

MTAS External Network Configuration

MTAS

USER GUIDE

Copyright

© Ericsson AB 2016–2019. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

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

Trademark List

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



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Overview	3
3	MTAS Interfaces	5
3.1	Dh Interface	5
3.2	Sh Interface	6
3.3	CNS Interface	6
3.4	SNM Interface	6
3.5	Rf Interface	7
3.6	Ro Interface	7
3.7	CDS Interface	7
3.8	DNS Interface	8
3.9	ISC, Ma, and Pw Interfaces	8
3.10	Ut Interface	8
3.11	CAI3G Interface	9
3.12	CAT Interface	9
3.13	Mr Interface	9
3.14	Mp Interface	10
3.15	CAPv2 Interface	10
3.16	UCS Interface	10
3.17	ETSI MAP Interface	11
3.18	Parlay X Interface	11
3.19	CEL Interface	11
4	Session Border Gateway	13
4.1	Call Pull with Replaces Header	13
4.2	ICMP Destination Unreachable Supervision	13
5	HSS Configuration	15
5.1	Initial Filtering Criteria	15
5.2	Implicit Registration Set	31
5.3	Service Indication	32
5.4	Originating MMTel AS	33



5.5	Settings for Test Announcement Service	34
6	Public Service Identities	35
6.1	Settings for Ad-hoc Conferencing Service	35
6.2	Settings for 3PTY Service	36
6.3	Settings for Group Call Admission Control	36
6.4	Settings for Single Radio Voice Call Continuity Release 10	37
7	Dynamic Allocation Configuration	39
7.1	DNS Configuration	39
7.2	Dynamic Allocation with AS Instance Caching	40
8	DNS-Based Redundancy and Load Sharing of External Server Nodes	43
8.1	SRV Records	43
8.2	A/AAAA Records	43
8.3	Actual IP Address List of an External Server	44
9	Configuration of Differentiated Services (DiffServ)	45
10	User Provisioning	47
10.1	Subscription and Service Profile Administration in HSS	47
10.2	Provisioning in MTAS	49
11	Rebalancing	51
12	Deployment-Dependent Configurations	53
12.1	AS-Controlled Forking	53
12.2	Originating AS Chaining	55
12.3	MTAS Services Suppression Based on the INVITE Method	56
12.4	Served User without MMTel Subscription	56
12.5	Deployment-Dependent Configurations for Multi-Mobile Support	56
13	Configuration for Sub-Network Manager	59
13.1	Configure SFTP Users and Port	59
14	Parameter Value Selection for Deployment-Dependent CM Attributes	69
15	Installation of Additional MTAS Nodes	71



1 Introduction

This document describes the high-level configuration of the neighboring IP Multimedia Subsystem (IMS) nodes needed for correct operation of the Multimedia Telephony Application Server (MTAS). In addition, it describes the configuration needed for using the specific capabilities of the MTAS.

1.1 Prerequisites

It is assumed that the user of this document is familiar with the Operation and Maintenance (O&M) area in general.

1.1.1 Licenses

Not Applicable.

1.1.2 Documents

Before starting any procedure in this document, ensure that the following documents are available:

- Ericsson Command-Line Interface User Guide
- Managed Object Model (MOM)

1.1.3 Conditions

The following condition must apply:

- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.





2 Overview

The MTAS is an Application Server (AS) on the IMS Service Control (ISC) interface in an IMS network. The MTAS can fulfill several different functional roles in a Multimedia Telephony (MMTel) solution. These roles are MMTel Telephony AS, Network AS, and Service Centralization and Continuity (SCC) AS.

As an MMTel Telephony AS, the purpose of the MTAS is to provide real time (real time to be understood as opposed to store-and-forward), and peer-to-peer communication services, including basic communication services and MMTel-specific Supplementary Services.

As a Network AS, the MTAS provides communication interworking SIP signaling between entities with missing precondition capability support. Currently, MTAS supports Precondition Interworking Function (PrIwf) and Forking Interworking Function (FoIwf). PrIwf supports Quality of Service (QoS) precondition SIP signaling interworking for terminating endpoints, which lack precondition support. FoIwf supports aggregation of multiple early dialogues to a single dialogue.

As an SCC AS, the MTAS provides the possibility to offer IMS Centralized Services (ICS) and Single Radio Voice Call Continuity (SRVCC) according to the following standards which are key components for a Voice over LTE (VoLTE) solution:

— [3GPP TS 24.292](#)

— [3GPP TS 24.237](#)

The MTAS also implements supporting functions that can be used by the communication service, such as charging and a built-in Multimedia Resource Function Control (MRFC) function. This is all implemented by the underlying platform.

On network level, an N+1 redundancy concept is used. This is implemented by using the so-called dynamic allocation concept, and the Sh interface towards the HSS.

The MTAS can be used in mobile, fixed, or FMC type of networks. In that sense, it is access agnostic.





3 MTAS Interfaces

The MTAS external interfaces are shown in Figure 1.

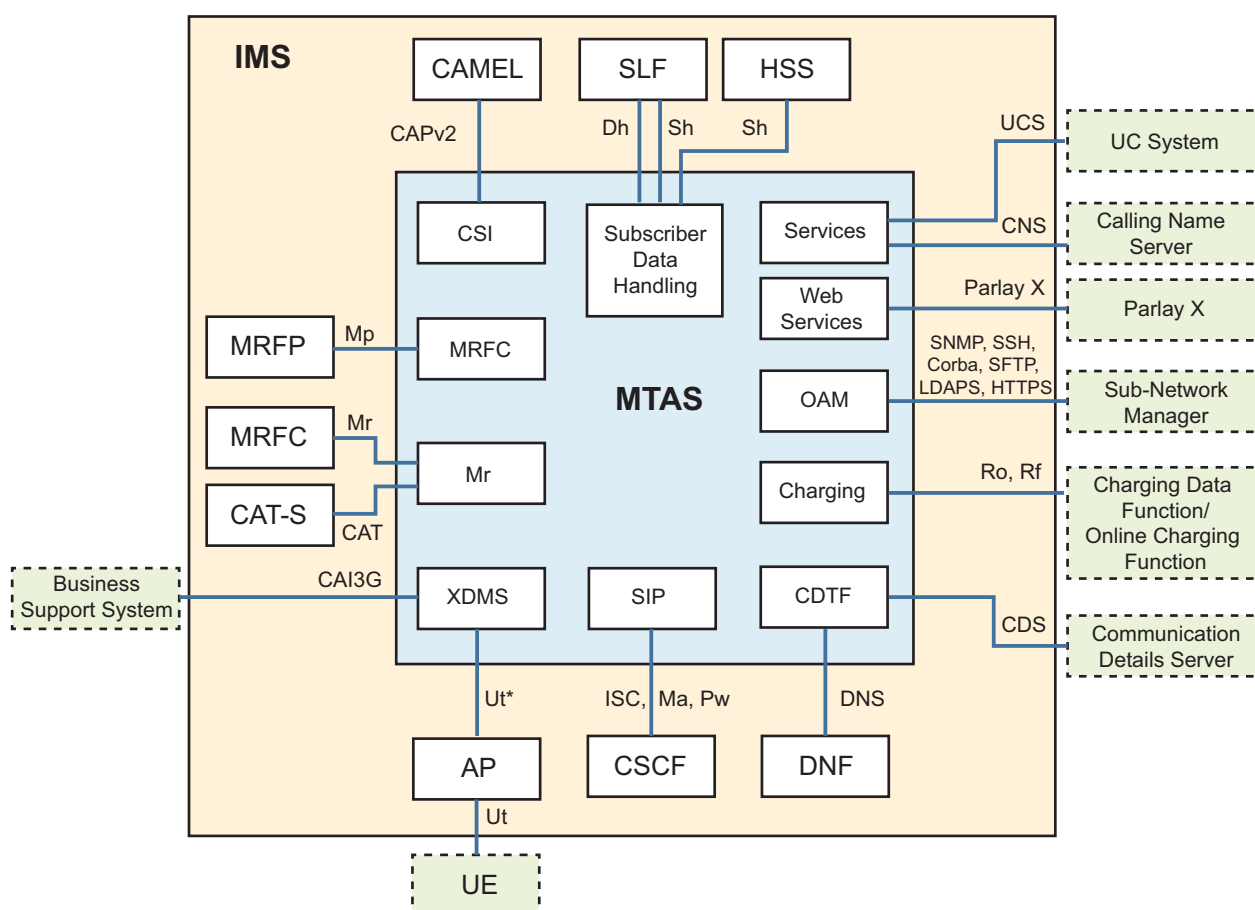


Figure 1 MTAS External Interfaces

3.1 Dh Interface

The Dh interface between the MTAS and the Subscriber Location Function (SLF) is used to retrieve the address of the HSS, which holds the subscription for a given user.

For more information about the Dh interface implementation and how to configure it in the MTAS, see the following documents:

- MTAS Subscriber Data Management Guide
- Sh/Dh Interface



3.2 Sh Interface

The Sh interface, which is between the MTAS and the HSS, is used for transferring user profile information such as user service-related information, user identities, or charging function addresses.

The messages on the Sh interface can be routed by two different routing mechanisms:

- Destination address based request routing (default)
- Realm Routing Table based request routing

For more information about the Sh interface implementation and how to configure it in the MTAS, see [MTAS Subscriber Data Management Guide and Sh/Dh Interface](#).

3.3 CNS Interface

The interface between the MTAS and the Calling Name Server (CNS) is used for obtaining calling name information using two different protocols as follows:

- Simple Object Access Protocol (SOAP) or alternatively SIP is used by Calling Name Identity Presentation (CNIP) flavor of the Originating Identity Presentation (OIP) service.
- SIP is used by Originating Calling Name Identity Presentation (OCNIP) service.

For more information about the CNS interface implementation and how to configure it in the MTAS, see [MTAS Calling Name Identity Presentation Management Guide and NameDb](#).

3.4 SNM Interface

The interface between the MTAS and the Sub-Network Manager (SNM) is using several protocols for different purposes, as follows:

- SNMPv2C and SNMPv3 for fault management
- FTP and SFTP for performance management
- LDAPv3 and LDAPS for configuration management
- Telnet and SSH for configuration management

For information about the MTAS Node Management procedures, see [MTAS VNF Management Guide](#).



3.5 Rf Interface

The Rf interface (Diameter Accounting Application) is used between the MTAS and the Charging Data Function (CDF) for transferring MMTel offline charging information.

For more information about the Rf interface implementation, how to configure it in the MTAS, and configuration of the Diameter layer used by the Rf interface in MTAS, see the following documents:

- [Diameter Management](#)
- [Diameter Offline Charging in MTAS](#)
- [MTAS Charging Management Guide](#)

3.6 Ro Interface

The Ro interface (Diameter Credit Control Application) is used between the MTAS and the Online Charging Function (OCF) for transferring MMTel online charging information. The Ro interface is also used by the Advice of Charge (AoC) Supplementary Service for accessing the AoC information related to a communication to be provided to the served user.

For more information about the Ro interface implementation, how to configure it in the MTAS, and configuration of the Diameter layer used by the Ro interface in MTAS, see the following documents:

- [Diameter Management](#)
- [Diameter Online Charging in MTAS](#)
- [MTAS Charging Management Guide](#)

3.7 CDS Interface

The Communication Details Servers (CDS) interface is based on the Diameter Accounting Application. It is used between the MTAS and the CDS by the Malicious Communication Identification (MCID) service to transfer communication details for Malicious Communication Identification purposes. It is also used by other Supplementary Services that allow the user to request actions that are based on earlier calls (that is, Dynamic Black List).

For more information about the CDS interface implementation, how to configure it in the MTAS, and configuration of the Diameter layer used by the CDS interface in MTAS, see the following documents:

- [Diameter Management](#)
- [Diameter Communication Details in MTAS](#)



— MTAS Charging Management Guide

3.8 DNS Interface

The DNS is a client/server system used in TCP/IP networks. The DNS is used to map alphanumeric names to IP addresses.

For information about how to configure the DNS interface in the MTAS, see [Managed Object Model \(MOM\)](#).

MTAS supports monitoring the availability of the configured DNS servers. For information about how to enable DNS server supervision, see the [MtasDns](#) MO.

3.9 ISC, Ma, and Pw Interfaces

The ISC interface is the interface between the MTAS and the Serving Call Session Control Function (S-CSCF). The ISC interface is implemented using the SIP protocol. The MTAS also uses the SIP protocol on the Ma interface with the Interrogating Call Session Control Function (I-CSCF) and the Pw interface to the Presence Server. From an MTAS perspective, the Ma and Pw interfaces are functionally equivalent to the ISC interface with one exception; when acting as User Agent Client (UAC), MTAS supports DNS-based redundancy of the I-CSCF.

For more information about the ISC, Ma, and Pw interface implementation in MTAS and how to configure these interfaces, see the following documents:

— [MTAS Interface to CSCF \(ISC, Ma, Pw\)](#)

— [MTAS SIP Management Guide](#)

3.10 Ut Interface

The OMA XDM-3 interface is used between the User Equipment (UE) and the AS to configure and manage groups, user access policies, URI lists, presence lists, and presence access policies. The 3GPP uses the name Ut for this interface, see [ETSI TS 183 023](#).

