

Add RBS

DESCRIPTION

Copyright

© Ericsson AB 2013 - 2015. 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
2	Prerequisites	3
2.1	Network	3
2.2	Services	4
2.3	Licenses	5
2.4	Documentation	5
3	Autointegration Process Overview	7
3.1	Network Topologies	7
4	End-to-End Workflow for Adding RBSs	11
4.1	Network Provisioning	11
4.2	Node Provisioning	15
4.3	Node Commissioning	16
4.4	Node Integration	16
5	Autointegration	17
5.1	Flowchart for Autointegration without Laptop	17
6	Semi-Automated Integration	25
6.1	Semi-Automated Integration Process	25
6.2	Stand-Alone Integration	27
6.3	Warehouse Installation	29



Add RBS



1 Introduction

This document provides an overview of how to add an RBS using autointegration, with and without laptop. Deployment for both trusted and untrusted networks is described. The semi-automated integration process is also described.

The process of adding an RBS using autointegration divides into the following steps:

- Network Provisioning. See Section 4.1 on page 11.

This section describes the configuration and preparations that must be made in the Operations Support System for Radio and Core (OSS-RC) and Transport Network before deploying the RBSs.

- Node Provisioning. See Section 4.2 on page 15.

The procedures in this section are performed using the Base Station Integration Manager (BSIM). BSIM is part of the OSS-RC feature FAJ 121 1298: RBS Auto-Provisioning (RAP).

- Node Commissioning. See Section 4.3 on page 15.

The following options can be used to bind the Hardware (HW), that is, to connect the HW serial number with OSS-RC RBS logical name:

- Automatic binding using the Ericsson Node Integration Scanner (ENIS).
- Manual binding, where the RBS serial number is entered manually in OSS-RC.

- Node Integration. See Section 4.4 on page 16.

The following options can be used for node integration:

- Autointegration - With or without laptop
- Semi-automated integration
- Stand-Alone Integration

Note: It is out of the scope of this document to provide details of each step of the process. Further details of each step of the process can be found in referenced documentation. See the relevant sections and Section 2 on page 3.

Figure 1 shows the different stages in the process of adding an RBS.

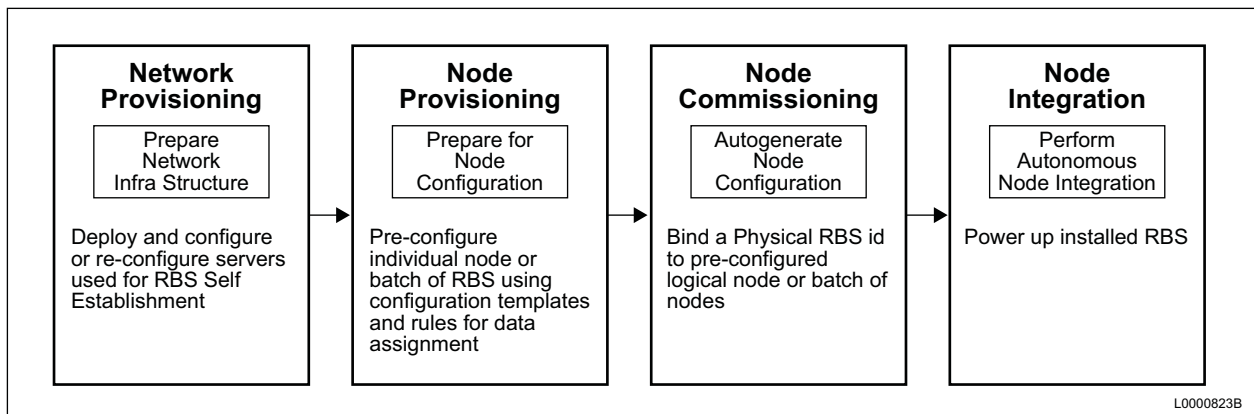


Figure 1 Process Overview



2 Prerequisites

This section describes the prerequisites that must be fulfilled in different parts of network before starting integration activities.

2.1 Network

To add an RBS to the network using RBS autointegration, the following conditions must be met:

- The OSS-RC is upgraded to enhanced deployment and the necessary infrastructure is deployed, as specified in Section 2.2.
Note: It is recommended to contact Ericsson to perform the upgrade to enhanced deployment.
- The Mobility Management Entity (MME) is installed, enabled, and prepared with tracking areas.
- The Transport Network is available for Operation and Maintenance (O&M) traffic, control plane traffic, and user plane traffic.
- Transport Network is equipped with Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Remote Authentication Dial-In User Service (RADIUS) servers as specified in Section 3.1 on page 7 to handle IP address allocation and Transport Network connectivity.

Note: For the semi-automated integration procedure, integration without the use of DHCP and DNS servers is an option. See Section 6 on page 25.

- Synchronization information is available. Possible synchronization methods are Global Positioning System (GPS), Precision Time Protocol (PTP), and Network Time Protocol (NTP).
- The RBS has Ericsson vendor credentials. The vendor credentials are used for initial secure identification in OSS-RC during the integration process and are stored by Ericsson during the manufacturing. The Security Gateway (SEG) configured to verify that the RBS has a trusted Ericsson vendor root certificate installed.
- If clusters are to be used, they must be set up in OSS-RC using Common Explorer (CEX). Refer to *CEX, OSS Common Explorer, User Guide* in the OSS-RC library.
- If deploying with IPsec, the following is required:
 - SEG



- The MSRBS-V1 managed elements Basic Software Package version must be compatible with the Upgrade Package (UP). For compatible software versions, refer to Release Notes.
- An Simple Mail Transfer Protocol (SMTP) mail server for hardware binding is installed and configured. Refer to *Pico OSS End to End Description* in the OSS-RC library.

Note: The mail server is only needed if ENIS is used to initialize the integration.

