System Description

Ericsson IMS Multimedia Telephony

DESCRIPTION

ERICSSON

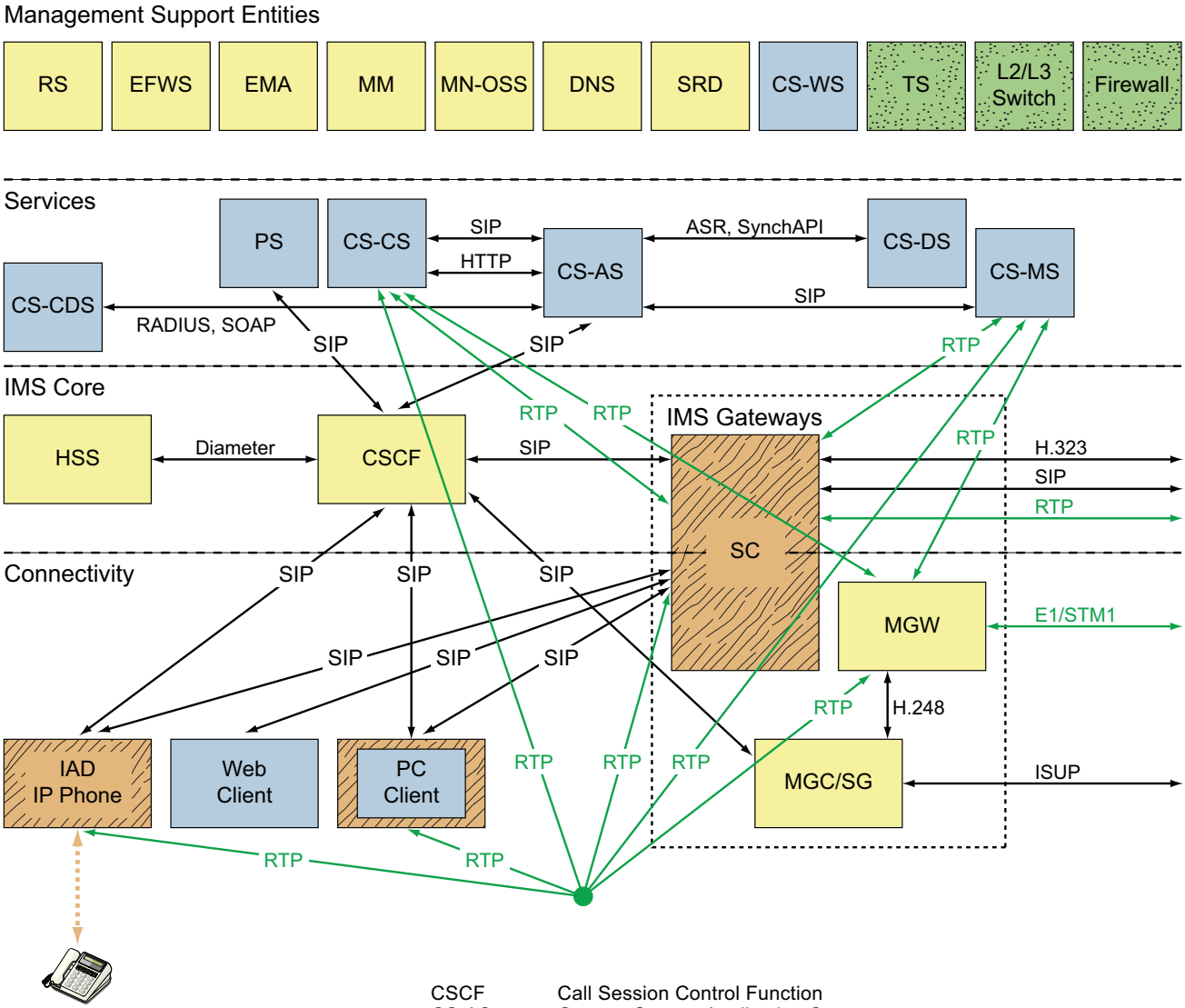
Contents

1 Introduction

This document contains a high level technical description of the Ericsson IMS Multimedia Telephony system, from now on referred to as the system. Obviously, the system is based on Ericsson IP Multimedia System (IMS).

The system enables the delivery of advanced multimedia services, such as IP telephony, video, conference calling, instant messaging, and handling of presence information. The system utilizes Internet Protocol (IP) technology over fixed broadband networks and uses the Session Initiation Protocol (SIP) for control signaling and Real-Time Protocol (RTP) for media transportation. The system supports ISDN User Part (ISUP) for ISDN/PSTN connectivity with SIP and H.323 for external IP network control signaling.

A system overview including the main media and signaling paths is shown in Figure 1 on page 2.



CSCF	Call Session Control Function
CS-AS	Centrex System Application Server
CS-DS	Centrex System Distribution Server
CS-CDS	Centrex System Call Detail Server
CS-CS	Centrex System Conference Server
CS-MS	Centrex System Media Server
CS-WS	Centrex System Web Server
DNS	Domain Name System
EFWS	Ericsson Front-end Web Server
EMA	Ericsson Multi Activation
HSS	Home Subscriber Server
IAD	Integrated Access Device
MGC	Media Gateway Controller
MGW	Media Gateway
MM	Ericsson Multi Mediation
MN-OSS	Multi-service Network Operations Support System
PS	Presence Server
SC	Session Controller
SG	Signaling Gateway
SRD	System Repository and Directory
TS	Terminal Server
RS	Registration Surrogate

Included in the Solution:

Ericsson Products

Integrated 3rd Party Products

Not Included in the Solution:

Off-the-Shelf 3rd Party Products

Interoperability Verification Products

it0106G

Figure 1 System Overview

1.1 Purpose

The purpose of this document is to provide a high-level technical overview of the system. The document includes references to other documents that contain more detailed information.

1.2 Scope

The scope of the document is to:

- Provide a fundamental understanding of the system's purpose and functionality
- Provide an architectural overview of the system and describe the system boundary, internal architecture, and interfaces

The definition and explanation of abbreviations and terminology is found in the following document:

- *Terms and Definitions – Ericsson IMS*, Reference [12]

1.3 Document Structure

The document provides the reader with a top-down presentation of the system, starting with high-level introduction defining the system boundary, explaining the main purpose of the system, and presenting a logical system overview.

The remaining parts of the document depict a number of architectural views to highlight different aspects of the system. Furthermore, the provided functionality for management and support functions are described.

Below is a short description of each section in the document:

System Boundary	This section defines the system boundary and describes the interfaces between the system and the external actors.
Services Overview	This section explains the main purpose of the system. Additional and supporting functionality are described later in the document.
System Overview	This section presents a logical overview of the system, its concepts and functional entities, providing a basic understanding of the system.
Standards, Interfaces, and Protocols	This section describes the standards, to which the system complies, as well as the internal and external interfaces and corresponding protocols used.

Basic Interworking	This section gives a short description of system supported codecs and basic services in the Ericsson IMS Multimedia Telephony solution.
Data Model	This section provides an overview of the distribution of subscription and user data in the system.
Data View	This section describes the high-level data models of the system and the dependencies between these models for storing subscriber, group, and service provider data.
Platform Technology	This section describes the platforms used by the system and maps the subsystem nodes to the platforms.
Deployment View	This section describes the deployment view of the system on a conceptual level.
Characteristics	This section contains information regarding the system characteristics. The principles for achieving high availability and scalability are also described.
Provisioning Services	This section describes the system's provisioning services.
Charging	This section describes the system's charging and mediation services.
Operation and Maintenance Services	This section describes the system's fault, configuration, and performance management services.
Security	This section describes the system's security mechanisms.
References	This section contains the list of references.

1.4 Revision Information

Other than editorial changes, this document has been revised from revision G to revision H according to this section.

1.4.1 Revised

References to Multi Mediation 5.0 documentation are updated.

2 System Boundary

This section defines the system boundary and describes the external actors.

The external interfaces and actors are shown in Figure 2 on page 5.

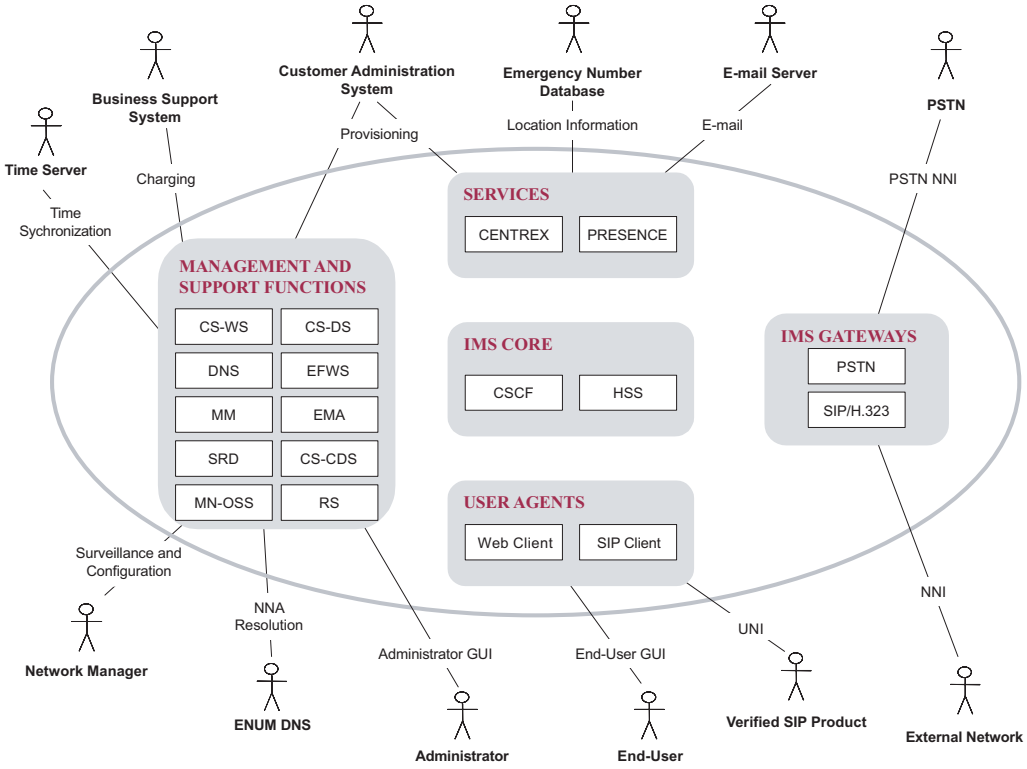


Figure 2 Actors and External Interfaces

The following subsections give a brief description of each actor and the interaction with the system. External interfaces and used protocols are defined in Section 5.2 External Reference Points on page 47.

2.1 End-User

The end-user is a person subscribing to the services offered by the system.

The end-user accesses the system through the End-User Graphical User Interface (GUI) for session establishment, media transportation, and configuration of end-user preferences (that is, using the client applications).

It is also possible that through this GUI provide the end-user with a possibility for self provisioning (activation and deactivation) of certain defined services.

The end-user services offered by the system are described in Section 3.1 End-User Services on page 9.

2.2 Administrator

The administrator is a person responsible to configure and maintain a group of end-users and their services in the system.

The following types of administrator exist:

- System Provider
- Service Provider
- Group Administrator
- Department Administrator

The administrators uses the web client to access the provisioning GUI, provided by the Centrex Services (CS) subsystem, to administer the end user's data and preferences. Additionally, system providers can also use a CLI.

The system's provisioning services are described in Section 12 Provisioning Services on page 87.

2.3 CAS – Customer Administration System

The Customer Administration System (CAS) is part of the system provider's legacy system and provides the customer care with a unified access point to the system's subscriber and service data through the provisioning reference point.

The Ericsson Multi Activation (EMA), described in Section 4.7.5 EMA – Ericsson Multi Activation on page 39, and the CS subsystem, described in Section 4.5 CS – Centrex Services on page 31, provide the system's core provisioning functionality.

2.4 EN-DB – Emergency Number Database

This is an external entity that may provide fully routable destinations to Emergency Call Centres based on location information provided by an emergency call. Its interface is based on SOAP/XML.

The basic idea is that if the network can provide reliable information about the physical location for a certain call, this information should be used to find a proper emergency call centre that serves the location in question.

Information about physical location can be provided in any SIP request.

2.5 BSS – Business Support System

The Business Support System (BSS) is part of the system provider's legacy system and is responsible for collecting and processing the charging data that is provided by the system.

The charging reference point is used for distribution of charging data from the Multi Mediation (MM) system to the BSS.

The MM is described in Section 4.7.6 MM – Ericsson Multi Mediation on page 39.

The system's charging services are described in Section 13 Charging on page 91.

2.6 Network Manager

The Network Manager uses the Surveillance and Configuration reference point for handling fault, configuration, and performance management of the system.

The Mult-service Network Operations Support System (MN-OSS), described in Section 4.7.7 MN-OSS – Multi-service Network Operations Support System on page 40, provides GUIs for surveillance and configuration support of the system. In addition, the system provider can integrate the MN-OSS functionality in the existing Operation Support System (OSS).

The system's Operation & Maintenance (O&M) services are described in Section 14 Operation and Maintenance Services on page 93.

2.7 DNS

Domain Name System (DNS) queries to DNS nodes are sent and received over the Number, Naming, and Addressing (NNA) resolution reference point.

The IPWorks, described in Section 4.7.8 DNS – Domain Name System on page 40, provides the external DNS interface.

2.8 E-mail Server

The E-mail Server enables the sending and receiving of e-mails to and from the CS subsystem described in Section 4.5 CS – Centrex Services on page 31. The CS subsystem utilizes the e-mail reference point for these issues used for storing and retrieving voice mails.

2.9 Time Server

The Time Server provides a Coordinated Universal Time (UTC) reference to all elements in the system.

All elements will be configured to use the same UTC time regardless of the geographical location of the element. In this way it is possible to compare the time-related information from different nodes distributed geographically in different time zones.

The system's internal DNS node hosts the Time Server according to RFC 1305.

2.10 External Network

External networks are IP-based networks using H.323 or SIP as signaling protocol and RTP for media transportation. The Multimedia Network-Network Interface (MM NNI) is used for session establishment and media transportation to and from external multimedia networks.

The Network Session Controller (N-SC), described in Section 4.6.3 SC – Session Controller on page 36, implements the system's support for interaction with external IP networks.

2.11 PSTN – Public Switched Telephone Network

The Public Switched Telephone Network Network-Network Interface (PSTN NNI) provides the possibility for users to communicate with PSTN users, and the opposite is also true. The system supports various market versions of ISUP over the PSTN NNI.

The Media Gateway Controller (MGC) with SS7 connectivity and the Media Gateway (MGW) implements the system's support for interaction with PSTN networks.

For further information about the MGC and MGW, see Section 4.6.1 MGC – Media Gateway Controller on page 35 and Section 4.6.2 MGW – Media Gateway on page 36 respectively.

2.12 Verified SIP Products

The Multimedia User-Network Interface (MM UNI) is used for session establishment and media transportation to verified SIP products. The supported functionality may vary depending on the used product.

3 Services Overview

The main purpose of the system is to provide end-users with advanced multimedia services, such as IP audio and video calling, conference calling, instant messaging, and handling of presence information. The system utilizes IP technology over fixed broadband networks and uses SIP for control signaling and RTP for media transportation.

Additional and supporting operational services can be found in Section 12 Provisioning Services on page 87 and Section 14 Operation and Maintenance Services on page 93.

3.1 End-User Services

An end-user typically has an analogue telephone used together with an Integrated Access Device (IAD), or a SIP telephone, to access the services offered by the system. Additionally, the end-user can access the services by using the provided web client, which is intended to enhance the end-user experience, making it easier for the end-user to configure and use the services. The web client can be used together with a telephone in order to invoke services easier, for example, to reject or transfer an incoming call.

End-users are divided into the following two main categories:

- Residential end-users
- Enterprise end-users

The residential end-user is usually a private individual that subscribes to the services by entering into a contract with an operator or other service provider.

The enterprise end-user is an employee of a company, who uses the services as a part of their job. In this case the company enters into a contract with the operator or other service provider for the whole company to use services.

End-user services are divided into the following three main categories:

- Personal services
- Group services
- Messaging services

Each category is described in more detail in the following sections:

- Section 3.1.1 Personal Services on page 10
- Section 3.1.2 Group Services on page 10

- Section 3.1.3 Messaging Services on page 11

For further information about traditional supplementary services, IP Centrex services, and other multimedia services provided by the system, see the following document:

- *Residential and Centrex Services, Ericsson IMS Multimedia Telephony*, Reference [9]

A brief overview on end-user interaction is provided in Section 4.2 End-User Interaction on page 22.

End-user interfaces are described in detail in the following document:

- *End-User Interface, Ericsson IMS Multimedia Telephony*, Reference [4]

3.1.1 Personal Services

Personal services are assigned to specific users, and are used, managed, and configured by the end-user. The services range from standard services, such as simple audio calling, to conferencing and other high-end services.

The personal services are used by both residential and enterprise end-users. Examples of personal services are the following:

- Audio, fax, and video calls
- Instant messaging
- Audio conferencing
- Presence management
- Voice and video mailboxes
- Selective call acceptance/rejection
- Basic services, such as call forwarding and last number redial
- Distinctive ringing

3.1.2 Group Services

Group services apply to groups of users and are often administered by a group administrator.

The group services are usually used by enterprise end-users. Examples of group services are the following:

- Auto attendant services, which serves as an automated receptionist that answers the phone and provides a personalized message to callers with options for connecting to the operator, dialing by name or extension
- Call centres with incoming calls received by a single phone number distributed among a group of users, or agents
- Basic hunt groups routing incoming calls that are not directed to a specific user number to the next available user in the hunt group, according to the group policy settings for the hunt group
- Call park and call park retrieve enables an end-user to hold a call and to retrieve it from another station within the group
- Calling plan for incoming, outgoing, and forwarded/transferred calls

Groups of users can be organized in many ways. In the simplest example, a group is just an arbitrary selection of users. But, users may also be organized into hierarchical departments within the structure of an enterprise. In this context, a group may consist of one or several departments.

Examples on services on an enterprise level are as follows:

- Enterprise-wide voice portal
- Enterprise-wide group services
- Enterprise directory

3.1.3 Messaging Services

Messaging services provide the end-user with the ability to send, receive, and manage messages.

The messaging services are used by both residential and enterprise end-users. Typical messaging services are the following:

- Voice messaging
- Video messaging

3.2 Centrex Services

There are a lot of Centrex services in the system. Two of them are described in Section 3.2.1 Calling Line Identity Presentation (CLIP) on page 12 and Section 3.2.2 Calling Line Identity Presentation Restriction (CLIR) on page 12.

3.2.1 Calling Line Identity Presentation (CLIP)

For SIP originating sessions, CLIP is supported to all networks. The Centrex System Application Server (CS-AS) inserts the E.164 number of the subscriber in the `P-Asserted-Identity` header of INVITE for all originating SIP sessions. For SIP-to-PSTN calls, the MGC maps the SIP `P-Asserted-Identity` into the Calling Party Address field of ISUP Initial Address Message (IAM).

For SIP-to-H.323 termination, the N-SC maps the SIP `From` header (as received, invalidated from the originating client) into the Source Address (E.164 number) of the H.323 SETUP. Thus, the CLIP support is limited for H.323 terminating calls.

For SIP terminating sessions, CLIP is supported if A-number information is correctly received from the originating Serving Call Session Control Function (S-CSCF) or Media Gateway Controller (MGC). If the call originates from an H.323-PBX, the A-number is inserted in the SIP `From` header only.

3.2.2 Calling Line Identity Presentation Restriction (CLIR)

For SIP originating sessions, CLIR is supported for all destinations except H.323-PBX. CLIR is indicated using the `Privacy` header of INVITE.

To untrusted networks (normally external SIP networks or Internet), the SC and the MGC can be set up to remove (not map or transfer) the calling party address information received in INVITE to prevent malicious and incorrect handling of the CLIR service in the external, untrusted network.

For SIP terminating session, the Anonymous Call Rejection feature of CS-AS is invoked (if active) if the `Privacy` header of the incoming INVITE is set, that is, if CLIR is active).

3.3 Network Services and Regulatory Requirements

This section describes network services and regulatory requirements provided by the system.

