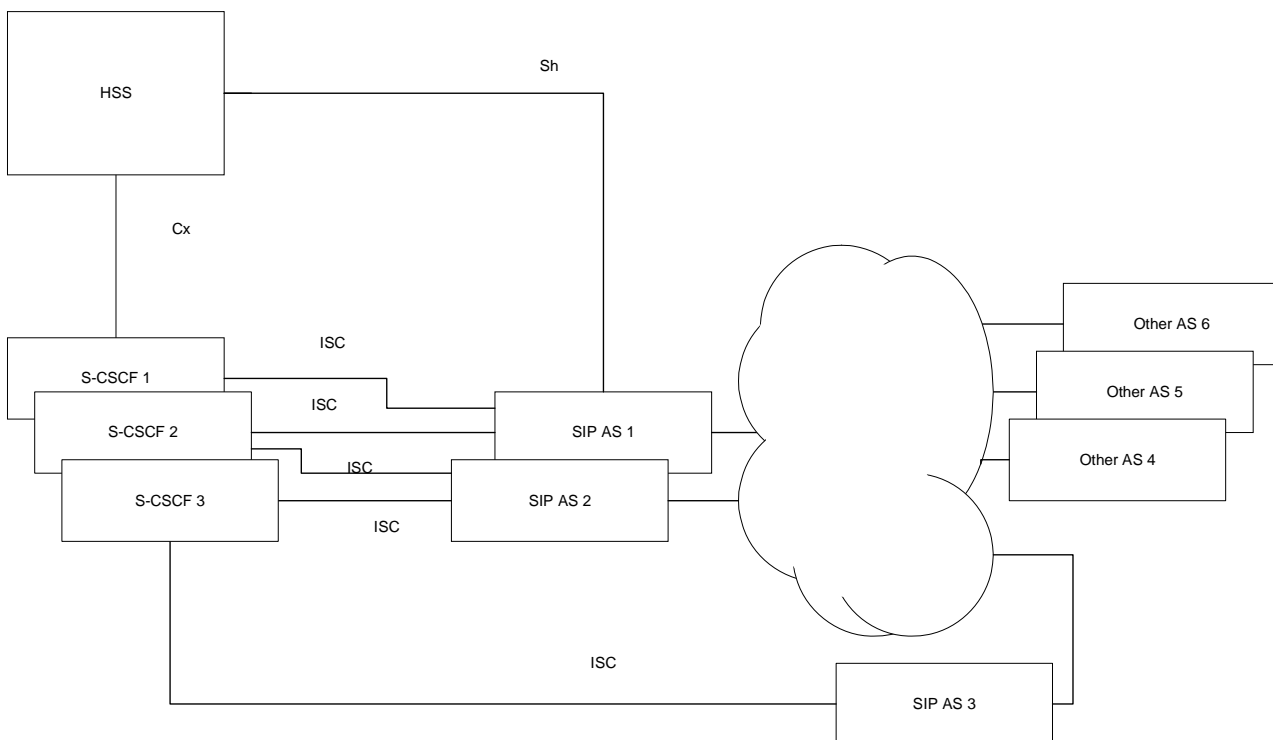


Figure A.2: Use of a hierarchy in a practical architecture for Application Servers

---

## Annex B (informative): Information flows for example services

This annex contains some informative example information flows that show the possible flow of information for some example services. These examples are intended only to help aid the understanding of the behaviour of the S-CSCF, MRFC and Application Servers for service provision for the IM CN subsystem and are not intended to recommend or specify how to create such services, (indeed the examples given may not even be a good idea for a practical implementation).

The following modes of operation are shown in these examples:

- Third Party Registration to Application Server subclause B.3.2;
- Application Server in Originating UA mode subclause B.3.2;
- Application Server in Redirect mode subclause B.1.3;
- Application Server in Terminating UA mode subclause B.3.1;
- Application Server in Proxy mode subclause B.1.4;
- Application Server in Third Party Call Control/B2BUA mode subclauses B.2.1, B.2.2, and B.2.3;
- Application Server with no involvement subclause B.1.4.

---

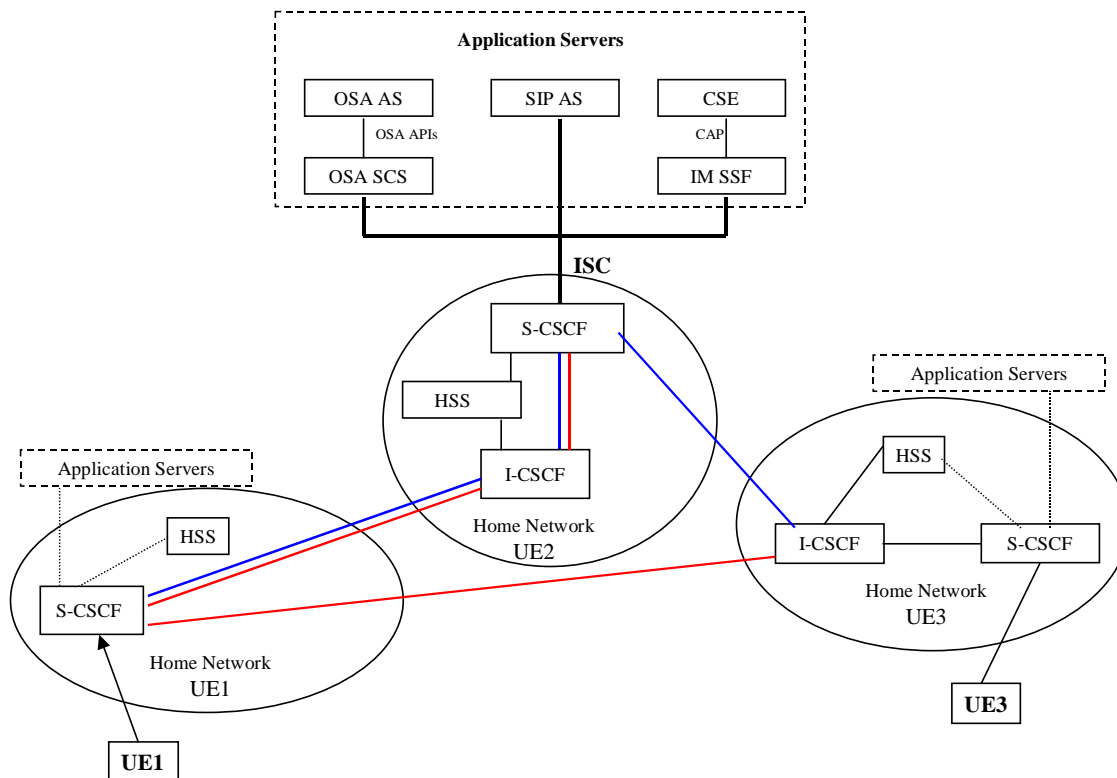
### B.1 Call forwarding example

#### B.1.1 Call forwarding through Application Servers

##### B.1.1.0 Introduction

Figure B.1.1.1 presents the network configuration for a call-forwarding scenario. Some interfaces between nodes have been omitted purely for clarity. In this configuration, the UE1 originates a call to the UE2. The UE2 is subscribed to a Call Forwarding (CF) service based on the Calling Line Identification (CLI). The CF service logic resides in an Application Server interfacing to the IM CN subsystem via the ISC interface. The Application Server is programmed to detect all incoming calls or terminating sessions with UE1's CLI and to instruct the S-CSCF to forward the calls/sessions to another destination, UE3, either directly or via the UE1. These two session forwarding scenarios are shown by the red and blue coloured flows. When the session redirection is carried out directly by the S-CSCF of the UE2, the network may notify the UE1 of its call/session redirection.

As shown in figure B.1.1.1, the Application Server may be a SIP AS, or an OSA AS or a CAMEL CSE. The latter two Application Servers interface the S-CSCF via the OSA SCS and IM SSF gateways, respectively.



**Figure B.1.1.1: Network configuration for the call forwarding examples**

In this configuration, the originating UE1 and the terminating UE3 are assumed to be in their respective home network. The UE2, not shown in figure B.1.1.1, may be either at its home network or roaming in a visited network.

The CF feature is invoked based on the detection of the originating party's CLI "pre-activated" for call forwarding. Upon invocation of the CFonCLI feature, the call will be forwarded to a pre-specified destination. These two steps and a few underlying assumptions are briefly described below:

### B.1.1.1 Service activation and programming

The UE2 activates its CFonCLI service and programs it with a Forward-to Number which is UE3's number, conditioning it to the originating party's line identity, CLI.

### B.1.1.2 Service invocation and control

The UE1 makes a call to the UE2. The CFonCLI is invoked and the call is forwarded to the UE3 following a "Session Redirection" that is initiated by either the S-CSCF or the UE1.

NOTE: 3GPP TS 23.228 [3] lists six redirection procedures as follows:

NOTE 1: Session Redirection initiated by S-CSCF to IMS;

NOTE 2: Session Redirection initiated by S-CSCF to CS-domain;

NOTE 3: Session Redirection initiated by S-CSCF to general endpoint;

NOTE 4: Session Redirection initiated by P-CSCF;

NOTE 5: Session Redirection initiated by UE;

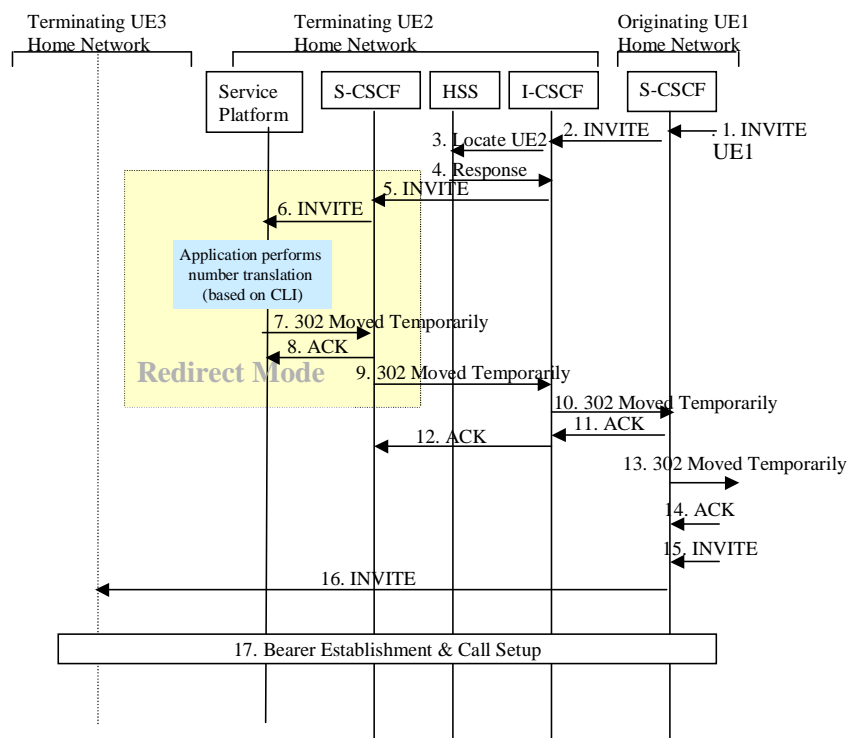
NOTE 6: Session Redirection initiated after Bearer Establishment.

