vvMTAS 1 Technical Product Description Common Features

TECHN PRODUCT DESCR

1/221 02-FGC 101 3266 Uen Rev A

Content

1 Introduction

1.1 Scope

MTAS Technical Product Description consists of a number of documents. They describe the telephony application server MTAS. MTAS executes services such as 3GPP defined Multimedia Telephony Service and Supplementary Services (MMTel) (ref [2], ref [3]) and supports Voice over LTE (VoLTE) according to GSMA IR.92 and IR.94 (ref [4], ref [5]) including Service Centralization and Continuity (SCC).

The scope of MTAS technical product description is to:

- Provide a fundamental understanding of the MTAS's role and functionality.
- Provide an architectural overview of MTAS and describe the system boundary, element management, characteristics and interfaces.

This document describes the MTAS product, vMTAS, to be deployed as virtualized network element in an IMS network. This deployment is by the network function virtualization (NFV) industry specification group referred to as a VNF (Virtualized Network Function) (ref [6]).

The MTAS VNF is a stand-alone software only product which has a central role in a Multimedia Telephony solutions and VoLTE solutions. The MTAS VNF is referred to as 'MTAS' in this document

The MTAS technical product description is composed of multiple documents dedicated to MTAS common features and application server specific features respectively:

MTAS Technical Product Description ---- Common Features

1/221 02-FGC 101 3266

MTAS Technical Product Description ---- MMTel AS Features

2/221 02-FGC 101 2990

MTAS Technical Product Description ---- SCC AS Features

4/221 02-FGC 101 2990

MTAS Technical Product Description ---- ST AS Features

5/221 02-FGC 101 2990

This document provides an overview of MTAS product, plus features that are common to all application servers.

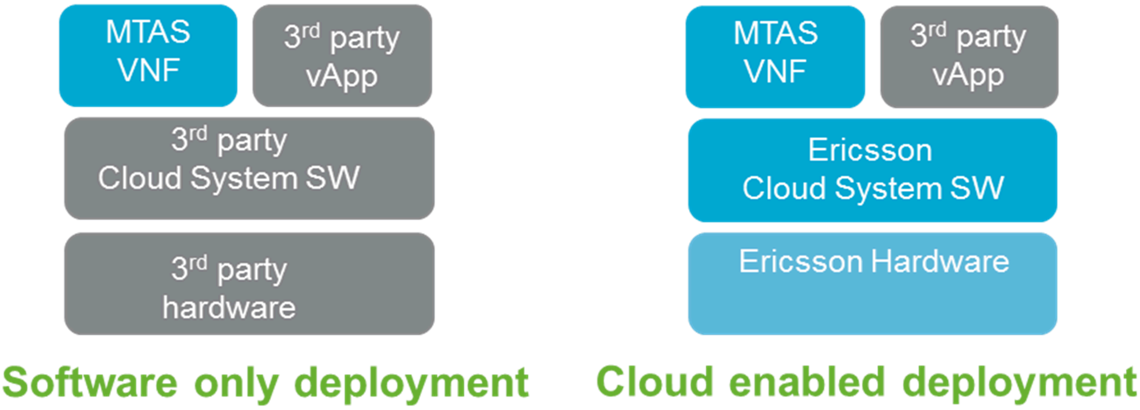
1.2 Change History

Revision	Date	Comments/Changes
PA	2016-08-29	Approved version.

2 Overview

2.1 Deployment options

An MTAS VNF can be deployed as a software only product or as a Cloud enabled product as shown in the picture below. The characteristics of the VNF are verified on a *reference configuration* which includes the MTAS VNF, the OpenStack Cloud Execution Environment, and the Ericsson Blade Server Platform. If a different environment is chosen there is a need for a system integration activity to verify and document the characteristics of the system.



2.2 Main features and benefits

MTAS can fulfill several different functional roles in a multimedia telephony solution. These roles are Multimedia Telephony application server (MMTel AS), Service Centralization and Continuity application server (SCC AS) and SIP Trunking application server (ST AS).

The MMTel AS provides multimedia telephony service and supplementary services according to 3GPP standards which also include TISPAN defined PSTN/ISDN Simulation Services (ref [2]-[4]). The MMTel AS also provides service creation interfaces.

The SCC AS provides the possibility to offer IMS centralized services (ICS) and single radio voice call continuity (SR-VCC) according to 3GPP standards (ref [8]-[9]) which are key components for a voice over LTE (VoLTE) solution.

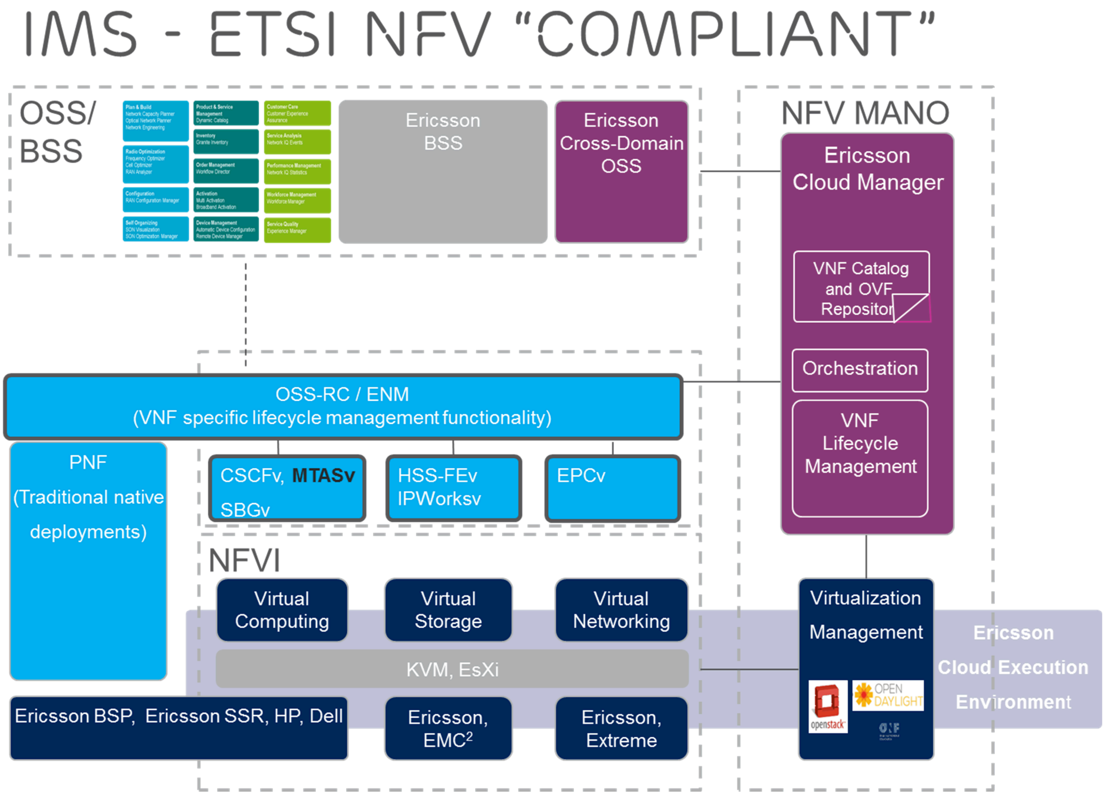
The ST AS provides access between operators IMS network and enterprise PBXs. In addition it serves the operator with regulatory and supplementary services. The ST AS provides the core functionality of a SIP Trunking solution.

For more information on which are basic and which are optional features in MTAS, please refer to MTAS Feature Description [1].

2.3 MTAS in the network

2.3.1 MTAS from a virtualization point of view

The MTAS product, vMTAS, is intended to be deployed as a virtualized network element in an IMS network as shown in the example below:



MTAS traditional services and data are managed by OSS over an NBI (COM CLI, COM NETCONF, COM SNMP, COM SFTP, and LDAP for configuration of DNM data).

MTAS as a VNF in a cloud is managed by a VNF manager. Basic cloud operations like deployment, start/stop, scaling in and out, and cloud related troubleshooting of a VNF is supported.

2.3.2 MTAS from an IMS point of view

All roles supported by MTAS (MMTel AS, Conf AS,SCC AS and ST AS) can be deployed as stand-alone network elements or all roles can be deployed collocated on the same network element.

Depending on how MTAS is deployed, each AS is invoked by separate triggers in the initial filter criteria (IFC). The separate triggers enables chaining of application servers and other application servers can be invoked in between the MTAS application servers if desired.

MTAS's place in IMS MMTel architecture is shown in Figure 1 Ericsson MMTel and associated Nodes.

