RBS Autointegration

MSRBS-V1

USER DESCRIPTION

203/1553-HSC 105 50/1-V1 Uen H

Contents

1 Introduction

This document describes the RBS Autointegration feature in MSRBS-V1 managed elements.

Semi-automated integration is described only briefly in this document. For more information about semi-automated integration, see *Add RBS*.

1.1 Basic Characteristics

This section describes the basic characteristics of the function.

Feature name: RBS Autointegration

RBS Autointegration consists of functions in RBS and in Operations Support System – Radio and Core (OSS-RC). For RBS it is part of LTE Basic. The Base Station Integration Manager (BSIM) in OSS-RC is a licensed feature.

Product identity:

See *Feature Overview*

Replaces: N/A

Dependencies

This feature has no prerequisite features.

This feature affects no other features.

1.2 Benefits

RBS Autointegration simplifies project coordination in terms of cooperation between staff at OSS-RC and at RBSs and in terms of managing node specific configuration data. Configuration data is stored by OSS-RC and automatically retrieved by the RBSs reducing manual configuration data administration in deployment projects. The technician at the RBS site is the only person involved during the on-site integration. It is not dependent on staff presence at OSS-RC.

Preparations before the integration are supported with preconfiguration services in OSS-RC. Only a limited amount of data must be scanned to initiate the automated integration bringing an RBS into service. Depending on selection by the operator, cells are locked or unlocked and ready to carry traffic as a result of the integration.

The differences between RBS Autointegration and semi-automated integration are summarized in Table 1.

Table 1 Autointegration and Semi-Automated Integration Compared

Type of RBS Integration	Description
Autointegration	At full autointegration, the OSS-RC staff are involved only for planning and data preparation. The OSS-RC stores the configuration data. The integration is initiated by a technician at site. The Initial Configuration File (ICF) is built at the start of the autointegration and is automatically downloaded to the RBS. No laptop is needed. No manual pre-configuration is used. With BSIM, autointegration proceeds without intervention from any personnel until the cell is unlocked.
Autointegration with laptop	An alternative to full autointegration is to use autointegration with laptop. The laptop is used to download a Combined file to the RBS. The Combined file contains a Site Installation file. The input data is, for example, VLAN ID, and addresses for SEG and AIWS. The scope of the of the pre-provisioned parameters is for autointegration only.

Type of RBS Integration	Description
Semi-Automated Integration	The semi-automated integration makes it easier to integrate a small number of nodes in an already operating network. A laptop is used to download a Combined file to the RBS. The Combined file could contain both an ICF and a Site Installation file. Static IP addresses can be deployed through the ICF. The scope of the parameter is post-autointegration. For more information, see *Add RBS*.
Stand-Alone Integration	The Stand-alone integration makes it possible to integrate without the use of Operations Support System – Radio and Core (OSS-RC). A laptop is used to download a Combined file to the RBS. For more information, see *Stand-Alone Integration*.

2 Feature Operation

This section describes the RBS Autointegration feature in more detail and impacts of the feature in the LTE RAN.

Basic principles for configuring the network are to store configuration data in OSS-RC and then distribute the data to the RBSs over the network. With RBS Autointegration, the distribution and activation of configuration data is automated.

Configuration data based on planning results are prepared by using the Base Station Integration Manager (BSIM). BSIM reduces the number of parameters to set manually. It processes and stores all configuration data in OSS-RC, making it available for RBSs to retrieve when connected. These preparations made at any time before the installation of the RBS at site.

An RBS is normally prepared with a basic configuration before it is shipped from the factory. To make it a unique node in the network additional configuration data must be defined. At site, when the hardware installation is ready, the field technician initiate the autointegration. Using the Ericsson Node Integration Scanner (ENIS) tool, the field technician performs the hardware binding, that is, scans the barcode on the RBS and the Quick Response (QR) code on the work order and sends the data to OSS-RC. After the RBS is powered up, the autointegration proceeds without intervention from any personnel until the cell is unlocked. The field technician completes the integration by checking the hardware status. The RBS is now in service.

Note: ENIS hardware binding can also be performed before going to the RBS site.

Note: An alternative to ENIS is manual hardware binding. In this case, the RBS serial number is entered manually in OSS-RC. See *Pico OSS End to End Description* in the OSS-RC library.

Figure 1 shows processes supported by RBS Autointegration.

