ETSI TS 128 314 V17.0.0 (2022-05)

5G;
Management and orchestration;
Plug and Connect;
Concepts and requirements
(3GPP TS 28.314 version 17.0.0 Release 17)

Reference
DTS/TSGS-0528314vh00

Keywords
5G

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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

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

TS 28.314: "Plug and Connect; Concepts and requirements".

TS 28.315: "Plug and Connect; Procedure flows".

TS 28.316: "Plug and Connect; Data formats".

1 Scope

The present document specifies concepts, use cases and requirements for *Plug and Connect* NE in 3GPP systems.

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 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[3] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol".

[4] IETF RFC 4211: "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms 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].

Plug and Connect: The procedure by which a NE gets basic connectivity information after it is powered up and gets connected to its management system.

Software and Configuration Server (SCS): A server that provides software and configuration functions for each connected network element.

3.2 Symbols

Void.

3.3 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	Domain Name System
FQDN	Fully Qualified Domain Name
NAT	Network Address Translation

NE	Network Element
PnC	Plug and Connect
RA	Registration Authority
SCS	Software and Configuration Server
SeGW	Security Gateway
VLAN	Virtual LAN

4 Concepts and background

4.1 Plug and Connect Concept

4.1.1 General description

Plug and connect is a list of procedures for connecting the NE to its management system. The basic steps of Plug and Connect are described in clause 6.1.1.

The entities involved in the PnC concept are NE, DHCP server, DNS Server, Certification Authority server, SCS (including the Initial and Serving SCS that could be the same in certain deployment scenarios), Security Gateway.

4.1.2 Network Scenarios

4.1.2.1 NE connected via a Non-Secure, Operator Controlled Network

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

In Figure 4.1.2.1.1, the NE is connected directly to a network controlled by the operator. The NE 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 NEs. Within the Secure Operator Network, there are also IP Infrastructure nodes.

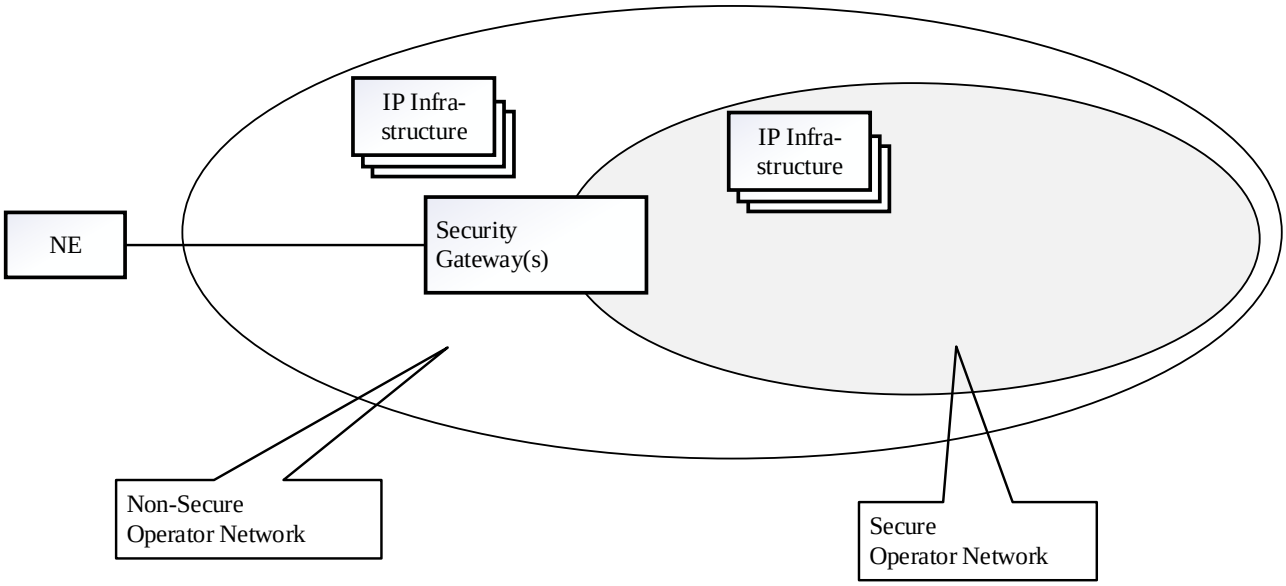

Figure 4.1.2.1.1: NE connected to a Non-Secure Operator Network

4.1.2.2 NE connected via an External Network

In Figure 4.1.2.2.1, the NE 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 NE needs to traverse the Security Gateway(s) to access the nodes in the Secure Operator Network.