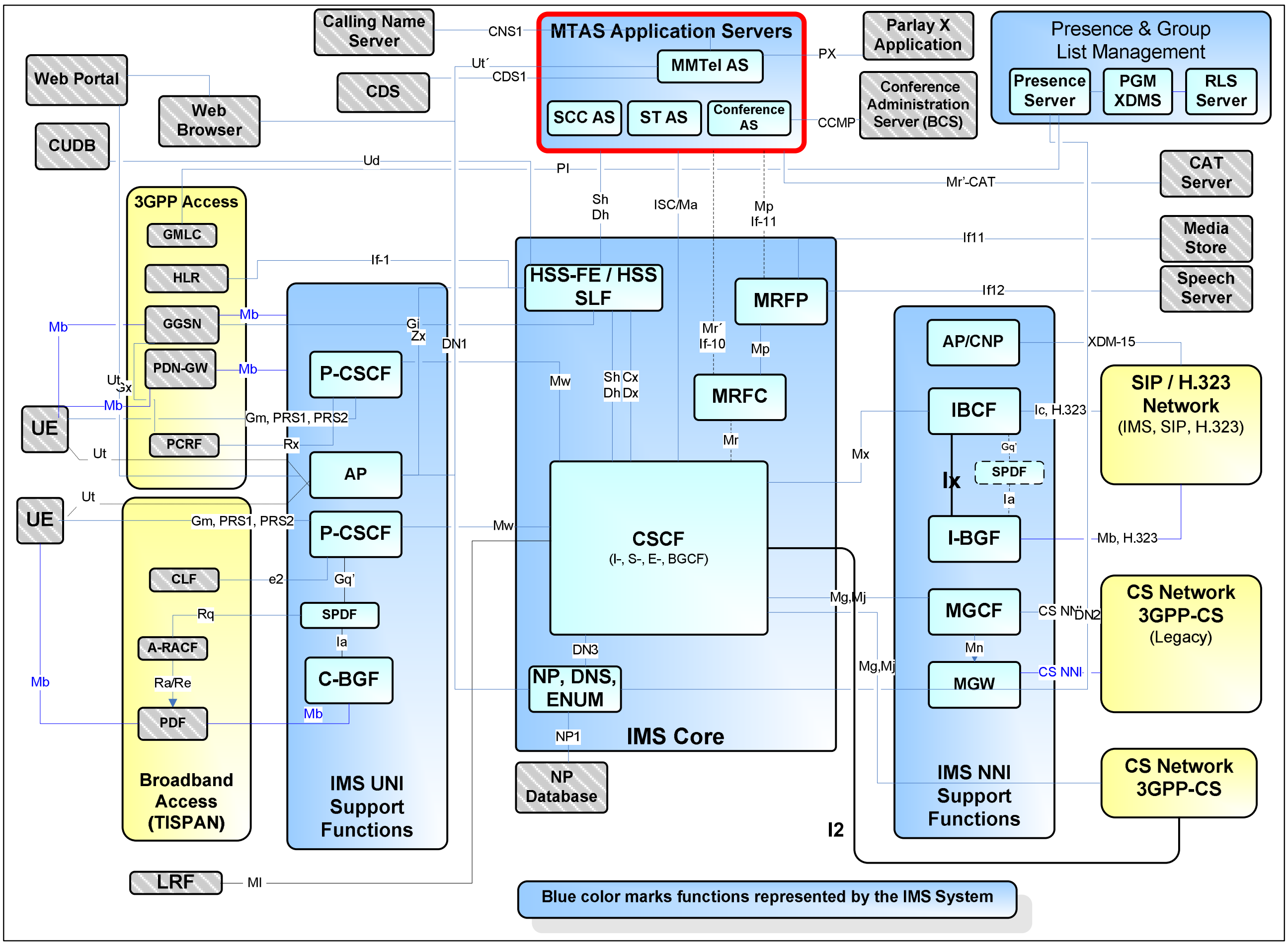


Figure 1 Ericsson MMTel and associated Nodes

2.3.3 B2BUA, Session Control and Service Interaction

MMTel AS is involved in both the originating and terminating MMTel signaling sessions and acts as Back-to-back User Agent (B2BUA) defined in RFC3261 [22].

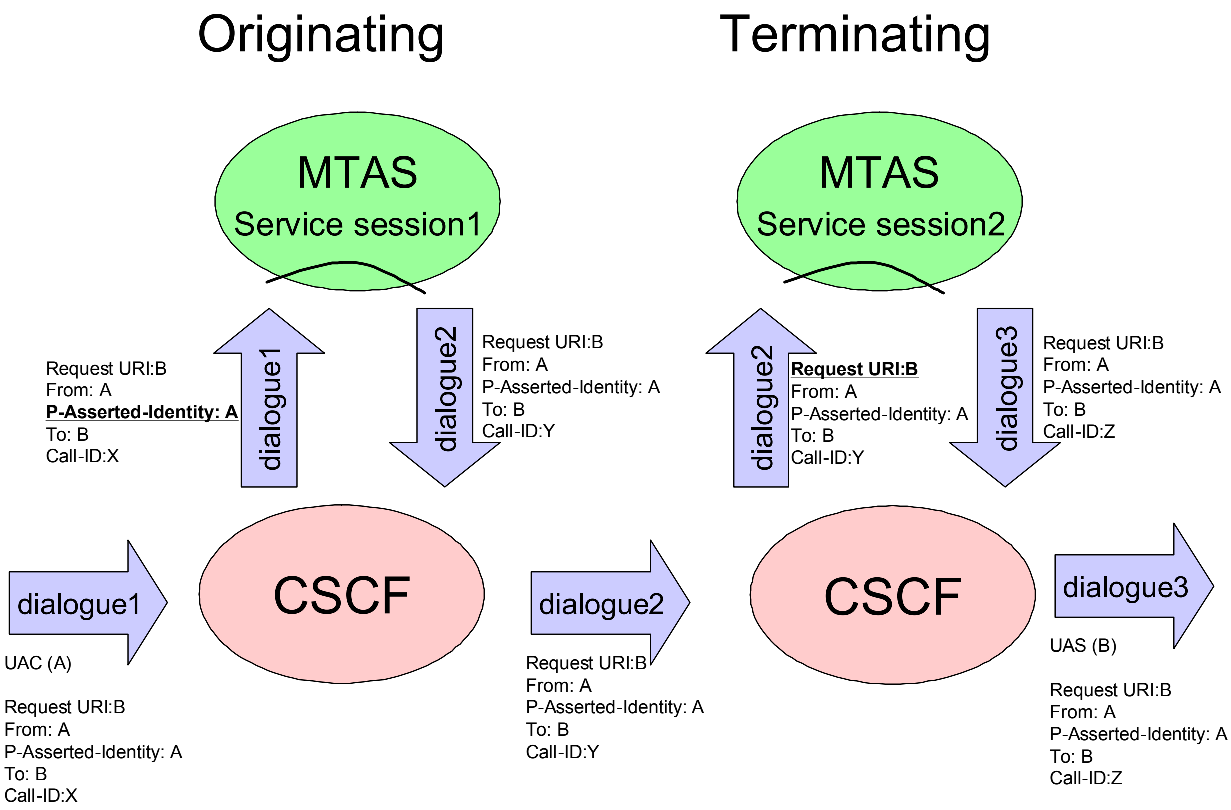


Figure 2: CSCF and MTAS inter working

In Figure 2, subscriber A, the user agent client (UAC), creates SIP dialog, dialog1 by sending an INVITE to the CSCF, which passes the INVITE on to an originating MMTel AS node, based on trigger received from HSS.CSCF indicates the session case (in this case originating registered) either with routing the INVITE to the originating port of MMTel AS (the ports are part of the trigger data in HSS), or by setting the *sescase* and *regstate* parameters of the P-Served-User header. This is how MMTel AS differentiates between an originating and terminating invocation.

The originating MMTel AS identifies the correct subscriber by looking at the P-Asserted-Identity (underlined in the figure above) or the P-Served-User in the INVITE message and exercises any originating services. A new SIP dialog, dialog 2, is created in order to forward the INVITE to the UAS. Internally in MMTel AS, dialog1 and dialog2 are bridged by the concept of a service session, session1. Since a second SIP dialog is created, the MMTel AS node works as a back-to-back user agent (B2BUA). Note that the INVITE on dialog2 is always sent back to the same CSCF where the INVITE came from.

On the terminating side the CSCF acts upon the terminating trigger and invokes a terminating MMTel AS node either using the port for terminating invocations or by setting the sescase and regstate parameters of the P-Served-User header. The terminating MMTel AS is controlling subscriber B, the user agent server (UAS), hence uses the request URI (underlined) or the P-Served-User to identify the correct subscriber in the node. This MMTel AS node also works as a B2BUA, creating dialog3 bridged by a new service session, session2. The INVITE sent on dialog3 finally ends up at subscriber B.

MMTel AS implements an asynchronous service framework API towards the MMTel services. MMTel AS also manages interaction between services. Service interaction is required when multiple services are executed simultaneously within one service session, and expected behavior of one or some of the services need to be differentiated from original behavior due to the combination of service. See section 4 for more details of MMTel services and interaction between them.

2.4 Interfaces and Protocols

MTAS is placed in the Signaling and Control domain, hence treated as a trusted server.

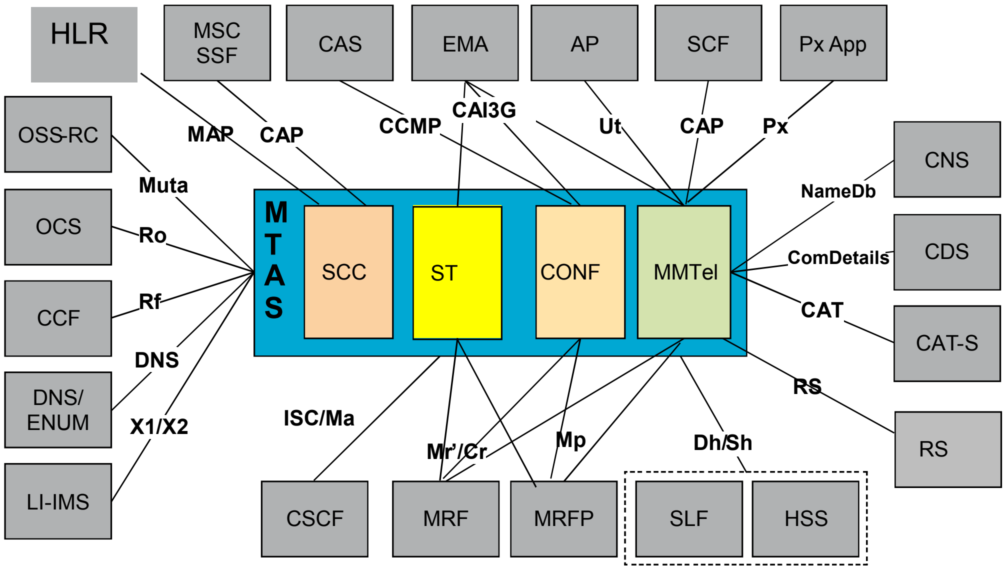


Figure 3 - Interfaces and Protocols supported by MTAS

MTAS has the following interfaces

1 **ISC – SIP over UDP/TCP**
S-CSCF executes originating, originating unregistered, terminating and terminating unregistered triggers for subscribers in order to route calls to MTAS.

2 **Ma – SIP over UDP/TCP**
Ma is the reference point between MTAS and I-CSCF. MTAS receives requests towards Public Service Identities (PSI) on the Ma interface in the conference service. MTAS also send SIP requests on the Ma

interface in case of call out of the blue (for example in Conference, Flexible Communication Distribution, Third Party Call, IMS Centralize Services). From an MTAS perspective the Ma interface is functionally equivalent to the ISC interface.

3 **Mp – H.248 over SCTP**
When the Mp interface is used MTAS takes the role of the MRFC function.

4 **Mr/Mr' – SIP over UDP/TCP**
Mr and Mr' is the interface between MTAS and MRFC. Mr means routing via CSCF while Mr' is a direct interface to MRFC.

5 **Cr – VoiceXML over HTTP**
This interface is used together with Mr/Mr'. It is used by MRFC for adding policies and instructions to media related services. VoiceXML scripts are fetched by MRFC from MTAS that acts as a policy server.

