ETSI TS 132 501 V17.0.0 (2022-04)

Universal Mobile Telecommunications System (UMTS);
LTE;
Telecommunication management;
Self-configuration of network elements;
Concepts and requirements
(3GPP TS 32.501 version 17.0.0 Release 17)

Reference
RTS/TSGS-0532501vh00

Keywords
LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document is part of a TS-family covering the 3rd Generation Partnership Project Technical Specification Group Services and System Aspects, Telecommunication management; as identified below:

32.501: Self-Configuration of Network Elements; Concepts and Integration Reference Point (IRP) Requirements;

32.502: Self-Configuration of Network Elements Integration Reference Point (IRP); Information Service (IS);

32.506: Self-Configuration of Network Elements Integration Reference Point (IRP); Solution Set (SS) definitions.

1 Scope

The present document describes the concepts how self-configuration works and what IRP requirements need to be met to support this functionality. The document also captures if a requirement shall be met via the Itf-N interface or via other protocols. This version of the TS is restricted to self-configuration of eNBs. The requirements in this document are not imposed on HNBs.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 32.101: "Telecommunication management; Principles and high level requirements".

[3] 3GPP TS 32.102: "Telecommunication management; Architecture".

[4] 3GPP TR 32.816: "Telecommunication management; Study on Management of Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and Evolved Packet Core (EPC)".

[5] 3GPP TS 32.531: "Telecommunication management; Architecture; Software Management Concepts and IRP Requirements ".

[6] ITU-T Recommendation X.800: "Security architecture for Open Systems Interconnection for CCITT applications".

[7] 3GPP TS 33.310: " Network Domain Security (NDS); Authentication Framework (AF)".

3 Definitions and abbreviations

For the purposes of the present document, the terms and definitions given in TS 32.101 [2], TS 32.102 [3] and TS 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TS 32.101 [1], TS 32.102 [2] and TS 21.905 [5], in that order.

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Credentials: Data that is transferred to establish the claimed identity of an entity, see ITU-T Recommendation X.800 [6].

Plug and Play: The process of connecting a minimally preconfigured node to the transport network, whereby the node, with minimum operator attention, can exchange information with the OAM system and other relevant nodes to an extent that the node is configured and ready to handle traffic.

Plug and Connect: The procedure by which an eNodeB gets basic connectivity information after it is powered up and gets connected to its EM system in a multi-vendor environment. Multi-vendor Plug and Connect is part of the Multi-Vendor Plug and Play.

Self Configuration: The process which brings a network element into service requiring minimal human operator intervention or none at all.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

CA	Certification Authority
CMP	Certificate Management Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Doman Name System
EM	Element Manager
FQDN	Fully Qualified Domain Name
IP@	IP address
MvPnC	Multi-vendor Plug and Connect
MvPnP	Multi-vendor Plug and Play
NAT	Network Address Translation
PnC	Plug and Connect
PnP	Plug and Play
RA	Registration Authority
SC	Self Configuration
SeGW	Security Gateway
TLS	Transport Layer Security
VLAN	Virtual LAN
VM	Vendor Mediator

4 Concepts and background

Provide here an update of See TS 32.816 [4] §5.1.3.1.1 “Establishment of new eNodeB in network”

4.1 Self-Configuration Concept

4.1.1 Logical Function Blocs

4.1.1.1 Address Allocation Function (AAF):

This functional bloc supports the following functions: [SC1], [SC3].

4.1.1.2 OAM Connectivity Establishment Function (OAM CO_EF):

This functional bloc supports the following functions: [SC2], [SC3], [SC4], [SC5], [SC13].

4.1.1.3 Software Management Function (SW_MF):

This functional bloc supports the following functions: [SC3], [SC6], [SC7], [SC8], [SC20], [SC21].

4.1.1.4 Inventory Update Function (Inv_UF):

This functional bloc supports the following functions: [SC16].

4.1.1.5 Self-Test Function (ST_F):

This functional bloc supports the following functions: [SC17].

This function performs eNodeB self-tests.

4.1.1.6 Self-Configuration Monitoring and Management Function (SC_MMF):

This functional bloc supports the following functions: [SC18].

This function monitors the self-configuration process and provides the operator with this information. This function must be able to get information about all other functional blocs. In addition to this it allows the operator to control the execution of the self-configuration process.

4.1.1.6.1 Self-Configuration Monitoring and Management Function (SC_MMF_NM):

SC_MMF_NM (IRP Manager): representing the NM portion of SC_MMF (necessary monitoring and limited interaction capabilities to support an automated optimization), as well as related IRPManager functionality

4.1.1.6.2 Self-Configuration Monitoring and Management Function (SC_MMF_EM):

SC_MMF_EM (IRP Agent): representing the portion of SC_MMF operating below Itf-N, as well as related IRPAgent functionality

4.1.1.7 Call Processing Link (CPL) Set Up Function (CPL_SUF):

This functional bloc supports the following functions: [SC14], [SC15].

4.1.1.8 Radio Network Configuration Data Function (R_CD_F):

This functional bloc supports the following functions: [SC9], [SC11], [SC12].

4.1.1.9 Transport Network Configuration Data Function (T_CD_F):

This functional bloc supports the following functions: [SC9], [SC11], [SC12].

4.1.1.10 NRM IRP Update Function (NRM_UF):

This functional bloc supports the following functions: [SC19].

This function updates the E-UTRAN and EPC NRM IRP with information about the new eNodeB.

4.1.1.11 Radio Network and Transport Network Configuration Data Preparation Function

This functional bloc supports the following functions: [SC10].

4.2 Automatic Radio Configuration Data handling Function (ARCF) Concept

4.2.1 Definitions

ARCF Data: ARCF data are the data which are required for successful activation (of e.g. cell, eNB) that require coordination between several cells and cannot be generated below Itf-N. Some of the ARCF data may be used directly as eNodeB configuration data and some of the ARCF data may be used to generate more other eNodeB configuration data. eNodeB will use the ARCF data together with other configuration data as initial eNodeB radio configuration data. The eNodeB initial radio configuration data will be used for self-configuration.

ARCF Handling: This includes ARCF data preparation, ARCF Data Transfer and ARCF Data Validation.

ARCF Data Preparation: This makes the ARCF data ready in operator's network management system. How to prepare the ARCF data in operator's network management system is out of scope of this specification.

ARCF Data Transfer: This transfers the ARCF data from IRPManager to the IRPAgent,

ARCF Data Validation: This validates the syntax and semantics of ARCF data. It takes place in the IRPAgent.