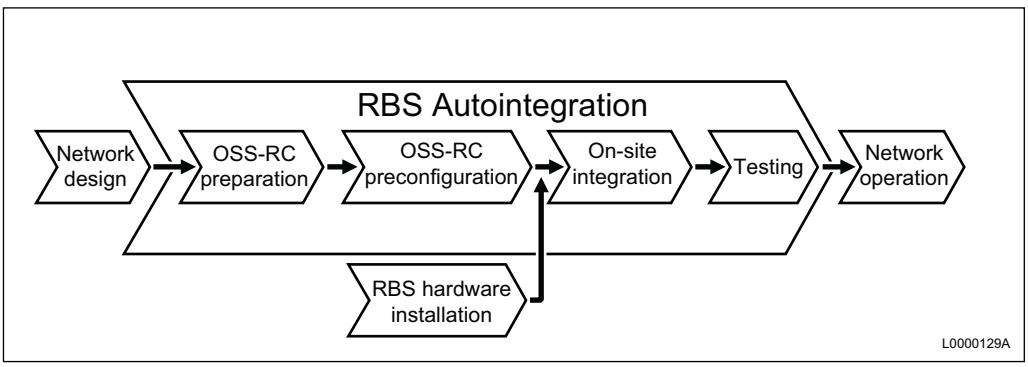

Figure 1 Processes Supported by RBS Autointegration

RBS Autointegration uses several services in OSS-RC, see Section 2.3 on page 7.

2.1 Network Configuration Requirements

The following must be fulfilled when using RBS Autointegration:

- The license for FAJ 121 1298: RBS Auto-Provisioning (RAP) is installed and activated, refer to *License Key Administration* in the OSS-RC library
- OSS system updated to sufficient version. Refer to latest *Network Impact Report*
- Operation and Maintenance Security Administration (OMSAS) is needed in OSS-RC
- OSS-RC is prepared for RBS integration according to *Pico OSS End to End Description* in the OSS-RC library
- The Base Station Integration Manager (BSIM) in OSS-RC is required

  See Section 2.3.1 on page 7 and Section 5.1 on page 19

The following documents must have been read and be available:

OSS-RC library documents

- *ARNE User Guide*
- *BSIM, Base Station Integration Manager, User Guide*
- *BSIM, Base Station Integration Manager, System Administrator Guide*
- *License Key Administration in OSS-RC*
- *Pico OSS End to End Description*
- *SMO, Software Management Organizer, User Guide*

LTE documents

- *Ericsson Node Integration Scanner (ENIS)*
- *Integrating RBSs On-Site Using ENIS*
- *Integrating RBSs On-Site Using ORI*
- *Install RBS*
- *IP Transport*
- *Managed Object Model (MOM) RBS*

2.2 Process Steps

Figure 2 shows the different stages of the process of adding RBSs using autointegration. For detailed information regarding the process, see *Add RBS*.

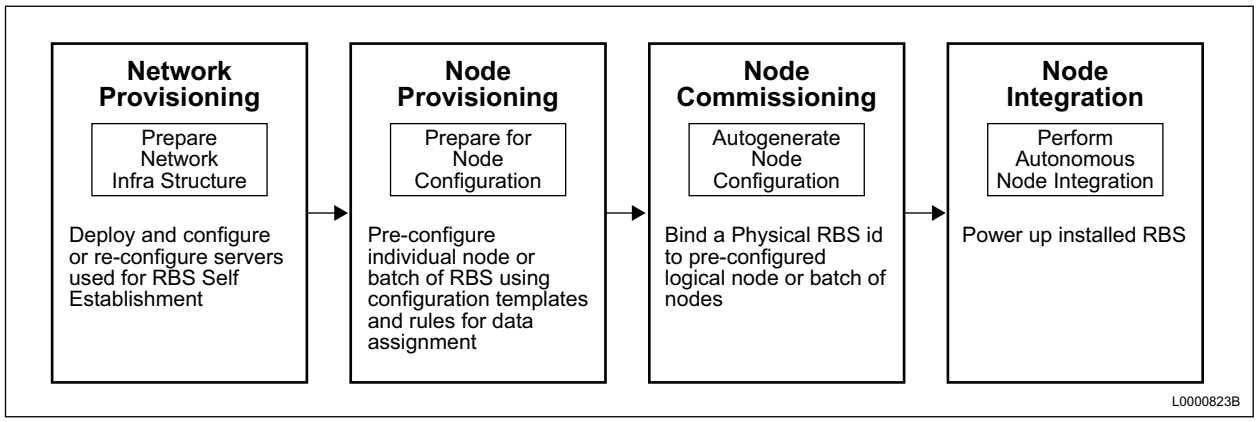

Figure 2 Process Overview

2.3 Applications and Services

This section describes how various applications and services are used for RBS Autointegration.