6 **Ro/Rf – Diameter over TCP**
MTAS communicates with charging servers using the Ro interface for online charging and the Rf interface for offline charging. MTAS does not generate CDRs itself. It provides charging information to online charging servers (OCS) in Credit-Control-Requests (CCR) messages and to offline charging servers/charging control function (CCF) in Accounting-Requests (ACR) messages. The charging servers then generate Charging Data Records (CDRs) using the charging information provided by MTAS.

7 **ComDetails – Diameter over TCP**
MTAS communicates with Communication Details Servers to transfer communication details for malicious communication identification purposes and for supplementary services that allow the user to request actions that are based on earlier calls. The ComDetails interface is a proprietary interface which is based on the Rf interface.

8 **Dh – Diameter**
In a network with multiple HSS network elements SLF holds which HSS each subscriber is provisioned in.

9 **Sh - Diameter**
HSS holds the subscriber Implicit Registration Set, subscriber data and service profile data used by the MMTel supplementary services.

10 **Muta – LDAP, SNMP, HTTP and SFTP**
MTAS node level configuration is performed using NETCONF, DNM data is configured using LDAP, alarms are sent over SNMP and backup is performed via SFTP.

11 **Ut – XCAP over HTTP**
The subscriber can read and update his/her service settings over the Ut interface.

12 **CAI3G – SOAP over HTTP**
The operator can provision end user service data, PBX referral and PBX service dataover the CAI3G interface

13 **NameDb – SOAP over HTTP or SIP**
A Calling Name Server (CNS) holds the mappings between global number identifiers and textual names. MMTel AS can fetch names either over SOAP or SIP.

14 **Px – Parlay X over HTTP**
A Parlay-X application can send and receive Parlay-X requests. This makes it possible to initiate and influence calls (ref [10]).

15 **DNS**
MTAS communicates with an ENUM/DNS server to perform the DNS lookup. The Number Portability (NP) lookup is one of the use cases.

16 **CAT – SIP over UDP/TCP**
This interface is used by the MTAS to trigger generation of customized alerting tone (e.g. selected music or welcome announcement) from the Customized Alerting Tone server (CAT-S) towards the caller when the served user is alerted.

17 **CAP (MMTel) – CAP over SIGTRAN**
CAMEL services executing in the SCP can control and influence MMTel calls over this CAP interface.

18 **CAP (SCC) – CAP over SIGTRAN**
SCC AS provides with the gsmSCF a CAMEL entity to MSC/GMSC for IMS Service Domain Selection.

19 **X1/X2**
This is the interface between MTAS and the legal intercept system.

20 **RS - SIP over UDP/TCP**
The RS (Redirect Server) is used to enable Location based routing of communication requests. The MMTel AS communicates with the Redirect Server over the RS interface using the SIP protocol.

21 **MAP (SCC) – MAP over SIGTRAN**
SCC AS provides an ETSI MAP interface to HLR for IMS Terminating Access Domain Selection.

MTAS supports both IPv4 and IPv6 on all interfaces.

3 Architecture

MTAS is implemented according to the Component Based Architecture (CBA), see Figure 4 .

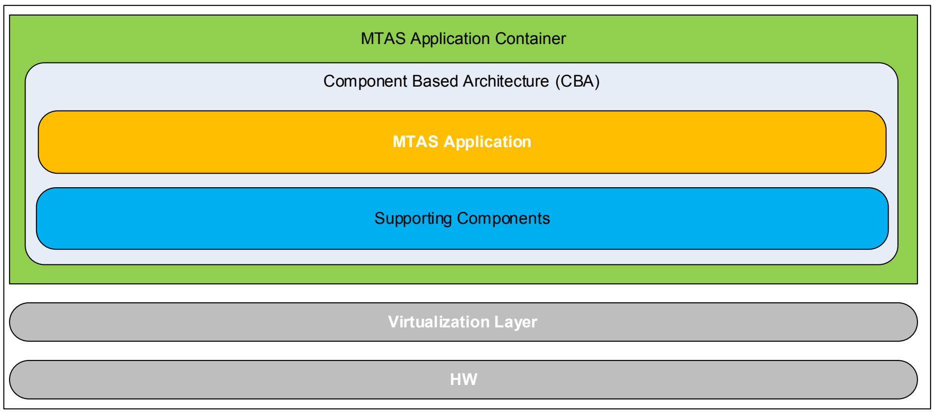


Figure 4 MTAS Application Container Architecture

The MTAS application container includes the MTAS application software and components needed for executing the MTAS application. The MTAS application container executes on a virtualization layer which hides the used physical hardware platform from the application. This enables portability to different hardware platforms which reduces the number of platforms in the operator network.

Figure 5 illustrates the functional architecture of the MTAS application. Subsequent sub-chapters explain each functional component.

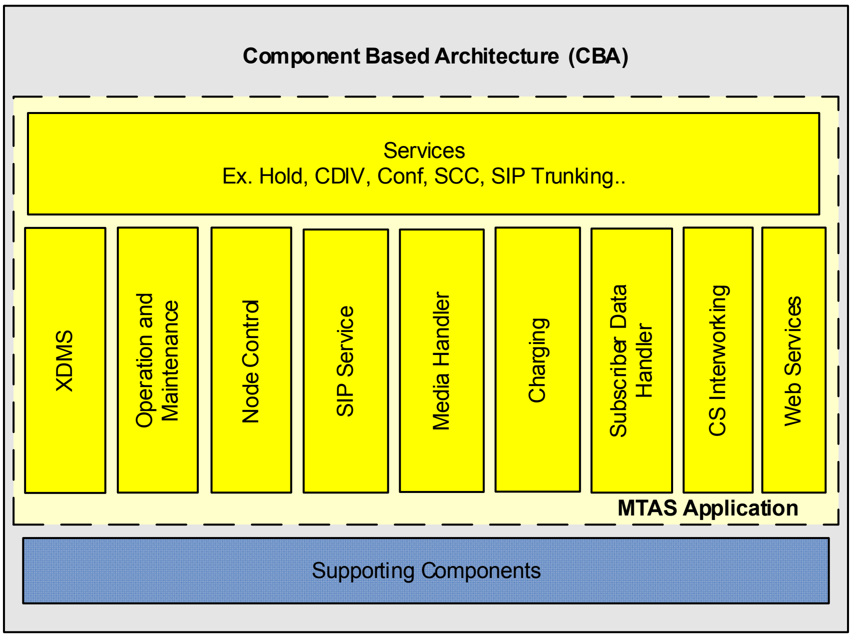


Figure 5 Ericsson MTAS Functional Architecture

The Component Based Architecture is further described in chapter 3.7.

3.1 Services

All services logic of MTAS is abstracted from the supporting functions like subscriber data handling, media handling and charging. Each service, like for example Communication Hold, Communication Diversion, Conferencing, Single Radio Voice Call Continuity and SIP Trunking, is implemented in a separate functional component. The service invocation layer handles in which order each service is invoked.

3.2 XDMS

The XDMS in MTAS provides the MMTel XDMS functionality for the end user's self administration of the MMTel services, the service provisioning possibilities per end user for the operator and service provisioning possibilities per PBX for the operator.

The service data for end user, conference and PBX are validated by MTAS but persistently stored in HSS via the Sh interface.

The end user, the operator, the CAS and PBX has different access points and access rights to the data.

3.2.1 End user self administration

The end user can do self administration of its MMTel services via an XCAP terminal or a Web Portal connected to the Ut interface. Ut is based on the XCAP protocol. This interface allows an end user to read and update his/her service data in the form of an XML document.

XCAP is based on HTTP, using the GET, PUT and DELETE methods. XCAP defines how the URI is encoded to refer to specific elements within documents.

XML schemas are used to define the valid contents of the subscription data document. Detailed conflict reports are returned in the case that errors are detected.

3.2.2 Operator provisioning

To support provisioning of the MMTel services per end user and ST Core and supplementary services for PBX, the XDMS also has a CAI3G interface for the operator. Provisioning is done via Ericsson Multi Activation (EMA) or other business support system. Through the provisioning interface the operator typically enable or disable a specific service for the end user, settings which are read-only for the end user through the Ut interface or a specific service for the PBX.

3.3 Subscriber Data Handler

The main purpose of subscriber data handling in MTAS is to fetch the subscription data relevant for MTAS's services from the HSS and cache it so that it is available when needed by the services.

MTAS may fetch the following subscriber data from HSS:

Transparent data

- MMTel service data
- Service number data
- SIP Trunking data, containing the main PBX identity
- SIP Trunking Service data, containing the service data for a PBX

Non-transparent data

- Implicit Registration Set (IRS) holding all Public User Identities of the subscriber associated with the same MMTel service data.
- MSISDN
- Location data of mobile subscribers
- S-CSCF identity of served user

MTAS may get the following contact data from S-CSCF via SIP extended 3rd party registration or by means of SIP Event Package for Registrations (ref.[22]):

- Contact address and instance
- IMPI
- Access domain (CS/PS) and UE type (Mobile/Fixed)

Subscriber data is fetched from HSS over the Diameter based Sh interface. In network configurations where more than one HSS is deployed, MTAS access SLF first in order to determine which HSS hosts a particular subscriber, and then redirects the Diameter message to the HSS.

IFC (Initial Filter Criteria) stored in the HSS for the subscriber instructs the S-CSCF to send 3rd party SIP REGISTER to MTAS nodes (MMTel AS and SCC AS).

MTAS supports the Sh interface efficiency feature that enhances the Sh interface with a more effective communication by allowing multiple Service Indications in the messages. For instance if a request message contains multiple Service Indications that are associated with a Public User Identity, the HSS will combine the data into a single answer message. Similarly if the Data Reference type is Repository Data, the MTAS will include several Repository Data instances in an update request message. This feature requires support in both HSS and MTAS.

3.4 Media Handler

MTAS is a pure signaling node; hence it does not handle the media streams. When interaction between sessions handled by MTAS and media handled by the Media Resource Function Control Processor (MRFP) is needed it is done over Mp, Mr or Mr'. Media handling operations are invoked by request from MTAS services e.g. Network Announcement or Conference as an example.

Depending on MTAS configuration, either Mr, Mr' or Mp can be used as external interface to control either an external Media Resource Function Control (MRFC) or Media Resource Function Control Processor (MRFP).

The Mr and Mr' interfaces are SIP based interfaces to control an external MRFC in accordance with 3GPP specifications (ref [17] and [18]), using protocol NetAnn described in RFC 4240 (ref [19]). The only difference between Mr and Mr' is whether MRFC requests are sent via CSCF or not.

