ETSI TS 128 315 V19.0.0 (2026-01)

TECHNICAL SPECIFICATION

5G;
Management and orchestration;
Plug and Connect;
Procedure flows
(3GPP TS 28.315 version 19.0.0 Release 19)

Reference
RTS/TSGS-0528315vj00

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 at 3GPP to ETSI numbering cross-referencing.

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 procedure flows 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 28.314: "Management and orchestration; Plug and Connect; Concepts and requirements".

[3] 3GPP TS 28.316: "Management and orchestration; Plug and Connect; Data formats".

[4] 3GPP TS 28.532: "Technical Specification; Management and orchestration; Generic management services".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1], TS 28.314 [2] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1] and TS 28.314 [2].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1], TS 28.314 [2] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1] and in TS 28.314 [2].

4 Architecture for Plug and Connect

4.1 Functional architecture

The functional architecture for plug-and-connect connection of NE to the network is described in 3GPP TS 28.314 [2] clause 4.1.2. It covers the scenarios where NE is connected to the Secure Operator Network either via an External

Network or via a Non-Secure Operator Network.
The entities (functional elements) involved in the PnC are listed and described in detail in clause 4.2.

4.2 Functional elements

4.2.1 IP Autoconfiguration services

The IP Autoconfiguration services such as DHCP servers and Router Advertisements are used primarily to provide the NE with basic IP configuration information (e.g. IP address, netmask, default gateway, domain name, IP address(es) of DNS servers, time servers). IP Autoconfiguration services may recognize the NE as a client (using, for example, the vendor class identifier DHCP option) and provide with information such as IP address or FQDN of CA/RA server, IP address or FQDN of SeGW, IP address or FQDN of SCS, etc.
The specific data formats used by IP Autoconfiguration services for **plug-and-connect** procedures are described in 3GPP TS 28.316 [3].

From the **plug-and-connect** feature perspective, the IP Autoconfiguration services may be categorized into secure (those located within a Secure Operator Network) and public (those located either within a Non-Secure Operator Network or within an External Network).

4.2.2 DNS server

DNS servers are used to resolve FQDNs into IP addresses. The FQDNs used for **plug-and-connect** may be factory programmed, provided by IP Autoconfiguration services, configured by SCS, or derived/generated within the NE using the vendor information, operator network domain name and name of the functional element.
The specific FQDN formats used in **plug-and-connect** procedures are described in 3GPP TS 28.316 [3].

From the **plug-and-connect** feature perspective, the DNS servers may be categorized into secure (those located within a Secure Operator Network) and public (those located either within a
Non-Secure Operator Network or within an External Network).

The DNS server is an optional functional element and is only required if particular Operator deployment scenario relies on resolution of FQDNs (e.g. FQDNs are configured at the IP Autoconfiguration services, NE and/or SCS, while IP addresses are configured at DNS servers).

4.2.3 Certification Authority server

The Certification Authority server (CA/RA) is used in the in the **plug-and-connect** procedures for security certificate enrolment (e.g. to provision operator certificates at the NE using the factory-installed vendor certificates).

There could be one or more CA/RA depending on a particular operator deployment scenario (e.g. one CA/RA per vendor).

4.2.4 Software and Configuration Server (SCS)

The SCS is a vendor-specific functional element that is used in **plug-and-connect** procedures to provide the NE with correct software and configuration information.

There could be one or more SCS depending on a particular Operator deployment scenario (e.g. initial SCS, serving SCS).

The configuration may contain an IP address or FQDN of (another) SCS that this specific NE shall use as SCS.

The configuration may contain an IP address or FQDN of (another) SeGW that should be used before connecting to the SCS.

SCS can be implemented in EM in IRP based architecture or MnF in SBMA.

4.2.5 Security Gateway (SeGW)

The SeGW is used to establish a secure connection between the NE and the Secure Operator Network.

Depending on a particular operator deployment scenario, there could be separate SeGW for connection to the OAM network and to the CN. The OAM SeGW and CN SeGW may or may not be in practice separate physical entities.

Depending on a particular operator deployment scenario, there could be more than one OAM SeGW (e.g. one per vendor).

5 Procedure flows

5.1 High-level plug-and-connect

The high level procedure for "plug-and-connect" is described next and illustrated in figure 5.1.1.

Operators may deploy their management infrastructure in different ways. The following options are possible:

- One or multiple SCS for each vendor (e.g. an Initial SCS and zero or more Serving SCS);
- One or more SeGW (e.g. one SeGW for OAM and one or more for each CN, and/or one SeGW per vendor);
- Zero or more IP Autoconfiguration services in the Secure Operator Network;
- Zero or more DNS servers in the Secure Operator Network;
- One or more IP Autoconfiguration services in the External Network / non-Secure Operator Network;
- Zero or more DNS servers in the External Network / non-Secure Operator Network;
- One or more CA/RA (e.g. one per vendor).

The procedure described in this clause applies to all deployment options listed above. In this procedure NE is the RAN NE. Other types of NE might also be compliant and use this procedure. Examples of NEs are:

- gNB
- eNB

The NE within virtualization is not addressed.

The procedure begins when the NE is powered up and ends when all mandatory steps in this procedure are completed or when an exception occurs.

The pre-conditions for this procedure are:

- The NE is physically installed;
- IP connectivity exists between involved telecom resources (functional elements listed in clause 4.2);
- The involved telecom resources (functional elements listed in clause 4.2) are functional;
- The relevant information is stored and available.

The post-conditions for this procedure are:

- One or more secure connection exists between NE and SCS and the Core Network(s);
- 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").

The exceptions:

- One of the steps outlined in the procedure fails.

Procedure steps:

1) 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.

2) In this step NE invokes the "Initial IP Autoconfiguration" procedure (described in clause 5.2) and acquires its IP address through stateful or stateless IP Autoconfiguration. There may be additional information provided to the NE.

3) In this step NE invokes the "Certificate Enrolment" procedure (described in clause 5.3).

4) In this step NE invokes the "Establishing Secure Connection" procedure (described in clause 5.4) and connects to the OAM SeGW.

5) In this step NE invokes the "Establishing Connection to SCS" procedure (described in clause 5.5). In this step SCS may provide the NE with new configuration. 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.