4.3 Multi-Vendor Plug and Play eNB connection to network Concept

4.3.1 General description

The basic idea of Plug and Play is to avoid pre-configuration of an eNB as far as possible. In an ideal PnP world an eNB equipment is totally agnostic of its future purpose, its location in the network, its addresses, its basic configuration parameters etc... All this information is only supplied step by step during the PnP process.

The required information for the new eNB is stored at specific places. The eNB needs to know how to access these places. The PnP process provides this information to the eNB.

The entities involved in the PnP concept are eNB, DHCP server, DNS Server, Certification Authority server, Element Manager (including the Initial and Serving Element Managers that could be the same in certain deployment scenarios), Security Gateway.

The Plug and Play includes "Plug and Connect" and Self-Configuration. The basic steps of Plug and Connect are described in clause 6.4.3.

After Plug and Connect Self-Configuration procedures are used to complete Plug and Play.

4.3.2 Network Scenarios

4.3.2.1 eNB connected via a Non-Secure, Operator Controlled Network

An eNB is typically connected to the operator's network according to one of the following scenarios:

In Figure 4.3.2-1, the eNB is connected directly to a network controlled by the operator. The eNB can use IP Infrastructure services (DHCP Server, DNS Server, etc.) in the Non-secure Operator Network. The Operator has full control of these nodes. One or more Security Gateways protect the Secure Operator Network from malicious eNBs. Within the Secure Operator Network, there are also IP Infrastructure nodes.

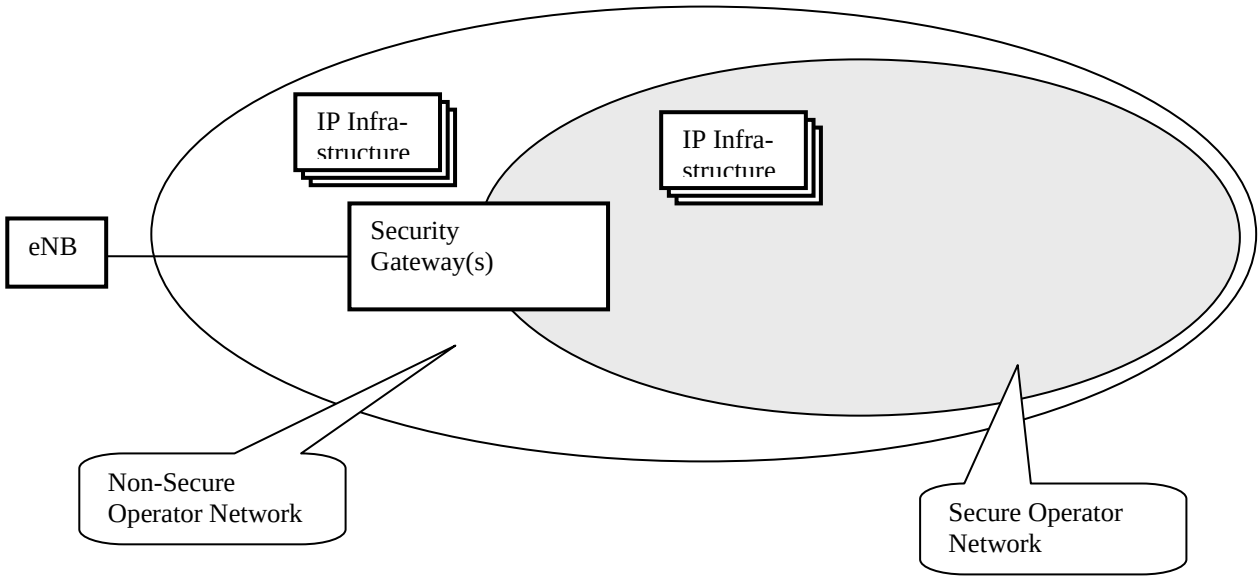

Figure 4.3.2-1 eNB connected to an Non-Secure Operator Network

4.3.2.2 eNB connected via an External Network

In Figure 4.3.2-2, the eNB is connected to a network controlled by an entity external to the Operator. In contrast to the first scenario, the IP Infrastructure nodes in the External Network are not fully controlled by the operator. In both cases, the eNB needs to traverse the Security Gateway(s) to access the nodes in the Secure Operator Network.

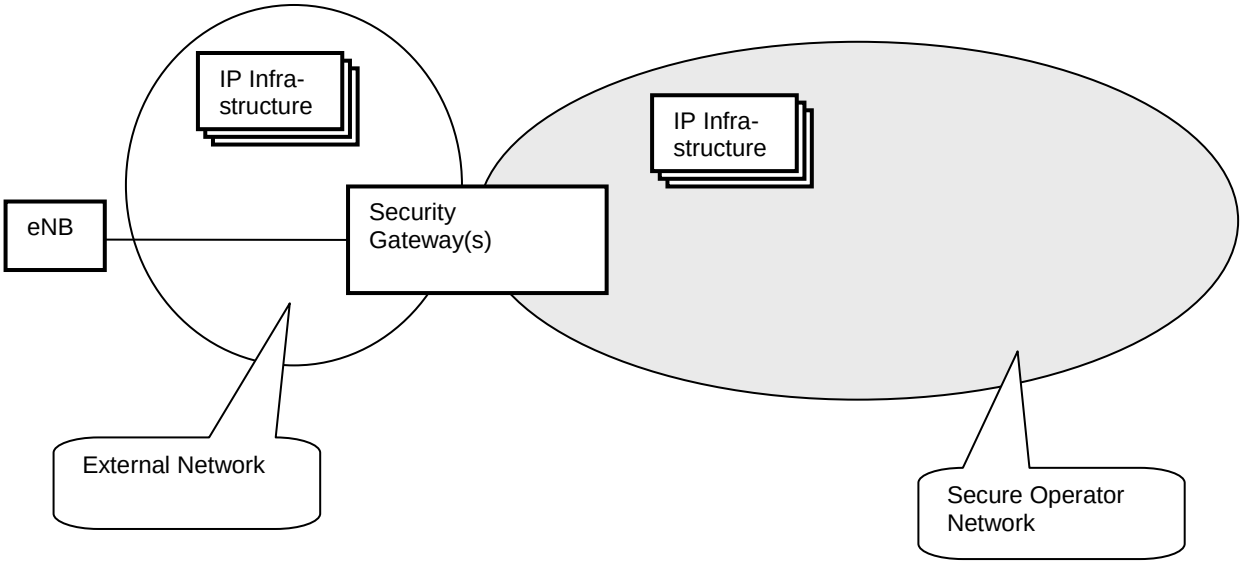

Figure 4.3.2-2 eNB connected to an External Network

4.3.2.3 eNB connection to the OAM Network and multiple CNs via separate SeGWs

Following certificate enrolment with the operator's CA, an eNB establishes a secure tunnel to the SeGW of the OAM network. Through this tunnel it then connects to its DM from which it receives software updates and configuration information, including its transport configuration to the core network(s) it is supposed to connect to. It then typically establishes a separate secure tunnel to the SeGW of the operator's core network. In the case of RAN Sharing, the eNB may establish further tunnels to other Participating Operators' core networks. The OAM and CN SeGWs may or may not be separate physical entities in practice.