The protocol used on the Ut interface is XML Configuration Access Protocol (XCAP). XCAP is a set of XML rules that conforms an XML document. This document is transported through HTTP.

The MTAS implementation is using the Ut interface. Ut interface requires that the messages from UE have already been authenticated before sending them to MTAS. The Aggregation Proxy (AP) node, see Figure 1, implements the authentication of Ut interface messages for MTAS.



For more information about the Ut interface, the implementation and configuration of the interface in the MTAS, see the following documents:

- [MTAS XDMS Management Guide](#)
- [MTAS Ut Interface](#)

3.11 CAI3G Interface

The Customer Administration Interface Third Generation (CAI3G) interface is used as a provisioning interface between the MTAS and Business Support System (BSS). CAI3G is based on the SOAP standard (XML/HTTP and XML/HTTPS). It can manage complex data models while hiding network complexity. There is support for notification to the business system.

For more information about the CAI3G interface implementation in the MTAS and how to configure these interfaces, see the following documents:

- [MTAS CAI3G Interface](#)
- [MTAS XDMS Management Guide](#)

3.12 CAT Interface

The Customized Alerting Tones Server (CAT-S) is a dedicated external MRF resource used for generating CAT signal. The CAT signal is music or an announcement played for the caller on terminating calls to the served user.

The MTAS supports DNS-based redundancy of the CAT-S.

For more information about the CAT interface implementation and configuration in the MTAS, see [MTAS Interface to CAT-S \(CAT\)](#).

3.13 Mr Interface

The Mr interface is used between MTAS and the MRFC to control media services. When acting as UAC, MTAS supports DNS-based redundancy of the MRFC.

The attribute `mtasMrControllerRoute` defines whether the External MRFC is directly routed to the MTAS (value 0), or through the S-CSCF (value 1). In rare cases, for example for Completion of Communication to Busy Subscriber (CCBS) recall announcement, the information about the S-CSCF is not available and the announcement request is routed directly. The recommended setting is to use direct routing to the MTAS, to save S-CSCF resources.



For more information about the Mr interface implementation and configuration in the MTAS, see the following documents:

- MTAS Interface to MRF (Mr)
- MTAS Media Control Management Guide
- Managed Object Model (MOM)

3.14 Mp Interface

The Mp interface is used between the integrated MRFC and the Multimedia Resource Function Processor (MRFP) whenever multimedia session manipulation is needed. The Mp interface is H.248-based.

For more information about the Mp interface implementation and configuration in the MTAS, and configuration of the Domain Name Server/System (DNS) interface in the MTAS, see the following documents:

- Configuring SS7, SCTP
- MTAS H.248 Support
- MTAS Media Control Management Guide

3.15 CAPv2 Interface

The CAMEL Application Protocol version 2 (CAPv2) interface is used to enable Intelligent Network (IN) interaction in the MMTel Telephony AS, and to allocate the IMS Routing Number (IMRN) for IMS Centralized Services (ICS) users. For CAMEL interaction, the MMTel calls are influenced and controlled by the services in the IN layer. The CAP operations are carried over SIGTRAN (SS7 over SCTP).

For more information about the CAPv2 interface implementation and configuration in the MTAS, see [MTAS CAPv2 Management Guide](#), [MTAS IMS Centralized Services Management Guide](#), and [MTAS SS7 Management Guide](#).

3.16 UCS Interface

The UCS interface, between the MTAS and the Unified Communication (UC) system, is used for routing originating or terminating sessions for business users to the UC system, where the enterprise communication services are executed.

For more information about the UCS interface implementation and configuration in the MTAS, see [MTAS Unified Communication Routing Management Guide](#).



3.17 ETSI MAP Interface

The ETSI Mobile Application Part (MAP) interface is used between SCC AS (acting as Gateway Mobile Switching Center (GMSC)) and Home Location Register (HLR) or visited Mobile Switching Center (vMSC). SCC AS can use the ETSI MAP interface to query the HLR for a Mobile Station Roaming Number (MSRN) to route the call to the Circuit Switched domain. SCC AS can also receive resume call handling request from vMSC when the mobile of a served user moves to another vMSC after the MSRN is allocated.

MAP is a Transaction Capabilities Application Part (TCAP) user and the operations are carried over SIGTRAN.

For more information about the ETSI MAP interface configuration in the MTAS, see [MTAS IMS Centralized Services Management Guide](#) and [MTAS SS7 Management Guide](#).

3.18 Parlay X Interface

The MTAS can interact with Parlay X enabled applications deployed on application servers. This interaction can be with the MTAS in client or server role, or both. MTAS supports DNS-based redundancy of the Parlay X enabled applications taking server role.

For more information about the Parlay X interface implementation and configuration in the MTAS, and configuration of the Parlay X interface in the MTAS, see the following documents:

- [Parlay X MMTel Extensions](#)
- [MTAS Parlay X Management Guide](#)
- [Parlay X in MMTel](#)
- [MTAS Parlay X in MMTel Management Guide](#)

3.19 CEL Interface

The CEL interface is a proprietary SIP-based interface between MTAS and the Event Server.

A PUBLISH message with a `call-event-info` event header and XML body is used to report communication events towards the external server whenever there is a communication attempt from served user. The event includes information about the type of session state event, time, calling party, called party, subscription information, and so on.

The type of session state event can be `established` or `unsuccessful attempt`.



Communication on the CEL interface is performed using SIP over UDP or TCP. On the network layer, either IPv4 or IPv6 addresses can be used. Either IPv4 or IPv6 addresses can be used in the SIP headers and bodies. The URI specifying the Event server address (hostname, port) is part of the CEL service configuration in MTAS.

For more information about the CEL interface implementation and how to configure it in MTAS, see [MTAS Communication Event Logging Management Guide](#).



4 Session Border Gateway

This section describes how to use SIP Message Manipulation (SMM) rules in Session Border Gateway (SBG).

4.1 Call Pull with Replaces Header

For Call Pull with replaces header service in MMTel AS to be able to interwork with the Ericsson SBG, two SMM rules need to be created and applied to SBG to prevent SBG from modifying the replaces header.

Two rulesets are applied as part of SBG incoming and part of SBG core outgoing SMM filter as follows:

Ruleset “For_SBG_access_incoming”

```
If
    is_request and
    SIP:cseq.method == "INVITE" and
    SIP:replaces exists and
    not SIP:replaces;from-tag ~= '^h7g4Esb_(.*)' and
    not SIP:replaces;to-tag ~= '^h7g4Esb_(.*)'
Do
    SIP:replaces;to-tag := "remove_" + SIP:replaces;to-tag
End
End
```

Ruleset “For_SBG_core_outgoing”

```
If
    is_request and
    SIP:cseq.method == "INVITE" and
    SIP:replaces exists and
    SIP:replaces;to-tag ~= '^h7g4Esb_remove_(.*)'
Do
    SIP:replaces;to-tag := $1.1
End
End
```

4.2 ICMP Destination Unreachable Supervision

ICMP destination unreachable supervision cannot be used with MTAS services where media endpoints are reconnected during call establishment, for example, call establishment following Call Return invocation.





5 HSS Configuration

This section describes how to configure the HSS.

5.1 Initial Filtering Criteria

The list of Initial Filtering Criteria (IFC) is part of the service profile, see Section 10.1 Subscription and Service Profile Administration in HSS on page 47, and Section 5.2 in [3GPP TS 23.218 \(V8.4.0\)](#).

An IFC consists of conditions to be met by the SIP request and the corresponding AS address where the request is routed to when the conditions are fulfilled. The AS address can either include an AS dedicated SIP port or a generic SIP port (can be used by MMTel AS, SCC AS, and NW AS). A session case is also defined in IFC, if an AS dedicated port is used, it is implicit by the AS address (port) or defined by P-Served-User header. If a generic SIP port is used, the P-Served-User header must be provided.

The mechanism for setting this data varies depending upon network configuration and the mechanisms used in the specific network. The subsections describe the recommended IFC configurations for the following MTAS installations:

- MTAS with base MMTel features
- MTAS with base MMTel features and Communication Completion service
- MTAS with base MMTel features and Ad-hoc Conferencing service
- MTAS with base MMTel features, Communication Completion service, and Ad-hoc Conferencing service
- MTAS with Group Call Admission Control service
- MTAS with Service Centralization and Continuity service
- MTAS with Scheduled Conferencing service
- MTAS with Flexible Communication Distribution service to primary User's Devices
- MTAS with Emergency Call Notification service
- MTAS with Charging Info Notification service
- MTAS with Dialog Event Notifier service

The configuration of the attributes used at determining the Session Case is described in [MTAS SIP Management Guide](#).



The examples in the following sections assume that the Session Case is determined by a dedicated SIP port. The logic is similar, when the Session Case is determined by the attributes of the P-Served-User header.

If the generic SIP port is used, the AS is determined by the AS name, which must be specified in the route parameter `as=`, and the Session Case is determined by the attributes of the P-Served-User header. In single invocation, the route parameter `as=` supports multiple names, for example, `as="foiwf, scc, mmt, priwf"`. The AS name used must match the configured AS name, for example, `mtasFunctionMmtAsName`, `mtasFunctionSccAsName`, or `mtasFunctionNwFoIwAsName`. The logic is the same as in the examples in the following sections, except that the generic SIP port, `mtasSipAsGenericPort`, is specified instead of the dedicated SIP ports.

Note: The MMTel Telephony AS is not to be included in the triggers for the Originating_CDIV session case, since the MMTel Telephony AS does not use the triggers for the Originating_CDIV session case.

If Originating AS Chaining is used, the Originating_CDIV session case does not apply, so inserting the MMTel Telephony AS in the triggers for the Originating_CDIV session case has no effect.

If Originating AS Chaining is not used, inserting the MMTel Telephony AS in the triggers for the Originating_CDIV session results in double execution of the originating services.

5.1.1 Base MMTel Settings

The following HSS pseudo configuration is recommended when base MMTel features are used:

1. Trigger the MTAS on the originating port (`mtasSipTrafficOriginatingIpPort`)

when:

`Method="INVITE" AND SessionCase="Originating"`
2. Trigger the MTAS on the originating unregistered port (`mtasSipTrafficOriginatingUnregIpPort`)

when:

`Method="INVITE" AND SessionCase="Originating_Unregistered"`
3. Trigger the MTAS on the terminating port (`mtasSipTrafficTerminatingIpPort`)

when:

`Method="INVITE" AND SessionCase="Terminating_Registered"`



4. Trigger the MTAS on the terminating unregistered port (mtasSipTrafficTerminatingUnregIpPort)

when:

Method="INVITE" AND SessionCase="Terminating_Unregistered"

5. Trigger the MTAS on the originating port (mtasSipTrafficOriginatingIpPort)

when:

Method="REGISTER" AND (RegistrationType="Initial" OR RegistrationType="De-registration")

Note: The MTAS must not be triggered on periodic re-registration.

If MTAS is configured for caching contact data (mtasSubsDataCacheContactData=1), then IFC must be configured to include the original REGISTER request and the 200 OK response in every 3rd-party REGISTER request sent to MTAS; see Section 5.1.11 Settings for Flexible Communication Distribution to Primary User's Devices on page 25. If caching contact data by MTAS is not needed, that is, Flexible Communication Distribution to Primary User's Devices is not used (mtasFcdDistributeToPrimaryUserDevices=0), then caching is to be disabled on MTAS instead (mtasSubsDataCacheContactData=0), to avoid superfluous SUBSCRIBES for "reg" event.

For more information about the triggered ports described in this section, see [Managed Object Model \(MOM\)](#).

5.1.2 Settings for Base MMTel Features and Communication Completion Service

The following HSS pseudo configuration is needed when the Communication Completion optional feature is used:

1. Trigger the MTAS on the originating port (mtasSipTrafficOriginatingIpPort)

when:

Method="INVITE" AND SessionCase="Originating" AND NOT RequestURI=".*noifc=orig.*"

2. Trigger the MTAS on the originating unregistered port (mtasSipTrafficOriginatingUnregIpPort)

when:

Method="INVITE" AND SessionCase="Originating_Unregistered"



3. Trigger the MTAS on the terminating port (mtasSipTrafficTerminatingIpPort)

when:

Method="INVITE" AND SessionCase="Terminating_Registered"
AND NOT RequestURI=".*noifc=term.*"
4. Trigger the MTAS on the terminating unregistered port (mtasSipTrafficTermUnregIpPort)

when:

Method="INVITE" AND SessionCase="Terminating_Unregistered"
AND NOT RequestURI=".*noifc=term.*"
5. Trigger the MTAS on the terminating port (mtasSipTrafficTerminatingIpPort)

when:

Method="SUBSCRIBE" AND NOT SessionCase="Originating"
AND (header="Event" Content="call-completion")
6. Trigger the MTAS on the originating port (mtasSipTrafficOriginatingIpPort)

when:

Method="REGISTER" AND (RegistrationType="Initial"
OR RegistrationType="De-registration")

Note: The MTAS must not be triggered on periodic re-registration.

