

MTAS Security Guide

MTAS

USER GUIDE

Copyright

© Ericsson AB 2016–2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

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

Trademark List

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



Contents

1	Introduction	1
1.1	Prerequisites	1
1.2	Environment	1
2	Product Security Functionality	3
2.1	Authentication	3
2.2	Authorization	3
2.3	Accountability	4
2.4	Integrity	4
2.5	Confidentiality	4
3	Security Configuration	7
3.1	Procedures	7
3.2	Recommended Periodic Operations	9
3.3	Handling of Patches	11
4	Default Parameter Values	13
5	Services, Ports, and Protocols	15
6	Privacy	17
6.1	Notice	17
6.2	Consent	17
6.3	Classification of Personal Data	17
6.4	Personal Data Quality	18
6.5	Personal Data Retention	19
6.6	Confidentiality and Integrity of Personal Data	20





1 Introduction

This document describes the security functions implemented by the Multimedia Telephony Application Server (MTAS). It also describes the security-related procedures that can be performed by the system administrators.

The MTAS is a telephony application server that is to be deployed as a virtualized network element in an IP Multimedia Subsystem (IMS) network. This deployment is referred to as a Virtual Network Function (VNF). For details about MTAS, the supported functionality, and the nodes it communicates with, refer to *vMTAS 1 Technical Product Description Common Features*.

1.1 Prerequisites

This section describes the prerequisites; conditions and information required for performing security management on the MTAS.

1.1.1 Conditions

Before performing the procedures in Section 3.1 Procedures on page 7, ensure that the following conditions are met:

- The MTAS VNF has already been installed and initially configured. The initial configuration includes the necessary settings for the authentication of Northbound Interface (NBI) users to a Lightweight Directory Access Protocol (LDAP) server and their authorization.
- The intended software level to be run in the MTAS is installed. The release information can be found in delivery reports, delivery specifications, delivery notes, release notes, or correction notes.
- The user has the required access privileges, and the required usernames and passwords are known.

1.2 Environment

This section describes the environment requirements for product operations.

MTAS belongs to the core network and is not facing directly to access networks. In addition, the system is to be deployed behind a firewall which offers protection from external attacks.

MTAS is placed in the Service & Control Virtual Private Network (VPN) group which includes Network Functions handling signaling traffic without direct



connection to external networks. This includes the following VPN for connecting the IMS Network Nodes in the group:

- The Signaling Service Control VPN for signaling traffic to and from other IMS Network Nodes.
- The Operation and Maintenance Service Control VPN for Operation & Maintenance (O&M) traffic used for IMS Network Nodes in the group. This also includes Charging (Ro/Rf) and Provisioning (CAI3G) traffic.

For more details, refer to *MTAS Internal and External Connectivity*.



2 Product Security Functionality

The following security functionality is supported in the product:

- Authentication
- Authorization
- Accountability
- Integrity
- Confidentiality

2.1 Authentication

2.1.1 O&M User Authentication

MTAS supports Local and Centralized O&M password-based user authentication. For more information, refer to *User Management*.

2.1.2 Mutual Authentication of Communication Channel Peers

MTAS supports certificate-based mutual authentication for:

- LDAP over Transport Layer Security (TLS), between MTAS and LDAP server, refer to *Certificate Management*.
- IKEv2 during the establishment of the IPsec Security Associations, between MTAS and any peer, refer to *eVIP Management Guide*.

2.2 Authorization

2.2.1 O&M User Authorization

Authorization is the capability to validate if the logged in user is allowed to perform a certain operation to a certain Managed Object (MO). The authorization is role-based, that is, the logged in user is mapped to a role and each role has one or several rules defining the access right to an MO.

The user management principles, user administration, and user roles are described in *User Management*.



2.3 Accountability

Audit Log function allows the operator tracking of the operator access to system and actions performed over resources such as files, directories, MOs, and attributes.

The log allows performing audits to detect fraudulent or misuse on the operations performed in the nodes.

For details, refer to *Audit Information*.

