This course will discuss the features and supported operations that align with RBS 6402 Release 16A.

At the end of this session, the viewer will be able to:

- Describe the features and capabilities of the RBS 6402
- List the variants of the RBS 6402
- Describe the hardware options
- Identify software streams and licenses
- List the deployment scenarios (trusted / untrusted)
- Explain the Installation and Integration functionalities

And

- Describe cases where a network could benefit from an RBS 6402 deployment

RBS 6402 FEATURES & FUNCTIONS

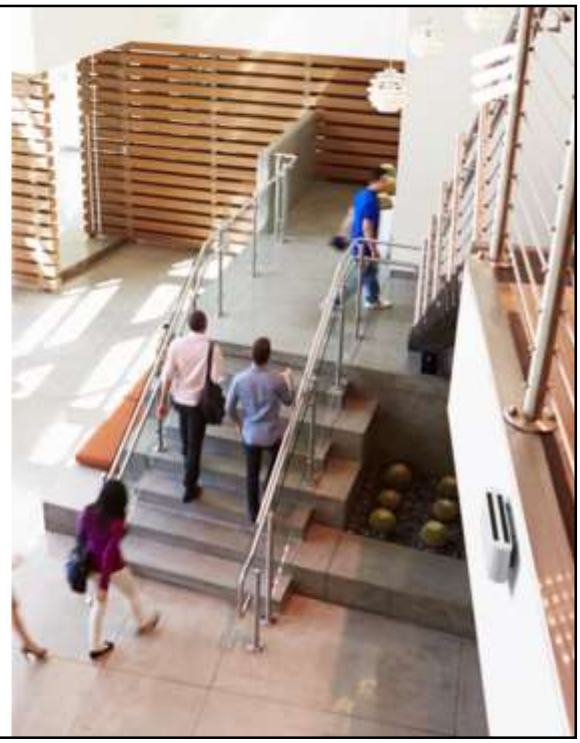
The RBS 6402 is one of several Small Cell products that Ericsson has on the market, as part of the integrated small cell vision.

The RBS 6402, sometimes internally referred to as “picoRBS”, is a multi-standard Radio Base Station supporting WCDMA, LTE and Wi-Fi.

GREATEST FLEXIBILITY

Full flexibility with multi standard and multi band

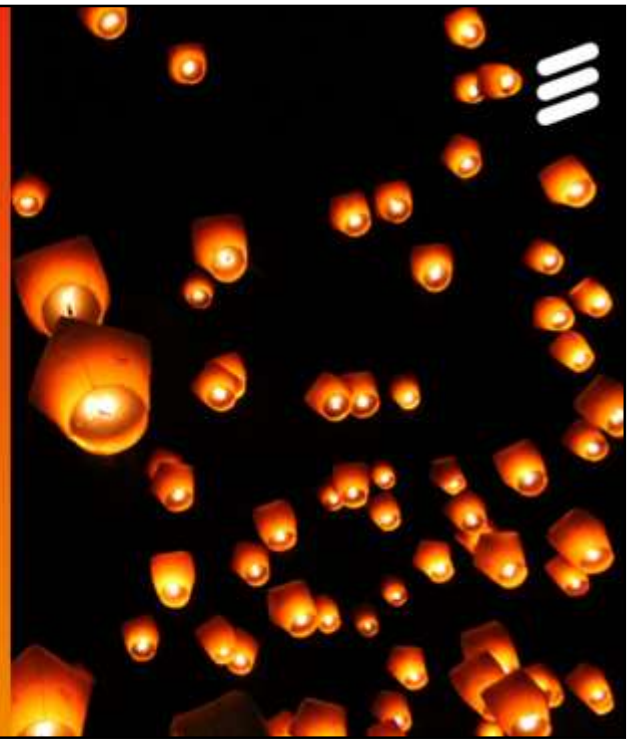
- 10 Frequency Bands (3GPP+Wi-Fi) supported in one unit
- 2 Bands 3GPP (LTE/WCDMA)+ 2 bands Wi-Fi simultaneous operation
- 3 Technologies: LTE or WCDMA and Wi-Fi simultaneous operation
- RF Power 3GPP: 2x250 mW per band (total 4x250 mW, B7 Europe:4x125 mW)
- Capacity up to 128 users (LTE)

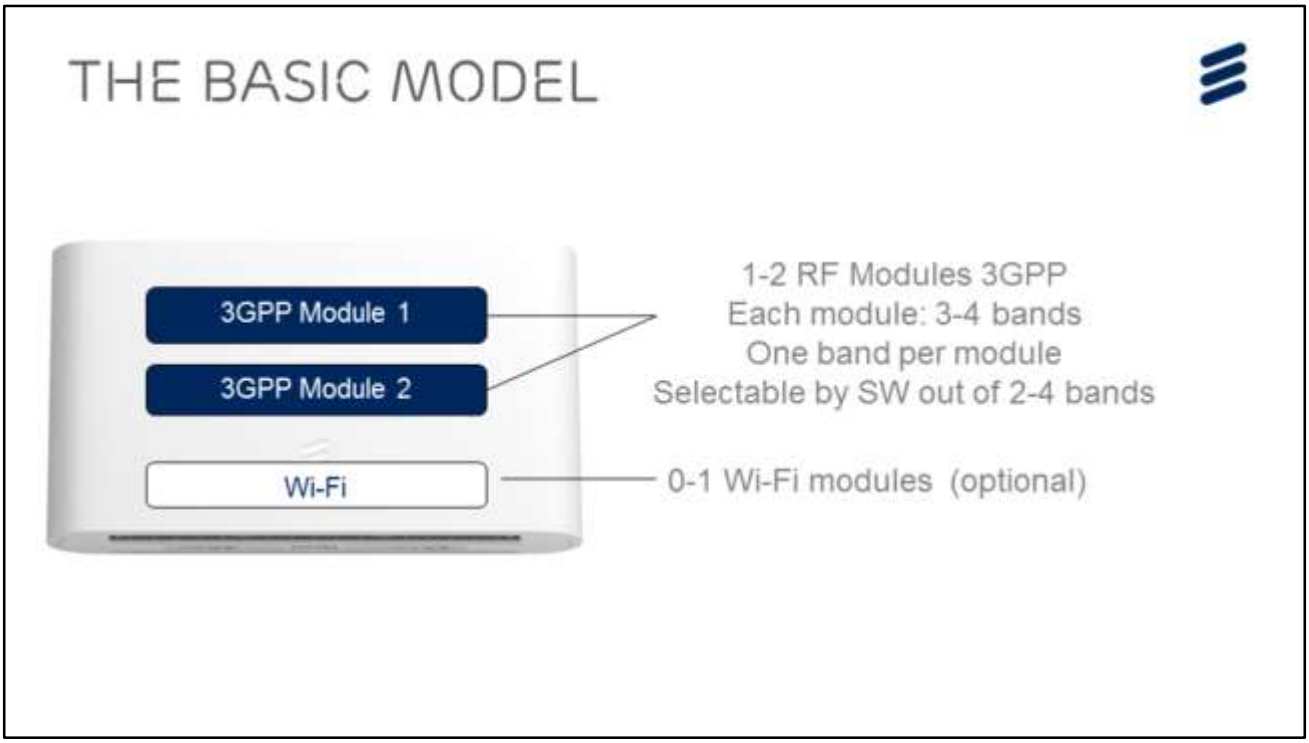


The RBS 6402 offers great flexibility with 10 frequency bands and options for 3 technologies (LTE , WCDMA and Wi-Fi). It provides data speeds up to 300 Mbps and up to 128 connected users.

The RBS6402 has the simplest deployment with IP Security for untrusted backhaul, Signed SW and secure Operation Administration and Maintenance access for untrusted locations. It can go Network live in 10 minutes with the Auto-integration feature.

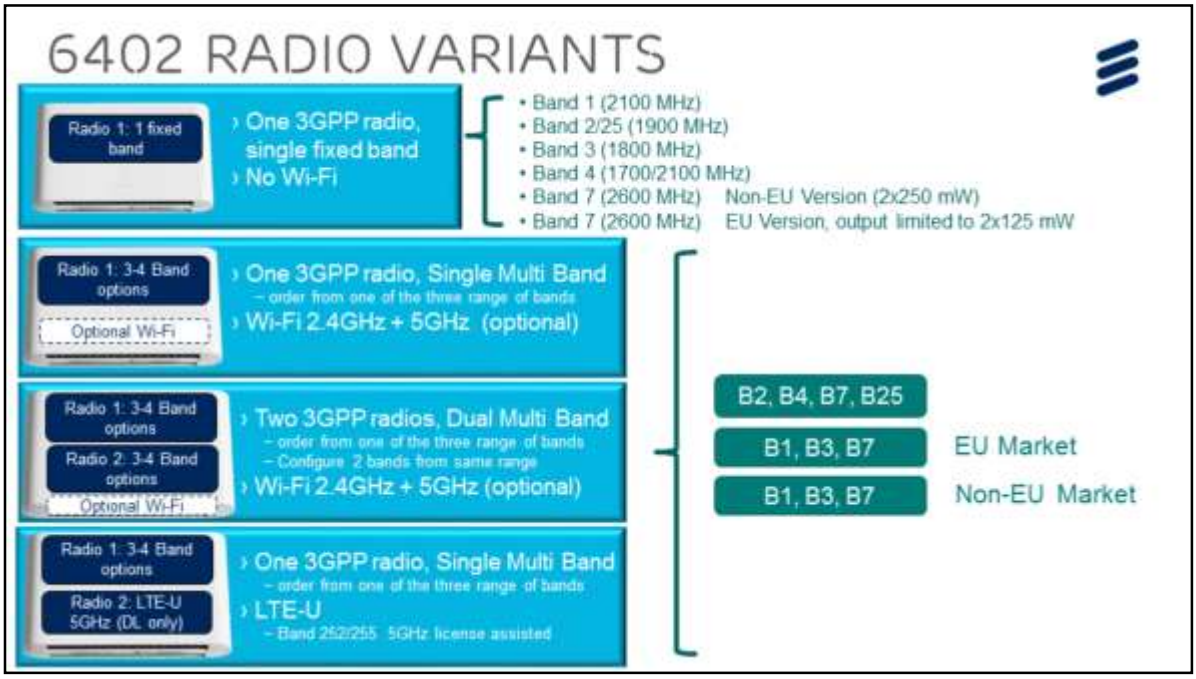
RBS 6402 HARDWARE OVERVIEW





The RBS 6402 can be equipped with 1or 2 RF modules and 0 or 1 Wi-Fi modules.

Each RF module covers several 3GPP bands and is remotely configurable to one band. 3GPP modules are HW prepared for operation of WCDMA or LTE.