6) If the configuration obtained in step 5 contains the address or FQDN of the SeGW and/or SCS different from the one that NE is currently connected to, the NE may execute steps 6.1 and 6.2 until the configured SeGW and SCS will match the connected SeGW and SCS. The configuration may also contain OAM VLAN Id to be used from this step onwards.

   6.1) In this step, if the NE is connected to the OAM SeGW different from the SeGW that is configured, it releases the connection to the current SeGW and invokes the "Establish Secure Connection" procedure (described in clause 5.4) and connects to the configured SeGW.

   6.2) In this step, if the NE is connected to the SCS different from the SCS that is configured, it releases the connection to the current SCS and invokes the "Establish Connection to SCS" procedure (described in clause 5.5) and connects to the configured SCS.

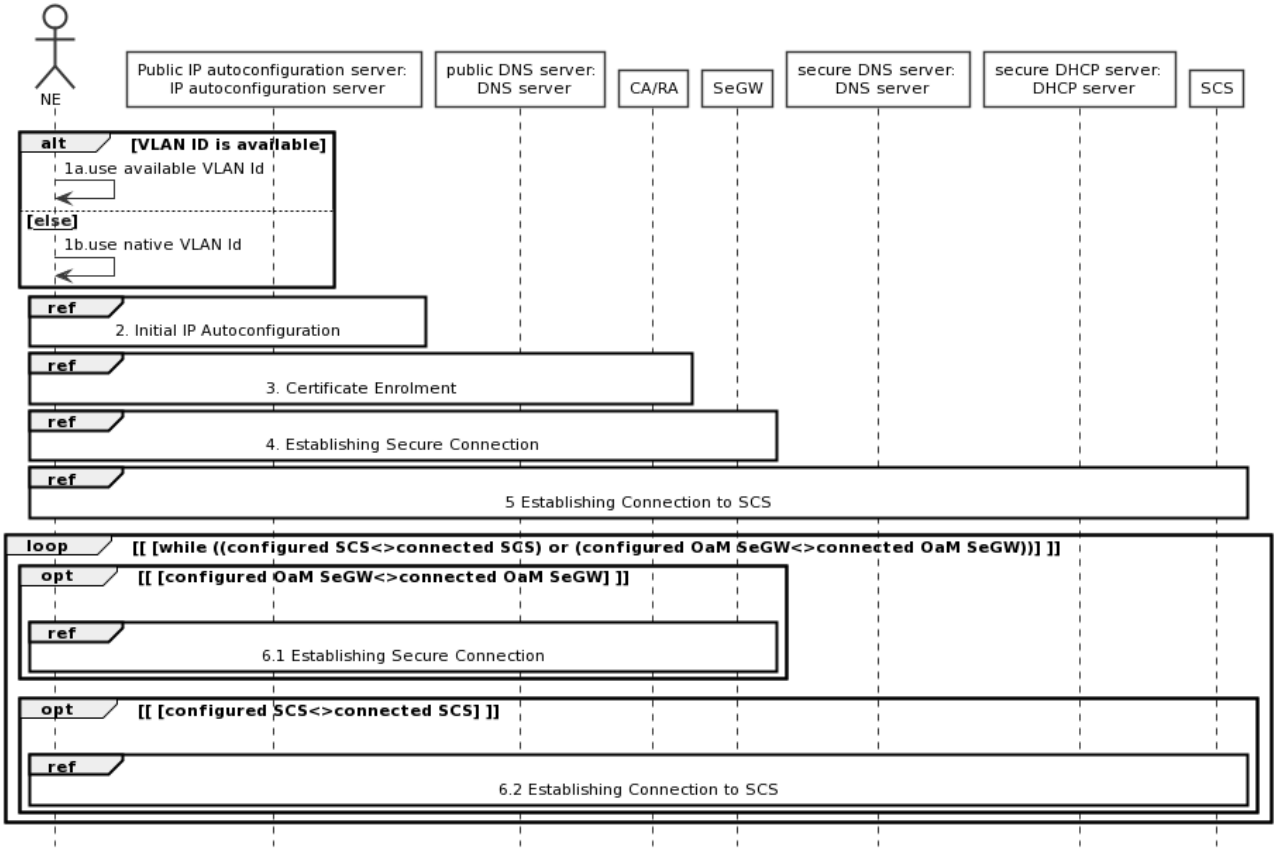

Figure 5.1.1: High-level plug-and-connect flow

5.2 Initial IP Autoconfiguration

The procedure for initial IP Autoconfiguration is described next and illustrated in figure 5.2.1.

Operators may deploy their management infrastructure in different ways. Specifically, the following options are possible:

- IP Autoconfiguration service is configured with basic IP configuration only (e.g. IP address, netmask, gateway, domain name, DNS server address);
- IP Autoconfiguration service is configured with basic IP configuration and the IP address of CA/RA, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;
- IP Autoconfiguration service is configured with basic IP configuration and the FQDN of CA/RA, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;
- IP Autoconfiguration service is configured with basic IP configuration and the IP addresses of CA/RA and SeGW, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;
- IP Autoconfiguration service is configured with basic IP configuration and the FQDNs of CA/RA and SeGW, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;
- IP Autoconfiguration service is configured with basic IP configuration and the IP addresses of CA/RA, SeGW and SCS, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;
- IP Autoconfiguration service is configured with basic IP configuration and the FQDNs of CA/RA, SeGW and SCS, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;
- IP Autoconfiguration service is unable to recognize that the client is an NE performing the **plug-and-connect** procedure;
- IP Autoconfiguration service is able to recognize that the client is an NE performing the **plug-and-connect** procedure;
- IP Autoconfiguration service is unable to recognize that the client is an NE performing the **plug-and-connect** procedure and the specific NE vendor.

The procedure described in this clause applies to all deployment options listed above.

The exceptions:

- One of the steps outlined in the procedure fails.

Procedure steps:

1.1) In this step NE sends a request for IP address configuration to the IP Autoconfiguration service (e.g. DHCP server). The NE may include the vendor specific identifier. The data format used by the NE in this step is specified in 3GPP TS 28.316 [3].