2.4 Integrity

2.4.1 Node Integrity

- Verification/protection of the integrity of the system configuration files.
- Node integrity protection prevents unauthorized modification of the selected files/folders.
- O&M Roles and Rules provide integrity protection by role and target-based access control.

2.4.2 Communication Integrity

- Integrity protection of O&M traffic (also including charging data records, backups, logs)
- Integrity protection of signaling traffic
- TLS provides for integrity protection

2.5 Confidentiality

2.5.1 Communication Confidentiality

- Confidentiality protection of O&M traffic (here, also including charging data records, backups, logs).
- Confidentiality protection of signaling traffic.
- TLS provides for confidentiality and integrity protection, and mutual authentication of the peers.
- NETCONF is protected using Secure Shell (SSH), in addition TLS can also be used.



- LDAP is protected using TLS, both for provisioning requests and for access to an external LDAP authentication and authorization server.
- CAI3G for provisioning is protected by using TLS.
- Signaling traffic like Session Initiation Protocol (SIP) and Diameter can be protected by IPsec tunnels with authentication and encryption of each IP packet in a communication session.





3 Security Configuration

This section describes how to operate the security functionality of the product.

3.1 Procedures

This section provides the instructions for operating the security functionality of the product.

3.1.1 Hardening

Perform hardening of the MTAS node according to the procedures described in *MTAS Hardening Guide*.

This includes:

- Allow or block ports for all listening services.
- Change default passwords, including predefined password for root which could be known by many persons.
- Disable root access through NBI, remote logon for root user is enabled by default.
- Enable strong password enforcement.
- Force password change and aging.
- Configure Command-Line Interface (CLI) inactivity timer.
- Create emergency user, at least one emergency user must be configured in the system.
- Delete unused local Linux® accounts, if additional users are created during installation, and they are not to be used, they must be deleted.
- Block Network File System (NFS) against access from external networks.

The operator can have own security policies, where the node must be hardened according to operator requirements, for example defining specific secure protocols or other ports different than the default ones.

After the hardening activities have been performed, create a backup of the system. It is also recommended to upload the backup to external storage.



3.1.2 Authentication and User Management

Create users and user groups, and assign privileges to a group.

Always use personal accounts instead of shared or generic user accounts.

The MTAS has five predefined default roles. These roles, and the corresponding rules, cannot be modified:

- System Administrator
- System Security Administrator
- MTAS Application Administrator
- MTAS Application Security Administrator
- MTAS Application Operator

LDAP must be configured with the strongest possible ciphers.

For details on LDAP Authentication and Local Authorization, and Roles/Rules refer to *User Management*.

3.1.3 Audit Trails

The audit log enables logging and tracking access to files, directories, and resources of the system, as well as tracing system calls. It enables monitoring of the system for application misbehavior or code malfunctions.

For information about where to find the audit and syslog log files, and how to read them, refer to *Audit Information*.

3.1.4 MTAS Configuration for Provisioning LDAP

There are provisioning related MOs that are not accessible through the normal NBI, a provisioning LDAP connection is used instead.

The procedures for setting up the LDAP connection using Secure Socket Layer (SSL) / Transport Layer Security (TLS) are described in *MTAS Configuration for Provisioning LDAP*.

3.1.5 MTAS Configuration for XDMS

The XDMS function supports a secured CAI3G interface to allow the operator to manage subscriber data in an encrypted and authenticated way.

The authentication of the MTAS is enabled by a trusted certificate.



The operator has the possibility to perform the operations on the CAI3G certificate, refer to *MTAS XDMS Management Guide*.

3.1.6 Change Logon Banner

By default, no information is provided to the user when logging on using the CLI. The operator can define own customized greeting message or legal message when a user logs on through the CLI.

The system provides the file `/cluster/etc/motd`, which allows a text message to be created and later displayed when user logs on to the system through CLI.

3.1.7 IPsec Support

If there are requirements to protect Signaling traffic, for example SIP or Diameter (when transferring charging or malicious call tracing data) IPsec tunnels can be used.