The Mp interface is H.248 based and in accordance the 3GPP standard Mp interface (ref [12]).

MTAS allows the operator to provision repeat, duration, delay and play parameters for each announcement.

3.4.1 Distributed MRF feature

MTAS can have several MRFC and MRFP nodes configured. For each call session, when the first media resource is allocated MTAS selects one MRFC (if external) or MRFP based on the location of the served user. The feature is available on both originating and terminating sides and it covers all call scenarios (basic call, recall, redirect, conference, etc.) and all media resources (announcement, user input, conference, etc.) allocated and controlled over the Mr, Mr', or Mp interfaces. When the internal MRFC is used an MRFP node is selected, otherwise MTAS selects an external MRFC node.

The MRF nodes are organized into MRF sites. For redundancy, an MRF site can have multiple nodes configured. The same node can be shared between different sites. MTAS selects an MRF node from the site which is geographically closest to the served user. The user location is identified by means of P-Access-Network-Info (PANI) header received in a SIP message at call setup which is either a request (INVITE) or a response (200 OK) depending on operational side (originating or terminating). When choosing an MRF site is not possible because there was no PANI or the received PANI doesn't match any site then MTAS uses the default site.

On Mp interface the operational state of the MRFP nodes is monitored and thus MTAS will select or not a node based on its operational state. On the Mr/Mr' interface the operational state of MRFC nodes is not monitored instead MTAS implements a DNS based failover mechanism. When an MRFC node fails to answer a replacement is found automatically based on the alternatives returned by the DNS.

A counter is used to monitor the number of total attempts to select an MRF site. Another counter is used to monitor the number of failed attempts to use an MRF node from a site. Further counters are available to monitor the use of individual MRFC or MRFP nodes.

When the Distributed MRF feature is not configured or locked, MTAS selects an MRF node from all the available ones regardless of sites and user location.

3.5 Charging

Offline and online charging is supported by MTAS using Diameter over TCP. Offline charging is a mechanism where charging information does not affect, in real-time, the service rendered. The offline charging function collects detailed information about multimedia sessions within IMS. The information is collected for the purpose of billing, capacity and trend analysis, cost allocation and auditing.

Online charging is a mechanism where the charging process is performed as a prerequisite for rendering a service, and therefore requires in real-time a direct interaction with the service and the online charging system when requesting reservation of service units.

The charging component communicate over the Rf interface (offline charging) and Ro interface (online charging) to the charging server. It collects data from the SIP messages, and provisioning, and reports time and event based data to the charging server.

3.6 Operation and Maintenance

This functional component provides the means to set and read node global configuration data (CM), handling alarms (FM), output statistical data (PM), control licenses (LM) and provide logging. The actual CM, FM and PM data that can be configured and/or generated is briefly described in the description of each application service itself Operation and maintenance is also further described in chapter 6.

3.7 Component Based Architecture (CBA)

MTAS is implemented according to the Ericsson's Component Based Architecture (CBA) consisting of OS, Middleware, OAM and application execution environments.

The MTAS application container includes functionality from CBA components providing an execution environment for the MTAS Application. The included components provide also O&M functionality to manage the MTAS application.

3.8 Network scaling and geographical redundancy

3.8.1 Dynamic allocation concept

To achieve scaling above one MTAS network element and geographical redundancy MTAS supports the dynamic allocation concept, also called resource pooling.

In the following example, DNS is configured to return the IP address of primary and secondary MTAS nodes based on the S-CSCF IP address. This can be achieved, for example, with Split DNS. S-CSCF normally sends requests to the primary node, but fail-over to the secondary when it determines that the primary is down.

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

The subscriber data is then fetched from HSS and cached as long as the subscriber remains registered.

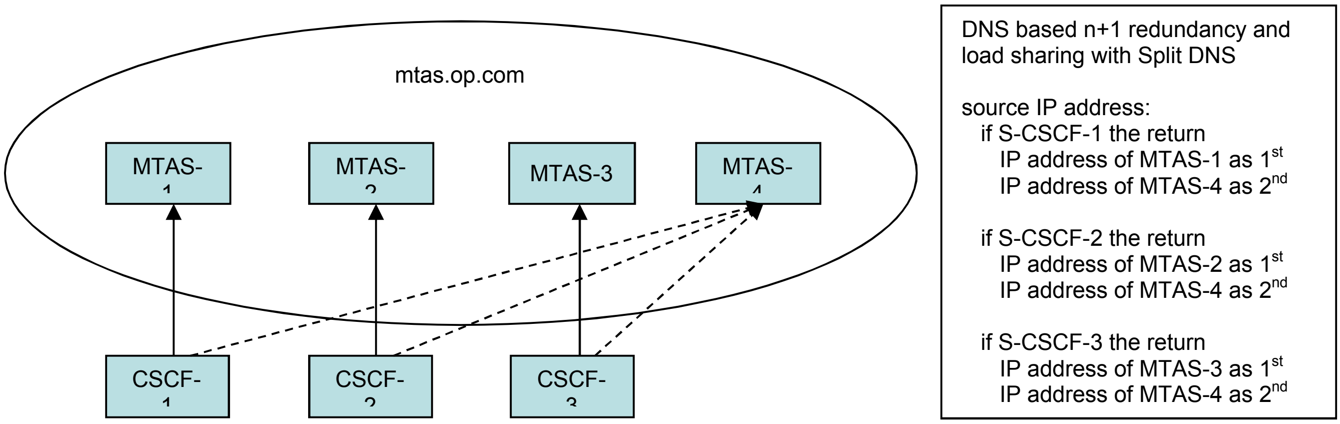


Figure 6 – An Example of redundancy configuration using Dynamic Allocation concept

MTAS handles all identities grouped in an Implicit Registration Set (IRS) as belonging to the same profile. MTAS only caches one set of transparent data (subscriber service data) per IRS.

When the terminating user is unregistered, or no third-party registration was received before session initiation, MTAS is allocated upon reception of INVITE message and then IRS and transparent data are fetched and cached until deregistration timer expires.

3.8.1.1 Example Call Flows

3.8.1.1.1 Main Scenario

Following diagram shows the example call flow of dynamic allocation in association with successful initial registration.

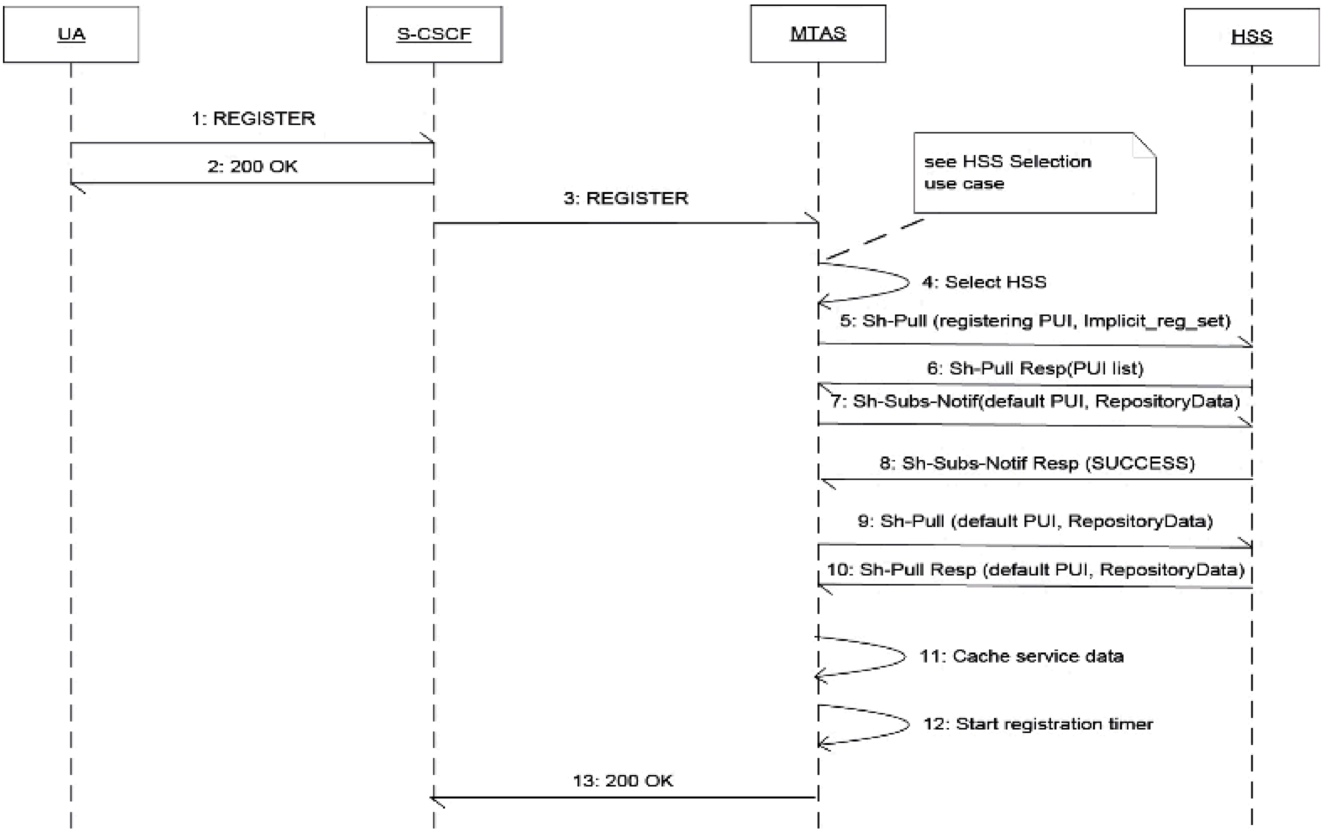


Figure 7 - Dynamic allocation of MTAS in association with successful registration

1. The User Agent (UA) registers in the IMS network. The S-CSCF receives the REGISTER message and processes the registration request. The details of message exchange between the P- and I-CSCFs are not shown on the diagram.

2. The S-CSCF accepts the REGISTER and sends a 200 OK response.

3. The S-CSCF sends a third-party REGISTER to the MTAS for one of the PUIs in the implicit registration set.

4. The MTAS interrogates SLF to determine which HSS to use for that PUI.

5. The Sh-Pull Request is sent to the HSS to retrieve the PUIs of the IRS.

6. The HSS replies with a successful Sh-Pull response. The response contains the PUIs of the IRS and the first PUI is the default PUI.