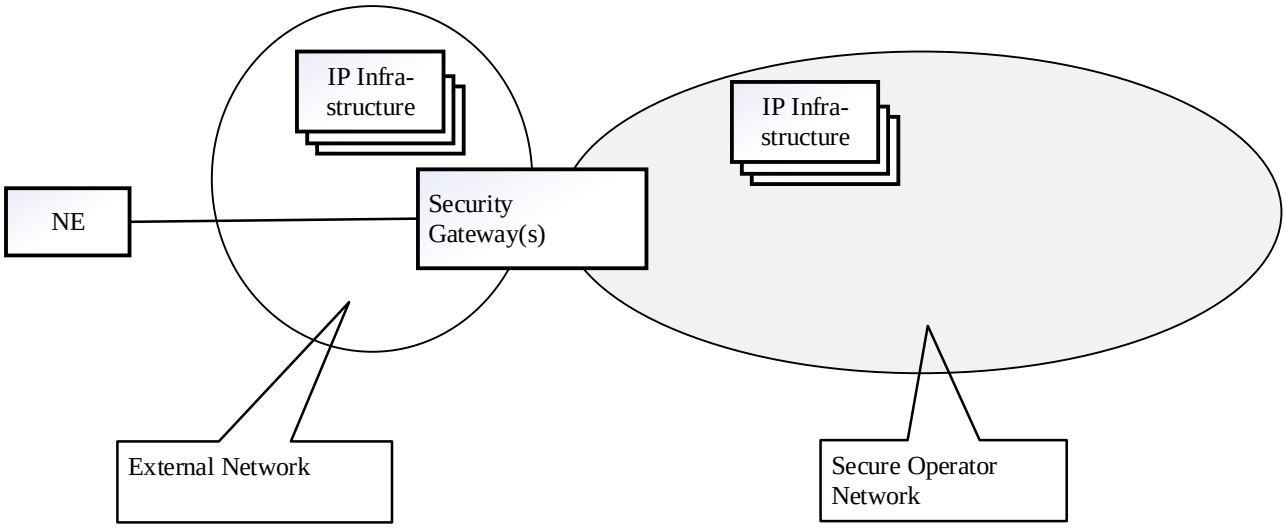

Figure 4.1.2.2.1: NE connected to an External Network

4.1.3 Security Aspects

4.1.3.1 Root Certificate Acquisition:

In accordance to TS 33.310 [2] clause 9.2 there are two options how to obtain the operator root certificate:

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

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

The required pre-provisioning in option 1 is against the basic idea of PnC to minimize pre-provisioning. Therefore from the PnC 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 happens timely during the actual CMP initialization run and the attacker has access to the access network between NE 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 NE to connect to the network, or to misuse of the new NE by the attacker. The operator should notice it soon if the NE 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 Connect importance).

The enrolment of NE shall use the CMPv2 protocol as specified in RFC 4210 [3] and RFC 4211 [4]. Security mechanism is further specified in TS 33.310 [2] clause 9.3.

4.1.3.2 Number of CA servers

There could be one or more RA/CA server, e.g. one per NE 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.

4.1.3.3 Number of OAM SeGWs

There could be one or more OAM SeGW, e.g. one per NE 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 Business Requirements for Plug and Connect

REQ_PnC_CON_1 Plug and Connect shall use standard protocols.

REQ_PnC_CON_2 VPN tunnels needed for Plug and Connect shall be set-up automatically.

REQ_PnC_CON_3 The complete key management during Plug and Connect shall be a fully automatic secure procedure, based on procedures defined by 3GPP SA3.

REQ_PnC_CON_4: It shall be possible to perform the Plug and Connect procedures using secure protocols and procedures between the NE and OAM.