The procedures for setting up IPsec tunnels to protect signaling traffic are described in *eVIP Management Guide*.

3.1.8 H.248

For H.248, there is a configured white list of MIDs that are supported.

If the Media Resource Function Processor (MRFP) uses any other MID than configured in MTAS, the Stream Control Transmission Protocol (SCTP) link to it is closed down.

3.2 Recommended Periodic Operations

This section describes recommended periodic operations.

The product has to be properly hardened before it is taken into use. Nevertheless, it is important that the daily operations on the product are performed in such a way that the security status of the product is not weakened.

New vulnerabilities which need to be mitigated are frequently found in the existing products. Therefore it is necessary to maintain the security posture of the product in service on a regular, ongoing basis.

The recommended periodic security-related operations are the following:

- Ensure that the latest software version is installed. It is recommended to get the latest available Emergency Package (EP) version of the MTAS.
- Ensure that Audit Logging is turned on and working.



- Regularly perform housekeeping of not used or obsolete software bundles, and backups stored at the node.
- Regularly perform system backups.
- Regularly export backups to external storage.
- Regularly export logs to external storage.
- Regularly fetch Performance Management (PM) data from the MTAS and store externally.
- Regularly check the TLS certificates to ensure that they do not expire.
- Run password checkers periodically to find weak passwords.
- Monitor the file system integrity periodically, either manually or as a scheduled task.
- Ensure that no unnecessary listening ports are open.
- Ensure that the ports for the insecure protocols Telnet and File Transfer Protocol (FTP) are closed.
- Ensure that no shared user accounts are used.
- Ensure that administrative user rights are assigned only to real needs.
- Run password checkers periodically with word lists to find weak passwords.
- Regularly check audit logs related to potential security events. Check anything that could be considered as strange according to the traffic model of the operator, besides error cases, for example, failures to authenticate, too much user activity, or too many dropped or rejected sessions.
- Regularly analyze log data and counters to reconsider the chosen security-related attributes.
- Monitor the following counters to detect unauthorized access:
 - `MtasXdmsCai3gLoginOk`
 - `MtasXdmsCai3gLoginNOkI`
 - `MtasXdmsCai3gLoginNOkE`
 - `MtasMrfcRejectedRegistration`
 - `MtasSipPresenceInvalid`



3.3 Handling of Patches

Patches are delivered in the form of Emergency Packages (EPs). The process to load EPs is described in the upgrade instruction for the actual MTAS EP.





4 Default Parameter Values

Not applicable.





5 Services, Ports, and Protocols

The services, ports, and protocols that are used by the products are listed in Table 1.

For details on IP Address Types and Ports, refer to *MTAS Hardening Guide*.

Table 1 Services, Ports, and Protocols Used by MTAS.

Service or Interface Name	Protocol	IP Address Type	Port	Transport Protocol	IP Version
NETCONF	SSH	Muta MIP	830	TCP	IPv4 or IPv6
NETCONF	TLS	Muta MIP	6513	TCP	IPv4 or IPv6
ECLI	SSH	Muta MIP	22	TCP	IPv4 or IPv6
SFTP	SFTP	Muta MIP	115	TCP	IPv4 or IPv6
SNMP FM	SNMP	Muta MIP	161	UDP	IPv4 or IPv6
SSH	SSH	SC-1 IP SC-2 IP	22	TCP	IPv4 or IPv6
SSH, SFTP, SCP	SSH	Muta MIP	22	TCP	IPv4 or IPv6
LDAP Provisioning	LDAP(S)	OAM VIP	7323 17323 7423 (S), 17423 (S)	TCP	IPv4 or IPv6
CAI3G	CAI3G/ SOAP/HT TP(S)	CAI3G VIP	8095 8443 (S)	TCP	IPv4 or IPv6
Ut	Ut / XCAP	Ut VIP	8090	TCP	IPv4 or IPv6
CCMP	CCMP /HTTP	CAI3G VIP	8096	TCP	IPv4 or IPv6
ISC	SIP	Traffic VIP	5060 5082 -5088, 5160 -5163	TCP/UDP	IPv4 or IPv6
Ma	SIP	Traffic VIP	5060 5090	TCP/UDP	IPv4 or IPv6