If MTAS is configured for caching contact data (mtasSubsDataCacheContactData=1), then IFC must be configured to include the original REGISTER request and the 200 OK response in every 3rd-party REGISTER request sent to MTAS; see Section 5.1.11 Settings for Flexible Communication Distribution to Primary User's Devices on page 25. If caching contact data by MTAS is not needed, that is, Flexible Communication Distribution to Primary User's Devices is not used (mtasFcdDistributeToPrimaryUserDevices=0), then caching is to be disabled on MTAS instead (mtasSubsDataCacheContactData=0), to avoid superfluous SUBSCRIBES for "reg" event.

For more information about the triggered ports described in this section, see Managed Object Model (MOM).



5.1.3 Settings for Base MMTel Features and Ad-Hoc Conferencing Service

The following HSS pseudo configuration is needed when the Ad-hoc Conferencing optional feature is used and the `mtasSipCallOutOfBlueRouting` CM attribute is set to 1 (I-CSCF):

Note: The settings for the Communication Completion optional feature include the listed configuration for the Ad-hoc Conferencing optional feature.

1. Trigger the MTAS on the originating port (`mtasSipTrafficOriginatingIpPort`)

when:

```
Method="INVITE" AND SessionCase="Originating"  
AND NOT RequestURI=".*noifc=orig.*"
```

2. Trigger the MTAS on the originating unregistered port (`mtasSipTrafficOriginatingUnregIpPort`)

when:

```
Method="INVITE" AND SessionCase="Originating_Unregistered"
```

3. Trigger the MTAS on the terminating port (`mtasSipTrafficTerminatingIpPort`)

when:

```
Method="INVITE" AND SessionCase="Terminating_Registered"
```

4. Trigger the MTAS on the terminating port (`mtasSipTrafficTermUnregIpPort`)

when:

```
Method="INVITE" AND SessionCase="Terminating_Unregistered"
```

5. Trigger the MTAS on the originating port (`mtasSipTrafficOriginatingIpPort`)

when:

```
Method="REGISTER" AND (RegistrationType="Initial"  
OR RegistrationType="De-registration")
```



Note: The MTAS must not be triggered on periodic re-registration.

If MTAS is configured for caching contact data (`mtasSubsDataCacheContactData=1`), then IFC must be configured to include the original REGISTER request and the 200 OK response in every 3rd-party REGISTER request sent to MTAS; see Section 5.1.11 Settings for Flexible Communication Distribution to Primary User's Devices on page 25. If caching contact data by MTAS is not needed, that is, Flexible Communication Distribution to Primary User's Devices is not used (`mtasFcdDistributeToPrimaryUserDevices=0`), then caching is to be disabled on MTAS instead (`mtasSubsDataCacheContactData=0`), to avoid superfluous SUBSCRIBES for "reg" event.

For more information about the CM attributes and triggered ports described in this section, see [Managed Object Model \(MOM\)](#).

5.1.4 Settings for Base MMTel Features, Communication Completion Service, and Ad-Hoc Conferencing Service

The following HSS pseudo configuration is needed when the Communication Completion optional feature is used:

1. Trigger the MTAS on the originating port (`mtasSipTrafficOriginatingIpPort`)

when:

`Method="INVITE" AND SessionCase="Originating" AND NOT RequestURI=".*noifc=orig.*"`
2. Trigger the MTAS on the originating unregistered port (`mtasSipTrafficOrigUnregIpPort`)

when:

`Method="INVITE" AND SessionCase="Originating_Unregistered"`
3. Trigger the MTAS on the terminating port (`mtasSipTrafficTerminatingIpPort`)

when:

`Method="INVITE" AND SessionCase="Terminating_Registered" AND NOT RequestURI=".*noifc=term.*"`
4. Trigger the MTAS on the terminating unregistered port (`mtasSipTrafficTermUnregIpPort`)

when:

`Method="INVITE" AND SessionCase="Terminating_Unregistered" AND NOT RequestURI=".*noifc=term.*"`



5. Trigger the MTAS on the terminating port (mtasSipTrafficTerminating IpPort)

when:

Method="SUBSCRIBE" AND NOT SessionCase="Originating"
AND (header="Event" Content="call-completion")

6. Trigger the MTAS on the originating port (mtasSipTrafficOriginating IpPort)

when:

Method="REGISTER" AND (RegistrationType="Initial"
OR RegistrationType="De-registration")

Note: MTAS must not be triggered on periodic re-registration.

If MTAS is configured for caching contact data (mtasSubsDataCache ContactData=1), then IFC must be configured to include the original REGISTER request and the 200 OK response in every 3rd-party REGISTER request sent to MTAS; see Section 5.1.11 Settings for Flexible Communication Distribution to Primary User's Devices on page 25. If caching contact data by MTAS is not needed, that is, Flexible Communication Distribution to Primary User's Devices is not used (mtasFcdDistributeToPrimaryUserDevices=0), then caching is to be disabled on MTAS instead (mtasSubsDataCacheContactData=0), to avoid superfluous SUBSCRIBEs for "reg" event.

For more information about the triggered ports described in this section, see Managed Object Model (MOM).

5.1.5 Settings for Base MMTel Features and Session Transfer to Own Device (STOD) Service

The following HSS pseudo configuration is needed when the STOD optional feature is used, where it replaces Trigger 3 in Section 5.1.1 Base MMTel Settings on page 16.

1. Trigger the MTAS on the terminating port (mtasSipTrafficTerminating IpPort)

when:

Method="INVITE" AND SessionCase="Terminating_Registered"
AND NOT RequestURI=".*noifc=term.*"

For more information about the triggered ports described in this section, see Managed Object Model (MOM).



5.1.6 Settings for Group Call Admission Control

All users who belong to a Call Admission Control (CAC) group must have their services delivered by the same MTAS. The IFC for all users belonging to the same CAC group must be configured so that when the user registers in the IMS, the same MTAS is chosen to provide the Group CAC (GCAC) service for the user as for all other members of the same CAC group.

For information about how to configure the CAC service in the MTAS, see [MTAS Call Admission Control Management Guide](#).

5.1.7 Settings for Service Centralization and Continuity

When the Service Centralization and Continuity AS (SCC AS) is deployed on the MTAS node, the following HSS pseudo configuration is recommended:

1. Trigger the SCC AS on the originating port (mtasSipSccOrigPort)

```
Method="INVITE" AND SessionCase="Originating"  
AND NOT RequestURI=".*noifc=orig.*"
```

2. Trigger the SCC AS on the originating unregistered port (mtasSipSccOrigUnregPort)

```
Method="INVITE" AND SessionCase="Originating Unregistered"  
AND NOT RequestURI=".*noifc=orig.*"
```

3. Trigger the SCC AS on the terminating port (mtasSipSccTermPort)

```
Method="INVITE" AND SessionCase="Terminating"
```

4. Trigger the SCC AS on the terminating unregistered port (mtasSipSccTermUnregPort)

```
Method="INVITE" AND SessionCase="Terminating Unregistered"
```

5. Trigger the SCC AS on the originating port (mtasSipSccOrigPort) for registration

Include REGISTER REQUEST AND Include REGISTER RESPONSE

If the S-CSCF supports the optimized 3rd Party Registration where subscriber registered first and added contacts, both are mapped to Initial RegistrationType and deregistered contact and last contact both are mapped to De-Register RegistrationType, the Re-Register only carries Refresh of contact and is not needed.

This is the case for Ericsson S-CSCF:

```
Method="REGISTER" AND (RegistrationType="Initial" OR  
RegistrationType="De-registration"
```



In other cases, the Re-Register RegistrationType is needed as well, to get information about all registered contacts:

```
Method="REGISTER" AND (RegistrationType="Initial" OR  
RegistrationType="Re-registration" OR  
RegistrationType="De-registration")
```

Note: The SCC AS must be triggered on re-registrations from non-Ericsson S-CSCF to get information about all registered contacts. SCC AS must be triggered as the first AS for originating and originating unregistered IFC, and as the last AS for terminating and terminating unregistered IFC.

The IFC definition must ensure that the SCC AS is not triggered in case subscribers send out-of-dialog SUBSCRIBE of conference event.

For more information about the CM attributes and triggered ports described in this section, see [Managed Object Model \(MOM\)](#).

5.1.8 SCC AS and MMTel Telephony AS Co-Located

When the SCC AS and MMTel Telephony AS are co-located on the same MTAS node, depending on the type of networks or service profiles MTAS serves, the following IFC configuration must be considered.

— Service profile for VoLTE or VoLTE with FMC:

The IFC must be configured as described in Section 5.1.7 Settings for Service Centralization and Continuity on page 22 and the triggers for MMTel Telephony AS as described in Section 5.1.1 Base MMTel Settings on page 16 but excluding the trigger to MMTel on registration. The MMTel registration trigger can be omitted because of an optimization where the registration procedure for MMTel Telephony AS is handled already in SCC AS registration when SCC AS and MMTel Telephony AS co-located.

— Service profile for Fixed:

The triggers for MMTel Telephony AS apply as described in Section 5.1.1 Base MMTel Settings on page 16. If the FCD multi-device distribution feature is used, the trigger on registration must be configured to include REGISTER REQUEST and REGISTER RESPONSE as described in Section 5.1.11 Settings for Flexible Communication Distribution to Primary User's Devices on page 25.

5.1.9 Settings for SCC with T-SDS

When the SCC AS with T-SDS is deployed on the MTAS node, the following HSS pseudo configuration is recommended:



1. Trigger the SCC AS for the IMS T-SDS service on the terminating port (mtasSipSccTermPort)

Method="INVITE" AND SessionCase="Terminating"

The ServerName property in the Server Profile must be configured to match the CM attribute mtasSdsTAsName.

2. Trigger the SCC AS for the IMS T-SDS service on the terminating unregistered port (mtasSipSccTermUnregPort)

Method="INVITE" AND SessionCase="Terminating Unregistered"

The ServerName property in the Server Profile must be configured to match the CM attribute mtasSdsTAsName.

Note: In addition to the IFCs in Section 5.1.7 Settings for Service Centralization and Continuity on page 22, the SCC AS must in this case be triggered as the first AS for terminating or terminating unregistered IFC.

For more information about the triggered port described in this section, see Managed Object Model (MOM).

5.1.10

Settings for SCC Supporting Mix of VoLTE and 2G/3G

When the SCC AS with supporting mix of VoLTE and 2G or 3G is deployed on the MTAS node, see [MTAS IMS Centralized Services Management Guide](#) for more details, the following HSS pseudo configuration is recommended:

1. Trigger the SCC AS on the terminating port (mtasSipSccTermPort).

Method="INVITE" AND SessionCase="Terminating"

One Service Profile must be configured for the 2G or the 3G user and another Service Profile for the VoLTE user.

The ServerName property in VoLTE Service Profile must be configured to start with a string that matches the CM attribute mtasSubsDataVolteCaseName.

2. Trigger the SCC AS service on the terminating unregistered port (mtasSipSccTermPort).

Method="INVITE" AND SessionCase="Terminating Unregistered"

One Service Profile must be configured for the 2G or the 3G user and another Service Profile for the VoLTE user.

The ServerName property in VoLTE Service Profile must be configured to start with a string that matches the CM attribute mtasSubsDataVolteCaseName.

Note: SCC AS must be triggered as the last AS for terminating and terminating unregistered IFC.



For more information about the triggered port described in this section, see Managed Object Model (MOM).

5.1.11 Settings for Flexible Communication Distribution to Primary User's Devices

If the FCD service is used to distribute calls to Primary User's Devices (mtasFcdDistributeToPrimaryUserDevices=1), which requires caching contact data to be enabled on MTAS (mtasSubsDataCacheContactData=1) and the MMTel Telephony AS is standalone (that is not co-located with SCC AS), the following HSS pseudo configuration is recommended for registration:

1. Trigger the MMTel Telephony AS on the originating port (mtasSipTrafficOriginatingIpPort) for registration.

Include REGISTER REQUEST AND Include REGISTER RESPONSE.

In case the S-CSCF supports the optimized 3rd Party Registration where subscriber registered first and added contacts both are mapped to Initial RegistrationType and deregistered contact and the last contact both are mapped to De-Register RegistrationType, the Re-Register only carries Refresh of contact and is not needed.

This is the case for Ericsson S-CSCF:

Method="REGISTER" AND (RegistrationType="Initial" OR RegistrationType="De-registration")

In other cases, the Re-Register RegistrationType is needed as well, to get information about all registered contacts:

Method="REGISTER" AND (RegistrationType="Initial" OR RegistrationType="Re-registration" OR RegistrationType="De-registration")

For more information about the triggered port described in this section, see Managed Object Model (MOM).

5.1.12 Settings for Emergency Call Notification

The following HSS pseudo configuration is recommended when the Emergency Call Notification feature is used:

1. Trigger the MTAS on the originating port (mtasSipTrafficOriginatingIpPort)

when:

Method="NOTIFY" AND SessionCase="Originating" AND



```
EventHeader="emergencyCall;.*"
```

2. Trigger the MTAS on the originating unregistered port (mtasSipTrafficOrigUnregIpPort)

when:

```
Method="NOTIFY" AND SessionCase="Originating_Unregistered"  
AND EventHeader="emergencyCall;.*"
```

For more information about the triggered ports described in this section, see [Managed Object Model \(MOM\)](#).