1.2) Depending on the particular operator deployment scenario, the information configured in the IP Autoconfiguration service may be different and the IP Autoconfiguration service may or may not be able to recognize the specific details about the client (whether it is an NE performing **plug-and-connect** procedure and the specific NE vendor). Therefore, in this step the following replies by the IP Autoconfiguration service are possible:

1.2.a) Client IP configuration only (e.g. IP address, netmask, gateway, domain name, DNS server address);

1.2.b) Client IP configuration and the IP address of CA/RA, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;

1.2.c) Client IP configuration and the FQDN of CA/RA, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;

1.2.d) Client IP configuration and the IP addresses of CA/RA and SeGW, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;

1.2.e) Client IP configuration and the FQDNs of CA/RA and SeGW, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;

1.2.f) Client IP configuration and the IP addresses of CA/RA, SeGW and SCS, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3;

1.2.g) Client IP configuration and the FQDNs of CA/RA, SeGW and SCS, and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3.

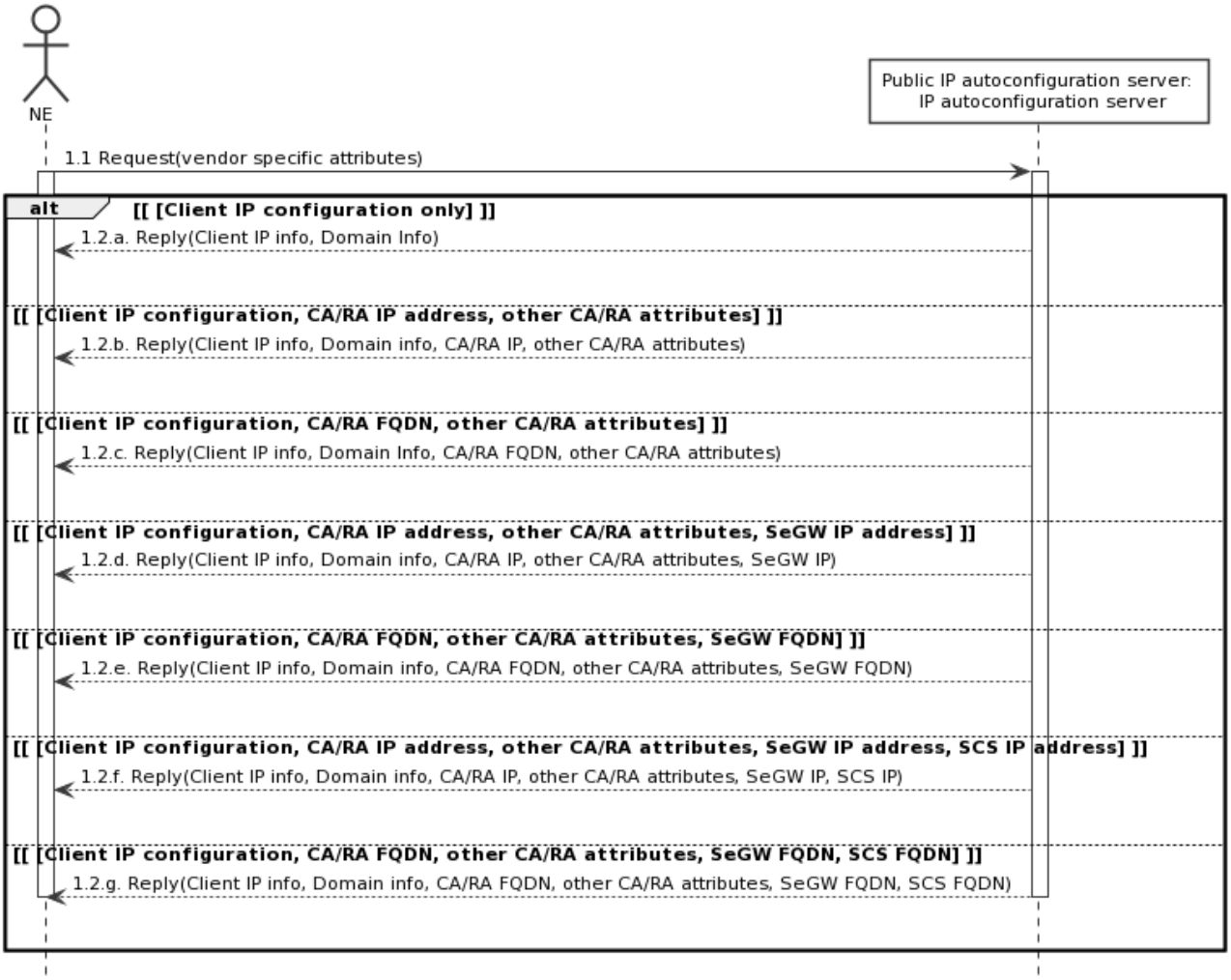

Figure 5.2.1: Initial IP Autoconfiguration flow

5.3 Certificate enrolment

The procedure for certificate enrolment is described next and illustrated in figure 5.3.1.

Operators may deploy their management infrastructure in different ways. The following options are possible:

- The IP address of the CA/RA is known to the NE (e.g. provided by the IP Autoconfiguration service);
- The IP address of the CA/RA is unknown to the NE, but the FQDN of the CA/RA is known to the NE (e.g. provided by the IP Autoconfiguration service, pre-configured at the factory);

The procedure described in this clause applies to all deployment options listed above.

The exceptions:

- One of the steps outlined in the procedure fails.

Procedure steps:

1) This step is executed only if the IP address of CA/RA is unknown to the NE, but the FQDN of the CA/RA is known (e.g. provided by the IP Autoconfiguration service, pre-configured at the factory). The format of the FQDN is specified in 3GPP TS 28.316 [3]:

   1.1) NE sends a request containing the FQDN of the CA/RA to the DNS server.

   1.2) DNS server resolves the FQDN of the CA/RA into the IP address and provides it to the NE.

2) In this step NE performs actual security certificate enrolment (e.g. using CMPv2 protocol). The sub-steps are included for the illustration purposes only:

   2.1) In this sub-step the NE enrols using the vendor certificate (e.g. pre-programmed at the factory) and other CA/RA attributes defined in TS 28.316 [3] clause 4.2.3 provided by IP Autoconfiguration service.

   2.2) In this sub-step the NE receives the Operator certificates from the CA/RA.