*Table 1 Services, Ports, and Protocols Used by MTAS.*

Service or Interface Name	Protocol	IP Address Type	Port	Transport Protocol	IP Version
Pw	SIP	Traffic VIP	5086	TCP/UDP	IPv4 or IPv6
Mp	H.248	Traffic VIP	2944	SCTP	IPv4 or IPv6
Cr	SOAP/HTTP	Traffic VIP	9080	TCP	IPv4 or IPv6
Px	SOAP/HTTP	Traffic VIP	9080	TCP	IPv4 or IPv6
Sh / Dh	Diameter	Traffic VIP	3868–3872	TCP	IPv4 or IPv6
Rf / Ro	Diameter	OAM VIP or Charging VIP	3868–3872	TCP	IPv4 or IPv6
CDS	Diameter	Traffic VIP	3868–3872	TCP	IPv4 or IPv6
CAPv2 / MAP	CAPv2 / MAP	SIGTRAN VIP1 SIGTRAN VIP2	2905	SCTP	IPv4 or IPv6



6 Privacy

MTAS handles personal subscriber data to be able to provide services in the network. The data of the subscribers is handled properly and the product supports different measures to protect the privacy of the subscribers. The personal data is listed in Table 2.

6.1 Notice

This product processes personal information and it can have an impact on the right to privacy of the data subjects (for example, subscribers), whose data is processed.

When operating this product, ensure that personal information processing is performed in a fair and lawful manner, and in accordance to the local data protection regulation in force. This can be achieved by providing notice to subscribers of privacy policies of the operator, for example at the moment of establishing the subscription.

6.2 Consent

This product can process personal data that can be considered sensitive information, such as network location, in addition to basic personal data.

The local data protection regulation where the node is operated can require obtaining subscriber consent to process this kind of personal information. Such consent must be obtained so to:

- Collect and maintain personal data of the subscriber, aimed at holding securely this information.
- Fulfill the purpose of installing, upgrading, and administering the MTAS.

The system can be required to activate trace information. The purpose of these traces is only for troubleshooting. Depending on the required information (level of the trace), it can contain personal data.

- Disclose the personal information to third parties.

6.3 Classification of Personal Data

Table 2 lists the personal data handled by the MTAS.

Table 2 Personal Data Handled by MTAS

Personal Data Category	Data Item
Basic data	IP address
	MSISDN
	IMSI
	IMEI code
	Mobile number
	First name
	Last name
	Private User Identity (IMPI)
	Public User Identity (IMPU)
	Mobile Device Serial Number
	Logon details
Sensitive data (identifiable user activity)	Call history
	Browsing/Connection history
	Metadata showing user activity
	Event Monitoring (Event Based Monitoring, Call Trace Recordings, General Performance Event Handling, ...)
	Content of communication: voice, text, sound, picture, or other content of the communication
	Browsing/Connection history, URL, originating IP
	Location history
	Location: LAC / CellID

6.4 Personal Data Quality

MTAS handles personal subscriber data to be able to provide services in the network. The personal data is listed in Table 2.

The source of the privacy data handled by MTAS is stored in HSS. MTAS does not maintain the quality of the data. To update or delete incorrect personal data in HSS is the responsibility of the operator. For this, MTAS provides interfaces towards HSS. (CAI3G, Ut, WEBS, GENSSC, and SSC).



6.5 Personal Data Retention

There are three places where personal data can be stored. Therefore there are several retention approaches:

- 1 Cache (Transparent Data)
- 2 Console logs
- 3 XDMS logs

6.5.1 Cache

Subscriber data is cached by MTAS during call handling. The registration message has a time limit for the cached data and it is also possible to delete the cache manually. The time limit is set during registration and after the time expires the data is deleted. For more information, refer to *MTAS Subscriber Data Management Guide*.