REQ_PnC_CON_5 An NE shall be able to get its own IP addresses and SCS IP address without manual configuration.

REQ_PnC_CON_6 For Plug and Connect the SCS shall only be accessible by authenticated and authorized NEs.

REQ_PnC_CON_7 For Plug and Connect the initial and final configuration of the NE (or the information how to retrieve them) shall only be accessible by authenticated and authorized NEs.

REQ_PnC_CON_8 The Plug and Connect solution shall be usable for IPv4-only networks, for IPv6-only networks and for dual stack IP networks.

REQ_PnC_CON_9 Plug and Connect procedures shall support connection of NEs with and without NAT and via External Networks or Non-Secure Operator Networks.

6 Specification Level Requirements

6.1 Use Cases

6.1.1 Use case Plug and Connect

Table 6.1.1.1

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	After physical installation, connect the NE to its SCS as automatically as possible.	
Actors and Roles	NE as user. In this use case NE is the RAN NE. Other types of NE might also be compliant and use this use case. Examples of NEs are: - gNB - eNB The NE within virtualization is not addressed.	
Telecom resources	NE; 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 SCS(s)	

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Assumptions	There is a functional power supply for the NE. There may be one or more IP Autoconfiguration Services like DHCP and Router Advertisements and zero or more DNS servers.	
Pre conditions	The NE 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 NE - 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 NE and/or FQDN or IP address of the initial OAM SeGW at the IP Autoconfiguration Service - FQDN of the CA/RA servers at the NE 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 SCS at the NE 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 NE at the SCS(s)	
Begins when	The NE is powered up.	
Step 1 (M)	If a VLAN ID is available the NE uses it. Otherwise the NE uses the native VLAN where PnC traffic is sent and received untagged	
Step 2 (M)	The NE acquires its IP address through stateful or stateless IP autoconfiguration. This may provide 0 or more DNS server addresses.	
Step 3 (M)	The NE acquires the IP address of the CA/RA server. The FQDN of the CA/RA server may be pre-configured in the NE 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 NE.	
Step 4 (M)	The NE performs Certificate Enrolment.	
Step 5 (M)	The NE acquires the IP address of the OAM SeGW. The FQDN of the OAM SeGW may be pre-configured in the NE 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 NE establishes a secure connection (tunnel) to the Security Gateway given by Step 5. The NE 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 NE acquires the IP address of the correct Element Manager by either, issuing a DHCP request including the NE's vendor information, resolving FQDNs via DNS if necessary, or by having a pre-configured FQDN (including the NE's vendor information) resolved via DNS.	Secure connection
Step 8 (M)	The NE establishes a connection to the provided SCS and acquires its configuration and software if any. The configuration may contain an address to another SCS that this specific node shall use as SCS. The configuration may contain an address to another SeGW that should be used before connecting to the SCS. The NE may then - release the connection to the current SCS and OAM SeGW and then restart (returning to step 1), - release the connection to the current SCS and OAM SeGW and then return to step 6, - release the connection to the current SCS and then repeat step 8.	Secure connection
Ends when	Ends when all mandatory steps identified above are successfully completed or when an exception occurs.	

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Exceptions	One of the steps identified above fails.	
Post Conditions	One or more secure connections exist between the NE and the SCS. Via the connection to the SCS the NE can receive further instructions to become operational and carry user traffic, e.g. the administrativeState is set to "unlocked".	
Traceability	All requirements of clauses 5.1 and 6.2.1.	

Security aspects – e.g. prevention of unauthorized network access and of fake parameters supplied to the NEs, etc. - have special importance. Security related sub-steps to establish secure connections are not shown in table 6.1.1.1. More security aspects are described in clause 4.1.3.

6.2 Requirements

6.2.1 Specification Requirements for Plug and Connect

REQ_PnC_FUN_1 The establishment of secure tunnels from the NE to the OAM shall support NAT traversal.

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

The NE Plug and Connect procedure, given in clause 6.1.1 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.

