ETSI TS 132 583 V18.0.0 (2024-05)

Universal Mobile Telecommunications System (UMTS);
LTE;
Telecommunication management;
Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P);
Procedure flows for Type 1 interface HNB to HNB Management System (HMS)
(3GPP TS 32.583 version 18.0.0 Release 18)

Reference
RTS/TSGS-0532583vi00

Keywords
LTE,UMTS

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

Introduction

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

3GPP TS 32.581: "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Concepts and requirements for Type 1 interface HNB to HNB Management System (HMS)".

3GPP TS 32.582: "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Information model for Type 1 interface HNB to HNB Management System (HMS)".

3GPP TS 32.583: "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Procedure flows for Type 1 interface HNB to HNB Management System (HMS)".

3GPP TS 32.584: "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); XML definitions for Type 1 interface HNB to HNB Management System (HMS)".

1 Scope

The present document describes the procedure flows between HNB & HMS for the OAM of HNB Management.

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 32.300: "Telecommunication management; Configuration Management (CM); Name convention for Managed Objects".

[5] TR-069 Amendment 2, CPE WAN Management Protocol v1.1, Broadband Forum, viewable at

[6] 3GPP TR 25.820 3G Home NodeB Study Item Technical Report

[7] 3GPP TS 25.401 Radio Access Network UTRAN Overall Description

[8] 3GPP TR 32.821: "Study of Self-Organizing Network (SON) related OAM for Home NodeB".

[9] 3GPP TS 25.467: "UTRAN architecture for 3G Home NodeB, stage 2".

[10] 3GPP TS 32.582: "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Information model for Type 1 interface HNB to HNB Management System (HMS)".

[11] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

3 Definitions and abbreviations

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

3.1 Definitions

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

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

DNS	Domain Name Server
FTP	File Transfer Protocol
HMS	Home NodeB Management System
HNB	Home NodeB
HNB-GW	Home NodeB Gateway
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
LAN	Local Area Network
MNO	Mobile Network Operator
RNC	Radio Network Controller
RPC	Remote Procedure Call
SeGW	Security Gateway
SSL	Secure Socket Layer
sFTP	Secure File Transfer Protocol
TLS	Transport Layer Security
URL	Unified Resource Locator

4 Architecture for HNB Management

4.1 HNB OAM functional architecture

This section provides the HNB OAM functional architecture. We distinguish the two following cases:

- A HNB is connected to a BB device (typically a residential gateway providing connectivity via an access provider domain). The BB device provides routing, NAT and firewall functionality.
- A BB device with an integrated HNB functionality.

The HNB Management System (HMS) main tasks are to provision configuration data on the HNB. It provides the following functional entities:

- A file server.
- A TR-069 auto-configuration server (ACS).

However the file server may be used by other applications in the MNO domain.