Figure 4.3.2-3 shows an example of an eNB connected to the OAM Network and multiple CNs via separate SeGWs.

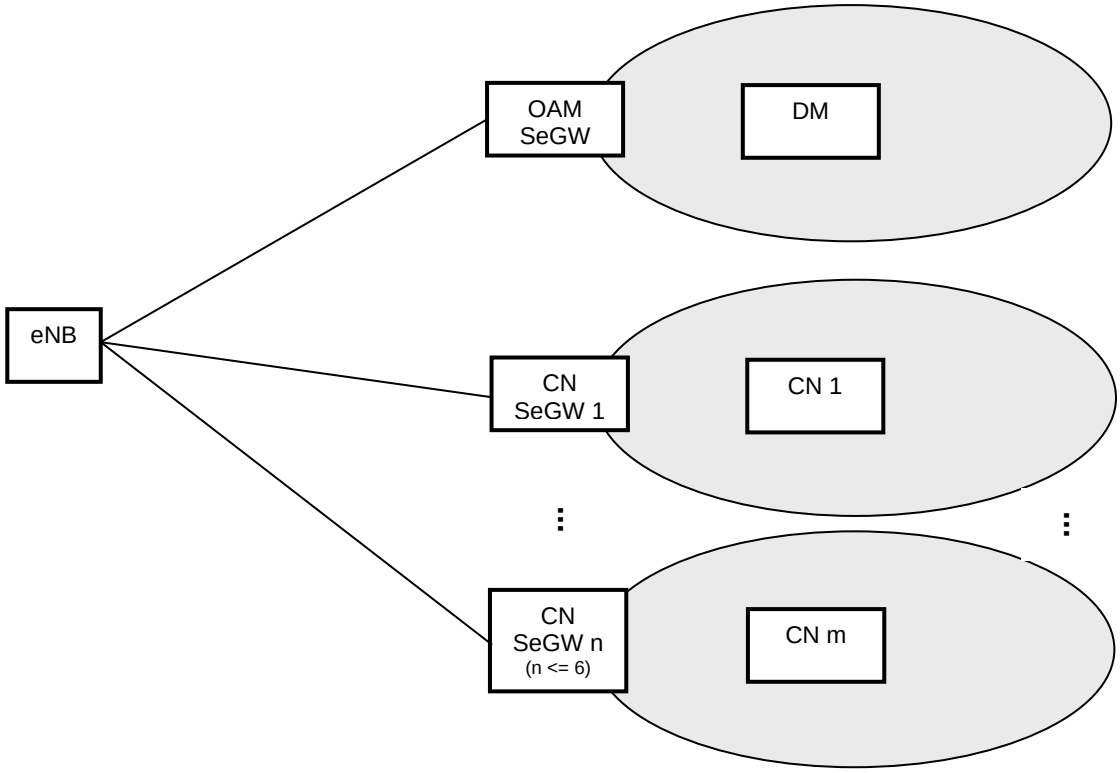

Figure 4.3.2-3 Example of eNB connected to OAM Network and multiple CNs via separate SeGWs

4.3.3 Security Aspects

4.3.3.1 Root Certificate Acquisition:

In accordance to TS 33.310 [yy] §9.2 there are two options how to obtain the operator root certificate:

Option 1: The operator root certificate is provisioned in the base station prior to the CMPv2 protocol run

Option 2: The operator root certificate is provisioned in the base station during the CMPv2 protocol run (as part of the Initialisation Response)

The required pre-provisioning in option 1 is against the basic idea of PnP to minimize pre-provisioning. Therefore from the PnP perspective Option 2 is more interesting. From a security point of view the following considerations are relevant:

Option 2 has the risk that during the CMP initialisation a man-in the middle attack could take place. In order to be successful, such an attack must happen timely during the actual CMP initialization run and the attacker must have access to the access network between base station and RA/CA.
This risk can be assessed as acceptable, given (a) the risks which are present at Options 1's prior provisioning – see below, (b) the short time window of vulnerability, (c) the closed access networks of many operators. In addition, most attacks will only lead to inability of the base station to connect to the network, or to misuse of the new base station by the attacker. The operator should notice it soon if the base station does not connect, and will investigate the issue.

Option 1 avoids the above "time window of vulnerability". On the other hand it requires pre-provisioning of the operator root certificate, either in factory or on-site by service personnel. There is the risk of a security leak during the provisioning of the root certificate within the vendor / commissioning environment.

It seems questionable from a security point of view to allow option 2 also in public Internet (without operator-trusted access network). There the attacks stated above are more probable, and an attacker may even install some (static) catching or spoofing equipment in the public Internet to always capture such "initialization requests".

It is up to the network operator to choose the option with is preferable from his point of view (risk assessment, Plug and Play importance).

4.3.3.2 Number of CA servers

There could be one or more RA/CA server, e. g. one per vendor. If more than one RA/CA server is deployed with one RA/CA server per vendor then the vendor identification would be needed either in the FQDN of the RA server or in the information from the IP AutoConfiguration Service carrying the information about RA/CA server.

4.3.3.3 Number of OAM SeGWs

There could be one or more OAM SeGW, e. g. one per vendor. If more than one OAM SeGW is deployed with one OAM SeGW per vendor then the vendor identification would be needed either in the FQDN of the OAM SeGW or in the information from the IP AutoConfiguration Service carrying the information about OAM SeGW.

5 Business Level Requirements

5.1 Self- Configuration of eNodeB's

REQ_SCMAN_CON_1 The actor on NM level shall be able to manage the self-configuration process.

REQ_SCMON_CON_1 The actor on NM level shall be able to monitor the execution of the self-configuration process.