7. The MTAS sends a Sh-Subs-Notif to the HSS to subscribe to notifications of changes to the service data.

8. The HSS replies with a successful Sh-Subs-Notif response.

9. The Sh-Pull Request is sent to the HSS to retrieve the service data.

10. The HSS replies with a successful Sh-Pull response. The response contains the service data encoded in XML.

11. The MTAS caches a record of the service data in the DBN database.

12. The MTAS starts a registration timer using the value in the Expires header.

13. The MTAS accepts the registration and sends a 200 OK.

3.8.1.1.2 Alternative Case - Allocation based on INVITE

This scenario occurs when the MTAS has not received the initial registration for a PUI belonging to a registered subscriber prior to receiving an INVITE. This could happen as a consequence of the fail-over situation from primary to secondary MTAS based on the dynamic allocation scheme.

Please note that steps 3 to 11 in the following call flow are identical to the steps 4 to 12 in Figure 7.

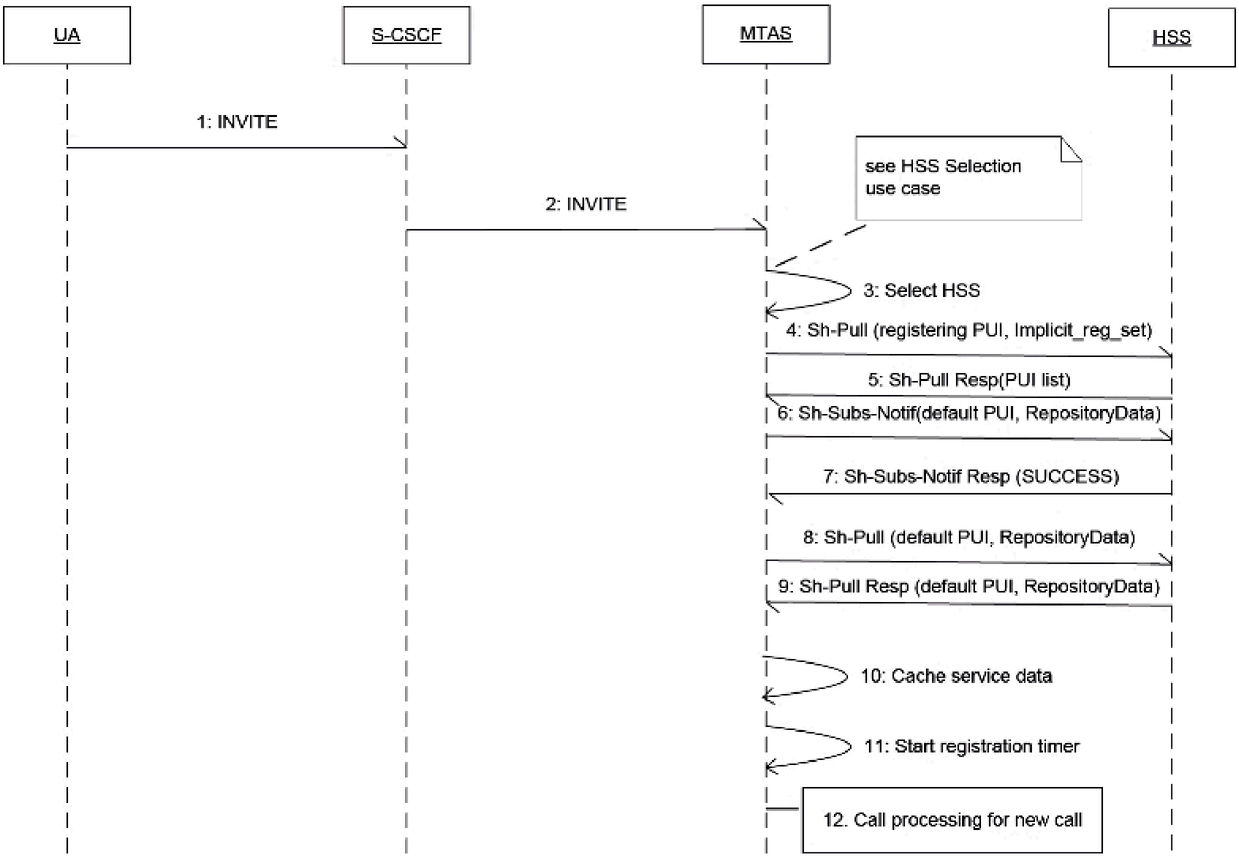


Figure 8 - Alternative case: dynamic allocation based on INVITE

3.8.2 DNS based redundancy of external server nodes

At a DNS SRV and/or A/AAA lookup the DNS may respond with two IP addresses. MTAS use these addresses to support geographical redundancy of external server nodes. In case MTAS encounter a transport failure or timeout when trying to send a request to an external server, MTAS will try the other IP address received from the DNS.

MTAS support DNS based redundancy on the following HTTP based interfaces:

- NameDb to Calling Name Server
- Px to Parlay-X application

MTAS support DNS based redundancy on the following SIP based interfaces:

- Ma to I-CSCF
- Mr’ to MRFC
- CAT to CAT-S

3.8.3 HSS load reduction

To reduce the network load at initial registrations MTAS support a feature called HSS load reduction.

Normally, MTAS fetches and caches all of the needed subscriber data from HSS when initial registration is performed by the subscriber. This can cause high load both on MTAS and on HSS when huge number of registrations is performed at the same time, like in some network disturbance cases. When HSS load reduction is enabled then fetching and caching of subscriber data is delayed until the first call attempt of the subscriber. As call attempts are usually more evenly distributed in time, this feature can help to distribute these high load periods more evenly.

HSS load reduction also supports a mode, where subscriber data fetching is only delayed when HSS overload condition is detected.

4 Provisioning

The operator can use MTAS for provisioning a subscriber with communication services via EMA (Ericsson Multi Activation) using the CAI3G interface. The data is stored in the HSS or in case of a layered architecture, in the backend database.

4.1 General operation

CAI3G is a synchronous, request/response-based provisioning interface. The interface is defined in XML and uses SOAP to format the interface into messages. SOAP messages are carried by HTTP methods. MTAS provides both secured (SSL/TLS) and unsecured CAI3G interface.

The Sh interface is used to access storage on the HSS. The MTAS subscription data is stored as ‘transparent data’ on the HSS. This means that the HSS is unaware of the structure of the data except that it must be well-formed XML.

Following is the successful creation of an MMTel document in HSS

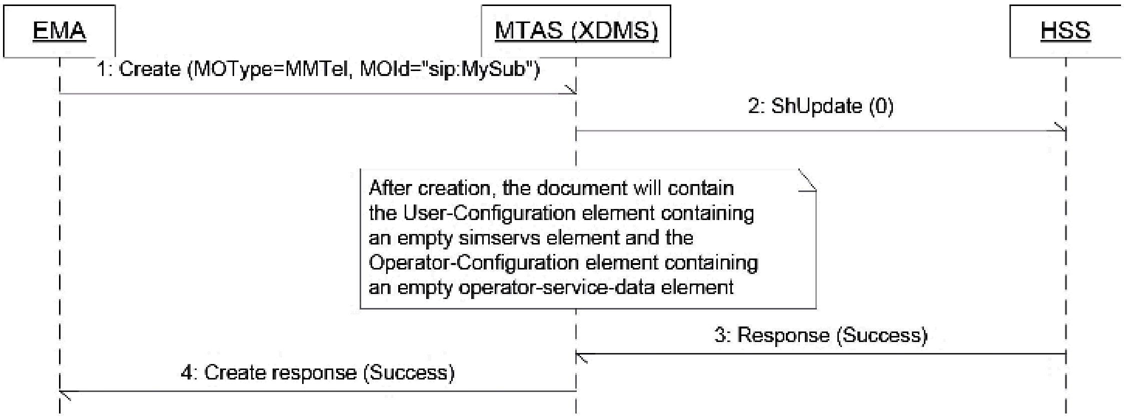


Figure 9 - Create a document, successful case

1. EMA sends a CAI3G Create Request to MTAS. The request defines the Managed Object Type to be created (MMTel) and the instance which identifies the type which is the public Id.
2. MTAS (XDMS) sends an Sh Update request to HSS with a sequence number of 0 which indicates it is a new document.
3. HSS responds with Success
4. MTAS (XDMS) sends a CAI3G Create response to EMA indicating success.

CAI3G interface can also be used to validate service data without provisioning.

4.2 Extended operation

Since the CAI3G interface is generic and defined in high level it is also suitable to perform provisioning with different service data models not just the one specified by Ericsson. Service elements/attributes of the different service data model should be aligned with Ericsson data model as much as possible in order that MTAS can understand data of the different model. Service elements/attributes that cannot be aligned with Ericsson data model can be mapped to so-called integration elements including key/value pairs. The integration elements are handled in transparent way in MTAS. That is, they are stored in the HSS but they are not understood by MTAS services. Similarly to the CAI3G interface the service data model used on the Sh interface is also extendable because MTAS can handle transparent information (present in the model but not understood by MTAS). In addition MTAS can also encode/decode different service data format than the one specified by Ericsson. The encoding/decoding rules are data model specific and need to be agreed with Ericsson.

5 Charging

5.1 Offline Charging

5.1.1 Description

The MTAS Offline Charging Function interacts with the services executing on the MTAS node and with the Charging Data Function (CDF).

The Offline Charging Function uses the Diameter Accounting Application (reference point Rf, see [13]) when interacting with the CDF. Session based charging, with timestamps reported to the nearest second, is used for charging successfully established communication sessions. One time event charging is used for reporting of:

- Unsuccessful attempts to establish communication sessions.
- Successful configuration of Supplementary Services with SSC commands or over Ut interface

A successfully established communication session, e.g. an MMTel session, is reported in a Diameter accounting session where accounting requests (ACRs) are sent from MTAS to the CDF when the media session is established, updated and terminated. Media update after session establishment is reported or not depending on configuration data.

The Offline Charging Function is responsible for reporting details of services used within MMTel sessions including information that is required to rate the service usage, e.g. called party address, start time of the session etc. The usage in this context is:

- The session duration.
- The media streams used in the session.

The charging cases supported are session based charging and one time event charging (see [13]).

5.1.2 Session Based Charging

Session based charging is used for the charging of successfully established MMTel and ST AS sessions. A charging session between MTAS and the CDF is started when the establishment of an MMTel or ST AS session has successfully completed and is stopped when the MMTel session is terminated. During the charging session, MTAS generates interim charging messages whenever media changes are performed. MTAS may also generate interim charging messages during the charging session at time intervals specified by the CDF in charging responses.