2.3.1 BSIM

The BSIM tool is used by the integration engineer to enter and prepare configuration data.

BSIM prepares the following services and servers with data to be retrieved by RBSs:

- Autointegration Web Service (AIWS)
- Operation and Maintenance Security Administration (OMSAS)
- OSS-RC Network Resource Model (ONRM)
- Software Management Repository Server (SMRS)

BSIM activates the planned areas and creates configuration versions.

BSIM uses an Initial Configuration File (ICF) template as initial source for RBS configuration data. The ICF template is populated with relevant operator network values.

Note: Make sure that the latest verified ICF template version is available in BSIM.

BSIM is a licensed feature in OSS-RC. Licenses for BSIM are validated when BSIM is launched by the user. Functions in BSIM are available depending on valid licenses.

2.3.2 AIWS Server

When autointegration starts, the ICF is built and uploaded to the AIWS server. The RBS then downloads the ICF from the AIWS server.

No logon credentials to the AIWS need to be entered at autointegration. The AIWS performs a secure identification of the RBS by using the RBS vendor credentials that are stored during manufacturing.

For more information regarding secure identification, see *Security Management*.

2.3.3 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) server provides the RBS with basic IP parameters. In requests for parameters from the DHCP server, the RBS identifies itself with the RBS logical name, or alternatively with the DHCP client identifier. The DHCP server responds with a number of parameters, for example, IP addresses for the DNS server, default gateway, and the AIWS server.

For more information regarding DHCP server, see *Add RBS* and *IP Transport*.

2.3.4 DNS

The Domain Name System (DNS) server maps host names and domain names to IP addresses. Examples are mapping of domain names to IP addresses for AIWS and Security Gateway (SEG). The DNS server is optional and is used as a complement to the DHCP server.

For more information regarding DNS server, see *Add RBS* and *IP Transport*.

2.3.5 Security Gateway

The Security Gateway (SEG) is a security enabled router that supports encrypted communication over an untrusted network using IPSec. The RBS receives the SEG IP addresses for an initial temporary IPSec tunnel from either the DHCP or DNS server. For the permanent IPSec tunnel that succeed the initial one, the ICF provides the IP addresses.

For more information regarding the SEG, see *Add RBS* and *IP Transport*.

2.3.6 EGIS

The Ericsson Global Integration Service (EGIS) provides the IP or FQDN addresses to the SEG and AIWS server during autointegration of an RBS in an untrusted network. EGIS allows the operator to use a shared DHCP server during autointegration in an untrusted network. The RBS sends an HTTPS request to EGIS, and uses the Vendor Credentials as authentication. The SEG and AIWS addresses are included in the HTTPS response to the RBS. The IP address to EGIS is provided to the RBS by the outer DNS server.

To use EGIS, information regarding the RBS, for example the serial number, must be entered in the EGIS database. The operator must send the RBS information to EGIS and then confirm that the data entered in EGIS is correct. For more information about what information that EGIS requires, see *Add RBS*.

2.3.7 Operation and Maintenance Security Administration Server

OMSAS in OSS-RC provides the following:

- Public Key Infrastructure (PKI) services

  See Section 2.4 on page 10

- Connectivity Packet Platform Authentication and Authorization Service (CAAS) for SLS users

- Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL): LDAPS

  LDAPS handles authentication and authorization requests for users logging on to an RBS on security level 3 through an SLS.

2.3.8 OSS-RC Master Server

The OSS-RC Master Server stores the configuration parameters before the autointegration starts. During the integration process, the parameters are fetched automatically when the ICF is built. The ICF is uploaded to the AIWS server from where the RBS can download the file.

2.3.9 OSS-RC Network Resource Model

ONRM on the OSS-RC master server is the common data store where topology, connectivity, and security data are modeled for the entire network to be managed.

BSIM and OMSAS interact with ONRM in the autointegration process.

2.3.10 Performance Management Support Service

The OSS-RC performance management support service automatically identifies and updates user-defined statistics profiles and user-defined cell trace profiles with the new RBSs to be monitored. Reporting of counters and cell traces are activated in added RBSs based on the profiles, see *Performance Management* and *Subscription Profiles and Performance Monitoring User Guide* in the OSS-RC library.