REQ_SCMON_CON_2 To support the monitoring of the execution of the self-configuration process, existing capabilities shall be reused as much as possible.

REQ_SCSW_CON_1 The software download, installation, activation and fallback should be automated as much as possible so that no or only minimal manual intervention is required.

REQ_SCSW_CON_1 see **REQ_SW_CON_4**

REQ_SCSW_CON_2 see **REQ_SW_CON_2**

REQ_SCOCE__CON_1 The OAM connectivity (incl. the IP address allocation) should be established in a fully automated manner.

REQ_SCOCE_CON_2 The amount of parameters that needs to be preconfigured should be minimized.

REQ_SCIU_CON_1 Inventory information about the new equipment shall be reported to the actor at NM level as part of the self-configuration process.

REQ_SCIU_CON_2 Inventory information shall be made available to the IRPManager reusing existing capabilities as much as possible.

REQ_SCRCD_CON_1 The radio configuration data shall be made available to the eNodeB as part of the self-configuration process.

REQ_SCTCD_CON_1 The transport configuration data shall be made available to the eNodeB as part of the self-configuration process.

REQ_SCCPLSU_CON_1 X2- and S1-interfaces shall be set up as part of the self-configuration process, based on the radio configuration, the transport configuration and Neighbour cell Relation information made available to the eNodeB.

Note: If there is no Neighbour cell Relation information provided, then no X2 interface is set up as part of the self-configuration process.

5.1.1 Actor roles

5.1.2 Telecommunications resources

5.1.3 High-level use cases

5.2 Business Requirements for Multi Vendor Plug and Play eNB connection to network

REQ_PnP_CON_1 Plug and Play for an eNB´s connection to the network shall use standard protocols.

REQ_PnP_CON_2 VPN tunnels needed for Plug and Play for an eNB´s connection to the network shall be set-up automatically.

REQ_PnP_CON_3 The complete key management during Plug and Play for an eNB´s connection to the network shall be a full automatic secure procedure, based on procedures defined by 3GPP SA3.

REQ_PnP_CON_4 After Plug and connect an eNB and potentially additional self-configuration of the eNB it shall be possible to bring an eNB into service

REQ_PnP_CON_5 As a result of Plug and Play for an eNB´s connection to the network and potentially additional self-configuration of the eNB, the newest software and parameter settings as defined by the network operator shall be used in the eNB.

REQ_PnP_CON_6: It shall be possible to perform the MvPnP procedures using secure protocols and procedures between the eNB and OAM.

REQ_PnP_CON_7 eNB shall be able to get its own IP addresses and EM IP address without manual configuration.

REQ_PnP_CON_8 For Plug and Connect the Element Manager shall only be accessible by authenticated and authorized eNBs.

REQ_PnP_CON_9 For Plug and Connect the initial and final configuration of the eNB (or the information how to retrieve them) shall only be accessible by authenticated and authorized eNBs.

REQ_PnP_CON_10 The MvPnP solution shall be usable for IPv4-only networks, for IPv6-only networks and for dual stack IP networks.

REQ_PnP_CON_11 MvPnP procedures shall support Network Sharing including the connection of an eNB to multiple core networks and PLMNs.

REQ_PnP_CON_12 MvPnP procedures shall support connection of eNBs with and without NAT and via External Networks or Non-Secure Operator Networks.

6 Specification level requirements

6.1 General

6.2 Actor roles

6.3 Telecommunications resources

6.4 Use cases

6.4.1 Use case for Automatic Radio Network Configuration Data Handling

6.4.1.1 Use case radio network configuration data request, transfer and validity check

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal (*)	Transfer the radio network configuration data to the IRPAgent and ensure that it is valid when it is used during self-configuration.	
Actors and Roles (*)	IRPManager as user	
Telecom resources	The E-UTRAN network including its OSS.	
Assumptions	OAM connection is working. IRPAgent cannot determine all radio configuration data on its own.	
Pre conditions	NA	
Begins when	Radio network configuration data is to be made known to the IRPAgent.	
Step 1 (O)	[ARCF-1-1] IRPAgent indicates need for radio configuration data to the IRPManager	
Step 2 (M)	[ARCF-1-2] IRPManager transfers the radio configuration data to IRPAgent or indicates to IRPAgent where the radio configuration data is available and IRPAgent retrieves the data from there	
Step 3 (O)	[ARCF-1-3] IRPManager requests IRPAgent to validate the received radio configuration data	
Step 4 (M)	[ARCF-1-4] IRPAgent validates the received radio configuration data	
Ends when	Ends when all steps identified above are completed or when an exception occurs	
Exceptions	One of the steps identified above fails.	
Post Conditions	The self-configuration process can use the radio configuration data.	
Traceability	FFS	

6.4.2 Use case Self-configuration of a new eNodeB

This use case starts with the first initial self test and ends when the eNodeB is taken into operation.

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal (*)	After physical installation, put in an automated manner the eNodeB into a state to be ready to carry traffic.	
Actors and Roles (*)	FFS	
Telecom resources	The E-UTRAN/EPC network including its OSS.	
Assumptions	IP network connectivity exists between the eNodeB and the OAM (sub) systems providing support for the self-configuration process.	
Pre conditions	The eNodeB is physically installed and physically connected to an IP network.	
Begins when	The field personnel start the self-configuration process. It is also possible that the process is triggered automatically after the completion of an eNodeB self-test.	
Step 1 (*) (M|O)	The order of the bullet points in the list below does not imply any statements on the order of execution. [SC1] An eNodeB IP address is allocated to the new eNodeB. [SC2] Basic information about the transport network (e. g. gateways) environment is provided to the eNodeB. With this information the eNodeB is able to exchange IP packets with other internet hosts. [SC3] The eNodeB provides information about its type, hardware and other relevant data about itself to the OAM (sub) systems providing support for the self-configuration process. [SC4] The address(es) of the OAM (sub) system(s) providing support for the self-configuration process (e.g. subsystem for software download, subsystem for configuration data download) is provided to the eNodeB. The address is equal to an IP address and a port number, or a DNS name and port number, or an URI. [SC5] The address(es) of the OAM (sub)system(s) providing support for normal OAM functions after completion of the self-configuration process are provided to the eNodeB. The address is equal to an IP address and a port number, or a DNS name and port number, or an URI. [SC6] The eNodeB connects to the OAM system providing support for the software download. [SC7] The decision which software or software packages have to be downloaded to the eNodeB is taken. [SC8] The software is downloaded into the eNodeB. [SC9] The eNodeB connects to the OAM system providing support for the configuration data download. [SC10] The (transport and radio) configuration data for the eNodeB is made available by either preparing it or making prepared configuration data available. [SC11] The (transport and radio) configuration data is downloaded into the eNodeB. [SC12] Dependent nodes (MMEs, eNodeBs) are updated with new configuration data as well (if required). [SC13] The eNodeB connects to the OAM (sub) system(s) providing support for normal OAM functions after completion of the self-configuration process. [SC14] The S1-links are be set up. [SC15] The (planned) X2-links are be set up. [SC16] The inventory system in the OAM is informed that a new eNodeB is in the field. [SC17] The eNodeB performs a self-test. Self-tests of different types can run at different places within the self-configuration procedure. [SC18] The operator is informed about the progess of the self-configuration process and important events occuring during the self-configuration process. [SC19] The network resource models visible over Itf-N are updated during and after the self-configuration process. [SC20] SW is installed, i.e. prepared in such a way, that the NE is ready to use it. For some implementations this step is done not at all or considered part of [SC21] or of [SC8]. [SC21] SW is activated, i.e. final provisions are done such that the NE is allowed to use the SW. For some implementations this step is considered part of [SC20] or of [SC8].	
Ends when (*)	Ends when all steps identified above are successfully completed or when an exception occurs.	
Exceptions	FFS.	
Post Conditions	The eNodeB is ready to carry traffic.	