3.3.1 Number Portability

Number portability is supported through interworking with legacy number portability functionality in the PSTN network. Imported telephone numbers are inserted in the ENUM database, while exported numbers are deleted from the ENUM database.

By default, the system routes calls to unknown telephone numbers, not resolved by an ENUM DNS query, to the PSTN network. The call is then handled by

the PSTN network, which queries the legacy number portability database and routes the call to the called party.

Accordingly, calls to imported telephone numbers are routed from the PSTN network to the MGC after number portability database query. Since imported numbers are present in the ENUM database, the MGC is able to route the call to the SIP user.

The support of number portability is thus dependant on the support for number portability in the PSTN network. Only voice and fax calls are supported to exported telephony numbers, for example, if a number has been exported to an external SIP network, it is not possible to originate video calls to this number since the call is routed through the MGC, the MGW, and the PSTN.

3.3.2 Implicit Registration in the Ericsson IMS Multimedia Telephony System

The implicit register function allows the users' Public IDs to implicitly register each other. In the Ericsson IMS Multimedia Telephony system this means that a contact that is registered for one Public ID automatically gets registered for all other Public IDs that the user has been given. The result is that a user is reachable on all his Public IDs even if only one of them has been configured in the terminal or client for registry. By default the Public ID shown in the CLID info is the one that the terminal used for the SIP REGISTER.

A user known to the Home Subscriber Server (HSS) has one Private ID and at least one Public ID. Several Public IDs may be associated with one user. During the SIP REGISTER event, the HSS is queried for the list of Public IDs related to the user in question. It is this list of Public IDs that is implicitly registered in the Call Session Control Function (CSCF).

It is also possible for the terminal to indicate that another of the Public IDs known to the HSS will be used as CLID. This CLID is then provided using the `P-Preferred-ID` parameter in the SIP REGISTER message sent from the terminal or client.

One of the Public IDs defined for a user is the default ID used when routing calls to a PSTN. This is an E.164 telephone number that is inserted in the SS7 signaling as CLID by the MGC.

3.3.3 Equal Access

Equal access is supported using prefixing and the breakout gateway selection function in the CSCF. When the end-user dials the required prefix, the breakout gateway selection function in the CSCF is triggered and the call is routed through the MGC and the PSTN to the selected carrier.

3.3.4 Carrier Pre-Select

Carrier pre-select is supported using the number normalization functionality in the CSCF, whereby the CSCF (based on user data) adds a routing/carrier prefix to the dialed number for routing through the MGC and the PSTN to the selected carrier.

3.3.5 External Network Selection

If a called number, that is, an E.164 number, a local number, an extension, or a `number@domain;user=phone`, does not belong to a subscriber in this system domain, the S-CSCF queries an internal breakout table that applies a number analysis.

Using the analysis function, Breakout Gateway Control Function (BGCF), in the CSCF provides for flexible breakout routing. Selection of routing destination can be based on both A and B number analysis.

Routing destination in this context should be regarded as a ‘‘next hop’’ destination. It is possible to define how the call will be handled in the next hop destination by using the optional trunk-context and trunk-group fields in the BGCF.

As an example, this makes it possible to provide for local PSTN breakout using a gateway residing on a locally addressed IP-VPN behind an SC.

3.3.6 Malicious Call Tracing

The system supports the following two types of malicious call tracing:

- System Administrator Configured Trace
- Customer Originated Trace

The System Administrator Configured Trace is activated by the system level administrator. When assigned and active, originating calls from and terminating calls to the user generate an alarm containing a large number of call parameters, for example, calling numbers, called numbers, redirecting numbers, and answer time, and so on.

The Customer Originated Trace is activated by the end-user by dialing a feature code. The information included in the alarm can be used to trace the CDRs associated with the call.

Malicious call tracing supports both voice and video calls and the service is implemented by the CS subsystem described in Section 4.5 CS – Centrex Services on page 31.

3.3.7 Emergency Calls

Emergency calls are treated as ordinary calls to the PSTN network and are thus routed as normal SIP-to-PSTN or IP-PBX-to-PSTN calls.

However, for SIP originating calls, all potentially disruptive Centrex System Application Server (CS-AS) services are disabled for that call (for example, Call Waiting, Call Hold), and the CS-AS also ensures that the call can only be released by the far-end agent, that is, the emergency call centre.

For destinations defined as receivers of emergency calls, it is possible to override blocking of CLID.

The CS-AS provides two services, Emergency Zone (not a recommended deployment option) and Physical Location, which provides possibilities to block calls where the physical origination of the call is unknown. Emergency Zone use the IP address of the originating call while Physical Location is based on usage of the `P-access-network-info` header in SIP invite messages together with provisioned data concerning subscriber devices.

The CS-AS also includes the External Emergency Routing function that provides the possibility to retrieve the emergency call centre destination for a certain location from an external Emergency Number database (EN-DB). The interface used by the CS-AS is called Emergency Call number SOAP translation interface.

Location information for the call in question is either included in the `P-access-network-Info` header of any SIP request or derived from the CS-AS database where information of subscriber devices, included their location, are stored.

3.3.8 Lawful Intercept

The system provides a Lawfully Authorized Electronic Surveillance (LAES) implementation, which is based on the J-STD-025 standard.

The following necessary services for lawful intercept are available:

- **Administration** – Enables a system provider or law agency to assign and configure surveillances against particular users
- **Event Monitoring** – Generates call events for users that are under surveillance and delivers the information to the law agencies requesting the surveillance
- **Media Monitoring** – Mixes the media of all parties of a call that are under surveillance and delivers the information to the corresponding law agencies

The services are implemented by the CS subsystem described in Section 4.5 CS – Centrex Services on page 31.

Lawful intercept is supported for voice and video calls to and from registered SIP clients.

Lawful intercept is not supported for instant messages and presence operations.

3.3.9 Operator Controlled Barring

In order to prevent a user in the system from making calls or use other services in the system, the service provider needs to have the possibility of barring a user (or group). The reason for barring can be, for example, fraudulent use or unpaid bills.

The barring is possible to perform on the following two levels:

- Individual user barring, performed by group administrator or, more likely, service provider administrator
- Barring on group level, performed by service provider administrator

For individual user barring, the following actions should be performed:

- The Intercept User service should be set in the CS-AS for the user
- The ‘‘active’’ flag for the user in the Presence server should be changed from ‘‘1’’ to ‘‘0’’, that is, inactivate the user

Operator controlled barring of voice and video calls is supported through the use of the CS-AS Calling Plan service. The following two types of barring exist:

- Barring of a user
- Barring of a group

The Calling Plan service allows the administrator to control the type of calls made, received, transferred, and forwarded by users in a group. The restrictions are applied by means of sets of call screening templates assigned to groups, departments, or single users. The templates specify various screening methods that should be applied to calls according to the call type or the digits dialled.

The administrator can define different screening templates for outgoing, incoming, and redirected calls.

3.3.10 Large Enterprise Function

The Large Enterprise service provided in the Ericsson IMS Multimedia Telephony solution is based on the CS-AS service ‘‘Large Multi Site Enterprises’’, where an enterprise can consist of several groups and calls between them can be made using a prefix (location code) and the extension number. The Large Enterprise service is solely a CS-AS service and a large enterprise user will look as any other from the system point of view.

3.3.11 Charging Output Details (CDRs) Correlation

The system supports correlation and aggregation of the Charging Output Details (CDRs) that are generated in the system using the SIP `Charging Vector` and `Call-Identity` headers. The system's charging data collection and consolidation process is further described in Section 13 Charging on page 91.

3.3.12 Authentication

The system authenticates the user entity using the HTTP Digest Authentication mechanism described in RFC 2617 and 3GPP TS 24.228.

The UE can be authenticated as part of the registration procedure, as well as when sending a SIP request, for example, when sending INVITE, MESSAGE, BYE, CANCEL, and so on. Which SIP methods to be authenticated is defined by means of the CSCF configuration.

3.3.13 Multi Access Extensions (MAE)

The MAE solution allows users in the GSTN (PSTN and PLMN) to register with the system and take advantage of the services that the system offers. This includes charging, user provisioning, self management, and routing.

Depending on how a user's registration set is provisioned a ‘‘one phone’’ functionality can be achieved (a user is presented as and contactable on one public user ID) or if wanted, the user can have a different public user ID for the circuit switched device.

3.3.14 Removal of P-Access-Network-Info (PANI) Header

Some SIP headers contain information, which may be considered sensitive from a privacy perspective. The operator needs mechanisms to ensure that headers, which contain sensitive information about a user are removed before the SIP message is forwarded to another user.

One such header is the P-Access-Network-Info (PANI) header, which contains information about a user's current location. IETF and 3GPP specifies that this header must be removed before the message leaves the trust domain by the originating S-CSCF when sending messages over the NNI.

Therefore it is possible to configure the session controller to remove this header when forwarding the message on the NNI to non trusted domains and for the header to always be removed for all messages routed over the UNI.

4 System Overview

This section presents a logical overview of the system, its concepts and functional entities, providing a basic understanding of the system.

The system is modeled fulfilling the following main architectural requirements:

- The system is based on and, as far as possible, follows the recommendations produced by the 3rd Generation Partnership Project (3GPP) and the Internet Engineering Task Force (IETF) in regards to architecture and philosophy.
- The system uses SIP for creating, modifying, and terminating multimedia sessions with one or more participants. The core network is based on the 3GPP IP Multimedia Subsystem (IMS).

The design is based on the following architectural principles:

- **Layered Architecture** – Separation of functions into service (application), control, and connectivity layers
- **Planes** – Separation of functions into control and user planes
- **Tiers** – Separation of functions into tiers, for example, client, presentation, business, and data tiers

4.1 Architecture

The system is based on the horizontal layered architecture that separates functionality into three layers – a service or application layer, a session control layer, and a connectivity layer. The horizontal layered architecture is illustrated in Figure 3 on page 19.

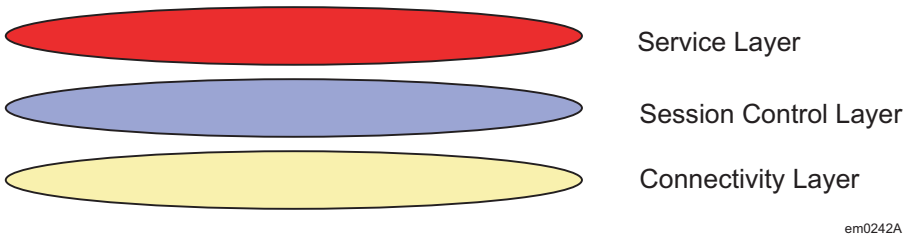


Figure 3 Horizontal Layered Architecture

The layered architecture is intended to allow each layer to evolve independently as market and technology evolve. For example, it supports the migration to new transmission technologies by making the upper layers independent of the transmission technology deployed in the connectivity layer. It also allows

different, optimized technologies to be deployed within the payload processing intensive connectivity layer as opposed to the transaction oriented control layer.

The service layer hosts application and content servers to execute value added services for the end-user.

The session control layer hosts network control servers, which manage call or session setup, modification, and release. The control servers also handle functions such as security, charging, and interaction to external networks on control plane level.

The connectivity layer hosts routers, switches, media gateways, and other user plane functions. The routers and switches provide transport capabilities for both control plane and user plane traffic. The media gateways provide different kinds of interaction on connectivity level, including interaction between different transmission technologies and interaction between different media formats.

Each layer consists of one or several modules, where each subsystem is responsible for a dedicated task in the system. This makes it possible to add new subsystems or replace old subsystems depending on the total network solution and needed services.

A logical overview of the system is shown in Figure 4 on page 21. Note that Figure 4 on page 21 does not include switches and routers in the connectivity layer.

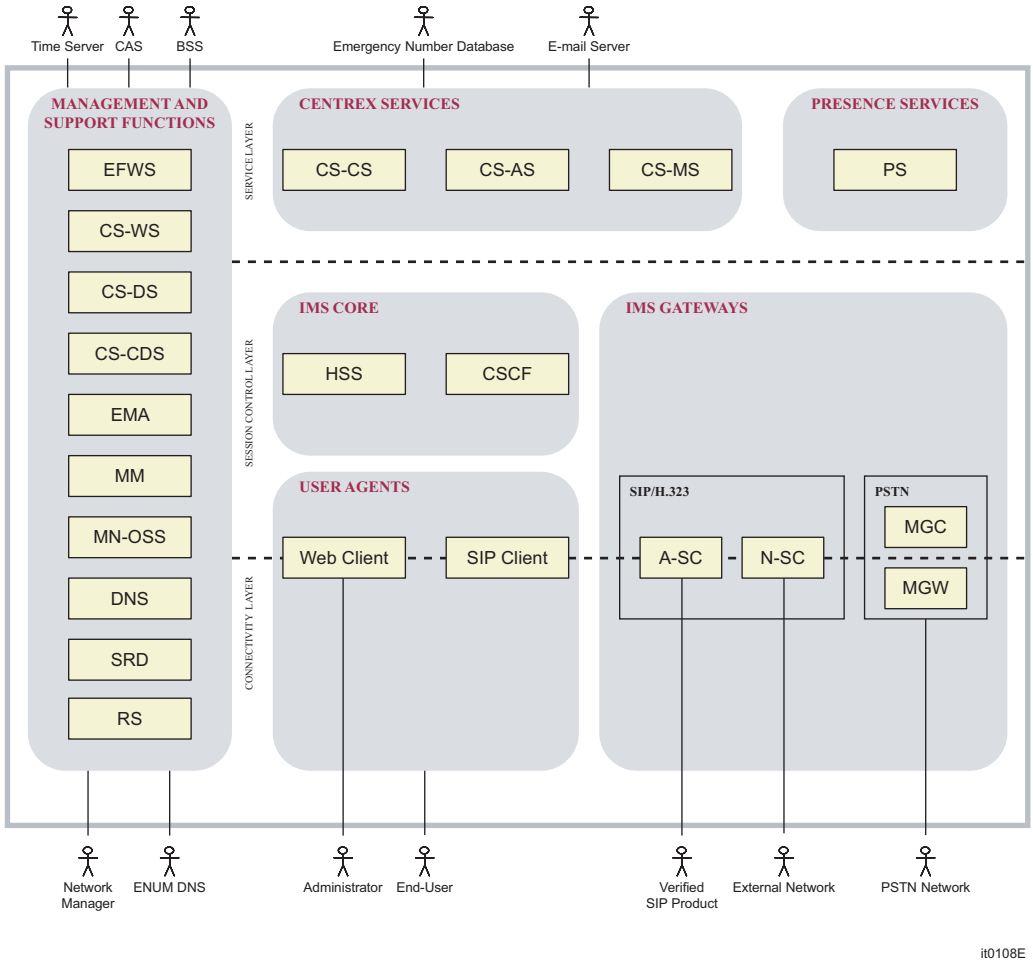


Figure 4 Logical System Overview

The following subsystems are defined in the system:

- **User Agents** – clients used for configuration, provisioning, and usage of the services supported by the system
- **IP Multimedia Subsystem Core** – handling core functionality such as SIP authentication and authorization of users, registration, and session handling
- **Presence Services** – handling SIP presence services
- **Centrex Services** – handling SIP services excluding presence and instant messaging. Examples of services are audio and video calls, conferencing, and other group services.
- **IP Multimedia Subsystem Gateways** – handling calls to and from external networks, such as PSTN and H.323 networks. Note that both signaling and media streams are handled by the subsystem, which therefore is included in both the session control layer and the connectivity layer.

- **Management and Support Functions** – O&M and support functions are included in the system in order to provide a complete end-to-end network solution

The system is also verified against a number of SIP compliant products.

The following subsections describe the different subsystems and their surroundings. The media interfaces are excluded to clarify the figures, but a complete description of all interfaces and supported protocols are found in Section 5 Standards, Interfaces, and Protocols on page 47.

4.2 End-User Interaction

In order for an end-user to interact with its services and to set up and receive calls, the following three components can be used:

- The web portal interface itself that resides in the Centrex System Web Server (CS-WS). Two different interfaces are supported by the web server; the new Open Client Interface (OCI) and, for backwards compatibility reasons, also the personal web portal interface. Both interfaces can be used concurrently.

- SIP compliant terminals and clients. These are devices or software that originate and terminate calls (for example, RTP streams) and that use the SIP protocol to manage and control these streams. In order to handle calls in a proper way, these devices must also support audio and video codec compliant to the Ericsson IMS Multimedia Telephony system.

- Web clients. These are applications that use proprietary protocols in order to manipulate call control in the CS-AS. Such an application may also include facilities to terminate calls, but in all cases, a separate call terminating device is used.

4.2.1 Web Portal

Before accessing the web portal, the end-user is authenticated in an external system or in the Ericsson Front-end Web Server (EFWS). The session is then transferred to the appropriate server in the CS-WS farm.

From the CS-WS farm, all available CS-ASs are visible from each individual CS-WS. Information about which CS-AS to use is collected from the Centrex System Distribution Server (CS-DS).

The web portal provides the end-users with the following functionality:

- View, configure, activate, and deactivate subscribed services

- Offline service configuration, that is, configuring of services when the end-user is not involved in a call

- List of end-user services they are subscribed to
- List of group services they are subscribed to
- Context-sensitive help for every service
- Feature access codes that are associated with subscribed-to services

For more details about the web portal, see the following document:

- *BroadWorks™ Application Server, User Web Interface, Administration Guide*, Reference [27]

4.2.2 SIP Terminals and Clients

SIP terminals and clients are the devices used for the actual communication, that is, which originates and terminates the RTP stream and turns it into something suitable for human communication by means of audio or video, or both.

It can be either a stand-alone physical device for voice or video, or both, a physical device for connection a traditional POTS or ISDN device, or an application running on a standard PC.

Movial Connect PC is an optional soft client that is verified to the Ericsson IMS Multimedia Telephony system. It can be customized in order to fit specific operator needs for branding, and so on. Examples on functionality provided by the client are the following:

- Call and hang up button
- Volume control
- Status bar for telephony status
- Mid-call control button in dial pad for mid call services
- Mute
- Set presence status – preconfigured available, busy, and away states or free text presence
- View presence of contacts in the contact list
- Communicate with a contact by any of the available communication means by clicking on the contact in the contact list
- Add and drop media – upgrade from an audio call to a video call, or the opposite, during the call
- Instant messaging with smileys or emoticons

- Directory search with filter on name, number, Public ID, and so on, using LDAP
- Invoking services using feature access codes by sending DTMF tones during a call or including ‘‘*’’ and ‘‘#’’ as part of a dialed number

4.2.3 Web Clients

A web client is an application interfacing the CS-AS through the CS-WS, stand-alone or web-based, used for manipulating calls. Normally, it does not include RTP termination, that is, a SIP terminal or client is still needed in order to establish the communication channel.

The following clients are optional in the Ericsson IMS Multimedia Telephony system:

- *Call Manager* client for enterprise end-users. This is a Java™ application with a web-based interface used to initiate and manage calls. Except from manipulating calls, the client also provides integration with Microsoft® Outlook®. The Call Manager client uses CCP for call control to the CS-AS through the CS-WS.
- *Assistant* is quite similar to the Call Manager client, but packaged in a different manner. It uses CAP as protocol to the Open Client Server (OCS). The OCS resides in the CS-WS and reroutes CAP to the appropriate CS-AS.
- *Receptionist* is a telephonist (receptionist) console, providing similar functionality as consoles used for similar purposes to traditional PBXs. The receptionist uses CAP/OCS for call control.

An overview of the user agents and interoperating entities is shown in Figure 5 on page 25.