Four basic models are available:

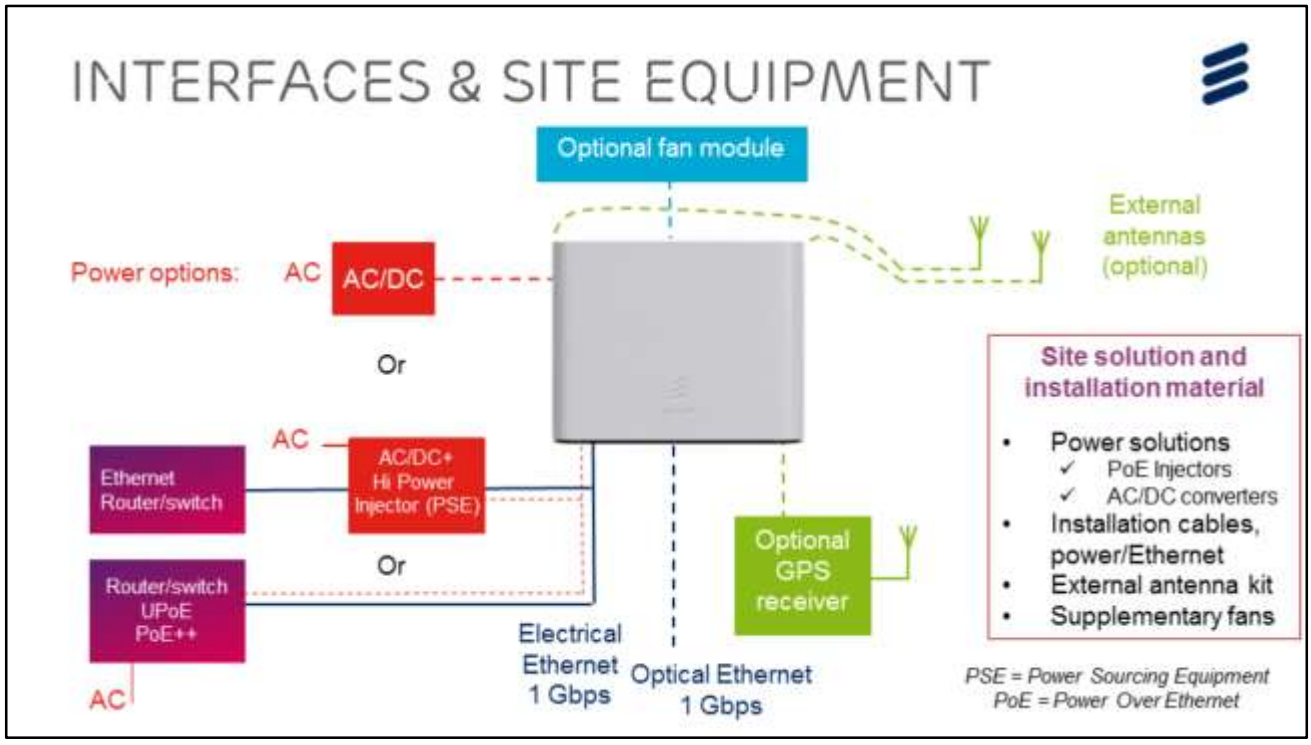
- The Single Band variant has one 3GPP radio that is orderable for one fixed frequency band. The single band options are shown on the right. This variant has no Wi-Fi support.
- Single Multi-Band variant has one 3GPP radio that is orderable for one of the three range of bands, shown on the right. The specific band in that range is then configured remotely. This variant also has optional dual band Wi-Fi support.
- Dual Multi-Band variant ships with two 3GPP radios. The same band range will be supported on both radios, with the specific band being configurable remotely. This variant also supports optional dual band Wi-Fi.
- Lastly, RBS 6402 can support the operation of LTE on unlicensed 5 GHz band. In this case, the 3GPP radio (or licensed band) is used for Uplink/Downlink and the LTE-U radio (or unlicensed band) is used for Downlink only. Note that the LTE-U option is presently restricted, meaning that the customer must obtain a special license from the governing regulatory body to operate in the unlicensed band.

WI-FI MODULE FOR PICO RBS 6402

APM-210

- 802.11ac 3x3 MIMO 5 GHz
  - 80 MHz channel
  - 256 QAM
  - Tx Beamforming
- 802.11n 3x3 MIMO 2.4 GHz
- 23 dBm EIRP each band
- IPsec connectivity from WLAN Controller to SeGW
- Full Aruba Enterprise feature set:
  - RF Protect
  - ClientMatch
  - AppRF
  - Many more . . .

- The integrated Wi-Fi module for the RBS 6402 is actually an embedded Aruba Wi-Fi AP
- The Wi-Fi module, the APM-210, delivers 802.11ac with 3x3 MIMO on the 5GHz channel and carries the full Aruba Enterprise feature set
- To use the Wi-Fi module within the RBS6402, the operator must deploy an Aruba controller to provision and manage the Wi-Fi.



- The RBS has the following power supply options:
  - The preferred power method is PoE, connecting external Power Sourcing Equipment (PSE) to the PoE port of the RBS.
    - The PSE can be either an endspan device or a midspan device.
    - The endspan PSE integrates the PoE within an Ethernet switch.
    - The midspan PSE, a PoE injector, is a device between the Ethernet switch and the RBS, and supplies power to the RBS.
  - If PoE power is not used, an external AC/DC converter can be connected to the DC port of the RBS.
- The transport options are electrical Ethernet or optical Ethernet connection. This makes it possible to connect both over the Enterprise LAN inside firewalls and/or over public internet as well as dedicated trusted transport. Timing and synchronization can be obtained via the network through NTP or IEEE 1588v2.
- The RBS 6402 has internal omni antennas that make it easy to place in any indoor environment, preferably mounted in the middle of the venue on the wall or a pillar. External antennas and ceiling mounting are also available.
- Other optional features include Supplementary fans and an external GPS receiver.

***(make this a hover over slide in Storyline to see more information on each item)

The Pico RBS HW product package, can be ordered with the following choices:

- Choice of basic model
- Choice of frequency band/bands
- Choice of market (EU or outside EU)
- Optional Wi-Fi, Multi band units only
- Optional RBS Specific site material (Power, SFP, Fan, GPS)

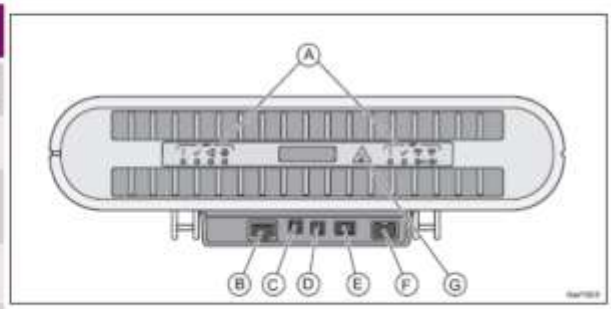
Here is a visual of the mandatory site components.

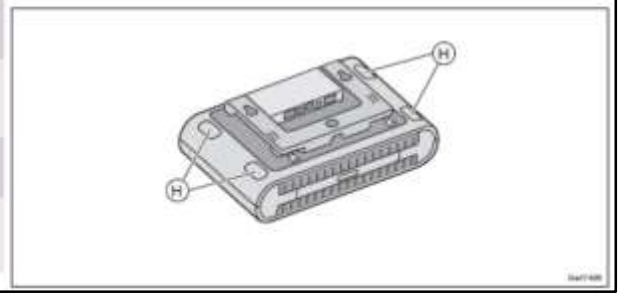
***(make this a hover over slide in Storyline to see more information on each item)

This slide shows the various *optional* site components.

INTERFACES AND CONNECTORS

Position	Description	Marking
A	Optical Indicators	! ✓
B	RJ-45 Connector PoE	WAN A / PoE
C	Power	48V (-) (+)
D	Fan	
E	GPS Connector	
F	SFP Connector for Optical Transmission	WAN B
G	Marking for ***Hot Surface***	
H	Knock out area for external antenna adapter	N/A





***(make this a hover over slide in Storyline to see more information on each item)

Here is a look at all the interfaces on the RBS6402.

A. Optical Indicators (more info on next slide)

B. Eth (RJ-45)

- Cable, min CAT5e, Max length 100m
- PoE injector BMK 905 012/x (Microsemi 9601G, 95W)

C. DC in

- AC/DC PSU BML 901 373/1

D. Fan module (BKV 106 175/1)

E. Mini I/O

- GRU (GPS Receiver Unit) NCD 901 57/1
- cable RPM 513 2372/2900 (2,9m)

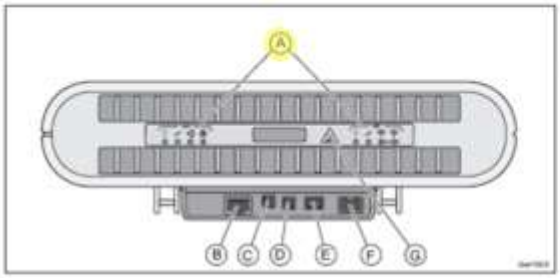
F. Eth SFP

- SFP cage
- SFP module (RYT copper, RDH fiber)
- SFP can support PON

G. Marking for Hot Surface

H. This is where you could mount the optional external antennas to the RBS6402.

OPTICAL INDICATORS



Marking	Indicator Name	Color	Mode	Description
!	Fault	Red	Off	Boot succeeded. No fatal HW faults detected.
			On	Fault in unit
✔	Operational	Green	Off	No power
			On	RBS ready to carry traffic.
			Flashing	Autointegration under process
	Status	Yellow	Off	No external or internal faults detected in Node
			On	Autointegration fails. (Used only during autointegration)
2.4	Wi-Fi (2.4 GHz)	Green	Off	Wi-Fi module not connected to Access Controller For future use
			On	Wi-Fi module connected to Access Controller For future use
5	Wi-Fi (5 GHz)	Green	Off	Wi-Fi module not connected to Access Controller For future use
			On	Wi-Fi module connected to Access Controller For future use
	Transport network status	Green	Off	Backhaul network not operational
			On	Backhaul network operational

***(make this a hover over slide in Storyline to see more information on each item)

Here is a close-up view of the optical indicators on the RBS6402.

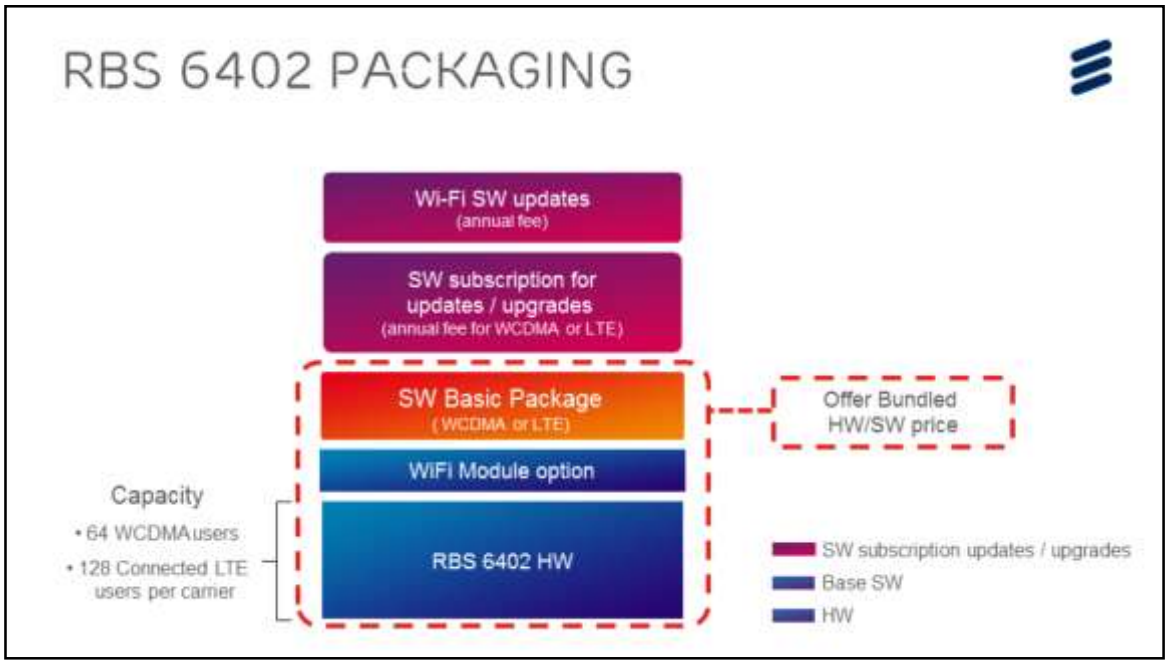
RBS 6402 SOFTWARE STREAMS & LICENSES

RBS 6402 MINIMUM SW LEVELS

	RBS 6402 RBS SW	RAN SW Level LTE RBS (Macro)	RAN SW Level RNC	Wi-Fi Aruba SW Level	OSS SW Level
LTE Single Band Single Carrier	L15B	L14B	-	-	O14B.1[1)]
LTE Dual Band/Carrier	L16A	L14B	-	-	O16A[1)]
WCDMA Single band	W16A	-	W14B	-	O14B.1[2)]
Wi-Fi	L16A/W16A	-	-	AOS 6.5.1	-

1) "Treat as" support in earlier OSS releases can be requested
2) When upgrading to O15B: Reintegration is needed. Full support in O15B

The following table describes the latest software versions that are supported for the commercially available RBS 6402.