5.1.13 Settings for Charging Info Notification

The following HSS pseudo configuration is recommended when the Charging Info Notification feature is used:

1. Trigger the MTAS on the originating port (mtasSipTrafficOriginatingIpPort)

when:

```
Method="NOTIFY" AND SessionCase="Originating" AND  
EventHeader="charging-info;.*"
```

2. Trigger the MTAS on the originating unregistered port (mtasSipTrafficOrigUnregIpPort)

when:

```
Method="NOTIFY" AND SessionCase="Originating_Unregistered" AND  
EventHeader="charging-info;.*"
```

3. Trigger the MTAS on the terminating port (mtasSipTrafficTerminatingIpPort)

when:

```
Method="NOTIFY" AND SessionCase="Terminating_Registered" AND  
EventHeader="charging-info;.*"
```

4. Trigger the MTAS on the terminating unregistered port (mtasSipTrafficTermUnregIpPort)

when:

```
Method="NOTIFY" AND SessionCase="Terminating_Unregistered" AND  
EventHeader="charging-info;.*"
```

For more information about the triggered ports described in this section, see [Managed Object Model \(MOM\)](#).



5.1.14 Settings for Dialog Event Notification

The following HSS pseudo configuration is recommended when the Dialog Event Notification feature is used:

1. Trigger the MMTel AS on the originating port (mtasSipTrafficOriginatingIpPort)

when:

Method="SUBSCRIBE" AND SessionCase="Originating" AND
(header="Event" Content ="dialog")

For more information about the triggered ports described in this section, see Managed Object Model (MOM).

5.1.15 Settings for Network AS

When the Network Application Server (NW AS) is deployed on the MTAS node, the following HSS pseudo configuration is recommended:

1. Trigger MTAS on the SIP generic port (mtasSipAsGenericPort)
Method="INVITE" AND SessionCase="Originating_Registered"

To trigger PrIwF, the following conditions must be met:

- The topmost route header must have an “as” parameter with value set to configured CM attribute mtasFunctionNwPrIwAsName
- The P-Served-User header must be present with parameters “sescase=orig” and “regstate=registered”

To trigger FoIwF, the following conditions must be met:

- The topmost route header must have an “as” parameter with a value set from the configured CM attribute mtasFunctionNwFoIwAsName.
- If the CM attribute mtasFoIwMode is set to ORIGINATING, the P-Served-User header must be present with parameters “sescase=orig”.
- If the CM attribute mtasFoIwMode is set to TERMINATING, the P-Served-User header must be present with parameters “sescase=term”.
- If the CM attribute mtasFoIwMode is set to ORIGINATING_AND_TERMINATING, the P-Served-User header can have “sescase=orig” or “sescase=term”.
- If the CM attribute mtasFoIwMode is set to DYNAMIC, the value configured in the CM attribute mtasFoIwInvocationHeaderValue must be a substring of the parameter in the header configured in the CM attribute mtasFoIwInvocationHeaderName. No extra IFC condition is recommended when the DYNAMIC value is set.



For more information about the CM attributes and triggered ports described in this section, see [Managed Object Model \(MOM\)](#).

5.1.16 Settings for MMTel AS for Business Line and Unified Communication Routing Service

The following HSS pseudo configuration is needed when the Unified Communication Routing optional feature is used:

1. Trigger the MTAS on the originating port (mtasSipTrafficOriginatingIpPort) when:

Method="INVITE" AND SessionCase="Originating"
2. Trigger the MTAS on the originating unregistered port (mtasSipTrafficOrigUnregIpPort) when:

Method="INVITE" AND SessionCase="Originating_Unregistered"
3. Trigger the MTAS on the terminating port (mtasSipTrafficTerminatingIpPort) when:

Method="INVITE" AND SessionCase="Terminating_Registered" AND NOT (header="Ericsson-UCMobility-UC-Ext")
4. Trigger the MTAS on the terminating unregistered port (mtasSipTrafficTermUnregIpPort) when:

Method="INVITE" AND SessionCase="Terminating_Unregistered" AND NOT (header="Ericsson-UCMobility-UC-Ext")
5. Trigger the MTAS on the terminating port (mtasSipTrafficTerminatingIpPort) when:

Method="INVITE" AND SessionCase="Terminating_Registered"
6. Trigger the MTAS on the terminating unregistered port (mtasSipTrafficTermUnregIpPort) when:

Method="INVITE" AND SessionCase="Terminating_Unregistered"
7. Trigger the MTAS on the originating port (mtasSipTrafficOriginatingIpPort) when:

Method="REGISTER" AND (RegistrationType="Initial" OR RegistrationType="De-registration")



Note: Triggers 3 and 4 routes the mobile terminated calls for the business users to the MMTel for the terminating-trunk session. The top most Route header must have the "sc=term-trunk" parameter for triggers 3 and 4. Terminating-trunk MMTel invocation only executes the UC Routing service to redirect the INVITE to the UC system. After executing the terminating enterprise services in the UC system, the UC system sends the INVITE back to the IMS. Triggers 5 and 6 are then executed and the call is routed to the MMTel for the typical terminating session.

For more information about the triggered ports, see [Managed Object Model \(MOM\)](#).

5.1.17 Settings for Multi-Persona on CS Access Feature

The following HSS pseudo configuration is required for using the Multi-Persona on CS access feature:

1. Trigger the MMTel AS on the generic SIP port or on the originating port (mtasSipTrafficOriginatingIpPort) when Method="MESSAGE" AND SessionCase="ORIGINATING_REGISTERED" AND Header="Content-Type" Content="application/vnd.call-id-info+xml"

For more information about the triggered ports described in this section, see [Managed Object Model \(MOM\)](#).

5.1.18 Settings for Service Centralization and Continuity with Multi Mobile Subscriptions Feature

When the SCC AS is deployed on the MTAS node with the Multi Mobile Subscriptions feature enabled (mtasSccMobileBehaviour=MOBILE_ENHANCEMENT_ON) and the Subscriber is a Multi Mobile subscriber, SCC AS handles INVITE for terminating registered session case that has cs-capable features tags in the Accept-Contact header.

It does not handle INVITE without cs-capable feature tag in the Accept-Contact header.

To avoid fixed UEs request processing at SCC AS, the following HSS pseudo configuration is optional and recommended to replace trigger 3 in Section 5.1.7 Settings for Service Centralization and Continuity on page 22 for the multi mobile subscriber:

1. Trigger the SCC AS on the terminating port (mtasSipSccTermPort) when:

Method="INVITE" AND SessionCase="Terminating" AND
(header="Accept-Contact" Content="cscapable=true" OR
Content="cscapable=false"))

Multi Mobile subscribers have their own profile if the trigger is to be changed as per what is recommended.



5.1.19 Settings for SCC Supporting Mix of VoLTE and 2G/3G with Multi Mobile Subscriptions Feature

When the SCC AS is deployed on the MTAS node with the Multi Mobile subscriptions feature enabled (`mtasSccMobileBehaviour=MOBILE_ENHANCEMENT_ON`) and the Subscriber is a Multi Mobile subscriber, SCC AS handles INVITE for terminating registered session case that has `cs-capable` features tags in the Accept-Contact header.

It does not handle INVITE without `cs-capable` feature tag in the Accept-Contact header.

To avoid fixed UEs request processing at SCC AS, the following HSS pseudo configuration is optional and recommended to replace trigger 1 in Section 5.1.10 Settings for SCC Supporting Mix of VoLTE and 2G/3G on page 24 for the multi mobile subscriber:

1. Trigger the SCC AS on the terminating port (`mtasSipSccTermPort`) when:

```
Method="INVITE" AND SessionCase="Terminating" AND  
(header="Accept-Contact" (Content="cscapable=true" OR  
Content="cscapable=false"))
```

One Service Profile must be configured for the 2G or the 3G user and another Service Profile for the VoLTE user. The `ServerName` property in the VoLTE Service Profile must be configured to start with a string that matches the CM attribute `mtasSubsDataVolteCaseName`.

Multi Mobile subscriptions users have their own profile if the trigger is to be changed as per what is recommended.

5.1.20 Single Invocation REGISTER

The following HSS pseudo configuration is recommended when the Single Invocation REGISTER feature is used:

1. Trigger MTAS on the SIP generic port (`mtasSipAsGenericPort`) when:

```
Method="REGISTER"
```

Note: For registration, the `P-Served-User` header is not required.

If the MMTel AS and the SCC AS are co-located, the registration must be done using the value of the Configuration Management attribute for SSC AS, `mtasFunctionSccAsName`, in the Route header parameter. For example, `as=scc`.

5.1.21 Single Invocation INVITE

The following HSS pseudo configuration is recommended when the Single Invocation INVITE feature is used:



1. Trigger MTAS on the SIP generic port (mtasSipAsGenericPort) when:
Method="INVITE"
2. Configure the order of the invoked ASs in the originating MTAS:
 - a. Make sure that the top most Route header has an as parameter that is set as follows:

`as="foiwf, scc, mmt, priwf"`

 The parameters represent the following Configuration Management attributes mtasFunctionNwFoIwAsName, mtasFunctionSccAsName, mtasFunctionMmtAsName, and mtasFunctionNwPrIwAsName.
 - b. Make sure that the P-Served-User header is present and set with the following parameters:

`— sescase=orig`

`— regstate=reg`
3. Configure the order of the invoked ASs in the terminating MTAS:
 - a. Make sure that the top most Route header has an as parameter that is set as follows:

`as="priwf, mmt, scc, foiwf"`

 The parameters represent the following Configuration Management attributes mtasFunctionNwPrIwAsName, mtasFunctionSccAsName, mtasFunctionMmtAsName, and mtasFunctionNwFoIwAsName.

Note: This is the reversed order of parameters compared to Step 2.
 - b. Make sure that the P-Served-User header is present and set with the following parameters:

`— sescase=term`

`— regstate=reg`

5.2 Implicit Registration Set

This section describes Implicit Registration Set (IRS).

5.2.1 Alias Identities

An IRS is a group of Public User Identities (PUI) that are registered through a single registration request. When one PUI within the set is registered, all PUIs associated with the IRS are registered at the same time. Similarly, when one of the



PUIs within the set is deregistered, all PUIs that have been implicitly registered are deregistered at the same time.

A PUI is an alias of another PUI if both identities belong to the same IRS, are linked to the same service profile, and have the same service data configured for each service, see [3GPP TS 23.228 \(V8.8.0\)](#).

The MTAS expects the first public identity in the received IRS to be the default one, and it has to be a SIP URI. This PUI is used as key for later HSS transactions on the Service Profile. The other identities in the IRS, that is, TEL-URIs, are alias identities.

5.2.2 Settings for Short Number Dialing Service

The Short Number Dialing (SND) service provides the members in a group with the ability to call each other by short numbers common to all members of the group.

For the SND service, the SND identities must be provisioned in the IRS of all SND users.

Note: The SND identity is not to be the default PUI.

The related SND domains must also be configured in the MTAS with proper settings of the `mtasSndDomains` CM attribute, see [Managed Object Model \(MOM\)](#).

For the concepts and configuration of the SND service in the MTAS, see [MTAS Short Number Dialing Management Guide](#).

5.2.3 Settings for AS-Controlled Forking

For the deployment-dependent IRS configuration for the AS-Controlled Forking feature, see [Section 12.1.1.1 IRS Configuration](#) on page 54.

5.3 Service Indication

This section describes the required Service Indication configuration in HSS.

The service indication is the identity (name) of the transparent service data container in which MTAS stores service-specific information.

The name of the listed service indications in the following sections reflects default identities used by MTAS. If other names have been configured, the same names must be defined in HSS.

5.3.1 MMTel Telephony Supplementary Services

Use of the MMTel Telephony Supplementary Services requires definition of a Service Indication in HSS.



5.3.2 MMTel Group Call Admission Control

Use of the Group Call Admission Control requires definition of a Service Indication in HSS.

5.3.3 MMTel Telephony Supplementary Services Service Profile

Use of the MMTel Telephony Supplementary Services Service Profile in MTAS requires definition of a Service Indication in HSS.

`MmtServiceProfileConfig` is the default service indication string used to identify the transparent data containing the MMTel Service Profile data. Service indication string different than the default value can be defined by the `mtasShIfMmtelServiceProfileInd` CM attribute in the MTAS.

5.3.4 Service Information Service Data

The Call Return service in MMTel AS requires, depending on service configuration, definition of a service indication in HSS. The service indication string is defined by the `mtasShIfServiceInformationServiceInd` CM attribute.

5.3.5 SCC AS Data

Use of Access Transfer Control Function (ATCF) info restoration requires definition of Service Indication with value of `ScpData` in HSS.

5.4 Originating MMTel AS

New service `OriginatingTestAnnService` added to the originating-outgoing container. When instantiating the container, the `OriginatingTestAnnServiceFactory` can only instantiate a service instance if the following conditions are true

- `mtasTaAdministrativeState = 1`
- `mtasTaSipDomain` includes a non-empty string.