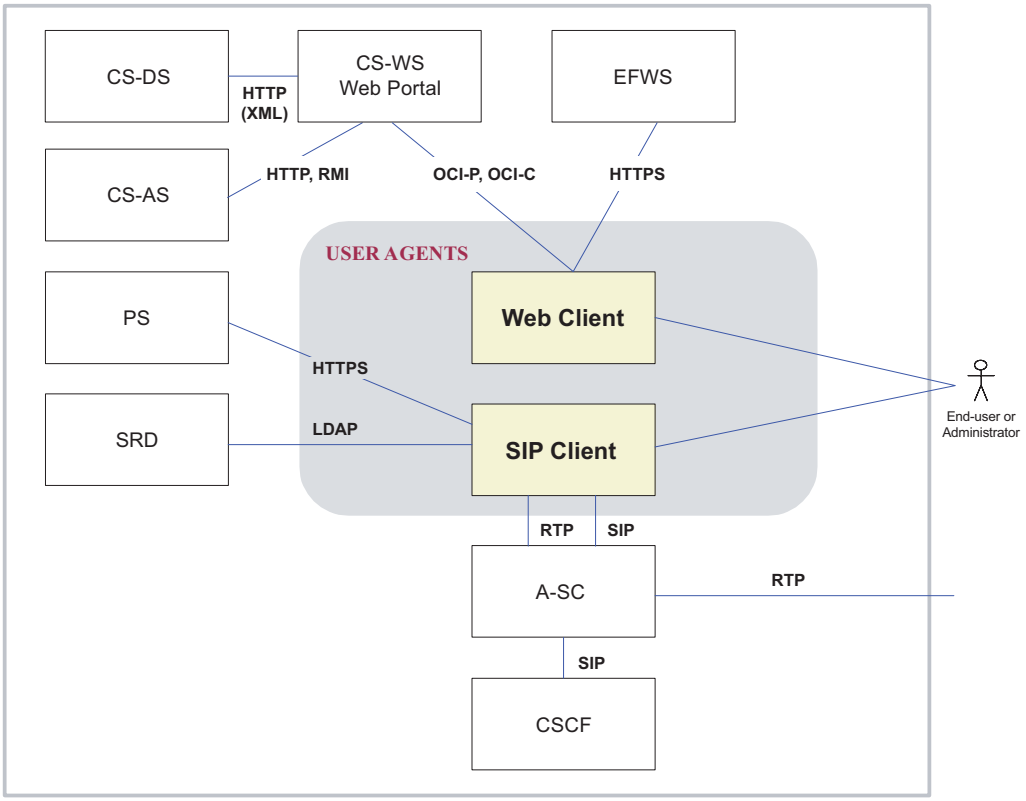


Figure 5 User Agents Overview

4.3 IP Multimedia Subsystem Core

The IP Multimedia Subsystem Core (IMS Core) includes functionality for authentication and authorization of users, registration, and session handling. It also provides interfaces to the other subsystems as well as external systems.

Note: The concept ‘‘IMS core’’ is used internally within Ericsson and has no relation to other similar concepts used in, for example, TISPAN.

An overview of the IMS Core is shown in Figure 6 on page 26.

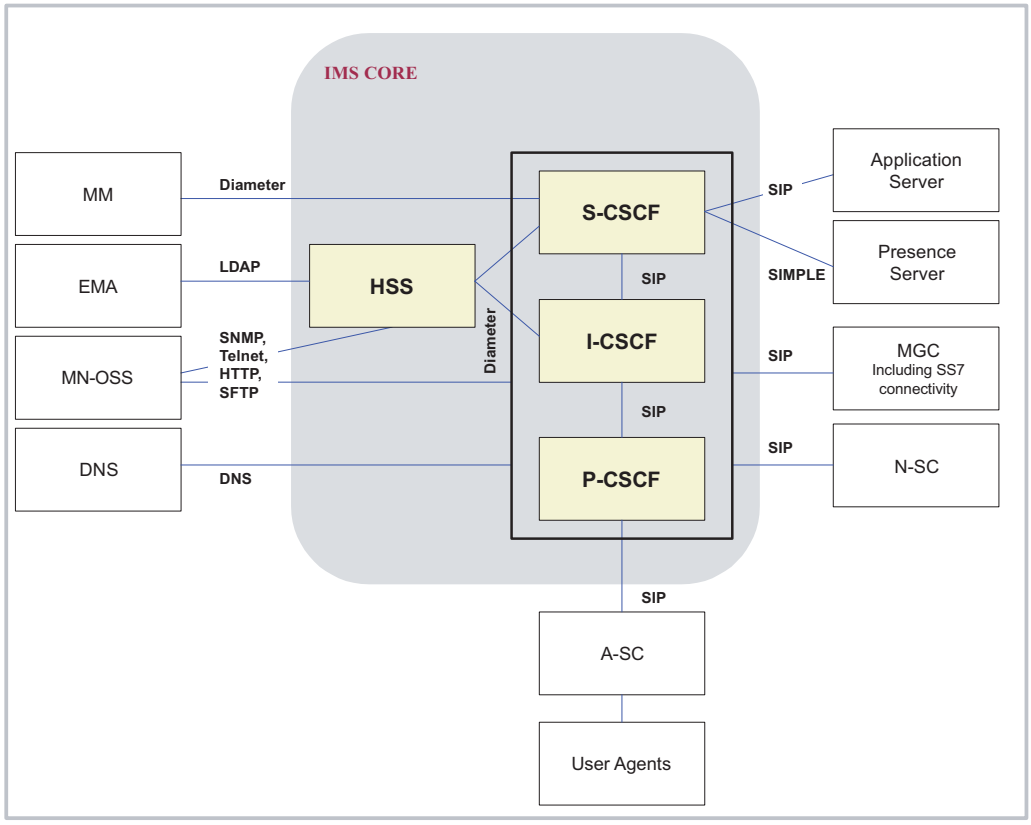


Figure 6 IMS Core Overview

The Session Control subsystem consists of the following entities:

- Proxy CSCF (P-CSCF)
- Interrogating CSCF (I-CSCF)
- Serving CSCF (S-CSCF)
- Home Subscriber Server (HSS)

For more details about the CSCF and the HSS, see the following documents:

- *CSCF Node Product Description*, Reference [16]
- *HSS 4.0, Technical Product Description*, Reference [22]

4.3.1 CSCF – Call Session Control Function

The CSCF is the core node of the IMS core and is responsible for handling the multimedia sessions, using SIP as the call signaling protocol. In the 3rd Generation Partnership Project for CDMA (3GPP2) this entity is named Session Control Manager (SCM) and in the IETF this node is referred to as a SIP server.

The CSCF can be configured to assume the following roles in the network:

- Proxy Call Session Control Function (P-CSCF)
- Interrogating Call Session Control Function (I-CSCF)
- Serving Call Session Control Function (S-CSCF)

Each role is described in detail in the following subsections.

The CSCF interfaces the Ericsson Multi Mediation (MM) for sending Charge Data Output (CDO), the DNS for NNA purposes, and the MN-OSS for surveillance and configuration.

4.3.1.1 P-CSCF

The P-CSCF is the first point of contact for the User Agent (UA), unless an Access Session Controller (A-SC) is placed in between the UA and the P-CSCF. The P-CSCF may modify (for example, modification of private headers) an outgoing request according to a set of provisioned rules defined by the network operator, for example, address analysis and message modification.

The P-CSCF provides the following capabilities:

- Forwarding of the SIP REGISTER request received from the UA to the I-CSCF
- Storage of contact addresses of the user equipment, as a part of the registration process
- Forwarding of SIP messages received from the UA to the S-CSCF, whose address the P-CSCF has received as a result of the registration procedure
- Forwarding of SIP requests or responses from S/I-CSCF to the UA

The P-CSCF interacts with the PC client and verified SIP products through the Gm reference point, using SIP.

4.3.1.2 I-CSCF

The I-CSCF is the contact point inside an operator's network for all connections destined to a subscriber of that network operator. It may hide the inner topology of the home network from other networks and locates the S-CSCF where a subscriber is located through interaction with the HSS. Multiple I-CSCFs can exist concurrently in an operator's network.

The I-CSCF provides the following capabilities:

- Dynamic allocation of S-CSCF instance to a user performing SIP registration

- Locating the S-CSCF where a subscriber is located through interaction with the HSS (for terminating calls)
- Routing of SIP requests received from another network to the S-CSCF
- Forwarding of the SIP request or response to the S-CSCF
- ENUM resolution for routing sessions from the PSTN to the S-CSCF (normally not used since the MGC does an ENUM query for calls from the PSTN)

4.3.1.3 S-CSCF

The S-CSCF performs the session control services for the UA. This includes routing of originating sessions to I-CSCF or external networks and routing of terminating sessions to P-CSCF. The S-CSCF supports establishment, modification, and release of IP multimedia sessions using the SIP/SDP (Session Description Protocol) protocol suite. It also provides indirect service invocation through the IP Multimedia Subsystem Service Control Interface (ISC) to the service layer. The S-CSCF decides whether an application server will be invoked based on information received from the HSS.

The S-CSCF provides the following capabilities:

- Subscriber registration by accepting REGISTER requests and interworking with the HSS
- User authentication through interworking with the HSS
- Caching of user profiles. Relevant information is downloaded from the user profile in the HSS to the S-CSCF and stored during the registration lifetime.
- Invocation of multimedia sessions, both originating and terminating
- Forwarding, redirection, and rejection of multimedia sessions
- Modification and clearing of multimedia sessions
- Invocation of application servers using SIP to the CS-AS and SIMPLE to the Presence Server (PS), in order to trigger multimedia services
- Number normalization of dialled digits
- ENUM resolution of E.164 numbers
- Breakout gateway selection for forwarding of SIP requests to external networks
- Resolving the address of the I-CSCF serving the destination subscriber through database look-up, and forwarding the SIP request or response to that I-CSCF
- Accounting data output using Diameter to the MM for charging purposes

- Create and delete private headers

4.3.2 HSS – Home Subscriber Server

The HSS is the master database that contains all user and subscriber information, and keeps track of which S-CSCF is handling the subscriber.

The HSS provides the following capabilities:

- Profile database – stores necessary subscriber and user information
- User security information generation – generates authentication data according to IETF specifications to protect the network against unauthorized use
- User security support – supports the authentication of user access through Hypertext Transfer Protocol (HTTP) digest authentication to the IP Multimedia Subsystem
- Identification – maintains the appropriate relations between the private ID identifying the user (NAI, SIP_URL) and the public IDs used for call establishment (SIP_URL, E.164)
- Access authorization – decides if the user is allowed to register in the system
- Mobility management – performs mobility management procedures as described by the 3GPP specifications
- Service information support – provides support for storage of trigger information, application server identities, and service keys, as part of the user profile
- Registration/de-registration – the HSS authorizes the registration procedure when required by the I-CSCF and provides the S-CSCF assigned to the user if the user is already registered

4.4 Presence Services

The Presence subsystem provides the following main features:

- Storage of presence information
- Support for subscription and notification of presence changes

An overview of the Presence Services is shown in Figure 7 on page 30.

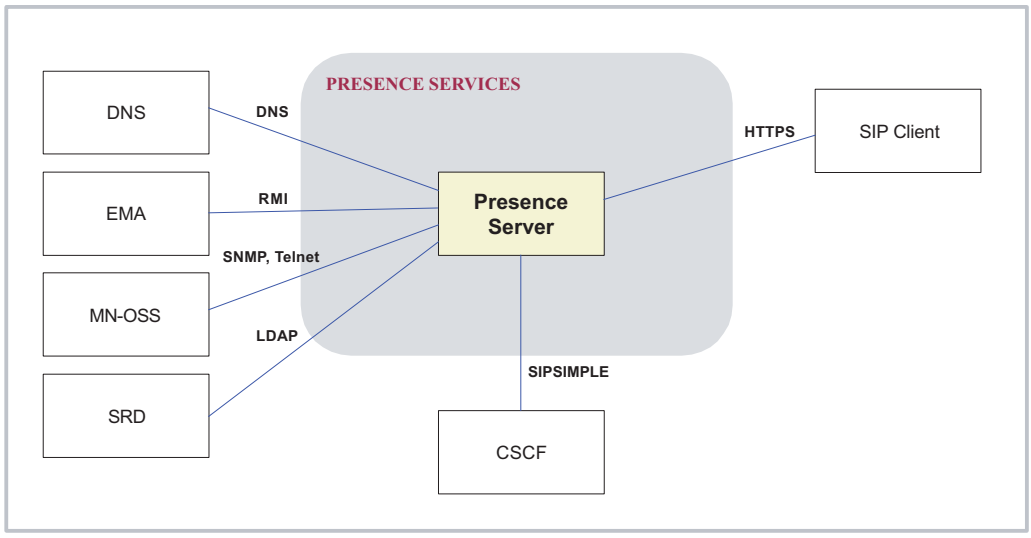


Figure 7 Presence Services Overview

The Presence Server (PS) is implemented on the Multimedia Communication Engine (M2CE®) and provides the functionality for handling SIP presence in the system.

The end-user accesses the presence services of the PS using the PC client described in Section 4.2 End-User Interaction on page 22.

4.4.1 PS – Presence Server

The PS supports presence management, subscription, and notification. User agents can publish and change presence information using the SIP PUBLISH method. Subscription and notification is accomplished using the SIP Event Notification method, using the SIP request SUBSCRIBE to subscribe to presence information, and the SIP request NOTIFY to notify user agents of presence changes.

The end-user's presence information is stored in the PS and includes the following information:

- Presence status – available, busy, idle, offline
- A free-text presence message, for example, ''At home'', ''In a meeting'', ''Happy'' to go with the presence status
- Devices information. For each device, the following information is available:
  - Device address, for example, sip:+468123456@emm.com
  - Status, for example, ''available'' and ''idle''
  - Timestamp, that is, time of last update

  - Description of the device, for example, ‘‘home PC’’

- Watchers – a record of people who have requested to subscribe to the user’s presence information, and whether or not they are authorized for this task

- Subscribers – the online subscribers to the user’s presence Information. A subscriber is currently logged on and will receive presence updates, whereas a watcher perhaps currently is not online

- Authorization policies – rules set by the user to determine who may subscribe to their presence information or not (white list and black list)

The core of the PS consists of a Java2™ Enterprise Edition (J2EE™) SIP engine deployed on a JBoss® Application Server and it is deployed on the following different servers:

- Traffic Server

- Provisioning Server

- Log Server

- Database

For more information about the M2CE, see the following document:

- *Presence Server, Oracle M2CE, Product Description*, Reference [35]

4.5 CS – Centrex Services

The Centrex Services (CS) subsystem delivers communication services over packet networks, providing support for the following:

- Call routing and translations

- Media-oriented applications, for example, conferencing, voice mail, auto attendant, and other Interactive Voice Response (IVR) applications

- Personal calling functions, for example, selective call forwarding and notification, call transfer, and integration with Microsoft Outlook for contact retrieval and dialing

- Administration functions, for example, management of end-users, groups, and service assignments

An overview of the CS is shown in Figure 8 on page 32.

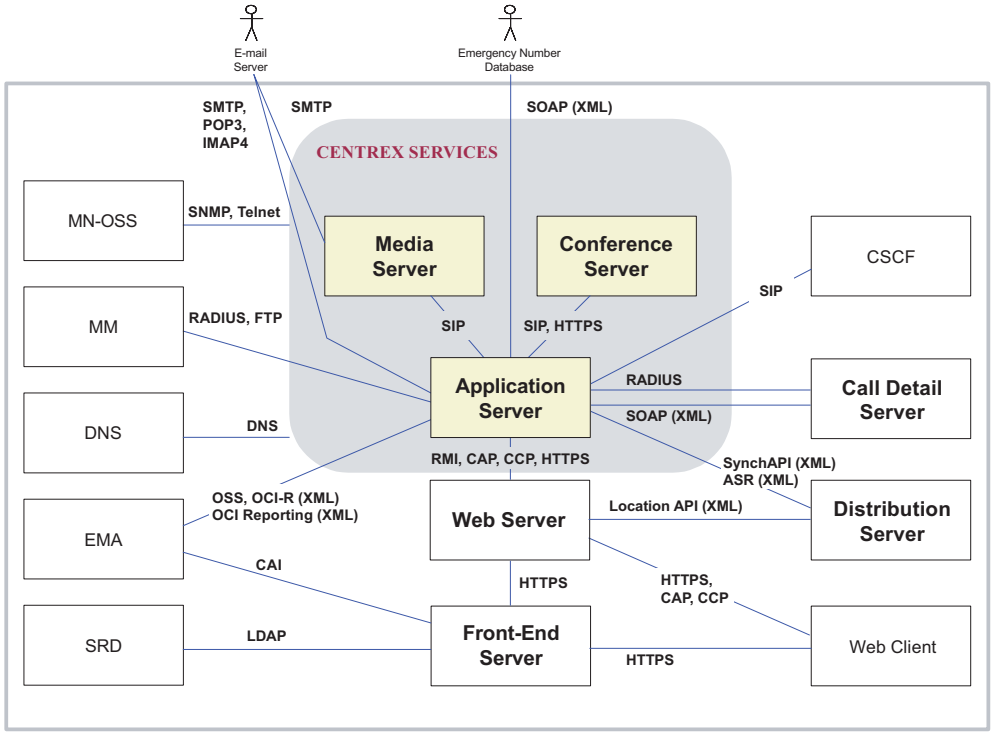


Figure 8 Centrex Services Overview

The CS subsystem consists of the following entities:

- Centrex System Application Server (CS-AS)
- Centrex System Media Server (CS-MS)
- Centrex System Conference Server (CS-CS)

All servers are part of the BroadWorks product suite. For more information about the CS subsystem, see the following document:

- *Centrex Services (CS) System, Product Description*, Reference [29]

4.5.1 CS-AS – Centrex System Application Server

The CS-AS is the core entity of the CS subsystem and the main access point for control signaling.

The CS-AS is implemented as a Back-To-Back User Agent (B2BUA) to allow implementation of enhanced call control services. The CS-AS makes use of the other servers to make a complete service solution.

4.5.2 CS-MS – Centrex System Media Server

The CS-MS provides specialized media resources including the following:

- Digit detection
- Announcement playback and recording
- Media mixing functions such as 3-party call conferencing
- Video media such as video greetings and video attendant

The CS-MS interfaces with the CS-AS for instructions and interfaces with the RTP media stream for detecting digits, recording audio, playing audio, and mixing streams. These resources are used for services such as voice messaging, auto attendants, conferencing, and so on.

The CS-MS does not contain a database, since all subscriber and service information is contained in the CS-AS.

4.5.3 CS-CS – Centrex System Conference Server

The CS-CS provides conferencing services including the following:

- Audio and web conferencing
- Scheduled, recurring and reservation-less
- Meet-me dial-in numbers
- Web collaboration
- Sharing of Microsoft PowerPoint, Excel, and Word files

4.5.4 Centrex Services Interfaces

The following interfaces and protocols are exposed:

- SIP – used to communicate with network devices to handle the session control signaling and for the communication between the CS-AS and the CS-MS
- HTTP/HTTPS – used for accessing the web portals
- OCI-C – Open Client Interface-Call Control, is an internal XML socket-based protocol used from and to the Call Manager handling call control
- OCI-P – Open Client Interface-Provisioning, is an internal XML) socket-based protocol used from and to the CS-AS
- OCI-R – Open Client Interface-Reporting, is an internal XML socket-based protocol used from and to the CS-AS

- SMTP, is used for e-mail dispatch. This is used for messaging and notification services. Services make use of this protocol to dispatch messages to a user's mailbox. The notification service makes use of this protocol to dispatch notifications to a user's e-mail account.
- POP3/IMAP4 – used for e-mail reception for messaging services. All voice and fax messages for a user are stored in a standard POP3 or IMAP4 server. The user can access these messages using a standard e-mail client or through the voice portal (part of the CS-MS).
- RADIUS according to RFC 2866 and the following document:
  - *BroadWorks, Call Detail Record, Interface Specification*, Reference [28]
- RTP – used to send and receive media to access and network devices. The CS-AS redirects a device's media stream to a particular resource on a CS-MS. The CS-MS terminates the media stream and performs the requested operations on the media stream.
- SOAP (XML) – an interface built on Axis and running under Tomcat. Used for retrieving call logs, service provider configuration, and for communication to an external Emergency Number Database.
- SNMP – used for fault and performance management
- Telnet – used for configuration management

4.6 IP Multimedia Subsystem Gateways

The subsystem of IP Multimedia Subsystem Gateways (IMS Gateways) consists of a PSTN gateway and a SIP/H.323 gateway.

An overview of the IMS Gateways is shown in Figure 9 on page 35.