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Traceability (*)		

Security aspects are FFS.

6.4.3 Use case Multi Vendor Plug and Connect eNB to network

Table 6.4.3-1

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	After physical installation, connect the eNB to its initial Element Manager and to the Core Network(s) as automatically as possible.	
Actors and Roles	eNB as user	
Telecom resources	eNB; IP networks: Non-Secure Operator Network, External Network, and its elements like DHCP server optionally DNS, CA/RA servers, Security Gateway(s) (each protecting one or more Secure Operator Networks), Secure Operator Network(s) including Element Manager(s), Core Network(s)	
Assumptions	There is a functional power supply for the eNB. There may be one or more IP Autoconfiguration Services like DHCP and Router Advertisements and zero or more DNS servers.	
Pre conditions	The eNB is physically installed. IP connectivity exists between the involved telecom resources. The involved telecom resources are functional. The relevant information is stored and available: - Vendor Certificate at the eNB - Operator Certificate at the CA/RA - For the External Network or Non-Secure Operator Network: - (Outer) IP autoconfiguration information at the IP Autoconfiguration Service - FQDN of the initial OAM SeGW at the eNB and/or FQDN or IP address of the initial OAM SeGW at the IP Autoconfiguration Service - FQDN of the CA/RA servers at the eNB and/or FQDN or IP address of the CA/RA servers at the IP Autoconfiguration Service - If FQDNs need to be resolved, corresponding IP address(es) at the DNS server(s) - For the Secure Operator Network: - (Inner) IP autoconfiguration information at the IP Autoconfiguration Service or at the initial OAM SeGW - FQDN or IP address of the initial EMS at the eNB and/or DHCP Server of the Secure Operator Network. - If FQDNs need to be resolved, corresponding IP address(es) at the DNS server(s) - Configuration and software for the eNB at the EM(s)	
Begins when	The eNB is powered up.	
Step 1 (M)	If a VLAN ID is available the eNB uses it. Otherwise the eNB uses the native VLAN where PnP traffic is sent and received untagged	
Step 2 (M)	The eNB acquires its IP address through stateful or stateless IP autoconfiguration. This may provide 0 or more DNS server addresses.	
Step 3 (M)	The eNB acquires the IP address of the CA/RA server. The FQDN of the CA/RA server may be pre-configured in the eNB or the FQDN or IP address of the CA/RA server may be provided by the IP Autoconfiguration Service. FQDNs are resolved through the DNS if necessary. Information provided by the IP Autoconfiguration Services shall supersede those pre-configured at the eNB.	
Step 4 (M)	The eNB performs Certificate Enrolment.	
Step 5 (M)	The eNB acquires the IP address of the OAM SeGW. The FQDN of the OAM SeGW may be pre-configured in the eNB or the FQDN or the IP address of the OAM SeGW may be provided by the IP Autoconfiguration Service. FQDNs are resolved through the DNS if necessary.	
Step 6 (M)	The eNB establishes a secure connection (tunnel) to the Security Gateway given by Step 5. The eNB receives its (inner) IP autoconfiguration information (which may be the same as the outer IP address obtained in step2) and optionally the address of one or more DNS servers within the Secure Operator Network from the Configuration Parameters of IKEv2 during tunnel establishment.	
Step 7 (M)	The eNB acquires the IP address of the correct Element Manager by either, issuing a DHCP request including the eNB's vendor information, resolving FQDNs via DNS if necessary, or by having a pre-configured FQDN (including the eNB's vendor information) resolved via DNS.	Secure connection

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Step 8 (M)	The eNB establishes a connection to the provided EM and acquires its configuration and software if any. The configuration may contain an address to another EM that this specific node shall use as EM. The configuration may contain an address to another SeGW that should be used before connecting to the EM. The eNB may then - release the connection to the current EM and OAM SeGW and then restart (returning to step 1), - release the connection to the current EM and OAM SeGW and then return to step 6, - release the connection to the current EM and then repeat step 8, or - continue with step 9.	Secure connection
Step 9 (M)	The eNB establishes a connection to the Core Network(s) using the transport (VLAN ID, IP addresses) and security parameters provided in step 8.	
Ends when	Ends when all mandatory steps identified above are successfully completed or when an exception occurs.	
Exceptions	One of the steps identified above fails.	
Post Conditions	One or more secure connections exist between the eNB and the Element Manager and the Core Network(s). Via the connection to the Element Manager the eNB can receive further instructions to become operational and carry user traffic, e.g. the administrativeState is set to “unlocked”.	
Traceability	All requirements of clause 5.2 and 6.5.3.	

Editor’s note: The CA/RA server itself may be protected by a SeGW.

Security aspects – e.g. prevention of unauthorized network access and of fake parameters supplied to the eNBs etc. - have special importance. Security related sub-steps to establish secure connections are not shown in table 6.4.3-1. More security aspects are described in a specific chapter (see clause 4.3.3).