The Diameter accounting request messages ACR[start], ACR [interim] and ACR[stop] are used for sending charging information to the CDF for session based charging. A Diameter accounting answer message (ACA) is returned by the CDF in response to each ACR.

An ACR message consists of a number of AVPs, holding the usage and rating information.

The Offline Charging Function uses the following sub-functions when performing session based charging:

- Capture Charging Information
- Start Charging Session
- Send Timer Triggered Interim
- Send Media Triggered Interim
- Terminate Charging Session

Capture Charging Information:
Information required for populating charging messages is copied from SIP messages throughout the MMTel/ST AS session and retained until the charging messages are actually generated.

Start Charging Session:
A charging session is triggered when the MMTel/ST AS session establishment is complete. An ACR[start] is sent to the CDF including SDP information describing the properties of the media session. An interim timer is started on receipt of the ACA response from the CDF (if a timer value is included in the ACA).

Send Timer Triggered Interim:
When the interim timer expires, a time-based ACR[interim] is generated. The time-based ACR[interim] does not include any SDP information, since the media has not been changed. An interim timer is started on receipt of the ACA response from the CDF (if a timer value is included in the ACA).

Send Media Triggered Interim:
When the media is changed, requested by either the calling or called user, an ACR[interim] may depending on configuration data be generated containing SDP information describing the new properties of the updated media session. An interim timer is started on receipt of the ACA response from the CDF (if a timer value is included in the ACA).

Terminate Charging:
When the MMTel/ST AS session is terminated, an ACR[stop] is generated. No action is taken on receipt of the ACA response.

Figure 10 shows a charging session between MTAS and a CDF at a conceptual level.

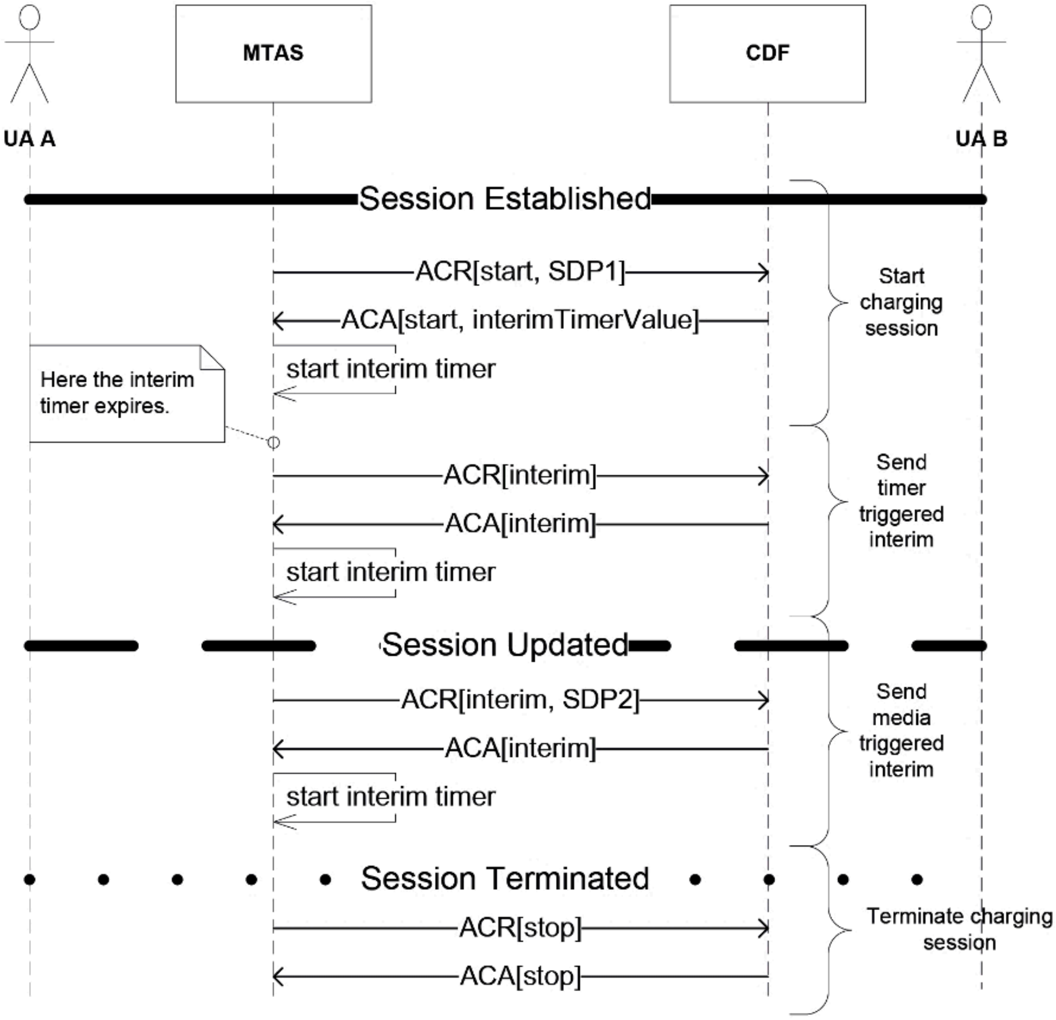


Figure 10 A charging session between MTAS and a CDF at a conceptual level.

5.1.3 One Time Event Charging

One time event charging is used for the charging of unsuccessful attempts to establish MMTel or ST AS sessions and for reporting the configuration of supplementary services.

The Diameter accounting request message ACR[event] is used for sending charging information to the CDF for one time event charging. A Diameter accounting answer message (ACA) is returned by the CDF in response to each ACR.

An ACR message consists of a number of AVPs, holding the usage and rating parameters.

The Offline Charging Function uses the following sub-functions when performing one time event charging:

- Capture Charging Information
- Send Unsuccessful MMTel/ST AS Session Establishment Event

- Send Event on successful configuration of Supplementary Services (SSC or Ut)

Capture Charging Information:
Information required for populating charging messages is copied from SIP messages throughout the MMTel/ST AS session establishment and retained until the charging message is actually generated.

Send Unsuccessful MMTel/ST AS Session Establishment Event:
An unsuccessful MMTel/ST AS session establishment event is triggered when the failure of an MMTel session that is being established is detected. An ACR[event] containing the cause of the failure is sent to the CDF.

Send Supplementary Service Event:
A supplementary service event is triggered in the following cases:

1. The configuration of a supplementary service is updated by the user (e.g. activate Communication Forwarding on Busy).

2. The status of a supplementary service is interrogated by the user.

5.1.4 Service Interaction

See chapter Ref [24] for the interaction with CDIV and CONF.

5.1.5 Configuration

MTAS provides the operator the following node-level configuration options which are configurable via LDAP:

- Configure behavior for originating and terminating charging (on/off, service format dependencies et c)
- Configure maintenance back-up and default charging destinations.
- Configure behavior of event based charging (for SSC, Ut, etc.)

5.1.6 Performance Management

A number of offline charging-related counters are provided and can be used to calculate the accessibility and retainability of the Diameter-based interface. The counters provide information about the exchange of information between the MTAS and the CDF(s). The following counters are provided as examples:

- Number of successfully initiated accounting sessions, session based or event based
- Number of failed initiations of charging sessions due to internal errors
- Number of failed initiations of charging sessions due to external errors
- Number of accounting answers with result code 3xxx

5.1.7 Fault Handling

When MTAS is unable to deliver charging data to a CDF it may attempt to communicate with an alternative CDF (i.e. failover). If failover is not possible MTAS will, dependent on configuration data, either buffer the charging messages for later delivery when communication with the CDF is possible (i.e. back-up) or store the messages in files for later retrieval by the use of sFTP.

These fault handling methods are described in detail below:

5.1.7.1 Failover

Should the primary CDF be unavailable (due to Diameter link failure or e.g. if the CDF is temporarily out of order), offline messages will be sent to the secondary CDF. The addresses for the primary and the secondary CDF are configured per subscriber in the HSS.

5.1.7.2 Backup handling for later delivery

Should both the primary and the secondary CDF be unavailable, offline messages may be buffered locally in the MTAS node. The buffered messages are sent to the CDF at a later time when the CDF is available again. The resending of messages is done at a slow rate so that MTAS will not overload the CDF. There is an alarm when CDF is unavailable and buffered event counter reaches above Arm Threshold value. This alarm is cleared once resending of messages starts and buffered event counter reaches below DisArm Threshold value.

5.1.7.3 Storage of offline messages in files on disk for later retrieval

As an alternative to the Backup handling for later delivery as described above, the messages may be stored in files on disk for later retrieval via sFTP.

5.2 Online Charging

5.2.1 Description

The Online Charging function consists of two sub-functions:

- Charge Service Online: handles the real-time interaction with the charging server to perform online charging for the services requested by the served user.

- Manage Online Charging: configures online charging.

The Online Charging function within MTAS provides online session charging for the multimedia telephony sessions used to control the media components associated with the multimedia telephony communication service. The message sequences in the following sections focus on the online charging aspects and do not attempt to show complete sessions/dialogs. Please refer to relevant documentation of functions and services that uses the Online Charging function to get a better picture of the complete sequences.

The Online Charging Function consists of Session based Charging with Unit Reservations (SCUR) and Immediate Event Charging (IEC).

The basic principles applicable to MTAS session based online charging are:

- Charging is performed for the overall MMTel communication session.
- The charging server is responsible for rating the requested communication service based on service information provided by MTAS, including SDP information describing the media session and components.
- The Online Charging Function establishes a charging session with a charging server in order to perform real time charging. A charging session is only established if there is a valid unexpired Online Charging License available on the MTAS node.
- The Online Charging Function initiates a charging session by sending a Diameter Credit Control Request (CCR) message, indicating ‘Initial Request’, to the charging server.
- During a SIP session establishment, credit reservation is performed based on the media components identified from the INVITE.
- If a SIP session is cancelled before the establishment is complete, the charging server is informed so that the reserved credit can be refunded to the user’s account.
- During an established SIP session, credit reservation may, depending on if trigger condition has been set for the media change event or if trigger condition has not been set depending on configuration data, be revised on receipt of a 200 OK response to an UPDATE and on receipt of a 200 OK response to a Re-INVITE containing an SDP answer.
- When the service units associated with the reserved credit have been consumed, the charging server is informed and further credit reservation is requested.
- The charging server can specify a ‘Time Quota Threshold’ (TQT) when granting service units. This threshold indicates the time, in seconds, before the granted service units have been consumed, that the Online Charging Function should initiate a new credit reservation request.
- The charging server can specify a validity time when granting service units. The validity time specifies the length of time for which the granted service units are valid, measured from the time that the CCA message is received.
- When a request is received to terminate a SIP session (e.g. receipt of a BYE message), the charging server is informed of the number of used service units, so that the user’s account can be updated accordingly.

