3GPP TSG SA WG5 Meeting 135-e S5-211227

electronic meeting, online, 25 January - 3 February 2021

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **32.508** | **CR** | **DraftCR** | **rev** | **-** | **Current version:** | **16.0.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Update procedures flows to applicable for RAN NE | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | S5 | | | | | | | | | |
| ***Source to TSG:*** | Huawei,China Telecom | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eSON\_5G | | | | |  | ***Date:*** | | | 2020.1.15 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The procedures defind in clause 5 (including "High-level plug-and-connect", "Initial IP Autoconfiguration" procedure, "Certificate Enrolment","Establishing Secure Connection","Establishing Connection to MnF") is specifc for eNB not for gNB in non-split scenario and gNB-DU in split scenario. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Update above procedures defined in TS 32.508 to be applicbale for generic RAN NE (which include eNB and gNB). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.1, 5.2, 5.3, 5.4, 5.5, Annex A(new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | | This is the draftCR input to TS 32.508 | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

|  |
| --- |
| **1st Change** |

## 5.1 High-level plug-and-connect

Editor’s Note: the term “RAN NE” and “MnF” used in the following procedures may need to be updated based on the further discussion.

The high level procedure for "multi-vendor plug-and connect" for RAN NE is described next and illustrated in figure 5.1-1. Examples of RAN NE are:

* eNB
* gNB in non-split scenario and gNB-DU in split scenario

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

- One or multiple MnFs for each vendor (e.g. an Initial MnF and zero or more Serving MnFs);

- 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).

Examples of MnF are:

* EM

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

The procedure begins when the RAN 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 RAN 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 RAN NE and MnF and the Core Network(s);

- Via the connection to the MnF the RAN 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 theRAN NE uses it. Otherwise the RAN NE uses the native VLAN where PnP traffic is sent and received untagged.

2) In this step RAN 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 RAN NE.

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

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

5) In this step RAN NE invokes the "Establishing Connection to MnF" procedure (described in clause 5.5). In this step MnF may provide the RAN NE with new configuration. The configuration may contain an address to another MnF that this specific node shall use as MnF. The configuration may contain an address to another SeGW that should be used before connecting to the MnF.