If the precondition is not fulfilled, a CONTINUE service is instantiated. The `OriginatingTestAnnService` only subscribes to an INVITE event. Having filtered SIP URI from all URI parameters, the service checks if the user part of the SIP URI matches with `mtasTestAnnNumbersNum` configured for any instance of the `TestAnnouncementNumbers` MOC. If yes, the tel embedded SIP URI of the Request-URI is transformed to a SIP identity by using the filtered user part and adding the value of `mtasTaSipDomain` as host. INVITE event is then continued.



5.5 Settings for Test Announcement Service

The following settings apply:

- Each test call number is provisioned as a distinct PSI in the HSS.
- Each fictive global number corresponding to a dialed test call number is provisioned as a distinct PSI in the HSS.
- The originating MMTel AS changes the dialed string to a fictive global number (for example +15555550001, 15555550002), and routes the call to the terminating domain, and allows all originating services started on the test announcement call.
- The originating MMTel AS sends out a normalized fictive number. The I-CSCF on the terminating side performs LIR towards the HSS. HSS replies with a LIA including the address (FQDN) of E-TAS, which the I-SCSF uses for incoming call routing, that is, directly to the terminating E-TAS answering the test call.



6 Public Service Identities

The concept of Public Service Identities (PSIs) is used to identity services, service features, and groups, which are hosted by application servers. Each PSI is hosted by an AS, which executes the service logic identified by the PSI. The PSIs are defined in [3GPP TS 23.228 \(V8.8.0\)](#).

1. Statically preconfigured PSIs in the filter information of the users (PSIs only on the originating side).
2. “PSI-users” configured in the HSS, with the following two subcategories:
 - Distinct PSIs, when they are specific public identities and there is a specific entry defined in the HSS for it (with its specific profile and assigned S-CSCF).
 - Wildcarded PSIs, when the PSI is in a range so that when the received public identity matches the wildcard it shares the data with the rest of the public identities matching that range (profile, assigned S-CSCF). Wildcarded PSIs are not sent through the traffic interfaces. They are defined in the SLF and HSS that check if a received specific public identity matches with a defined wildcard.
3. Subdomain-based PSIs, where the AS hosting the PSIs are looked up from the DNS. For this purpose, subdomains can be defined by the operator in the DNS infrastructure.

Depending on the service nature, different mechanisms can be used for configuration and routing of PSIs according to operator preference, see Section 5.4.12 in [3GPP TS 23.228 \(V8.8.0\)](#).

6.1 Settings for Ad-hoc Conferencing Service

The Ad-hoc Conferencing service allows the subscribers to start a conference and invite other users (Conference Participants, CPs) to the conference. The Ad-hoc Conferencing service requires configuration of the following entities:

1. The conference factory - the logical entity responsible for automatically creating a conference focus on demand from a user agent. The conference factory is addressed by the conference factory URI.

The `mtasConfFactoryUri` CM attribute defines the conference factory URI, consisting of a username and a subdomain.

Example: `conference@factory.operator.net`

It is recommended to configure this PSI in the IMS core domain as a subdomain-based PSI.



The MTAS expects the SIP requests destined to the `mtasConfFactoryUri` on the port defined by the `mtasSipPsiPort` CM attribute.

2. The conference focus - the centralized manager of the conference. The focus is addressed by a conference URI.

The `mtasConfUriPrefix` CM attribute defines the username prefix part of the conference URI.

Example: `conf`

The `mtasConfUriSubdomain` attribute defines the subdomain part of the conference URI.

Example: `as1.operator.net`

The prefix and subdomain, together with a non-configurable and automatically generated number, constitute an entire conference URI, `<prefix><auto_number>@<sub_domain>`.

In the MTAS implementation, the requests are routed internally from the conference factory to the conference focus. No external configuration is needed for the conference focus URI.

For more information about the CM attributes described in this section, see [Managed Object Model \(MOM\)](#).

6.2 Settings for 3PTY Service

The 3PTY service allows a user who is involved in two separate 2-party sessions with another two participants to convert to a 3PTY session by reusing the existing dialogs from the 2-party sessions.

The service is triggered in the MTAS by reception of an initial INVITE that has the Request-URI set to the 3PTY factory URI.

The `mtas3ptyFactoryUri` CM attribute defines the 3-party factory URI, consisting of a username and a subdomain. For more information, see [Managed Object Model \(MOM\)](#).

In the MTAS implementation, the requests to the 3PTY factory URI are handled in the originating MTAS, so no routing is done on the Request-URI. No external configuration is needed for the 3PTY factory URI.

6.3 Settings for Group Call Admission Control

The GCAC Supplementary Service enables the operator to restrict the number of sessions the users in the group are involved in. The group-specific configuration of the GCAC service is stored in user data where the group identity is a Public User Identity (PUI). So, for each group a user must be created in the HSS. This user is a



distinct PSI-user. No IFC is to be created for this PSI-user as its purpose is just to hold the group configuration data.

For configuration of the Call Admission Control service in MTAS, see [MTAS Call Admission Control Management Guide](#).

6.4 Settings for Single Radio Voice Call Continuity Release 10

The Single Radio Voice Call Continuity service in the SCC AS uses session anchoring to provide VoLTE UE with continuous MMTel call session when it runs out from coverage of the LTE Packet Switched domain, and needs to transfer its call to the Circuit Switched domain. The SRVCC Release 10 anchors the session in the home IMS network but the media is anchored in the serving IMS network to provide the VoLTE UE with a fast access transfer.

The registration procedure in SRVCC Rel-10 allows dynamic STN-SR allocation. When the VoLTE moves to another network, then the ATCF of the visited network allocates its own STN-SR for the given VoLTE contact. In that case, SCC AS sends a SIP MESSAGE to ATCF with ATU-STI associated with C-MSISDN of the registering contact on receipt of 3rd Party Registration. The SCC AS also updates the HSS with the new STN-SR / C-MSISDN allocation.

The `mtasSrvccAtuSti` CM attribute defines the ATU-STI value assigned to the SCC AS node that is used for initiating access transfer using SRVCC. For more information, see [MTAS SRVCC Management Guide](#).





7 Dynamic Allocation Configuration

The MTAS does not store user subscription data. Instead the HSS transparent data repository is used as centralized storage of all MTAS data (subscriber service profiles, Supplementary Services data). This means that there is no resource in a given physical MTAS tied to any subscriber. A given MTAS AS is allocated to a user at IMS registration time.

This dynamic allocation concept brings the following benefits:

- Pooling concept, to have better resource use
- Increased network availability
- Cost effective N+1 network redundancy
- Centralized storage of subscriber service profiles in the HSS facilitates provisioning (use of transparent data repository)

This dynamic allocation concept is described in Annex J in [3GPP TS 23.228 \(V8.8.0\)](#).

The dynamic allocation mechanism for the MTAS is based on DNS.

7.1 DNS Configuration

Dynamic allocation concept, also called resource pooling, is based on DNS look up. This functionality is triggered when the user registers in the IMS network. The S-CSCF always sends requests to the primary node but failover to the secondary when it determines that the primary is down. The subscriber data is then fetched from the HSS by the selected MTAS and cached as long as the subscriber remains registered.

An example of redundancy configuration using Dynamic Allocation concept is shown in Figure 2. For load sharing purposes, DNS is configured to return the IP address of the primary MTAS nodes based on the S-CSCF IP address. This can be achieved with, for example, Split DNS.

Note: The existence of such traffic steering feature is DNS implementation dependent.

The fourth MTAS is used as stand-by for the other three primary nodes. DNS is configured to return the IP address of the fourth MTAS as secondary address for all S-CSCF source addresses.

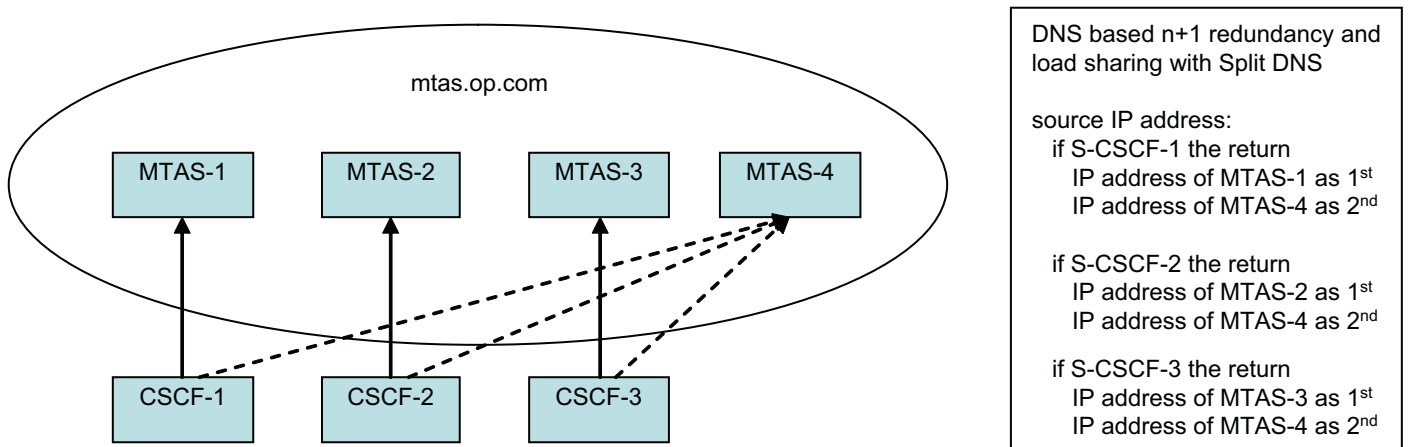


Figure 2 Example of Redundancy Configuration Using Dynamic Allocation Concept

Load sharing can be achieved also by configuring different MTAS nodes for different users in the IFC. If load sharing is achieved through the IFC configuration, similar N+1 redundancy scheme is recommended to be used. The DNS returns the IP address of the same stand-by MTAS as secondary address when translating the domain name of any other primary nodes.

7.2 Dynamic Allocation with AS Instance Caching

If the S-CSCF supports AS instance caching, the S-CSCF caches the IP address of the assigned AS and stores it during the IMS registration period of the user.

The S-CSCF always routes the subsequent originating or terminating service requests directly to the assigned MTAS without DNS lookup. The cached instance address is valid during the registration time of the user.

For AS instance caching to work, MTAS must be configured to support the P-Served-User header. For more information, see [MTAS SIP Management Guide](#).

An example of redundancy configuration using Dynamic Allocation concept with AS instance caching is shown in Figure 3.

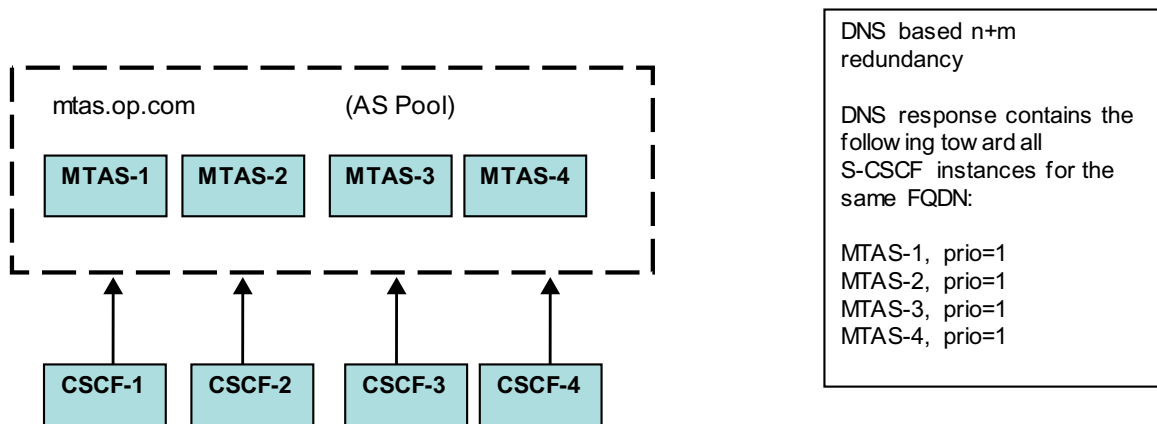


Figure 3 Example of Redundancy Configuration with AS Instance Caching

The DNS is configured to return the IP addresses of all the MTASs from the AS Pool and CSCF selects the AS based on round-robin providing n+m redundancy.

If CSCF determines that the assigned MTAS is down, it selects the next available MTAS, routes the request, and caches the AS for subsequent request. However for users with group-based MMTel Services, since the services must be delivered by the same MTAS, the IFC for the users must be still configured with dedicated AS.





8 DNS-Based Redundancy and Load Sharing of External Server Nodes

When acting as User Agent Client (UAC), the MTAS supports DNS-based redundancy of the next hop SIP server (proxy or User Agent Server (UAS)). MTAS also supports the DNS-based redundancy of the external HTTP servers.

When more than one IP address is received from the DNS, the request is resent to the next address if the connection to the first one cannot be established because of connectivity problems, or the request encounters time-out.

The queries used on the DNS interface for an external server node depend on how the address of the external server node is configured in MTAS, see Table 1 for more details.