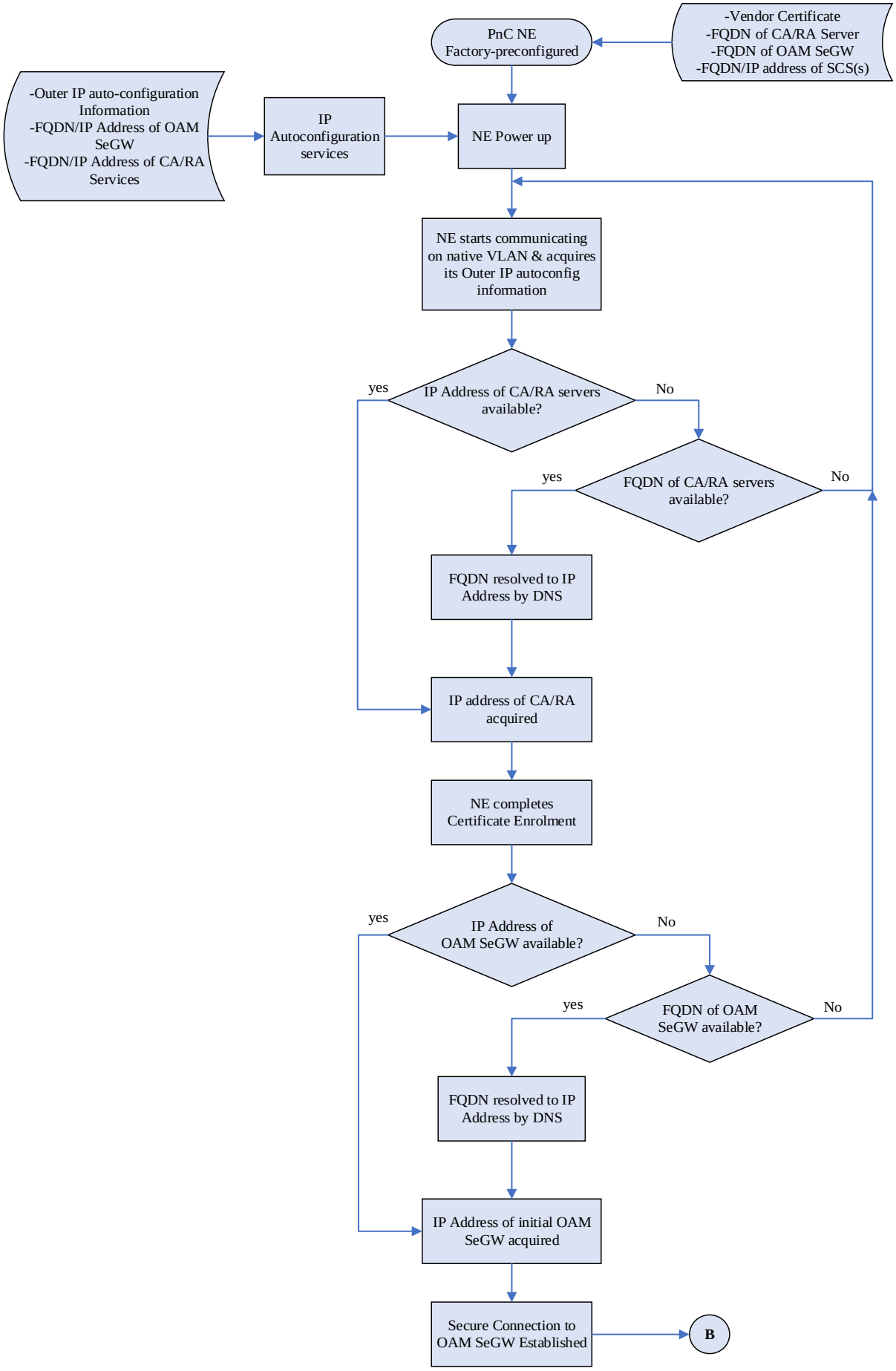

Figure A.1: PnC procedure for the External Network or Non-secure Operator Network