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

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

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

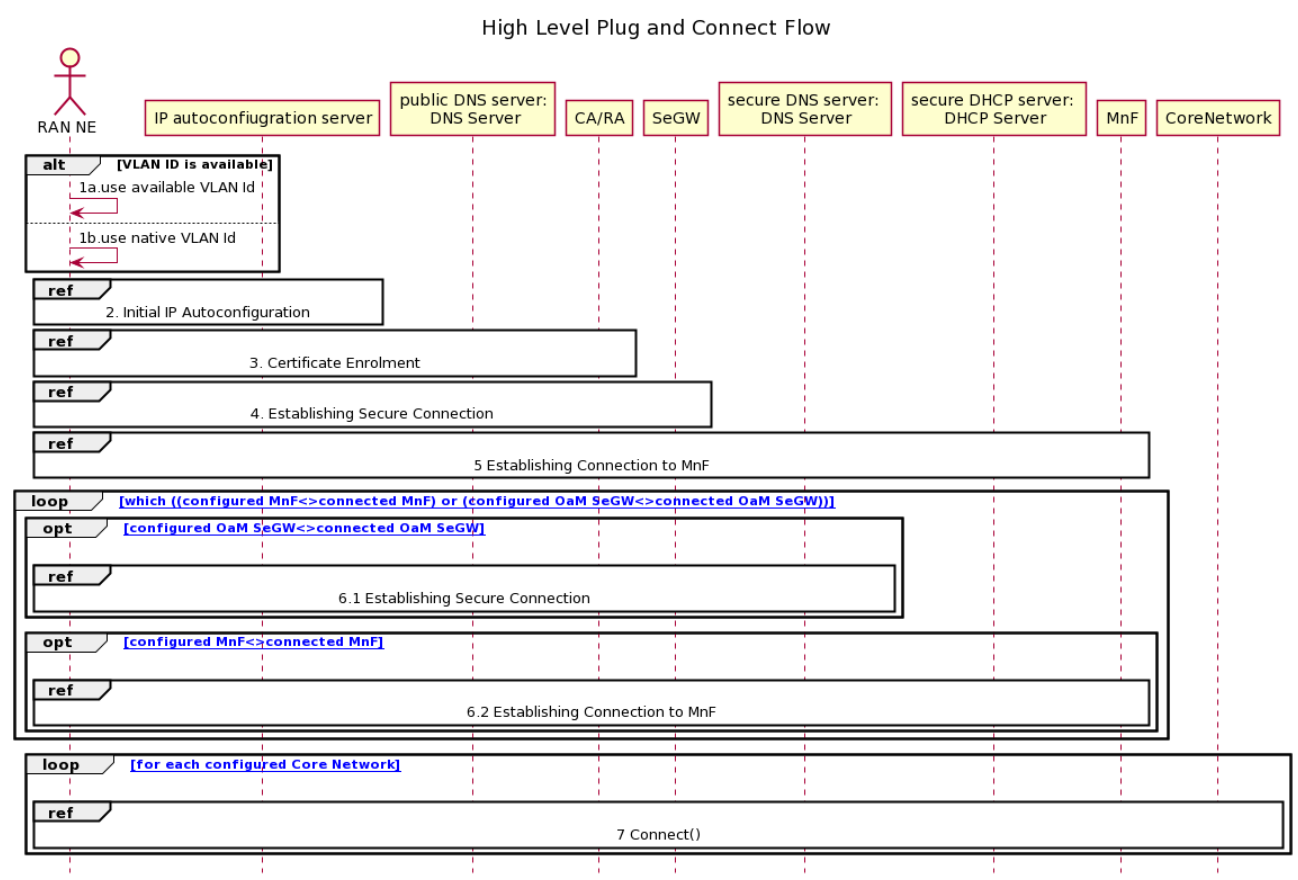


Figure 5.1-1: High-level plug-and-connect flow

|  |
| --- |
| **2nd Change** |

## 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 32.509 [5] section 4.2.2;

- IP Autoconfiguration service is configured with basic IP configuration and the FQDN of CA/RA, and other CA/RA attributes defined in TS 32.509 [5] section 4.2.2;

- 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 32.509 [5] section 4.2.2;

- 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 32.509 [5] section 4.2.2;

- IP Autoconfiguration service is configured with basic IP configuration and the IP addresses of CA/RA, SeGW and MnF, and other CA/RA attributes defined in TS 32.509 [5] section 4.2.2;

- IP Autoconfiguration service is configured with basic IP configuration and the FQDNs of CA/RA, SeGW and MnF, and other CA/RA attributes defined in TS 32.509 [5] section 4.2.2;

- IP Autoconfiguration service is unable to recognize that the client is an RAN NE performing   
the **multi-vendor plug-and-connect** procedure;

- IP Autoconfiguration service is able to recognize that the client is an RAN NE performing   
the **multi-vendor plug-and-connect** procedure;

- IP Autoconfiguration service is unable to recognize that the client is an RAN NE performing   
the **multi-vendor plug-and-connect** procedure and the specific RAN 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 RAN NE sends a request for IP address configuration to the IP Autoconfiguration service (e.g. DHCP server). The RAN NEmay include the vendor specific identifier. The data format used by the RAN NE 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 RAN NE performing **plug-and-connect** procedure and the specific RAN 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 32.509 [5] section 4.2.2;

1.2.c) Client IP configuration and the FQDN of CA/RA, and other CA/RA attributes defined in TS 32.509 [5] section 4.2.2;

1.2.d) Client IP configuration and the IP addresses of CA/RA and SeGW, and other CA/RA attributes defined in TS 32.509 [5] section 4.2.2;

1.2.e) Client IP configuration and the FQDNs of CA/RA and SeGW, and other CA/RA attributes defined in TS 32.509 [5] section 4.2.2;

1.2.f) Client IP configuration and the IP addresses of CA/RA, SeGW and MnF, and other CA/RA attributes defined in TS 32.509 [5] section 4.2.2;

1.2.g) Client IP configuration and the FQDNs of CA/RA, SeGW and MnF, and other CA/RA attributes defined in TS 32.509 [5] section 4.2.2.