## B.1.2 Assumptions

For the CFonCLI service invocation and service control procedure, the following are assumed to hold:

- Normal case scenario, showing successful cases only;
- Subscriber data of all three UE1, UE2 and UE3 are stored in their respective HSS;
- All call/session control for the UE1, UE2, and UE3 is done in their respective home network S-CSCF;
- The UE2 has already subscribed to the CFonCLI service with a service provider operating an Application Server where the service control logic resides;
- The pre-selected numbers (e.g., UE3) to which the originated calls are forwarded, are stored by the CFonCLI service control logic upon activation of the feature by the UE2.

## B.1.3 UE redirect based call flows



**Figure B.1.3.1: CFonCLI information flows with UE re-direct**

Figure B.1.3.1 presents the information flow for the invocation and control of the CFonCLI service based on the configuration of figure B.1.1.1.

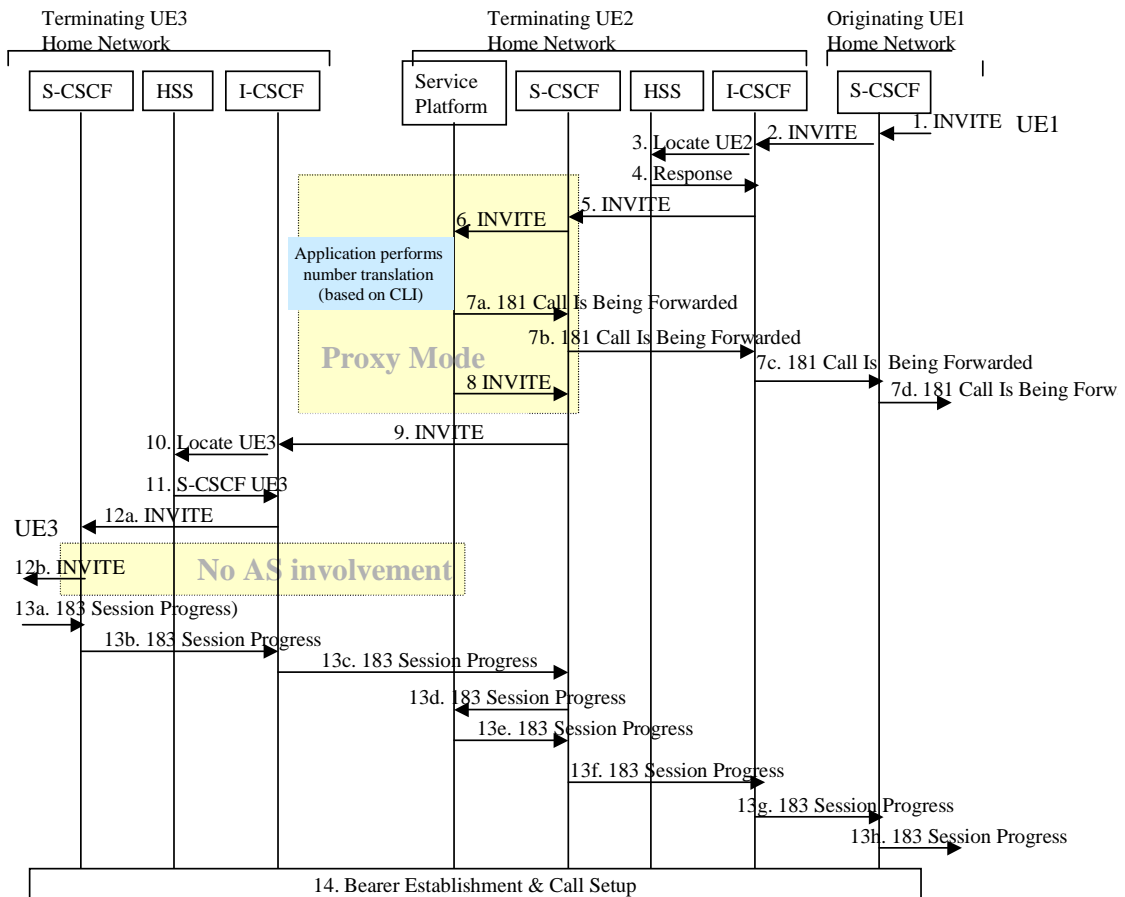
The UE1 initiates a call to UE2. The CFonCLI service logic is invoked in the Application Server when the S-CSCF for UE2 detects that service invocation is required. The call is forwarded to the UE3 by the UE1 according to the "Session Redirection initiated by UE" procedure. The UE3 accepts the (forwarded) call. A detailed description for each flow is given below:

- 1) The S-CSCF of UE1 receives a SIP INVITE request form UE1.

- 2) The I-CSCF of the UE2 receives a SIP INVITE request from the S-CSCF of the originating user, UE1. UE1's CLI is included in this INVITE request.
- 3) The I-CSCF of the UE2 queries the HSS to obtain the S-CSCF of the UE2.
- 4) The HSS returns the S-CSCF location.
- 5) The I-CSCF forwards the INVITE request to the S-CSCF of UE2.
- 6) Based on the information obtained from the UE2 Service Profile (during registration), the S-CSCF of the UE2 detects that the criteria for certain pre-defined triggers are met. The INVITE request is forwarded to the Application Server. The service logic is invoked in the Application Server.
- 7) Based on the outcome of the execution of the service logic, the Application Server instructs the S-CSCF to REDIRECT the session to UE3. The behaviour of the Application Server follows the description of a 'redirect server'. It sends the 302 Move Temporary response with UE3 as the redirect address to UE1. The Application Server plays no further part in the session establishment.
- 8) S-CSCF of UE2 sends ACK request back to the Application Server to acknowledge the receiving of the 302 (Moved Temporarily) response.
- 9) S-CSCF of UE2 forwards the 302 (Moved Temporarily) response to the I-CSCF of UE2.
- 10) The I-CSCF of UE2 forwards the 302 Move Temporary to the S-CSCF of UE1.
- 11) The S-CSCF of UE1 sends ACK request to acknowledge the receiving of the 302 Move Temporary.
- 12) The I-CSCF of UE2 forwards the ACK request to the S-CSCF of UE2.
- 13) The S-CSCF of UE1 forwards the 302 (Moved Temporarily) response to the next downstream hop.
- 14) The S-CSCF of UE1 receives the ACK request for that 302 (Moved Temporarily) response from the downstream hop.
- 15) The UE1 re-issues an INVITE request with UE3 as the destination.
- 16) The originating S-CSCF redirects the SIP INVITE request to the UE3's home network.
- 17) Bearer establishment & call setup between from the UE1 to the UE3 is performed following the procedure described in the basic call flow sections for originating, inter-network and terminating segments.

## B.1.4 S-CSCF based redirect call flows

Figure B.1.4.1 presents the information flow for the invocation and control of the CFonCLI service based on the configuration of figure B.1.1.1, where redirection is made by the S-CSCF after instructions from the service logic in the Application Servers.



**Figure B.1. 4.1: CFonCLI information flow with S-CSCF redirect**

The UE1 (located in the originating visited network) makes a call to UE2. The CFonCLI is invoked and the CFonCLI service logic is executed by an application residing in the Application Server.

The call is forwarded to the UE3 by the S-CSCF of UE2 according to the "Session Redirection" instructed by the Application Server. The S-CSCF sends a SIP 181Call Is Being Forwarded to UE1 and a SIP INVITE request to UE3. The UE3 accepts the (forwarded) call. A detailed description for each flow is given below:

- 1) - 6) are identical to flows by the same number in the UE Redirect example provided in B.1.3.
- (7a, 7b, 7c and 7d) The Application Server notifies the UE1 that the call is being forwarded, by sending a 181 (Call Is Being Forwarded) response.
- 8) The service logic forwards the INVITE request back to S-CSCF modifies the destination address by inserting the identity of the UE3. The Application Server is in SIP proxy mode.
- 9) The S-CSCF of UE2 forwards the modified INVITE request it received from the Application Server to the I-CSCF of UE3.
- 10) The I-CSCF of the UE3 queries the HSS to obtain the S-CSCF of the UE3.
- 11) The HSS returns UE3's S-CSCF location.
- (12a and 12b) The I-CSCF forwards the SIP INVITE request the UE3 via its S-CSCF.
- (13a, 13b, 13c, 13d, 13e, 13f, 13g, 13h and 13g) The UE3 accepts the incoming call and sends an 183 (Session Progress) response back to UE1.
- 14) Bearer establishment & call setup between from the UE1 to the UE3 is performed following the procedure described in the basic call flow subclauses for originating, inter-network and terminating segments.



---

## B.2 Announcement, conferencing and transcoding examples using MRFC

### B.2.1 Example information flow for a UE-originating IP multimedia session that results in playing an announcement

Figure B.2.1.1 shows an example of playing an announcement for a UE-originating IP multimedia session. An AS (acting as B2BUA) performs third party call control with the MRFC, where the S-CSCF is in the signalling path.