In the Ericsson Software Model, the software for the RBS 6402 is divided into the following parts:

1. The **base package** is a license for the basic software that is necessary for the operation of the RBS 6402. Two base packages exist:
   - For WCDMA, one RBS 6402 WCDMA RAN Base Package must be ordered per HW unit.
   - For LTE, one RBS 6402 LTE RAN Base Package must be ordered per HW unit. This provides support for one LTE carrier and up to 64 connected users.
2. The **value package** is a license for optional software that can be added on top of the base package. One license item shall be ordered for each HW unit. When LTE software is chosen, the RBS 6402 LTE RAN Performance Package can provide support for two bands, carrier aggregation and up to 128 users.
3. The **SW subscription** gives access to software updates including enhancements and Software corrections for the RBS 6402. Each base and value package includes a Software subscription.

The RBS 6402 Wi-Fi software requires a “right to use” license, and is ordered together with the Aruba Wi-Fi controller.

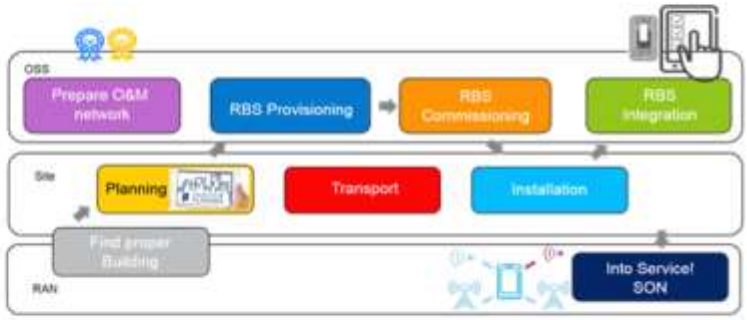
To Summarize:

- For RBS 6402 WCDMA RAN: Basic Software (one per HW unit) **and** SW Update & Upgrade Subscription must be ordered.
- For RBS 6402 LTE RAN: Basic Software (one per HW unit) for L16A Support for one LTE carrier and up to 64 connected users **and** Basic Software Update Subscription must be ordered. Optionally, one can also order RBS 6402 LTE RAN Performance Package for support for two bands, carrier aggregation and up to 128 users **and** LTE RAN Performance Package Update Subscription.

Next, we'll delve into the ways in which the RBS 6402 can be deployed in the network.

RBS 6402 DEPLOYMENT SUMMARY

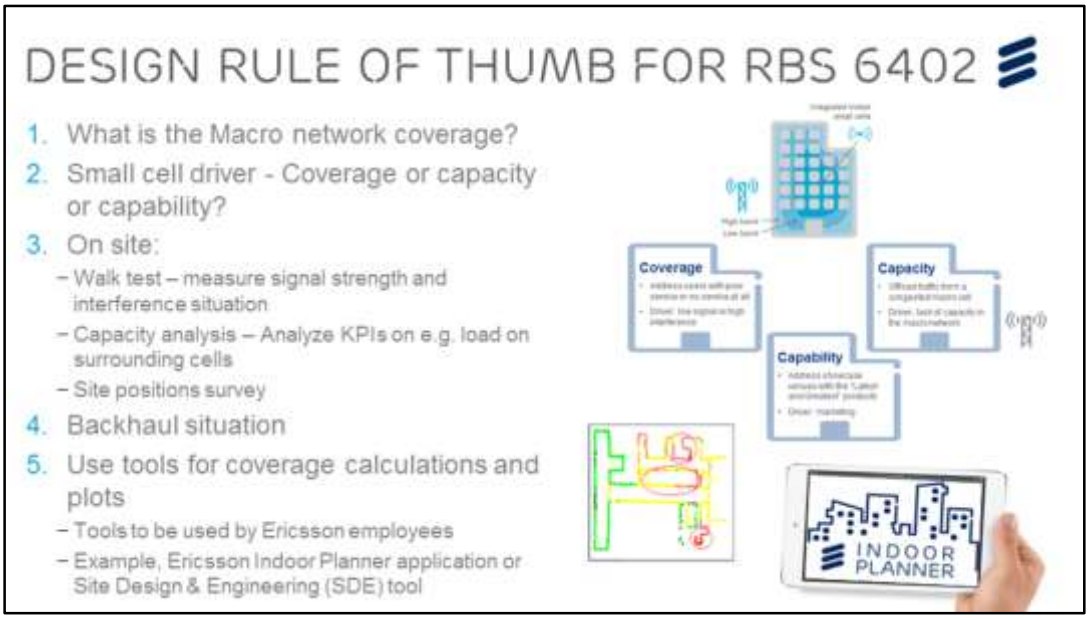
- Preparation
  - Rule of thumb planning
  - Secure network setup
  - Batch configuration
- Flexible and easy to deploy
  - Auto integration in 10 minutes
- SON functionality
  - Adapt to operator radio environment



Now that we have a general understanding of the RBS 6402 components, we are ready to step through the deployment of an RBS 6402 node in the operator's network.

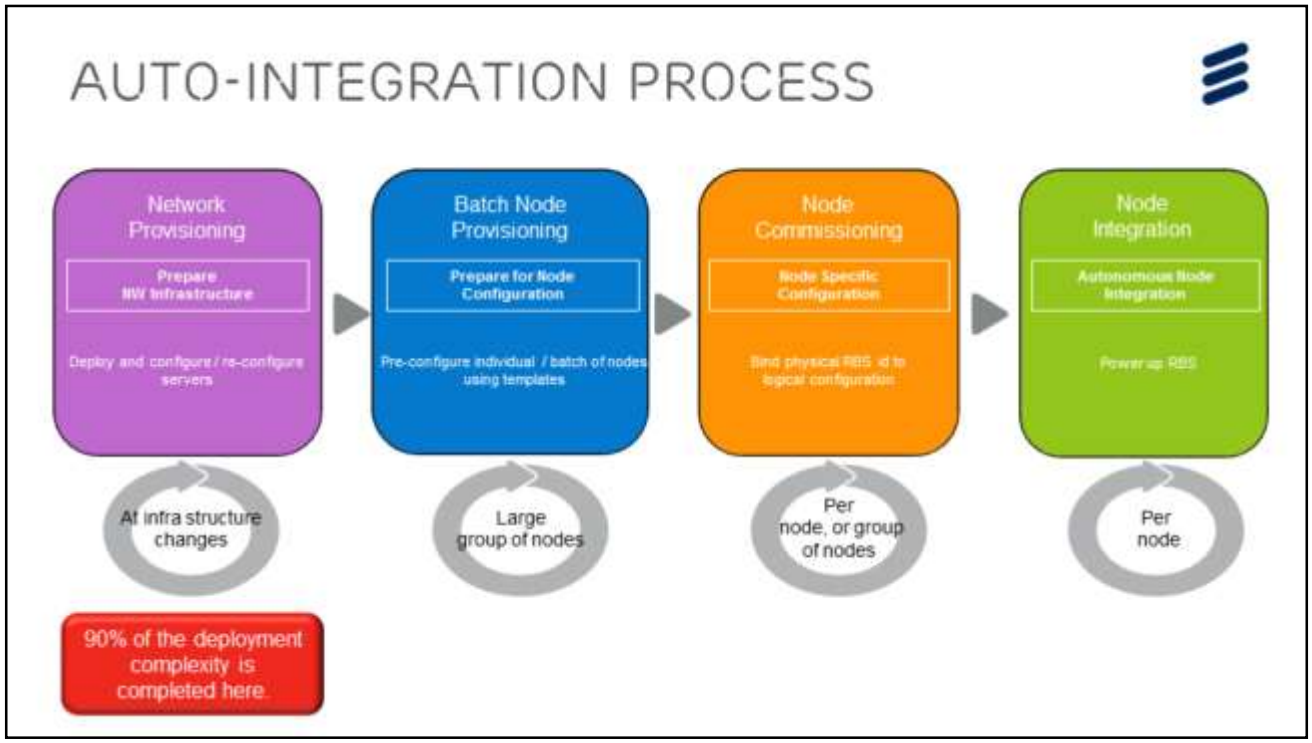
First, we must prepare the network. This includes planning where the RBS 6402 node should be deployed so that it best complements the macro network. We also have to setup the infrastructure for a secure network, and finally create the initial configuration files for the nodes in the network.

If the planning and preparation are done in advance to take advantage of the self-organizing network functionality, the entire autointegration should take only 10 minutes.



So first, we must plan our network. The following items must be considered when determining where to put the RBS nodes in a network.

1. What is the Macro network coverage?
   - You can use the same frequency for your RBS network as you do for the macro network
   - Be prepared to adjust RBS receiver sensitivity and take advantage of balancing features to avoid interference with the macro network.
   - RBS 6402 will adapt to surrounding cells using the Automatic Neighbor Relations functionality
2. What is your driver behind installing the small cell? Is it coverage, capacity, or capability?
   - The coverage area per RBS 6402 is 800-3000 m2, typically one per floor
   - Consider the macro network – deploy RBS 6402 at the poorest macro coverage
   - The RBS6402 capacity is 64 WCDMA users or 128 LTE concurrent users (voice or data)
3. What needs to be done on site?
   - A Walk test should be performed to measure signal strength and interference
   - Perform a capacity analysis; analyze KPIs, for example the load on surrounding cells
   - And do a site positions survey. One mounting suggestion is in the middle of the room, for example on a pillar or wall, preferably vertically.
4. What is the existing backhaul situation?
   - If using Ethernet for Transport, CAT 5/6/7 has a max length restriction of 100 m
   - You must also consider the power options available indoors for power consumption of 30-50W
   - The various Power Alternatives are an Ethernet Power injector, an AC/DC power converter located close to the RBS 6402, or PoE++, from a router for example.
5. Next, you must analyze the Floorplan. Open or concrete walls can impact placement and number of nodes on a floor. You can use several different tools for coverage calculations and plots:
   - Ericsson Indoor Planner is an iOS app that can be used to plan the coverage and capacity of RBS6402 nodes in a building. By uploading an image of the floor plan and providing information about the dimensions and building materials, it can estimate the best number of RBS nodes for the required coverage and capacity. Please contact your customer interface for additional information on how to activate Indoor Planner access after downloading Ericsson Indoor Planner from the Apple App store.
   - The Site Design & Engineering (SDE) tool is also available for site engineers. It provides an Electronic site survey, Bill of Material compilation, Site Installation Documentation preparation, and Customized templates for local project needs.