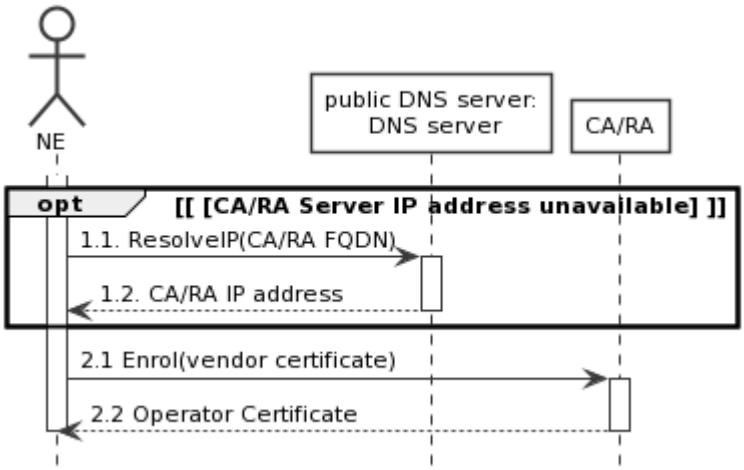

Figure 5.3.1: Certificate enrolment flow

5.4 Establishing secure connection

The procedure for establishing the secure connection is described next and illustrated in figure 5.4.1.

Operators may deploy their management infrastructure in different ways. Specifically, the following options are possible:

- The IP address of the SeGW is known to the NE (e.g. provided by the IP Autoconfiguration service, configured by SCS);
- The IP address of the SeGW is unknown to the NE, but the FQDN of the SeGW is known to the NE (e.g. provided by the IP Autoconfiguration service, configured by SCS, pre-configured at the factory);
- The SeGW provides NE only with internal IP configuration;
- The SeGW provides NE with internal IP configuration and the IP address of the secure (internal) DHCP server;
- The SeGW provides NE with internal IP configuration and the IP address(es) of the secure (internal) DNS server(s);
- The SeGW provides NE with internal IP configuration and the IP addresses of the secure (internal) DHCP and DNS servers.

The procedure described in this clause applies to all deployment options listed above.

The exceptions:

- One of the steps outlined in the procedure fails.

Procedure steps:

1) This step is executed only if the IP address of SeGW is unknown to the NE, but the FQDN of the SeGW is known (e.g. provided by the IP Autoconfiguration service, configured by SCS, pre-configured at the factory). The format of the FQDN is specified in 3GPP TS 28.316 [3].

   1.1) NE sends a request containing the FQDN of the SeGW to the DNS server.

   1.2) DNS server resolves the FQDN of the SeGW into the IP address and provides it to the NE.

2) In this step NE establishes secure tunnel to the SeGW using IKEv2 protocol. The sub-steps are included for the illustration purposes only.

   2.1) In this sub-step the NE establishes secure connection using the operator certificate (e.g. provided in the Certificate Enrolment procedure described in clause 5.3).

   2.2) In this sub-step the NE receives its inner IP configuration from the SeGW in the Configuration Parameters of IKEv2. The "inner" IP address may be the same as the "outer" IP address (e.g. obtained in the Initial IP Autoconfiguration procedure described in clause 5.2).

   2.3) In this optional sub-step the NE receives the IP addresses of one or more secure (internal) DNS servers from the SeGW in the Configuration Parameters of IKEv2.

   2.4) In this optional sub-step the NE receives the IP address of secure (internal) DHCP server from the SeGW in the Configuration Parameters of IKEv2.

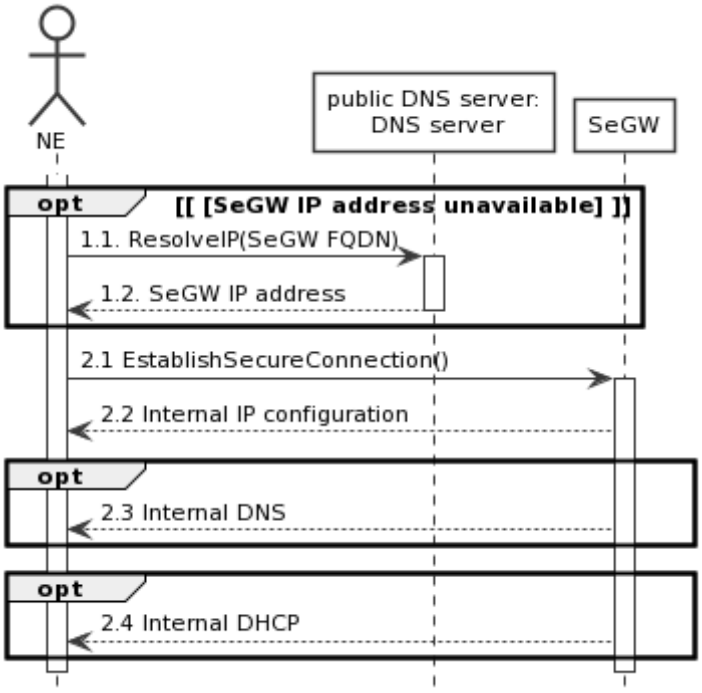

Figure 5.4.1: Establishing secure connection flow

5.5 Establishing connection to Software and Configuration Server (SCS)

The procedure for establishing connection to Software and Configuration Server (SCS) is described next and illustrated in figure 5.5.1.

Operators may deploy their management infrastructure in different ways. Specifically, the following options are possible:

- The IP address of the SCS is known to the NE (e.g. provided by the IP Autoconfiguration service, configured by SCS);
- The IP address of the SCS is unknown to the NE, but the FQDN of the SCS is known to the NE (e.g. provided by the IP Autoconfiguration service, configured by SCS, pre-configured at the factory);
- The IP address of secure (internal) DHCP server is known to the NE (e.g. provided in the Configuration Parameters of IKEv2);
- The IP address of secure (internal) DNS server is known to the NE (e.g. provided in the Configuration Parameters of IKEv2);
- The IP address of the SCS configured in the secure (internal) DHCP server;
- The FQDN of the SCS configured in the secure (internal) DHCP server.

The procedure described in this clause applies to all deployment options listed above.

The exceptions:

- One of the steps outlined in the procedure fails.