The "[x]" notation in the figure is an indicator of a unique SIP dialog. The "dot" notation on the AS line indicates B2BUA actions are taking place along with AS service logic. The 100 (Trying) responses are not shown in the figure, but it is assumed that a 100 (Trying) response is sent in response to each INVITE request.

The B2BUA AS interacts with the UE as usual to establish the dialog. The B2BUA AS interacts with the MRFC using a third party control model to establish the dialog. The B2BUA AS manages the interactions between the two dialogs.

The offer/answer model as defined in IETF RFC 3264 [15] is used for SDP negotiation between the AS/S-CSCF and the MRFC. The MRFC should always grant the requests from the AS (unless there is a resource problem). The MRFC responds to the INVITE request with a 200 (OK) response indicating the selected codec in the SDP. The MRFC will also reserve the requested local resources at that time. The selected codec is included by the B2BUA AS in the 183 (Session Progress) response to the UE. The receipt of the ACK request at the MRFC triggers the playing of the tone or announcement.

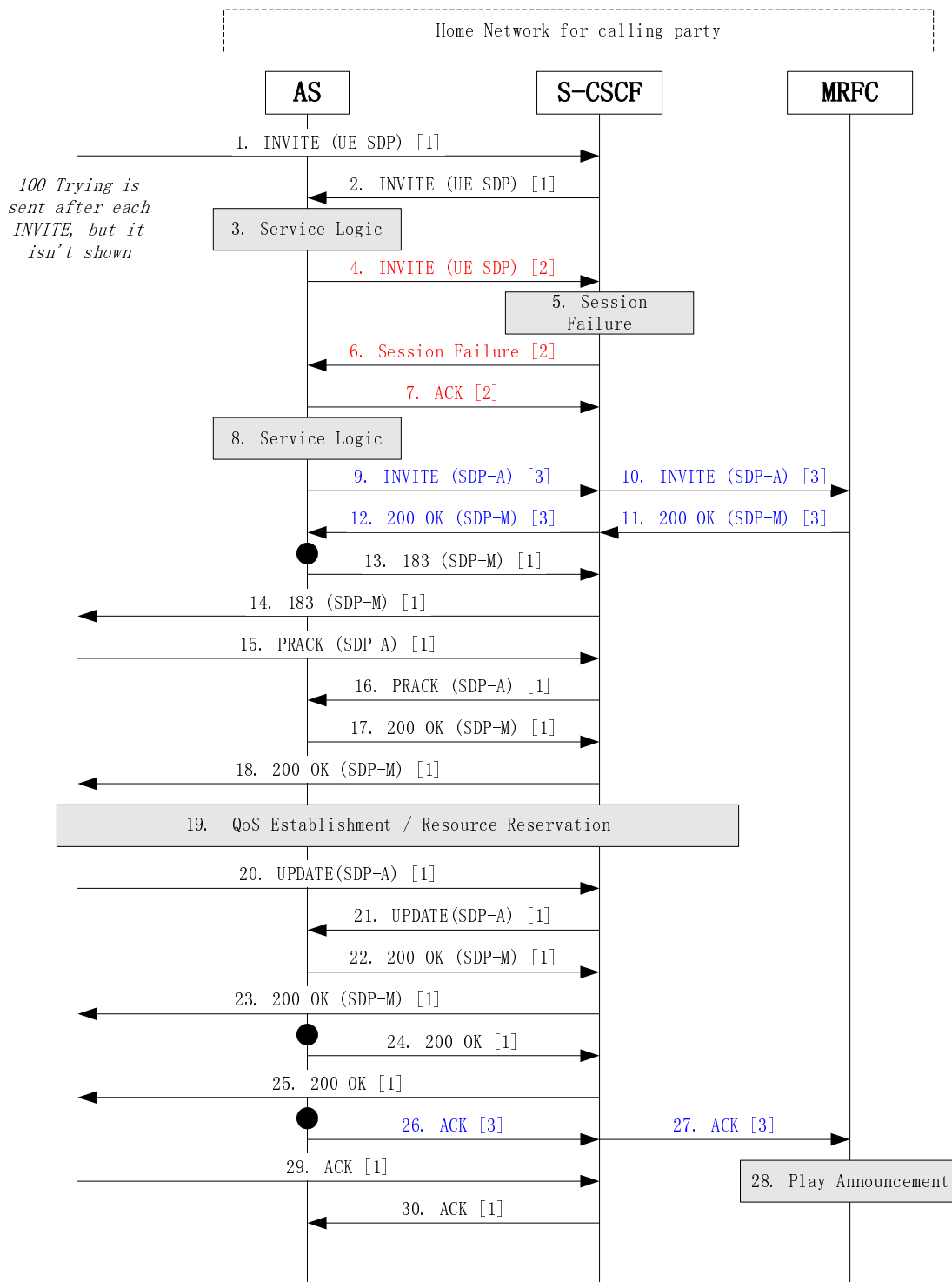


Figure B.2.1.1: Tones and announcements call flow

Notes for figure B.2.1.1:

- 1) INVITE request is received at the S-CSCF [Call-ID 1].
- 2) INVITE request is forwarded to an AS, based on the filter criteria.
- 3) The AS service logic determines to proceed with the call.
- 4) New INVITE request is sent towards destination, via the S-CSCF, to establish a new dialog [Call-ID 2].
- 5) S-CSCF experiences a failure, such as not being able to determine the next hop for the SIP URL.

- 6) Session failure returned to the AS.
- 7) ACK request returned to complete this dialog [Call-ID 2].
- 8) The AS service logic determines to play an announcement to the calling party.
- 9) New INVITE request is sent to the MRFC, via the S-CSCF, to establish a new dialog for playing an announcement [Call-ID 3]. Sufficient information is included to specify the details for the announcement.
- 10) S-CSCF relays the INVITE request to the MRFC.
- 11) The MRFC allocates the requested resource and returns a 200 (OK) response, with SDP-M indicating selected media.
- 12) S-CSCF relays 200 (OK) response to the AS.
- 13 - 30) The B2BUA AS manages the dialog for Call-ID 1 as normal, with the SDP-M supplied from the MRFC. The MRFC is instructed to play the announcement using the ACK request at flow 26 for Call-ID 3.

## B.2.2 Example information flow for a UE-originating IP multimedia ad-hoc conferencing session (multiparty call)

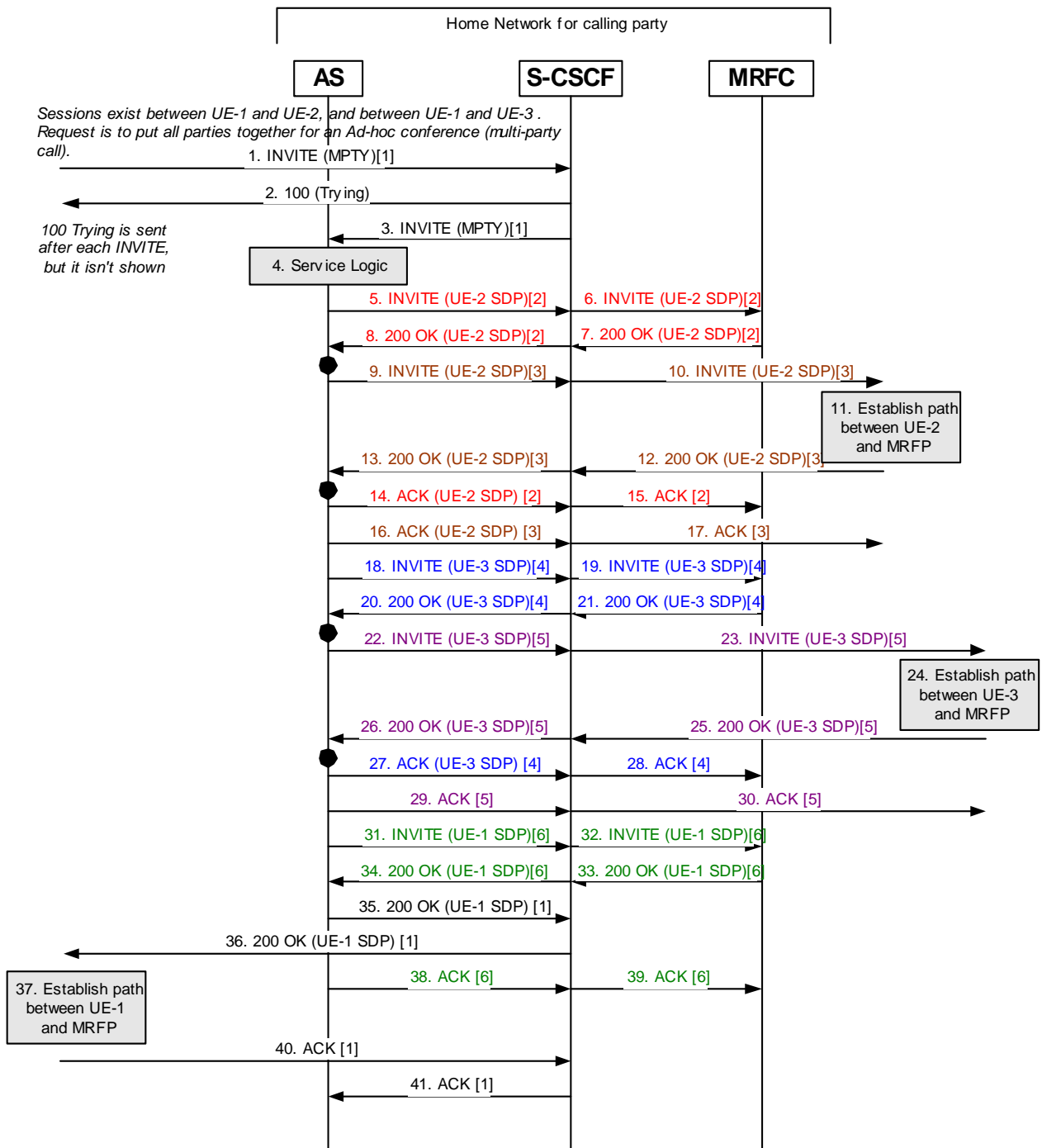
Figure B.2.1.1 shows an example of an ad hoc conference (multiparty call). An AS (acting as B2BUA) performs third party call control with the MRFC, where the S-CSCF is in the signalling path.

