Security for O&M Node Access

DESCRIPTION

Copyright

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

This document describes the management model and concepts for the *Security for O&M Node Access* Managed Area (MA). It provides an understanding of how the area is modelled, the functions related to the area, and how they are managed.

An MA represents a group of functions and the corresponding Managed Objects (MO) within the node. The grouping of MAs defines areas relatively independent of one another.

This MA represents the basic functions and MOs for certificate management and Authentication and Authorization (AA) for Operation and Maintenance (O&M) access.

1.1 Related Documents

The following documents relate to this MA:

- *WCDMA RAN Security Management* provides basic information about Radio Access Network (RAN) O&M security.
- *IP Transport* describes the basic functions and MOs for IP transport, IP transport security, and IP-based O&M access to the node.

2 Functions and Concepts

This section describes the functions and concepts that apply to the MA.

2.1 Security Level

The RBS 6402 is configured as equivalent to security level 3 in other nodes. For more information about security levels, see *WCDMA RAN Security Management*.

The following applies to O&M node access:

- Local O&M access is not supported.
- O&M traffic is implemented through secure protocols only.
- Local AA is not supported. A central AA database is required, as described in Section 2.3.2 on page 5.

2.2 O&M Interfaces, Services, Protocols and Ports

This section provides information about O&M interfaces, IP services, protocols, and ports.

2.2.1 O&M Interfaces and Services

The main O&M interface for RBS 6402 is Operations Support System for Radio and Core (OSS-RC), which is described in a separate CPI library.

File transfer is secured by the Secure Shell (SSH) File Transfer Protocol (SFTP).

IPsec is optional but highly recommended. Refer to *IP Transport* for more information about secure IP transport.

2.2.2 Protocols and Ports

The information in this section is an aid, for example, when configuring a firewall. Table 1 provides a list of all ports used for O&M traffic, User Plane Traffic and Control Plane Signaling. The ports supported are of types TCP, UDP and SCTP. All other ports than those in the table must be closed in the firewall.

The firewall must be a stateful firewall, which allows the IP traffic back to the dynamic ports as long as the traffic comes into an open port. The context in the packets remains the same. If a stateless firewall is used, all ports from the node to the O&M intranet must remain open.

Table 1 O&M Protocols and Ports

Port	Usage
22	SFTP
161	SNMP
389	LDAP
500	IPsec/IKE
636	LDAP
829	CMPv2
830	NETCONF
831	NETCONF
4500	IPsec/IKE
9830	Ericsson CLI

2.3 Authentication and Authorization

This section provides information about the AA required for Managed Object Model (MOM) operations.

When managing node resources, an authentication request that contains a user-ID and a password is sent to the AA service. The response to this request contains the authentication result and the set of roles associated to the user.

2.3.1 IPsec Negotiation

The RBS uses certificate-based authentication. During autointegration the RBS first uses the factory installed vendor credentials, which is a node unique certificate and a private key. The RBS then performs certificate enrollment using CMPv2 to acquire a certificate from the operator OSS-RC Certificate Authority (CA) server. This certificate is then used for all subsequent IPsec tunnels.

Because the RBS acts as an initiator during the Internet Key Exchange Version 2 (IKEv2) handshake, all requests are proposals to the responder, which chooses the configuration used in the negotiated IPsec connections.

The proposal includes the inner IP addresses, which are initially requested in the IKEv2 Configuration Payload (CP) during the autointegration procedure. If an inner IP address is changed through the MOM, after autointegration the new address is not used unless the new proposal is accepted by the responder.

Note: IKEv2 CP is mandatory for the autointegration procedure. For LMT (Local Maintenance Terminal) integration, on-site configuration, it is sufficient that the SEG supports IKEv2.

Refer to *RFC 5996* for more information about the IKEv2 protocol.

The RBS uses the following IKE ID when setting up the IPsec tunnel:

- For the O&M IPsec tunnel, certificate subject (DN) in format `O=Ericsson, CN=<RBS serial number>.ericsson.com`
- For Iub IPsec tunnel, `subjectAltName` in format `<RBS serial number>.ericsson.com`

The Security Gateway (SEG) will assign one inner IP address to the RBS for each IPsec tunnel. At the end of the autointegration sequence, the RBS reports to the OSS-RC which IP addresses it has acquired for the O&M and Iub traffic.