6.5.2 System Logs

When a call-related capsule abortion happens the 'CA' contains the user data as well for debugging reason. These log files rotating out periodically. This log rotation can be size-based or time-based.

By default, the following folders have time-based log rotation:

dataCollection: `/cluster/storage/no-backup/dc`

Default values:

- `maxFileGroupSize:` 1048576kB
- `Retention Time:` 1440min

healthCheck: `/cluster/storage/no-backup/hc`

Default values:

- `maxFileGroupSize:` 1048576kB
- `Retention Time:` 1440min

healthCheckReports: `/cluster/storage/no-backup/hc_reports`

Default values:

- `maxFileGroupSize:` 10240kB
- `Max. Number of Files:` 24pcs



- Retention Time: 1440min

For more information, refer to *Configure Preventive Maintenance Policy Deleting Files in Logical File System*.

6.5.3 XDMS Logs

Provisioning related activities are logged in 'Catalina' logs and can contain privacy data. These logs do not have time-based log rotation function therefore operational activity must ensure deletion of log entries to fulfill retention policy.

These are the locations of XDMS logs:

- Catalina Logs (on the PLs): `/opt/mmas/appserver/traffic_instance<integer>/logs`

6.6 Confidentiality and Integrity of Personal Data

6.6.1 Data in Transfer

CAI3G traffic is protected by HTTPS. For more information, refer to the section *Secure CAI3G Interface* in *MTAS XDMS Management Guide*.

Other traffic that can have privacy data can be protected by IPsec.

6.6.2 Data in Rest

MTAS stores the logs and dumps in plain text, but the file system is protected by access control. Operators are to ensure proper access control for the users. For hardening the node, refer to the *MTAS Hardening Guide*.

If the data has to be moved from the node, the encryption is highly recommended. To encrypt the data, use the following example:

6.6.2.1 Create A Public Key

First, the receiver of the file must have a public key for the encryption.

To generate a public key, perform the following on a Linux system of the receiver side:

1. `gpg --gen-keygen`
2. Select the type of key:



Please select what kind of key you want:

- (1) DSA and Elgamal (default)
- (2) DSA (sign only)
- (5) RSA (sign only)

Select the first one.

3. Choose the key size. A DSA key pair is 1024 bits long; ELG keys can be 1024–4096 bits long:

What keysize do you want? (2048)

The higher the amount, the better. A recommendation is to use a 4096-bit key.

4. Specify the expiration period:

Please specify how long the key should be valid.

- 0 = key does not expire
- <n> = key expires in n days
- <n>w = key expires in n weeks
- <n>m = key expires in n months
- <n>y = key expires in n years

Key is valid for? (0)

Do not use the '0' option, and do not use a too long expiration period; only for as long as it is needed. For example, in a situation where the file is transferred only once, the one-day option is sufficient.

Key expires at <date>
Is this correct? (y/N) **y**

5. Provide name, email address, and comment if needed, for example:

Real name: **John Smith**
Email address: **john.smith@ericsson.com**
Comment: **Log analysis**
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?

6. Press **O** to continue.

7. Provide a password:

Write your password.
Repeat your password.

6.6.2.2

Export the Public Key

Perform the following commands on the same machine where the key was generated:



```
gpg --armor --export john.smith@ericsson.com >  
john.smith.gpg
```

6.6.2.3 Import the Public Key on the Node

After the public key is exported, it has to be uploaded to the node. To export the key, perform the following on the node:

```
gpg --import john.smith.gpg
```

6.6.2.4 Encrypt the Log File

First, the file must be copied to the `/root` folder:

```
cp /cluster/storage/no-backup/cdclsv/dumps/logdump-<...>.  
tgz ./
```

6.6.2.5 Decrypt the Log File

After the log file was encrypted, it can be sent to the recipient. On the recipient Linux machine, perform the following and give the password which was given during public key creation:

```
gpg --output logdump-<...>.tgz --decrypt logdump-<...>.t  
gz.gpg
```

Use the same method for any other file that can contain privacy data.