- If Ericsson Global Integration Service (EGIS) is to be used during autointegration in an untrusted network, an internet-connection must exist.
- To use EGIS, information needed during the autointegration must be added in EGIS, see Section 4.1.10 on page 14.

2.2 Services

In OSS-RC, the following services must be available:

- OSS system updated to version O14.1A or later
- Software Management Repository Services (SMRS) with individual user accounts and a stored UP version
- Registration Authority (RA) service for operator certificate enrollment
- Autointegration Web Service (AIWS)

Note: AIWS can be omitted in semi-automated integration, See section Section 6 on page 25.

In OSS-RC, the following security services must be available:

- Operation and Maintenance Security Administration Server (OMSAS) with Certificate Signing Authority (CSA) based Public Key Infrastructure (PKI) services and Connectivity Packet Platform Authentication and Authorization Service (CAAS)
- Security Configuration Service (SCS)
- Single Logon Server (SLS) prepared with individual user accounts, that must have CAAS access profiles

For security information, refer to *Security Management* and *Security System Administration Guide, OSS-RC* in the OSS-RC library.



2.3 Licenses

To provide the required OSS-RC functionality, the license for FAJ 121 1298: RBS Auto-Provisioning (RAP) must be installed and activated. Refer to *License Key Administration in OSS-RC* in the OSS-RC library.

2.4 Documentation

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*
- *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*



Add RBS



3 Autointegration Process Overview

This section gives an overview of the process of adding RBSs using autointegration.

3.1 Network Topologies

Figure 2 and Figure 3 present a high-level topology description of the applications and network elements involved when performing an autointegration using ENIS.

Figure 2 shows a topology without IPSec, that is, a trusted network. The untrusted network topology with IPSec is presented in Figure 3.

Note: In the semi-automated integration, inner and outer DNS server can be omitted. Also the inner DHCP/RADIUS server and outer DHCP server are possible to omit.