The "[x]" notation in the figure is an indicator of a unique SIP dialog. The "dot" notation on the AS line indicates B2BUA actions are taking place along with AS service logic. The 100 (Trying) responses are not shown in the figure, but it is assumed that a 100 (Trying) response is sent in response to each INVITE request.

The Application Server is in control of the ad hoc conference, is aware of the MRFC capabilities and is also operating as a B2BUA performing third party call control.

An INVITE request is generated from UE-1 indicating a desire to start a multiparty call (ad hoc conference) by taking the existing sessions, between UE-1 to UE-2 and UE-1 to UE-3, and bringing them together. The AS uses third party call control to request the conference facilities from the MRFC. A separate dialog is established from the AS to the MRFC for each of the three parties (UE-1, UE-2, UE-3). New dialogs are also established between the AS and each of the UE endpoints. The media from each UE is connected at the conferencing resource at the MRFP. The first INVITE request to the MRFC should contain a unique conference identifier. The same conference identifier will be used for subsequent INVITE requests to add or drop parties to the conference.

The offer/answer model as defined in IETF RFC 3264 [15] is used for SDP negotiation between the AS/S-CSCF and the MRFC. The MRFC should always grant the requests from the AS (unless there is a resource problem). The MRFC responds to the INVITE request with a 200 (OK) response indicating the selected media in the SDP. The MRFC will also reserve the requested local resources at that time and return the appropriate resource identifiers in the 200 (OK) response.



**Figure B.2.2.1: Ad hoc conference call flow**

Notes for figure B.2.2.1:

- 1) INVITE request received at S-CSCF from UE-1 indicating desire to start ad hoc conference (multiparty call) for the existing sessions between UE-1 to UE-2 and UE-1 to UE-3.
- 2) 100 (Trying) response returned.
- 3) INVITE request forwarded to AS.
- 4) AS performs service logic and allows attempt to start ad hoc conference.
- 5 - 8) New INVITE request sent to MRFC with a unique conference identifier to initiate multiparty call, and prepare dialog for UE-2 [Call-ID 2].
- 9 - 13) ReINVITE request sent to UE-2 to establish dialog between AS and UE-2 [Call-ID 3].

- 14 - 17) ACK request sent for Call-ID 2 and Call-ID 3.
- 18 - 21) New INVITE request sent to MRFC using the same conference identifier and prepare dialog for UE-3 [Call-ID 4].
- 22 - 26) ReINVITE request sent to UE-3 to establish dialog between AS and UE-3 [Call-ID 5].
- 27 - 30) ACK request sent for Call-ID 4 and Call-ID 5.
- 31 - 34) New INVITE request sent to MRFC using the same conference identifier and prepare dialog for UE-1 [Call-ID 6].
- 35 - 36) 200 (OK) response returned to UE-1 with SDP.
- 37) The session is established.
- 38 - 41) ACK request sent for Call-ID 1 and Call-ID 6.

### B.2.3 Example information flows for a UE-originating IP multimedia session that requires transcoding

The two figures B.2.3.1 and B.2.3.2 that follow illustrate the MRFC providing transcoding for a UE-originating session, where the MRFC is receiving directions from the AS operating as a B2BUA.

The "[x]" notation in the figure is an indicator of a unique SIP dialog. The "dot" notation on the AS line indicates B2BUA actions are taking place along with AS service logic. The 100 (Trying) responses are not shown in the figure, but it is assumed that a 100 (Trying) response is sent in response to each INVITE request.

The B2BUA AS interacts with the originating UE as usual to establish the dialog. The B2BUA AS interacts with the MRFC using a third party control model to establish the dialog with the called party after receiving the initial failure indication. The B2BUA AS manages the interactions between the two dialogs.

An INVITE request is generated from a UE. A 606 (Not Acceptable) response is received from the called party. The AS uses third party call control to request transcoding facilities from the MRFC. A separate dialog is established from the AS to the MRFC for each of the two parties. New dialogs are also established between the AS and each of the UE endpoints. The media from each UE is connected at the transcoding resource at the MRFP.

In the first figure B.2.3.1 below, the called party returns an indication of an acceptable codec. For this case, the request to the MRFC will include the appropriate codec for the called party and the offer/answer model as defined in IETF RFC 3264 [15] with the MRFC is used. In figure B.2.3.2 below, the called party does not indicate any SDP, which means that more steps will be required on the subsequent INVITE request to set up transcoding with the MRFC. An INVITE request without SDP is sent to the MRFC to get the list of codecs it supports. The AS then sends that list of codecs in the new INVITE request that it sends to the called party. The B2BUA function of the AS matches up the responses.

The offer/answer model is used for SDP negotiation between the AS/S-CSCF and the MRFC. The MRFC should always grant the requests from the AS (unless there is a resource problem). The MRFC responds to the INVITE request with a 200 (OK) response indicating the selected codec in the SDP. The MRFC will also reserve the requested local resources at that time. The selected codec is included by the B2BUA AS in the 183 (Session Progress) response to the UE. The receipt of the ACK request at the MRFC triggers the playing of the tone or announcement.

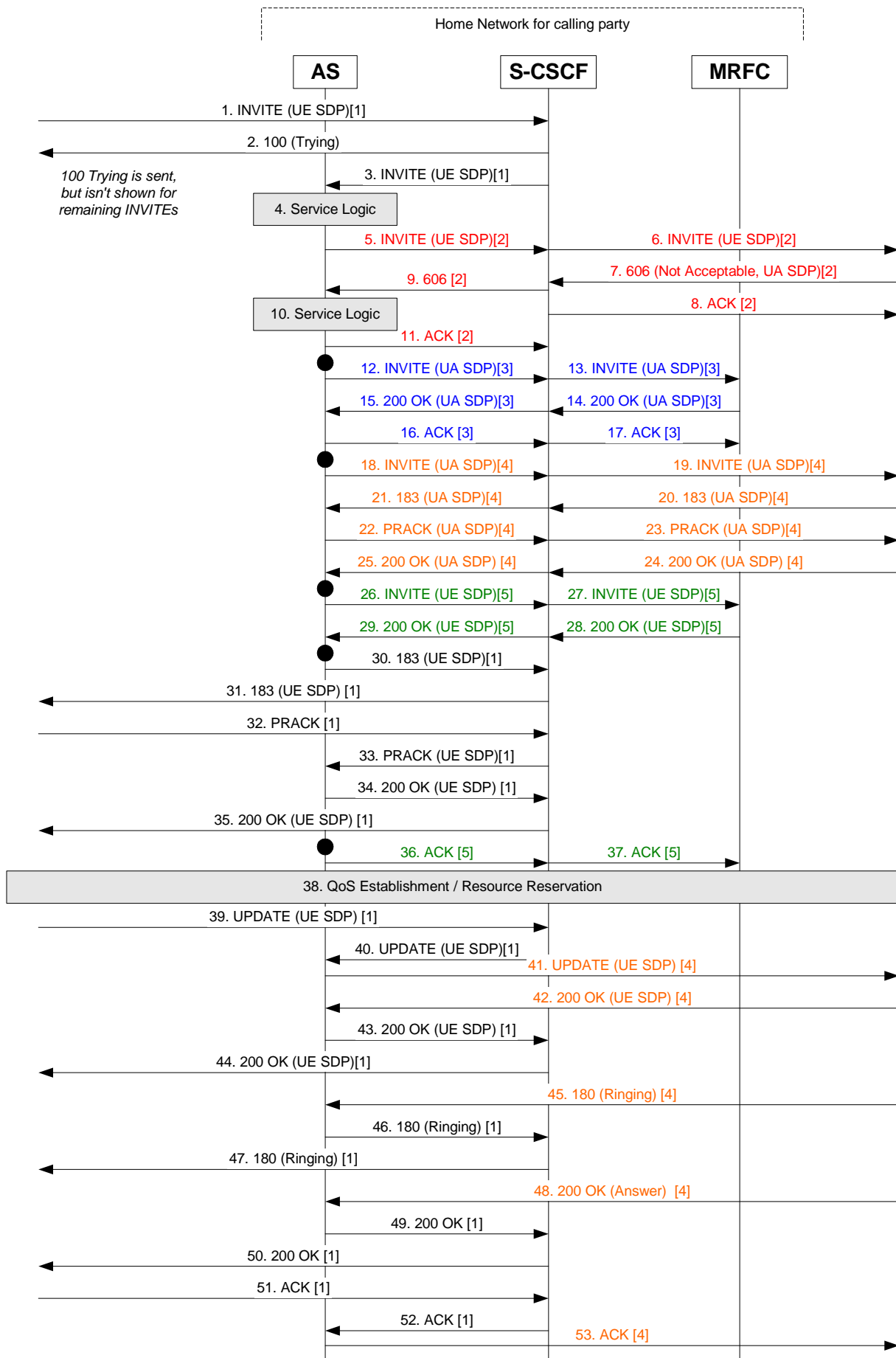
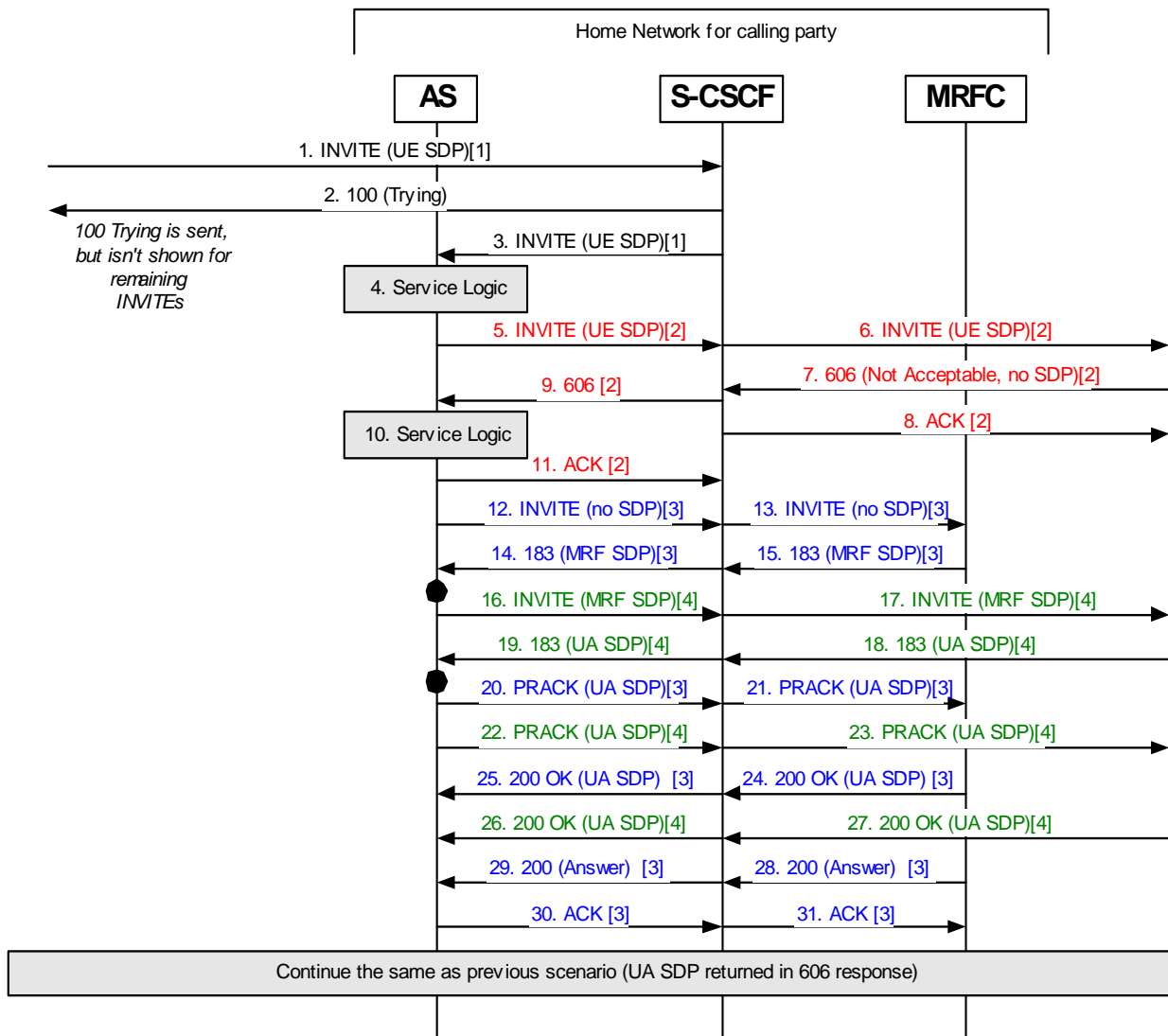