Procedure steps:

1) This step is executed only if the IP address of SCS is unknown to the NE, but the IP address of the secure (internal) DHCP server is known (e.g. provided by the SeGW in the Configuration Parameters of IKEv2):

   1.1) NE sends a request to the secure DHCP server. The NE may include the vendor specific identifier. The data format used by the NE in this step is specified in 3GPP TS 28.316 [3].

   1.2) DHCP server provides the IP address of the SCS to the NE. The data format used by the DHCP server in this step is specified in 3GPP TS 28.316 [3].

2) This step is executed only if the IP address of SCS is unknown to the NE, but the FQDN of the SCS is known (e.g. provided by the IP Autoconfiguration service, configured by SCS, pre-configured at the factory) and the IP address of the secure (internal) DNS server is known (e.g. provided by the SeGW in the Configuration Parameters of IKEv2). The format of the FQDN is specified in 3GPP TS 28.316 [3]:

   2.1) NE sends a request containing the FQDN of the SCS to the secure (internal) DNS server.

   2.2) DNS server resolves the FQDN of the SCS into the IP address and provides it to the NE.

3) and 4) These steps are executed only if the IP address and FQDN of the SCS are unknown to the NE, but the IP addresses of the secure (internal) DHCP and DNS servers are known (e.g. provided by the SeGW in the Configuration Parameters of IKEv2):

   3.1) NE sends a request to the secure DHCP server. The NE may include the vendor specific identifier. The data format used by the NE in this step is specified in 3GPP TS 28.316 [3].

   3.2) DHCP server provides the FQDN of the SCS to the NE. The data format used by the DHCP server in this step is specified in 3GPP TS 28.316 [3].

   4.1) NE sends a request containing the FQDN of the SCS to the secure (internal) DNS server.

   4.2) DNS server resolves the FQDN of the SCS into the IP address and provides it to the NE.

5) In this step NE establishes communication with SCS. The protocol used for communication between NE and SCS is vendor specific and is out of scope of the present document. The sub-steps listed below are for illustration purposes only:

   5.1) In this step NE connects to the SCS and identifies itself. The NE may provide SCS with its current software version and configuration.

   5.2) In this step SCS may provide the NE with new configuration.

5.3) In this step SCS may provide the NE with new software.

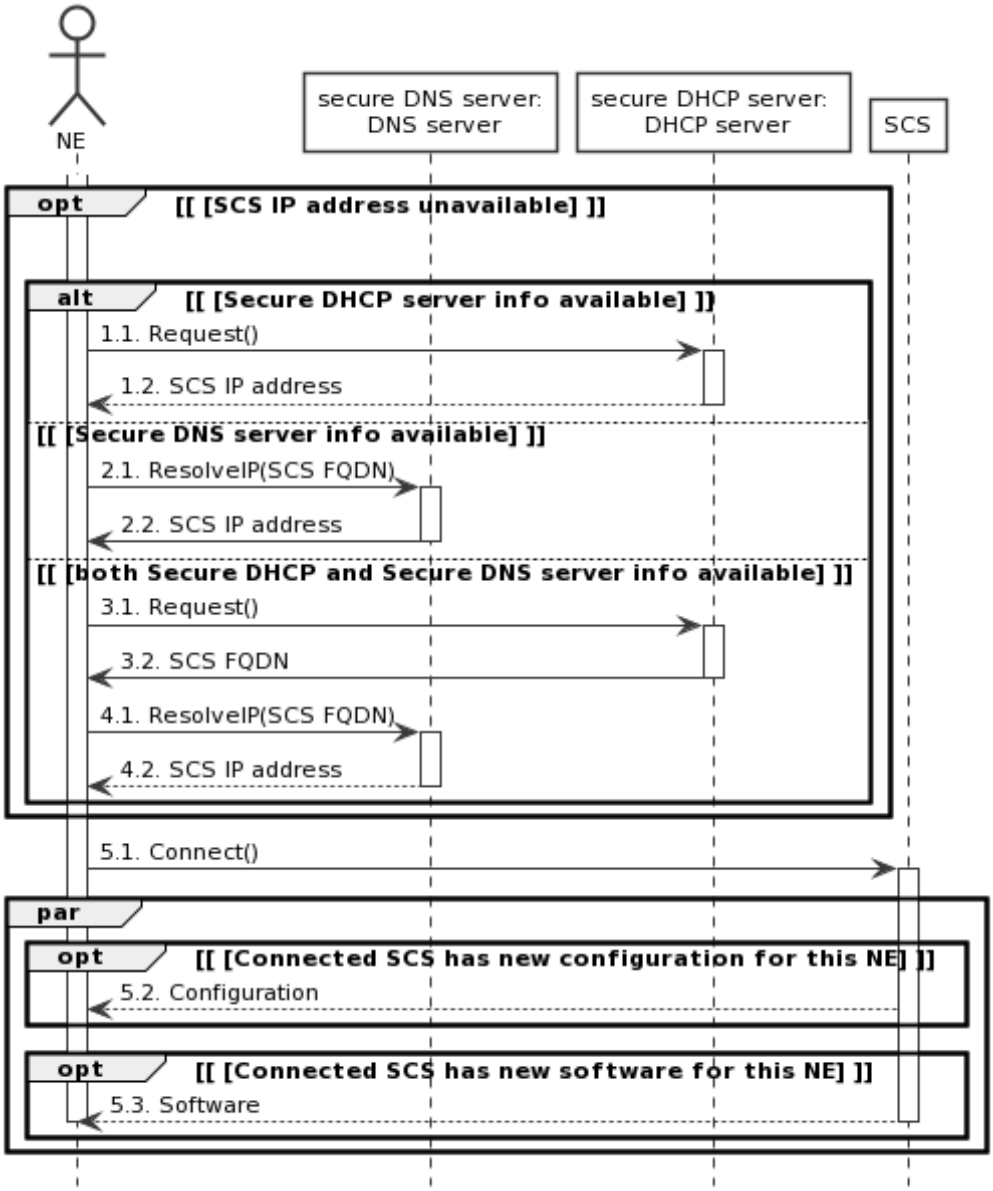

Figure 5.5.1: Establishing connection to Software and Configuration Server (SCS) flow

5.6 IAB-node connects to management system

IAB-node connects to management system at power up and during mobiltiy by following PnC steps as described in clause 6.1.x of TS 28.314 [2]. The management system that IAB-node connects to may change due to IAB-node mibility behaviours. The procedures for IAB-node connectiong to management system based on its locations are illustrated in Figure 5.6.1, this includes step 2 of obtaining IP configuration via notification mechanism instead of initial IP autoconfiguration procedure.