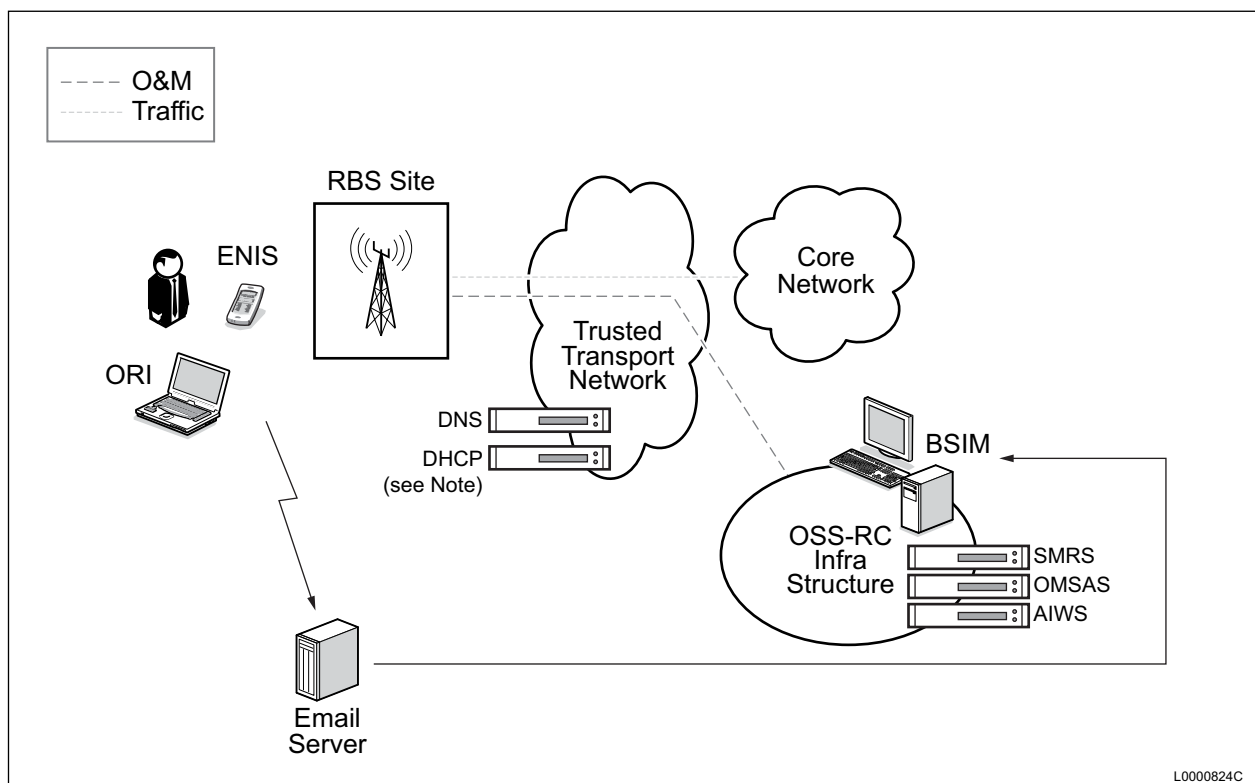


Figure 2 Network Topology - Trusted Network without IPSec

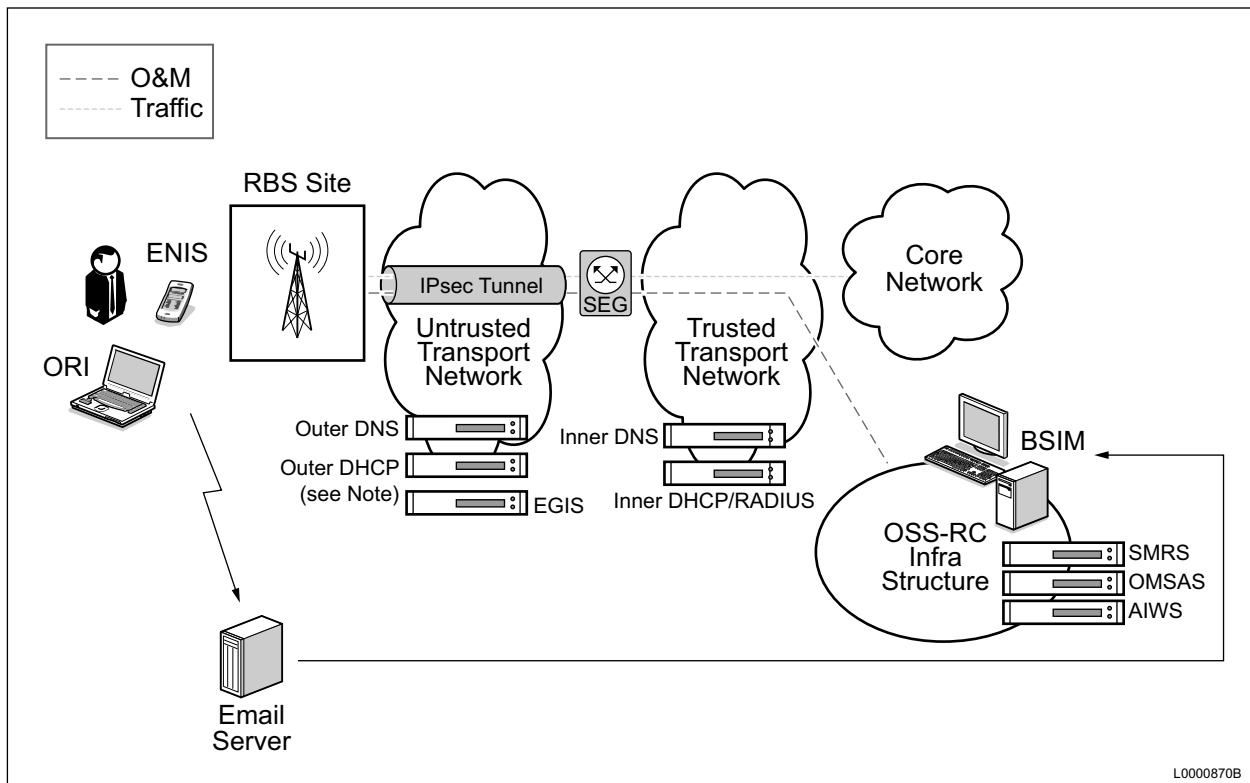


Figure 3 Network Topology - Untrusted Network with IPsec

The following abbreviations are used in the illustrations:

AIWS	Autointegration Web Service
BSIM	Base Station Integration Manager
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EGIS	Ericsson Global Integration Service
ENIS	Ericsson Node Integration Scanner
O&M	Operation and Maintenance
OMSAS	Operation and Maintenance Security Administration Server
ORI	On-Site RBS Integrator
OSS-RC	Operations Support System for Radio and Core
RADIUS	Remote Authentication Dial-In User Service



RBS	Radio Base Station
SEG	Security Gateway
SMRS	Software Management Repository Services



Add RBS



4 End-to-End Workflow for Adding RBSs

This section describes the end-to-end workflow for adding RBSs using autointegration. Before starting the process, make sure that the prerequisites listed in Section 2 on page 3 are fulfilled.

4.1 Network Provisioning

This section describes the setup and configuration of servers that need to be performed before node provisioning can start.

The following users are involved in the autointegration process:

Field Technician: Performs all activities at the RBS site.

Integration Engineer: Plans the RBS integration and prepares configuration data and involved servers and services. The process described in this document involves Integration Engineers from OSS, Radio and Transport Network.

OMC Technician: Monitors the network from an Operation and Maintenance Center (OMC). Alarm management is one of the main tasks.

4.1.1 Preparation in OSS-RC

This section lists pre-integration preparations. Refer to the instructions in *Pico OSS End to End Description* in the OSS-RC library to perform the procedures:

1. Configure the number of RBS nodes on the OSS-RC master server.
2. Implement Core Configuration.
3. Configure the AIWS. This step includes the BSIM jks creation file since this file is needed to establish communication between BSIM and the AIWS.

For information regarding the BSIM jks creation file, see *Ericsson Node Integration Scanner (ENIS)*.

4. Configure the SMRS.
5. Confirm that the Certificate Distribution Point (CDP) is defined in the DNS server and in the certificates.
6. Enable support for Common Operation and Maintenance (COM). The OSS-RC COMInf infra server must be running with COM enabled.



7. Check that the security certificates contain a Subject Alternative Name (SAN) value.
8. If the SAN value is missing, reconfigure the CDP and SAN.
9. Download the latest software UP through the SHM/NSS GUI.
10. Prepare the OSS-RC for Ericsson vendor certificates. The vendor credentials are used for initial secure identification in OSS-RC during the integration process and stored by Ericsson during manufacturing.
11. Prepare NETCONF (COM user). The COM user must be assigned a proper role before integration starts.
12. If deploying with IPsec, prepare the connection between the SEG and OSS-RC on the OMSAS. This step requires that the needed certificates are signed by the OSS-RC Security Authority (CA) and transferred and installed on the SEG.

4.1.2 DHCP Configuration

The DHCP configuration ensures RBS IP connectivity to the Transport Network and O&M during integration. Depending on SEG implementation in the IPsec solution, two DHCP servers can be deployed: one outer DHCP located in the untrusted transport network and one inner DHCP in the trusted transport network. See Figure 3.

This step can be performed using IPworks, the Ericsson supplied product for standard DNS and DHCP service.

For more information about the DHCP servers, see Section 5 on page 17 and *IP Transport*.

Note: For IP connectivity to work, the router closest to the RBS must be configured to support relay of DHCP messages, or the DHCP server must be in the same Ethernet broadcast domain as the RBS.

As a complement, a DNS can resolve the IP addresses to the AIWS, and if IPsec is used, the IP address to the Security Gateway (SEG).

Note: The DNS and DHCP servers are non-OSS-RC equipment.