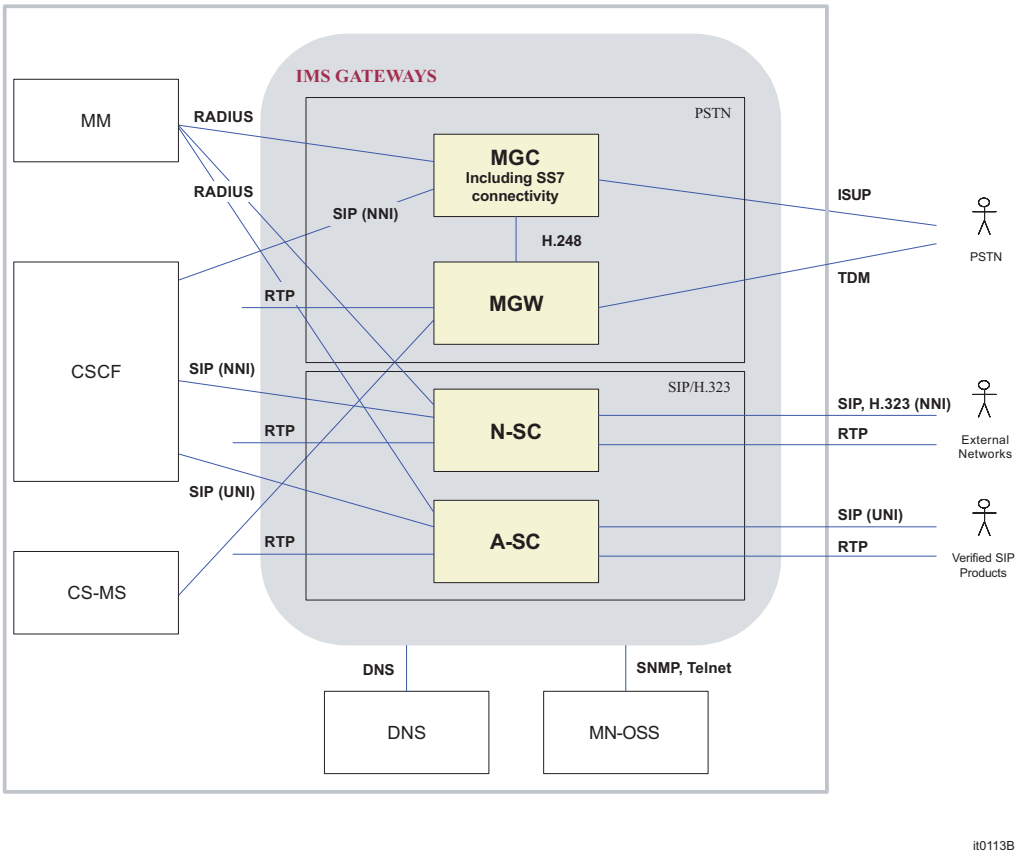


Figure 9 IMS Gateways Overview

The PSTN Gateway consists of the Media Gateway Controller (MGC) including the Signaling Gateway (for SS7/ISUP connectivity) and the Media Gateway (MGW).

The SIP/H.323 system consists of the Session Controller (SC).

4.6.1 MGC – Media Gateway Controller

The MGC provides interworking between the SIP session control signaling and ISUP call control signaling to and from external PSTN/PLMN networks. Furthermore, it controls the MGW resources using the H.248 protocol and generates RADIUS information for charging and interconnect accounting.

The MGC provides the following capabilities:

- Handles multimedia session establishment, modification, and termination using the SIP protocol in the IP Multimedia domain and appropriate ISUP protocol in the circuit switched domain
- Supports addressing and routing of multimedia sessions to and from CSCFs and interconnected PSTN nodes

- Controls one or more MGWs using the H.248 protocol
- Performs mapping of application level signaling (SIP/ISUP)
- Sends RADIUS request to the MM system

4.6.2 MGW – Media Gateway

The MGW provides interworking between PSTN and SIP media streams, that is, conversion between circuit-switched Time Division Multiplexing (TDM) bearer circuits and packet-switched media streams (RTP). It is controlled by the MGC using H.248.

The Media Gateway functionality is provided by the AXD 301 and described in the following document:

- *AXD 301, System Description*, Reference [15]

4.6.3 SC – Session Controller

The SC is situated at crossings between IP networks, where it funnel sessions – signaling together with associated media streams – of real time IP voice, video, and other data across the borders between the IP networks. The SC supports the signaling protocols H.323 and SIP.

The aim of the SC is to manage SIP sessions across the IP network borders in order to ensure security, Quality of Service (QoS), Service Level Agreements (SLAs), Network Address Translation (NAT), or firewall traversal, and other critical functions for IP streams.

Additionally, the SC provides the MM system with charging information by means of RADIUS requests.

The SC has the following roles in the system's network:

- Situated as an Access Session Controller (A-SC) in the crossing between an access network and the Ericsson IMS Multimedia Telephony system to funnel sessions from User Agent Clients (UACs) to the CSCF
- Situated as a Network Session Controller (N-SC) in the crossing between an external network and the local Ericsson IMS Multimedia Telephony core system to funnel sessions from external network elements to the CSCF
- The SC manipulates SIP private headers in the signaling interface

The SC is configured to run as a SIP Back-To-Back User Agent (B2BUA), that is, SIP sessions are terminated and re-originated as new sessions as they are routed through the SC. For each session, NAT translations are established and SDP is re written to force all session related media to be routed through the SC.

4.7 Management and Support Functions

This section describes the Management and Support Functions subsystem.

4.7.1 CS-WS – Centrex System Web Server

The CS-WS, also known as the web portal, provides a number of easy-to-use portals for different purposes (system administration, group administration, and so on). Except for access to service portals, it also includes interfaces (OCI-P and OCI-C) used for call control signaling between external clients and the CS-AS.

For detailed information about the CS-WS, see the following document:

- *BroadWorks Web Server, Configuration Guide*, Reference [32]

4.7.2 CS-DS – Centrex System Distribution Server

This entity is used by the CS-WS in order to allocate end-user requests to an appropriate CS-AS.

In the provisioning process, changes in, for example, user and group data are generated either by an external system or by an interactive administrator working directly to the CS-AS. In both cases it is normally the EMA which distributes data to the target systems. However, in the case of the CS-DS this is handled somewhat different.

Changes in user and group data are transferred from the EMA, or entered by an on-line administrator, to the CS-AS and it is the CS-AS who updates the CS-DS using a BroadSoft™ proprietary SynchAPI, based on XML over HTTP.

4.7.3 CD-CDS – Centrex System Call Detail Server

The sole purpose for this server is to relive some log writing pressure from the CS-AS. In a large system, the amount of call log data that needs to be stored in a local database may have impact on system performance. In order to soften this burden from the CS-AS, this function is moved to a separate node.

It is also possible to extend the number of call logs per user compared to the storage capacity available when using the CS-AS. Present limit for the CS-AS is 20 call logs per user.

One Centrex System Call Detail Server (CS-CDS) is designed to support one or more CS-ASs. Configurations for redundant CS-CDSs are not supported.

4.7.4 EFWS – Ericsson Front-end Server

The EFWS provides the following functions:

- HTTP login and CS-WS selection
- Password management
- One-time passwords and account lockout

Details regarding the EFWS can be found in the following document:

- *Ericsson Front-End Web Server 2.0, User Guide*, Reference [17]

4.7.4.1 HTTP Login and CS-WS Selection

The EFWS is situated between the web client and the CS-WS during the login procedure. It can act as the authenticating entity of the client, or it can relay a login request from an already authenticated, trusted source (for example, operator portal), or it can have both roles at the same time.

After successful login, the EFWS retrieves an FQD from the System Repository and Directory (SRD), representing the CS-WS farm, before it redirects the web client to the CS-WS using a login token that the EFWS received from the CS-WS.

Selection of CS-AS is then made by the CS-WS based on information from the CS-DS.

4.7.4.2 Password Management

The EFWS includes a password management function enabling management of the SIP and web passwords. The server has logic to enforce user category access control based on session origin in order to not allow for, for example, an end-user to practice system administration rights from outside a controlled network segment.

The passwords stored in the SRD are updated using the EMA's Customer Administration Interface (CAI) or Customer Administration Interface 3rd Generation (CAI3G).

4.7.4.3 One-time Passwords and Account Lockout

The EFWS supports web account lockout, that is, the account is automatically locked after a number of consecutive failed login attempts. In case the account is locked, only an authorized operator may unlock it.

It is also possible to define a one-time password, that is, a password that has to be changed after being used once. The user is forced to change password directly after logging in using the one-time password.

4.7.5 EMA – Ericsson Multi Activation

The EMA Classic is used for provisioning. All end-users and groups, with the data that are required, are created, modified, and deleted using the EMA. The EMA hides the distribution of data to multiple entities and provides one uniform interface (CAI or CAI3G) through which all databases can be accessed.

Additionally, the EMA contains a CS-AS Reporting Receiver (CS-AS RR). The task of the CS-AS RR is to distribute CS-AS data that has been updated using the web client to the other nodes in the system. When subscriber data has been modified, the CS-AS sends the updated information to the CS-AS RR using the OCI reporting interface.

The system's provisioning interfaces are described in Section 12 Provisioning Services on page 87.

4.7.6 MM – Ericsson Multi Mediation

Accounting data are sent to, or collected by, the MM system for filtering, consolidation, formatting, and distribution to the external Business Support System (BSS), for example, billing system.

Although the term CDR includes the word ‘‘Call’’ it is used generically to refer to the record that can be produced for any type of chargeable operation, for example, a call, a service, a multimedia session, an event, and so on.

From a functional perspective, the MM can be divided into the following three different functional areas:

- **Consolidation** – Sorting and merging based on `P-Charging-Vector` and `P-charging-Function-Address`.
- **Formatting** – Preparation for export to an external billing system.
- **Event collection** – Receiving or fetching of accounting records from the relevant nodes in the system. The collection process may also include primitive filtering.

In a small Ericsson IMS Multimedia Telephony system, all three functions can be executed in a single computer. But, as the system grows, it is possible to scale by, for example, running the Event Collection process in a separate computer. In such case, it is essential that the computer, or computers, running the Event Collection process is physically placed in close proximity to the system that it collects information from.

Adaptation of the MM scripts is possible for every customer in order to fulfill their specific needs, on CDR content that is, sent to the Business Support Systems (BSS).

For more information about the MM, see the following documents:

- *Ericsson Multi Mediation 5.0, File and Event Mediation - Network Element Description*, Reference [19]
- *Ericsson Multi Mediation 5.0, Online Mediation - Network Element Description*, Reference [20]

4.7.7 MN-OSS – Multi-service Network Operations Support System

The MN-OSS is used for fault, configuration, and performance management of the system.

The MN-OSS is a client server management system that integrates a number of applications to provide a network view of the managed network, including the following:

- Fault management support for receiving and present alarms
- Configuration management support with the facility to launch node centric applications, for example, element managers, from a central point. These applications can be launched from the MN-OSS toolbar or from the fault manager application.
- Performance management support for collection and presentation of performance data
- Security management in terms of authentication and authorization (based on given access rights) of the MN-OSS system operator
- Operation and maintenance support allowing the scheduling and execution of maintenance scripts and providing access to a centralized online document store

The system's O&M services are described in Section 14 Operation and Maintenance Services on page 93.

For more information about the MN-OSS, see the following document:

- *MN-OSS 7.0, System Description*, Reference [24]

4.7.8 DNS – Domain Name System

The DNS is used for NNA resolution by almost every node in the system. In addition, the DNS provides the CSCF and the MGC with translation of E.164 numbers into public, routable SIP URIs through ENUM.

The IPWorks is used for DNS and ENUM queries.

The IPWorks also contains support for acting as a Dynamic Host Configuration Protocol (DHCP) server when this functionality is required.

Finally, the IPWorks support for Active Select is utilized to achieve network redundancy, that is, the IPWorks can query the status of the hosts of the destination node before returning the IP address of the selected host.

For more information about the IPWorks, see the following document:

- *IPWorks 4.2, Technical Product Description*, Reference [23]

4.7.9 SRD – System Repository and Directory

The SRD is used for the following main purposes:

- To enable ‘‘white pages’’ searches from the self-management feature on the PC client. Searchable attributes in the SRD are the following:
  - First name
  - Last name
  - SIP addresses
  - Phone numbers

  The user can search all open groups or be restricted to its closed groups. The group concept is described in Section 8.3 Groups on page 63.
- To support the EMA provisioning activities by acting as a LDAP repository where the EMA acts as the front-end
- To support the EFWS web client login and password management activities, that is, the EFWS can access the user’s passwords and the CS-WS address stored in the SRD
- To support the PS with authentication

The SRD is implemented using the Sun Java System Directory Server and the EMA update the directory data using LDAP.

For more information about the SRD, see the following document:

- *SRD 2.0, Technical Product Description*, Reference [26]

4.7.10 RS – Registration Surrogate

The Registration Surrogate (RS) node is part of the Multi Access Extensions (MAE) solution for the Ericsson IMS Multimedia Telephony system. The MAE is described in Section 3.3.13 on page 17.

The purpose of the RS is to perform registrations on the CSCF on behalf of non SIP terminals. This way, a multimedia subscriber could have multiple contacts

registered on the CSCF, with these contacts not necessarily associated to a SIP terminal.

The RS basically fetches users' contact information from an LDAP directory server (the SRD) and sends a SIP registration header to the CSCF for each user entry coming from the directory.

In order to provide the required functionality, the RS makes use of two client protocols:

- **LDAP client** – in charge of fetching contact information for every user subscribed to the MAE functionality.
- **SIP client** – the RS acts as a SIP user agent sending registration requests to the CSCF for every contact list retrieve from the SRD.

In addition, the RS offers an SNMP interface in order to communicate counters, alarms, and notifications to the MN-OSS, and the possibility for the MN-OSS to retrieve performance management reports in XML format through FTP, see Figure 10 on page 42.

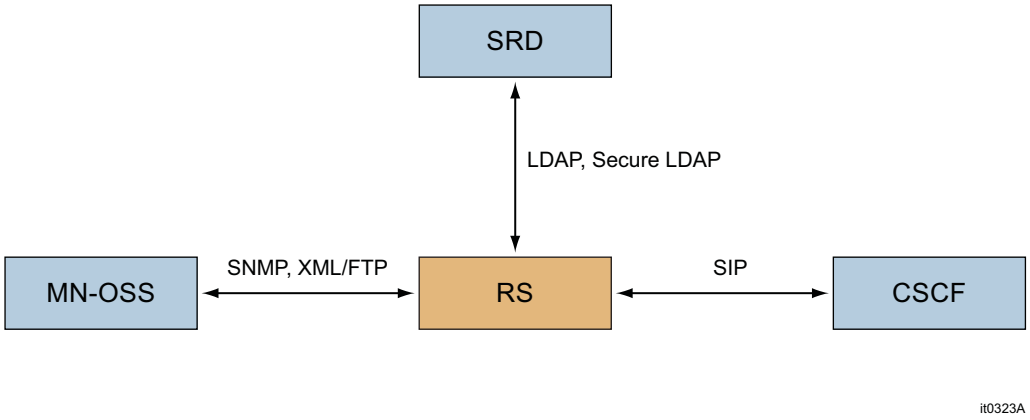


Figure 10 Registration Surrogate Overview

The registration process is indefinitely repeated in cycles. In every cycle all the MAE users are registered in a SIP server (the CSCF). The duration of every registration cycle must be shorter than the registration expiration time configured in the CSCF, and it is recommended to be half of it in order to avoid the risk of expiration of any contact.

4.8 Addressing

This section describes the addressing area within the system, such as address types, user categories, number normalization, and so on.

4.8.1 Address Types

A subscriber (user) can be associated with the types of addresses shown in Table 1 on page 43.

Table 1 Address Types in the System

Address Type	Example	Usage
Private User Identity	u72364623@domain.com	Master identity, used for authentication, authorization, and so on.
Public User Identity	SIP: john.doe@domain.com or Tel: +46 8 123456	The public address that can be used for addressing of terminating SIP sessions to the user.
Alias	john@domain.com	Alternate public SIP address that can be used for addressing of terminating SIP sessions to the user.
E.164 Number	+46 8 123456	A public, international phone number associated with the user, which can be used for addressing of terminating SIP sessions to the user.
Extension Number	1234	The user's extension number within a group.
UA Address	468123456@138.85.84.61:5060	IP address used to address the User Agent (UA) where currently registered (dynamic address).

4.8.2 User Categories

The system supports four different user categories. Each type can have different sets of address types associated with the user as described in Table 2 on page 44.

In addition, it is possible to call (or receive calls from) external users using SIP addresses or normal E.164 numbers.

Table 2 User Categories and Address Types

User Category	Address Type					
	Private User ID	**Public User ID**	**Alias**	**E.164 Number**	**Extension Number**	**Description**
Residential	Mandatory	Mandatory	Optional	Mandatory	–	Normal residential user registered in the system.
Enterprise DID	Mandatory	Mandatory	Optional	Mandatory	Optional	Normal business user registered in the system.
Enterprise Phantom	Mandatory	Mandatory	Optional	–	Mandatory	Business user not having an E.164 number, but an extension number only.
Virtual User(1)	Mandatory	Mandatory	–	Mandatory	Optional	Virtual subscription used to route calls to the CS.

(1) For example, Call Center, Auto Attendant, Hunt Group.

4.8.3 Number Normalization

For originating calls, the originating CS-AS is responsible for detecting dialed digits in the request URI in the received SIP INVITE message. The dialed number received in the SIP INVITE may be normalized into national or international format by the CS-AS or S-CSCF, or by both, when needed.

Extension numbers (“Short Numbers”) are translated by the originating CS-AS into the corresponding full number based on the private numbering plan of the group that the originating user belongs to. In case the originating CS-AS detects that all characters before the domain part in the request URI are digits, and the caller and the callee does not belong to the same group, it adds the tag “user=phone” to the request URI and to the `TO` header before returning the INVITE to the S-CSCF.

If the S-CSCF receives a SIP INVITE containing the tag ‘‘user=phone’’, or a TEL URI, in the request URI, number normalization is performed by the S-CSCF using a normalization scheme, that is, a table of number translation rules. The number normalization scheme to apply is selected based on the dialing context to be applied for the call. The dialing context is downloaded from the HSS to the S-CSCF at registration. After successful number normalization, the dialed number has been translated into a public, routable E.164 number.

Note: All users belonging to the same group must be provisioned in the same CS-AS.

4.8.4 ENUM Query

After number normalization, the S-CSCF generates a NAPTR DNS query of ENUM requesting resolution of the E.164 number. In case the E.164 number is associated with a registered system subscriber, ENUM returns the public SIP address of the user and the INVITE is routed to the I-CSCF based on the domain name of the SIP address. Otherwise, remote breakout is performed.

For a PSTN originating session, the MGC can query ENUM for translation of the E.164 number into the associated public SIP address of the subscriber before sending an INVITE to the I-CSCF.

4.8.5 DNS Query

A DNS query (for resolution of FQDN into IP address and port) is executed by all system entities performing routing of messages based on SIP URIs containing FQDNs. Detailed information regarding DNS lookups in the system is described in RFC 3263.

4.8.6 External Network Selection

If a called E.164 number does not belong to a subscriber in the system domain, the BGCF in the CSCF queries an internal breakout table that applies a simple number analysis based on the calling party number (A-number) and the called party number (B-number) to select an MGC or N-SC. The S-CSCF proxies the INVITE to the MGC or N-SC, for further routing to the external network.

5 Standards, Interfaces, and Protocols

This section describes the standards to which the system complies and the interfaces and corresponding protocols that are used within, to, and from the system.

5.1 Standards

Ericsson is participating in the standard committees related to IP Multimedia subsystems, for example, 3GPP, 3GPP2, TISPAN, and IETF. The system is compliant to the relevant parts of these standards and is aligned with the standards as much as possible.

The system is based on the following standards:

- 3GPP release 6 IP Multimedia Subsystem architecture specifications
- 3GPP2 IP Multimedia Subsystem architecture specifications
- SIP compliant according to IETF RFC 3261 (and associated RFCs)

5.2 External Reference Points

The external reference points that have been defined according to Figure 2 on page 5 are listed in Table 3 on page 47.

Table 3 External Reference Points

Reference Point	Description	Protocols
End-User GUI	This is the client application GUI provided by the User Agent to the end-user.	
Administrator GUI	This is the web client GUI used by the administrators for provisioning.	
Provisioning	Interface from the CAS to the EMA and the CS subsystem for subscriber and service provisioning.	CAI or CAI3G
Charging	Interface between the BSS and the MM.	

