3GPP TS 32.508 V1.0.2 (2013-10)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Procedure flows for multi-vendor plug-and-play eNB connection to the network (Release 12)

Keywords
SON, plug-and-play, PnP, management, eNB

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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:

TS 32.501: "Self-configuration of network elements; Concepts and requirements".

TS 32.508: "Procedure flows for multi-vendor plug-and-play eNB connection to the network".

TS 32.509: "Data format for multi-vendor plug-and-play eNB connection to the network".

1 Scope

The present document describes the procedure flows between network entities involved in the **multi-vendor plug-and-play** eNB connection to network.
These procedures are based on requirements and use cases specified in 3GPP TS 32.501 [4].
The format of the data exchanged in these procedures is defined in 3GPP TS 32.509 [5].

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 TS 32.501: "Telecommunication management; Self-configuration of network elements; Concepts and requirements".

[5] DRAFT 3GPP TS 32.509: "Telecommunications management; Data format for multi-vendor plug-and-play eNB connection to the network".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1], TS 32.501 [4] 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] and in TS 32.501 [4].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], TS 32.501 [4] 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] and in TS 32.501 [4].

DHCP	
DNS	
EM	Element Manager
FQDN	
PnC	
PnP	Plug-and-Play
SeGW	Security Gateway
SON	
VLAN	

4 Architecture for multi-vendor plug-and-play

4.1 Functional architecture

The functional architecture for **multi-vendor plug-and-play** connection of eNB to the network is described in 3GPP TS 32.501 [4] clause 4.3.2.
It covers the scenarios where eNB 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 eNB 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 eNB 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 EM, etc.
The specific data formats used by IP Autoconfiguration services for **multi-vendor plug-and-play** procedures are described in 3GPP TS 32.509 [5].

From the **multi-vendor plug-and-play** 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 **multi-vendor plug-and-play** may be factory programmed, provided by IP Autoconfiguration services, configured by EM, or derived/generated within the eNB using the vendor information, operator network domain name and name of the functional element.
The specific FQDN formats used in **multi-vendor plug-and-play** procedures are described in 3GPP TS 32.509 [5].

From the **multi-vendor plug-and-play** 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, eNB and/or EM, 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 **multi-vendor plug-and-play** procedures for security certificate enrolment (e.g. to provision operator certificates at the eNB 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 Element Manager (EM)

The EM is a vendor-specific functional element that is used in **multi-vendor plug-and-play** procedures to provide the eNB with correct software and configuration information.

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

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

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

4.2.5 Security Gateway (SeGW)

The SeGW is used to establish a secure connection between the eNB 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 "multi-vendor 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 EMs for each vendor (e.g. an Initial EM and zero or more Serving EMs);
- 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.

The procedure begins when the eNB 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 eNB 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 eNB and EM and the Core Network(s);
- Via the connection to the EM the eNB 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) In this step eNB uses the native VLAN to start communicating on, where PnP traffic is sent and received untagged.

2) In this step eNB 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 eNB.

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

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

5) In this step eNB invokes the "Establishing Connection to EM" procedure (described in clause 5.5).

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

   6.1) In this step, if the eNB 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 and connects to the configured SeGW.

6.2) In this step, if the eNB is connected to the EM different from the EM that is configured, it releases the connection to the current EM and invokes the "Establish Connection to EM" procedure and connects to the configured EM.

7) In this step eNB connects to each configured CN using the transport (VLAN ID, IP addresses) and security parameters provided by EM in the previous step.