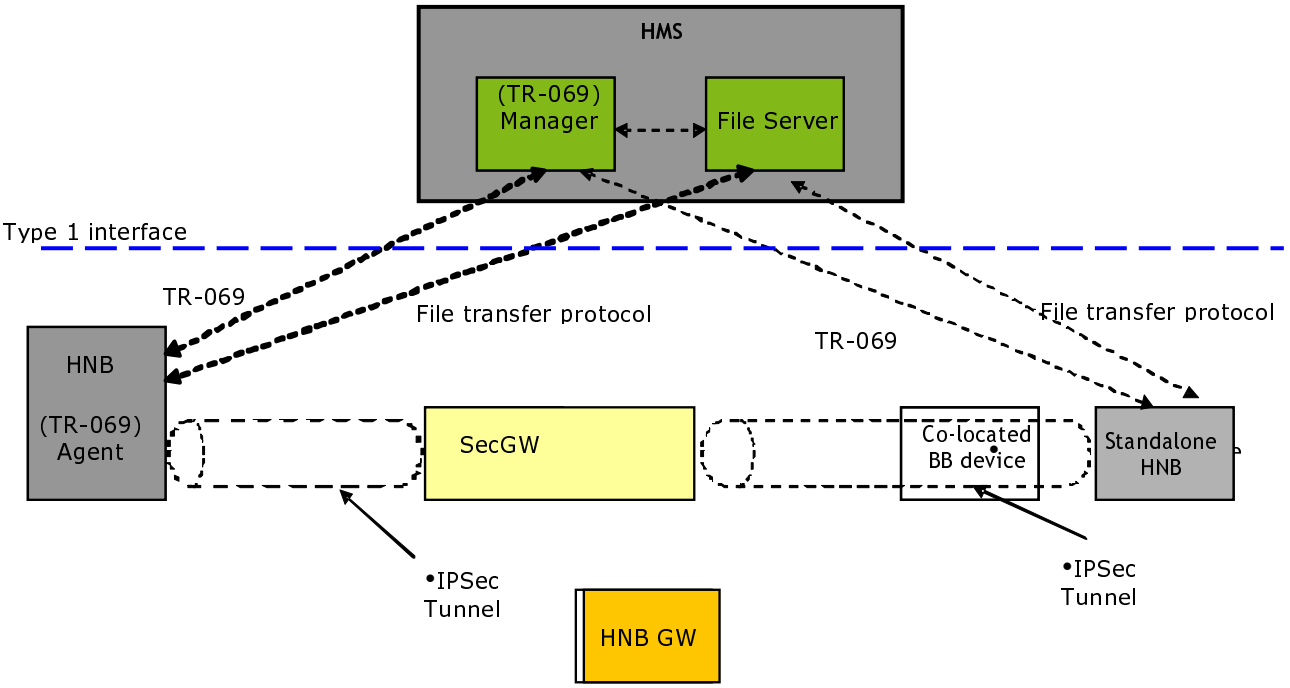

Figure 4.1.1-1: Architecture for HNB Management

4.2 Functional Elements

4.2.1 HNB Management System (HMS)

The HMS is composed of a TR-069 manager and a file server. The TR069 manager implements the Auto-Configuration Server function as defined in TR-069 standard and performs CM, FM and PM functionalities to the HNB. The file server may be used for file upload or download, as instructed by TR-069 manager

4.2.1.1 Initial HNB Management System (HMS)

The initial HMS may provide location verification of HNB and assigns appropriate serving elements (Serving HMS, Security Gateway and HNB-GW).

4.2.1.2 Serving HNB Management System (HMS)

Provides the following functionalities:

- TR-069 Auto-configuration server.
- File server for file upload or download.
- Provisioning of configuration data to the HNB.
- Performance & Fault updates.
- Provides Serving SeGW discovery.

4.2.2 Security Gateway (SeGW)

SeGW terminates Secure tunnelling for TR-069 as well as Iuh. It is used for authentication of HNB & provides access to HMS and HNB-GW.

4.2.2.1 Initial Security Gateway (SeGW)

The URL of the Initial SeGW may be factory programmed in the HNB so as to allow initial establishment of an IPSec security association and communication with the initial HMS.

4.2.2.2 Serving Security Gateway (SeGW)

Terminates IPSec security association and implements a forwarding function to allow forwarding IP packets upstream and downstream:

- Downstream: packets are forwarded on appropriate IPSec tunnels towards the HNB based on their destination IP addresses
- Upstream: forwarding IP traffic to the appropriate HNB-GW, HMS or other network elements based on destination IP addresses

4.2.3 HNB Gateway (HNB-GW)

Terminates Iuh from HNB. Appears as a RNC to the existing Core network using existing Iu interface.

5 Procedure Flows

5.1 Discovery procedures (Mandatory)

When the HNB is initially powered up, it shall contact with HMS (initial) to discover HNB-GW for the first step. HMS (initial) assigns the HNB corresponding local access information of Security Gateway (serving), HMS (serving) and optionally HNB-GW according to the HNB's location information. The HNB-GW information shall be provided either by the HMS (initial) or the HMS (serving). The HNB is pre-configured with the address information of HMS (initial) and Security Gateway (initial) and with an operator trusted root CA certificate allowing the validation of the certificate presented by HMS (as TLS server) or Security Gateway (as IKEv2 responder), while HMS (serving) may be physically different from HMS (initial). The address information of Security Gateway (initial) should be consistent with that in the certificate presented by Security Gateway (initial). When authentication between HNB and HMS (initial) is needed, the address information of HMS (initial) should be consistent with that in the certificate presented by HMS (initial).

There are two scenarios that need to be distinguished for the HNB-GW discovery:

- HMS (initial) is accessible via IPSec to the Security Gateway (initial) on the MNO Intranet.
- HMS (initial) is accessible on the public Internet.