Refer to *IP Transport* and *RBS Autointegration* for information on DNS and DHCP server settings.

4.1.3 RADIUS

Remote Authentication Dial In User Service (RADIUS) is a protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service. In the IPsec solutions in Figure 3, the RADIUS server is used to allocate inner IP addresses of the RBS. One inner IP address will terminate the S1/X2 connection and the



two other inner IP addresses will terminate a temporary or permanent O&M connection from OSS-RC.

For more information regarding RADIUS, refer to *RFC 2865* and *RFC 2866*.

4.1.4 Security Gateway

A Security Gateway (SEG) is an IPSec supported device used to encrypt and decrypt data between a trusted and a untrusted network.

The SEG must support IKEv2 Configuration Payload (CP) for assigning inner IP addresses using an IP address pool. The pool can be implemented by the SEG in various ways, for example, using a RADIUS or a DHCP service, or both.

Note: For the semi-automated integration procedure, it is sufficient that the SEG supports only IKEv2. The additional IKEv2 CP is not used. See section Section 6 on page 25.

Refer to *IP Transport* and *RBS Autointegration* for generic information on SEG settings.

For detailed information, refer to the vendor's product information.

4.1.5 Initial Configuration File Template Preparation

Populate the Initial Configuration File (ICF) template delivered with BSIM with relevant operator network values.

The xml elements in the ICF template corresponds to Managed Objects (MOs) and attributes in the Managed Object Model (MOM). See *RBS Autointegration* and *Managed Object Model (MOM) RBS* for descriptions of the attributes.

Elements must be removed from the ICF template depending on Transport Network configuration, refer to *IP Transport* for more information.

BSIM operates on substitution variables in the ICF template. Percentage characters (%) indicate the substitution variables. They must normally not be manipulated during this preparation.

For procedures and tools, refer to *Pico OSS End to End Description* and *BSIM, Base Station Integration Manager, User Guide* in the OSS-RC library.

4.1.6 Mail Server Configuration

The server is external to, but accessible from OSS-RC. The mail server is used to send email to and from the ENIS application. Since the server is not Ericsson property, documentation provides general guidelines only.



Note: The mail server, independent of vendor, must support clients using POP3/IMAP and SMTP over TLS. This presents no security risk since OSS-RC is properly safe guarded and ENIS messages are encrypted using Secure/Multipurpose Internet Mail Extensions (S/MIME).

Refer to *Pico OSS End to End Description* for more information.

4.1.7 **BSIM Mail Client Configuration**

This section summarize the activities for configuration of the BSIM mail client. For procedures, refer to *Pico OSS End to End Description* and *BSIM, Base Station Integration Manager, System Administrator Guide* in the OSS-RC library.

1. Set up Telecom Security Services (TSS). Selected protocols require passwords to access the mail server. These passwords are associated with BSIM email accounts and must be stored in TSS.
2. Set up security context. Both BSIM and ENIS mail clients must have a private key and corresponding certificates. These are handled by the security administrator on OMSAS.
3. Configure BSIM and mail server communication. For BSIM to communicate with the mail server, parameters must be set on the OSS-RC master server.

4.1.8 **BSIM Configuration File Generation**

The .bsim configuration file is not delivered with the BSIM application but created from the OSS-RC master server. Refer to *Pico OSS End to End Description* and *BSIM, Base Station Integration Manager, System Administrator Guide* in the OSS-RC library.

4.1.9 **ENIS Installation**

This section summarizes the installation of the Ericsson Node Integration Scanner (ENIS) application and .bsim configuration file. The ENIS application runs on Android smartphones and initiates the autointegration by binding the RBS hardware identity with generated RBS configuration data. Refer to *Ericsson Node Integration Scanner (ENIS)* for system requirements and details of how to install ENIS.

1. Install the ENIS application on Android smartphone.
2. Once the ENIS application is installed, copy the .bsim configuration file onto the smartphone's SD card.

4.1.10 **EGIS Preparation**

EGIS can provide the SEG and the AIWS server addresses when a node is autointegrated in an untrusted network.



EGIS consists of a database and an HTTPS server. The HTTPS server acts as an interface between EGIS and the RBS.

For an RBS to receive the AIWS and SEG addresses from EGIS, the operator must send the following information to the EGIS-operator:

- The node serial number
- The SEG address to be used at integration
- The AIWS address to be used at integration

The operator must confirm that the data entered in EGIS is correct.

4.2 Node Provisioning

This section summarizes the node provisioning activities. Node provisioning is performed using the OSS-RC feature FAJ 121 1298: RBS Auto-Provisioning (RAP). For procedures, refer to instructions in *Pico OSS End to End Description* and *BSIM, Base Station Integration Manager, User Guide* in the OSS-RC library.

Preparation for node provisioning includes activities as follows:

1. Add the RBS batch
2. Select **Manual** or **Automatic Activation** to control the planned configuration handling
3. Configure node specific information
4. Enter the batch size
5. Configure the RBS
6. Optionally configure RBS termination points for S1 control and user plane and for X2 control plane
7. Configure the autointegration process
8. Check the batch provisioning result
9. Verify the success of the above procedures (1–9)

Following the completion of the preparations for batch provisioning, the field technician goes on site to perform hardware binding, install the RBS, and initialize autointegration. Node provisioning must be successfully completed before node commissioning can start.



4.3 Node Commissioning

This section summarizes the node commissioning activities.

Node commissioning consists of binding the RBS hardware with prepared configuration data. At the site, the field technician uses ENIS to scan the BSIM-generated Quick Response (QR) code on the work order and the serial number barcode on the RBS. Hardware binding can also be performed as an early binding, before going to site. Refer to *Integrating RBSs On-Site Using ENIS* for detailed instructions.

Hardware binding can alternatively be performed using manual binding without the use of ENIS. In this case the RBS serial number is entered manually in OSS-RC before the field technician goes on site. Refer to *Pico OSS End to End Description* in the OSS-RC library.