Table 3 External Reference Points

Reference Point	Description	Protocols
Surveillance & Configuration	Interfaces to the MN-OSS and node specific element managers.	
NNA Resolution	Interface between the system's DNS (external) and the system external DNS actor.	DNS, ENUM
E-mail	Interface between the external E-mail server and the CS subsystem to support sending (SMTP) and receiving (POP3, IMAP4) e-mails.	SMTP, POP3, IMAP4
Time Synchronization	The system nodes uses the Simple Network Time Protocol (SNTP), specified in RFC 2030, or the Network Time Protocol (NTP), specified in RFC 1305 for synchronizing their clocks with the Time Server. The Time Server (part of the Solaris™ OS) is hosted on the DNS node host.	SNTP, NTP
MM NNI	The Multimedia Network-Network Interface (MM NNI) is used for session establishment and media transportation to and from external H.323 and SIP networks.	SIP, H.323 for signaling, RTP for media
PSTN NNI	The PSTN Network-Network Interface (PSTN NNI) provides the possibility for users to communicate with PSTN users, and the opposite is also true. The system supports various market versions of ISUP over the PSTN NNI.	ISUP for signaling, TDM for media

Table 3 External Reference Points

Reference Point	Description	Protocols
MM UNI	The Multimedia User-Network Interface (MM UNI) is used for session establishment and media transportation to verified SIP products.	SIP for signaling, RTP for media
Location Information	A BroadSoft specified interface used by the CS-AS in order to retrieve call centre information based on physical location.	SOAP/XML

5.3 Internal Reference Points

This section describes the internal reference points and internal interfaces and protocols within the system.

5.3.1 Overview

The following reference points between ‘‘sub-networks’’ within the system are illustrated in Figure 11 on page 50:

ICSN Reference point between the IMS Core (IC) and the Services (SN)

IGIC Reference point between the IMS Gateways (IG) and the IMS Core (IC)

IGSN Reference point between the IMS Gateways (IG) and the Services (SN)

MSIC Reference point between the Management and Support Functions (MS) and the IMS Core (IC)

MSIG Reference point between the Management and Support Functions (MS) and the IMS Gateways (IG)

MSSN Reference point between the Management and Support Functions (MS) and the Services (SN)

MSUA Reference point between the Management and Support Functions (MS) and the User Agent (UA)

UAIG Reference point between the User Agent (UA) and the IMS gateways (IG)

UASN Reference point between the User Agent (UA) and the Services (SN)

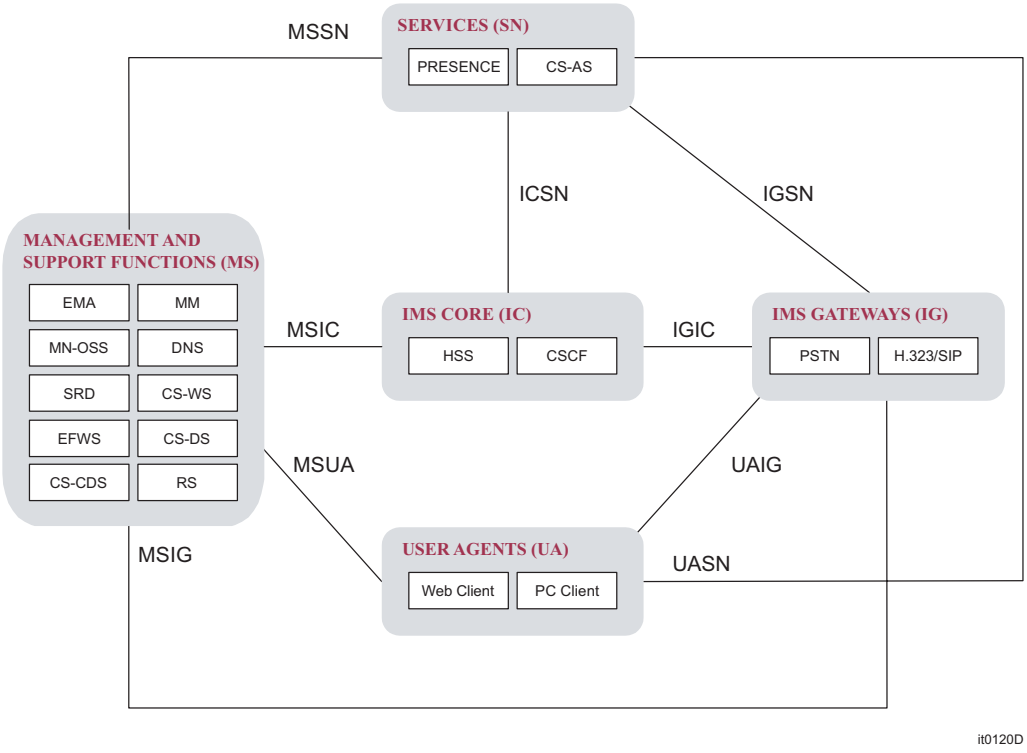


Figure 11 Sub-Network Reference Points

5.3.2 Internal Interfaces and Protocols

Interfaces and protocols defined inside and between the “sub-networks” are defined in Table 4 on page 50.

Note: Internal interfaces to optional nodes might also be external interfaces.

Table 4 Internal Interfaces and Protocols

Reference Point	Description	Protocol
IC-internal	Used between the S-CSCF and the HSS.	DIAMETER
	Used between the P-CSCF and the S-CSCF.	SIP
	Used between the S-CSCF and the I-CSCF.	SIP
ICSN	Used between the S-CSCF and the CS-AS for invocation of Centrex services.	SIP (ISC)
	Used between the S-CSCF and the PS for signaling of presence operations.	SIP SIMPLE

Table 4 Internal Interfaces and Protocols

Reference Point	Description	Protocol
IG-internal	Used between the A-SC and the N-SC for media transfer.	RTP
	Used between the A-SC and the MGW for media transfer.	RTP
	Used between the N-SC and the MGW for media transfer.	RTP
	Used between the MGC and the Signaling Gateway (SG).	ISUP
	Used between the MGC and the MGW for media control.	H.248
IGIC	Used between the A-SC and the P-CSCF for control signaling.	SIP (UNI)
	Used between the N-SC and the S/I-CSCF for control signaling.	SIP (NNI)
	Used between the MGC and the S/I-CSCF for control signaling.	SIP (NNI)
IGSN	Used between the A-SC and the CS-MS for media transfer.	RTP
	Used between the A-SC and the CS-CS for media transfer.	RTP
	Used between the N-SC and the CS-MS for media transfer.	RTP
	Used between the N-SC and the CS-CS for media transfer.	RTP
	Used between the MGW and the CS-CS for media transfer.	RTP
	Used between the MGW and the CS-MS for media transfer.	RTP

Table 4 Internal Interfaces and Protocols

Reference Point	Description	Protocol
MS-internal	Used by the MN-OSS for O&M of the SRD.	SNMP, HTTPS
	Used by the MN-OSS for O&M of the MM.	SNMP, HTTPS
	Used by the MN-OSS for O&M of the EMA.	SNMP, HTTPS
	Used by the MN-OSS for O&M of the DNS.	SNMP, HTTPS
	Used by the MN-OSS for O&M of the EFWS.	SNMP, HTTPS
	Used by the MN-OSS for O&M of the CS-WS.	SNMP, HTTPS
	Used by the MN-OSS for O&M of the RS.	SNMP, XML/FTP
	Used by the EFWS to access the CS-WS.	HTTPS
	Used by the EFWS to send password modification requests to the EMA.	CAI over SSH
	Used by the EMA for provisioning of data in the DNS.	Telnet
	Used by the EMA for provisioning of data in the SRD.	LDAP
	Used by the RS to retrieve data from the SRD.	LDAP, Secure LDAP
	Used by the EFWS to retrieve data from the SRD.	Secure LDAP
	Used by the CS-DS to inform the CS-WS about which CS-AS that is serving a specific user.	Location API, XML over HTTP
MSIC	Used for transfer of charging information from the CSCF to the MM.	Diameter
	Used between the S-CSCF and the DNS to resolve E.164 addresses into SIP addresses.	DNS (ENUM)
	Used by the MN-OSS for O&M of the CSCF.	SNMP, HTTPS
	Used by the MN-OSS for O&M of the HSS.	SNMP, HTTPS
	Used by the EMA for provisioning of data in the HSS.	LDAP

Table 4 Internal Interfaces and Protocols

Reference Point	Description	Protocol
MSIG	Used for transfer of charging information from the MGC to the MM.	RADIUS
	Used for transfer of charging information from the N-SC to the MM.	RADIUS
	Used between the MGC and the DNS to resolve E.164 addresses into SIP addresses.	DNS (ENUM)
	Used for O&M of the MGC.	SNMP, HTTPS
	Used for O&M of the MGW.	BNSI, HTTPS
	Used for O&M of the N-SC.	SNMP, HTTPS
	Used for O&M of the A-SC.	SNMP, HTTPS
MSSN	Used for transfer of charging information from the CS-AS to the MM.	RADIUS, SFTP
	Used by the MN-OSS for O&M of the CS-CS.	SNMP, HTTPS
	Used by the MN-OSS for O&M of the CS-AS.	SNMP, HTTPS
	Used by the MN-OSS for O&M of the CS-MS.	SNMP, HTTPS
	Used by the MN-OSS for O&M of the PS.	SNMP, HTTPS
	Used by the CS-AS to inform the CS-DS when users migrate from primary to secondary, and the opposite is also true.	ASR, XML over HTTP
	Used by the CS-WS to access the CS-AS.	HTTPS
	Used by the EMA for provisioning of data in the CS-AS. Also used by the CS-AS for sending update notifications to the EMA.	OSS, OCI-P
	Used by the EMA for provisioning of data in the PS.	RMI
	Used by the EFWS to retrieve data (SIP password) from the SRD.	Secure LDAP
	Used by the PS to the SRD in order to authenticate users logging into the PS.	Secure LDAP
	Used by the CS-AS to automatically push changes in groups and users to the CS-DS.	SynchAPI, XML over HTTP
	Transferring of call log information in real time.	RADIUS
	Retrieval of call log information.	SOAP (XML)
	Used between the web client and the CS-WS for transfer of Call Manager commands.	OCI-C

Table 4 Internal Interfaces and Protocols

Reference Point	Description	Protocol
MSUA	Used by the EFWS to access the CS-WS (for web login).	HTTPS
	Used by the web client to access the CS-WS.	HTTPS
	Used by the PC client to look up users in the SRD (white pages).	LDAP
	Used between the web client and the CS-WS for transfer of Call Manager commands.	OCI-P
SN-internal	Used between the CS-AS and the CS-MS for media server device control.	SIP
	Used between the CS-AS and the CS-CS for conference device control.	SIP, CORBA
UAIG	Used between the PC client and the A-SC for media transfer.	RTP
	Used between the PC client and the A-SC for control signaling.	SIP (UNI)
UASN	Used by the PC client to edit presence preferences in the PS.	HTTPS

6 Basic Interworking

This section gives a description of system supported codecs and basic services in the Ericsson IMS Multimedia Telephony solution.

6.1 Video

CS-MS

The CS-MS supports the following video codecs:

- H.263 – 1998
- H.263 – 2000
- H.264

SC

The SC is video codec transparent.

6.2 Audio

MGW

The MGW supports the following audio codecs:

- ITU-T G.711 (11/88), Pulse Code Modulation (PCM) of voice frequencies
- ITU-T G.723.1, Dual Rate Speech Coder for Multimedia Communications Transmitting at 5.3 and 6.3 kbit/s
- ITU-T G.723.1 annex A, Dual Rate Speech Coder for Multimedia Communications Transmitting at 5.3 and 6.3 kbit/s. Annex A: Silence Compression Scheme
- ITU-T G.726 (12/90), Adaptive Differential Pulse Code Modulation (ADPCM)
- ITU-T G.729 annex A (11/96), Reduced complexity 8 kbit/s CS-ACELP speech coder
- ITU-T G.729 annex B (10/96), A silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70

- ITU-T T.38, Procedures for real-time Group 3 facsimile communication over IP networks

The MGC and MGW support codec prioritization by means of node configuration, as follows:

- For PSTN originating calls, either G.711 or G.729 is configured to be preferred

- Optionally, for SIP originating calls, the MGC/MGW preferred codec is selected by the MGC/MGW provided that the PC client supports the MGC/MGW preferred codec

  Example: For a SIP-to-PSTN call, the SIP client prefers to use G.711 (but also supports G.729), while the MGC/MGW is configured to prefer G.729. Then, MGC/MGW selects G.729.

CS-MS

The CS-MS supports the following audio codecs:

- G.711 a-law and μ-law

- G.726 32 kbit/s voice encoding

- G.729

CS-CS

The CS-CS supports the following audio codecs:

- G.711 a-law and μ-law

SC

The SC is audio codec transparent.

6.3 Fax

The MGW supports facsimile/modem bypass (G.711) and Fax Relay (T.38).

The MGC 4.2 T.38 fax support requires that the call is first setup as a normal voice connection (for example, with G.711) before a switchover from voice to T.38 fax is done with SIP re-INVITE practices.

6.4 DTMF Transport and Detection

The system supports RFC 2833 for support of transfer/detection of DTMF information in both the RTP payload and the RTP header information. The CS-MS and CS-CS forwards detected DTMF information to the CS-AS, while the MGW forwards the detected DTMF information to the MGC.

If the MGW detects out-of-band DTMF information in the RTP header, the MGC can instruct the MGW to generate in-band TDM DTMF signaling to the PSTN.

6.5 Early Media

For SIP terminating calls, early media can be injected in-band in the backward direction to the PSTN before call establishment. The MGC maps the received call set up messages, such as SIP ringing, by instructing the MGW to play in-band ringing tones after through-connecting the call in the backward direction.

7 Data Model

This section provides an overview of the provisioning data model. Subscriber data is distributed on the HSS, DNS, SRD, CS-AS, and PS as illustrated in Figure 12 on page 60. Note that the main data, but not all data is shown.

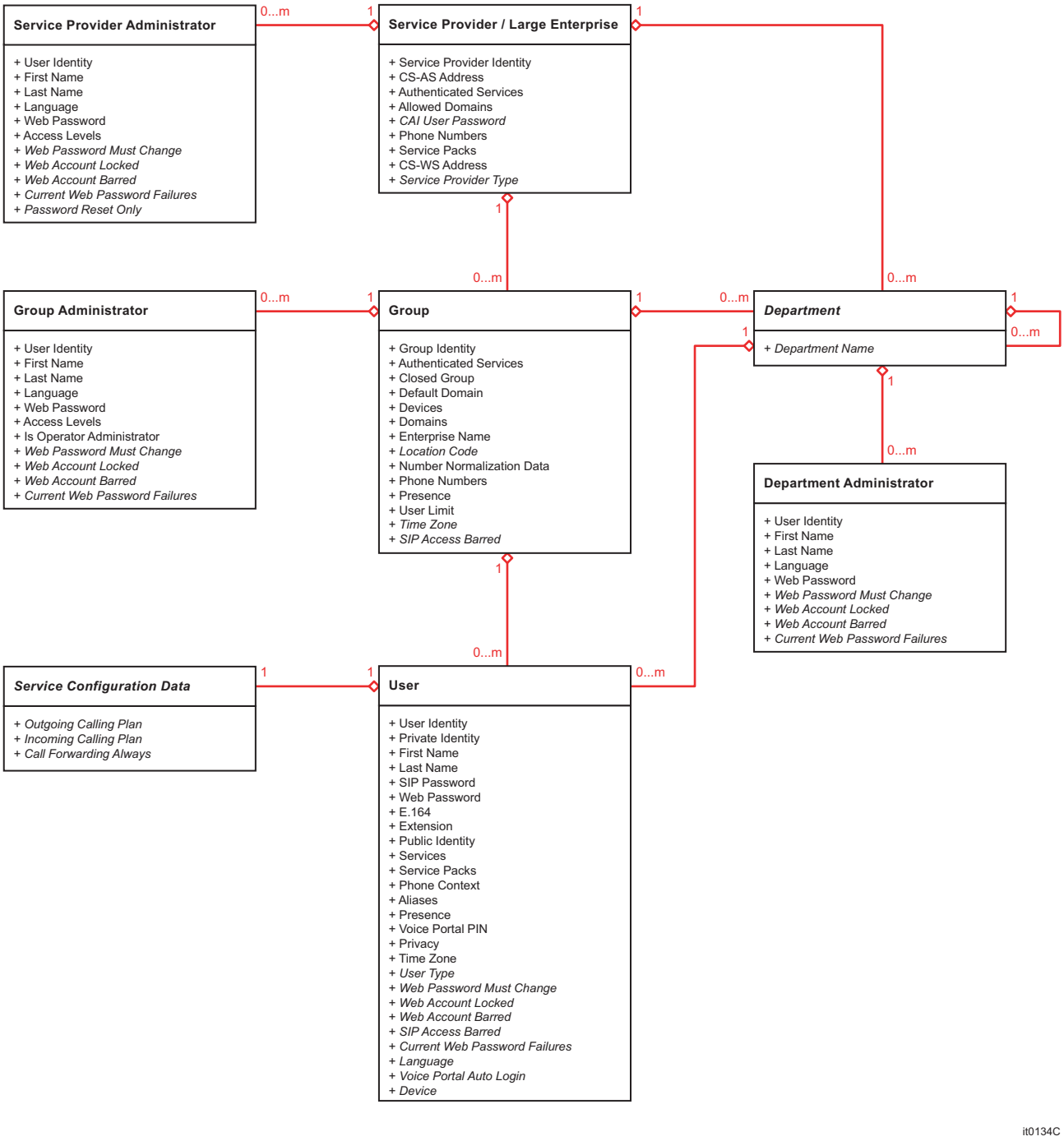


Figure 12 Data Model

8 Data View

This section describes the data model of the system and the distribution of subscriber data on the different system entities.

8.1 Data Models

This section deals with data replication, interfaces to external provisioning systems, and organizational structure.

8.1.1 Data Replication

The EMA is the central data replication source in the Ericsson IMS Multimedia Telephony system. Provisioning data received from either an external system or from web administrators are replicated by the EMA according to Figure 13 on page 61. The EMA also converts data to the correct format as used by each node respectively.

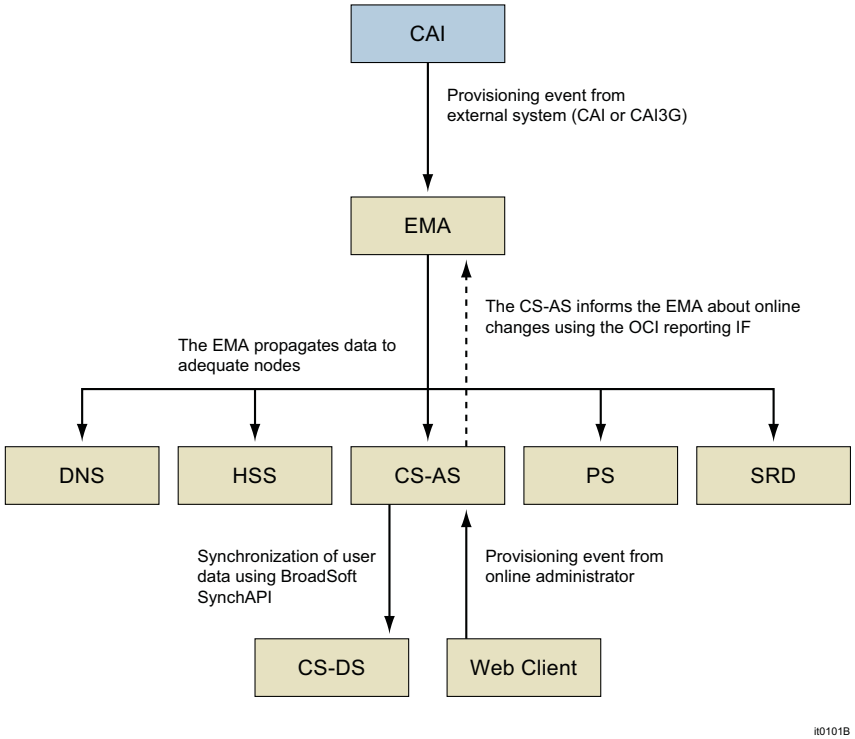


Figure 13 Data Replication

8.1.2 CAI or CAI3G Interface

The EMA provides a Customer Administration Interface (CAI) to external systems for provisioning purposes. This interface also supports CAI3G as defined by Ericsson. However, the operator has to choose to use either CAI or CAI3G, not both.