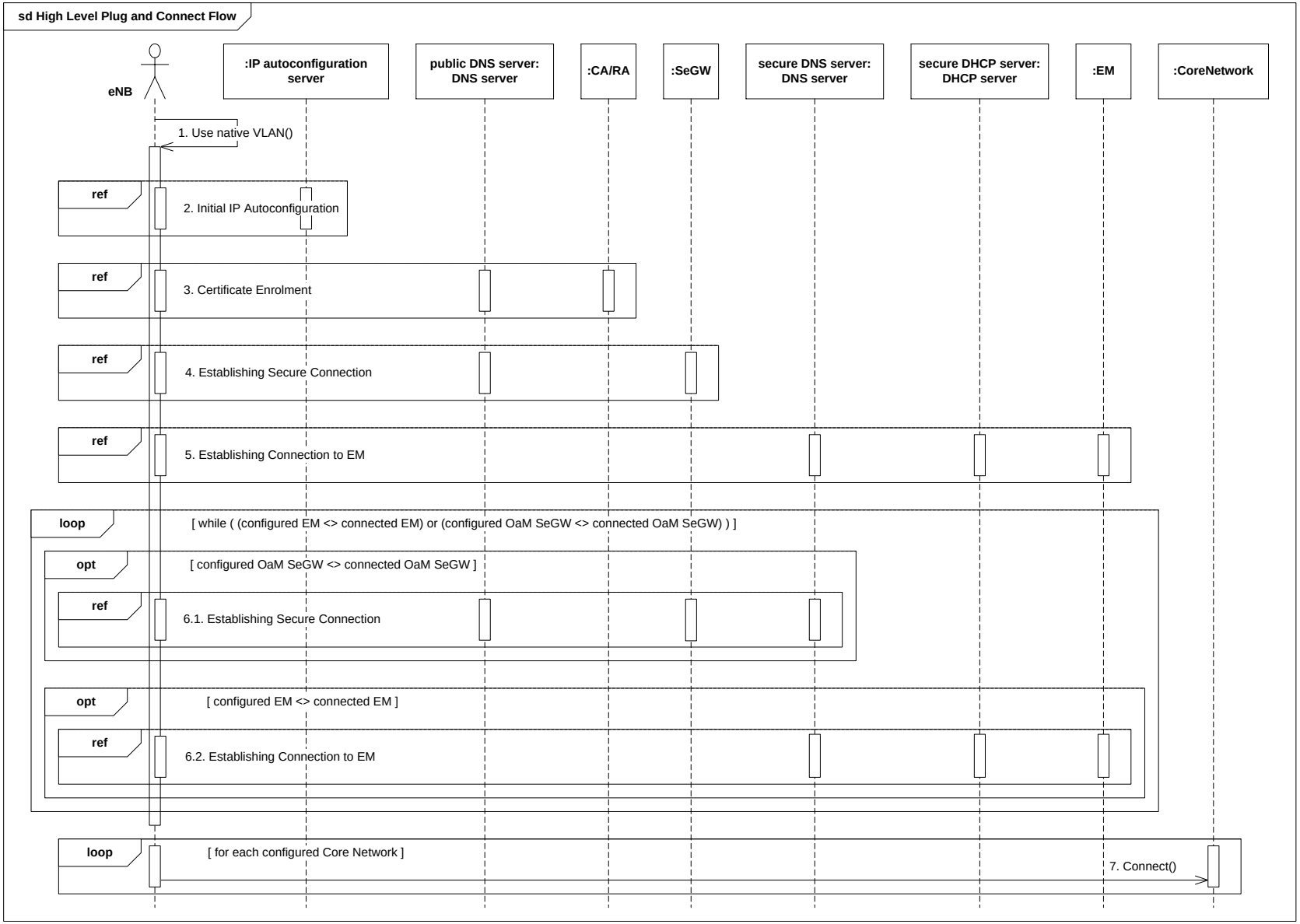

Figure 5.1-1: High-level plug-andconnect flow

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;
- IP Autoconfiguration service is configured with basic IP configuration and the FQDN of CA/RA;
- IP Autoconfiguration service is configured with basic IP configuration and the IP addresses of CA/RA and SeGW;
- IP Autoconfiguration service is configured with basic IP configuration and the FQDNs of CA/RA and SeGW;
- IP Autoconfiguration service is configured with basic IP configuration and the IP addresses of CA/RA, SeGW and EM;
- IP Autoconfiguration service is unable to recognize that the client is an eNB performing the **multi-vendor plug-and-connect** procedure;
- IP Autoconfiguration service is able to recognize that the client is an eNB performing the **multi-vendor plug-and-connect** procedure;
- IP Autoconfiguration service is unable to recognize that the client is an eNB performing the **multi-vendor plug-and-connect** procedure and the specific eNB 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 eNB sends a request for IP address configuration to the IP Autoconfiguration service (e.g. DHCP server). The eNB may include the vendor specific identifier. The data format used by the eNB in this step is specified in 3GPP TS 32.509 [5].

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 eNB performing **plug-and-connect** procedure and the specific eNB 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;

1.2.c) Client IP configuration and the FQDN of CA/RA;

1.2.d) Client IP configuration and the IP addresses of CA/RA and SeGW;

1.2.e) Client IP configuration and the FQDNs of CA/RA and SeGW;

1.2.f) Client IP configuration and the IP addresses of CA/RA, SeGW and EM.