4.4 Node Integration

This section lists the on-site procedures, including installation, integration, and verification of the RBS. Refer to *Install RBS* for detailed instructions.

For autointegration without laptop, the following steps are included in the procedure:

1. Install and power up the RBS. The autointegration starts automatically when the RBS is powered up. The procedure runs for approximately 10 minutes but can take longer, depending on network performance. The optical indicators provide information on progress. Refer to *RBS Description* for optical indicator information.
2. When the green indicator is on, the integration procedure is finished.
3. Verify autointegration. Check the optical indicators to verify that the hardware is functioning correctly and that the RBS is integrated.

ORI is used for semi-automated integration and for stand-alone integration. ORI is a Graphical User Interface (GUI) in the RBS software. It is used to download the configuration file to the RBS. Refer to *Integrating RBSs On-Site Using ORI*.



5 Autointegration

Autointegration is a function which reduces the workload required to bring a node into service.

For semi-automated integration. See Section 6 on page 25.

5.1 Flowchart for Autointegration without Laptop

The flowchart in Figure 4 gives a high-level overview of a fully automatic autointegration process in an untrusted network with IPSec. IP addresses are set through Dynamic IP Configuration. Some of the steps are SEG implementation specific.

Figure 4 describes the automatic steps in the process with information exchanged between the nodes in the system. These steps are performed at the end of the process of adding the RBS, see Section 4.4 on page 16. Preparations and configuration described in Sections 4.1, 4.2, and 4.3 must be performed before the autointegration process can start.

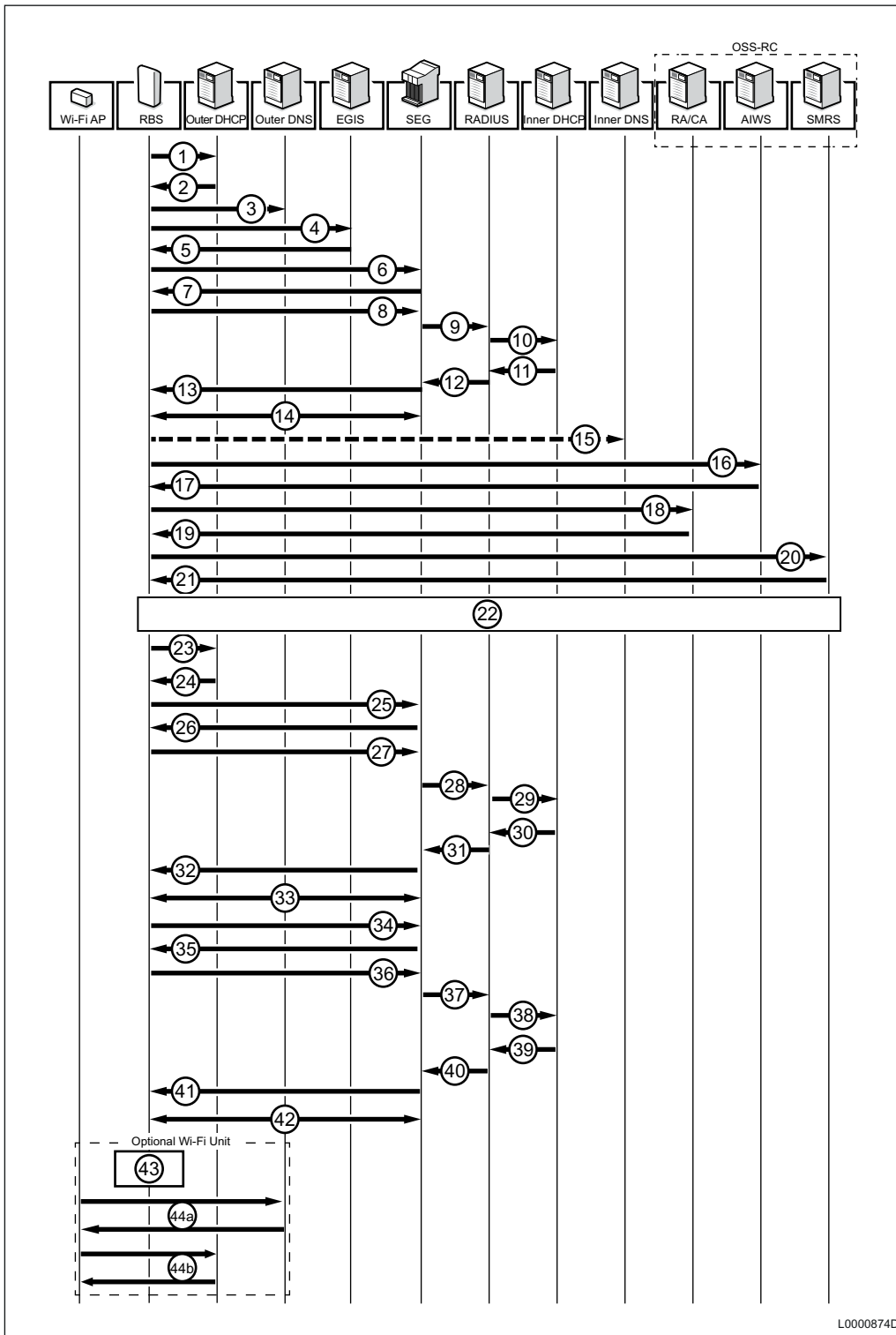


Figure 4 Flowchart Autointegration - IPSec

The autointegration starts when the field technician powers up the RBS. The process is automatic so no intervention from field technician, OMC technician,



or integration engineer is required. The process continues until the RBS is fully configured.