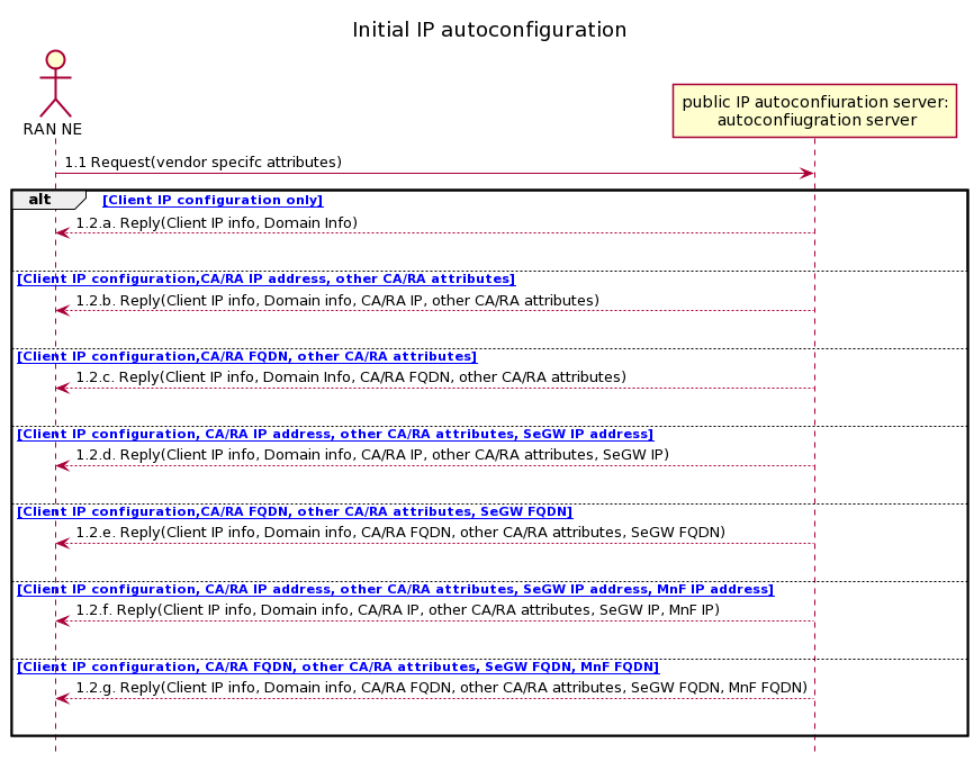


Figure 5.2-1: Initial IP Autoconfiguration flow

|  |
| --- |
| **3rd Change** |

## 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 RAN NE (e.g. provided by the IP Autoconfiguration service);

- The IP address of the CA/RA is unknown to the RAN NE, but the FQDN of the CA/RA is known to the RAN 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 RAN 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 32.509 [5].

1.1) RAN 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 RAN NE.

2) In this step RAN 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 RAN NE enrols using the vendor certificate (e.g. pre-programmed at the factory) and other CA/RA attributes defined in TS 32.509 [5] section 4.2.2 provided by IP Autoconfiguration service.

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

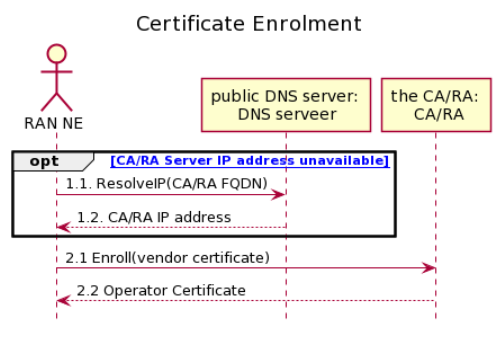


Figure 5.3-1: Certificate enrolment flow

|  |
| --- |
| **4th Change** |

## 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 RAN NE (e.g. provided by the IP Autoconfiguration service, configured by MnF);

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

- The SeGW provides RAN NE only with internal IP configuration;

- The SeGW provides RAN NE with internal IP configuration and the IP address of the secure (internal) DHCP server;

- The SeGW provides RAN NE with internal IP configuration and the IP address(es) of the secure (internal) DNS server(s);

- The SeGW provides RAN 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 RAN NE, but the FQDN of the SeGW is known (e.g. provided by the IP Autoconfiguration service, configured by MnF, pre-configured at the factory).   
The format of the FQDN is specified in 3GPP TS 32.509 [5].

1.1) RAN 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 RAN NE.

2) In this step RAN NE 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 RAN 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 RAN 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 RAN 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 RAN NE receives the IP address of secure (internal) DHCP server from the SeGW in the Configuration Parameters of IKEv2.

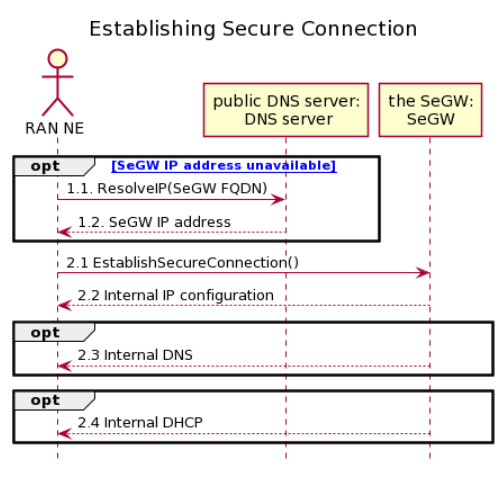


Figure 5.4-1: Establishing secure connection flow

|  |
| --- |
| **5th Change** |

## 5.5 Establishing connection to Management Function (MnF)

The procedure for establishing connection to MnF 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 MnF is known to the RAN NE (e.g. provided by the IP Autoconfiguration service, configured by MnF);