2.3.11 Security Configuration Service

Security Configuration Service (SCS) in OSS-RC handles security configuration operations on RBS nodes. This includes installation of certificates, and installation of local authentication and authorization database files.

BSIM requests security configurations from SCS. SCS coordinates the communication between BSIM, ONRM, and OMSAS. The service also synchronizes ONRM with the authentication and authorization database on OMSAS.

2.3.12 SMRS

The SMRS server is the Secure File Transfer Protocol (SFTP) server for storage of the software upgrade package (UP).

SMRS is configured with individual user accounts. To configure user accounts in SMRS, see the OSS-RC documentation.

2.3.13 ENIS

The Ericsson Node Integration Scanner is the Android application used by the field technician to initiate integrations at RBS sites. No laptop is needed.

The ENIS application scans the QR code of the work order and the barcode on the RBS, and sends the information to OSS-RC.

Read more about the ENIS in *Ericsson Node Integration Scanner* in the OSS-RC library.

2.3.14 ORI

The On-Site RBS Integrator (ORI) is a Graphical User Interface (GUI) in the RBS software.

ORI is used in autointegration with laptop to download the Combined file from the laptop to the RBS.

For more information regarding ORI, see *Integrating RBSs On-Site Using ORI*.

2.4 Certificate Enrollment

The PKI services provide certificates for activation of O&M security and IPSec. RBSs send certificate enrollment requests to OMSAS using the Certificate Management Protocol version 2 (CMPv2). The requests are administrated by the Registration Authority (RA) and digital certificates for public keys are signed by the Certificate Authority (CA). Signed certificates are returned to RBSs and are necessary for activation of O&M security and IPSec.

For more information, see*IP Security* and *Security for O&M Node Access*.

2.5 Software Upgrade

Software Upgrade is used to add new functions to the RBS, to improve performance or to correct software faults. Both new or updated Load Modules (LMs) are included in the upgrade scope.

Directly after a software upgrade, a data conversion is performed. That is, a synchronization between deprecated and new Managed Object Model (MOM) parameters is made. Data conversion is only supported during upgrade to a new software release.

For more information, see*Software Management*.

2.6 Software and Configuration Files

This section describes the software and configuration files involved in the autointegration process.

Table 2 shows where the files are stored.

Table 2 Storage Location of Software and Configuration Files used in Autointegration

File Type	Type of Data	Storage Location
Basic Software Package	Factory installed RBS software	RBS
Upgrade Package (UP)	For upgrade of the RBS software	SMRS server

Table 2 Storage Location of Software and Configuration Files used in Autointegration

File Type	Type of Data	Storage Location
Initial Configuration File (ICF)	For initial configuration of the RBS, IP transport, Internet Protocol Security (IPSec), and servers for management and control	The following locations: • OSS-RC master server • AIWS server When autointegration starts, the ICF is built with data from the ICF Template on the OSS-RC master server. Data sources like DHCP and DNS servers can also be included. The ICF is then uploaded to the AIWS server and downloaded to the RBS
Site Installation file	The Site installation file contains temporary IPSec configuration data, VLAN ID and AIWS server address. The content of the Site Installation file are used for initial autointegration scope only.	Client laptop, as a part of the Combined file.

3 Parameters

This section describes parameters introduced by the RBS Autointegration function and parameters affected when using the function.

Integrating an RBS in an LTE RAN is basically to set all parameters necessary for making the RBS a unique network element ready to carry traffic. Parameters in interfacing network elements must also be set.

3.1 Introduced Parameters

This section provides a brief description of the parameters introduced with RBS Autointegration.

BSIM operates on substitution variables in the ICF template. Percentage characters (%) indicate the substitution variables.

The xml elements in the ICF template corresponds to Managed Objects (MOs) and attributes in the Managed Object Model (MOM). Refer to the Section 7.3 on page 23 and *Managed Object Model (MOM) RBS* for attribute descriptions.

For details about autointegration parameters, refer to *Pico OSS End to End Description* and *BSIM, Base Station Integration Manager, User Guide* in the OSS-RC library.

3.2 Affected Parameters

This function does not affect the use of any parameters other than the ones already listed in Section 3.1 on page 13.

3.3 Parameters to Set when Adding RBSs

This section summarizes where to find information about parameters to set when adding RBSs to a network using RBS Autointegration.