For further information about provisioning, see the following document:

- *User and Service Provisioning, Ericsson IMS Multimedia Telephony*, Reference [14]

8.1.3 Organizational Structure

In the Ericsson IMS Multimedia Telephony system, it is possible to organize user IDs in very flexible ways. For residential users this is most likely not an issue, while it is quite important when organizing user belonging to large enterprises. Basic possibilities for organizing data are shown in Figure 14 on page 62. Note that departments may be hierarchical and users may be attached to arbitrary levels in the hierarchy.

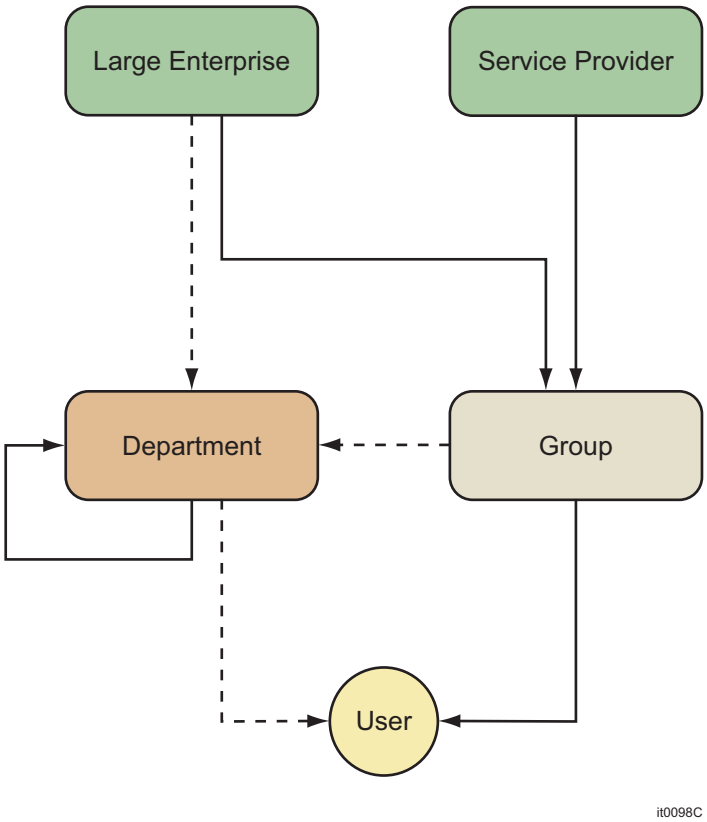


Figure 14 Information Hierarchies

8.2 Service Providers and Large Multi-site Enterprise

The system can be used by one or several service providers. Each service provider consists of one or several groups.

In parallel with the service provider structure, it is also possible to organize business users into a hierarchical department structure within the scope of a large enterprise.

Large enterprise and service provider both reside under the system provider and they are mutually exclusive. Users at different sites can call each other using only extensions, as an option it is also possible to use location codes.

Placing the users into departments enhances managing the users in very large enterprises.

Departments may be created either at the enterprise level or within a particular group. Departments belong to either the enterprise or the group where they were created. A hierarchy of departments is supported in such a way that a parent department can have multiple sub-departments. A department created within a group can extend an enterprise department or another department within the same group. A department created within an enterprise cannot extend departments created at the group level.

All the departments that belong to a group must have a unique name within that group. Likewise, all the departments created at the enterprise level must have a unique name within the enterprise. However, it is possible to have duplicate department names in different groups or a department at the enterprise level with the same name as a department at the group level.

Users created within a group may be assigned to any department created at the enterprise level or departments created within the same group. In this way, departments can span across multiple geographic locations.

8.3 Groups

The group concept is used in the system to group users of the same type, and enable the provisioning of all services common for all end-users within a group once. Examples of such services are short number dialing, control the access to directory information, and enterprise phone book.

8.3.1 Business Groups

Enterprise end-users belong to a business group. Larger enterprises can optionally further split the users of a group into multiple departments.

The end-users inside a business group can perform white pages searches of the other group members' data using the PC client.

8.3.2 Residential Groups

Residential end-users are grouped into one or several groups.

8.3.3 Open and Closed Groups

A group can be open (public) or closed (private). An open group implies that it is searchable for external end-users while a closed group is accessible only by its own members. The SRD stores the information regarding the group's open/close state.

In addition, an individual end-user can decide to hide their presence using the PS Privacy Flag.

8.4 Administrators

This section deals with the different administrator roles within the system.

8.4.1 Service Provider or Enterprise Administrator

This role is provided with the possibility to create groups, departments, and department hierarchies with the scope of a large enterprise.

8.4.2 Department Administrators

Users can be assigned department administrator privileges. The department administrator can modify a department's user preferences.

8.4.3 Group Administrators

Users can be assigned group administrator privileges. The group administrator can modify a group's user preferences, as well as create and modify individual users. However, the group administrator can only create users after being authenticated inside the system, that is, authentication using external trusted portal is not enough.

The user who receives administration right may or may not exist as user in the network.

8.5 Application Server and Presence Server Triggering

The S-CSCF applies trigger filter criteria to determine when to invoke a CS-AS or a PS, that is, when to forward the SIP request to a CS-AS or a PS. These Initial Filter Criterias (iFCs) are stored together with Service Trigger Routing Data in the HSS as part of the user profile and are downloaded to the S-CSCF

upon user registration or upon a terminating initial request for an unregistered user. The iFC is valid throughout the registration lifetime of a user or until the User Profile is changed.

8.5.1 Initial Filter Criteria

This section lists the triggers which are needed for the most common Ericsson IMS Multimedia Telephony services, like Centrex services and the Presence service.

The iFC logic is triggered by the S-CSCF depending if the session is originating or terminating. The triggering information is downloaded from the HSS at initial registration or in case of a terminating session for a not registered user.

The iFC contain the following information:

- Session case; originating, terminating, and terminating to unregistered user
- Trigger point. The trigger points can only be based on the SIP method. The following SIP methods are used in the system:
  - INVITE
  - SUBSCRIBE
  - PUBLISH
  - NOTIFY
- Values of a specific SIP header
- Content of a request URI

The most common triggers used in the Ericsson IMS Multimedia Telephony solution are the following:

CS-AS Triggers

- Originating trigger on INVITE including a contact NOT equal to the CS-AS IP addresses
- Not originating trigger on INVITE, NOT including the parameter ‘‘cscf’’ in the To header
- Not originating trigger on SUBSCRIBE including Event: dialog

PS Triggers

- Originating trigger on PUBLISH including Event: presence
- Not originating trigger on SUBSCRIBE including Event: presence

- Originating trigger on SUBSCRIBE including Event: presence.winfo

8.5.2 Service Trigger Routing Data

The Service Trigger Routing Data contains the following information:

- CS-AS or PS name: The SIP URI that defines where to send the request when the Filter Criteria are fulfilled.

9 Platform Technology

This section describes the platforms used by the system and maps the nodes to the platforms. Hardware such as terminals, power inverters, and extra discs are not included in the description.

9.1 Ericsson Telecom Server Platform

The Ericsson Telecom Server Platform (TSP) is Ericsson's common platform for the next generation network servers and controller nodes. The TSP is intended for telecom and datacom related server and control node applications requiring scalable capacity and high availability.

From an application perspective, the TSP provides a scalable and highly available processor cluster that uses Dicos and Linux™ as operating systems on different processors coordinated by common TSP cluster configuration, distribution, and communication mechanisms. TelORB is the ''clusterware'' that enables the multi processor environment with high availability. Programs can be developed in both C/C++ and Java to handle a large range of processing domain requirements. The TSP 5.2 with Network Server Platform, NSP 5.0 hardware offers redundancy in all components – meaning in case of failure, the load will be automatically redistributed within the node.

The hardware platform includes traffic processors, support processors with their peripherals, signaling processors, Ethernet switches, power supplies, and fans. All processors are off-the-shelf, single-board Compact Peripheral Component Interface (cPCI) standard computers sourced from commercial suppliers. The inherent modular design of the TSP also allows for easy upgrading.

The unit is housed in an Ericsson BYB 501 cabinet and all hardware is accessible from the front panel, ensuring easy maintenance and replacement.

The TSP provides the following:

- Robustness by use of data replication and recovery of crashed processes
- Load control and overload protection
- Scalability (both with respect to processor capacity and data availability)
- Fault detection and fault isolation
- Tracing and debugging support
- Loading, linking, and function change (software and hardware upgrades)
- Correction handling (source code corrections)

- Redundancy in all hardware components
- Industry standard hardware creating a future proof architecture
- Modular platform for maximum flexibility

The CSCFs and the HSS run on TSP 5.2 with Dicos OS.

For more information about the TSP, see the following document:

- *Ericsson Telecom Server Platform TSP 5, Product Description*, Reference [21]

9.2 AXD 301

The system uses AXD 301 as MGW. This is a Carrier Class platform that can be modularly extended from 10 Gbit/s to 160 Gbit/s switching capacity. The AXD 301 hardware duplication and automatic software fault handling minimizes the service disruption in an event of equipment unit failure, and both hardware and software can normally be upgraded without stopping ongoing traffic. The AXD 301 has fully redundant switch fabric, mated-pair redundant control processors and option for auxiliary control processors.

The 10 Gbit/s, 20 Gbit/s, and 40 Gbit/s switch configurations are compliant with ETS 300 119 and can be mounted in any rack or cabinet meeting this specification. They can also be mounted in any NEBS compliant (GR-63-CORE) rack. Switch configurations with the 160 G switch core can only be mounted in Ericsson BYB 501 cabinets.

AXD 301 provides 16 slots per sub-rack for exchange terminals, where each sub-rack can handle up to totally 10 Gbit/s. Each exchange terminal is made up of a front board performing traffic management and forwarding functions, and a rear line interface board that performs transmission and line termination.

The packet termination front board supports either 1xGigabit Ethernet and 1xFast Ethernet, or 2xFast Ethernet, while the circuit termination front board supports a number of E1 and STM-1 configurations, for example, 32xE1 CE or 2xSTM-1 CE.

The control processors run OTP on a Solaris operating system kernel and the device processors use a Vrtx operating system kernel.

For more information about the AXD 301, see the following document:

- *AXD 301 & 305, System Description*, Reference [15]

9.3 Unix and Windows Platforms

Standard platforms.

9.4 Ericsson Integrated Site Infrastructure

The SBG is based on the Integrated Site (IS) framework AZE 101 01/1 and is a blade system domain composed of two types of IS application blade systems; the Session Gateway Controller (SGC) and the Media Proxy (MP), and employs three types of IS infrastructure blade systems. The different blade systems are shown in Figure 15 on page 70.

The IS provides functions for common tasks at a telecom network site, such as hardware and software management, layer 2 and layer 3 transport and resiliency, and perimeter protection. The IS concept makes use of the fact that more and more powerful technologies become available to provide these functions. This is true for payload processing as well as control processing. The highly integrated hardware enables complete node solutions to be integrated on one or a few boards.

The availability of open source and open standards, such as:

- Institute of Electrical and Electronics Engineers (IEEE) Ethernet
- Internet Engineering Task Force (IETF)
- Network Processing Forum
- Service Availability Forum
- Advanced Telecommunications Computing Architecture (ATCA)
- Open Source Development Labs (OSDL),

facilitate the use of new technologies and provides multiple open third-party systems for these technologies. The IS takes advantage of the new technologies, and the application blade systems contribute with added value.

A description of the IS can be found in the following document:

- *Ericsson Integrated Site Infrastructure, Source System Description*, Reference [18]

IS ISP data is collected by an FTP server, see the following document for more details:

- *Section 4.2 IS – Integrated Site* in *Configuration Management Guide, Ericsson IMS Multimedia Telephony*, Reference [2]

The SBG utilizes switching, routing, and support functions provided by the following IS infrastructure blade systems:

- Main Switch Board (MXB)
- IS Edge Router (ISER)
- Site Infrastructure Support (SIS)

– IS common OAM and support functions

– Graphical User Interface (GUI) support

The SGC and MP blade systems contain most of the main SBG functions, control plane and media plane respectively. The SGC implements the B2BUA function and the SIP-H.323 interworking function that controls the dynamic pinhole firewall function implemented on the MP. The MP also implements SBG OAM functions and interworks with the IS common OAM function.

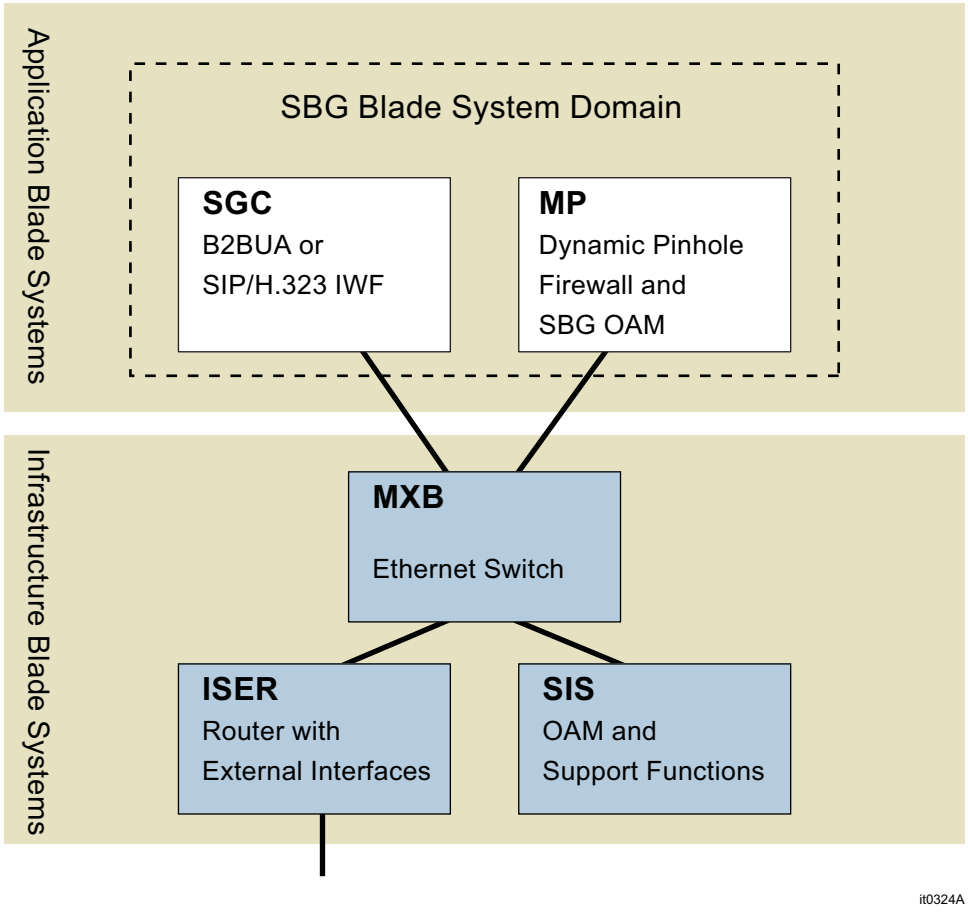


Figure 15 Application and Infrastructure Blade Systems

In the IS, there is a difference between Plug-In Units (PIUs), blades, blade systems, and blade system domains. The following apply:

- A blade is the smallest unit recognized by the IS and consists of a PIU and one or more operating systems.

- A PIU is a hardware unit that can be inserted or removed from an IS subrack and may consist of one or several boards (for example, a motherboard and a daughterboard).

- A blade system contains one or more blades and the software running on them. If a blade system consists of more than one blade, one of the blades handles all communication with the IS OAM and support functions on SIS.

- Multiple blade systems may also form a blade system domain, which means those blades are managed as one entity, for example, from a sales or OAM perspective.

The SBG blade system domain consists of the following application blades that are grouped into application blade systems:

- two or more SGC blades. The SGC blades are grouped in pairs, where each pair form an SGC blade system.

- two MP blades, which form a single MP blade system.

The SBG employs the following IS infrastructure blades grouped into blade systems:

- two MXB blades, which each is a separate blade system

- two SIS blades, which together form a single blade system

- two ISER blades, which each is a separate blade system

All application and infrastructure blades are duplicated in order to provide redundancy.

Further information about the SBG can be found in the following document:

- *SBG, System Description*, Reference [25]

9.5 Firewall – NetScreen-500

The NetScreen®-500 is a purpose-built, security system that integrates firewall, Denial of Service (DoS), Virtual Private Network (VPN), and traffic management functionality.

It provides high throughput for firewall and VPN traffic, and supports the usage of virtual systems and security zones. The hardware architecture incorporating modular physical interfaces, redundant power supplies, fans, and high availability interface.

For more information about the firewall, see the following document:

- *NetScreen-500, User's Guide*, Reference [34]

9.6 L3 Switch – Summit™ 48si

Summit 48si is a one-rack unit Layer 3 (L3) switch with 48x10/100 Mbit Ethernet and 2xGbit Ethernet interfaces. The Summit 48si supports a number of L3 switched services, such as Open Shortest Path First (OSPF), prioritization and bandwidth management, QoS, Access Control Lists (ACLs), and DoS protection.

For more information about the Summit 48si, see the following document:

- *ExtremeWare™ 7.4, User Guide*, Reference [33]

9.7 L3 Switch – Alpine™ 3804

Alpine 3804 is an L3 switch with up to four modules, each module supporting up to 64x10/1000 Mbit Ethernet interfaces.

For more information about the Alpine 3804, see the following document:

- *ExtremeWare 7.4, User Guide*, Reference [33]

9.8 Environmental Performance

Ericsson is working continuously with environmental and sustainability issues, and in 2001 this effort was rewarded when Ericsson was ranked ‘‘the sustainability leader in the communications technology industry’’ on the Dow Jones Sustainability World Index. In 2001 Ericsson also received the world’s first global ISO 14001 (Environmental Management System Standard) certification covering manufacturing and non-manufacturing operations.

In order to secure that environmental requirements are included in the design process of a new product, Ericsson has created the Design for Environment (DfE) concept. These rules covers the following areas:

- Material content the *Ericsson list of banned and restricted substances* lists substances that are not aloud in Ericsson products or substances that should be phased out
- Energy consumption of the product, including support
- Marking of the product
- End of Life treatment

Ericsson works actively with their suppliers in order to minimize the occurrence of hazardous substances in their products. The suppliers are required to comply with the *Ericsson list of banned and restricted substances*. Main goals are to achieve lead free soldering and reduction of use of halogenated flame-retardants and beryllium oxide.

Further information about environmental and sustainability issues can be found at the following URL:

- http://www.ericsson.com/ericsson/corporate_responsibility/environ_sustain/index.shtml

10 Deployment View

This section describes the deployment view of the system on a conceptual level since each installation has dependencies on a number of requirements, for example, number of subscribers, type of traffic, network topology, local security aspects, and so on.

10.1 Network Configuration

The system can be configured in different configurations, to enable logical and geographical distribution of the system into different zones depending on the operator needs. Depending on the network topology, some resources, for example, media resources, may be geographically distributed into multiple instances to prevent latency and enable scalability. In the present solution the following types of zones have been defined:

- Service and Session Control including the system's control signaling nodes; CSCF, HSS, PS, CS-AS, MGC including SS7 connectivity, and internal DNS including NTP
- Management and Support including the system's O&M nodes; EMA, MM, and MN-OSS
- Demilitarized Zone (DMZ) including nodes available for external access; CS-WS, EFWS, and external DNS
- Unprotected including MGW, A-SC, N-SC, CS-CS, and CS-MS enabling communication to external networks

The distribution of different nodes into different zones (and sites) enables separation of different types of traffic and signaling.

10.1.1 Geographical Distribution

The system supports geographical distribution of nodes. It is recommended to deploy the media related nodes on sites close to the access network in order to minimize the media latency and transmission costs.

The nodes handling service and session control can be located anywhere, for example, centrally, in the network, as the signaling latency is not a critical factor.

11 Characteristics

This section contains information regarding the system characteristics and describes the principles for system scalability and availability. Consult the product packaging documentation for available and supported configurations.

11.1 Scalability and Availability

This section provides short description of the availability improving mechanisms on a per platform basis.

11.1.1 Ericsson Telecom Server Platform Entities

The TSP is linearly scalable in processing, memory, and signaling capacity with different standard configurations. Each hardware component can be scaled to provide increased capacity. Traffic processors, support processors, memory cards, disks, and signaling terminals can be added to increase the system capacity.