Table 1 Queries on the DNS Interface

Address Type	DNS Query	Redundancy	Load Sharing
IP address	No	No	No
Hostname (port != 0)	A or AAAA	Yes	DNS-based
Domain name (port == 0)	<ul style="list-style-type: none"> • SRV • A or AAA 	Yes	DNS- and MTAS-based

The order of the IP addresses used when sending request to the external server nodes, depends on configuration of both of the DNS and of the MTAS.

8.1 SRV Records

The SRV records usually identify host machines serving both load sharing and redundancy purposes. The MTAS internal DNS Resolver first sorts the received SRV records based on their priority, and then execute weighted randomization of the records with same priority according to their weight.

8.2 A/AAAA Records

The A/AAAA records usually identify interfaces of a host machine serving both redundancy purposes. The MTAS internal DNS Resolver does not rotate A/AAAA records. However, the DNS servers can include a configuration option to rotate the A/AAAA records at each DNS query. To rotate the addresses for each traffic session, the TTL of the A/AAAA record must be set to 0; this way the DNS Resolver is forced to query the DNS for each new session to the external node.



8.3 Actual IP Address List of an External Server

The MTAS services are receiving a full list of IP addresses of an external server from the DNS Resolver (after all applicable SRV and A/AAAA queries) for each new session. The MTAS services are using the IP addresses, considered to be reachable, in the same order as received from the DNS Resolver.

When an address is considered to be not reachable at that moment of the session setup, it is moved to the end of the list.

For more information on the MTAS configuration of the DNS-based redundancy, see the following documents:

- Managed Object Model (MOM)
- MTAS Calling Name Identity Presentation Management Guide
- MTAS SIP Management Guide
- MTAS Parlay X Management Guide
- MTAS Customized Alerting Tones Management Guide



9 Configuration of Differentiated Services (DiffServ)

The MTAS supports Differentiated Services Code Point (DSCP) marking of the outgoing SCTP, SIP messages, and DNS queries. The DSCP is the six most significant bits of the (former) IPv4 TOS octet or the (former) IPv6 Traffic Class octet. It is used to identify the level of service a packet receives in the network. All routers in the DiffServ domain must be configured to be able to deal with the DSCP and provide the desired Per-Hop Behavior.

To achieve consistent and predictable behavior, signaling protocols involved in establishment of communication such as DNS, SIP, and Diameter, are recommended to be configured with the same DSCP marking.

For configuration of the DSCP marking value in the MTAS, see the following:

- DNS-Application Managed Object (MO)
- MTAS SIP Management Guide
- MTAS SS7 Management Guide





10 User Provisioning

This section describes user provisioning.

10.1 Subscription and Service Profile Administration in HSS

The 3GPP user profile is described in [3GPP TS 29.228 \(V8.6.0\)](#).

For details on configuration within the MTAS, see *MTAS Subscriber Data Management Guide*.

In general, without referring to any specific HSS, the following sections describe the data that must be configured for a user.

10.1.1 IMS Subscription Administration

The IMS Subscription Administration configures the subscriber. The subscriber is the entity responsible for the payment of the charges applied to the associated users.

The following attribute is provisioned for a subscriber:

— Charging Node Addresses

This attribute identifies the primary and secondary CDFs and OCF nodes that perform the charging for the subscriber.

Note: The `mtasChargingDefaultCdfAddress` CM attribute defines the CDF address to be used by the MTAS node for offline charging purposes in the absence of charging function Address Information from the S-CSCF. For more information about the attribute, see *Managed Object Model (MOM)*.

During Ad-hoc Conferencing sessions, the conference focus gets the charging function address and MSISDN information configured against the Conference Creator from the HSS. The information is used when sending charging messages from the conference focus for Conference Participant legs.

For more information about the interface used in Ad-hoc Conferencing, see *Sh/Dh Interface*.

10.1.2 Service Profile Administration

The Service Profile Administration configures the Public Identities, MSISDNs, and the IFC associated with an IMS Subscription.



The following attributes are provisioned for a service profile:

— PUI

This attribute is used by any user requesting communication with other user.

— MSISDN

This attribute is used to identify the MSISDN number assigned to the user.

Note: The MTAS uses the MSISDN as the Subscription ID for charging purposes when it is present in the Route header. When the MSISDN number is not present in the Route header, the default PUI is used. During Ad-hoc Conferencing sessions the conference focus gets the MSISDN information configured against the Conference Creator from the HSS, see [Sh/Dh Interface](#).

— IFC

This attribute defines the Service Trigger Points and their relations to Application Servers. For more information, see [Section 5](#) on page 15.

— IRS

This attribute identifies the Implicit Registration Set of the user which the public identity belongs to. There can be several Implicit Registration Sets per IMS subscription.

— Is Default Indicator

This attribute indicates if the public identity is the default one of it is IRS.

Note: The MTAS expects the first public identity in the received IRS to be the default one, and it must be a SIP URI. This PUI used as key for later HSS transactions on the Service Profile.

— Maximum Simultaneous Session

This attribute indicates the maximum number of SIP sessions allowed at the same time.

Note: Some HSS implementation supports this attribute. However, this is not defined by 3GPP and not supported by the MTAS either. The maximum number of parallel MMTel sessions that a PUI can have, is defined by the `mtasMmtMaxNumberOfSessions` CM attribute. For more information about that attribute, see [Managed Object Model \(MOM\)](#).

The Call Admission Control (CAC) Supplementary Service enables the operator to restrict further the number of sessions a served user or a group of users are involved in. For more information, see [MTAS Call Admission Control Management Guide](#).



10.2 Provisioning in MTAS

The user provisioning in the MTAS is supported through the CAI3G interface, see Section 3.11 CAI3G Interface on page 9.

CAI3G is a synchronous, request, or response-based provisioning interface. The interface is defined in XML and uses SOAP to format the interface into messages. SOAP messages are carried by HTTP methods.

The Sh interface is used to access storage on the HSS. The MTAS subscription data is stored as “transparent data” on the HSS. This means that the HSS is unaware of the structure of the data except that it must be well-formed XML. For details on Sh interface, see Section 3.2 Sh Interface on page 6.





11 Rebalancing

The rebalancing feature can be deactivated manually by operator or automatically when the active number of subscribers registered on the node falls below the configured threshold.

The rebalancing can also be deactivated when subscribers are deregistered from the node upon expiry of the MTAS registration timers `mtasSubsDataDefaultRegTimer` and `mtasSubsDataDeregTimer`.

The values of following MTAS registration timers that are related to the caching interval of user data must be synchronized between the S-CSCF and the MTAS nodes:

`mtasSubsDataDefaultRegTimer`

This attribute defines what value is used for registration timer for registered users in Subscriber Data component. This timer defines the maximum time subscriber data remains in the cache. The value is to be greater than or equal to the typical registration lifetime in the S-CSCF to allow receiving a re-registration before the expiry of the timer.

`mtasSubsDataDeregTimer`

This attribute defines the duration of the deregistration timer for unregistered users in Subscriber Data component. This timer defines how long subscriber data remains in the cache after termination of the last session for an unregistered subscriber. The timer is started when the last call for the unregistered subscriber is completed. It is stopped when a new session is initiated for the subscriber.

When rebalancing is active and the registration timer expires for an idle user, the deregistration procedure is implemented as follows:

- If the number of registered users falls below the threshold upon de-registration, the rebalancing feature is deactivated. Else, it remains active.
- The deregistration is graceful. MTAS sends terminating NOTIFY to devices with DEN subscription.

For more information on rebalancing, see [MTAS Subscriber Data Management Guide](#).





12 Deployment-Dependent Configurations

The following sections describe the network configurations of the MTAS services that depend on deployment, that is, on the capabilities and configuration of other nodes in the IMS network.

12.1 AS-Controlled Forking

The AS-Controlled Forking feature makes it possible for other MTAS services to address specific terminals of the served user registered with the same IRS with the help of the terminal selectors.

The AS-Controlled Forking is based on the following concepts and procedures introduced in [RFC 3840](#) and [RFC 3841](#):

Callee Preferences

[RFC 3840](#) (Indicating User Agent Capabilities in the Session Initiation Protocol) defines mechanisms by which a UE can convey its capabilities and characteristics to other user agents and to the registrar for its domain. This information is conveyed as feature parameters of the Contact-header field of the REGISTER method. The MTAS supports only the feature tags without values.

Caller Preferences

[RFC 3841](#) (Caller Preferences for the Session Initiation Protocol) defines a set of extensions to the SIP which allow a caller to express preferences about request handling in servers. These preferences include the ability to select which Uniform Resource Identifiers a request gets routed to, and to specify certain request handling directives in proxies and redirect servers. It does so by defining three new request header fields, Accept-Contact, Reject-Contact, and Request-Disposition, which specify the preferences of the caller. The MTAS uses only the Accept-Contact header.

The terminal selector is a feature parameter that is used for addressing a single terminal when more than one terminal belongs to the same PUI or IRS. The terminal selector used in SIP signaling by the MTAS consists of two parts; the provisioned terminal selector and the configured terminal selector prefix defined by the `mtasMmtTerminalSelectorPrefix` CM attribute. For the concepts and configuration of the terminal selectors in relation with the AS-Controlled Forking feature in the MTAS, see [MTAS Target Handling Management Guide](#).

For use of the terminal selectors by the MTAS services, see the relevant service User Guides.

The AS-Controlled Forking feature expects the feature parameters identifying the terminals included in the Contact header field of the REGISTER method.

The feature parameters can be provided by the terminals. If in the actual network deployment the terminals provide the needed feature parameters in the Contact-header field of the REGISTER method, no further configuration is needed in the network.

If the terminals cannot provide the needed feature parameters, a network-based workaround is needed. One example of the network-based workaround is described in Section 12.1.1 Network-Based Workaround on page 54.

12.1.1 Network-Based Workaround

An overview of the example workaround is shown in Figure 4.

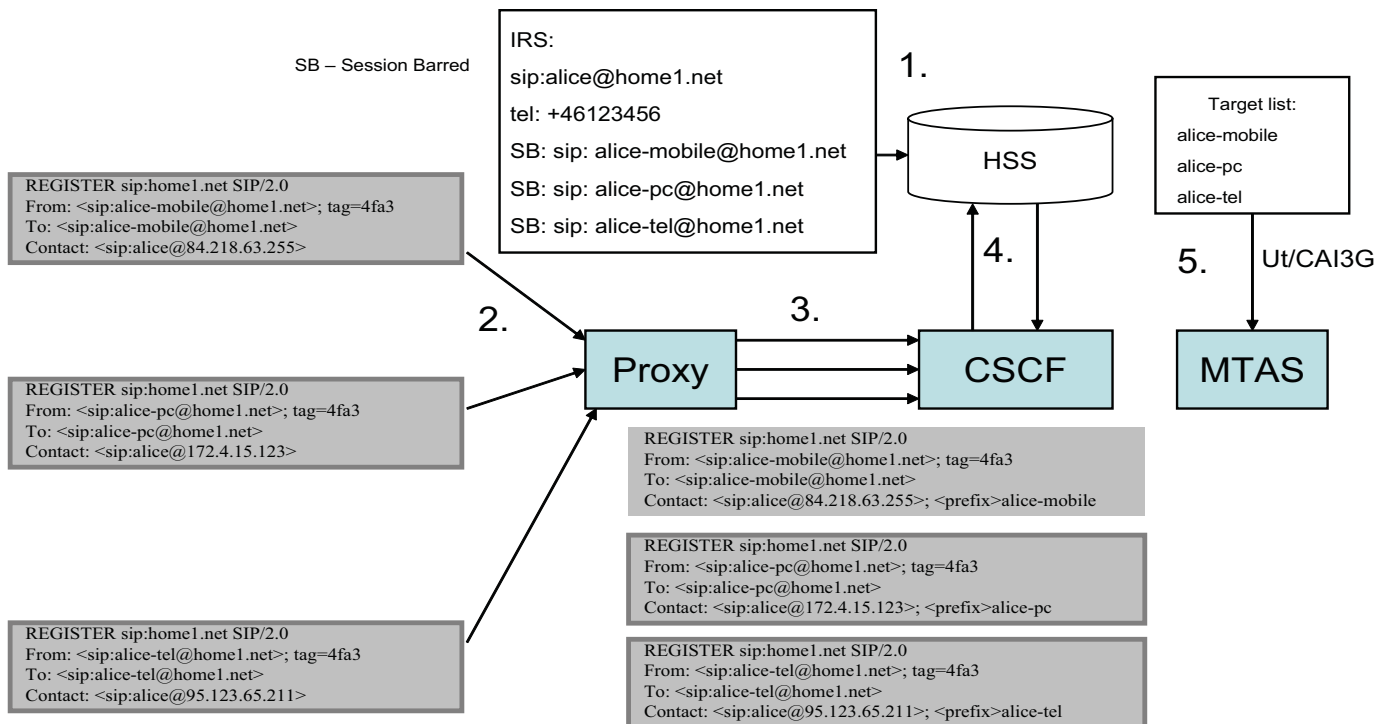


Figure 4 Example of Network-Based Workaround of Feature Parameter Registration

12.1.1.1 IRS Configuration

It is a common feature of the IMS terminals to allow the selection of the registered public identity.