The following automated processing is included:

1. The RBS starts with a Virtual Local Area Network (VLAN) scan to find a DHCP server. The RBS broadcasts a DHCP request message on all VLANs until a DHCP response is received.
2. The outer DHCP server answers with a DHCP response. The response contains an outer IP address and the IP addresses to the SEG, DNS and the AIWS server. For DHCP option values, refer to *IP Transport*.
3. The RBS turns to the DNS to resolve the IP address to EGIS. If the IP addresses in step two are not received from the outer DHCP server, the RBS also queries the DNS to resolve the pre-configured DNS names. Refer to *IP Transport* for more information regarding DNS names.
4. The RBS sends an HTTPS request to EGIS, to resolve the IP addresses to the SEG and the AIWS server.
5. EGIS responds to the HTTPS request. If the data described in Section 4.1.10 on page 14 has been entered in EGIS database, the response includes the IP addresses to the SEG and the AIWS server. The RBS uses the IP addresses to the SEG and the AIWS server from the DHCP or the DNS, if the response from EGIS HTTPS server is any of the following:
 - The IP addresses to the SEG and the AIWS server are not found in EGIS database.
 - EGIS is not active
 - EGIS database is not responding.
6. The RBS sends an IKEv2 request to authenticate itself using the vendor certificate.
7. The SEG uses the Ericsson vendor root certificate to authenticate the RBS and acknowledges the IKEv2 authorization request.
8. The RBS sends an IKEv2 CP request to the SEG to obtain the inner IP address to set up a temporary IPsec tunnel.
9. The SEG requests an IP address for the RBS by sending a RADIUS access request to the RADIUS server.
10. The RADIUS server performs a DHCP discover to obtain an inner IP address for the RBS. The DHCP discover has an IKE ID based on the vendor certificate, as client ID.
11. The inner DHCP server responds with an inner IP address based on the client ID. The response to the RADIUS server also includes the inner DNS IP address.



12. The RADIUS server sends an access accept message to the SEG including the temporary inner IP address and the inner DNS IP address.

Note: Step 9 to 12 can be omitted if the SEG solution does not require an inner DHCP server, that is, the RADIUS server manages the IP pool.

13. The SEG sends an IKEv2 CP response to the RBS including the inner IP address, the inner IP address mask, and the inner DNS IP address in order for the RBS to resolve the nodes in the OSS-RC.
14. A temporary IPsec tunnel is established between the RBS and the SEG.
15. If not received earlier, the RBS resolves the AIWS IP address through the inner DNS.
16. The RBS sends a request to the AIWS for the ICF. The ICF contains Traffic Network and Radio Network configurations.
17. The RBS receives the ICF from the AIWS.
18. The RBS requests operator certificates from OSS-RC. The certificates are used to establish the permanent IPsec tunnel after the RBS reboot, and to communicate securely with OSS-RC over Transport Layer Security (TLS) protocol.
19. The RBS receives the node credentials from Certificate Authority (CA).
20. The RBS sends a request to the SMRS for the software UP to be used by the RBS.
21. The RBS receives the software UP from the SMRS.
22. The RBS reboots in order to load the UP and the ICF and to establish a permanent network connection.
23. The RBS performs a DHCP discovery to obtain an outer IP address.
24. The outer DHCP server provides the RBS with a permanent external IP address, and the default route in order to reach the SEG.
25. The RBS sends an IKEv2 authorization request to authenticate itself using the operator CE-NE certificate.
26. SEG uses the operator root certificate to authenticate the RBS and acknowledges the IKEv2 authorization request.
27. The RBS sends an IKEv2 CP request to the SEG to obtain the inner IP address for setting up a permanent IPsec tunnel for the O&M traffic.
28. The SEG requests an IP address for the RBS by sending a RADIUS access request to the RADIUS server.



29. Upon receiving a request from the SEG, the RADIUS server performs a DHCP discover to obtain an IP address for the RBS.
30. The inner DHCP server responds with a permanent inner IP address based on the client ID. The response to the RADIUS server also includes the inner DNS IP address.
31. The RADIUS server sends an access accept message to the SEG including the permanent inner IP address and the DNS IP address.
32. The SEG sends an IKEv2 CP response to the RBS, including the inner IP address and the DNS IP address. This is done in order for the RBS to establish a permanent O&M traffic connection with the nodes in the OSS-RC.
33. A permanent IPSec tunnel for the O&M traffic is established between the RBS and the SEG.
34. The RBS sends an IKEv2 authorization request to authenticate itself using the operator CE-NR certificate.
35. SEG uses the operator root certificate to authenticate the RBS and acknowledges the IKEv2 authorization request.
36. The RBS sends an IKEv2 CP request to the SEG to obtain the inner IP address for setting up a permanent IPSec tunnel for the Radio Access Network (RAN) traffic.
37. The SEG requests an IP address for the RBS by sending a RADIUS access request to the RADIUS server.
38. After a request from the SEG is received, the RADIUS server performs a DHCP discover to obtain an IP address for the RBS.
39. The inner DHCP server responds with a permanent inner IP address based on the client ID. The response to the RADIUS server also includes the inner DNS IP address.
40. The RADIUS server sends an access accept message to the SEG including the permanent inner IP address and the DNS IP address.
41. The SEG sends an IKEv2 CP response to the RBS, including the inner IP address and the DNS IP address in order for the RBS to establish a permanent RAN traffic connection with the nodes in the OSS-RC.
42. A permanent IPSec tunnel for the RAN traffic is established between the RBS and the SEG. The RBS performs a self-test and then sends a Simple Network Management Protocol (SNMP) trap to OSS-RC to indicate that it is ready for service.

If the RBS is equipped with the optional integrated Wi-Fi module, the following steps are added:

43. The RBS receives the VLAN ID from the ICF.

44. The Wi-Fi Access Point (Wi-Fi AP) receives the Wi-Fi Access Controller (WIC) connection IP address. One of the following alternatives are used:
 - a. The Wi-Fi AP sends a request to the DNS server for the WIC IP address. The DNS server responds with the address.
 - b. The Wi-Fi AP sends a request to the DHCP server for the WIC IP address. The DHCP server responds with the address. Option 43 must be set in the DHCP server.