Table 3 gives an overview of configuration files and parameter descriptions.

Table 3 Configuration Files

Configuration File Type	Parameters Described in...	For Parameter Import to...
ICF	*Managed Object Model (MOM) RBS*(1).	RBS
RBS node	The OSS-RC document *BSIM, Base Station Integration Manager, User Guide*	OSS-RC

(1) Described also in Section 7.3 on page 23

Parameters to set are entered through BSIM. Default values or network-common values are used for most parameters, leaving a small amount of RBS-unique values to set.

3.4 DNS Configuration

A DNS server used as a complement to a DHCP server to resolve the IP addresses to the AIWS, and if IPSec is used, the IP address to the Security Gateway (SEG).

This section lists parameters possible to set with DNS queries. See Table 4.

3.4.1 Neighboring eNodeB Lookup

An RBS can automatically set up X2 interfaces to other eNodeBs. The RBS constructs an eNodeB domain name based on the global eNodeB identity of the neighboring eNodeB. The global eNodeB identity is based on Mobile Country Code (MCC), Mobile Network Code (MNC), and eNodeB identity, see *3GPP TS 36.413*. The RBS sends the eNodeB domain name to the DNS server, which returns IP addresses for the neighboring eNodeB.

For automatically created MO structures and MO naming conventions, see *X2 Configuration*.

3.4.2 DNS Communication

DNS servers must be configured to respond to the queries and map host names or domain names to IP addresses. Table 4 specifies the queries and the resulting parameter setting. Table 5 specifies the formats of domain names and IP addresses in the DNS communication. Data formats and DNS communication are further specified in *RFC 1035* and in *3GPP TS 23.003*.

Table 4 DNS Queries and RBS Parameters

In DNS Query	DNS Answer
AIWS domain name	IP address to the AIWS

Table 4 DNS Queries and RBS Parameters

In DNS Query	DNS Answer
SEG domain name	IP address to the SEG
EGIS domain name	IP address to EGIS

Table 5 Data Format in the DNS Communication

In DNS Queries and Responses	Format
IP address	D.c.b.a in format IN-ADDR.ARPA as specified in *RFC 1035*. D.c.b.a is the IP address a.b.c.d in reversed byte order.
AIWS domain name	`aiws.ai.ericsson`
SEG domain name	`secgw.ai.ericsson` or `secgw.ai.domain`. `domain` must be replaced by the appropriate domain name.

3.5 DHCP Configuration

The Dynamic Host Configuration Protocol (DHCP) provides an internal framework for passing configuration information in the network. Configuration parameters are carried in tagged data items stored within protocol messages exchanged between the DHCP server and its clients. These data items are called options. Standard DHCP options are defined in *RFC 2132*.

Table 6 shows the RBS parameters supported in DHCP communication:

Table 6 Parameters in the Communication between RBSs and DHCP Server

DHCP Option	Description
Option code 1	The DHCP server subnet mask
Option code 3	The Default Gateway IP address
Option code 6	The DNS server IP address
Option code 15	The DNS server domain name
Option code 43	The Wi-Fi Controller (WIC) IP address Only required if RBS is equipped with optional Wi-Fi unit, and if the address is not configured in DNS server

Table 6 Parameters in the Communication between RBSs and DHCP Server

DHCP Option	Description
Option code 72	The AIWS server IP address The address can also be resolved using DNS The port is hard coded to `2497` in the RBS
Option code 241	The SEG IP address Only required if IPSec is used The address can also be resolved using DNS

4 Network Impact

This function is not affecting traffic capacity, coverage, or handover. However, autointegration sets parameters for several system functions and features, based on the planned radio network and transport network defined in OSS-RC. The parameters affect the performance of the network in several ways but this is not within the scope of this document.

Processing capacity and storage capacity in OSS-RC:

- Up to 100 RBSs processed in one batch, including generating and storing the configuration files.
- OSS-RC can handle autointegration of five RBSs simultaneously. Additional integration requests are queued.

Fore more information, refer to *BSIM, Base Station Integration Manager, User Guide* and *BSIM, Base Station Integration Manager, System Administrator Guide* in the OSS-RC library.

5 Associated Features and Affected Functions

This section describes how RBS Autointegration affects other features and functions.

5.1 Prerequisite Features

There are no prerequisite features for RBS Autointegration.

5.2 Affected Features

This function does not affect any other feature.