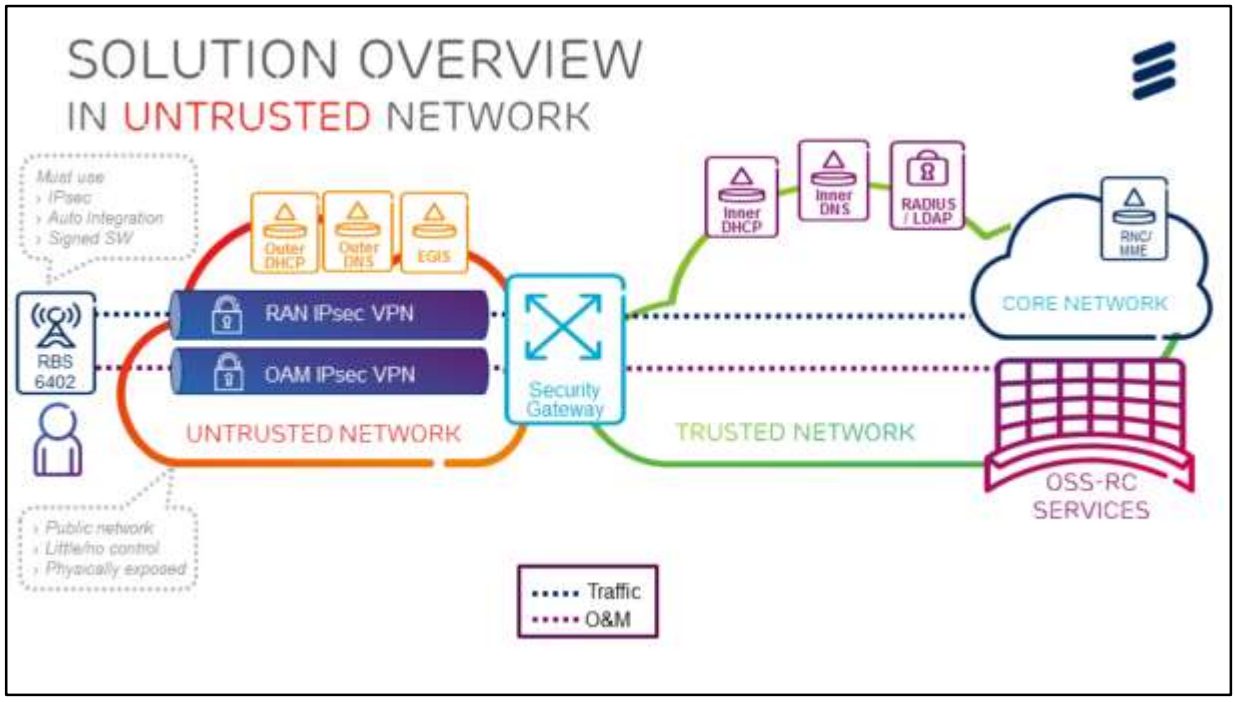


Once the planning is complete, we're ready to move into the deployment process.

This diagram shows an overview of the four phases that are part of the complete deployment process for auto-integration.

Regardless of the method employed for integration and whether it is a trusted or untrusted network, the transport network for example; the routers, switches and firewalls must be deployed and ready to support integration. Before integration, other supporting nodes must also be ready, such as the DHCP, DNS, RADIUS/LDAP, and the services that are encompassed by the Operations Support System for Radio and Core (OSS-RC), including private keys and certificates, the initial configuration file, and upgrade package.

Therefore, the first step in the process is OAM network provisioning. In the case of Zero Touch Integration, 90% of the deployment complexity is completed in this one step.

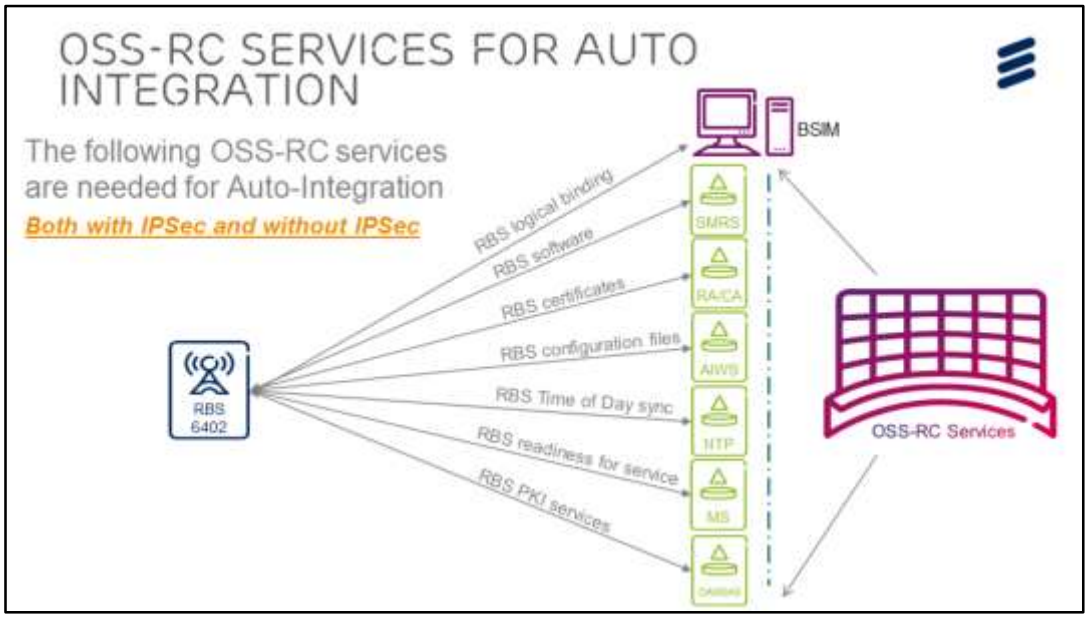


Before we go any further, let's take a look at the end-to-end network. Often small base stations are deployed in untrusted environments, where both the transport network is unsecured and the location is physically exposed.

For an untrusted network scenario, a security enabled router, called a Security Gateway, is introduced between the trusted and untrusted networks. It uses IPsec, forcing the remote RBS node to authenticate using the combination of a node certificate and the corresponding private key (securely stored in the node).

The core network would be either an LTE network or a WCDMA network.

You'll also see that the RBS node connects to the OSS-RC which stands for Operations Support System for Radio and Core. The OSS-RC is a network management server for small networks that is responsible for managing, configuring, monitoring, and upgrading the network. Within the OSS "umbrella" are a number of servers and services. Since there are a variety of different ways of integrating the RBS 6402 into the network and each option requires different network components, we'll introduce the OSS-RC services in the next slide so you have their definitions and functionalities in mind before we go through the integration options.



This diagram shows the OSS services and their role in auto-integration deployments.

Hover over each icon to get more details on the role of this service or server in the network.

BSIM: The Base Station Integration Manager (BSIM) stores the XML templates that it then uses to create or modify the initial configuration file (ICF). This OSS service is required to make the logical binding between the node logical name and the node equipment/serial number when using Zero Touch Integration.

SMRS: The Software Management Repository Service (SMRS) is required for software installations for nodes, backup of node Configuration Version (CV), and storage and distribution of license keys for the nodes. The SMRS server is the Secure File Transfer Protocol (SFTP) server for storage of the software upgrade package (UP).

RA/CA: Registration Authority (RA) is the software which inspects certificate requests from network nodes and forwards legitimate requests to the Certificate Authority (CA), which signs the certificate requests and issues certificates. RA/CA services are provided by OSS and prepared as part of network provisioning. Typically, the CA service resides on the Operation and Maintenance Security Administration Server (OMSAS) while RA is configured on the Infra server.

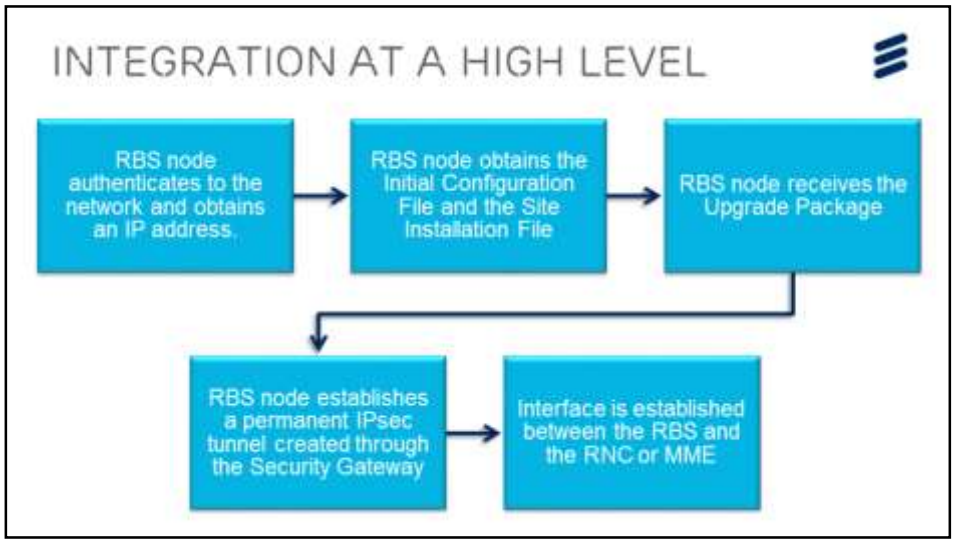
AIWS Server: Autointegration Web Service (AIWS) is required to provide authenticated access to the configuration files for the newly integrated nodes.

When auto integration starts, the Initial Configuration File (ICF) is built in BSIM 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 auto integration. The AIWS performs a secure identification of the RBS by using the RBS vendor credentials that are stored during manufacturing.

ToD: This OSS service is required for synchronizing the Time of Day (ToD) reference and validating the time stamps within certificates. NTP servers are used for time of day synchronization. Appropriate time synchronization is required for X.509 certificate validations and licenses to work correctly.

MS/ONRM: The OSS-RC Master Server (sometimes called the Infra 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 where it can be fetched by the RBS node during auto-integration. The 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.

OAMSAS: Operation and Maintenance Security Administration server (OMSAS) is located in the OSS-RC. OMSAS provides Public Key Infrastructure (PKI) services

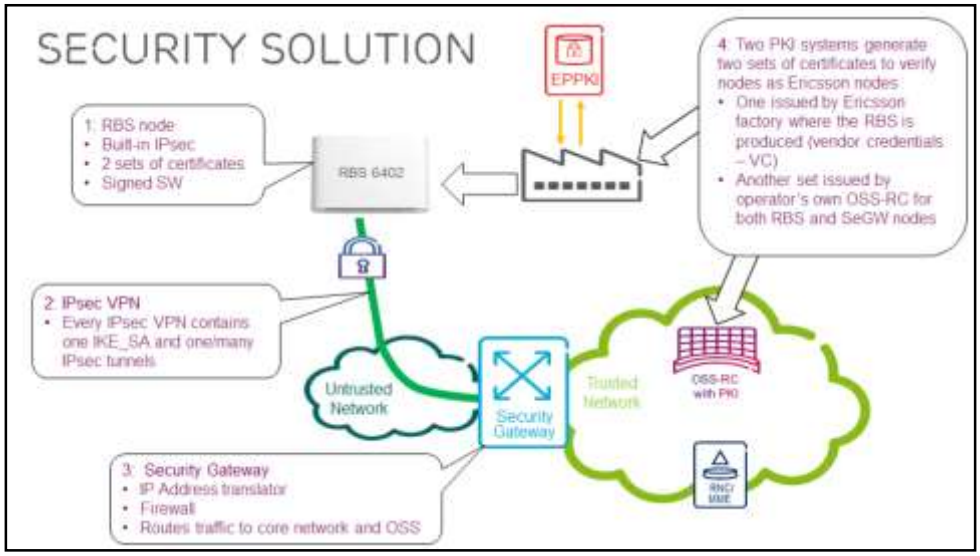


At a very very high level, this is what needs to happen during RBS integration:

1) The RBS node needs to authenticate to the network and obtain an IP address.
2) Next, it must obtain the Initial Configuration File (which contains with relevant operator network values) and the Site Installation File (which contains temporary IPSec configuration data, VLAN ID and AIWS server address).
3) Then, it must receive the Upgrade package in order to upgrade the RBS node to the right load for the network.
4) Next, the RBS node must establish a permanent IPsec tunnel created through the Security Gateway.
5) In the final step, an interface is established between the RBS and the Radio Network Controller (RNC) or MME and the cell is up.