The IRS that is provisioned for the user in HSS includes both the IMPUs that are used in the session handling as well as the “temporary” IMPUs that correspond to the terminals that Alice owns. These temporary IMPUs are “session barred” in HSS, which means they can be used for registration only. They are not included



in the P-Associated-URI list either, which means that the terminals cannot be addressed by using them.

Note: The existence of “session barred” IMPU attribute is HSS implementation-dependent.

12.1.1.2 Proxy Configuration

The proxy node in the network extracts either the whole user part or a fragment of the user part from the To-header and inserts it as a feature parameter in the Contact-header.

A prefix can be defined on the network level by the operator, so that the resulting feature parameter is always unique, for example, `<prefix>="+g.operator."`. If such a prefix is defined in the network by the operator, the same prefix must be configured in the proxy node, and in the MTAS `mtasMmtTerminalSelectorPrefix` CM attribute.

Note: The existence of such a proxy node capable to SIP header modification is deployment-dependent.

The SIP Message Manipulation feature of the Session Border Gateway (SBG) node can do such header modification, see the documentation for SBG for further information.

12.2 Originating AS Chaining

MTAS can be configured to support Originating AS chaining, this means to support external triggering of originating services in one or more AS after a call has been retargeted.

For more information about Originating AS chaining in MTAS, see the following documents:

- MTAS SIP Management Guide
- MTAS Interface to CSCF (ISC, Ma, Pw)

When an S-CSCF is configured to trigger originating services after retargeting (the Originating CDIV session case), an IFC trigger is set per user, the user is then allocated to an MTAS that has this behavior enabled.

For more information about the Originating CDIV session case, see [3GPP TS 29.228 \(V8.6.0\)](#).

Note: For callout of blue sessions, the maximum number of sessions defined in the MMTel CM Parameter `mtasMmtMaxNumberOfSessions` must be increased when all Conference Dial-Out requests start originating sessions for the Conference Creator in the originating AS.



12.3 MTAS Services Suppression Based on the INVITE Method

An S-CSCF or an AS before MTAS in the ISC chain can trigger suppression of some selected and configured services in MTAS by providing an INVITE method that contains a header and parameter in pair that matches the regular expression configured in the `MtasFsfsPattern` managed object by the Flexible Service Format Selection (FSFS) service.

For more information about the FSFS service, see [MTAS Flexible Service Format Selection Management Guide](#).

When the MTAS services are suppressed, the communication session is processed as if the services were not active.

12.4 Served User without MMTel Subscription

MTAS can be configured to support served user without MMTel subscription, that is, user without a provisioned MMTel service document in HSS. CSCF adds a specific Route header parameter with the same value configured in the CM attribute `mtasMmtNoSubscriptionRouteParameter`. This attribute specifies whether the user has an MMTel subscription. Outgoing calls of users without MMTel subscription are by default barred, unless the called number matches a white listed destination.

SCC AS is not triggered for the scenario.

12.5 Deployment-Dependent Configurations for Multi-Mobile Support

MMTel AS supports user with multiple mobile subscriptions within a single IRS, ensuring the same end-user experience for each mobile subscription. All PUIs of the user are in the same IRS/IMS subscription and all IMPIs associated with the Mobile subscription are also connected to same IRS/IMS subscription, see Figure 5.

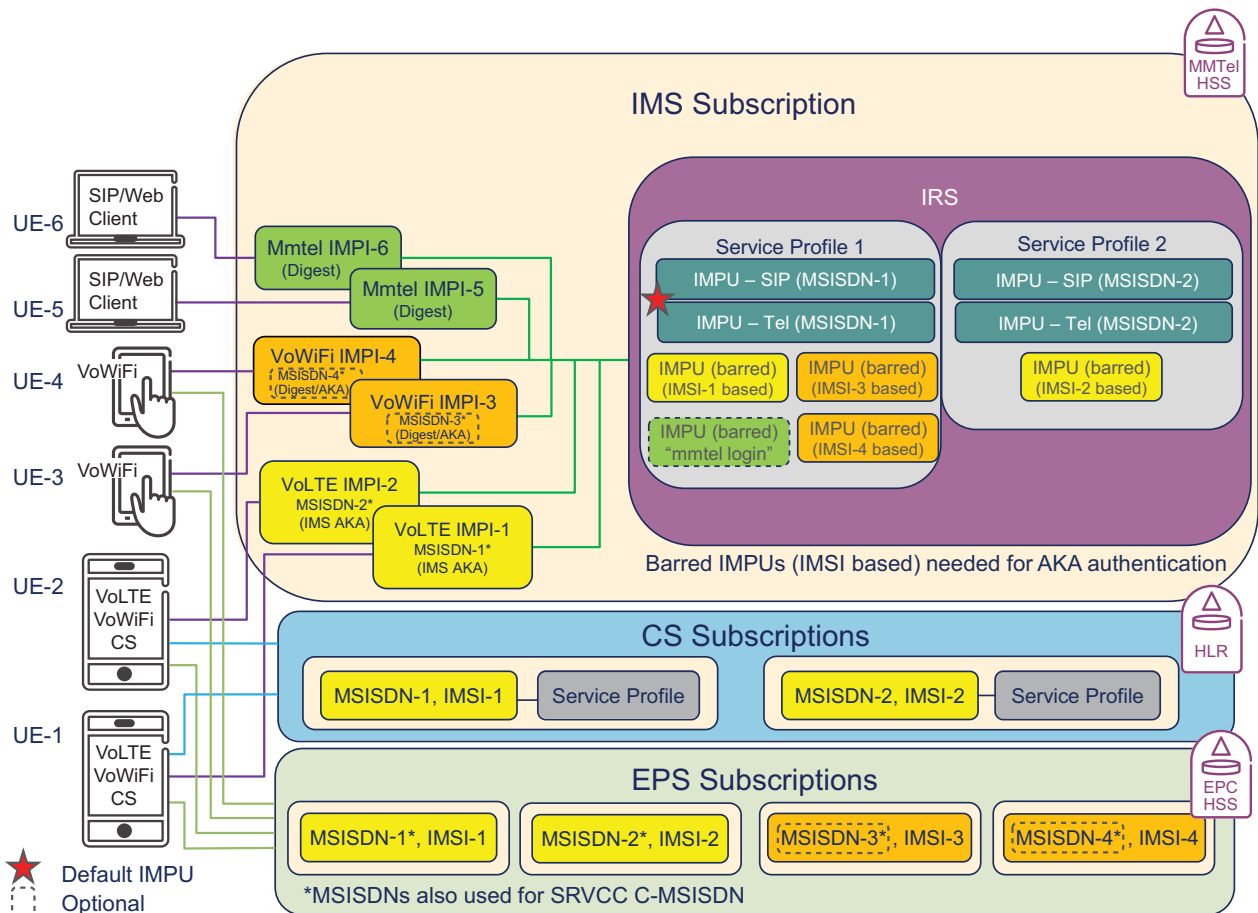


Figure 5 HSS Data Model

To distribute a call to provisioned mobile subscriptions, Originating UE supports the P-Early-Media header field as defined in IETF RFC 5009 and includes a P-Early-Media header field with the supported parameter to INVITE requests it originates as specified in 3GPP TS 24.229.

For calls originated not (directly) from an IR.92 UE, there must be an upstream node capable of P-Early-Media header-based media gating, acting on behalf of the originating UE. In the Ericsson portfolio, the SBG is capable to this gating.

For identification of the originating calls from a registered mobile, the Contact header or the P-Ericsson-Original-Contact header is used. If there is a B2BUA before the SCC AS changing the Contact header in the INVITE or SUBSCRIBE message, There must be a node copying the original Contact header to the P-Ericsson-Contact header. In the Ericsson portfolio, the SBG is capable to this header copying with an SMM script.

For the Multi-Mobile feature to work, MTAS must be able to match registered Contacts with IMPIs provisioned in the Mobile-Subscription-List. In failover cases, registration data is fetched from the S-CSCF through the registration event package (SUBSCRIBE/NOTIFY messages). The registration information sent by S-CSCF must contain the IMPIs of the registered Contacts. In Ericsson S-CSCF, this



can be configured by enabling the `scscfExtendedRegistrationEventEnabled` CM parameter. For more information, see the Managed Object Model (MOM) in the CSCF Customer Product Information (CPI).



13 Configuration for Sub-Network Manager

This section describes the configuration of the MTAS for remote access by Sub-Network Manager (SNM) or any other Network Management System.

13.1 Configure SFTP Users and Port

SFTP users and port must be configured for remote access by the SNM for file collection.

A dedicated `oss_pm` user and port 115 are used for SFTP access.

Prerequisites

- An ECLI session in Exec mode is in progress.
- The user is connected to the node using CLISS.

Steps

1. Change password policy, see Section 13.1.1 Change Password Policy on page 59.
2. Create account policy for the `oss_pm` user, see Section 13.1.2 Create Account Policy for `oss_pm` User on page 60.
3. Create password policy for the `oss_pm` user, see Section 13.1.3 Create Password Policy for `oss_pm` User on page 61.
4. Create user account for the `oss_pm` user and assign `Mtas_Application_Operator_OSSUser` role, see Section 13.1.4 Create `oss_pm` User and Assign `Mtas_Application_Operator_OSSUser` Role on page 62.
5. Configure the minimum password quality points to the Password Quality, see Section 13.1.5 Configure Minimum Password Quality Points to Password Quality on page 63.
6. Reset Password, see Section 13.1.6 Reset Password on page 64.
7. Activate the `oss_pm` user, see Section 13.1.7 Activate User on page 64.
8. Unlock Local Authorization method, see Section 13.1.8 Unlock Local Authorization Method on page 65.
9. Ensure that the `oss_pm` user has user access permissions, see Section 13.1.9 Ensure `oss_pm` User Has User Access Permissions on page 66.

13.1.1 Change Password Policy

Steps



1. Navigate to the `LocalAuthenticationMethod` MO, for example:

```
>dn ManagedElement=1,SystemFunctions=1,SecM=1,UserManagement=1
,LocalAuthenticationMethod=1
```

2. Enter Config mode:

```
(LocalAuthenticationMethod=1)>configure
```

3. Create the `PasswordPolicy` MO, for example:

```
(config-LocalAuthenticationMethod=1)>PasswordPolicy=1
```

4. Set the `PasswordPolicy` attributes according to operators password policy, in case the values differ from default values, for example:

```
(config-PasswordPolicy=1)>minLength=10
```

5. Set the password quality by giving a reference to the `PasswordQuality` MO, for example:

```
(config-PasswordPolicy=1)>passwordQuality="ManagedElement=1,Sys
temFunctions=1,SecM=1,UserManagement=1,LocalAuthenticationMetho
d=1,PasswordQuality=1"
```

6. Verify the settings:

```
(config-PasswordPolicy=1)>show -v
```

The following is an example output:

```
PasswordPolicy=1
  expireWarning=7 <default>
  failureCountInterval=1800 <default>
  historyLength=12 <default>
  lockoutDuration=[] <empty>
  maxAge=90 <default>
  maxFailure=3 <default>
  minAge=15 <default>
  minLength=10 <default>
  passwordPolicyId="1"
  passwordQuality="ManagedElement=1,SystemFunctions=1,SecM=1,⇒
  UserManagement=1,LocalAuthenticationMethod=1,PasswordQuality=1"
  reservedByAccount=[] <empty> <read-only>
  userLabel=[] <empty>
```

7. Commit the settings:

```
(config-PasswordPolicy=1)>commit
```

13.1.2 Create Account Policy for oss_pm User

Steps

1. Navigate to the `LocalAuthenticationMethod` MO, for example:

```
>dn ManagedElement=1,SystemFunctions=1,SecM=1,UserManagement=1
,LocalAuthenticationMethod=1
```




2. Enter Config mode:

```
(LocalAuthenticationMethod=1)>configure
```

3. Create the `AccountPolicy` MO, for example:

```
(config-LocalAuthenticationMethod=1)>AccountPolicy=1
```

4. Set `AccountPolicy` attributes according to operators account policy, in case the values differ from defaults, for example:

```
(config-AccountPolicy=1)>dormantTimer=360
```

5. Commit the settings:

```
(config-AccountPolicy=1)>commit
```

6. Verify the settings:

```
(AccountPolicy=1)>show -v
```

The following is an example output:

```
AccountPolicy=1
  accountPolicyId="1"
  dormantTimer=360
  reservedByAccount=[] <empty> <read-only>
  userLabel=[] <empty>
```

13.1.3

Create Password Policy for oss_pm User

Steps

1. Navigate to the `LocalAuthenticationMethod` MO, for example:

```
>dn ManagedElement=1,SystemFunctions=1,SecM=1,UserManagement=1
,LocalAuthenticationMethod=1
```

2. Enter Config mode:

```
(LocalAuthenticationMethod=1)>configure
```

3. Create the `PasswordPolicy` MO, for example:

```
(config-LocalAuthenticationMethod=1)>PasswordPolicy=1
```

4. Set the `PasswordPolicy` attributes:

```
(config-PasswordPolicy=1)>minLength=6
```

5. Verify the settings:

```
(config-PasswordPolicy=1)>show -v
```



The following is an example output:

```

PasswordPolicy=1
  expireWarning=7 <default>
  failureCountInterval=1800 <default>
  historyLength=12 <default>
  lockoutDuration=[] <empty>
  maxAge=90 <default>
  maxFailure=3 <default>
  minAge=15 <default>
  minLength=6 <default>
  passwordPolicyId="1"
passwordQuality="ManagedElement=1, SystemFunctions=1, SecM=1, ⇒
  UserManagement=1, LocalAuthenticationMethod=1, PasswordQuality=1"
  reservedByAccount=[] <empty> <read-only>
  userLabel=[] <empty>

```

6. Commit the settings:

```
(config-PasswordPolicy=1)>commit
```

13.1.4 Create oss_pm User and Assign Mtas_Application_Operator_OSSUser Role

Steps

1. Navigate to the `UserAccountM` MO, for example:

```
(PasswordPolicy=1)>dn ManagedElement=1, SystemFunctions=1, SecM=1
, UserManagement=1, LocalAuthenticationMethod=1, UserAccountM=1
```

2. Verify that no user account for username `oss_pm` exists:

```
(UserAccountM=1)>show UserAccount=oss_pm
```

Result:

ERROR: Specific element not found

3. Enter Config mode:

```
(UserAccountM=1)>configure
```

4. Create the `oss_pm` `UserAccount` MO:

```
(config-UserAccountM=1)>UserAccount=oss_pm
```

Note: `oss_pm` is the username used at logon.