The TSP is designed for uninterrupted operation. All hardware and software upgrades can be performed on the node while in operation. The high degree of availability and support for uninterrupted operation is achieved through a number of features as described below.

Processing Redundancy

- The node control processors operate in a redundant pair (1+1) configuration.
- The application processors work in an N+1 redundant configuration, that is, if one processor fails, then any one of the remaining takes over.
- The internal switch is operating in a redundant pair configuration.
- In the event of processor failure, the running processes on that processor are switched to another processor automatically. In case of persistent software faults, rollback to the previous configuration takes place automatically.

Load Sharing

Above certain configurable thresholds, the system will start rejecting requests. The platform provides the application with measurement tools to give information on current load situation. Load sharing is distributed deterministically over the available processors.

11.1.1.1 HSS

The HSS works as a single node and is scalable according to the principles of the TSP.

Redundancy is achieved through functions in the TSP platform described in Section 11.1.1 Ericsson Telecom Server Platform Entities on page 77.

The HSS works as a single node and can therefore not be deployed on multiple TSP platforms.

11.1.1.2 CSCF

The CSCF is scalable according to the principles of the TSP. It is also possibly to achieve network scalability by adding new nodes and distribute the traffic among these nodes.

In addition, the CSCF is scalable by functionality according to the 3GPP specification using the P-CSCF, the I-CSCF, and the S-CSCF as described in Section 4.3.1 CSCF – Call Session Control Function on page 26.

Redundancy is achieved through functions in the TSP platform described in Section 11.1.1 Ericsson Telecom Server Platform Entities on page 77.

Network redundancy can be achieved by deploying multiple TSP platforms with the same node.

11.1.2 AXD 301

Adding processors, servers, and interfaces can extend the capacity of the AXD 301 platform.

The MGW is built upon the Carrier Class AXD 301 platform and has fully redundant switch fabric, mated-pair redundant control processors and optional interface redundancy.

The AXD 301 hardware duplication and automatic software fault handling minimizes the service disruption in an event of equipment unit failure, and both hardware and software can normally be upgraded without stopping ongoing traffic.

The MGW has an overload control function to protect it from malfunction in overload situations.

One AXD 301 can be controlled by two MGCs using the virtual MGW concept, whereby the AXD 301 is configured to act as consisting of two virtual MGWs, the first controlled by one MGC, the other controlled by another MGC. Both virtual MGWs share the RTP/voice interfaces, while each signaling interface, as well as TDM link, only can be allocated and used by one of the virtual MGWs.

11.1.3 Presence Services

The entry-level commercial PS configuration consists of the following:

- One Traffic Server
- One Provisioning Server
- One Database and Log Server
- One Standby Database and Log Server

The system can by scaled by adding more Traffic Servers.

The Traffic Servers can be added incrementally up to approximately five Traffic Servers. The CSCF distributes the request between the Traffic Servers based on DNS Active Select.

Database redundancy is achieved using a redundant 2-host hot standby configuration based on Linux High Availability (HA).

Traffic Server redundancy is supported by deploying minimum N+1 Traffic Server hosts. Routing from the CSCF to the PS Traffic Server is done using DNS Active Select, that is, using the same method as for routing to the MGC, as described in Section 11.1.6 MGC on page 82.

Support for Traffic Server redundancy requires customization.

11.1.4 Centrex Services

This section deals with the scalability of the Centrex Services.

11.1.4.1 Hardware Redundancy

The Solstice DiskSuite™ provides a comprehensive data-redundancy solution. It transparently maintains a mirror copy of data on another disk and automatically uses the surviving copy in the event of disk failure.

All Centrex Services Sun™ servers should be configured to use DiskSuite in RAID 1 mode.

11.1.4.2 CS-AS

The CS-AS is scalable by adding additional primary and secondary redundant pairs.

CS-ASs are deployed in primary and secondary redundant pairs. During normal operation, the primary CS-AS will process all calls for its user base. User modifications, additions, and deletions are replicated across the database of both the primary and secondary CS-AS, making all service and user profiles

available on both servers. Database replication is done in real-time, as additions and modifications are made.

In the event that the primary server fails, or is simply inaccessible from one or more endpoints in the network, then those endpoints will be able to route their calls through the secondary server. The fail-over time required for an endpoint to retry the secondary server after a non-response from the primary server is typically engineered to be less than one second. This type of redundancy may be geographically distributed, thereby protecting against server failures as well as against IP networking failures (for example, router and circuit failures).

The CS-AS cluster provides information to the CD-DS about which server, primary or secondary, that serves a certain user. This information is sent using the Application Server Redundancy (ASR) protocol.

For more detailed information about scalability of the CS, see the following documents:

- *BroadWorks, Redundancy Guide*, Reference [30]
- *BroadWorks, Server Security Guide*, Reference [31]

11.1.4.3 CS-MS Pools

Media Servers are deployed in pools of N+1 units. CS-ASs utilize a CS-MS selection policy and a list of available CS-MSs from which media resources may be requested. This enables unlimited scaling of the CS-MS. The CS-AS requests a media resource from the first CS-MS in the list. If the selected CS-MS does not respond, then the next available CS-MS is attempted until success. The fail-over time is engineered to be less than one second. Also, CS-MSs can be added and removed from the network without affecting overall service.

11.1.4.4 CS-CS Stack

The Conference Server is deployed in a stack model divided into two separate physical servers; the Conferencing Application Server (CAS) and the Conferencing Media Server. Each customer installation is then deployed with two CASs and minimum two and maximum ten Conferencing Media Servers.

For non-fail-over conditions, all system signaling and application features use the CAS. The conferencing Media Servers are treated as a single logical stack for both dial-in and dial-out functionality.

The conferencing server is deployed in a stack model divided into two separate physical servers; the CAS and the Conferencing Media Server. Each customer installation is then deployed with two CASs and from two to ten Conferencing Media Servers. One CAS is considered the primary (CAS_1) and the other the secondary (CAS_2).

For non-fail-over conditions, all system signaling and application features use the CAS_1. The Conferencing Media Servers are treated as a single logical stack for both dial-in and dial-out functionality. When there is a conferencing Media Server failure, call logs in-progress on that physical system are dropped and overall system port capacity is reduced. Affected callers can then immediately re-enter a call.

11.1.4.5 CS-WS Pools

The CS-WS farm are deployed in pools of N+1 units.

11.1.4.6 CS-DS

The purpose of the CS-DS is to provide the CS-WS with information about which CS-AS cluster (primary and secondary server) that is serving a specific user. It also holds the information about which server (primary or secondary) that handles the user in case the user is migrated between primary and secondary server.

It can be deployed for scalability and redundancy according to an N+1 scheme. The database, 10times10, which holds the information about the relation between users and the active CS-AS provides facilities for automatic replication of data to all CS-DS servers in the system.

11.1.4.7 CS-CDS

The CS-CDS is an optional server in the CS system that breaks out the management of call logs from the CS-AS. With the CS-CDS, providers can collect of a broader array of call data and distribute those records to other systems in real-time.

More extensive call data from the CS-CDS can be used to offer new feature-functionality to users, such as BroadWorks Enhanced Call Logs. Also, the separation of call log management from the CS-AS enables carriers to further optimize system performance and hardware utilization.

The CS-CDS is not available in a redundant configuration.

11.1.5 EFWS

The EFWS is scalable by adding more memory, or upgrading to a platform with higher processing speed. Any other scaling of the EFWS requires customization.

The EFWS supports node redundancy according to the N+1 principle.

Network redundancy is not supported.

11.1.6 MGC

The MGC, including SS7 connectivity, node is scalable by adding more memory, CPUs, or upgrading to a better performing platform.

It is also possibly to achieve network scalability by adding nodes and distribute the traffic among these nodes.

A single MGC does not itself provide any redundancy.

The High Available MGC (HA-MGC) consists of two physical MGC nodes that form one logical MGC entity. This HA-MGC has one SS7 Originating Point Code (OPC) and one IP address for call and media control signaling (SIP, H.323, RTSP, H.248, and MGCP).

The HA-MGC works as an Active/Standby fashion; one MGC is currently active and processing all the traffic whereas the other one is working as a standby not involved with the traffic at all.

In the HA-MGC both of the physical MGC nodes have their own O&M functionality and are operated separately.

The HA-MGC is configured to the SS7 as one OPC. However, since there are two physical nodes, two physical SS7 termination cards (ISR cards) are needed, one at each node. Both of these cards are active and they both are processing traffic. The traffic between the cards is separated by different link sets, each card has own link sets. The traffic between the cards (link sets) is configured either to work according to load balancing or priority order.

The HA-MGC is configured to the traffical IP network as one IP address with the help of the Ethernet switch. The switch is controlled by the MGC to always route the traffic to the active MGC. The MGC is using SNMP to either active or passive the connected port in the switch to enable only one port being active for the MGC's traffical IP address.

In the case of the failure in the active MGC, the standby MGC detects the lost of the heartbeat and performs a changeover. During a changeover the former standby MGC becomes active and it controls the switch by SNMP to route traffic to the current active MGC. Also during the changeover all the ongoing calls are disconnected.

The MGC supports DNS NAPTR records to resolve the correct server for SIP sessions as defined in RFC 3263 and RFC 2782. However, it uses the first server of the highest priority without (weight-based) random selection among the servers with the same priority. The other servers are not tried in case the selected one would not be available.

The MGC application does not implement any application internal DNS cache, thus the results from the RFC 3263 and RFC 2782 processing is dependent on the order the DNS server has organized the NAPTR records when sending the DNS response to the MGC. Unless the DNS server feeding the MGC application with the NAPTS records is varying the contents and the order of the server records between each DNS query, the following is true for the SIP server redundancy and load sharing for SIP sessions initiated from the MGC:

- There is no redundancy in the SIP interface. The services provided by the addressed server will not be available in the case of failure. All the calls to that server will be rejected.

- There is either no load sharing between the SIP servers; the SIP traffic will be routed only to the first one among the same highest priority value in the NAPTR records.

11.1.7 EMA

The EMA operates as a single node in the system.

The EMA is scalable by adding more memory, or upgrading to a platform with higher processing speed.

Any other scaling of the EMA requires a customization.

The EMA does not support node redundancy.

Network redundancy is not supported.

Node redundancy can be provided as a customization based on the Sun Microsystems™ Sun Cluster software.

11.1.8 MM

The MM is divided in two physical entities; Online Mediation hosting Event Collector functionality and File and Event Mediation. The Event Collector node terminates the charging output signaling from the traffic nodes and performs filtering of data while the File and Event handles more advanced filtering, correlation, consolidation, and formatting of CDRs.

The Event Collector is scalable in number of physical nodes.

The File and Event Mediation is scalable by adding more memory and CPUs and by adding more nodes.

Node redundancy for the Event Collectors is provided by deploying the Event Collectors in pools of N+1 units. The traffic nodes will be configured to load balance between the Event Collectors.

Node redundancy for File and Event Mediation can be achieved using a cluster solution consisting of a 1+1 solution, that is, two hosts working together in a cluster. In case of failure on one of the File and Event Mediation hosts, the cluster solution makes it possible for one Online Mediation host to take over network interfaces and processing from the other Online Mediation host. The advantage of this solution is that the cluster software detects errors and conducts a fail-over instantaneously, and automatically. The failover is not dependent on functions in the network.

11.1.9 MN-OSS

The MN-OSS operates as a single node in the system.

The MN-OSS is scalable by adding more memory and CPUs according to a number of predefined deployment alternatives described in the following document:

- *MN-OSS 7.0, System Description*, Reference [24]

Any other scaling of the MN-OSS requires customization.

The MN-OSS does not support node redundancy.

Network redundancy is not supported.

Node redundancy can be provided as a customization based on local site requirements.

11.1.10 DNS

The DNS is, in most cases, linearly scalable with processing and memory capacity. Different configurations and platform characteristics may alter scalability of the system. The DNS also supports scaling by adding servers to the network. Both DNS and DHCP capacity can be increased with the addition of more servers.

High availability and reliability are built into the DNS protocol, resolvers, and servers. Resolvers are usually configured to talk to several DNS servers. If one of the servers is unavailable, the resolver will choose the next server on the list and attempt to query it.

For most DNS network solutions, a minimum of two DNS servers are deployed in a master and slave configuration. More slave servers can be deployed if additional reliability or capacity is required. Data between the two servers is synchronized using standard DNS features including zone transfers, incremental zone transfers, and notify. The combination of the features ensures that updates propagate to all DNS servers.

11.1.11 SRD

The SRD is scalable by adding more memory and CPUs. Additionally, the SRD can be configured to use replication to support scalability among several nodes.

Any other scaling of the SRD requires customization.

SRD provides a 1+1 HA concept where read operations are evenly distributed between the two nodes and where one of the nodes acts a default server for write operations.

In case of failure in one of the nodes, the remaining one will handle all read operations and will also take over as default node for write operations.

The SRD-HA solution is implemented using the two front-end Ethernet switches belonging to the core system.

11.1.12 RS

The RS node is stateless. There could be as many instances of the RS as required.

Scalability of the RS is based in the way MAE users are grouped in the SRD. One single RS takes care of one group of MAE users in the SRD.

At provisioning time, every MAE user should be marked with a group identifier in the SRD. The group identifier corresponds to the MAE flag indicating if a user is subscribed to the MAE service. The absence of this identifier indicates a user which is not subscribed to the MAE service.

In a network with N instances of the RS, the provisioning system should take care of provision MAE users with N different MAE flags (for example, RS_01, RS_02... RS_N) evenly distributing the users in the different groups.

Then, the search filter in every RS node should be set to serve the corresponding user group.

11.1.13 SBG

An IS subrack contains 26 slots of which 16 are available for the SBG application blade systems after the mandatory IS infrastructure blade systems have been inserted. The SBG application blade systems need four slots each (two blades of two slots width). The SBG is configured with one MP blade system and one, two, or three SGC blade systems, depending on the signaling traffic intensity in relation to the media plane traffic. There is no limit on the amount of subracks that can be used.

12 Provisioning Services

The system provides two types of provisioning interfaces, a machine-machine interface (MMI) used by the CAS and Graphical User Interfaces (GUIs) used by the administrators and users (for self provisioning). The provisioning solution is illustrated in Figure 16 on page 87.

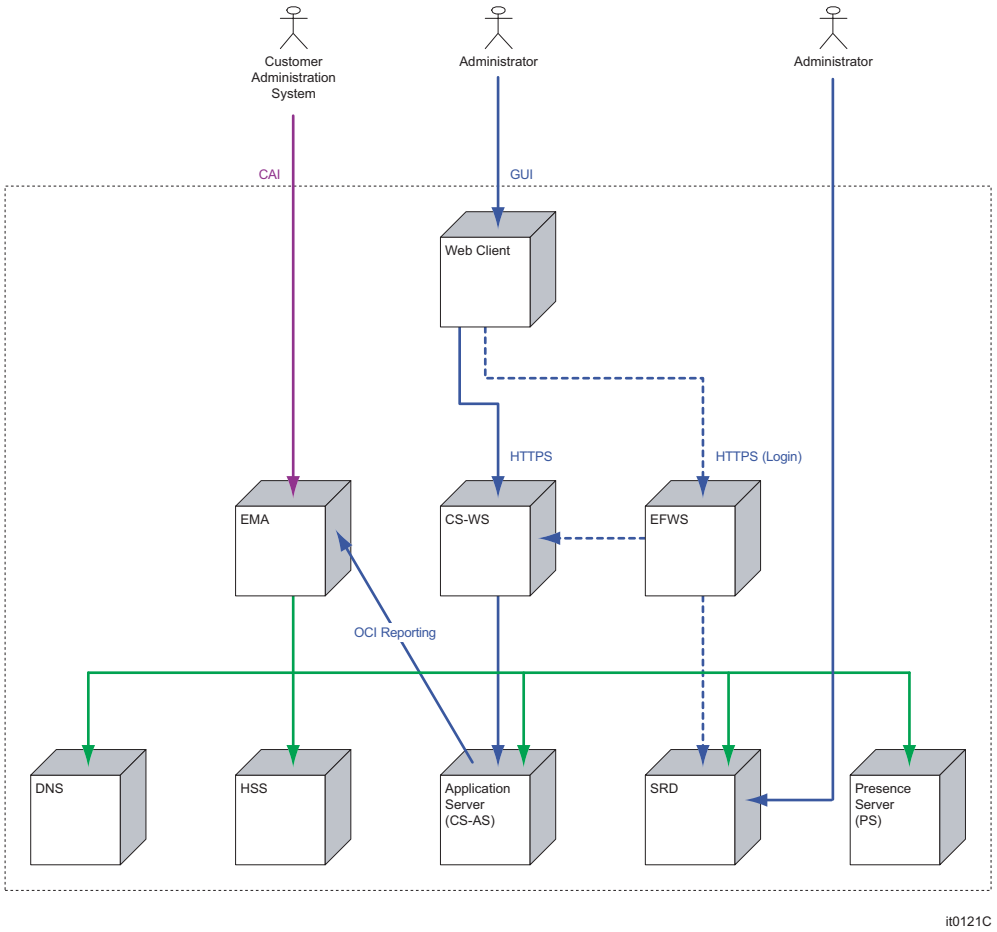


Figure 16 Provisioning Overview

The CAS accesses the EMA using the CAI (or CAI3G), while the administrators access the CS GUI (through the CS-WS) using a web client.

Changes made using the CS GUI, that is, by accessing a BroadWorks web portal, are propagated to relevant nodes in the system through the EMA and the CS OCI reporting interface.

Note that service providers and groups must be created through the CAI (or CAI3G), but they can be modified using both the CAI (or CAI3G) and the CS GUI.

All web client access to the provisioning interfaces and portals are always authorized through the EFWS.

Users have to be manually provisioned in the SRD in the first release of the MAE. In following MAE releases all provisioning should be performed through the EMA.

12.1 Creation, Modification, and Removal of Subscriptions

This section describes how creation, modification, and removal of subscriptions can be performed.

12.1.1 End-Users

End-user subscriptions can be created, modified, or removed using both the CAI (or CAI3G) and the CS GUI.

12.1.2 Groups

Groups must be created through the CAI (or CAI3G), but can be modified using both the CAI (or CAI3G) and the CS GUI.

12.1.3 Group and Department Administrators

Group and department administrators can be provisioned using either the CAI (or CAI3G) or the CS GUI.

The group administrator can administer the users of the group (according to their administrator credentials) through the CS GUI. The department administrator can, except from organizing users, also administer department hierarchies.

12.1.4 Service Providers and Large Enterprises

Service providers and large enterprises must be created through the CAI (or CAI3G), but can be modified using both the CAI (or CAI3G) and the CS GUI.

12.2 Service Provisioning

Provisioning of services (for example, Voice Mail, Call Forwarding, and so on) can be done using either the CAI (or CAI3G) or the CS GUI. However, note that activation and deactivation of the presence service only can be done through the CAI (or CAI3G).

Service assignment can be performed by group administrators, service providers, system providers, and in some cases through self provisioning.

12.3 Self Provisioning

The web client can be used for user self provisioning tasks, for example, activation of Call Forwarding.

For further information about end-user interfaces, see the following document:

- *End-User Interface, Ericsson IMS Multimedia Telephony*, Reference [4]

13 Charging

A simplified example of the charging data collection and consolidation process is shown in Figure 17 on page 91.