5.1.1 Discovery procedures via HMS (initial) accessible on the MNO Intranet (Mandatory)

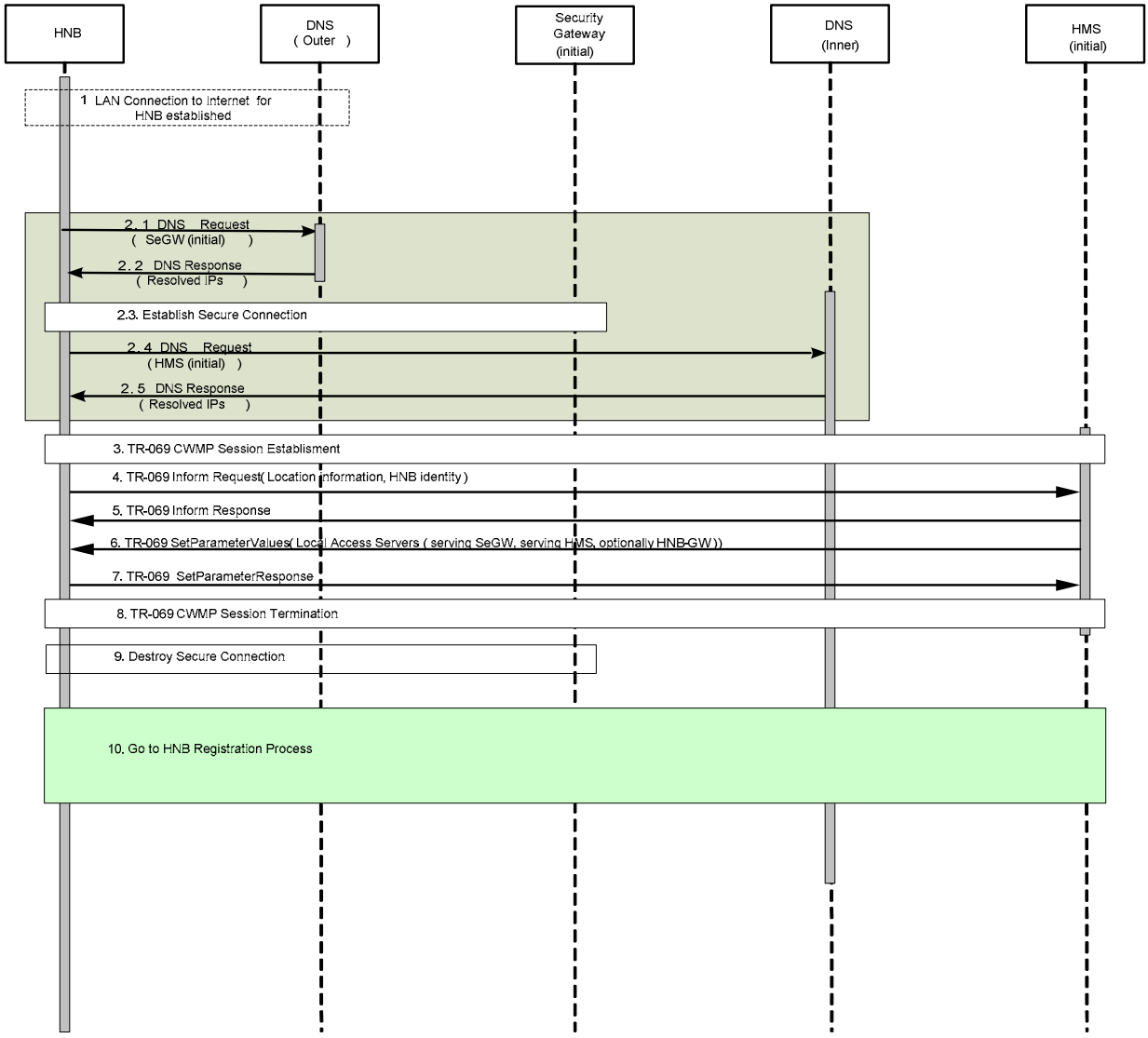

Figure 5.1.1-1: HNB-GW discovery via HMS (initial) accessible on the MNO Intranet

1. The HNB establishes a LAN connectivity to the Internet when it is initially powered up.

2. The HNB initiates a process to get IP address of Security Gateway (initial).

   2.1 The HNB requests outer DNS (Domain Name Server) server for the address of Security Gateway (initial)'s URL.

   2.2.DNS responds to the HNB with the IP addresses of Security Gateway (initial) URL.