5.3 Affected System Functions

No system functions are affected by this function.

6 Performance

There are no counters, events or Key Performance Indicator (KPI) definitions associated with this function.

The RBS logs the integration results in the `AutointegrationLog` file. The log contains information about autointegration activities and status.

In OSS-RC, the log file is accessible using the following file system path:

`/oss/permanent/AutointegrationLog.txt`

6.1 KPIs

This feature has no associated Key Performance Indicators (KPIs).

6.2 Counters

This feature has no directly associated counters.

6.3 Events

This feature has no directly associated events.

7 O&M Information

This section describes how to activate and use the autointegration function.

7.1 Activating the Feature

This feature introduces a new licensed feature in OSS-RC: The BSIM.

To install the license, see the OSS-RC document *BSIM, Base Station Integration Manager, User Guide*.

There is no other activation of the function, but services in OSS-RC must be available as indicated in Section 2.1 on page 6.

7.2 Using the Function

For an overview of the process of adding an RBS, see document *Add RBS*.

For an overview of activities in OSS-RC, see *BSIM, Base Station Integration Manager, User Guide* in the OSS-RC Library.

To prepare configuration file templates in OSS-RC, see *OSS Utility Services, User Guide* in the OSS-RC Library.

For integration activities on the RBS site, see *Integrating RBSs On-Site Using ENIS*.

For ICF template example files, see the following files:

- Without IPSec. See *ICF Template without IPSec*
- With IPSec. See *ICF Template with IPSec*

7.3 Appendix - ICF Parameters

Table 7 ICF Parameters Description

XML Element Name	Substitution variable	Mapping to MOM	Dependency	Individual Value per			Mandatory	Value Provisioning	Value Example
				Node	Batch	Network			
dnPrefix	%dnPrefix%	*ManagedElement.dnPrefix*	Provides additional naming context that allows the managed objects to be partitioned into logical domains.	x			Yes	Yes - Special Handling	SubNetwork=ONRM_RootMo_R,SubNetwork=RNC01,
networkManagedElementId	%Node Name%	*ManagedElement.networkManagedElementId*	Must match RDN of the node.	x			Yes	Yes - Auto provisioning function	RBS78
eNBId	%eNBId%	*ENodeBFunction.eNBId*	The next free sequence number. Before the eNB ID is set, the ID is checked by ONRM to see if it is unique.	x			Yes		50
mcc	Dummy values used - Input needed	*PlmnIdentity.mcc*	Operator must define a valid value.		x		Yes - For a golden template	No	344
mnc	Dummy values used - Input needed	*PlmnIdentity.mnc*	Operator must define a valid value.		x		Yes - For a golden template	No	20
mncLength	Dummy values used - Input needed	*PlmnIdentity.mncLength*	Operator must define a valid value.		x		Yes - For a golden template	No	2
eUtranCellFDDId	%Node Name%_EutranCellFDD_1	*EUtranCellFDD.eUtranCellFDDId*		x			Yes	Yes - Auto provisioning function	RBS78_EutranCell_1
alpha	Smart Defaults used	*EUtranCellFDD.alpha*			x		No	Smart Defaults used	8
administrativeState	Smart Defaults used	*EUtranCellFDD.administrativeState*			x		Yes	No	UNLOCKED
earfcndl	Dummy values used - Input needed	*EUtranCellFDD.earfcndl*	Defines a valid value for a batch-specific template.			x	Yes - For a golden template	No	150
earfcnul	Dummy values used - Input needed	*EUtranCellFDD.earfcnul*	earfcndl+18000			x	Yes - For a golden template	No	1950