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

- The IP address of secure (internal) DHCP server is known to the RAN NE (e.g. provided in the Configuration Parameters of IKEv2);

- The IP address of secure (internal) DNS server is known to the RAN NE (e.g. provided in the Configuration Parameters of IKEv2);

- The IP address of the MnF configured in the secure (internal) DHCP server;

- The FQDN of the MnF 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 MnF is unknown to the RAN 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) RAN NE sends a request to the secure DHCP server. The RAN NE may include the vendor specific identifier. The data format used by the RAN NE in this step is specified in 3GPP TS 32.509 [5].

1.2) DHCP server provides the IP address of the MnF to the RAN NE. 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 MnF is unknown to the RAN NE, but the FQDN of the MnF is known (e.g. provided by the IP Autoconfiguration service, configured by MnF, 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) RAN NE sends a request containing the FQDN of the MnF to the secure (internal) DNS server.

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

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

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

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

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

5) In this step RAN NE establishes communication with MnF. The protocol used for communication between RAN NE and MnF 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 RAN NE connects to the MnF and identifies itself. The RAN NE may provide MnF with its current software version and configuration.

5.2) In this step MnF may provide the RAN NE with new configuration

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

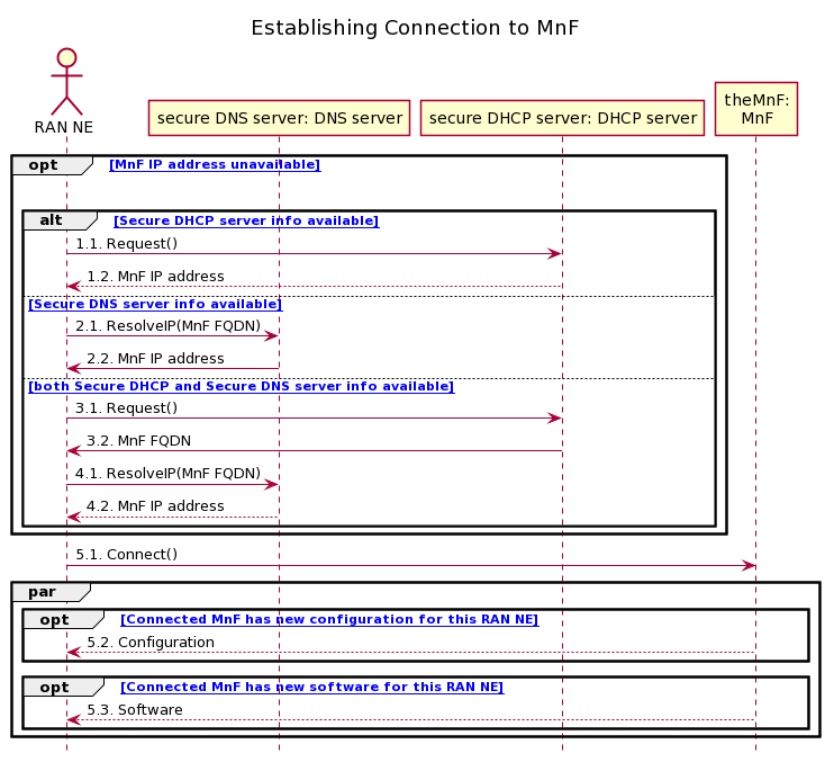


Figure 5.5-1: Establishing connection to Management Function (MnF) flow

|  |
| --- |
| **6th Change** |

Annex A (informative):  
PlantUML source code

# A.1 High-level plug-and-connect

title " High Level Plug and Connect Flow"

actor "RAN NE" as NE

participant "IP autoconfiugration 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: \nDNS Server" as S\_DNS\_Server

participant "secure DHCP server: \nDHCP Server" as S\_DHCP\_Server

participant MnF

participant CoreNetwork

alt VLAN ID is available

NE->NE: 1a.use available VLAN Id

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,MnF: 5 Establishing Connection to MnF

loop [ [which ((configured MnF<>connected MnF) 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,S\_DNS\_Server:6.1 Establishing Secure Connection