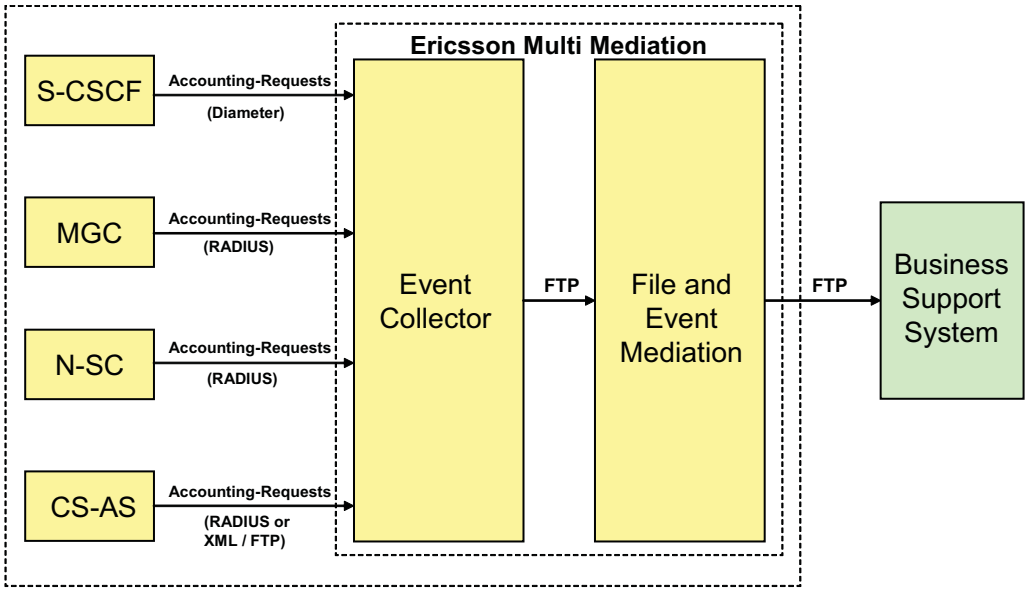


Figure 17 SIP-to-GSTN Call – CDR Collection Example

Charging data generated by the core nodes in the Ericsson IMS Multimedia Telephony system are first sent to an MM event collector. For load balancing purposes, it is possible to implement several instances of event collectors. The MM event collectors are part of the MM system.

In the MM event collector, basic data filtering can be made, for example, to make sure that surplus data not is wasting bandwidth in the data collection network.

Charging data can then be consolidated by an MM data consolidator instance, File and Event Mediation, before sent to a billing system. It is possible to implement several instances of the MM data collectors in an Ericsson IMS Multimedia Telephony system.

13.1 P-Charging-Vector

Support for P-Charging-Vector is needed in order for the offline systems to be able to correlate, for example, originating CDRs generated by different nodes for the same call. The P-Charging-Vector includes the IMS Charging Identifier (ICID) as correlation identity and the Originating and Terminating Inter

Operator Identifiers (O-IOI and T-IOI) identifying the operators that originates and terminates the call, respectively. The first charging data outputting node involved in a call defines and creates the ICID while the originating S-CSCF and terminating S-CSCF nodes involved in a call defines and creates the O-IOI and T-IOI, respectively.

This header is included both in inter-nodal SIP signaling (in trusted domain) and in the nodal charging output.

13.2 P-Charging-Function-Address

A number of consolidation processing MMs can be used to handle the charging requests. This header indicates to the MM Event Collector which MM consolidation processing address to send the charging information to when several consolidation processing MMs are used in the Ericsson IMS Multimedia Telephony system.

The P-Charging-Function-Addresses is assigned in the HSS to balance the load between the consolidation processing MMs.

14 Operation and Maintenance Services

This section describes the system's operation and maintenance services. The International Organization for Standardization (ISO) has developed an international network management model known as the FCAPS model. This model identifies the following five key areas that make up the basis of network management:

- **Fault Management** – Fault management is the detection and correction of abnormal network operation. It provides the means to collect and correlate alarms from the network elements and to present this information to the network operator.

- **Configuration Management** – Configuration management encompasses activities such as providing and updating the network elements with the data, parameter settings, and connectivity information necessary for them to provide the services and functions within the network for which they were intended. This also includes software update and maintenance.

- **Accounting Management** – Accounting management includes tasks such as tracking of service usage and billing of services. Charging is described in Section 13 Charging on page 91.

- **Performance Management** – Performance management provides functions to report upon and evaluate the behavior and the effectiveness of the network or network element. Its role is to gather and analyze statistical data for the purposes of monitoring and correcting the behavior and effectiveness of the overall network as well as that of the individual network elements.

- **Security Management** – Security management is the control and monitoring of access to a network, its elements and to the services it provides to minimize unauthorized or accidental access to network control functions. All security issues are described in Section 15 Security on page 103.

For a detailed overview of the system's O&M support, see the following document:

- *Operation and Maintenance Overview, Ericsson IMS Multimedia Telephony*, Reference [7]

14.1 Remote Management

The O&M network can be configured in two different ways to enable remote access. The first alternative is to use a physically separate WAN for the O&M and the second alternative is to use the same physical WAN for all traffic, including O&M. The second alternative requires that the traffic must be separated using security zones.

14.1.1 Terminal Server

It is recommended to use a Terminal Server to enable remote management of the system's nodes through the console port. The terminal server will support the needed amount of console ports to access all nodes in the system.

14.2 Fault Management

Fault management is implemented with the Ericsson Fault Manager (FM) included in the MN-OSS and it provides the functionality to detect and correct abnormal network operation. The FM provides Java-based Alarm Status Viewer, Alarm List Viewer, and Alarm Log Browser.

In the presentation view, the FM displays the network elements and their connections graphically. Any network element, that is, faulty is indicated on this view by its representation changing color or shape. It is possible to launch the appropriate alarm lists and element managers by clicking on the graphical representation of the network element.

Alarms are collected from the various network elements using a fault management interface (see Table 5 on page 100). The interfaces used are currently one of the following:

- CORBA (TSP)
- SNMP (the majority of nodes)
- BNSI (AXD 301)

The OSS internals work using BNSI, this being an Ericsson proprietary interface and so those nodes not using BNSI but CORBA or SNMP have mediation software that convert their incoming alarms into this BNSI alarm format, which are then forwarded into the OSS FM kernel (BNSI manager).

The generated faults may in some cases also be monitored using the node's element managers, described in Section 14.3 Configuration Management on page 95.

Supported nodes are listed in Section 14.5 MN-OSS Supported Network Elements on page 100 and details regarding fault management can be found in the following documents:

- *Fault Management, Ericsson IMS Multimedia Telephony*, Reference [3]
- *Troubleshooting, Ericsson IMS Multimedia Telephony*, Reference [13]
- *HW Repair, Ericsson IMS Multimedia Telephony*, Reference [5]

14.3 Configuration Management

The element manager of each node is used to support the configuration management activities of the system. These element managers can be launched from within the MN-OSS integrated one-screen view.

Some element managers may also be used for other O&M purposes, such as fault and performance management.

Configuration (provisioning) of subscribers and services is described in Section 12 Provisioning Services on page 87.

Further information about configuration management related tasks can be found in the following documents:

- *Configuration Management Guide, Ericsson IMS Multimedia Telephony*, Reference [2]
- *Backup Handling, Ericsson IMS Multimedia Telephony*, Reference [1]
- *Restore Handling, Ericsson IMS Multimedia Telephony*, Reference [10]
- *Maintenance, Ericsson IMS Multimedia Telephony*, Reference [6]

14.3.1 Element Management of CSCF and HSS

The O&M Toolbox is the element manager of the TSP and its applications. It handles fault, configuration, performance, and security management tasks and can be launched from a standard web browser.

The element manager supports the following functions:

- Configuration management, which comprises system configuration, service provisioning, and software and hardware management
- Fault management, which comprises receiving and filtering of alarms and managing alarm list
- Performance management, which comprises data collection and performance management presentation
- Security management, which comprises authentication, access control, and authorization administration

14.3.2 Element Management of Presence server

The PS has no element manager. Configuration is done through configuration of the servers file and is simplified with what is called the Sapphire Shell or SASH. SASH is a shell, similar to that of an ordinary ‘‘shell’’ that can be started inside an operating system and simplifies some of the tasks performed in the

PS's environment/platform (M2CE). For the service provisioning parts of the PS a CLI is provided.

14.3.3 Element Management of CS Nodes

The element manager of the CS-AS, CS-MS, CS-CS, CS-DS, CS-WS, and CS-CDS is a CLI. It handles configuration, performance, fault, and security management tasks. There is also a web GUI available but this can only be used for service provisioning tasks.

The element manager supports the following functions:

- Configuration management, which comprises system configuration and service provisioning
- Fault management, which comprises inspect alarm logs and clear alarms
- Performance management, which comprises data collection and presentation
- Security management, which comprises authentication, access control, and authorization administration

14.3.4 Element Management of MGC

The MGC has a management solution that comprises of four different softwares; MGC Management Server, Management Console, Bootstrap server, and the most commonly known of them all, the MeGaCo Manager. Between these four management tools the MGC is supported for configuration, fault, performance, and security management tasks.

14.3.5 Element Management of MGW

The MGW provides a web-based GUI using HTTP for built-in element management and a FTP client is used for file transfer. The web-based GUI handles configuration, fault, performance, and security management tasks. The web-based GUI accesses the same MIB information as the supported SNMP interface and supports the following functions:

- Configuration management, which comprises system configuration
- Fault management, which comprises display, acknowledge, and clear alarms
- Performance management, which comprises data collection and presentation
- Security management, which comprises authentication, access control, and authorization administration

14.3.6 Element Management of EMA

The element manager of the EMA is a web-based GUI. It handles configuration, performance, fault, and security management tasks.

The element manager supports the following functions:

- Configuration management, which comprises system configuration and service provisioning
- Fault management, which comprises inspect alarm logs
- Performance management, which comprises data collection and presentation
- Security management, which comprises authentication, access control, and authorization administration

14.3.7 Element Management of MM

The element manager of the MM is a web-based GUI. It handles configuration, performance, fault, and security management tasks.

The element manager supports the following functions:

- Configuration management, which comprises system configuration and service provisioning
- Fault management, which comprises inspect alarm logs
- Performance management, which comprises data collection and presentation
- Security management, which comprises authentication, access control, and authorization administration

14.3.8 Element Management of DNS Server

The IPWorks element manager is the element manager of the IPWorks Protocol Server. It handles configuration, performance, and security management tasks.

The element manager supports the following functions:

- Configuration management, which comprises system configuration and service provisioning
- Performance management, which comprises data collection and presentation
- Security management, which comprises authentication, access control, and authorization administration

14.3.9 Element Management of SRD

The SRD has no element manager in the same sense as the other network elements. However, there is an ‘‘Administrator console’’ that could be considered as a ‘‘basic’’ CLI.

The console supports the following functions:

- Configuration management, which comprises system configuration
- Security management, which comprises authentication and access control

14.3.10 Element Management of NetScreen Firewall

The element manager of the firewall is a web-based GUI or a CLI, both handling configuration, performance, fault, and security management tasks.

The element manager supports the following functions:

- Configuration management, which comprises system configuration
- Performance management, which comprises data collection and presentation
- Fault management, which comprises alarm log inspection
- Security management, which comprises authentication, access control, and authorization administration

14.3.11 Element Management of Summit 48si and Alpine 3804 Switch

The element manager of the switch is either a web-based GUI or a CLI. They both handle configuration, performance, fault, and security management tasks.

The element manager supports the following functions:

- Configuration management, which comprises system configuration
- Performance management, which comprises data collection and presentation
- Fault management, which comprises alarm log inspection
- Security management, which comprises authentication, access control, and authorization administration

14.3.12 Element Management of SBG

The SBG is a managed function in the IS with the management interfaces located on the SIS blade system. There are three parts of the SBG OAM functionality, as follows:

- The IS provides a set of common functions, which are used when operating a SBG, like a GUI portal, hardware, software management, fault management, and log services.
- The ISER configuration and performance monitoring is a separate function that allows the operator to tailor filters rules and so on for each specific network scenario.
- The SBG-specific OAM function provides the means to configure and report status, statistics, and logs of the SBG blade system domain and also has the task of automatic establishment of the internal H.248 links between the SGCs and MP.

The IS Management system (ISM) is the web-based element manager with the operator interface for IS common functions and the SBG. The IS common functions also have northbound interfaces for integration with the MN-OSS. In addition, there is a CLI to the ISER.

The management traffic is routed to external management systems, like the MN-OSS, through the ISER, where the physical interfaces to remote systems are located. The SIS ISM and the ISER CLI can also be accessed from a locally connected terminal connected on the SIS Ethernet port. The ISER CLI can also be accessed from a terminal directly connected to the ISER.

14.3.13 Element Management of RS

The RS is configured manually.

Configuration of the RS is performed by accessing the configuration files through SSH. Every update to the configuration files requires an RS client restart in order for the new configuration to take effect.

14.4 Performance Management

The MN-OSS Analyzer application is the core of the performance management in the system. It assists the operator in the short-term surveillance (monitoring) of the network and is therefore useful in locating faults and trouble spots within the network and is an aid to traffic management. In addition, the Analyzer can collect performance data over a longer period of time to provide reliable statistics for long-term network planning.

The Analyzer collects measurement data from the network elements and aggregates and manipulates this data according to a user (operator) definable data model. The results of this aggregation are then placed in a relational

database from where they can be retrieved by other applications, which use SQL.

The Analyzer supports a web-based application that presents performance data reports in a variety of formats, which can be defined by the operator. The application is delivered with a number of pre-defined reports for the more common performance management tasks. The Analyzer can also be set up to monitor network elements and to provide alarms when user defined thresholds have been exceeded.

For details regarding performance management, see the following document:

- *Performance Management, Ericsson IMS Multimedia Telephony*, Reference [8]

14.5 MN-OSS Supported Network Elements

The MN-OSS manages the following products and network elements:

Table 5 MN-OSS Supported Network Elements

Network Element	Functionality	Management Protocol
HSS	– Alarm Mediation with Synchronization	SNMP
	– Element Manager Integration	HTTPS
	– Performance Management	SFTP
CSCF	– Alarm Mediation with Synchronization	SNMP
	– Element Manager Integration	HTTPS
	– Performance Management	SFTP
MGC including SS7 connectivity	– Alarm Mediation with Synchronization	SNMP
	– MeGaCo	SNMP
	– Performance Management (signaling report)	SNMP
MGW	– Alarm Mediation with Synchronization	BNSI
	– AXD Operational Suite (AOS)	HTTPS
	– Performance Management (signaling report)	BNSI
A-SC	– Alarm Mediation	SNMP
	– Element Manager Integration	Telnet/SSH/CLI
N-SC	– Alarm Mediation	SNMP
	– Element Manager Integration	Telnet/SSH/CLI

Table 5 MN-OSS Supported Network Elements

Network Element	Functionality	Management Protocol
PS	– Alarm Mediation	SNMP
	– Sapphire Shell	Telnet/SSH/CLI
	– Performance Management	SNMP
CS-MS CS-AS CS-CS CS-WS CS-DS CS-CDS	– Alarm Mediation, SNMPv3 – Element Manager Integration – Performance Management	SNMP HTTPS and Telnet/SSH/CLI
EFWS	– Alarm Mediation	SNMP
DNS	– Alarm Mediation	SNMP
	– Element Manager Integration	HTTP
EMA	– Alarm Mediation with Synchronization	SNMP
	– Element Manager Integration	HTTP
MM	– Alarm Mediation with Synchronization	SNMP
	– Element Manager Integration	HTTP
SRD	– Alarm Mediation	SNMP
RS	– Alarm Mediation	SNMP
	– Performance Management	FTP
	– Configuration	SSH
SBG	– Alarm Mediation	SNMP
	– Element Management Configuration	HTTP/SSH
	– Performance Management	FTP
NetScreen-500	– Alarm Mediation	SNMP
	– Element Manager Integration	HTTP
L3 Switch Summit 48si	– Alarm Mediation with Synchronization	SNMP
	– Element Manager Integration	HTTP
L3 Switch Alpine 3804	– Alarm Mediation with Synchronization	SNMP
	– Element Manager Integration	HTTP

15 Security

Security is not one function or feature but a consistent set of functions that need to be available throughout the system. The security is divided into the following sub-areas:

- *Access security* covering security between end-users and the home Ericsson IMS Multimedia Telephony network.

  Note: The use of DHCP in the access network must be well defined to avoid that a DHCP IP address is re-used before the SIP registration has expired for a previous user. For further information on how to avoid this kind of double registrations, contact the local Ericsson office.

- *Network domain security* covering perimeter protection and communication protection to co-operating external IPMM networks (operators) and between dispersed sites. It also covers node protection and security audit logging.

- *O&M security* covering access control for management operations and the protection of O&M, provisioning, and charging interfaces.

- *Security management* covering the management of security functions and attributes. Security management also covers general management procedures for enhancing security.

  For further information about security management, see the following document:

  – *Security Management, Ericsson IMS Multimedia Telephony*, Reference [11]

Reference List

System Documents

[1] *Backup Handling, Ericsson IMS Multimedia Telephony*, 7/198 17-HSC 113 03/4

[2] *Configuration Management Guide, Ericsson IMS Multimedia Telephony*, 2/198 17-HSC 113 03/4

[3] *Fault Management, Ericsson IMS Multimedia Telephony USER GUIDE*, 1/198 17-HSC 113 03/4

[4] *End-User Interface, Ericsson IMS Multimedia Telephony*, 1/155 17-HSC 113 03/4

[5] *HW Repair, Ericsson IMS Multimedia Telephony*, 12/198 17-HSC 113 03/4

[6] *Maintenance, Ericsson IMS Multimedia Telephony*, 11/198 17-HSC 113 03/4

[7] *Operation and Maintenance Overview, Ericsson IMS Multimedia Telephony DESCRIPTION*, 2/1551-HSC 113 03/4

[8] *Performance Management, Ericsson IMS Multimedia Telephony USER GUIDE*, 4/198 17-HSC 113 03/4

[9] *Residential and Centrex Services, Ericsson IMS Multimedia Telephony,* , 9/155 17-HSC 113 03/4

[10] *Restore Handling, Ericsson IMS Multimedia Telephony*, 8/198 17-HSC 113 03/4

[11] *Security Management, Ericsson IMS Multimedia Telephony USER GUIDE*, 5/198 17-HSC 113 03/4

[12] *Terms and Definitions – Ericsson IMS*, 0033-HSC 113 03

[13] *Troubleshooting, Ericsson IMS Multimedia Telephony*, 6/198 17-HSC 113 03/4

[14] *User and Service Provisioning, Ericsson IMS Multimedia Telephony*, 9/198 17-HSC 113 03/4

Ericsson Node Documents

[15] *AXD 301 SYSTEM DESCRIPTION*, 1551-AXD 301 01

[16] *CSCF Node Product Description* , 221 02-FAP 901 0600/2

[17] *Ericsson Front-End Web Server 2.0*
USER GUIDE, 2/1551-APR 901 811

[18] *Ericsson Integrated Site Infrastructure, Source System Description*, 1551-HSC 901 63

[19] *Ericsson Multi Mediation 5.0, File and Event Mediation - Network Element Description*, 1/1551-FAM 901 346

[20] *Ericsson Multi Mediation 5.0, Online Mediation - Network Element Description*, 1/1551-FAM 901 344

[21] *Ericsson Telecom Server Platform TSP 5*
PRODUCT DESCRIPTION, 221 01-ANA 901 04/1

[22] *HSS 4.0, Technical Product Description*, 221 02-FGC 101 948

[23] *IPWorks 4.2*
TECHNICAL PRODUCT DESCRIPTION, 221 02-FGC 101 873

[24] *MN-OSS 7.0*
SYSTEM DESCRIPTION, 1/1551-AOM 901 031

[25] *SBG, System Description*, 2/1551-HSD 101 96/1

[26] *SRD 2.0, Technical Product Description*, 221 02-HDA 104 02/3

Other Node Documents

[27] *BroadWorks Application Server, User Web Interface*
ADMINISTRATION GUIDE, 190 89-LZN 708 0093/10

[28] *BroadWorks, Call Detail Record*
INTERFACE SPECIFICATION, 190 89-LZN 708 0093/15

[29] *BroadWorks Centrex Services (CS) System*
PRODUCT DESCRIPTION, 190 89-LZN 708 0093/1

[30] *BroadWorks, Redundancy Guide*, 190 89-LZN 708 0093/19

[31] *BroadWorks, Server Security Guide*, 190 89-LZN 708 0093/3

[32] *BroadWorks Web Server, Configuration Guide*, 190 89-LZN 708 0093/21

[33] *ExtremeWare 7.4*
USER GUIDE, 190 89-LZN 768 0011/5

[34] *NetScreen-500*
USER GUIDE, 190 89-LZN 768 0012/2

[35] *Presence Server, Oracle M2CE*
PRODUCT DESCRIPTION, 190 89-LZN 708 0094/1

Online References

[36] *Ericsson Internet Site, Environment & Sustainability*, http://www.ericsson.com/ericsson/corporate_responsibility/environ_sustain/index.shtml