6.5 Requirements

6.5.1 Automatic Radio Network Configuration Data Handling

REQ-ARCF-FUN-1: IRPManager shall be able to transfer the ARCF data to IRPAgent or indicate to IRPAgent where the ARCF data is available for downloading.

REQ-ARCF-FUN-2: IRPManager should be able to request IRPAgent to validate the previously downloaded ARCF data.

REQ-ARCF-FUN-3: IRPAgent shall be able to check the consistency, syntax and semantic of the downloaded ARCF data to ensure that the ARCF data can be implemented in the network.

6.5.2 Self-configuration of a new eNodeB

The following requirements apply to the macro eNB only. Requirements for the HNB can be found in TR 32.821.

The way to make any information available to eNB is outside the scope of standardisation.

Conflict resolution in case of contradicting information made aware to the eNodeB is outside the scope of standardisation.

6.5.2.1 Self-Configuration Management and Monitoring

6.5.2.1.1 Management Part

REQ_SCMAN_FUN_1
It shall be possible for an IRPManager to retrieve

- information regarding how an NE or a group of NEs behaves during self-configuration, i.e. in which sequence the essential steps of self-configuration are executed
- information regarding where the IRPManager can interact with a self-configuration - by suspending the self-configuration process at one or more self-configuration stop points.
Steps, their sequence and their stop point qualification are not imposed by the standard.

REQ_SCMAN_FUN_2
If choices for stop points to suspend the SWM process are offered, then it shall be possible for an IRPManager to choose/select among them where it will suspend (stop) a self-configuration process (i.e. to ensure fulfillment of pre-conditions for the step like the fulfillment of the presence of required input data for the step).
The IRPManager shall be able to read or select or de-select the stop points offered.
The IRPManager shall be informed about creation and deletion of a profile which is a holder of information regarding the offered self configuration steps, the offered sequence of the steps and the configuration steps stop points.
The IRPManager should be able to change the content of a created profile and be informed about the change.

REQ_SCMAN_FUN_3
It shall be possible for an IRPManager to resume a suspended self-configuration for one or multiple NEs.

REQ_SCMAN_FUN_4
It shall be possible for an IRPManager to terminate an currently ongoing self-configuration for one or multiple NEs.
After a terminattion it is not possible to resume the self-configuration.

6.5.2.1.2 Monitoring Part

REQ_SCMON_FUN_1
The IRPAgent shall send an alarm in case of failures during the self-configuration process.

REQ_SCMON_FUN_2
The IRPAgent should report the progress of a self-configuration of one or multiple NEs to the IRPManager.

REQ_SCMON_FUN_3
When a self-configuration profile is created or deleted, then the IRPAgent shall inform the IRPManager about this creation and deletion.
When the optional change of a self-configuration profile is performed, then the IRPAgent shall inform the IRPManager about such a change.

REQ_SCMON_FUN_4
It shall be possible for IRPManager to retrieve information about the progress of a self-configuration.

REQ_SCMON_FUN_5
The IRPAgent shall send a notification about the start, stop, completion and optionally cancellation of a self-configuration.

REQ_SCMON_FUN_6
The IRPAgent shall inform the IRPManager whenever the self-configuration process has been suspended or resumed

6.5.2.2 Software Management

REQ_SCSW_FUN_1 see **REQ_SWM_FUN_1 in 32.531**

REQ_SCSW_FUN_2 see **REQ_SWM_FUN_2 in 32.531**

REQ_SCSW_FUN_3 see **REQ_SWM_FUN_4 in 32.531**

REQ_SCSW_FUN_4 see **REQ_SWM_FUN_5 in 32.531**

REQ_SCSW_FUN_5 see **REQ_ASWM_FUN_1 in 32.531**
REQ_SCSW_FUN_6 see **REQ_ASWM_FUN_2 in 32.531**
REQ_SCSW_FUN_7 see **REQ_ASWM_FUN_3 in 32.531**
REQ_SCSW_FUN_8 see **REQ_ASWM_FUN_4 in 32.531**

REQ_SCSW_FUN_9 see **REQ_ASWM_FUN_5 in 32.531**

6.5.2.3 Address Allocation and OAM Connectivity Establishment

REQ_SCOCE_FUN_1
The automatic establishment of the OAM connectivity shall be fully secured.

REQ_SCOCE_FUN_2
The IRPManager shall be informed that the eNB has reached OAM connectivity.

6.5.2.4 Inventory Update

The details of the inventory information to be reported are FFS.

6.5.2.5 Self-Test

FFS

6.5.2.6 Radio Configuration Data

FFS

6.5.2.7 Transport Configuration Data

FFS

6.5.2.8 Call Processing Link Set-Up

FFS

6.5.2.9 NRM IRP Update

REQ_SCNRMU_FUN_1
The related E-UTRAN NRM IRP and EPC NRM IRP instances shall be created and updated.

6.5.3 Specification Requirements for Multi-Vendor Plug and Play eNB connection to network

REQ_PnP_FUN_1 The establishment of secure tunnels from the eNB to the OAM or Core Network(s) shall support NAT traversal.

7. Functions and Architecture

7.1 Self-Configuration Logical Architecture

The lines between the functional blocks do not indicate specific 3GPP interfaces.

For the abbreviations used, please see the headlines of chapter 4.

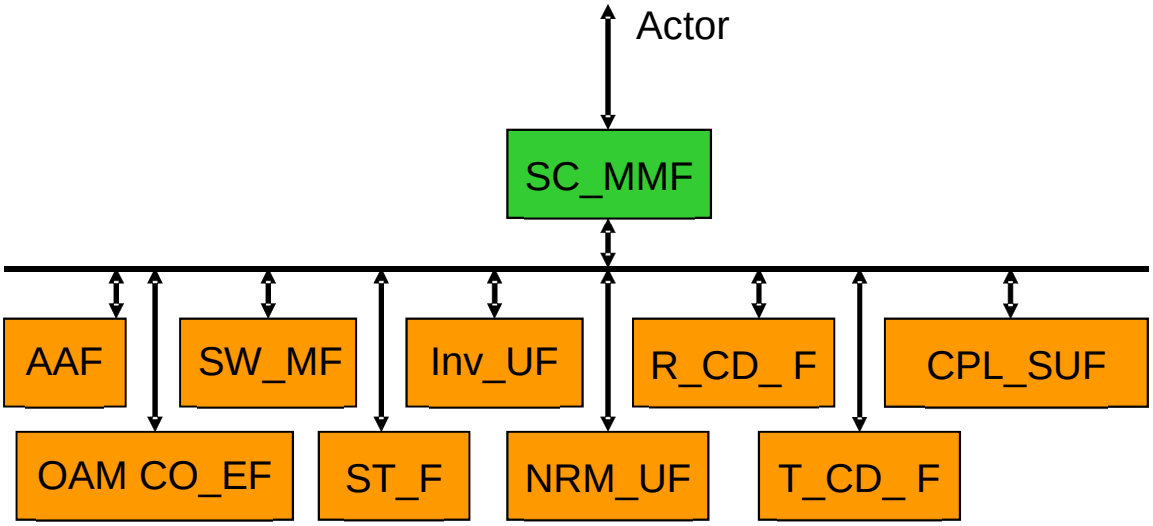

Figure 7.1-1: Self-Configuration Logical Architecture

7.2 Self-Configuration Reference Model

The SC_MMF has a part located in the EM and a part located at the NM.