Now this is where it gets complicated. There are a number of ways to achieve each step in the process! There are four main methods to integrate the RBS node and each of them have different dependencies on the network.

Regardless of the method employed, several factors are unchanging. The first is that security must be used in the network. The second is that the RBS node must have an initial configuration file to integrate into the network. Let's discuss these next.



Security is a very important aspect of the untrusted network scenario. As we mentioned, an untrusted network implies that the RBS node is mounted in a public location that leaves it exposed to tampering or it reaches the operator's core network using public internet. Obviously, we must ensure that only genuine nodes will have access to the security gateway and then indirectly to the core nodes and the management system OSS-RC. We solve these dilemmas by connecting a secure IPsec VPN over the untrusted transport network and we provide each node with a unique certificate to be used for authentication, ensuring that only the operator's unique and genuine RBS node is accessing the network.

Here's a more in-depth breakdown of the security features implemented in an RBS 6402 untrusted network:

1) The IPsec function is integrated into the RBS node and communicates with a Security Gateway normally placed on the border between the untrusted network and the operator's trusted core and OAM networks.

The RBS 6402 comes with factory-installed vendor credentials (which include a node-unique certificate and a private key). During autointegration, the RBS performs certificate enrollment to acquire signed operator credentials and operator's certificates from the operator OSS-RC Certificate Authority (CA) server.

During this process, the RBS receives up to two certificates: The O&M over TLS certificate is always enrolled, whereas the IPsec certificate is only enrolled if IPsec tunnels are used.

When this procedure is complete, the RBS only uses operator credentials and trusts other nodes that have certificates signed by the operator Certificate Authority server.

The Signed Software function ensures that only the software that contains a valid Ericsson signature is allowed to be installed on the RBS. This feature improves the security against malicious software.

2. In an untrusted network, IPsec VPNs are required to establish connectivity with the Security Gateway. The key management and distribution between the RBS and the Security Gateway is handled by the protocol Internet Key Exchange version 2 (IKEv2). To secure a bidirectional communication between the RBS and the Security Gateway using IKEv2, an IKE Security Association (SA) is established. Every IPsec VPN contains one IKE_SA and one or many IPsec tunnels.

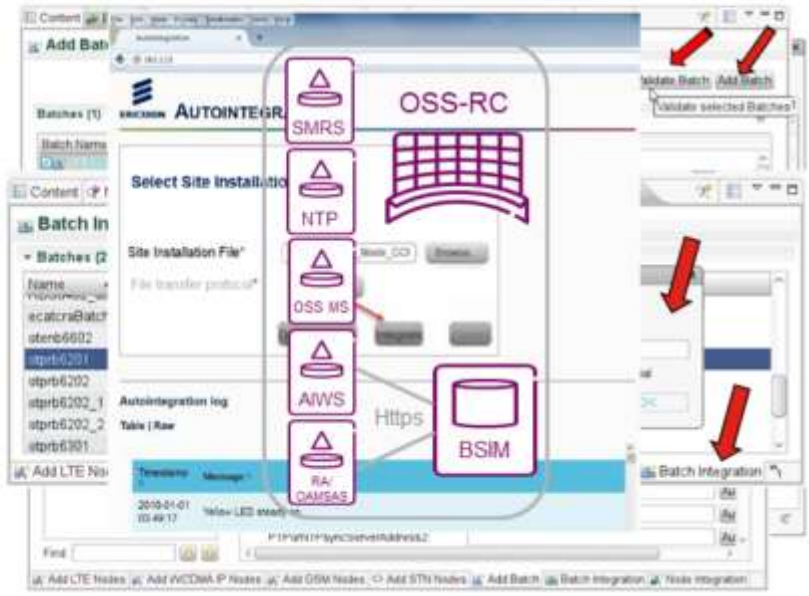
3. The Security Gateway acts as a translator for IP addresses in order to keep the private IPs hidden. It also acts as a firewall blocking everything except for the traffic travelling within established IPsec tunnels. Further, the Security Gateway is also a router, routing user plane and control plane traffic to the core network and OAM traffic to the OSS.

4. Certificates and corresponding private keys are needed when an RBS authenticates itself while establishing the IPsec VPNs. Two organizations issue certificates:

- Ericsson production PKI issues certificates and keys for all nodes produced at the factory. The customer can be sure new nodes are genuine Ericsson equipment as Ericsson issues unique "vendor credentials" for every node. This is used during the initial phase of integration.
- At the OSS-RC, The customer issues "operator credentials" for every integrated RBS node. This is used during normal operation. This certificate is used by the RBS while establishing the permanent IPsec VPN to authenticate itself as genuine operator equipment toward the Security Gateway.

CREATION OF THE ICF

1. From OSS Common Explorer, open the **BSIM** tab
2. Select **Add Batch** tab
3. Click: **New Batch** icon
4. Enter general details under **General** tab
5. Enter transport details in **Transport** tab
6. Enter radio details from **Radio** tab
7. Enter Auto Integration details from **Auto Integrate** tab
8. Click: **Validate Batches** and **Add Batch**
9. a) Bind the serial Number of the RBS in the **Batch Integration** tab, or
   b) Select No Bind and create Site Installation File
10. ICF File is generated and uploaded to **AIWS**



In all 4 integration scenarios, the RBS node requires an Initial Configuration File (ICF), created through BSIM.

Recall that the Base Station Integration Manager (BSIM) is an OSS service that uses its XML templates to create the initial configuration file (ICF).

Steps 1-3: The operator logs into the BSIM GUI in the **OSS Common Explorer.** From the **BSIM** tab, you will select the **Add batch** tab. Then you would select the **New Batch** icon.

Steps 4-7: Under each of the tabs in the **Batch Details** screen, enter the network specific parameters that are necessary for the RBS node to integrate into the network.

Step 8: Then you would select the **Validate batch** button and finally, the **Add batch** button.

Step 9: Next you have to decide whether or not this is a zero-touch integration where you would right-click on the batch and select **manual bind**, and then bind the serial number of the RBS hardware to the initial config file, or if this is a Local Maintenance Terminal (LMT) integration, and you right click on the batch file and select **no hardware bind**, and you require the Site Installation file to be configured. After filling out the details for the Site Installation File this will be combined with the Initial Configuration File into a Combined Configuration file that can be exported to the laptop.

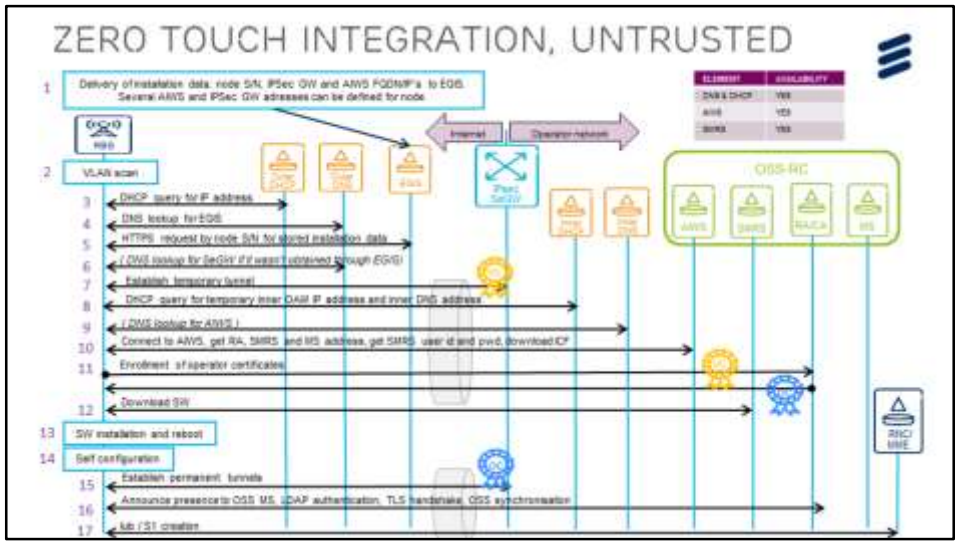
Step 10: It this was a Zero-Touch Integration, the initial Configuration File is generated after binding, and sent to the AIWS server.

INTEGRATION ALTERNATIVES

Method	Description	SIF & ICF location	Upgrade Package location	Node Bind Options	IPsec implementation
Zero Touch Integration (on-site)	Uses the OSS-RC during the integration process. A laptop is not used with this alternative.	AIWS	SMRS	BSIM (bind)	SeGW with IKEv2 CP
Local Maintenance terminal Integration (LMT) (off-site)	Offsite: SIF is loaded onto a laptop and BSIM (bind) is used to create ICF onsite. Alternatively, BSIM (no bind) can be used offsite to create a combined configuration file (SIF+ICF). SMRS is used onsite for the Upgrade Package.	1) SIF: Laptop to node (offsite); ICF: AIWS (onsite) 2) CCF: laptop to node (offsite)	SMRS	1) BSIM (bind) 2) BSIM (no hardware bind)	SeGW with IKEv2 CP
Local Maintenance terminal Integration (LMT) (on-site)	Same description as LMT off-site, except the laptop with SIF or CCF is brought to site to load onto RBS.	1) SIF: Laptop to node (offsite); ICF: AIWS (onsite) 2) CCF: laptop to node (offsite)	SMRS	1) BSIM (bind) 2) BSIM (no hardware bind)	SeGW with IKEv2 CP
Zero Touch Integration (off-site)	Pre-configuration is in a lab or warehouse environment using with access to operator's OSS-RC.	Laptop to node (offsite)	Node, or SMRS	BSIM (no bind)	SeGW no IKEv2 CP

Now we are at the stage where we can talk about the different methods of integration. While there are countless ways in which to bring an RBS node into service in an operator's network, there are 4 general terms used to describe integration.