Note: The X2 interface is only compatible with a SEG that can support direct inter-RBS connectivity with single traffic selector.

Table 2 describes the default settings for the IKEv2 and Encapsulating Security Payload (ESP) algorithm suite and their respective priority in the cryptographic algorithm negotiation. The settings cannot be changed.

Table 2 Default settings for the IKEv2 and ESP Algorithm Suite

Priority in Negotiation	Cipher	Integrity Protection Algorithm	Diffie-Hellman Group
1	AES128 CBC	SHA1	Group 14 - 2048-bit MODP
2	AES128 CBC	SHA1	Group 2 - 1024-bit MODP

2.3.2 Central AA Database

The RBS 6402 AA service is a central AA database in OSS-RC. It is an LDAP server, which stores user credentials and allows them to be queried over a secure LDAP interface.

2.3.3 Roles

The response to an authentication request contains the authentication result and the role associated to the user. Depending on the authorized role, the user can either access all functions and data in the node, or a subset of functions and data in the node. Roles can also control access to files and Ericsson CLI.

The `LocalAuthorizationMethod` MO and its child MOs provide more information about the roles.

The roles are defined as follows:

SystemAdministrator
Provides full access the entire MOM containment tree, except security management MOs.

SystemSecurityAdministrator
Provides full access to security management MOs only.

RBS_Application_Operator
Provides read access to the entire MOM containment tree, except security management MOs. An application operator can also trigger MO actions.

Note: If the `administrativeState` attribute of the `LocalAuthorizationMethod` MO is set to `LOCKED`, all users authenticated via LDAP will have access too all resources in the node, that is, the access is no longer controlled by the roles.

2.3.4 Session Handling

A session starts when a user is granted node access and ends when the user logs out or when the session time-out occurs because the user has been inactive for a certain time frame. For NETCONF this timeframe is 10 minutes, for CLI it is two minutes.

If the user is not authorized for any role at all, the user session is immediately disconnected.

Authentication responses from the AA service are not cached on the RBS.

2.4 Certificates on the Node

The node relies on asymmetric cryptography and digital signatures for the authentication of communicating peers and validation of signed files. To ensure the correctness and validity of the keys used for such purposes, certificates and trust relationships ordered in a Public Key Infrastructure (PKI) are required.

2.4.1 Certificate Types

The following sets of keys and certificates must be present on the node:

Vendor Credentials

Vendor credentials are pre-installed on the node and are used during integration to authenticate network access and to enroll certificates for both node and IPsec credentials.

Node Credentials

Node credentials are used for NETCONFTLS authentication in O&M communication and are also used for IPsec.

Trusted Certificates

Trusted certificates are paired to a trusted CA. The RBS trusts external nodes that present a certificate signed by a trusted CA.

2.4.2 Certificate Enrollment

The RBS performs CMPv2 certificate enrollment with an RA/CA server during autointegration. It receives signed operator credentials and the operator's CA certificates. When this procedure is complete, the RBS only uses operator credentials and trusts other nodes that have certificates signed by the operator CA or sub-CA. The O&M over TLS certificate is always enrolled, whereas the IPsec certificate is only enrolled if IPsec is used.

2.4.3 Certificate Renewal

Certificate renewal is normally performed using the CMPv2 protocol, as in the initial enrollment procedure. The difference is that the authentication of the node and the signing of CMPv2 messages is performed using the old node credentials instead of the vendor credentials. Certificate renewal is triggered by the following MOM actions:

- *startOnlineEnrollment*
- *startOfflineCsrEnrollment*
- *installTrustedCertFromUri*

The RBS will automatically perform the certificate renewal before the old certificates expire. This is controlled by the *renewalMode* attribute.

Certificate renewal can also be performed manually by downloading them from the Universal Identifier (URI). However this method is not recommended as it will expose the private key identity outside the node.