Figure B.2.3.1: Transcoding call flow (called party indicates codec)

Notes for figure B.2.3.1:

- 1) INVITE request received at S-CSCF from UE [Call-ID 1].
- 2) 100 (Trying) response returned.
- 3) INVITE request forwarded to an AS, based on filter criteria.
- 4) AS service logic determines to proceed with the call.
- 5) New INVITE request is sent towards destination, via the S-CSCF, to establish a new dialog [Call-ID 2].
- 6) S-CSCF forwards the INVITE request.
- 7) Called UA returns 606 (Not Acceptable) response to the INVITE request. Included in the response is an indicator that the offered codec is not acceptable plus information on what codec would be acceptable.
- 8) An ACK request is sent to the called UA to complete the dialog for Call-ID 2.
- 9) 606 (Not Acceptable) response is forwarded to the AS.
- 10) AS service logic determines that there is an MRFC that can perform the transcoding.
- 11) ACK request sent to S-CSCF to complete the dialog for Call-ID 2.
- 12 - 17) New INVITE request sent to MRFC to establish transcoding for called UA [Call-ID 3].
- 18 - 25) New INVITE request sent to called UA to establish session between UA and MRF [Call-ID 4].
- 26 - 29) New INVITE request sent to MRFC to establish transcoding for calling UE [Call-ID 5].
- 30 - 53) Normal call establishment procedures from here on, with B2BUA AS performing the appropriate signalling translations between the associated dialogs.



**Figure B.2.3.2: Transcoding call flow (called party codec negotiated)**

Notes for figure B.2.3.2:

- 1) INVITE request received at S-CSCF from UE [Call-ID 1].
- 2) 100 (Trying) response returned.
- 3) INVITE request forwarded to an AS, based on filter criteria.
- 4) AS service logic determines to proceed with the call.
- 5) New INVITE request is sent towards destination, via the S-CSCF, to establish a new dialog [Call-ID 2].
- 6) S-CSCF forwards the INVITE request.
- 7) Called UA returns 606 (Not Acceptable) response to the INVITE request. Included in the response is an indicator that the offered codec is not acceptable but there is no information on what codec would be acceptable (no SDP).
- 8) ACK request sent to called UA to complete the dialog for Call-ID 2.
- 9) 606 (Not Acceptable) response is forwarded to the AS.
- 10) AS service logic determines that there is an MRFC that can perform the transcoding.
- 11) ACK request sent to S-CSCF to complete the dialog for Call-ID 2.



- 12 - 15) New INVITE request sent to MRFC to establish transcoding for called UA and to get the list codecs supported by the MRF [Call-ID 3].
- 16 - 19) New INVITE request sent to called UA with SDP for all codecs supported by the MRF to establish session between UA and MRF [Call-ID 4]. UA returns SDP with acceptable codecs.
- 20 - 23) A new offer with the codecs provided by the UA is sent in PRACK request and the 200 (OK) response indicates the selected codec.
- 24 - 31) Acknowledgements sent to complete Call-ID 3.

Call establishment procedures from here on are common with the previous transcoding call flow.

---

## B.3 Example information flows for a voicemail service

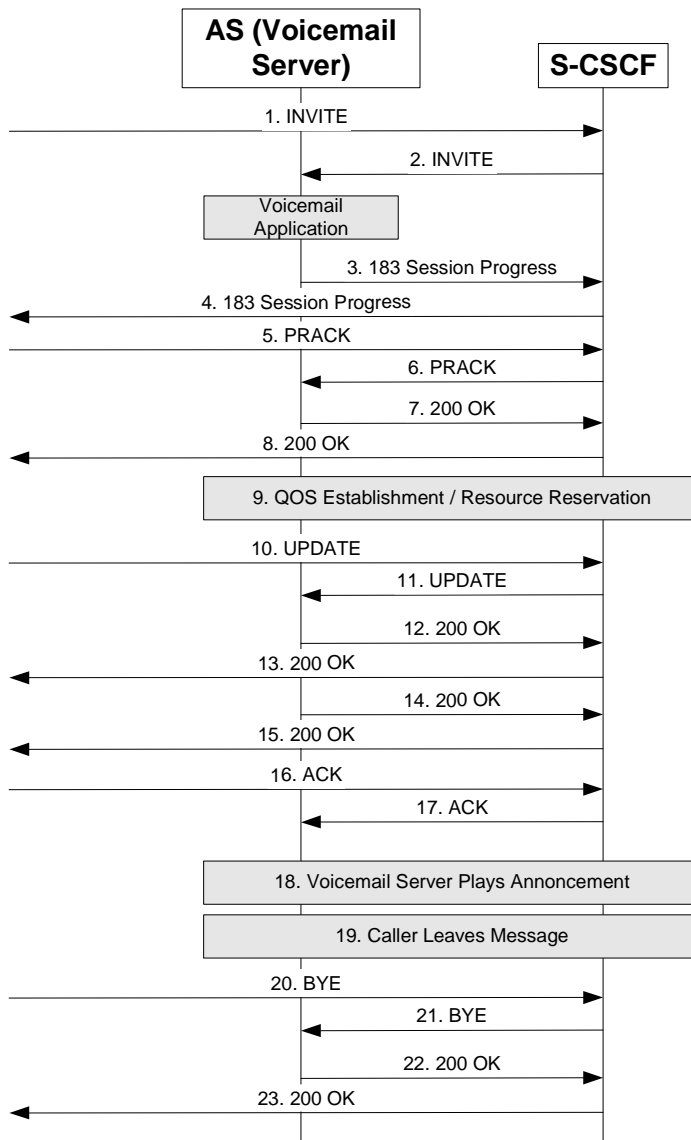
### B.3.1 User out of coverage message recording

Figure B.3.1.1 shows a possible scenario of an Application Server, which acting as a terminating UA performs the function of a Voicemail Server in order to terminate a call and record a message on behalf of a UE that is out of coverage or powered off. The Application Server's use of the MRF to record a message is not shown in this example.

An initial INVITE destined for a UE that is not currently IMS registered is forwarded to a S-CSCF. The Default Filter Criteria in the S-CSCF indicates that for the case of an unregistered user the INVITE request should be forwarded to the Voicemail and Announcement Server.

Upon receiving the INVITE request the Voicemail and Announcement Server determines that the destination UE has subscribed to the Voicemail Service (possibly by downloading some subscriber profile information via the Sh interface). The Voicemail and Announcement Server therefore in addition to playing an announcement to inform the caller that the called party is either powered off or out of coverage also informs the caller that he may leave a message for the called party.

The calling party leaves a message for the called party and then hangs up the call by sending a BYE request.



**Figure B.3.1.1: Voicemail server records messages**

Notes for figure B.3.1.1:

NOTE: For simplicity the 100 (Trying) response returned or received by the S-CSCF in response to requests is omitted from figure B.3.1.1.