5. Set the account policy for the account by giving a reference to the appropriate `AccountPolicy` MO, for example:

```
(config-UserAccount=oss_pm)>accountPolicy="ManagedElement=1, Sys
temFunctions=1, SecM=1, UserManagement=1, LocalAuthenticationMet
hod=1, AccountPolicy=1"
```

6. Set the password policy for the account by giving a reference to the appropriate `PasswordPolicy` MO, for example:



```
(config-UserAccount=oss_pm)>passwordPolicy="ManagedElement=1,SystemFunctions=1,SecM=1,UserManagement=1,LocalAuthenticationMethod=1>PasswordPolicy=1"
```

7. Set the full name of the oss_pm user account:

```
(config-UserAccount=oss_pm)>userName="OSSNBI"
```

Note: This attribute contains a descriptive name of the user, not the logon ID.

8. Assign the roles for the oss_pm user, for example:

```
(config-UserAccount=oss_pm)>roles=[Mtas_Application_Operator_OSSUser]
```

9. Commit the settings:

```
(config-UserAccount=oss_pm)>commit
```

10. Verify the settings, for example:

```
(UserAccount=oss_pm)>show -v
```

The following is an example output:

```
UserAccount=oss_pm
  accountPolicy="ManagedElement=1,SystemFunctions=1,SecM=1,⇒
UserManagement=1,LocalAuthenticationMethod=1,AccountPolicy=1"
  accountState=UNLOCKED <read-only>
  accountUsageState=UNUSED <read-only>
  administrativeState=UNLOCKED
  lastLoginTime="" <read-only>
  lockedTime="" <read-only>
  passwordChangedTime="20151110161432Z" <read-only>
  passwordFailureTimes=[] <empty> <read-only>
  passwordPolicy="ManagedElement=1,SystemFunctions=1,SecM=1,⇒
UserManagement=1,LocalAuthenticationMethod=1>PasswordPolicy=1"
  passwordState=EXPIRED_MUSTCHANGE <read-only>
  roles
    "Mtas_Application_Operator_OSSUser"
  userName="OSSNBI"
```

13.1.5 Configure Minimum Password Quality Points to Password Quality

Steps

1. Navigate to the PasswordQuality MO, for example:

```
(UserAccount=oss_pm)>ManagedElement=1,SystemFunctions=1,SecM=1,UserManagement=1,LocalAuthenticationMethod=1>PasswordQuality=1
```

2. Enter Config mode:

```
(PasswordQuality=1)>configure
```

3. Set the minPoints attribute for the oss_pm user:



```
(config-PasswordQuality=1)>minPoints=1
```

4. Verify the settings:

```
(config-PasswordQuality=1)>show -v
```

The following is an example output:

```
PasswordQuality=1
minDigit=1
minLower=1
minOther=1
minPoints=1
minUpper=1
passwordQualityId="1"
reservedBy <read-only>
"ManagedElement=1,SystemFunctions=1,SecM=1,UserManagement=1,⇒
LocalAuthenticationMethod=1,AdministratorAccount=la-admin"
"ManagedElement=1,SystemFunctions=1,SecM=1,UserManagement=1,⇒
LocalAuthenticationMethod=1>PasswordPolicy=1"
userLabel=[] <empty>
```

5. Commit the settings:

```
(config-PasswordQuality=1)>commit
```

13.1.6

Reset Password

Steps

1. Set the password for the created oss_pm user:

```
(UserAccount=oss_pm)>resetPassword --noChange --password
```

2. Enter the new password:

```
(UserAccount=oss_pm)>resetPassword --noChange --password
*****
```

13.1.7

Activate User

Steps

1. Enter Config mode:

```
(UserAccount=oss_pm)>configure
```

2. Activate the oss_pm user, set the administrative state to UNLOCKED:

```
(config-UserAccount=oss_pm)>administrativeState=UNLOCKED
```

3. Commit the settings:

```
(config-UserAccount=oss_pm)>commit
```

4. Verify the settings, for example:

```
(UserAccount=oss_pm)>show -v
```



The following is an example output:

```
UserAccount=oss_pm
  accountPolicy="ManagedElement=1, SystemFunctions=1, SecM=1, UserManagement=1, ⇒
  LocalAuthenticationMethod=1, AccountPolicy=1"
  accountState=LOCKED <read-only>
  accountUsageState=UNUSED <read-only>
  administrativeState=UNLOCKED
  lastLoginTime=[] <empty> <read-only>
  lockedTime="2017-11-30T09:58:36Z" <read-only>
  passwordChangedTime=[] <empty> <read-only>
  passwordFailureTimes=[] <empty> <read-only>
  passwordPolicy="ManagedElement=1, SystemFunctions=1, SecM=1, UserManagement=1, ⇒
  LocalAuthenticationMethod=1, PasswordPolicy=1"
  passwordState=[] <empty> <read-only>
  roles
    "Mtas_Application_Operator_OSSUser"
  userAccountId="oss_pm"
  userLabel=[] <empty>
  userName="OSSNBI"
```

13.1.8 Unlock Local Authorization Method

Steps

1. Navigate to the `LocalAuthorizationMethod` managed object, for example:

```
>dn ManagedElement=N0DE06ST, SystemFunctions=1, SecM=1, UserManagement=1, LocalAuthorizationMethod=1
```
2. Enter Config mode:

```
(LocalAuthorizationMethod=1)>configure
```
3. Unlock the local authorization method:

```
(config-LocalAuthorizationMethod=1)>administrativeState=UNLOCKED
```
4. Commit the setting:



Attention!

Risk of data loss or data corruption.

The change of state affects existing and new ECLI and NETCONF sessions, possibly closes open connections and blocks logon access for users not defined in `LocalAuthenticationMethod`.

```
(config-LocalAuthorizationMethod=1)>commit
```

5. Connect to ECLI again, if needed.



6. Verify the result:

```
(LocalAuthorizationMethod=1)>show
```

The following is an example output:

```
LocalAuthorizationMethod=1
  administrativeState=UNLOCKED
  [...]
```

The authorization is now enforced according to the defined roles and rules.

13.1.9 Ensure oss_pm User Has User Access Permissions

Steps

1. Verify that the oss_pm user has needed permission on ECLI for the defined Role Mtas_Application_Operator_OSSUser:

```
ssh -p 830 -t -s <sftp user>@<OAM MIP> cli
```

Enter the newly created password from Section 13.1.6 Reset Password on page 64.

2. Copy the sshd template file, and customize the copied file so that the configuration only allows users belonging to the group system_oam to log on and SFTP is the only service available:

```
cp /cluster/storage/system/config/mtas/sshd_config_sftp_filem.
template /cluster/storage/system/config/mtas/sshd_config_sftp
_filem
```

3. Update the sshd_config_sftp_filem with the system-oam group:

```
AllowGroups system-oam
```

```
Match Group system-oam
```

4. Restart COM on the active System Controller (SC) host to trigger the MutaMIP activate and deactivate scripts, to reconfigure the SSH daemon.

- a. Determine activeSCindex and standbySCindex, on any of the SCs enter command:

```
amf-state siass | grep -A 1 -i ComSa
```

The following is an example output:

```
safSISU=safSu=Cmw2\,safSg=2N\,safApp=ERIC-ComSa,safSi=2N,safApp=ERIC-ComSa
saAmfSISUHASstate=STANDBY(2)
--
safSISU=safSu=Cmw1\,safSg=2N\,safApp=ERIC-ComSa,safSi=2N,safApp=ERIC-ComSa
saAmfSISUHASstate=ACTIVE(1)
```



If saAmfSISUHASState=ACTIVE(1 for safSu=Cmw1, then activeSCindex is 1 and standbySCindex is 2.

If saAmfSISUHASState=ACTIVE(1) for safSu=Cmw2, then activeSCindex is 2 and standbySCindex is 1.

- b. Restart the SC:

```
lde-reboot -n <NODE_ID>
```

Where <NODE_ID> is 1 or 2, depending on the active COM.

- c. Restart the COM Availability Management Framework (AMF) component on a campaign-based system:

```
amf-adm lock safSu=Cmw<standbySCindex>,safSg=2N,safApp=ERIC-ComSa
```

```
amf-adm lock-in safSu=Cmw<standbySCindex>,safSg=2N,safApp=ERIC-ComSa
```

```
amf-adm lock safSu=Cmw<activeSCindex>,safSg=2N,safApp=ERIC-ComSa
```

```
amf-adm lock-in safSu=Cmw<activeSCindex>,safSg=2N,safApp=ERIC-ComSa
```

```
amf-adm unlock-in safSu=Cmw<activeSCindex>,safSg=2N,safApp=ERIC-ComSa
```

```
amf-adm unlock safSu=Cmw<activeSCindex>,safSg=2N,safApp=ERIC-ComSa
```

```
amf-adm unlock-in safSu=Cmw<standbySCindex>,safSg=2N,safApp=ERIC-ComSa
```

```
amf-adm unlock safSu=Cmw<standbySCindex>,safSg=2N,safApp=ERIC-ComSa
```

5. Verify that SFTP on port 115 is working for COM FileM Northbound Interface (NBI) to access PMReportFiles, AlarmLogs, and AlertLogs.

```
sftp -oPort=115 <sftp user>@<OAM MIP>
```

Password:

The following is an example output:

```
Connected to 192.168.83.100.
```

6. After connecting to the node, ensure that the oss_pm user can access the system NBI data that is specified to the new role:



```
ls -lrt
```

The following is an example output:

```
drwxrwx--- 2 305 system-nbi-data 4096 Nov 13 05:54 AlertLogs
drwxrwx--- 2 305 system-nbi-data 4096 Nov 13 05:54 AlarmLogs
drwxrws--- 2 311 system-nbi-data 4096 Nov 13 05:55 PerformanceManagementReportFiles
```

7. Verify that SSHD is listening on the active SC host:

```
netstat -tlnp | grep sshd
```

The following is an example output when SSHD listens on port 115:

```
tcp      0      0 0.0.0.0:830      0.0.0.0:*        LISTEN    18295/sshd
tcp      0      0 0.0.0.0:115     0.0.0.0:*        LISTEN    20231/sshd
tcp      0      0 0.0.0.0:22      0.0.0.0:*        LISTEN    18295/sshd
tcp      0      0 192.168.83.100:115 192.168.83.254:36118 ESTABLISHED 11205/sshd: oss_pm
tcp      0      0 :::830         :::*             LISTEN    18295/sshd
tcp      0      0 :::115         :::*             LISTEN    20231/sshd
```




14 Parameter Value Selection for Deployment-Dependent CM Attributes

The deployment-dependent attributes are marked with Access Category “Site Specific” or “Solution Integration” in Managed Object Model (MOM).

Special care must be taken when setting or changing these parameters as coordination with other deployed Network Elements could be necessary. The setting and changing of the attributes marked as “Solution Integration” are normally to be performed by Ericsson trained personnel only.





15 Installation of Additional MTAS Nodes

When installation of additional MTAS nodes is needed for capacity or redundancy reasons, the following external configuration activities are needed:

- Configure the interfaces to the new MTAS node in the neighboring nodes, that is, in MRFP, BSS, SNM, and so on.

Note: Configuration in the CSCF could be necessary, specifically for the domain-based PSIs addressing the new MTAS.

- Configure firewalls, if needed.
- Select the used load sharing method; IFC-based or DNS-based (that is, Split DNS) accordingly.
- Configure the DNS.

Note: Configuration of the ATU-STI with multiple IP addresses in DNS is necessary for the redundant SCC AS configuration.

- Configure IFCs in the HSS, if needed.