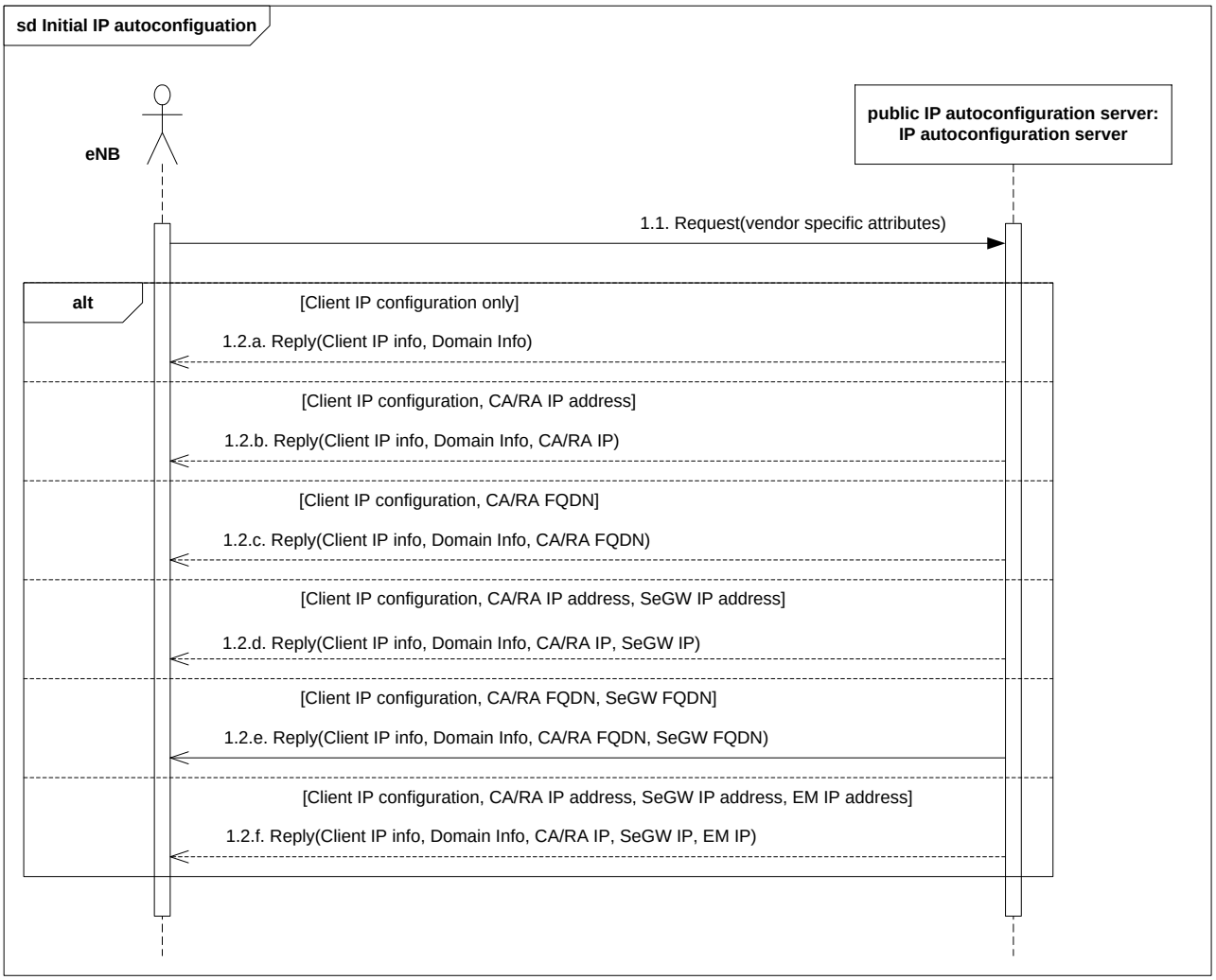

Figure 5.2-1: Initial IP Autoconfiguration flow

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 eNB (e.g. provided by the IP Autoconfiguration service);
- The IP address of the CA/RA is unknown to the eNB, but the FQDN of the CA/RA is known to the eNB (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 eNB, 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 32.509 [5].

   1.1) eNB 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 eNB.

2) In this step eNB 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 eNB enrols using the vendor certificate (e.g. pre-programmed at the factory).