Once connected, the Wi-Fi AP and the WIC communicate through a Control and Provisioning of Wireless Access Point (CAPWAP) tunnel. Two channels are used: a control and management channel and a data channel. The proprietary Carrier Grade CAPWAP Management (CGCM) protocol is used for communication between Ericsson Wi-Fi APs and a WIC.

For more information regarding the Wi-Fi module, refer to Wi-Fi Solution library.

5.1.1

Node Integration Flow for Autointegration

Figure 5 shows the node integration flow for Autointegration without laptop, starting from Batch Provisioning.

At the start of the integration process, the ICF is downloaded directly from the AIWS server to the RBS.

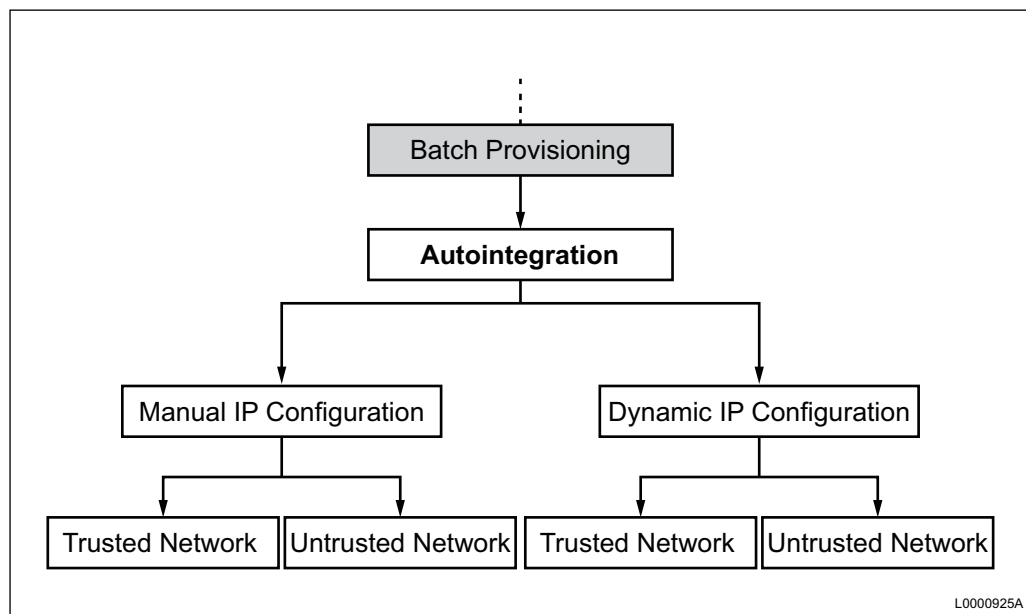


Figure 5 Autointegration Provisioning Scheme

The IP configuration methods are defined the following way:

- Manual IP Configuration



IP addresses for permanent tunnels are entered manually in the ICF. IP addresses for temporary tunnels are resolved through DHCPv4 and IKEv2 CP.

- Dynamic IP Configuration

IP addresses for temporary and permanent tunnel tunnels are resolved through DHCPv4 and IKEv2 CP.

Note: IKEv2 only for untrusted network.



Add RBS



6 Semi-Automated Integration

The semi-automated integration makes it easier to integrate a small number of nodes in an already operating network. It also makes it possible to avoid changes in existing network infrastructure. In the semi-automated integration, a Combined file is stored on a laptop and downloaded to the RBS on site.

The semi-automated integration can also be performed without the need of an OSS-RC access. This procedure is called stand-alone integration. See Section 6.2 on page 26.

The configuration file can also be downloaded to the RBS before the RBS is transported to site. This procedure is called Warehouse installation. See Section 6.3 on page 28.

Semi-automated integration provides the following benefits:

- No need for DHCP and DNS servers - IP addresses and other IP configurations are set from the configuration file
- No need for AIWS to download Combined file - The file is stored on laptop
- SEG uses IKEv2 - The additional feature IKEv2 CP is not required
- Permanent IP addresses and IPSec Traffic Selector proposals are possible to configure in the ICF

6.1 Semi-Automated Integration Process

For the semi-automated integration, the Site Installation file and the ICF are merged together to a Combined file.

The Combined file is stored on a laptop and downloaded to the RBS using ORI.

The Site installation file contains temporary IPSec configuration data. The file contains information that in the Autointegration case is provided from DHCP server, SEG or ORI.

The ICF contains permanent IPSec configuration data.

Note: The operator must keep track of manually set IP-addresses in the Site Installation file and the ICF. This is not maintained by OSS-RC.

The integration process is performed in the following order:

1. Bring the RBS and a laptop with a stored configuration file to site
2. Use ENIS to bind the hardware, if not already performed as an early binding



For more information, see Section 4.3 on page 15 and *Integrating RBSs On-Site Using ENIS*.

3. Install the RBS
4. Power on the RBS
5. Download the configuration file from the laptop to the RBS using ORI

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

6. The RBS starts the integration process, based on the downloaded IP configuration data

6.1.1

Node Integration Flow for Semi-Automated Integration

Figure 6 shows the node integration flow for Semi-automated integration, starting from Batch Provisioning.