In step 1, IAB-node has established a connection with its management system via PnC

In step 2, It reuses the existing notifications and operations as defined in TS 28.532 [4] to obtain IP configuration for OAM connectivity:

The provisioning MnS producer of IAB-node should provide IAB-node location information via any of the following notifications:

- notifyMOICreation

- notifyMOIAttributeValueChanges

- notififyMOIChanges

The provisioning MnS consumer (management system) should provide IP configuration for OAM connectivity via any of the following operations upon the reception of notifications:

- createMOI

- modifyMOIAttributes

In step 3, IAB-node connects to new management system by following subsequent PnC steps including connection to CA/RA, SeGW and SCS.

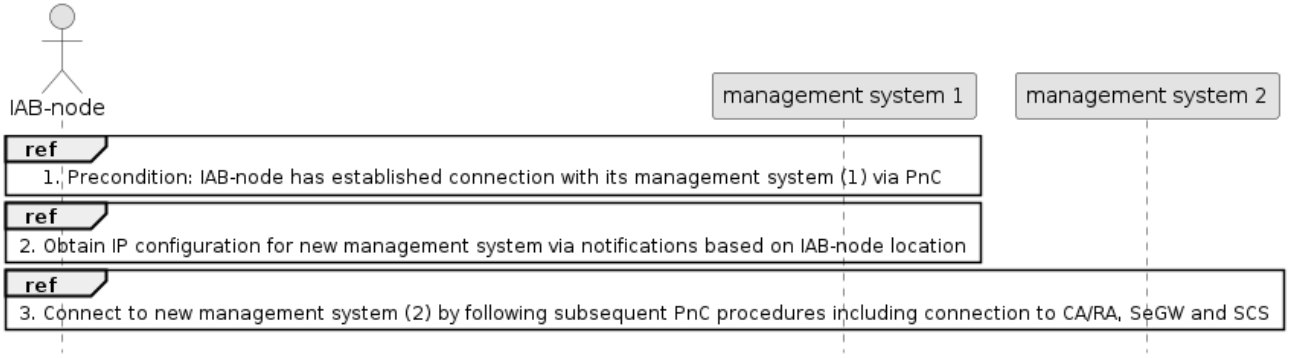

Figure 5.6.1: Procedure flows for IAB-node connects to management system

5.7 Management of NTN secure backhaul

In ground based terrestrial networks the connectivity between RAN nodes and SeGW is based on physical connectivity. As a result, the underlying IP network design seldom changes, and the logical connectivity between the RAN nodes and SeGW remains relatively stable.

However, in airborne Non-Terrestrial Networks (NTN) the connectivity between RAN nodes and SeGW is not stable since the RAN nodes are moving. E.g. a satellite in LEO, MEO or GEO orbit. A non-terrestrial node provides a service link and relies on a feeder link to communicate with other nodes comprising the NTN, including the SeGW.

As NTN nodes move the availability of terrestrial connectivity is subject to change. This has potential impact to the security associations between the NTN node, SeGW and CN.

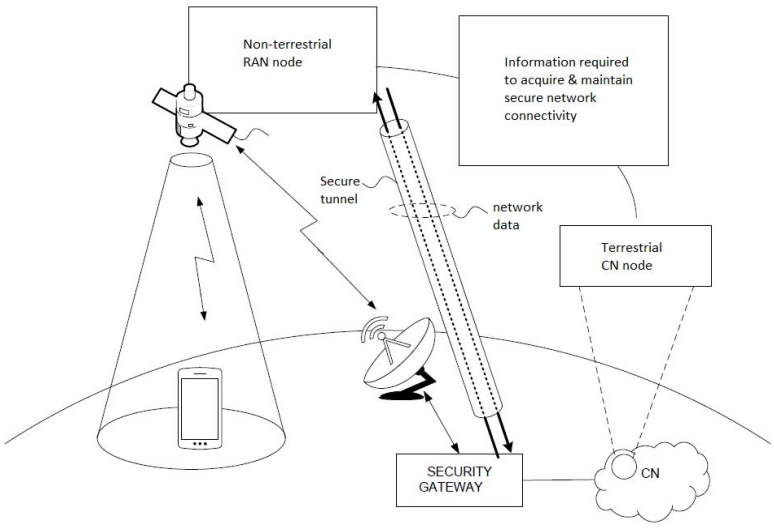

Figure *5.7*-1: Secure connectivity between non-terrestrial RAN node and terrestrial CN node(s)

As NTN nodes move their security associations should be updated subject to the availability of new terrestrial connectivity to a new SeGW. In some cases, such SeGW transitions may be able to be performed in anticipation of the upcoming feeder link update (i.e. "make then break") whereas in others the new connectivity may not be available in advance (i.e. "break then make"). Both scenarios should be supported, and different information may be required to setup and maintain the secure associations subject to which security protocols and features are configured.

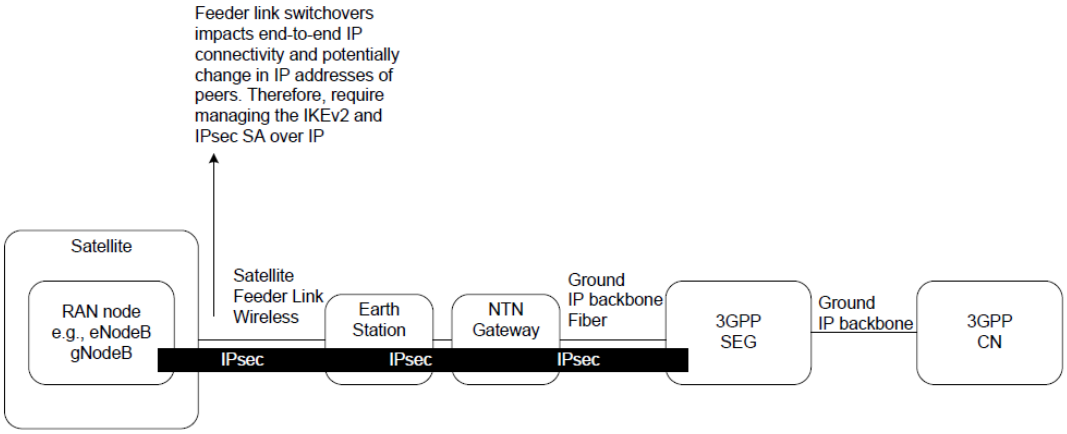

Figure 5.7-2: Impact of feeder link switchover between NTN node, SeGW and CN

The IP configuration requires correlation with the state of connect/disconnect of the IP link itself. For example, for satellite-based NTN node the following may need to be considered:

- satellite may only ever connect to ground stations allowed by policy. As a result, when the satellite moves out of ground station's catchment location, it loses the ground connectivity via the feeder link and the IP transport during such period, and then reestablishes the IP connectivity.

- when the satellite orbit is passing over the earth surface (e.g. oceans, mountains, deserts, forests etc.) where there is no ground station and supporting infrastructure, the satellite may by-design route data over to Inter Satellite Link (ISL) to other satellites that may have connectivity with the ground infrastructure over a feeder link, but the ground infrastructure may reside in jurisdiction not permitted by regulations.

To further ensure the security associations are maintained, additional information should also be made available to the NTN node about the anticipated terrestrial connectivity based on criteria such as flight path and/or time windows.

In summary, movement of the NTN nodes mean the backhaul connection should traverse multiple feeder links and its security associations should be maintained throughout lifecycle phases of IP connectivity. As a result, NTN nodes require information not only to setup the initial secure communications channel, but to maintain such communications as the NTN moves.

Annex A (informative): PlantUML source code

A.1 High-level plug-and-connect

The following PlantUML source code is used to describe the procedure for High-level plug-and-connect, as depicted by Figure 5.1.1:

```
@startuml
actor NE
participant "Public IP autoconfiguration server: \n IP autoconfiguration server" as IP_Server
participant "public DNS server:\n DNS server" as P_DNS_Server
participant "CA/RA" as CA_RA
participant SeGW
participant "secure DNS server: \n DNS server" as S_DNS_Server
participant "secure DHCP server: \n DHCP server" as S_DHCP_Server
participant SCS
alt VLAN ID is available
NE->NE: 1a.use available VLAN Id
Else [[else]]
NE->NE: 1b.use native VLAN Id
End
Ref over NE, IP_Server: 2. Initial IP Autoconfiguration
Ref over NE, IP_Server,CA_RA: 3. Certificate Enrolment
Ref over NE, IP_Server,CA_RA,SeGW: 4. Establishing Secure Connection
Ref over NE, IP_Server,CA_RA,SeGW,SCS: 5 Establishing Connection to SCS

loop [ [while ((configured SCS<>connected SCS) or (configured OaM SeGW<>connected OaM SeGW))] ]
opt [ [configured OaM SeGW<>connected OaM SeGW] ]
|||
Ref over NE,IP_Server,P_DNS_Server,CA_RA, SeGW:6.1 Establishing Secure Connection
End
opt [ [configured SCS<>connected SCS] ]
|||
Ref over NE,IP_Server,P_DNS_Server,CA_RA, SeGW,S_DNS_Server,S_DHCP_Server,SCS:6.2 Establishing
Connection to SCS
End
End

hide footbox
skinparam DefaultFontSize 11

skinparam sequenceActorBackgroundColor #FFFFFF
skinparam sequenceParticipantBackgroundColor #FFFFFF
skinparam noteBackgroundColor #FFFFFF
autonumber "#'.'"
skinparam monochrome true
skinparam shadowing false
@enduml
```

A.2 Initial IP Autoconfiguration

The following PlantUML source code is used to describe the procedure for Initial IP Autoconfiguration, as depicted by Figure 5.2.1:

```
@startuml
actor NE
participant "Public IP autoconfiguration server: \n IP autoconfiguration server" as IP_Server

NE -> IP_Server: 1.1 Request(vendor specific attributes)
activate NE
activate IP_Server
Alt  [ [Client IP configuration only] ]
IP_Server --> NE: 1.2.a. Reply(Client IP info, Domain Info)
|||
Else  [ [Client IP configuration, CA/RA IP address, other CA/RA attributes] ]
IP_Server --> NE: 1.2.b. Reply(Client IP info, Domain info, CA/RA IP, other CA/RA attributes)
```

```
|||
Else [ [Client IP configuration, CA/RA FQDN, other CA/RA attributes] ]
IP_Server -->NE: 1.2.c. Reply(Client IP info, Domain Info, CA/RA FQDN, other CA/RA attributes)
|||
Else [ [Client IP configuration, CA/RA IP address, other CA/RA attributes, SeGW IP address] ]
IP_Server -->NE: 1.2.d. Reply(Client IP info, Domain info, CA/RA IP, other CA/RA attributes, SeGW
IP)
|||
Else [ [Client IP configuration, CA/RA FQDN, other CA/RA attributes, SeGW FQDN] ]
IP_Server -->NE: 1.2.e. Reply(Client IP info, Domain info, CA/RA FQDN, other CA/RA attributes, SeGW
FQDN)
|||
Else [ [Client IP configuration, CA/RA IP address, other CA/RA attributes, SeGW IP address, SCS IP
address] ]
IP_Server --> NE: 1.2.f. Reply(Client IP info, Domain info, CA/RA IP, other CA/RA attributes, SeGW
IP, SCS IP)
|||
Else [ [Client IP configuration, CA/RA FQDN, other CA/RA attributes, SeGW FQDN, SCS FQDN] ]
IP_Server -->NE: 1.2.g. Reply(Client IP info, Domain info, CA/RA FQDN, other CA/RA attributes, SeGW
FQDN, SCS FQDN)
|||
deactivate IP_Server
deactivate NE
End

hide footbox
skinparam defaultFontSize 11

skinparam sequenceActorBackgroundColor #FFFFFF
skinparam sequenceParticipantBackgroundColor #FFFFFF
skinparam noteBackgroundColor #FFFFFF
autonumber "#'.'"
skinparam monochrome true
skinparam shadowing false
@enduml
```