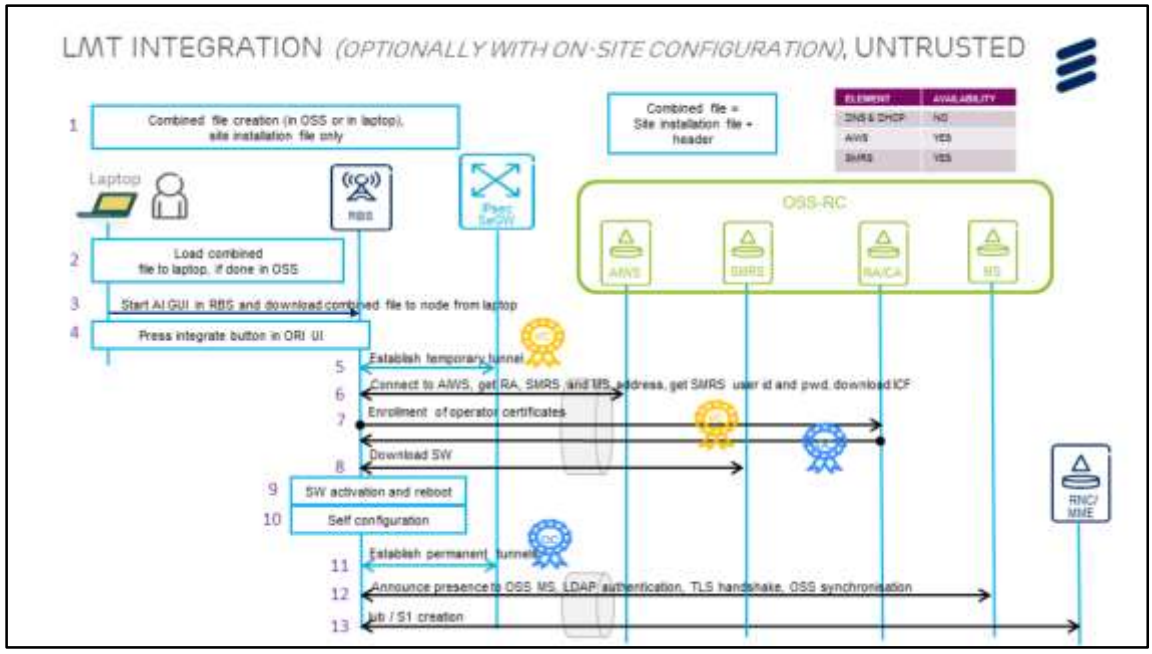
1) The first one is called Zero Touch Integration. This is the way Ericsson recommends RBS integration. Assuming all of the OSS-RC services and network devices are pre-configured, the RBS node can be installed and network live in 10 minutes using this option.
2) The second option is called Local Maintenance Terminal, off-site. This scenario could be used if the operator does not have a DHCP or DNS server that could resolve the IP address of the Security Gateway. In this case, The installer connects to the operator's OSS-RC network remotely and uses BSIM (with the bind option) to generate a combined file that consists of only the site installation file. This CCF is placed on a laptop and then loaded to the RBS node manually offsite. Once the RBS node is brought to site it can power up with a static IP address and locate the Security Gateway to begin the integration process, getting the ICF from the AIWS. A second option would be to use BSIM (with the no bind option) to generate a combined file that consists of the site installation file and the initial configuration file. This file would be loaded on the RBS node and then brought to site to complete the rest of its integration.
3) The third option is called LMT, on-site. It is very similar to the LMT off-site option. The only difference is that the installer brings the laptop to the site to manually load the SIF or the combined configuration file onto the RBS node on site.
4) The last option is not as common. It is called Zero Touch off-site. This option might be used if the Security Gateway does not support IKEv2 Configuration Protocol, or the customer does not want to create a temporary IPsec tunnel to the OAM. In this case, the node is configured off-site at a warehouse and then brought to site with the configuration files and software already installed and ready to integrate in the network.



The table on the previous screen gave a high-level overview of the various integration options. Now, we're going to walk through the steps for integration of the RBS node using each of the different methods.

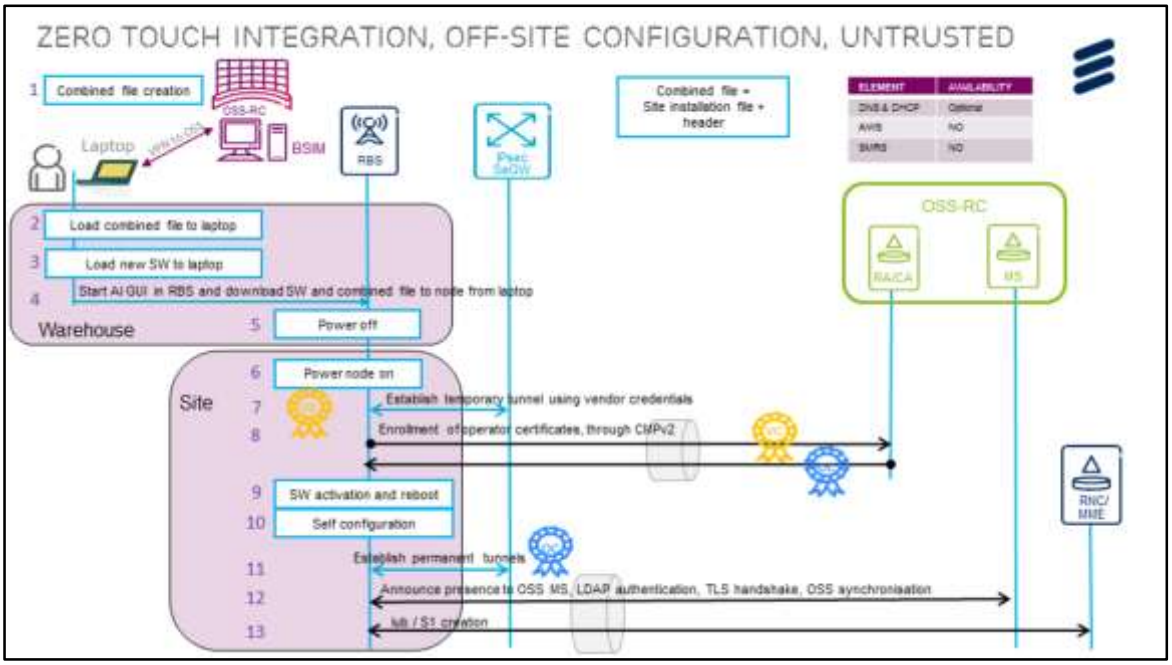
Zero Touch Integration onsite, requires very little handling of the RBS node, but there is a significant amount or preparation work to be done on the back end.

1. As we discussed in an earlier slide, the Initial Configuration File must be created in BSIM and then it is sent to the AIWS server for distribution to the RBS at a later step. That's why you won't see BSIM in this process; the generation of the initial configuration file has already occured and has been set to the AIWS server. Also, note that the SMRS server must be pre-loaded with the software upgrade package. And also before beginning the integration process, the node S/N, Security gateway and AIWS IP addresses must be sent to EGIS (Ericsson Global Integration Server).
2. Once the RBS node is installed and powered on at the site, the first thing it will do is initiate a VLAN scan to find a DHCP server.
3. Then it queries the DHCP server to get and IP address.
4. Next, the RBS will perform a DNS lookup to get the IP address for EGIS (Ericsson Global Integration Server).
5. The node will use its serial number to send an https request to EGIS to obtain the IP address of the Security gateway and the AIWS server.
6. If EGIS did not provide the IP address for the security gateway, the RBS node will now perform a DNS lookup for the security gateway.
7. Then, the RBS node will send its vendor credentials to the security gateway to authenticate itself and establish a temporary OAM IPsec VPN.
8. The RBS retrieves the temporary inner OAM IP address and the inner DNS address from the inner DHCP server through the Internet Key Exchange version2 Configuration Payload protocol.
9. In the next step the RBS resolves the address of the Auto Integration Web Service (AIWS) server from the inner DNS sever.
10. The RBS downloads the Initial Configuration File from the AIWS server. The Initial Configuration File is based on the logical binding made before the integration process between the Radio Base Station logical name and serial number in the Base Station Integration Manager. The Initial Configuration File also contains the address to the Registration Authority, Certificate Authority, SMRS, and the permanent addresses on the security gateway to establish the permanent IPsec VPNs.
11. Next, the RBS gets the operator credentials from the Certificate Authority for establishing the permanent IPsec VPNs in a later stage of the Auto Integration process.
12. The RBS downloads the software from the Software Management Repository Service.
13. Then it reboots.
14. Next it will self-configure based on the Initial Configuration File.
15. After it repeats the IP connectivity steps with the outer DHCP server, the RBS node establishes the permanent IPsec VPNs with the security gateway using operator credentials, and gets the permanent inner IP addresses for establishing the S1 or Iub interfaces.
16. Next, the RBS sends an SNMP trap to the OSS-RC Master Server using the inner management IP address to indicate readiness for service, performs AAA authentication, and synchronizes itself with the OSS-RC server.
17. In the final step the RBS configuration in the MME or Radio Network Controller (RNC) is done and the S1 or Iub interface is established between the RBS and the MME or RNC and the cell is up.



Next we'll talk about the Local Maintenance Terminal Integration off site method. This method might be used if there is no DHCP or DNS server available for the RBS node to locate the security gateway. In this case…

1. the installer connects to the operator's OSS-RC remotely, and uses BSIM (bind option) to create the site installation file. (Recall from the table we presented earlier that they could also have used the no bind option in BSIM and generated a combined configuration file, but we'll keep this example simple).
2. The site installation file is loaded onto the laptop.
3. The laptop is then connected to the maintenance port of the RBS node and the combined file is loaded onto the node, using its Auto-Integration GUI.
4. After the Site Installation file is loaded, the node is powered down and brought to site. (This is where the LMT onsite and LMT offsite scenarios differ. In the On-site scenario, the laptop is brought to the site and the file is loaded onto the RBS node at the site. Other than that, the two scenarios are the same and we'll continue our integration…)
5. When it is installed and powered up, the RBS node will use the static IP address it was given in the site installtion file and establish a temporary IPsec tunnel to the Security Gateway using it's vendor credentials for authentication.
6. The RBS downloads the Initial Configuration File from the AIWS server. The ICF also contains the address to the Registration Authority, Certificate Authority, SMRS, and the permanent addresses on the security gateway to establish the permanent IPsec VPNs.
7. Next, the RBS gets the operator credentials from the Certificate Authority for establishing the permanent IPsec VPNs in a later stage of the Auto Integration process.
8. The RBS downloads the software from the Software Management Repository Service.
9. Then it reboots.
10. Next it will self-configure based on the Initial Configuration File.
11. After it repeats the IP connectivity steps with the outer DHCP server, the RBS node establishes the permanent IPsec VPNs with the security gateway using operator credentials, and gets the permanent inner IP addresses for establishing the S1 or Iub interfaces.
12. Next, the RBS sends an SNMP trap to the OSS-RC Master Server using the inner management IP address to indicate readiness for service, performs AAA authentication, and synchronizes itself with the OSS-RC server.
13. In the final step the RBS configuration in the MME or Radio Network Controller is done and the S1 or Iub interface is established between the RBS and the MME or RNC and the cell is up.

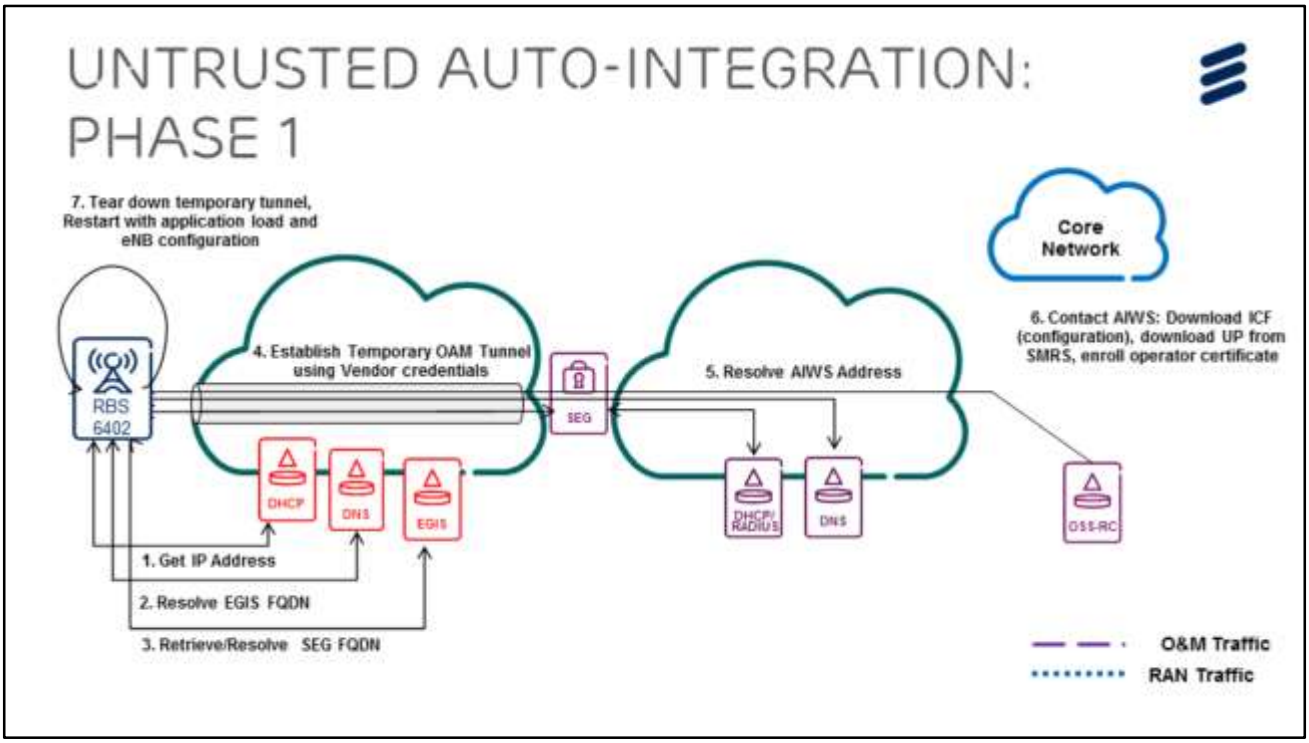


This last deployment scenario is rare, but we'll discuss it since it is a supported method of integration.