   2.3 The secure connection is established between the HNB and Security Gateway (initial).

   2.4 The HNB requests DNS (inner) via IPSec tunnel secure connection for the address of HMS (initial) URL.

   2.5 DNS (inner) responses to the HNB with the IP addresses of HMS (initial).

3. The CWMP Session is established between the HNB and HMS (initial).

4. The HNB sends to HMS (initial) an Inform Request containing location parameters and HNB Identity etc.

5. HMS (initial) returns an Inform response to accept the HNB location information.

6. HMS (initial) then prepares for the local access information (including serving Security Gateway and serving HMS) and sets the values on the HNB using the SetParameterValues message. The Initial HMS may also optionally provide the HNB-GW information to the HNB.

Note: If the Initial HMS does not provide HNB-GW then the serving HMS shall provide it during the HNB registration procedure.

7. The HNB acknowledges the updation by returning a SetParameterValues Response message. If HMS (serving) is the same physical entity as HMS (initial), then go to step 10.

8. The HNB releases the CWMP Session between the HNB and HMS (initial).

9. The IP secure tunnel connection may be destroyed between the HNB and Security Gateway (initial).

10. Next to execute HNB registration process.

5.1.2 Discovery procedures via HMS (initial) accessible on the public Internet (Mandatory)

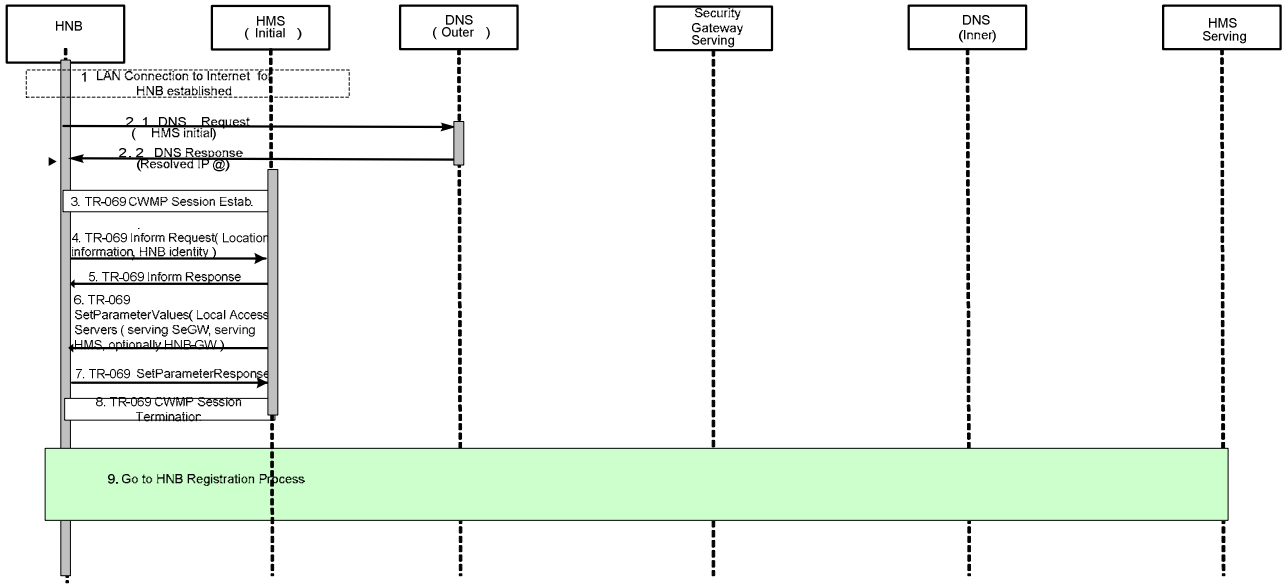

Figure 5.1.2-1: HNB-GW discovery via HMS (initial) accessible on the public Internet

In this case the HNB is factory programmed with the initial TR-069 manager URL. The MNO needs to publish the initial TR-069 manager domain name in the outer DNS. At the initial switch-on, the HNB performs the following steps:

1. The HNB establishes a LAN connectivity to the Internet when it is initially powered up.

2. The HNB resolves the host name of the HMS (initial) through going to the outer DNS

3. TR-069 session establishment with the HMS (initial) that is accessible on the public Internet using TLS/SSL security.

4. The HNB sends to HMS (initial) an Inform Request containing location parameters and HNB Identity etc.

5. HMS (initial) returns an Inform response to accept the HNB location information.

6. HMS (initial) then prepares for the local access information (including serving Security Gateway and serving HMS) and sets the values on the HNB using the SetParameterValues message. The Initial HMS may also optionally provide the HNB-GW information to the HNB.