A.3 Certificate enrolment

The following PlantUML source code is used to describe the procedure for Certificate enrolment, as depicted by Figure 5.3.1:

```
@startuml
actor NE
activate NE
participant "public DNS server:\n DNS server" as P_DNS_Server
participant "CA/RA" as CA_RA
opt [ [CA/RA Server IP address unavailable] ]
NE->P_DNS_Server: 1.1. ResolveIP(CA/RA FQDN)
activate P_DNS_Server
P_DNS_Server -->NE: 1.2. CA/RA IP address
deactivate P_DNS_Server
End
NE->CA_RA: 2.1 Enrol(vendor certificate)
activate CA_RA
CA_RA-->NE: 2.2 Operator Certificate

deactivate CA_RA
deactivate NE

hide footbox
skinparam defaultFontSize 11

skinparam sequenceActorBackgroundColor #FFFFFF
skinparam sequenceParticipantBackgroundColor #FFFFFF
skinparam noteBackgroundColor #FFFFFF
autonumber "#'.'"
skinparam monochrome true
skinparam shadowing false
@enduml
```

A.4 Establishing secure connection

The following PlantUML source code is used to describe the procedure for Establishing secure connection, as depicted by Figure 5.4.1:

```
@startuml
actor NE
participant "public DNS server:\n DNS server" as P_DNS_Server
participant SeGW
activate NE
opt [ [SeGW IP address unavailable] ]
NE -> P_DNS_Server: 1.1. ResolveIP(SeGW FQDN)
activate P_DNS_Server
P_DNS_Server -->NE: 1.2. SeGW IP address
deactivate P_DNS_Server
End
NE->SeGW: 2.1 EstablishSecureConnection()
activate SeGW
SeGW -->NE: 2.2 Internal IP configuration
opt
SeGW -->NE: 2.3 Internal DNS
End
opt
SeGW -->NE: 2.4 Internal DHCP
End

deactivate SeGW
deactivate NE

hide footbox
skinparam defaultFontSize 11

skinparam sequenceActorBackgroundColor #FFFFFF
skinparam sequenceParticipantBackgroundColor #FFFFFF
skinparam noteBackgroundColor #FFFFFF
autonumber "#'.'"
skinparam monochrome true
skinparam shadowing false
@enduml
```

A.5 Establishing connection to Software and Configuration Server (SCS)

The following PlantUML source code is used to describe the procedure for Establishing connection to SCS, as depicted by Figure 5.5.1:

```
@startuml
actor NE

participant "secure DNS server:\n DNS server" as S_DNS_Server
participant "secure DHCP server: \n DHCP server" as S_DHCP_Server
activate NE
opt [ [SCS IP address unavailable] ]
|||
alt [ [Secure DHCP server info available] ]
NE -> S_DHCP_Server: 1.1. Request()
activate S_DHCP_Server
S_DHCP_Server --> NE: 1.2. SCS IP address
deactivate S_DHCP_Server
Else [ [Secure DNS server info available] ]
NE->S_DNS_Server: 2.1. ResolveIP(SCS FQDN)
activate S_DNS_Server
S_DNS_Server->NE: 2.2. SCS IP address
deactivate S_DNS_Server
Else [ [both Secure DHCP and Secure DNS server info available] ]
NE->S_DHCP_Server: 3.1. Request()
activate S_DHCP_Server
S_DHCP_Server->NE: 3.2. SCS FQDN
deactivate S_DHCP_Server
NE->S_DNS_Server: 4.1. ResolveIP(SCS FQDN)
activate S_DNS_Server
```

```
S_DNS_Server-->NE: 4.2. SCS IP address
deactivate S_DNS_Server
End
End
NE->SCS: 5.1. Connect()
activate SCS
par
opt [ [Connected SCS has new configuration for this NE] ]
SCS --> NE: 5.2. Configuration
End
opt [ [Connected SCS has new software for this NE] ]
SCS-->NE: 5.3. Software
deactivate SCS
deactivate NE
End
End

hide footbox
skinparam DefaultFontSize 11

skinparam sequenceActorBackgroundColor #FFFFFF
skinparam sequenceParticipantBackgroundColor #FFFFFF
skinparam noteBackgroundColor #FFFFFF
autonumber "#'.'"
skinparam monochrome true
skinparam shadowing false
@enduml
```

A.6 IAB-node connects to management system

The following PlantUML source code is used to describe the procedure flows for IAB-node connects to management system, as depicted by Figure 5.6.1:

```
@startuml
actor “IAB-node” as IAB
participant "management system 1" as OAM_1
participant "management system 2" as OAM_2
Ref over IAB, OAM_1: 1. Precondition: IAB-node has established connection with its management system
(1) via PnC
Ref over IAB, OAM_1: 2. Obtain IP configuration for new management system via notifications based on
IAB-node location
Ref over IAB, OAM_2: 3. Connect to new management system (2) by following subsequent PnC procedures
including connection to CA/RA, SeGW and SCS
hide footbox
skinparam DefaultFontSize 11
skinparam sequenceActorBackgroundColor #FFFFFF
skinparam sequenceParticipantBackgroundColor #FFFFFF
skinparam noteBackgroundColor #FFFFFF
autonumber "#'.'"
skinparam monochrome true
skinparam shadowing false
@enduml
```

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2021-06	**SA5#137-e**	**S5-213663**					**0.1.0**
2021-10	**SA5#139-e**	**S5-215629**					**0.2.0**
2021-12	**SA5#140-e**	**S5-216603**					**0.3.0**
2022-01	**SA5#141-e**	**S5-221709**					**0.4.0**
2022-03	**SA#95e**	**SP-220123**				**Presented for information and approval**	**1.0.0**
2022-03	**SA#95e**					**Upgrade to change control version**	**17.0.0**
2024-04	**-**	**-**	**-**	**-**	**-**	**Update to Rel-18 version (MCC)**	**18.0.0**
2025-06	SA#108	SP-250543	0001	1	B	Procedure IAB-node connects to management system	19.0.0
2025-06	SA#108	SP-250546	0002		B	Rel-19 CR 28.315 Add secure backhaul requirements for NTN	19.0.0

History

Document history		
V19.0.0	January 2026	Publication