2.5 Supported Cipher Suites

This section provides information about supported cryptographic algorithms.

The system software images are protected with secure boot that utilizes hash functions and asymmetric algorithms to sign the software images. The hardware verifies the signature before running the software image. To ensure confidentiality of user data (that is speech and data traffic) and control signaling between end users' mobile devices and the RNC , all communication is encrypted with symmetric algorithms and the integrity is protected with Keyed-Hash Message Authentication Code (HMAC) algorithms.

The connection between the RBS and the operator's network is encrypted to prevent unauthorized access to the RBS. The communication parties are authenticated using asymmetric algorithms. The storage of private keys in the product is protected by storing the keys in encrypted form using symmetric algorithms to prevent unauthorized access to them.

Below are the supported cryptographic algorithms listed with the encryption algorithms key lengths in brackets.

- AES (256)
- 128-EEA1 (128)
- 128-EIA1 (128)
- 128-EEA2 (128)
- 128-EIA2 (128)
- RSA (8192)
- SHA1
- SHA2
- HMAC-SHA (512)

3 Managed Object Model (MOM)

This section describes the management model defined for the MA. Refer to Section 2.3 on page 4 for more information about the authorization required to view the `SecM` MO and its child MOs.

Note: If an unsupported value is set, traffic may be affected. A few MOs, parameters, counters, and value ranges may be visible in the (MOM) even though they are not yet supported. This is due to consideration of future system aspects.

Refer to *Managed Object Model (MOM) User Guide* for information about the managed object model concept.

Refer to *Managed Object Model (MOM) RBS* for information about all MO classes.

3.1 Certificate Management

Figure 1 provides an overview of MOs that relate to certificate management.

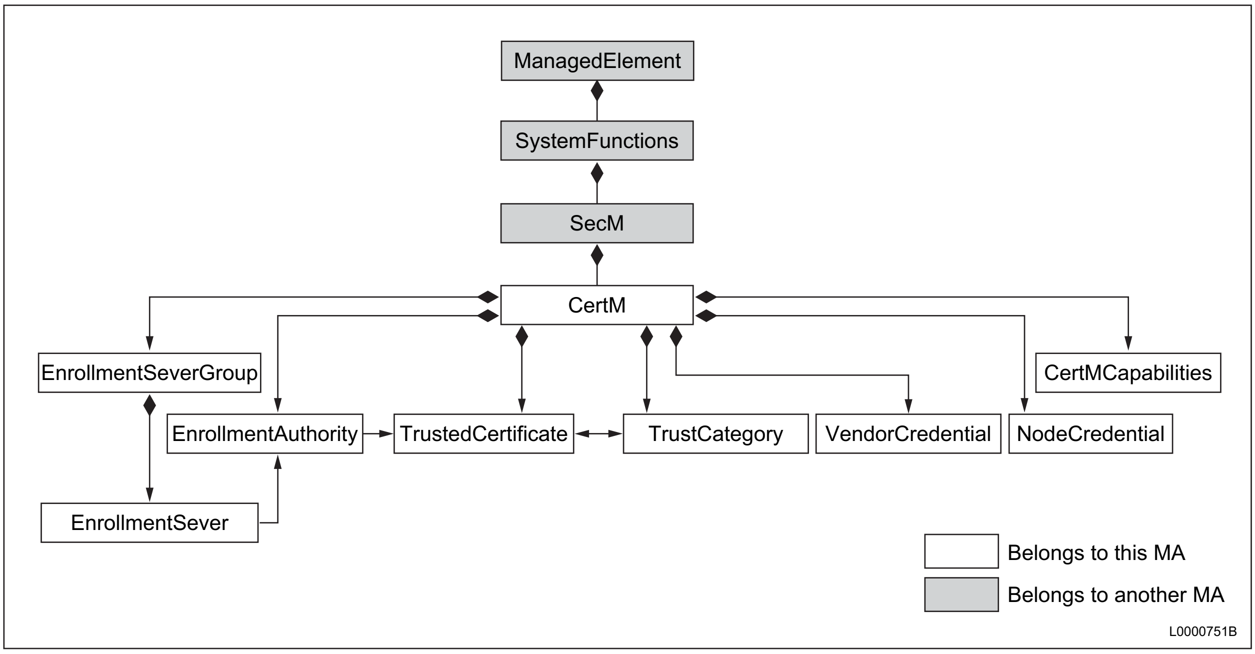

Figure 1 Certificate Management MO Overview

Table 3 describes the MO classes of the MA.