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

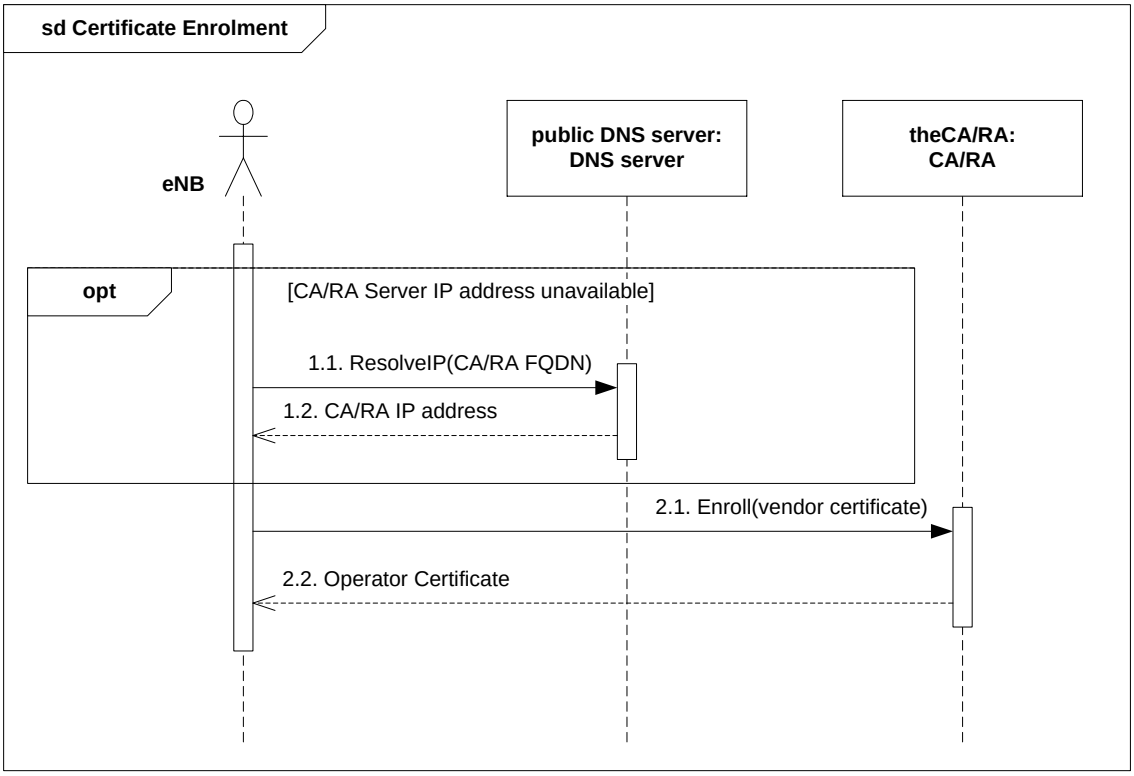

Figure 5.3-1: Certificate enrolment flow

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 eNB (e.g. provided by the IP Autoconfiguration service, configured by EM);
- The IP address of the SeGW is unknown to the eNB, but the FQDN of the SeGW is known to the eNB (e.g. provided by the IP Autoconfiguration service, configured by EM, pre-configured at the factory);
- The SeGW provides eNB only with internal IP configuration;
- The SeGW provides eNB with internal IP configuration and the IP address of the secure (internal) DHCP server;
- The SeGW provides eNB with internal IP configuration and the IP address(es) of the secure (internal) DNS server(s);
- The SeGW provides eNB 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 eNB, but the FQDN of the SeGW is known (e.g. provided by the IP Autoconfiguration service, configured by EM, pre-configured at the factory). The format of the FQDN is specified in 3GPP TS 32.509 [5].

   1.1) eNB 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 eNB.