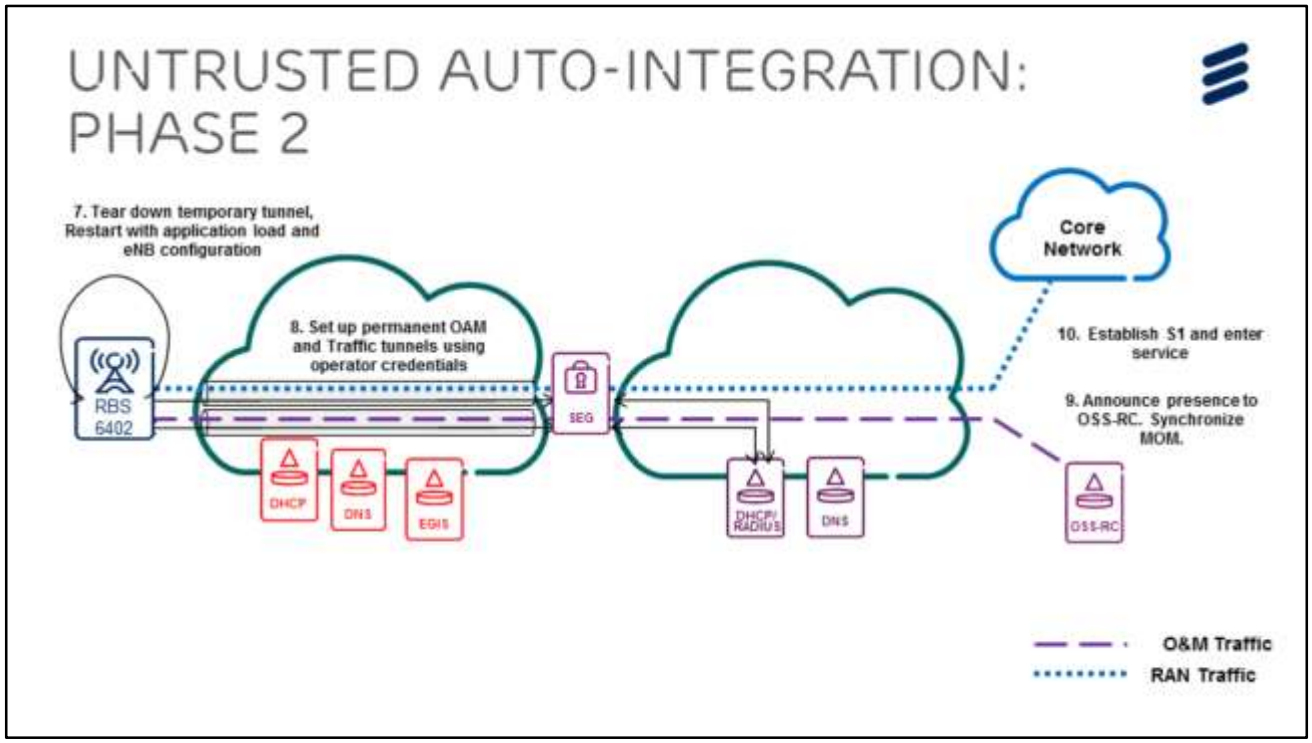
Let's say that the operator wants to deploy an RBS node at a location that has no DHCP and DNS servers, or the Security Gateway does not support IKEv2 Configuration Protocol, or the customer does not want to create a temporary IPsec tunnel to the OAM .

1. In this case, the operator would have to manually install two files onto the RBS node using a laptop back at a warehouse. First, the installer must connect to the operator's OSS-RC network (likely through a VPN tunnel) and use BSIM to generate the Combined Configuration File (CCF) comprised of the Site Installation File and Initial Configuration File (ICF).
2. Then, this combined file is saved to the installer's laptop.
3. The second file to be downloaded to the laptop is the zipped software file from Ericsson's Software Gateway containing the upgrade package. This file must be unzipped on the laptop and the file path is added to the Combined Configuration File already on the laptop.
4. Once these files are prepared with the correct network configuration information, the laptop would be directly connected to the RBS node's maintenance port, where the operator would run the RBS's auto-integration GUI to install these files.
5. The node is then powered off and sent to site.
6. Once the node is installed it is powered on.
7. The first thing the RBS node will do is use the static IP address it was given in the site installtion file and establish a temporary IPsec tunnel to the Security Gateway using it's vendor credentials for authentication.
8. These credentials are then sent to the OSS-RC Registration Authority (RA) server which inspects the node's certificate request and then sends it an operator certificate.
9. This will activate the software on the node and a reboot.
10. After the RBS reboots, it will perform a self-configuration, and
11. Establish a permanent IPsec tunnel with the operator's certificate.
12. Next, the RBS node sends a trap to the OSS Master Server to announce that it is fully operational, completes its AAA authentication in the network and synchronizes itself with the OSS network.
13. Finally the RBS node will establish its S1 interface to the MME or its Iub interface to the RNC in the core network.

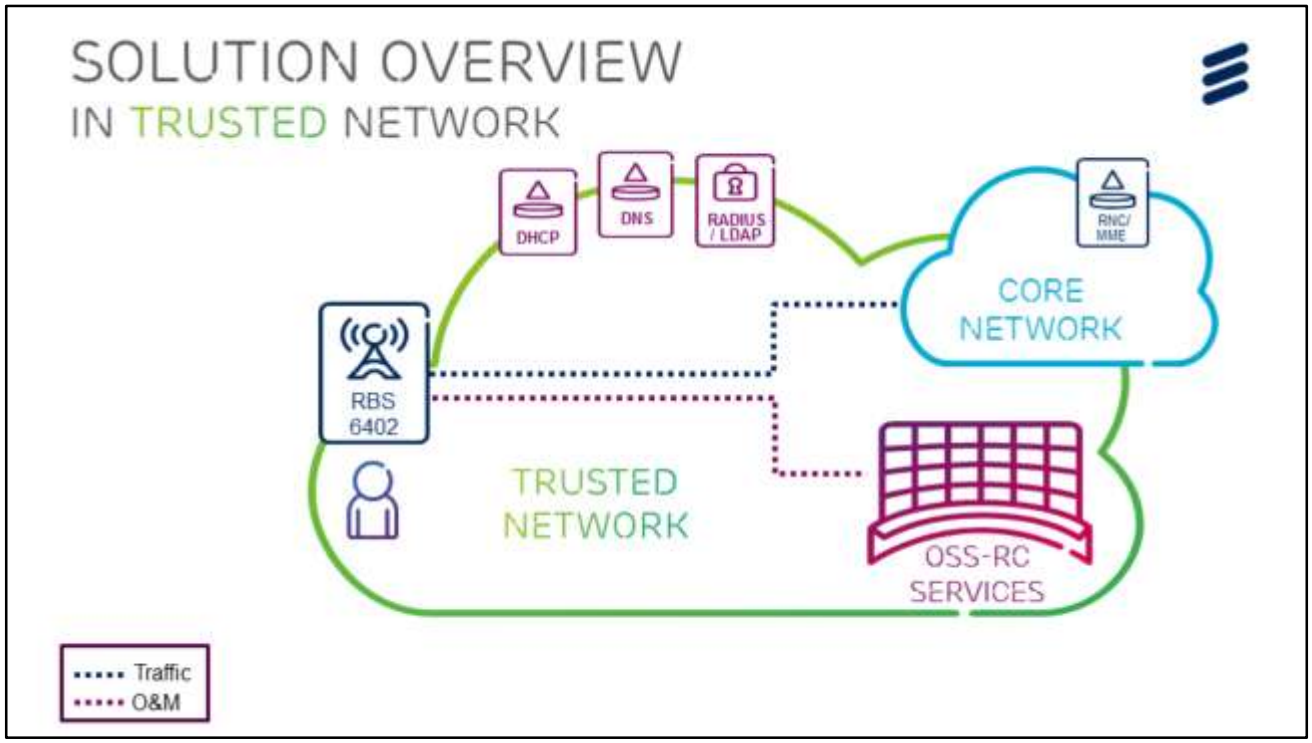
UNTRUSTED AUTO-INTEGRATION: PHASE 1



1. In the first step the RBS boots up and does a VLAN scan to find a DHCP server and get its own IP address.
2. Next, it will talk to the outer DNS server to resolve the IP address of Ericsson's Global Integration Server (EGIS).
3. In the third step, the RBS node, retrieves the fully qualified domain name for the security gateway from EGIS.
4. In the fourth step the RBS establishes the temporary OAM IPsec VPN with the security gateway using the Ericsson vendor credentials to authenticate itself, and the RBS gets the inner DHCP server address through the Internet Key Exchange version2 Configuration Payload protocol.
5. In the fifth step the RBS resolves the address of the Auto Integration Web Service (AIWS) server from the inner DNS sever.
6. In the sixth step the RBS downloads the Initial Configuration File from the AIWS server, downloads the software upgrade package from the Software Management Repository Service, and enrolls the operator certificates.
7. In the seventh step, the RBS self-configures based on the Initial Configuration File and reboots.



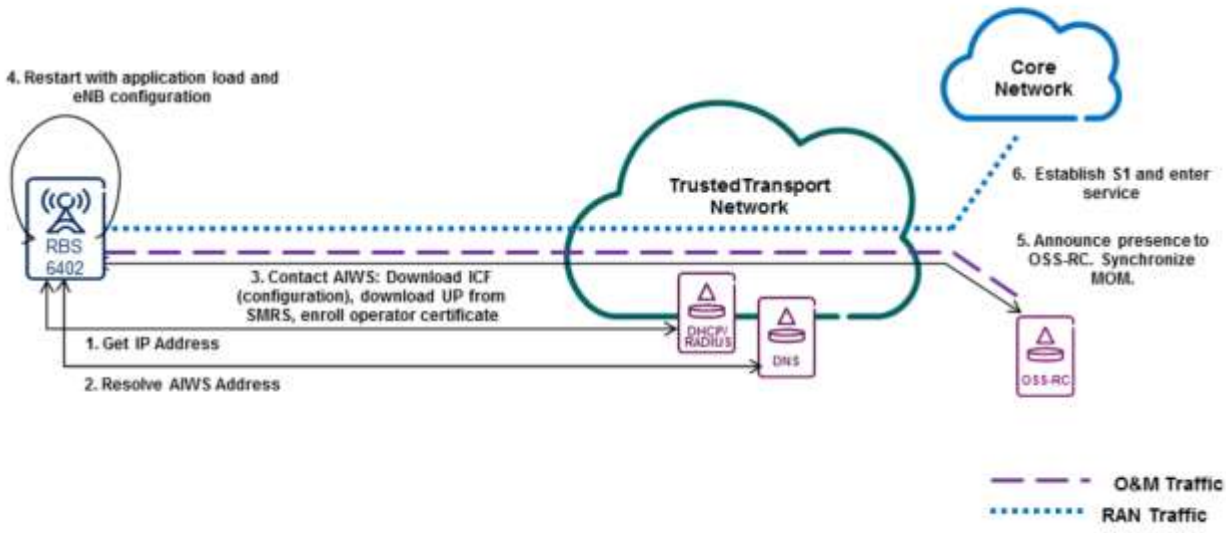
8. In the eighth step the RBS, after rebooting, repeats the IP connectivity steps with the outer DHCP server, establishes the permanent IPsec VPNs with the security gateway using operator credentials, and gets the permanent inner IP addresses for establishing the **S1** interfaces.
9. In the ninth step the RBS sends an SNMP trap to the OSS-RC Master Server using the inner management IP address to indicate readiness for service.
10. In the final step the RBS configuration in the MME is done and the **S1** interface is established between the RBS and the MME and the cell is up.