Table 7 ICF Parameters Description

XML Element Name	Substitution variable	Mapping to MOM	Dependency	Individual Value per			Mandatory	Value Provisioning	Value Example
				Node	Batch	Network			
cellId	%FDDcellId%	*EUtranCellFDD.cellId*	RBS internal ID attribute for EUtranCell. Must be unique in the RBS.	x			Yes	Yes - Auto provisioning function	2
dlChannelBandwidth	Smart Defaults used	*EUtranCellFDD.dlChannelBandwidth*				x	No	Smart Defaults used	10000
physicalLayerCellIdGroup	%physicalLayerCellIdGroup%	*EUtranCellFDD.physicalLayerCellIdGroup*	Value range: { 0..167 } A sequence with one unique number for every EUtranCellFDD that is created.	x			Yes	Yes	50
physicalLayerSubCellId	Dummy values used - Must be updated by using PCI SON function	*EUtranCellFDD.physicalLayerSubCellId*	Value range: { 0..2 } Will be updated by OSS functions to valid value. A sequence with one unique number for every EUtranCellFDD that is created.		x		Yes	No	2
pMaxServingCell	Smart Defaults used	*EUtranCellFDD.pMaxServingCell*			x		No	Smart Defaults used	-30
pZeroNominalPucch	Smart Defaults used	*EUtranCellFDD.pZeroNominalPucch*			x		No	Smart Defaults used	-100
pZeroNominalPusch	Smart Defaults used	*EUtranCellFDD.pZeroNominalPusch*			x		No	Smart Defaults used	0
qQualMin	Smart Defaults used	*EUtranCellFDD.qQualMin*			x		No	Smart Defaults used	-34
qQualMinOffset	Smart Defaults used	*EUtranCellFDD.qQualMinOffset*			x		No	Smart Defaults used	0
qRxLevMin	Smart Defaults used	*EUtranCellFDD.qRxLevMin*			x		No	Smart Defaults used	-65
qRxLevMinOffset	Smart Defaults used	*EUtranCellFDD.qRxLevMinOffset*			x		No	Smart Defaults used	1000
tac	%FDDtac%	*EUtranCellFDD.tac*				x	Yes	No	12594

Table 7 ICF Parameters Description

XML Element Name	Substitution variable	Mapping to MOM	Dependency	Individual Value per			Mandatory	Value Provisioning	Value Example
				Node	Batch	Network			
partOfSectorPower	Smart Defaults used	*EUtranCellFDD.partOfSectorPower*			x		No	Smart Defaults used	100
qHyst	Smart Defaults used	*SIB3.qHyst*			x		No	Smart Defaults used	4
a3offset	Smart Defaults used	*ReportConfigEUtraBestCell.a3offset*			x		No	Smart Defaults used	30
hysteresisA3	Smart Defaults used	*ReportConfigEUtraBestCell.hysteresisA3*			x		No	Smart Defaults used	10
eUtranCellFDDId	%NodeName%_EutranCellFDD_2	*eUtranCellFDD.eUtranCellFDDId*	x				Yes	Yes - Auto provisioning function	RBS78_EutranCell_2
physicalLayerCellIdGroup	physicalLayerCellIdGroup2	*eUtranCellFDD.physicalLayerCellIdGroup*	Value range: { 0..167 } A sequence for every EUtranCellFDD that is created for a node must be unique.	x			Yes	Yes	100
ipAddress1	%TermPointToMmeipAddress1%	*TermPointToMme.ipAddress1*			x		Yes	Smart Defaults used	12.2.3.42
ipAddress2	%TermPointToMmeipAddress2%	*TermPointToMme.ipAddress2*			x		Yes	Smart Defaults used	12.2.3.43
administrativeState	Smart Defaults used	*TermPointToMme.administrativeState*			x		No	No	UNLOCKED
vlanId	Dummy values used - Input needed	*VlanPort.vlanId*	Defines a valid value for a batch specific template.			x	No	No	2201
address	%OAMSecurityGateWayAddress%	*PeerIPv4.address*				x	Yes - If IPSec is used	No	12.2.3.45
address	%trafficSecurityGateWayAddress%	*PeerIPv4.address*				x	Yes - If IPSec is used	No	12.2.3.45
syncServerNetwork	Must be updated if synchronization servers accessed through IPSec	*Synchronization.syncServerNetwork*	Update to PRIVATE if Sync servers accessed through traffic VLAN.			x	Yes - For a golden template	No	PUBLIC