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

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

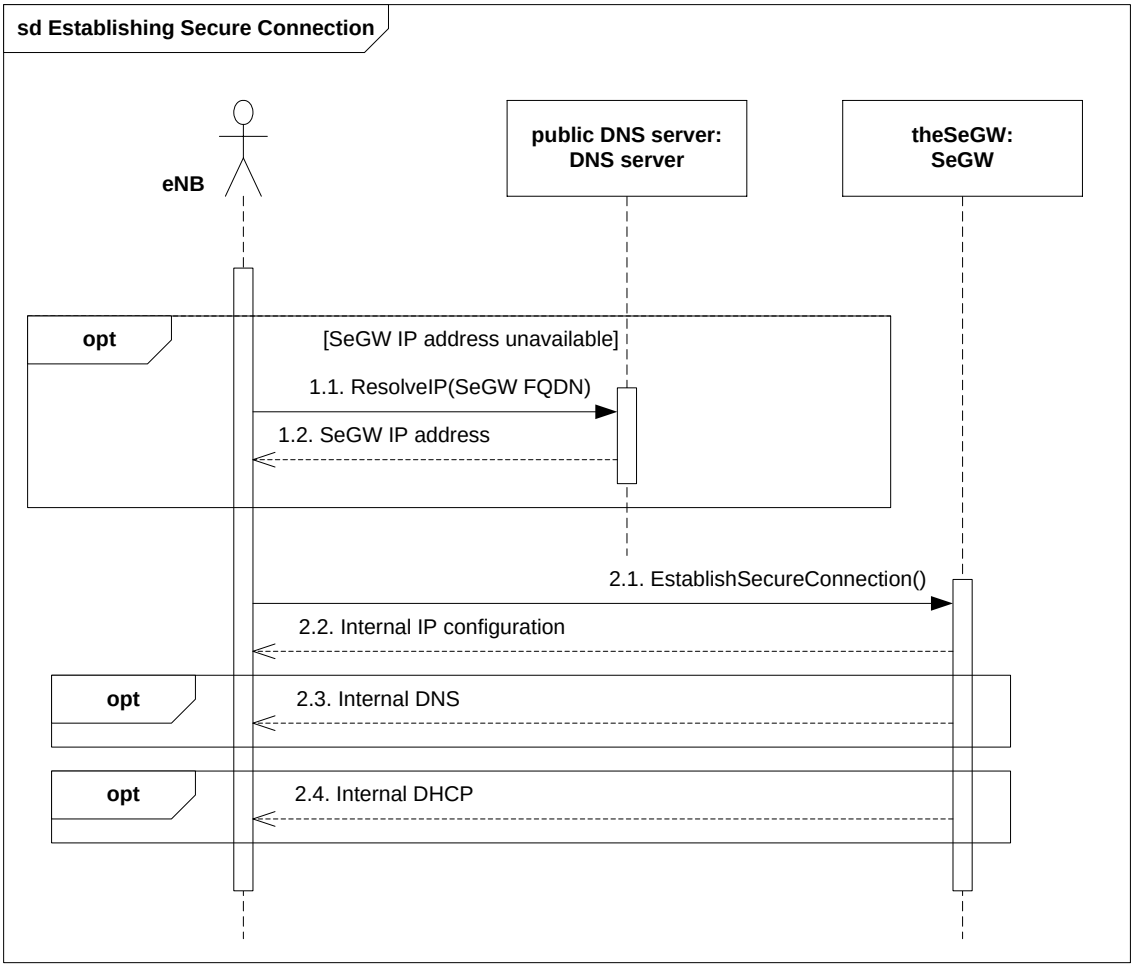

Figure 5.4-1: Establishing secure connection flow

5.5 Establishing connection to Element Manager (EM)

The procedure for establishing connection to EM 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 EM is known to the eNB (e.g. provided by the IP Autoconfiguration service, configured by EM);
- The IP address of the EM is unknown to the eNB, but the FQDN of the EM is known to the eNB (e.g. provided by the IP Autoconfiguration service, configured by EM, pre-configured at the factory);
- The IP address of secure (internal) DHCP server is known to the eNB (e.g. provided in the Configuration Parameters of IKEv2);
- The IP address of secure (internal) DNS server is known to the eNB (e.g. provided in the Configuration Parameters of IKEv2);
- The IP address of the EM configured in the secure (internal) DHCP server;
- The FQDN of the EM 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 EM is unknown to the eNB, 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) eNB sends a request to the secure DHCP server. The eNB may include the vendor specific identifier. The data format used by the eNB in this step is specified in 3GPP TS 32.509 [5].

   1.2) DHCP server provides the IP address of the EM to the eNB. The data format used by the DHCP server in this step is specified in 3GPP TS 32.509 [5].

2) This step is executed only if the IP address of EM is unknown to the eNB, but the FQDN of the EM is known (e.g. provided by the IP Autoconfiguration service, configured by EM, 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 32.509 [5].

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

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

3) and 4) These step are executed only if the IP address and FQDN of the EM are unknown to the eNB, 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) eNB sends a request to the secure DHCP server. The eNB may include the vendor specific identifier. The data format used by the eNB in this step is specified in 3GPP TS 32.509 [5].

   3.2) DHCP server provides the FQDN of the EM to the eNB. The data format used by the DHCP server in this step is specified in 3GPP TS 32.509 [5].

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

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

5) In this step eNB establishes communication with EM. The protocol used for communication between eNB and EM is vendor specific and is out of scope of this specification. The sub-steps listed below are for illustration purposes only.