Online Immediate Event Charging (IEC) is used for notifying the OCS of:

- Communication sessions that are rejected before any unit reservation is performed.
- Supplementary service configuration actions requested using SSC codes.
- Supplementary service configuration actions requested via the Ut interface.

5.2.2 Example Call Flow

Figure 11 illustrates the establishment of a SIP session with online charging where the SDP offer is conveyed in the INVITE message and the SDP answer is returned in the 200 OK INVITE response.

The Online Charging Function behaves in a similar manner when the SDP answer is conveyed in a 1xx-rel INVITE response instead of in the 200 OK INVITE response. In these cases the CCR (Update Request) message is still sent on receipt of the 200 OK INVITE response but the content of the message is based on the latest negotiated SDP (as there may not be an SDP in the 200 OK). The latest negotiated SDP is either (a) the SDP answer conveyed in a 1xx-rel INVITE response, or (b) the SDP from the latest 2xx UPDATE Response (where an UPDATE has occurred).

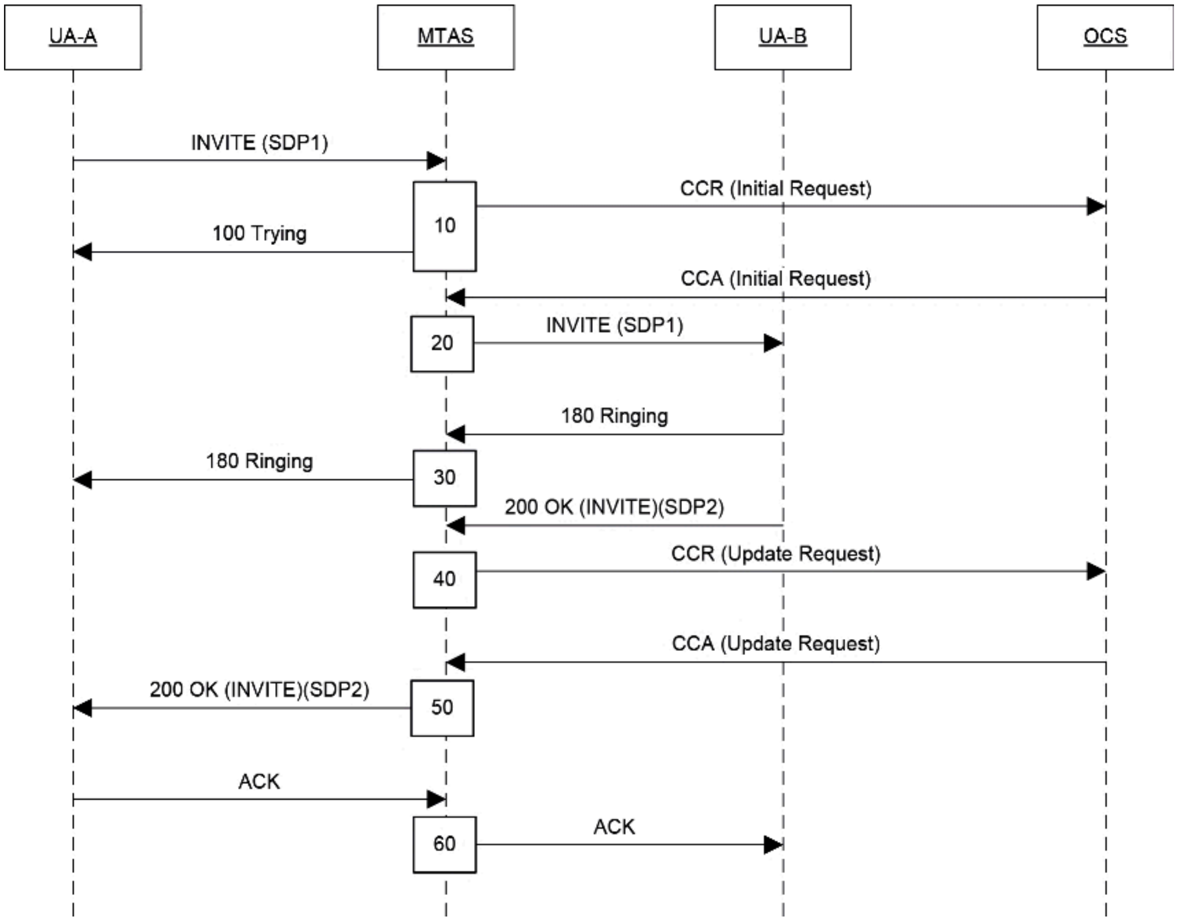


Figure 11 – Session establishment with SDP offer in INVITE and answer in 200 OK.

5.2.3 Offline and Online interaction

The Online Charging Function and the Offline Charging Function operate independently within MTAS.

Online charging is triggered when the following conditions are met:

- Online charging is enabled for the appropriate SIP session case at the Node level, and
- The service level configuration data for the appropriate SIP session case is configured for ‘Online charging’, ‘Online and offline charging’ or ‘Online charging precedence’, and
- A valid unexpired Online Charging License is available on the MTAS node and
- One or more ECF addresses are available.

Offline charging is triggered when the following conditions are met:

- Offline charging is enabled for the appropriate SIP session case at the Node level, and
- The service level configuration data for the appropriate SIP session case is configured for ‘Offline charging’ or ‘Online and offline charging’, and
- One or more CDF addresses are available.

or

- Offline charging is enabled for the appropriate SIP session case at the Node level, and
- The service level configuration data for the appropriate SIP session case is configured for ‘Online charging precedence’,
- One or more CDF addresses are available, and
- Online charging is not triggered.

or

- Offline charging is enabled for the appropriate SIP session case at the Node level, and
- The service level configuration data for the appropriate SIP session case is configured for ‘Online charging precedence’,
- One or more CDF addresses are available,
- Online Charging is triggered but MTAS fails to send a CCR (Initial Request).

For originating and terminating SIP communication sessions the ECF and CDF addresses are taken from the ECF and CCF parameters in the P-Charging-Function-Addresses header of the initial INVITE message. When the initial INVITE message does not contain any ECF or CDF addresses, the default CDF address (if available) is used instead.

For conference sessions, MTAS obtains the per-subscriber ECF and CDF addresses directly from the HSS using the Sh interface. When the subscriber data does not contain any ECF or CDF addresses, the default CDF address (if available) is used instead

5.2.4 Service Interaction

Generally the service identity is can be set to the online charging information per invoked service.

5.2.4.1 Communication Hold

No specific charges apply to the use of the HOLD service, however media changes resulting from the use of the service may affect the charging.

5.2.4.2 Communication Diversion

A communication request that is diverted or deflected by the Communication Diversion Service is treated as two separate MMTel sessions from a charging perspective.

See Ref [24] for more interaction with CDIV.

5.2.4.3 Conference

Conference ID is added to the online charging information. See Ref [24] for more interaction with CDIV and Ref **Error! Reference source not found.** for the interaction with CONF.

5.2.5 Configuration

MTAS provides the operator the following node-level configuration options which are configurable via LDAP:

- Configure behavior for originating and terminating charging (on/off, service format dependencies et c)
- Configure maintenance back-up and default charging destinations.
- Configure behavior of event based charging (for SSC, Ut et c)

5.2.6 Performance Management

A number of online charging-related counters are provided and can be used to calculate the accessibility and retainability of the Diameter-based interface. The counters provide information about the exchange of information between the MTAS and the CDF(s). The following counters are provided as examples:

- Number of successfully initiated accounting sessions, session based or event based
- Number of failed initiations of charging sessions due to internal errors
- Number of failed initiations of charging sessions due to external errors
- Number of accounting answers with result code 3xxx

5.2.7 Fault Handling

When MTAS is unable to deliver charging data to a CDF it may attempt to communicate with an alternative CDF (i.e. failover) or buffer the charging messages for later delivery when communication with the CDF is possible (i.e. back-up).

These fault handling methods are described in detail below:

- Failover:
  Should the primary CDF be unavailable (due to Diameter link failure or e.g. if the CDF is temporarily out of order), online messages will be sent to the secondary CDF. The addresses for the primary and the secondary CDF are configured per subscriber in the HSS.
- Backup handling:
  Should both the primary and the secondary CDF be unavailable, offline messages may be buffered locally in the MTAS node. The buffered messages are sent to the CDF at a later time when the CDF is available again. The resending of messages is done at a slow rate so that MTAS will not overload the CDF.

  MTAS also supports the restoration of the data after a process restart. A process restart can happen after process or board failure. All data will be lost in the case of a zone reload. When the online charging function is started after a process restart, the persistent data stored in the database is fetched and used to recreate the state as it were before the restart.

There is an alarm for absent online charging license.

5.3 Flexible AVP

Flexible charging AVP is a function that allows the operator to define SIP message header fields to be reported in AVPs of charging requests (ACR and CCR). If the configured SIP header field is found in the message, a flexible AVP called Transaction-Info AVP will be used to report the content of the matching SIP header.

The Flexible AVP function can be enabled or disabled per charging profile, and the SIP headers to report are also defined for each profile.

To be able to use the Flexible AVP function, a Flexible AVP Capacity License must be installed. The capacity of the license defines the maximum number of SIP headers that can be defined in each charging profile.

6 Operation and Maintenance

6.1 Load and memory Control

MTAS has a number of load and memory control functions.

6.1.1 Load Regulation

MTAS try to regulate the average virtual CPU (vCPU) load to 85% by rejecting requests, except for BYE, CANCEL, UPDATE and PRACK.

The rejection of messages shall be performed as cheaply as possible i.e. before SIP stack is initiated to save some processor power, otherwise the rejection of the message will contribute to system load.

H248 AUDIT requests will be queued up and run when the average load has dropped below 85%.

6.1.2 Overload Protection

MTAS handles transient overload situations when the scheduling queue length for a Virtual Machine (VM) grows above a system defined threshold.