For the abbreviations used, please refer to Chapter 4.

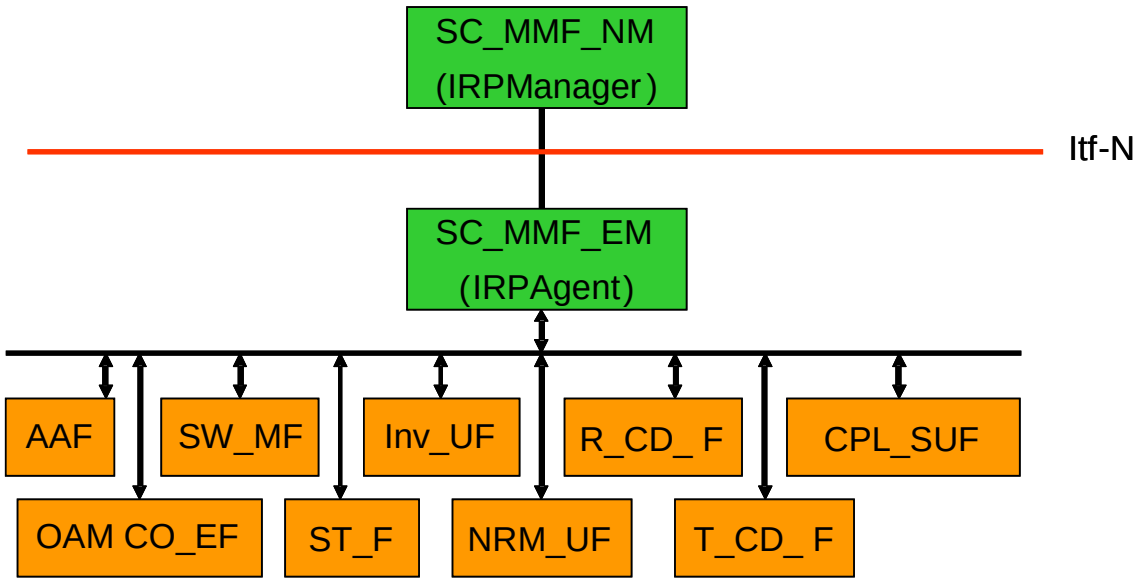

Figure 7.2-1: Self-Configuration Reference Model

Annex A (informative): Graphical representation of the PnC Use Case

The Multi-Vendor eNB Plug and Connect procedure, given in section 6.4.3 are classified into two sets corresponding to those conducted at External Network (or Non-secure Operator Network) and those conducted at the Secure Operator Network. An interpretation of these procedures is depicted in figures A.1 and A.2 respectively.