Table 3 Certificate Management MO Class Descriptions

Managed Object	Description
`CertM`	Contains MOs for certificate management, that is, management of node credentials and of trusted certificates.
`CertMCapabilities`	Provides information about the certificate management capabilities of the managed element.
`EnrollmentAuthority`	Represents a Certification Authority (CA) or Registration Authority (RA) for certificate enrollment.
`EnrollmentServer`	Represents an enrollment server that implements Certificate Management Protocol version 2 (CMPv2). Simple Certificate Enrollment Protocol (SCEP) is not supported.
`EnrollmentServerGroup`	Represents a group of enrollment servers, for load balancing.
`NodeCredential`	Represents the node credential and contains information about the corresponding certificate.
`SecM`	Contains MOs for security management functions such as user management and certificate management.
`TrustCategory`	Represents a group of trusted certificates.
`TrustedCertificate`	Represents a trusted certificate.
`VendorCredential`	Represents the pre-installed vendor credential.

3.2 User Management

The MOs that relate to user management are shown in Figure 2. Refer to Section 2.3.2 on page 5 for more information about the central AA database.

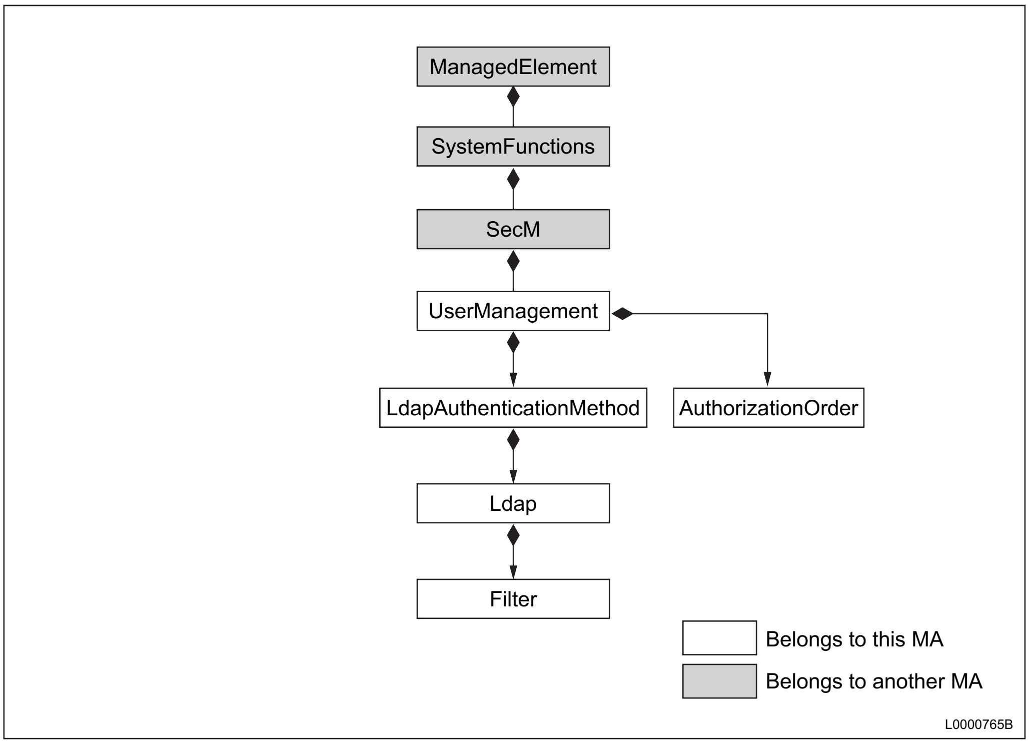

Figure 2 User Management MO Overview

Table 4 describes the MO classes that relate to user management.