6.1.3 Memory Regulation

MTAS regulates the memory utilization such that the RAM utilization level on a node as measured by the underlying OS (Linux) is limited to system defined value. The default value for the memory utilization level is set to 95%

6.2 Fault Management

Fault management provides functions for detection and isolation of improper behavior within MTAS. MTAS provides fault information based on international standards, including CCITT recommendation X.733, which defines an information model for all alarms including the alarm information structure and semantics and the transfer interface.

MTAS network element complies with ITU-T X.731 standard for state management.

MTAS sends all alarms to a network management system (NMS) over SNMP. Each MTAS alarm indicates the severity of the alarm and for each fault there is an operational procedure to assist in correcting the fault.

MTAS alarms can also be displayed to the operator in an active alarm list using the COM North Bound Interface (NBI).

Fault Management logs all events and alarms to files independent of any filters. These log files can also be viewed and accessed via the EM.

6.3 Performance Management

The task of Performance Management (PM) is to collect, store, present and report performance measurement result data.

The performance data generated by the active measurements are stored in eXtensible Markup Language (XML) files, compliant to the 3GPP Performance Management specification for XML output file format (TS32.104 v3.4.0 Appendix D), for parsing by external Performance Management tools.

6.4 Configuration Management

Configuration management is a set of management functions, which allow the operator to manage and control the application.

The COM component provides a machine-machine interface based on the IETF NETCONF standard, the Ericsson NETCONF interface, and a human-machine user interface, the Ericsson Command-Line Interface (ECLI).

Both interfaces are model-driven, which means that the configuration data of the Managed Element (ME) is represented as a set of Managed Objects (MOs). The complete set of MOs and their relationships are described in a Managed Object Model (MOM). The MOM is exposed through the Ericsson NETCONF interface and the ECLI, and provides a consistent view of the configuration and state data. This property implies essentially that what can be done over the ECLI can also be done over the Ericsson NETCONF interface and conversely.

Both interfaces provide commands to read state data and configuration data as well as adding, modifying, and deleting configuration data. The capability to read or modify the configuration data on the ME is governed by LDAP authentication.

6.5 Logging and Tracing

MTAS supports Network Tracing, this allows tracing of SIP transactions that traverse the MTAS depending on user defined filter criteria. These transactions are formatted and output in standardized XML file format according to the *Subscriber and equipment trace* 3GPP Specification [16].

It is possible to trace SIP transactions at two levels:

- At min Trace Level, the SIP transactions are represented by a number of XML elements. Not all SIP headers are represented when tracing at this level. SIP headers are output in plain text inside XML elements.

- At max Trace Level, the SIP transactions are encoded into hexadecimal format and output as raw data. The complete contents of each SIP request/response are output as raw data.

MTAS also provides support for:

- Logging of Error Reponses on external interfaces
- Signaling history and code execution logging that is reported in case of error
- Tracing per User ID, where an entire call can be traced as it propagates through MTAS
- Preconfigured Trace profiles available in deliveries, used by trace-user to initiate tracing for selected cases
- Logging on the CAI3G interface

Logging and tracing information can also be collected by using the data collection functionality in MTAS.

6.6 Automatic Health Check

Health check is a recommended set of procedures to be performed before and after a system update/upgrade, a normal backup, or during the periodic maintenance. Automatic health check is a function to ease this task by collecting, storing and presenting information and creating a health check log. Partial evaluation of the information is also performed; other parts require verification by the operator.

Automatic health check is used to check the health of the node and the function fetches information regarding configuration and current node status and generates a report. Examples of checks included:

- Installed software versions
- Running software versions
- MTAS operational state
- Alarms and notifications
- Memory usage on VMs
- Processor usage on VMs
- Restart and reload events
- Internal network connectivity
- External VIP addresses
- Status of SIP and Diameter ports

- LDAP connectivity
- SS7 connectivity
- System environmental variables

7 Characteristics

7.1 Availability

MTAS supports different level of redundancy in order to eliminate system downtime caused by unintentional disruptions in operations and limit system downtime for planned activities. The overall availability of MTAS for all node types is expected to be 99.999%.

- Logical node level redundancy: MTAS uses an 1+1 for SC VM redundancy and an N+1 PL VM redundancy. MTAS temporarily tolerates a loss of the SC domain, i.e. no impact on established sessions in this case.
- Virtual network infrastructure redundancy: the virtual network infrastructure should support OSPF, and optionally ECMP, which will improve the load distribution among the redundant interfaces.
- Solution level redundancy: failover between VMs is transparent for the client/end user who has established the session and the session survives. Not yet established sessions are lost at fail-over, and the client/end user needs to make a new session. No specific solution configuration aspects are needed to provide redundancy to the MTAS.
- Geographical redundancy: Geographical redundancy is a solution whereby Service Availability is ensured in a multi-site deployment. MMTel Geographical redundancy will protect against disaster scenarios where a whole site has failed, but also against individual nodes failures.
- MTAS SW upgrade: During software upgrade all sessions without ongoing signaling procedures, with or without used MRFP resources, are kept, together with the allocated MRFP resources, independent of whether there is any active signal on any MRFP resource. Sessions with ongoing signaling procedures are terminated, together with the allocated MRFP resources.

7.2 Scalability

MTAS has a user model where provisioning is independent of which node the user is allocated to. This gives a high and flexible scalability.

When capacity requirements increase, more VMs can be added to increase the total node capacity. The capacity increases linearly with the number of VMs added to the system. Scale-in and scale-out operations can be triggered manually by an operator or automatically by a VNF manager based on performance data provided by MTAS.

Scaling-in operations
One or more VM's can be removed.

- Ongoing calls – no impact
- Calls being established – some calls are lost
- Registrations – no impact
- Re-registrations – no impact

Scaling out operations
One or more VM's can be added. The VNF will extend itself to include the new VM's and fully utilize the added resources.

- Ongoing calls – no impact
- Calls being established – no impact
- Registrations – no impact
- Re-registrations – no impact

8 Acronyms and Abbreviations

3GPP	3rd Generation Partnership Project
ACR	Anonymous Communication Rejection
API	Application Programming Interface
AS	Application Server
BFD	Bidirectional Forwarding Detection
CA	Charge Area
CAI3G	Customer Administration Interface 3rd Generation
CAMEL	Customized Application for Mobile Enhanced Logic
CAP	CAMEL Application Protocol
CAS	Conference Administration Server
CAT	Customized Alerting Tones
CCMP	Centralized Conferencing Manipulation Protocol
CDF	Charging Data Function
CM	Configuration Management
CNS	Calling Name Server (NameDb)
CSCF	Call Session Control Function
ECMP	Equal-Cost Multi-Path routing
EMA	Ericsson Multi Activation
ENUM	E.164 NUmber Mapping
ETSI	European Telecommunication Standards Institute
FCH	Flexible Charging
GSM	Global System for Mobile Communications
gsmSCF	GSM Service Control Function
gsmSSF	GSM Service Switching Function
HLR	Home Location Register
HSS	Home Subscriber Server

I-CSCF	Interrogating CSCF
ICS	IMS Centralized Services
IEC	Immediate Event Charging
IETF	Internet Engineering Task Force
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IRS	Implicit Registration Set
ISC	IP multimedia Service Control
ISDN	Integrated Service Digital Network
ISUP	ISDN User Part
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
MAP	Mobile Application Part
MMTel	Multi-Media Telephony
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber Integrated Service Digital Network
MTAS	Multimedia Telephony Application Server
NBI	North Bound Interface
OSPF	Open Shortest Path First
PANI	P-Access-Network-Information
PSTN	Public Switched Telephony Network
RFC	Request for Comment
S-CSCF	Serving-CSCF
SCP	Service Control Point

SCUR	Session based Charging with Unit Reservations
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SCC	Service Centralization and Continuity
SDS	Service Domain Selection
SR-VCC	Single Radio Voice Call Continuity
SSC	Supplementary Service Code
SSF	Service Switching Function
TCP	Transport Control Protocol
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Network
UA	User Agent
UE	User Equipment
URI	Uniform Resource Identifier
vCPU	Virtual CPU
VM	Virtual Machine
VoLTE	Voice over LTE
XCAP	XML Configuration Access Protocol
XDMS	XML Data Management Server
XML	eXtensible Markup Language

9 Reference Documents

[1] MTAS 15A Feature Description, 221 04-FGC 101 2545

[2] 3GPP TS 22.173 - Multimedia Telephony Service and Supplementary Services; Stage 1

[3] 3GPP TS 24.173 - IMS Multimedia Telephony Service and Supplementary Services; Stage 3

[4] GSMA IR.92 – IMS Profile for Voice and SMS

[5] GSMA IR.94 – IMS Profile for Conversational Video Service

[6] ETSI GS NFV 002 - Network Functions Virtualisation (VNF); Architecural Framework

[7] 3GPP TS 24.147 - Conferencing using the IP Multimedia (IM) Core Network (CN) Subsystem

[8] 3GPP TS 24.292 – IP Multimedia (IM) Core Network (CN) subsystem Centralized Services (ICS); Stage 3

[9] 3GPP TS 24.237 - IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) Service Continuity; Stage 3

[10] Open Service Access, 3GPP TS 23.198, v8.0.0

[11] 3GPP TS 26.114 - Multimedia telephony; Media Handling and Interaction

[12] 3GPP TS 29.333 – MRFC-MRFP Mp Interface; Stage 3

[13] 3GPP TS 32.240 - Charging Management; Charging architecture and principles

[14] 3GPP TS 32.260 - Charging Management; IP Multimedia Subsystem (IMS) charging

[15] Open Service Access, 3GPP TS 23.198, v8.0.0

[16] 3GPP TS 32.423, 8.1.0 - Telecommunication management; Subscriber and equipment trace; Trace data definition and management

[17] 3GPP TS 23.218 - IP Multimedia (IM) session handling

[18] 3GPP TS 23.228 - IP Multimedia Subsystem (IMS)

[19] IETF RFC 4240 - Basic Network Media Services with SIP

[20] GSMA PRD IR.92 – ”IMS Profile for Voice and SMS” 3.0, 22 December 2010

[21] IETF RFC 4412 – Communications Resource Priority for SIP

[22] IETF RFC 3680 – A Session Initiation Protocol (SIP) Event Package for Registrations

[23] IETF RFC 3261 - SIP: Session Initiation Protocol, Internet Engineering Task Force

[24] MTAS Technical Product Description ---- MMTel AS, 2/221 02-FGC 101 2990

[25] MTAS Technical Product Description ---- SCC AS, 3/221 02-FGC 101 2990

[26] MTAS Technical Product Description ---- ST AS, 5/221 02-FGC 101 2990