Note: If the Initial HMS does not provide HNB-GW then the serving HMS shall provide it during the HNB registration procedure.

7. The HNB acknowledges the update by returning a SetParameterValuesResponse message.

8. The HNB releases the CWMP Session between the HNB and HMS (initial).

9. Next to execute HNB registration process.

5.2 HNB Registration (Mandatory)

5.2.1 HNB registration Procedure (Mandatory)

HNB registration is a process to put the HNB into service when it is initially powered up. The process contains two sub-processes of registration: registration to HMS (serving) and registration to HNB-GW. In this section, the HNB registration is mainly focused on registration to HMS (serving), and registration to HNB-GW has a reference to the definition of TS 25.467 Section 5.2.2. HMS (serving) may be physically different from HMS (initial).

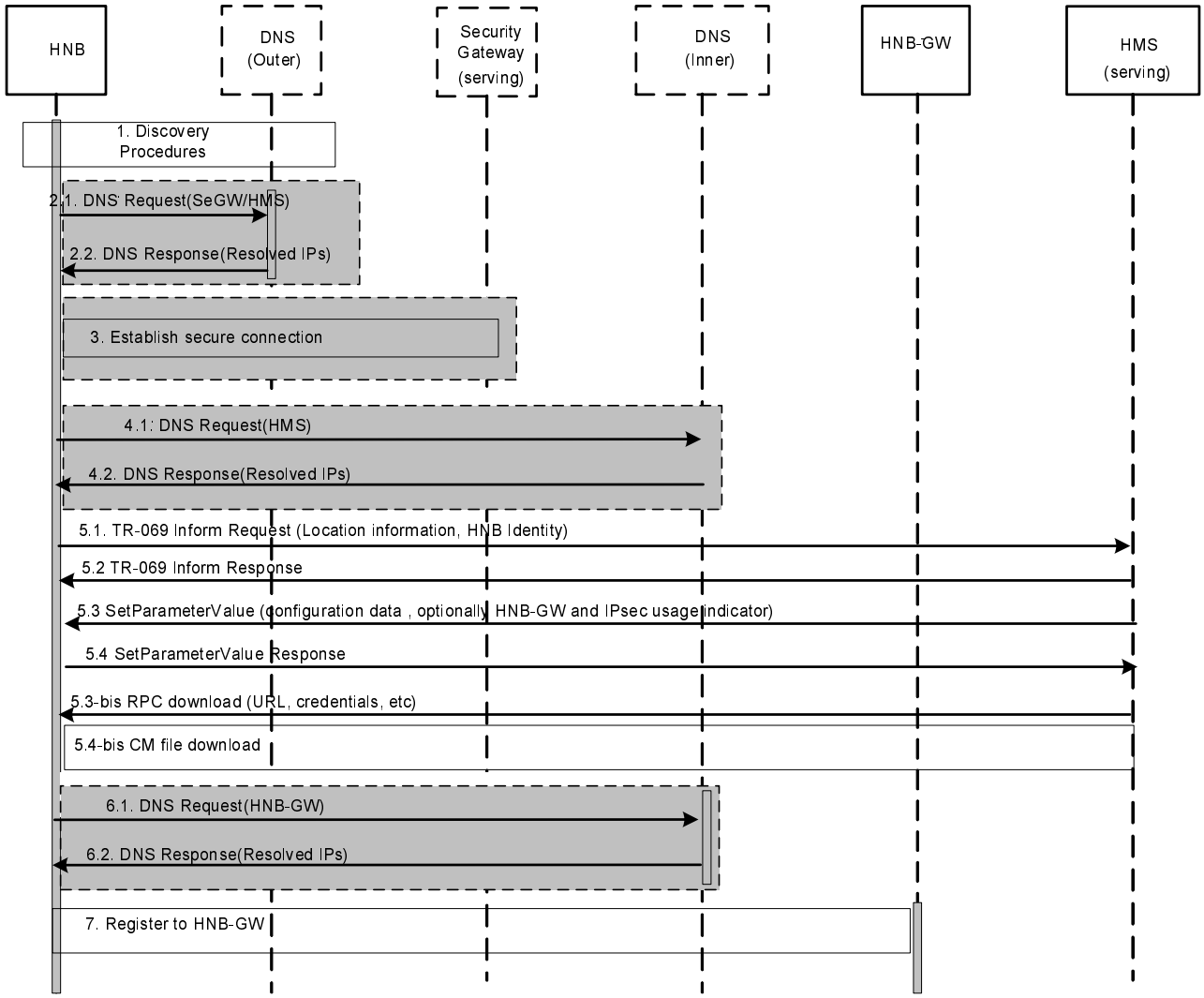

Figure 5.2.1-1: HNB Registration procedure flow

1. The HNB has discovered the Serving SeGW and the Serving HMS and optionally HNB-GW (if the HMS (initial) provided the HNB-GW during the discovery procedures) and start the registration process. If the secure connection between the HNB and HMS (serving) has already been established, then go directly to step 4. In this case, HMS (serving) is the same physical entity as HMS (initial).

   Note: If the HNB-GW information is not provided during the discovery procedure flow then it shall be provided in step 5.3.

1. If the local access information of Security Gateway (serving) obtained by the HNB is URL, then the HNB fetches the IP address of Security Gateway (serving) from public outer DNS. If the HMS connection is to be established outside the IPSEC tunnel and the HMS (serving) obtained by the HNB is URL, then the HNB also fetches the IP address of HMS (serving) from outer DNS

   2.1 The HNB requests public outer DNS (Domain Name Server) server for the IP address of the Security Gateway (serving)'s URL and optionally the HMS (serving)'s URL.

   2.2. Public Outer DNS responds to the Home NodeB with the IP addresses of the Security Gateway (serving) URL and optionally the IP address of HMS (serving) URL.

1. A secure connection is established between the HNB and Security Gateway (serving).