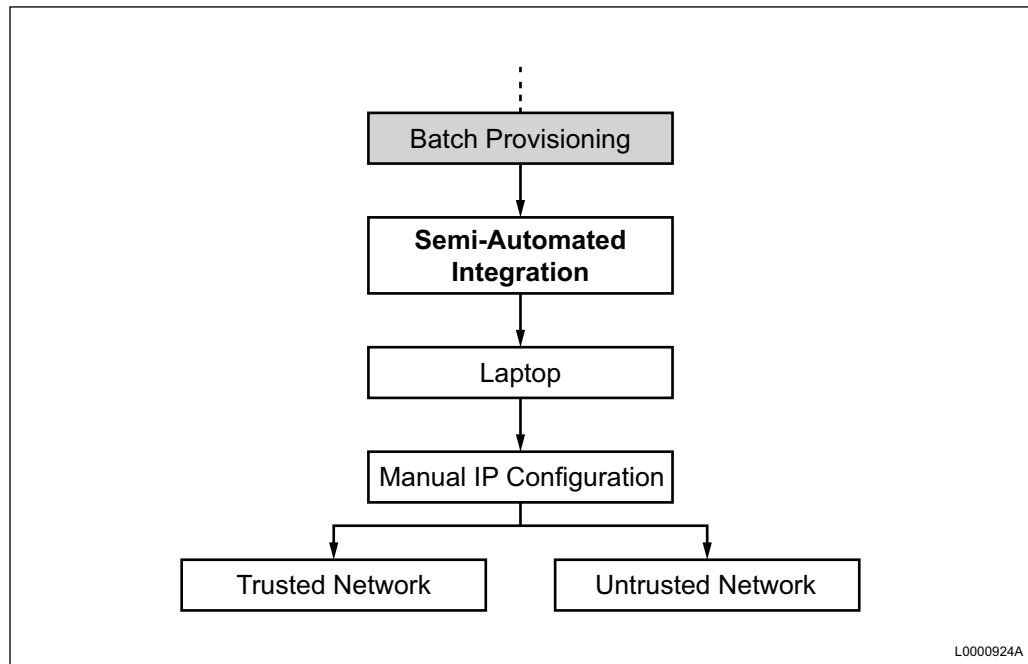


Figure 6 Semi-Automated Integration Provisioning Scheme

Only Manual IP Configuration is used. IP addresses are entered manually in the configuration files.

A Combined file is downloaded from the laptop to the RBS. For more information about the file content, see Section 6.1 on page 25.



6.2 Stand-Alone Integration

Stand-alone integration makes it possible to integrate an RBS without using OSS-RC. Stand-alone integration enables O&M access using manually installed node credentials and CA certificates.

The field technician uses a laptop to download a Combined file to the RBS. For the stand-alone integration case, the Combined file consists of a mandatory ICF and an optional Site Installation file. The Site Installation file is not needed if the node receives the O&M IP addresses from the DHCP server.

To use stand-alone integration the following preparations must be done before the integration process starts:

- Create a local super user account for the RBS, see Section 6.2.1 on page 27.
- Prepare node certificate and trusted CA certificate.
- Prepare the ICF with the installation data for the certificates.

The operator must create the following certificates:

- Trusted CA certificate.
- Operator certificate for the RBS.
- Operator certificate for the SEG is needed when integrating the RBS into an untrusted network.

Note: If the operator has access to the CA certificate that has been used for signing the existing SEG certificate, a new operator certificate for the SEG is not needed.

The certificates need to be stored in a PKCS12 container. This is the only supported certificate format for stand-alone integration. To integrate the RBS into an untrusted network an operator certificate for the SEG is needed. The certificate must be installed in the SEG before starting the integration process. The certificate for the SEG must be signed with the same trusted CA certificate that will be installed in the RBS during integration. The trusted CA certificate and the certificate for the RBS must be installed on the integration laptop. These certificates will be installed in the RBS during the integration process.

The newly created certificates need to be entered in the ICF. For more information regarding what to enter in the ICF, see *IP Transport*.

The stand-alone integration procedure is the same as for semi-automated integration. For information on the integration process, see Section 6.1 on page 25.

For more information about stand-alone integration, see *Stand-Alone Integration*.



6.2.1 Local Super User Account

The local super user account is used to provide O&M access to the node without the need to use an LDAP server. The local super user account can be used in both semi-automated and stand-alone integration. For stand-alone integration the account is mandatory for O&M access to the node. Using the local super user account in semi-automated integration does not exclude the use of authentication using an LDAP server.

The local super user account uses SSH certificate based authentication. This means that the clients SSH RSA public key is signed with the private key of another key pair created by the operator. The later key pair acts as CA. The public key of the CA is imported into the RBS during semi-automated or stand-alone integration. During the integration process the public CA key makes it possible for O&M to create and enable the local super user account.

To create a local super user account, do the following:

1. Create the CA key pair on the integration laptop
2. Create the key pair for the client on the integration laptop.
3. Sign the client public key with the private key from the CA key pair, to create the client certificate on the integration laptop.
4. Add the public key from the CA key pair in the Combined file, see Example 1.

```
<superUserAccount>  
<superUserName>oam</superUserName>  
<usersCA>ssh-rsa AAB3NzaC1yc/4Yalbatross@fid652403</usersCA>  
</superUserAccount>
```

Example 1 Public Key from CA Key Pair in Combined File

The local super user account is enabled during the semi-automated or stand-alone integration process. When the combined file is imported to the RBS using ORI, the following will be visible in the autointegration log:

```
Local super user account configured from combined file
```

The local super user account information is stored on the RBS until it is reset. If the user wants to do another attempt of semi-automated or stand-alone integration the content and the tags, shown in Example 1, from the ICF or the Combined file.

For more information about local super user account, see *Stand-Alone Integration*.



6.3 Warehouse Installation

In a Warehouse installation, the integration process is initiated before the RBS is transported to site. The technician performs the hardware binding, downloads the Combined file to the RBS, and sets parameter values with ORI.

To resume the integration process on site, the only action needed is to power up the RBS.

The integration process is performed in the following order:

At the warehouse:

1. Use ENIS to perform a hardware binding
2. Download the configuration file to the laptop
3. Power up the RBS
4. Download the configuration file from the laptop to the RBS using ORI

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

5. Power off the RBS

On site:

6. Install the RBS
7. Power up the RBS
8. The integration process proceeds, based on data from the file downloaded in Step 2

The integration continues as described in Section 4.4 on page 16 until the RBS is fully integrated.

For more information regarding ENIS, see Section 4.3 on page 15 and *Integrating RBSs On-Site Using ENIS*