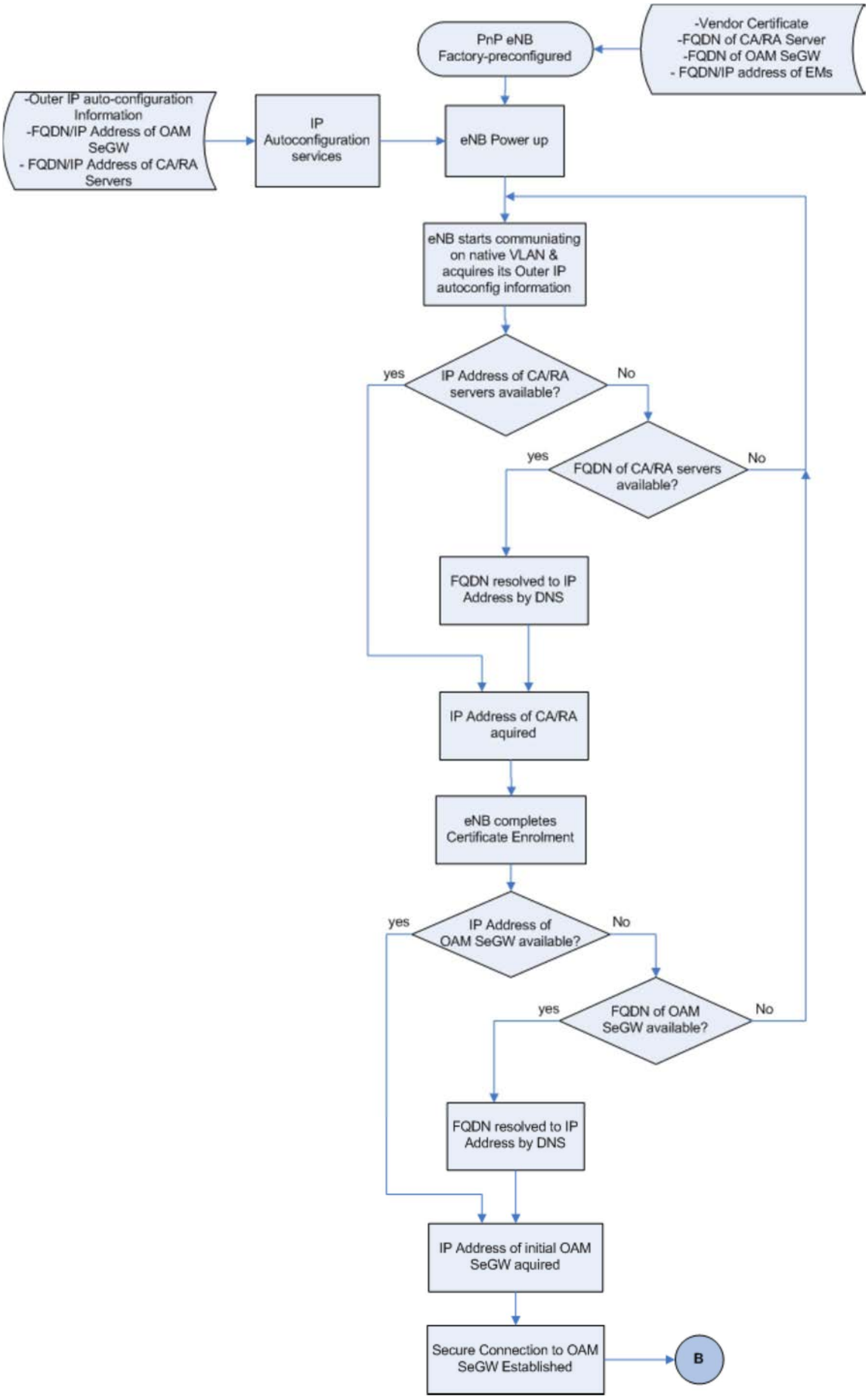

Figure A.1: PnC procedure for the External Network or Non-secure Operator Network.

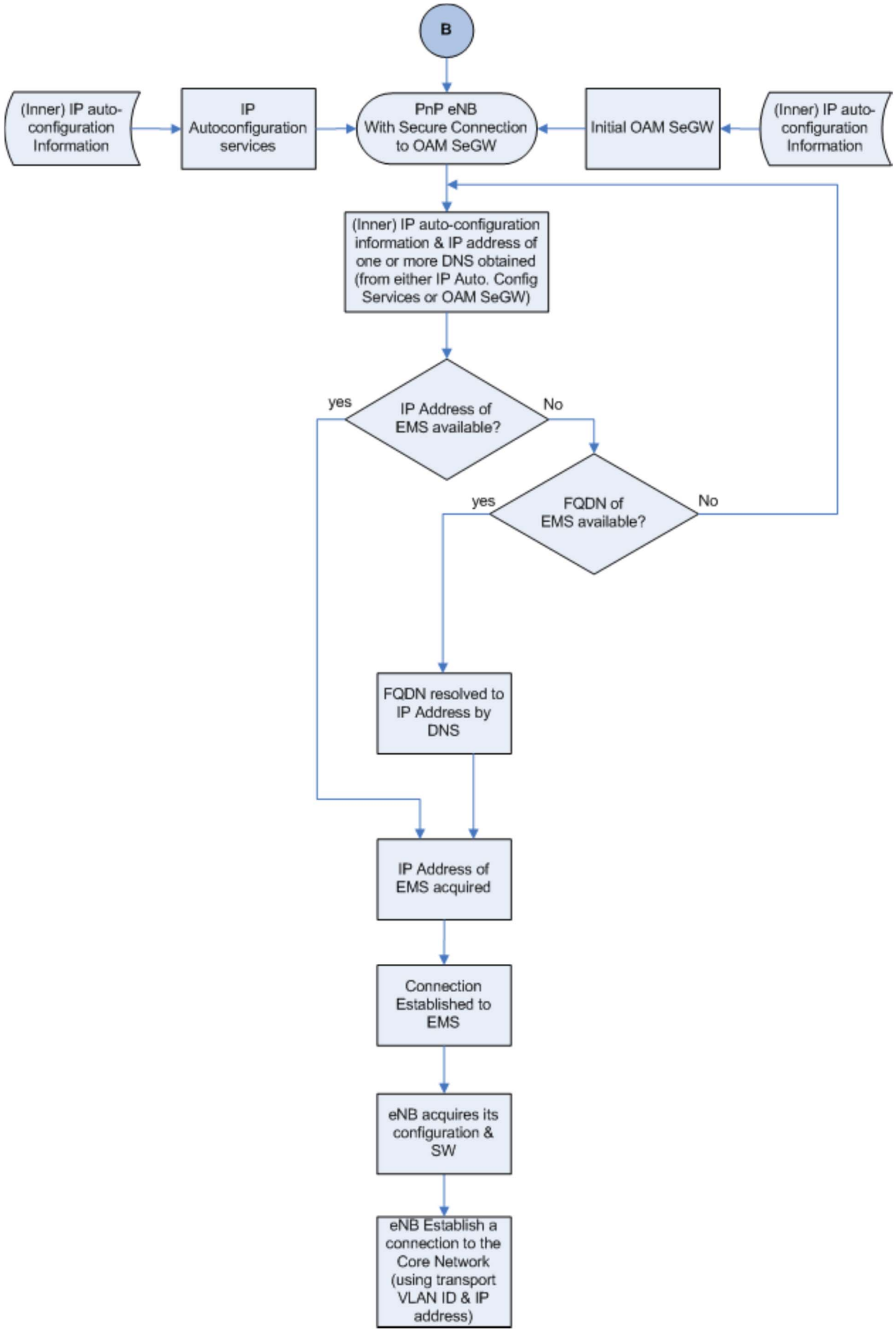

Figure A.2: PnC Procedure for the secure Operator Network.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2008-12	SP-42	SP-080713	--	--	Submitted to SA#42 information and approval	1.0.0	8.0.0
2009-09	SP-45	SP-090627	001	--	Removal of inconsistency	8.0.0	9.0.0
2010-03	SP-47	SP-100035	002	--	Clarifying Editor's Notes in TS 32.501	9.0.0	9.1.0
2010-03	SP-47	SP-100035	003	--	Introducing ARCF (Automatic Radio Configuration Function)	9.0.0	9.1.0
2011-03	-	-	-	-	Update to Rel-10 version (MCC)	9.1.0	10.0.0
2012-09	SP-57	SP-120645	004	1	Clarification of eNodeB state after self-configuration	10.0.0	11.0.0
2013-09	SP-61	SP-130465	006	-	Introducing MUPPET features	11.0.0	12.0.0
2013-12	SP-62	SP-130629	007	3	VLAN option for Stage 1	12.0.0	12.1.0
2016-01	-	-	-	-	Update to Rel-13 version (MCC)	12.1.0	**13.0.0**
2017-04	SA#75	-	-	-	Promotion to Release 14 without technical change	13.0.0	**14.0.0**
2018-06	-	-	-	-	Update to Rel-15 version (MCC)	14.0.0	**15.0.0**
2020-07	-	-	-	-	Update to Rel-16 version (MCC)	15.0.0	**16.0.0**
2022-04	-	-	-	-	Update to Rel-17 version (MCC)	16.0.0	**17.0.0**

History

Document history		
V17.0.0	April 2022	Publication