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

   5.2) In this step EM may provide the eNB with new configuration. 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.

   5.3) In this step EM may provide the eNB with new software.

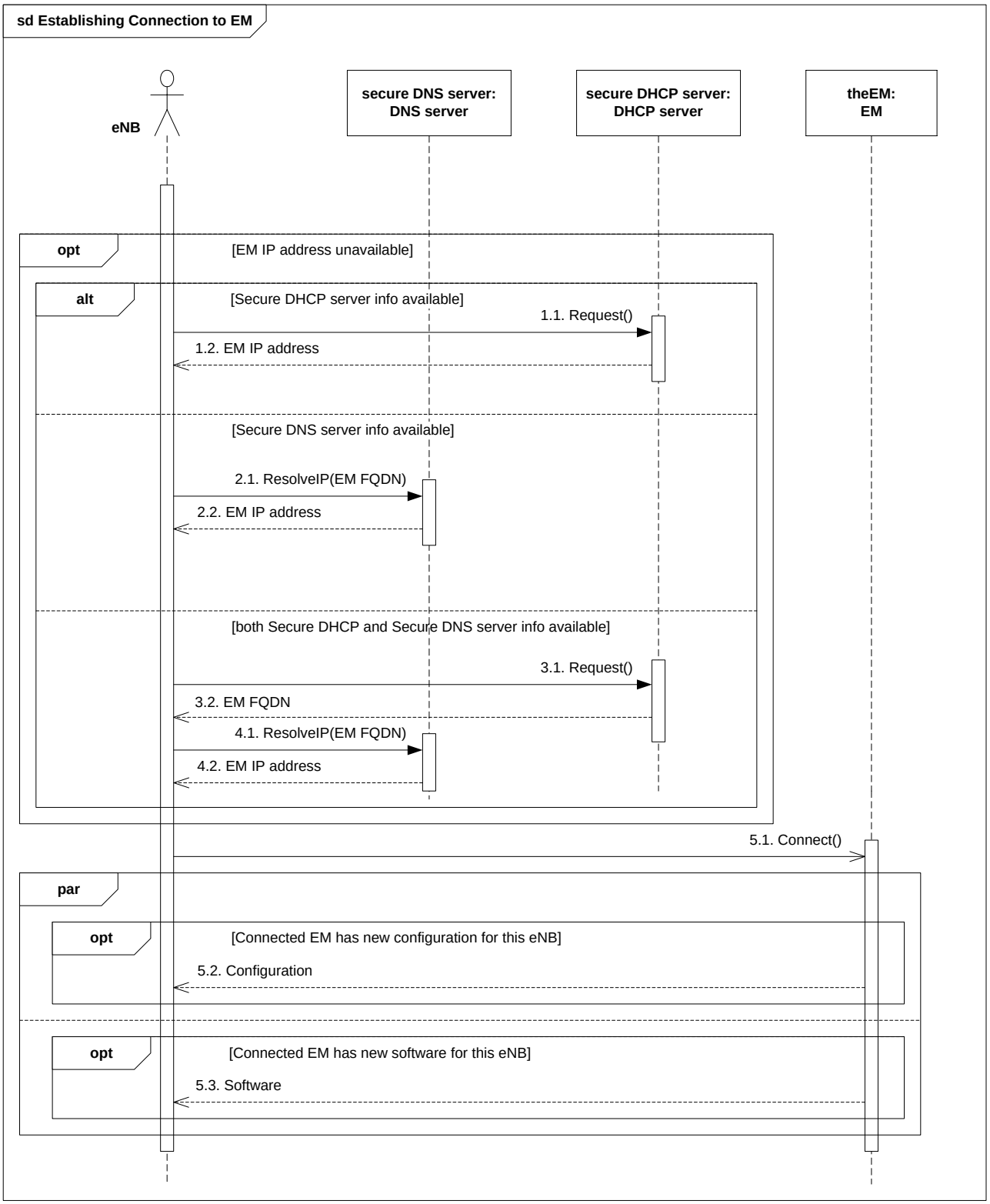

Figure 5.5-1: Establishing connection to Element Manager (EM) flow

Annex A (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2013-08	SA5#90	S5-131428			First version approved after SA5#90		0.1.0
2013-09	SA#61	SP-130452			Presented to SA#61 for information	0.1.0	1.0.0
2013-09	-	-			MCC clean-up for SA5 review	1.0.0	1.0.1
2013-10	-	-			MCC clean-up	1.0.1	1.0.2