Another, but less likely, scenario is to deploy an RBS 6402 node in a Trusted network.

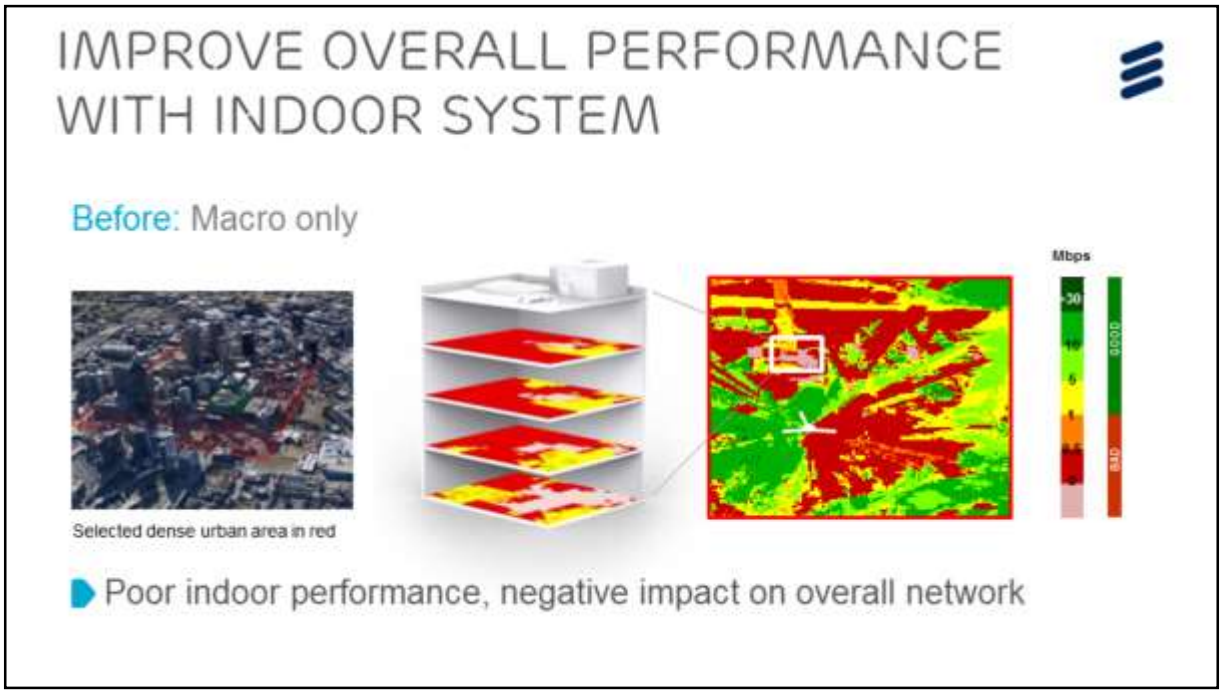
“Trusted” means that the RBS node and the transport network are in a physically secure location and do not require the additional security measures offered by IPSec and the Security Gateway.

TRUSTED AUTO-INTEGRATION



1. In the first step the RBS boots up and retrieves its IP address from the DHCP server.
2. Next the RBS resolves the address of the Auto Integration Web Service (AIWS) server from the DNS sever.
3. Then the RBS downloads the Initial Configuration File from the AIWS server, downloads the software upgrade package from the Software Management Repository Service, and enrolls the operator certificates.
4. In the fourth step, the RBS self-configures based on the Initial Configuration File and reboots.
5. In the fifth step the RBS sends an SNMP trap to the OSS-RC Master Server to indicate readiness for service.
6. In the final step the RBS configuration in the MME is done and the **S1** interface is established between the RBS and the MME and the cell is up.

RBS 6402 DEPLOYMENT SCENARIOS

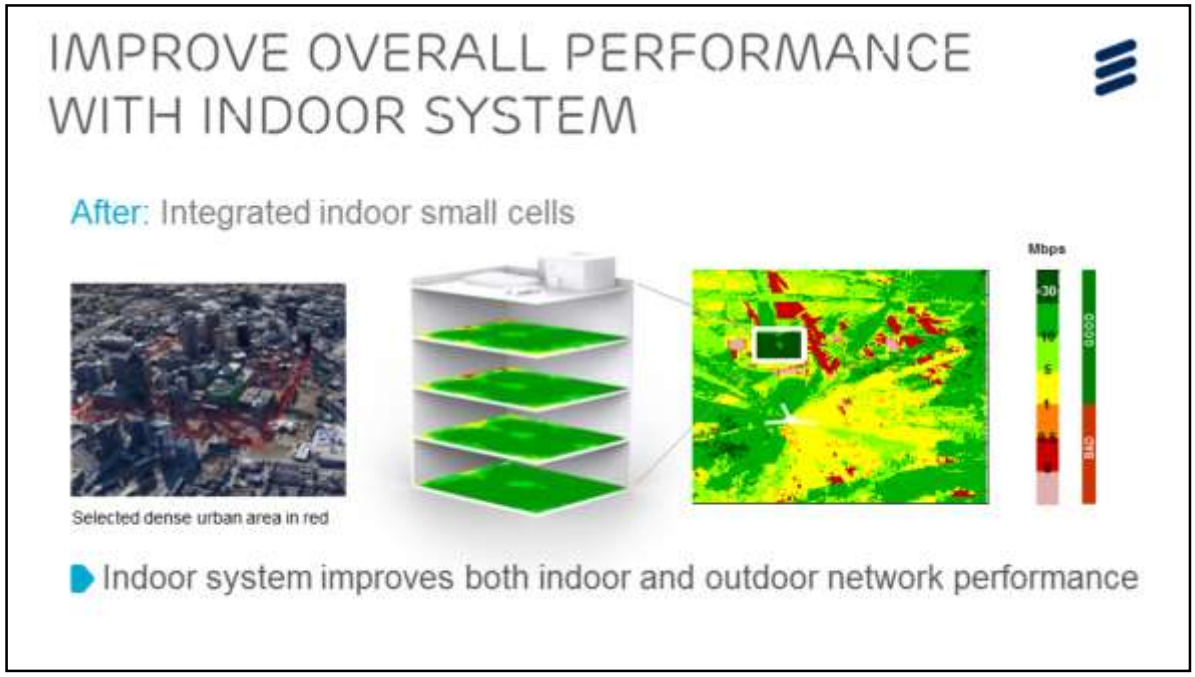


Now that we understand the features of the RBS 6402 node and how to deploy it, let's look at a couple of examples for WHY an operator would want to deploy RBS 6402 in their network.

The first picture on the left shows a downtown core powered by only a macro network. In this use case, the traffic load is on average 13 Mbps/km^2 in the whole 33 km^2 area, and 90 Mbps/km^2 in the downtown area. This traffic load corresponds to roughly 0.6 GB/month per user. Notice the little green square surrounding one building in the center.

We can blow this image up and look at the interior coverage of this building. In this case the macro network experiences severe interference inside the building which results in low throughput rates in a majority of the studied buildings.

Also, when looking in the surrounding downtown area, a large part experience low rates.



Now, with an indoor RBS 6402 network deployed inside the building, we can see an obvious increase in indoor performance. But also look at what happened outside the building, in the surrounding areas. Everything is now in a much better situation thanks to the right integration of the indoor system in the existing macro cluster.

USE CASE EXAMPLE 2:

RBS 6402 IN OPERATOR STORE

Challenges:

- Poor coverage in telco shops
- Expansion of macro network too expensive or too long to deploy
- High performance HD Voice + premium data

Solution:

- Deploy RBS 6402 in 200+ shops
- Use existing backhaul (VDSL/fiber)
- Same frequency/RNC as macro

In this second example, customers complained that their cellular coverage was extremely poor inside the shopping center. Given the construction materials inside the building and its exterior, expanding the macro network would be too costly and much too lengthy to deploy.

The best solution in this case is to deploy an RBS 6402 network within the building, using the same frequency bands as the macro network. You can see from the coverage map that the RBS 6402 deployment offered a huge improvement to the network.

This concludes the overview of the RBS 6402.

To recap, we have discussed:

- The features and capabilities of the RBS 6402, including the supported frequency bands and technologies.
- The variants of the RBS 6402, specifically, the single 3GPP band, Single 3GPP Multi-Band with a Wi-Fi option, Dual 3GPP Multi-Band with a Wi-Fi option, and the single 3GPP band and restricted LTE-U option.
- The available hardware options, including the choice of radios, Power, SFP, Fan, and GPS modules.
- The software streams and licenses currently available.
- The differences between a trusted and untrusted network.
- The steps involved in integrating an RBS node into the network.
- And we provided a couple of examples of how the RBS network can be used to improve indoor and outdoor coverage.

Please take a few minutes to complete the following quiz.

Thanks for watching.


QUIZ

QUIZ

1. True or False? In a Trusted deployment, a security gateway is required between the RBS and the core network.
2. Which service stores the XML templates used to create the initial configuration file?
   a) Base Station Integration Manager (BSIM)
   b) Software Management Repository Service (SMRS)
   c) Autointegration Web Service (AIWS)
   d) Operation and Maintenance Security Administration server (OMSAS)
3. Which device acts as a firewall and routes traffic to the trusted core network and OSS?
   a) RADIUS/LDAP server
   b) Ericsson Global Integration Server
   c) Security Gateway
   d) Operation and Maintenance Security Administration server
4. True or False? Local Maintenance Terminal (LMT) Integration does NOT require the operator to interface with the RBS 6402 in order to achieve initial configuration.
5. True or False? With Zero Touch Integration, 90% of the work is done before the RBS node is installed onsite.

QUIZ

6. True or **False**? The RBS node can only be powered by POE.
7. After the Initial Configuration File is generated in BSIM, where is it stored?
   a) **AIWS server**
   b) OMSAS server
   c) EGIS
   d) SMRS
8. Which server is responsible for storing the RBS 6402 upgrade package?
   a) AIWS server
   b) OMSAS server
   c) EGIS
   d) **SMRS**
9. True or **False**? RBS vendor credentials are the only certificates issued in a secure network.
10. **True** or False? A reboot of the RBS 6402 node is part of the configuration process.

QUIZ

11. True or **False**? An "Untrusted network" means that the RBS node has already been compromised and left the core network vulnerable.
12. Identify the technology type(s) that are supported on the RBS 6402:
    a) LTE
    b) WCDMA
    c) Wi-Fi
    d) **All of the above**
13. Which items are optionally supported with the RBS 6402?
    a) GPS
    b) Fan module
    c) External antennas
    d) **All of the above**
14. **True** or False? If two radios are used, the RBS 6402 can support up to 128 LTE users.
15. **True** or False? The Wi-Fi radio on the RBS 6402 runs on Aruba software.


ERICSSON