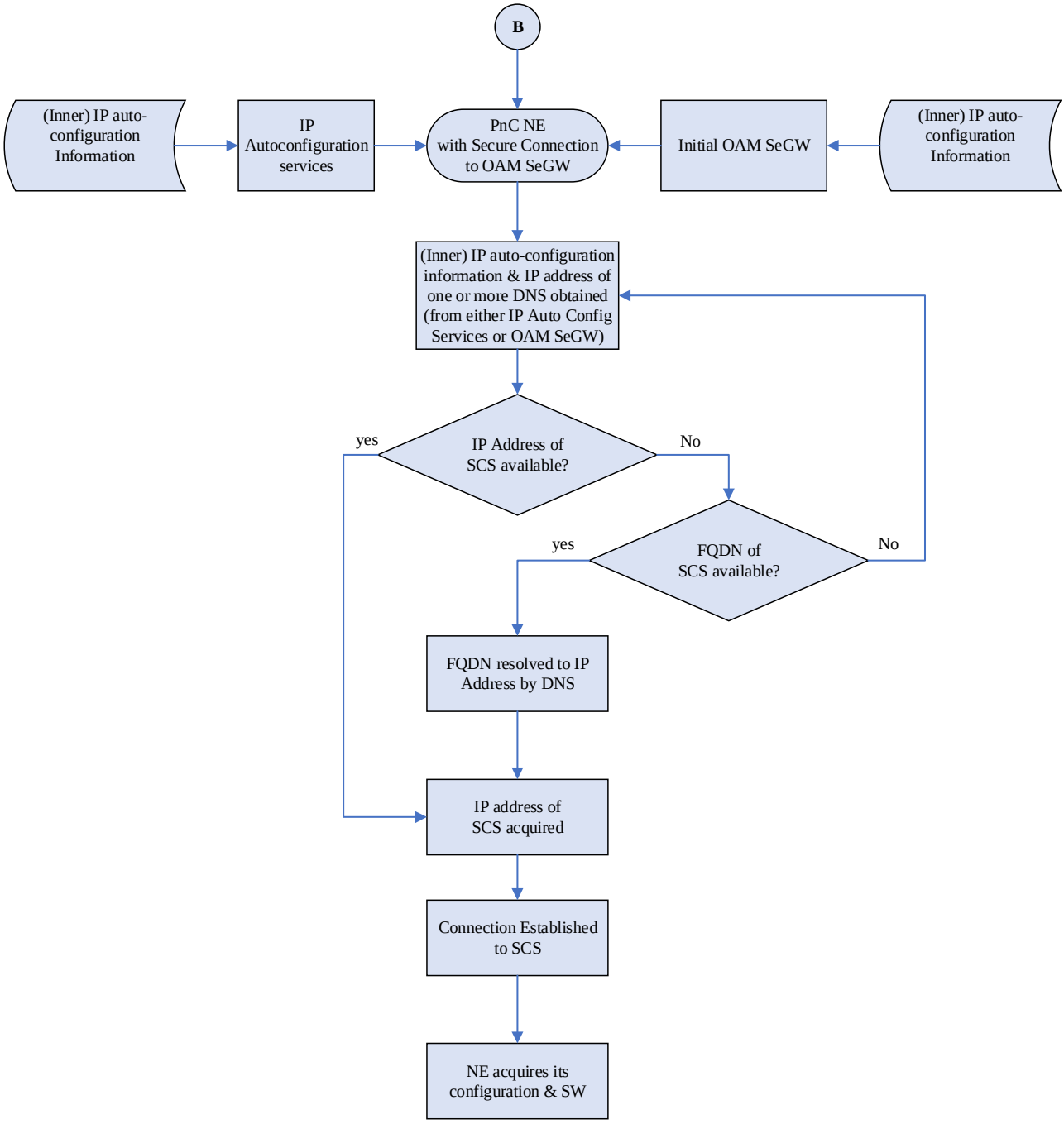

Figure A.2: PnC Procedure for the secure Operator Network

Annex B (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2021-06	SA5#137-e	S5-213662					0.1.0
2021-09	SA5#138-e	S5-214659					0.2.0
2021-10	SA5#139-e	S5-215628					0.3.0
2021-12	SA5#140-e	S5-216602					0.4.0
2022-01	SA5#141-e	S5-221749					0.5.0
2022-03	SA#95e	SP-220122				Presented for information and approval	1.0.0
2022-03	SA#95e					Upgrade to change control version	17.0.0

History

Document history		
V17.0.0	May 2022	Publication