- 1) INVITE request destined for an unregistered user is received at the S-CSCF.
- 2) Based on trigger point of the initial Filter Criteria S-CSCF proxies the INVITE request to the AS (Voicemail Server).
- 3 - 4) The AS starts the voicemail application and responds with a 183 (Session Progress) response containing SDP which is proxied back to the caller by the S-CSCF.
- 5 - 8) The caller responds with a PRACK request containing SDP, which the S-CSCF proxies to the AS and the AS responds with a 200 (OK) response containing SDP which the S-CSCF proxies back to the caller.
- 9) QOS establishment and resource reservation takes place.
- 10 - 13) After completing resource reservation the caller sends a UPDATE request containing SDP which is proxied by the S-CSCF to the AS which responds with a 200 (OK) response containing SDP which is proxied back to the caller by the S-CSCF.

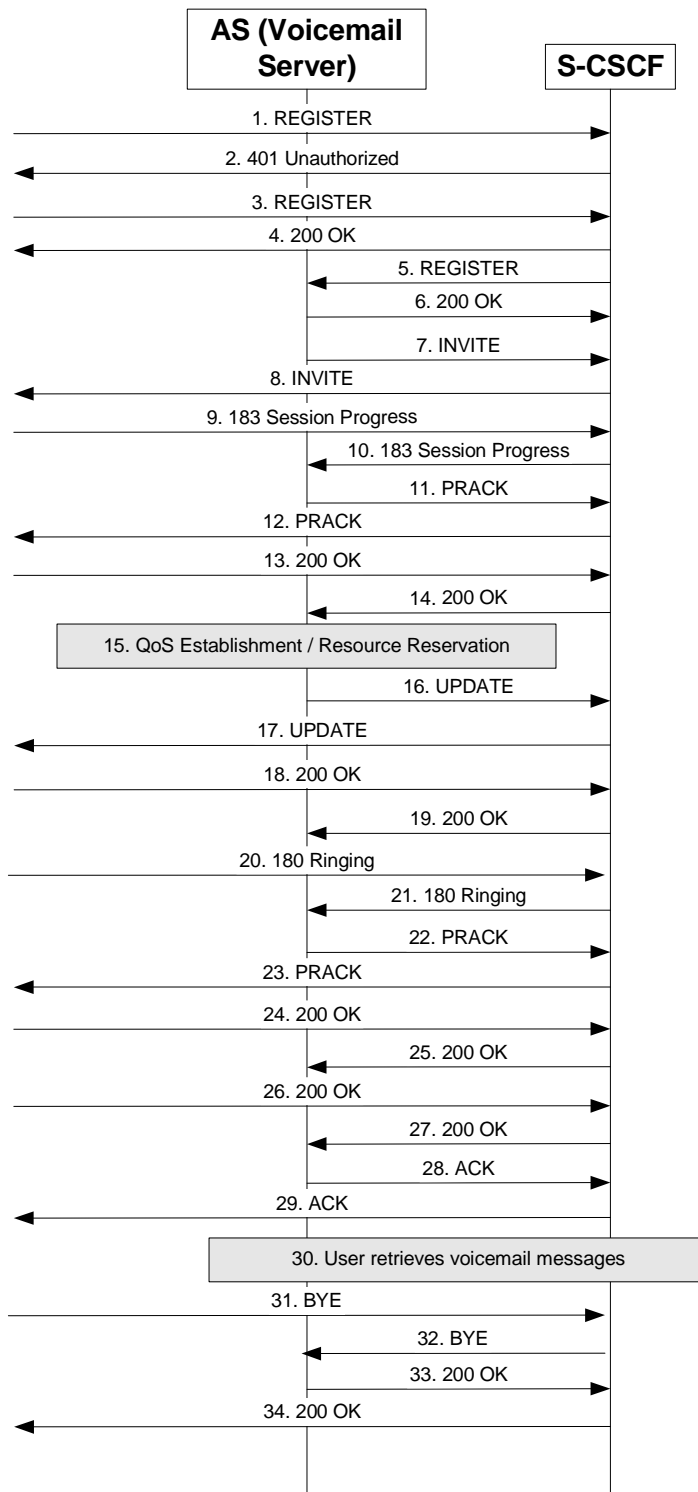
- 14 - 15) The AS then sends a 200 (OK) response to the initial INVITE request which the S-CSCF proxies to the caller.
- 16 - 17) The caller returns an ACK request to the 200 (OK) response.
- 18) The AS plays an announcement using the session established indicating that the caller is powered off but that the caller may leave a message.
- 19) The caller leaves a message using the session established.
- 20 - 21) The caller hangs up by sending a BYE request which the S-CSCF proxies to the AS.
- 22 - 23) The AS responds with a 200 (OK) response, which the S-CSCF proxies back to the caller.

## B.3.2 User IMS registers voice mail service plays back messages

Figure B.3.2.1 shows the scenario when the UE that has subscribed to a voicemail service with a feature enabled that contacts the user upon registration informing him of any recorded messages. The Application Server's use of the MRF to play announcements and to select and play the recorded messages is not shown in this example.

The Filter Criteria downloaded by the S-CSCF indicates that a third party REGISTER request should be sent to the Voicemail Server. Upon receiving the third party registration of the UE, the Voicemail Server acting as an originating UA contacts the UE by sending an INVITE request to inform him that he has voicemail messages recorded while he was not registered.

The user listens to the messages played back by the voicemail server, (only streaming class QOS is required for this session) and then terminates the session with a BYE request.



**Figure B.3.2.1: Upon registration voicemail server replays messages**

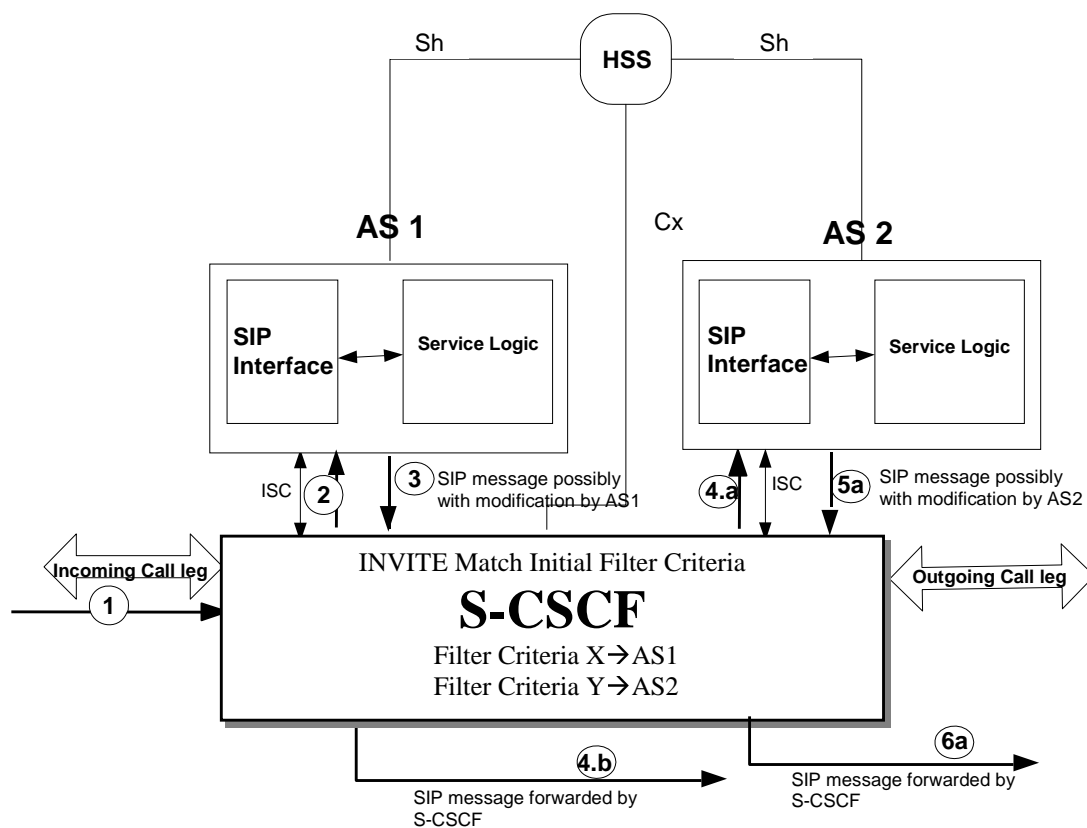
Notes for figure B.3.2.1:

NOTE: For simplicity the 100 (Trying) response returned or received by the S-CSCF in response to requests is omitted from figure B.3.2.1.

- 1 - 4) The UE sends a REGISTER request to the S-CSCF which authenticates with a 401 (Unauthorized) response challenge with the authentication response being supplied in a second REGISTER request. The registration completes with a 200 (OK) response from the S-CSCF to the UE.
- 5 - 6) The S-CSCF downloads Filter Criteria for the UE from the HSS which indicates the S-CSCF should send a third party REGISTER request on behalf of the UE to an AS that performs a voicemail service. The AS responds to the REGISTER request with a 200 (OK) response.
- 7 - 8) The AS downloads subscriber data for the subscriber (possibly from the HSS via the Sh interface) that indicates that the subscriber has enabled a feature that has the voicemail application contact the subscriber upon registration to deliver recorded messages. The AS sends an INVITE request containing SDP for the UE to the S-CSCF which proxies it to the UE.
- 9 - 10) The UE responds with 183 (Session Progress) response containing SDP which the S-CSCF proxies to the AS.
- 11 - 14) The AS sends a PRACK request, which the S-CSCF proxies to the UE and the UE respond with a 200 (OK) response which the S-CSCF proxies to the AS.
- 15) QOS establishment and resource reservation takes place.
- 16 - 19) The AS sends an UPDATE request, which the S-CSCF proxies to the UE and the UE responds with a 200 (OK) response which the S-CSCF proxies to the AS.
- 20 - 21) The UE sends a 180 (Ringing) response indicating that it is alerting the user which the S-CSCF proxies to the AS.
- 22 - 25) The AS to indicate receipt of the 180 (Ringing) response sends a PRACK request which the S-CSCF proxies to the UE and the UE responds with a 200 (OK) response which the S-CSCF proxies to the AS.
- 26 - 27) When the subscriber answers the UE sends a 200 (OK) response to the initial INVITE request which the S-CSCF proxies to the AS.
- 28 - 29) The AS acknowledges the 200 (OK) response with an ACK request which the S-CSCF proxies to the UE.
- 30) The AS plays an announcement indicating the number of messages stored and then plays back the messages to the UE using the session established.
- 31 - 32) The UE hangs up by sending a BYE request, which the S-CSCF proxies to the AS.
- 33 - 34) The AS responds with a 200 (OK) response, which the S-CSCF proxies back to the UE.