Table 7 ICF Parameters Description

XML Element Name	Substitution variable	Mapping to MOM	Dependency	Individual Value per			Mandatory	Value Provisioning	Value Example
				Node	Batch	Network			
administrativeState	Smart Defaults used	*SyncServer.administrativeState*				x	Yes	No	UNLOCKED
ServerAddress	PTPorNTPsyncServerAddress1	*SyncServer.ServerAddress*				x	Yes	No	12.2.3.42
protocol	Smart Defaults used	*SyncServer.protocol*				x	No	Smart Defaults used	NTP
administrativeState	Smart Defaults used	*SyncServer.administrativeState*				x	Yes	No	UNLOCKED
ServerAddress	PTPorNTPsyncServerAddress2	*SyncServer.ServerAddress*				x	Yes	No	12.2.3.43
protocol	Smart Defaults used	*SyncServer.protocol*				x	No	Smart Defaults used	NTP
administrativeState	Smart Defaults used	*SyncServer.administrativeState*				x	No	No	UNLOCKED
administrativeState	Smart Defaults used	*LdapAuthenticationMethod.administrativeState*	Must match LDAP account created in OSS.			x	Yes	No	UNLOCKED
ldapIpAddress	%LDAPIpAddress%	*Ldap.ldapIpAddress*	Must match LDAP account created in OSS.			x	Yes	No	12.2.3.45
fallbackLdapIpAddress	%fallbackLDAPIpAddress%	*Ldap.fallbackLdapIpAddress*	Must match LDAP account created in OSS.			x	No	No	12.2.3.45
baseDn	%LDAPbaseDn%	*Ldap.baseDn*	Must match LDAP account created in OSS.			x	Yes	No	CN=Users,DC=yourdomain,DC=com
bindDn	%LDAPbindDn%	*Ldap.bindDn*	Must match LDAP account created in OSS.			x	Yes	No	cn=administrator,cn=Users,dc=domain,dc=com
bindPassword->cleartext	<bindPassword struct ="EcimPassword"><cleartext/><password>%LDAPbindPassword%</password></bindPassword	*Ldap.bindPassword*	Must match LDAP account created in OSS.			x	Yes	No	true

Table 7 ICF Parameters Description

XML Element Name	Substitution variable	Mapping to MOM	Dependency	Individual Value per			Mandatory	Value Provisioning	Value Example
				Node	Batch	Network			
subjectName	%nodeCredentialDn%	*NodeCredential.subjectName*	Operator domain part for subject of certificates to be enrolled.			x	Yes	No	C=SE,O=Ericsson
renewalMode	Smart Defaults used	*NodeCredential.renewalMode*				x	Yes	No	AUTOMATIC
subjectName	%nodeCredentialDnIPsec%	*NodeCredential.subjectName*	Operator domain part for subject of certificate(s) to be enrolled			x	Yes	No	C=SE,O=Ericsson
enrollmentAuthorityName	%tlscertAuthDn%	N/A	Identity of the enrollment TLS CA provided by specifying its X.509 DN.			x	Yes	No	OU=ericssonOAM,O=Ericsson,CN=atclvm668NECertCA
enrollmentAuthorityName	%ipseccertAuthDn%	N/A	Identity of the enrollment IPSec CA provided by specifying its X.509 DN.			x	Yes	No	O=Ericsson,CN=LTEIPSecNEcusRootCA
uri	%TLSenrollmentServerAddressUri%	*EnrollmentServer.uri*	Must match OSS PKI RA server IP address and port.			x	Yes	Yes- Special Handling	1.2.3.4:26772
uri	%IPsecenrollmentServerAddressUri%	*EnrollmentServer.uri*	Must match OSS PKI RA server IP address and port.			x	Yes	Yes- Special Handling	1.2.3.4:26772
address	%snmpTargetAddress%	*SnmpTargetV3.address*	Must Match OSS SNMP Manager.			x	Yes	No	12.2.3.42
serverAddress	%primaryNtpServerAddress%	*NtpServer.serverAddress*				x	Yes	No	12.2.3.42
serverAddress	%secondaryNtpServerAddress%	*NtpServer.serverAddress*				x	Yes	No	12.2.3.42
uri	%softwarePackageURI%	*SwM.createUpgradePackage*	Must match SWP installed on OSS.		x		Yes	Yes - Auto provisioning function	sftp://<Unique NodeID>@<SMRS_MASTER>:. //CORE/CommonPersistent/Software/7UXxpL5ZWKMRp3zeAs-I6Mu4j9c/

Table 7 ICF Parameters Description

XML Element Name	Substitution variable	Mapping to MOM	Dependency	Individual Value per			Mandatory	Value Provisioning	Value Example
				Node	Batch	Network			
password	%SMRSPassword%	*SwM.createUpgradePackage*	Must match SFTP account created on OSS.	x			Yes	Yes - Auto provisioning function	"dasfasrwer"
ipAddress1	%TermPointToMmeipAddress1%	*TermPointToMme.ipAddress1*			x		Yes	Yes	12.2.3.42
confOutputPower	Smart Defaults used	*SectorEquipmentFunction.confOutputPower*			x		No	Smart Defaults used	330