End

opt [ [configured MnF<>connected MnF] ]

|||

Ref over NE,IP\_Server,P\_DNS\_Server,CA\_RA, SeGW,S\_DNS\_Server,S\_DHCP\_Server,MnF:6.2 Establishing Connection to MnF

End

End

loop [ [for each configured Core Network] ]

|||

Ref over NE,IP\_Server,P\_DNS\_Server,CA\_RA, SeGW,S\_DNS\_Server,S\_DHCP\_Server,MnF,CoreNetwork:7 Connect()

End

skinparam shadowing false

hide footbox

@enduml

# A.2 Initial IP Autoconfiguration

@startuml

title "Initial IP autoconfiguration"

actor "RAN NE" as NE

participant "public IP autoconfiuration server:\n autoconfiugration server" as IP\_Server

NE -> IP\_Server: 1.1 Request(vendor specifc attributes)

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, MnF IP address] ]

IP\_Server --> NE: 1.2.f. Reply(Client IP info, Domain info, CA/RA IP, other CA/RA attributes, SeGW IP, MnF IP)

|||

Else [ [Client IP configuration, CA/RA FQDN, other CA/RA attributes, SeGW FQDN, MnF FQDN] ]

IP\_Server -->NE: 1.2.g. Reply(Client IP info, Domain info, CA/RA FQDN, other CA/RA attributes, SeGW FQDN, MnF FQDN)

|||

End

skinparam shadowing false

hide footbox

@enduml

# A.3 Certificate enrolment

@startuml

title "Certificate Enrolment"

actor "RAN NE" as NE

participant "public DNS server: \nDNS serveer" as P\_DNS\_Server

participant "the CA/RA: \n CA/RA" as CA\_RA

opt [ [CA/RA Server IP address unavailable] ]

NE->P\_DNS\_Server: 1.1. ResolveIP(CA/RA FQDN)

P\_DNS\_Server -->NE: 1.2. CA/RA IP address

End

NE->CA\_RA: 2.1 Enroll(vendor certificate)

CA\_RA-->NE: 2.2 Operator Certificate

skinparam sequenceActorBackgroundColor #FFFFFF

skinparam sequenceParticipantBackgroundColor #FFFFFF

skinparam noteBackgroundColor #FFFFFF

autonumber "#'.'"

skinparam monochrome true

skinparam shadowing false

hide footbox

@enduml

# A.4 Establishing secure connection

@startuml

title "Establishing Secure Connection"

actor "RAN NE" as NE

participant "public DNS server:\n DNS server" as P\_DNS\_Server

participant "the SeGW:\nSeGW" as SeGW

opt [ [SeGW IP address unavailable] ]

NE -> P\_DNS\_Server: 1.1. ResolveIP(SeGW FQDN)

P\_DNS\_Server -->NE: 1.2. SeGW IP address

End

NE->SeGW: 2.1 EstablishSecureConnection()

SeGW -->NE: 2.2 Internal IP configuration

opt

SeGW -->NE: 2.3 Internal DNS

End

opt

SeGW -->NE: 2.4 Internal DHCP

End

skinparam shadowing false

hide footbox

@enduml

# A.5 Establishing connection to Management Function (MnF)

@startuml

title "Establishing Connection to MnF"

actor "RAN NE" as NE

participant "secure DNS server:\n DNS server" as S\_DNS\_Server

participant "secure DHCP server: \nDHCP server" as S\_DHCP\_Server

participant "theMnF:\nMnF" as MnF

opt [ [MnF IP address unavailable] ]

|||

alt [ [Secure DHCP server info available] ]

NE -> S\_DHCP\_Server: 1.1. Request()

S\_DHCP\_Server --> NE: 1.2. MnF IP address

Else [ [Secure DNS server info available] ]

NE->S\_DNS\_Server: 2.1. ResolveIP(MnF FQDN)

S\_DNS\_Server->NE: 2.2. MnF IP address

Else [ [both Secure DHCP and Secure DNS server info available] ]

NE->S\_DHCP\_Server: 3.1. Request()

S\_DHCP\_Server->NE: 3.2. MnF FQDN

NE->S\_DNS\_Server: 4.1. ResolveIP(MnF FQDN)

S\_DNS\_Server-->NE: 4.2. MnF IP address

End

End

NE->MnF: 5.1. Connect()

par

opt [ [Connected MnF has new configuration for this RAN NE] ]

MnF --> NE: 5.2. Configuration

End

opt [ [Connected MnF has new software for this RAN NE] ]

MnF-->NE: 5.3. Software

End

End

skinparam shadowing false

hide footbox

@enduml

|  |
| --- |
| **End of Change** |