## Annex C (informative): Example for Initial filter criteria triggering

This example applies both for UE-originating and UE-terminating procedures. But we assume this is a call UE-originating procedure. User has registered with the network. Its filter criteria and addresses of the assigned application servers have been downloaded to its S-CSCF during registration via Cx interface. Also, the application server specific data may have been downloaded via the Sh interface to the application server during registration.



**Figure C.1: Initial Filter Criteria Triggering Example**

There is a flow example in figure C.1:

In this example, two application servers are assigned to provide additional services to a subscriber and they are showed as AS1 and AS2 in this example.

1. User initiates a SIP session by sending a SIP initial request to its S-CSCF.
2. On receiving this request, the S-CSCF evaluates the SPTs and checks if they match the initial filter criteria X for AS1. If they match, the S-CSCF forwards this request to AS1.
3. The AS1 performs any needed service logic based on the Service Key and sends the SIP request possibly with service related modification back to the S-CSCF.
- 4.a On receiving the request from the AS, the S-CSCF evaluates the SPTs and checks if they match the initial filter criteria Y for AS2. If they match the S-CSCF forwards the request to the associated Application Server AS2.
- 4.b If the request doesn't match any further filter criteria, the S-CSCF forwards this request to the next hop based on the route decision.
- 5.a The AS2 performs any needed service logic based on the Service Key and sends the SIP request possibly with service related modification back to the S-CSCF.

6.a The S-CSCF checks the request sent by AS2 and finds that no initial criteria is matched, then the S-CSCF forwards this request to next hop based on the route decision.

## Annex D (informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	Re v	Subject/Comment	Old	New	WG doc
Nov 2000		N1-001300			First draft created. Presented to CN1 meeting #14.			
21/11/00		N1-001352			V 0.1.0 created based on discussion in CN1#14. Additional clause on OSA API added.			
22/11/00		N1-001386			V 0.2.0 created based on discussion in CN1#14. The clause on scope modified.			
28/11/00		N1-001448			V 0.3.0 created based on discussion in CN1/SA2 joint meeting. The title modified.			
Jan 2001		N1-010069 NJ-010102			V0.3.1 created. Specification number TS 23.218 allocated to TS 23.cde.			
16/1/01		NJ-010106			V0.4.0 created. Clause 8 on OSA API updated to include the proposal in NJ-010104 agreed at joint CN1/2/4 meeting on 23.218.			
Mar 2001		N1-010762			V0.5.0 created. Clause 6.5 updated to include the proposal in NJ-010117 agreed at the joint CN1/2/3/4 Feb meeting in Sophia. Reference to Visited Network updated.			
Jun 2001		N1-010981			V0.5.1 created. Informative Annex B created containing N1-010749 agreed at Joint CN1/2/3/4 meeting in Puerto Rico.			
Aug 2001		N1-011090			V0.5.2 created. Section 5 updated to include the proposals in N1-010982, N1-011013 and N1-011043; Section 6 updated to include the proposals in N1-011044 and N1-011045, agreed at CN1#18 and joint CN1/2/3/4 meetings in Dresden.			
Sep 2001		N1-011365			V0.6.0 created. Document layout reorganized and content updated to conform to proposal in N1-011277; Section 6 and Section 9 updated to include the proposals in N1-011342, agreed at CN1#19 meeting in Helsinki.			
Oct 2001		N1-011522			V.0.7.0 created. Appendix B.1 added based on N1-011423 agreed at CN1#19bis meeting in Sophia Antipolis			
Oct 2001		N1-011707			V.0.8.0 created using Tdocs: N1-011596, N1-011597, N1-011599, N1-011600	0.7.0	0.8.0	
Nov 2001		N1-011867			V.0.9.0 created using Tdocs: N1-011751, N1-011778	0.8.0	0.9.0	
Dec 2001		NP-010640 N1-020033			V.1.0.0 created using Tdocs: N1-011999, N1-012051 agreed at CN#21 in Cancun. To be presented for information at CN#14	0.9.0	1.0.0	
Jan 2002		N1-020343			V.1.1.0 created using Tdocs: N1-020035, N1-020036, N1-020069, N1-020071 N1-020072, N1-020107, N1-020109, N1-020110, N1-020114, N1-020115 N1-020116, N1-020119 N1-020137, N1-020153, N1-020156, N1-020164 agreed at CN1 SIP Adhoc 0102 in Phoenix.	1.0.0	1.1.0	
Feb 2002		N1-020552			V.1.2.0 created using Tdocs: N1-020231, N1-020385, N1-020387, N1-020392, N1-020393, N1-020448, N1-020450, N1-020451, N1-020452, N1-020453 agreed at CN1#22 in Sophia Antipolis, and corrected implementation error of N1-020156.	1.1.0	1.2.0	
Feb 2002					V.2.0.0 created using Tdocs: N1-020607, N1-020620, N1-020633, N1-020634, N1-020637, N1-020653, N1-020661, N1-020662, N1-020667 agreed at CN1#22 bis in Oulu.	1.2.0	2.0.0	
Mar 2002					Editorial clean-up by ETSI/MCC.	2.0.0	2.0.1	
Mar 2002	TSG CN#1 5	NP-020047			The draft was approved and decided to be 'frozen', and 3GPP TS 23.218 was then to be issued in Rel-5 with the needed new RFC numbers allocated in NP-020134 incorporated.	2.0.1	5.0.0	
Jun 2002	NP-16	NP-020226	002	3	HSS providing to the S-CSCF the subset of the relevant end user profile	5.0.0	5.1.0	N1-020972
Jun 2002	NP-16	NP-020226	003	10	Clarification on SPI related text	5.0.0	5.1.0	N1-021405
Jun 2002	NP-16	NP-020226	004	4	Passing charging correlation information	5.0.0	5.1.0	N1-021423
Jun 2002	NP-16	NP-020226	006	1	Correction of terminology in 23.218 regarding Offer-counter offer answer	5.0.0	5.1.0	N1-020951
Jun 2002	NP-16	NP-020226	012	5	Update of the S-CSCF AS relationship, for REGISTER	5.0.0	5.1.0	N1-021425
Jun 2002	NP-16	NP-020226	014	1	User profile filter criteria updates	5.0.0	5.1.0	N1-021384