2. If the HMS connection is to be established inside the IPSEC tunnel and the If the HMS (serving) obtained by the HNB is URL, then the HNB fetches the IP address of HMS (serving) from DNS server (inner) via the secure connection.

   4.1 The HNB requests DNS server (inner) via secure connection for the IP address of the HMS (serving) URL.

   4.2. DNS (inner) responds to the Home NodeB with the IP addresses of HMS (serving) URL.

3. Registration to HMS (serving)

   5.1 The HNB sends to HMS (serving) an Inform Request message containing HNB general information as location parameters and HNB Identity, which has a reference to TS 25.467 Section 5.2.2 etc.

   5.2 HMS (serving) returns an Inform Response message to accept the HNB general information.

   5.3 The HMS (serving) provisions the HNB with configuration data optionally including HNB-GW and IPsec usage indicator (if the HNB-GW is not provided in the discovery procedures then it must be provided in step 5.3)

   5.4 The HNB acknowledges the provisioning data by sending a SetParameterValue Response

   Optionally if CM is done by means of a file download then step 5.3 and step 5.4 are replaced by 5.3-bis and 5.4 bis:

      5.3-bis HMS (Serving) may trigger by means of download RPC a CM file download providing CM data.

      5.4-bis CM file download procedure optionally including the HNB-GW and IPsec usage indicator.

4. If the HNB-GW obtained by the HNB is URL, then the HNB fetches the IP address of the HNB-GW from DNS server (inner) via the secure connection.

   6.1 The HNB requests DNS server (inner) via secure connection for the IP address of the HNB-GW URL.

   6.2. DNS (inner) responds to the Home NodeB with the IP addresses of HNB-GW URL.

7. Registration to HNB-GW, which is already defined in TS 25.467 section 5.2.2.

5.2.2 HNB IPSec IP address change procedure (Conditional Mandatory)

The precondition is to configure HNB using IPsec. If the inner IPsec tunnel IP address of the HNB changes and HNB is connected to HMS via IPSec Tunnel then the HNB shall notify the TR-069 manager using TR-069. To this end the HNB shall establish a connection to the Serving TR-069 manager and use the inform method to update the IPSec IP address. The following flow diagram provides the details of this procedure flows.