Table 4 User Management MO Class Descriptions

Managed Object	Description
AuthorizationOrder	Manages the order of authorization methods.
Filter	Represents an LDAP filter, which defines the filter search that locates the user's role definitions in the LDAP directory.
Ldap	Contains attributes that manage the communication to the primary and secondary LDAP directories.
LdapAuthenticationMethod	Contains MOs that set up the LDAP authentication method.
ManagedElement	This is the top level MO of the node.
SecM	Contains MOs for security management.
SystemFunctions	Contains MOs for O&M functions provided by the Managed Element.
UserManagement	Contains MOs for user management.

4 Configuration Management

This section describes the changes and additions that can be made to the basic configuration that is set up during autointegration.

Attention!

Risk of data loss or data corruption.

Attention!

Risk of system malfunction or traffic disturbance.

Note: If an unsupported value is set, traffic can be affected. A few MOs, parameters, counters, and value ranges can be visible in the Managed Object Model (MOM) even though they are not yet supported. This is due to consideration of future system aspects.

4.1 Certificate Management

This section describes configuration management activities that relate to certificate handling.

4.1.1 Changing the URI of an Enrollment Server

To change the address of an enrollment server, set attribute *`uri`* of the appropriate *`EnrollmentServer`* MO.

Note: Only Certificate Management Protocol (CMP) can be used in *`uri`*.

4.1.2 Installing a Trusted Certificate

To install a trusted certificate, use action *`installTrustedCertFromUri`* of MO *`CertM`*.

The *`uri`* parameter of the action must be an HTTP URL (`http://`). The certificate file format must be Privacy Enhanced Mail (PEM).

4.1.3 Removing a Trusted Certificate

Before a trusted certificate is removed, all references to the certificate must be deleted.

Do the following to delete the references to a trusted certificate:

1. Navigate to a *TrustCategory* MO.
2. Remove the appropriate certificate reference from the list in the *trustedCertificates* attribute.
3. Repeat steps 1 and 2 for all *TrustCategory* MOs.

Finally, use action *removeTrustedCert* of MO *CertM* to remove the trusted certificate.

4.1.4 Renewing Node Credentials

Do the following to renew the node credentials:

1. Navigate to the *NodeCredential* MO.
2. Ensure that the *certificateState* attribute value is `VALID`.
3. Set the *renewalMode* attribute to `MANUAL`.
4. Set the *keyInfo* attribute.
5. Set the *enrollmentServerGroup* attribute to `ManagedElement=1, SystemFunctions=1, SecM=1, EnrollmentServerGroup=1`.
6. Optionally, set the *enrollmentTimer* attribute.
7. Use action *startOnlineEnrollment* of MO *NodeCredential*.

4.1.5 Adding Trusted Certificates to Trust Categories

A trusted certificate cannot be used by the certificate user before has been added to *TrustCategory*.

To add a trusted certificate to a trust category, set attribute *trustedCertificates* of MO *TrustCategory*. For settings, refer to Table 5.

A trusted certificate can only belong to one trust category at a time.

4.1.6 Credential MO Instances

Table 5 describes credential types and their corresponding MO instances.

Table 5 Credential MO Instances

Credential Type	MO Instance

O&M/TLS	TrustCategory=1
	NodeCredential=1

IPsec	TrustCategory=2
	NodeCredential=2

4.2 Changing LDAP Settings for Authentication and Authorization

Refer to the descriptions of MOs *Ldap* and *Filter* for information about LDAP settings.

Note: If the `administrativeState` attribute of the *`LdapAuthenticationMethod`* MO is set to `LOCKED`, all access to the RBS is prevented. All authentication attempts will fail. To access the node in order to change the setting of the `administrativeState` attribute, an on-site reset to factory settings is required. To perform a reset, see *Recovering a Node on Site*.

5 Fault Management

Refer to the *Alarm and Event List* for information about alarms and Fault Management (FM) events.

6 Performance Management

Refer to the *WCDMA RAN Counter List* for information about Performance Management (PM) counters.