Jun 2002	NP-16	NP-020226	015	1	Add references for Sh and Si interfaces	5.0.0	5.1.0	N1-021385
Jun 2002	NP-16	NP-020226	016	1	SIP Application Server acting as a Gateways to an external Application Server; and OSA API usage.	5.0.0	5.1.0	N1-021404
Jun 2002	NP-16	NP-020226	017	1	Clarification to Handling of IP multimedia registration for barred public user identities	5.0.0	5.1.0	N1-021424
Jun 2002	NP-16	NP-020226	019		Correction of COMET to UPDATE in 23.218	5.0.0	5.1.0	N1-021252
Sep 2002	NP-17	NP-020373	021	1	Service profiles and implicitly registered public user identities	5.1.0	5.2.0	N1-021828
Sep 2002	NP-17	NP-020373	022	2	Clarification on specialized charging server	5.1.0	5.2.0	N1-021859
Sep 2002	NP-17	NP-020373	025	1	Clarification on location information for IMS	5.1.0	5.2.0	N1-021829
Sep 2002	NP-17	NP-020373	026	1	Proposed change of term SPI to SPT	5.1.0	5.2.0	N1-021830
Sep 2002	NP-17	NP-020373	027	1	Support of originating requests from Application Servers	5.1.0	5.2.0	N1-021831
Dec. 2002	NP-18	NP-020552	029	1	Clarification on CCF/ECF addresses	5.2.0	5.3.0	N1-022142
Dec. 2002	NP-18	NP-020553	030	3	Clarification on MRFP reference point	5.2.0	5.3.0	N1-022468
Dec. 2002	NP-18	NP-020552	031	1	Support of originating requests from Application Servers	5.2.0	5.3.0	N1-022144
Dec. 2002	NP-18	NP-020552	033		Addition of Request-URI as SPT	5.2.0	5.3.0	N1-022297
Dec. 2002	NP-18	NP-020552	034	1	Clarifications on Annex C (Informative)	5.2.0	5.3.0	N1-022469
Dec. 2002	NP-18	NP-020552	038	1	Clarification to use of Service Information	5.2.0	5.3.0	N1-022475
Mar 2003	NP-19	NP-030045	040	2	Clarification on Sh interface for charging purposes	5.3.0	5.4.0	N1-030309
Mar 2003	NP-19	NP-030046	042		Correction related to implicit public user identities in third party REGISTER	5.3.0	5.4.0	N1-030197
Jun 2003	NP-20	NP-030272	043	5	Correction on Handling of MO request	5.4.0	5.5.0	N1-030943
Jun 2003	NP-20	NP-030272	044	1	Corrections regarding SPTs and Filter Criteria handling on REGISTER request	5.4.0	5.5.0	N1-030516
Jun 2003	NP-20	NP-030272	046	1	Clarifications on SPT.	5.4.0	5.5.0	N1-030517
Jun 2003	NP-20	NP-030272	048		Service Key Clarification	5.4.0	5.5.0	N1-030663
Jun 2003	NP-20	NP-030272	051	1	S-CSCF behavior correction to enable call forwarding	5.4.0	5.5.0	N1-030855
Jun 2003	NP-20	NP-030272	055	1	Filtering of unknown header fields and header parameters	5.4.0	5.5.0	N1-030924
Sept 2003	NP-21	NP-030411	057		Removal of Incorrect Information	5.5.0	5.6.0	N1-031070
Dec 2003	NP-22	NP-030475	053	3	Flow number corrections in Annex B	5.6.0	5.7.0	N1-031630
Dec 2003	NP-22	NP-030482	059		Corrections on charging specification number	5.7.0	6.0.0	N1-031468
Mar 2004	NP-23	NP-040032	064	1	Dh interface	6.0.0	6.1.0	N1-040158
Mar 2004	NP-23	NP-040032	066	2	Initiating Back to Back User Agent	6.0.0	6.1.0	N1-040472
Sep 2004	NP-25	NP-040384	69		IFC process termination at R-URI change	6.1.0	6.2.0	N1-041440
Sep 2004	NP-25	NP-040384	70	1	Third party registration optimization	6.1.0	6.2.0	N1-041562
Mar 2005	NP-27	NP-050069	76		Filter criteria matching and generation of third-party REGISTER request for network-initiated deregistration	6.2.0	6.3.0	N1-050223
Mar 2005	NP-27	NP-050073	072		Resolution of references to 24.228	6.2.0	6.3.0	N1-050061
Mar 2005	NP-27	NP-050073	074	1	Default handling	6.2.0	6.3.0	N1-050288
Dec 2005	CT-30	CP-050550	079		Mobile originated request unregistered	6.3.0	7.0.0	C1-051428
Mar 2006	CT-31	CP-060160	0080	2	Change of originating and terminating terminal terminology	7.0.0	7.1.0	C1-060122
Mar 2006	CT-31	CP-060124	0081	1	Editorial corrections	7.0.0	7.1.0	C1-060122
Mar 2006	CT-31	CP-060124	0082	-	Correction for the description of the contents of the clauses	7.0.0	7.1.0	C1-060409
Jun 2006	CT-32	CP-060274	0086	1	Amend the playing announcement call flow	7.1.0	7.2.0	C1-061081
Jun 2006	CT-32	CP-060262	0085	1	3Rd party registratin clarification	7.1.0	7.2.0	C1-061005
Sept 2006	CT-33	CP-060466	0089	2	Impact of GRUU on Service Control in 23.218	7.2.0	7.3.0	C1-061364
Sept 2006	CT-33	CP-060468	0090	1	Clarification of Cases of Downloading iFC to S-CSCF	7.2.0	7.3.0	C1-061704
Sept 2006	CT-33	CP-060468	0091	1	S-CSCF handling of terminations when AS modifies the Req-URI	7.2.0	7.3.0	C1-061760
Oct 2006					Version 7.3.1 created by MCC to correct styles	7.3.0	7.3.1	
Nov 2006		CP-060660	0092	3	Introduction of communication service concept in TS 23218	7.3.1	7.4.0	C1-062521
Mar 2007	CT-35	CP-070153	0094	1	The IMS Communication sevice identifier can be included in the SIP response message	7.4.0	7.5.0	C1-070559
Jun 2007	CT-36	CP-070383	0095	6	IMS Communication Service ID	7.5.0	7.6.0	C1-071477
Jun 2007	CT-36	CP-070387	0097	1	Dynamic Service Activation Info	7.5.0	7.6.0	C1-070977
Sep 2007	CT-37	CP-070586	0100	2	Additions in TS 23.218 due to ICSI/IARI	7.6.0	7.7.0	C1-072182
Sep 2007	CT-37	CP-070586	0101	2	Completing 23.218 ICSI procedures	7.6.0	7.7.0	C1-072160
Sep 2007					Correction in History table (new version column) done by MCC	7.7.0	7.7.1	
Dec 2007	CT-38	CP-070806	0104	3	Completing 23.218 ICSI text	7.7.1	7.8.0	C1-073100
Dec 2007	CT-38	CP-070810	0103	1	Correction of request handling in terminating unregistered case	7.8.0	8.0.0	C1-072664
Dec 2007	CT-38	CP-070810	0102	1	Enabling service triggering after call forwarding	7.8.0	8.0.0	C1-072662
Mar 2008	CT-39	CP-080140	0105	2	Addition of other access network types.	8.0.0	8.1.0	C1-080415
Jun 2008	CT-40	CP-080418	0108	3	B2BUA AS influence of filter criteria evaluation	8.1.0	8.2.0	C1-082032
Jun 2008	CT-40	CP-080365	0111	1	Cr interface description	8.1.0	8.2.0	C1-081341
Jun 2008	CT-40	CP-080354	0113	1	Editorial changes to subclauses 6.4 and 6.5	8.1.0	8.2.0	C1-082026
Jun 2008	CT-40	CP-080344	0116	-	Correction of GRUU references	8.1.0	8.2.0	C1-081797
Sep 2008	CT-41	CP-080536	0117	2	Enhancement of Filter Criteria to Include Incoming Register in Third Party Register	8.2.0	8.3.0	C1-083098

Sep 2008	CT-41	CP-080537	0118	1	MRB	8.2.0	8.3.0	C1-083361
Dec 2008	CT-42	CP-080854	0120		Cr interface addition to architecture diagram	8.3.0	8.4.0	C1-084751
Dec 2008	CT-42	CP-080854	0121		Media example fixes	8.3.0	8.4.0	C1-084753
Dec 2008	CT-42	CP-080873	0122		Enhancement of Filter Criteria to include final response to Incoming Register in Third Party Register	8.3.0	8.4.0	C1-085056
Dec 2008	CT-42				Editorial cleanup by MCC	8.3.0	8.4.0	
Dec 2009	CT-46	CP-090894	0127		Updating of GRUU references	8.4.0	8.5.0	C1-094829
Dec 2009	CT-46	CP-090923	0124	2	Allowing direct routing between AS and MRFC	8.5.0	9.0.0	C1-094735
Dec 2009	CT-46	CP-090936	0125		Registration of IMS media plane security capabilities	8.5.0	9.0.0	C1-094418
Mar 2010	CT-47	CP-100110	0129		Resolve EN on terminating request handling	9.0.0	9.1.0	C1-100467
Jun 2010	CT-48	CP-100366	0130		Updating references to OMA specifications	9.1.0	9.2.0	C1-101714
Mar 2011	CT-51				Upgrade to Rel-10	9.2.0	10.0.0	
Sep 2011	CT-53	CP-110693	0132	2	Identifying Application Server capabilities on the signaling route	10.0.0	11.0.0	C1-113592
Sep 2011	CT-53	CP-110688	0133	2	Adding MRB between AS and MRFC	10.0.0	11.0.0	C1-113725
Dec 2011	CT-54	CP-110889	0137	1	Border control elements and the MRB	11.0.0	11.1.0	C1-115156
Dec 2011	CT-54	CP-110889	0138		MRB interfaces	11.0.0	11.1.0	C1-114812
Mar 2012	CT-55	CP-120119	0136	3	AS selection of MRF resources	11.1.0	11.2.0	C1-120753
Mar 2012	CT-55	CP-120119	0139	1	Revisions to Rc interface	11.1.0	11.2.0	C1-120754
Jun 2012	CT-56	CP-120320	0141		Editorial correction in border control concepts	11.2.0	11.3.0	C1-120991
Jun 2012	CT-56	CP-120307	0143		Correction of reference to TS 33.328	11.2.0	11.3.0	C1-121958
Jun 2012	CT-56	CP-120320	0144	1	Access to MRB and to MRF resources by entities other than an application server	11.2.0	11.3.0	C1-122241
Jun 2012	CT-56	CP-120316	0145	3	Creation of a new functional entity to support application servers in the enterprise	11.2.0	11.3.0	C1-122479
Jun 2012	CT-56	CP-120320	0146	1	Correction of MRF and MRB related interfaces	11.2.0	11.3.0	C1-122242
Jun 2012	CT-56	CP-120320	0147		MRB to MRB operation	11.2.0	11.3.0	C1-122140
Sep 2012	CT-57	CP-120597	0148	1	Usage of visited network MRB address when allocating MRF resources	11.3.0	11.4.0	C1-123276
Sep 2012	CT-57	CP-120591	0149		Addressing an editor's note relating to interface naming	11.3.0	11.4.0	C1-122926
Sep 2012	CT-57	CP-120591	0150	1	Addressing an editor's note supported functionality for the ISC gateway function	11.3.0	11.4.0	C1-123268
Sep 2012	CT-57	CP-120597	0152		Addressing an editor's note relating to resources in multiple VPLMNs	11.3.0	11.4.0	C1-122934
Sep 2012	CT-57	CP-120597	0153	1	Addressing an editor's note relating to border control functions on Mr, Mr' and Cr interfaces	11.3.0	11.4.0	C1-123278
Sep 2012	CT-57	CP-120597	0154		Addressing an editor's note relating to border control concepts for the Rc interface	11.3.0	11.4.0	C1-122936
Sep 2012	CT-57	CP-120597	0155		Addressing an editor's note relating to IBCF usage on media resource allocation architecture	11.3.0	11.4.0	C1-122970
Sep 2012	CT-57	CP-120591	0157	1	Functionalities of the IBCF on the ISC interface	11.3.0	11.4.0	C1-123269
Dec 2012	CT-58	CP-120804	0158	1	Recover screened information	11.4.0	11.5.0	C1-124096
Dec 2012	CT-58	CP-120809	0160	2	Transit Function – ISC alternative	11.4.0	11.5.0	C1-124938
Dec 2012	CT-58	CP-120818	0162	1	Transferring IMS CAMEL Data with Sh Protocol	11.5.0	12.0.0	C1-124878
Mar 2013	CT-59	CP-130127	0168	1	Interface IM-SSF / HSS with Diameter	12.0.0	12.1.0	C1-130505
Jun 2013	CT-60	CP-130249	0170	1	Renaming the Mz reference point to be Mf	12.1.0	12.2.0	C1-131618
Sep 2013	CT-61	CP-130513	0171	1	Updating TS 23.218 to RFC 6665	12.2.0	12.3.0	C1-133235

---

# History

<b>Document history</b>		
V12.3.0	October 2014	Publication