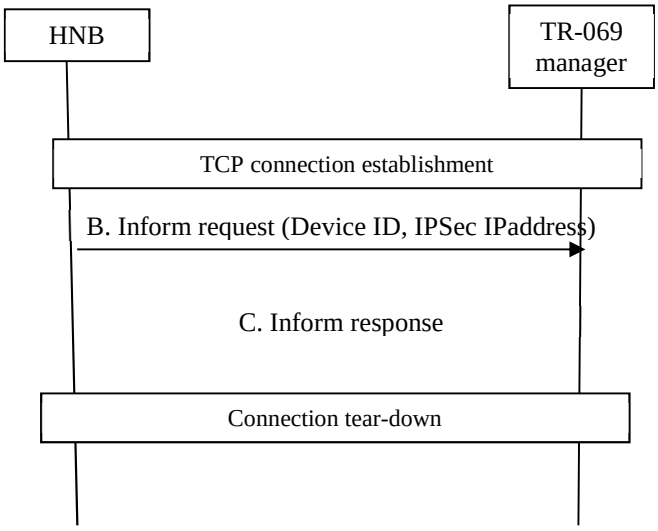

Figure 5.2.2-1

The basic steps for the IPSec IP address update are as follows:

A. Connection establishment triggered by the HNB to the TR-069 manager as soon as possible following a change of the IPSec IP address (the procedure for changing the IPSec IP address are outside the scope of this document).

B. The HNB uses the Inform request method of TR-069 to provide the TR-069 manager with the new IPSec IP address of the HNB in conjunction with the HNB identity (manufacturer serial number)

C. The TR-069 manager acknowledges the receipt of the new IPSec IP address of the HNB.

5.3 HNB Configuration Management (Mandatory)

This section specifies the procedure flows for HNB configuration management using TR-069. As per TS 32.581, CM can be achieved by means of RPC as a mandatory feature or by means of file download as an optional feature:

- RPC set parameter values method: Following a registration of the HNB to the TR-069 manager, the TR-069 starts updating CM data on the HNB by means of the Set Parameter Value method of RPC in any combination or order. Subsequent updates of the CM data are done using the same procedure (for any combination of parameters).

- File download: Following a registration of the HNB to the TR-069 manager, the TR-069 manager may trigger the HNB to start a file download of CM data. Subsequent to this initial phase the TR-069 may trigger at any point in time the HNB to start a file download to allow an update of the CM data.

5.3.1 HNB configuration management by means of file download (Optional)

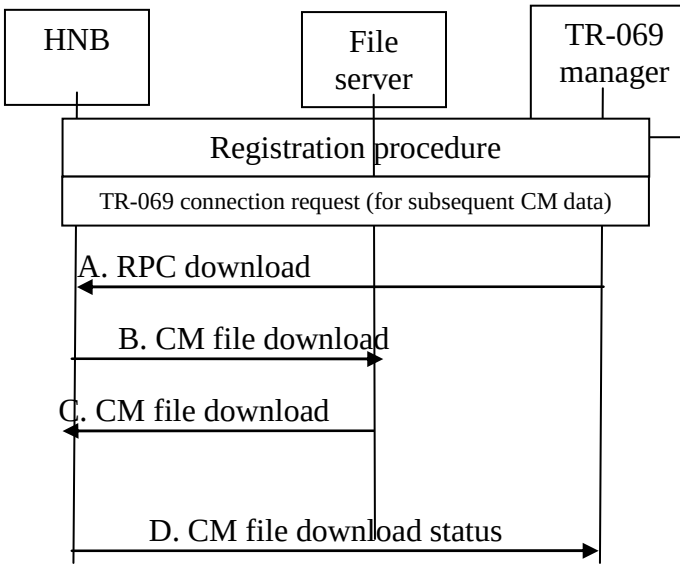

Figure 5.3.1-1

Following the HNB registration procedure or subsequently when the TR-069 manager decides to update CM data (in this case the TR-069 manager needs to issue a connection request to the HNB), the following sequence of exchange takes place

A. The TR-069 manager instructs the HNB by means of an RPC method, namely download, to start a CM file download. The parameters for the download method can refer to TR-069 Amendment 2 [5] Table 30 - download arguments.

B. The HNB starts a CM file download request to the File server by using one of the available interfaces (FTP, HTTP, etc) as specified in the URL

C. The CM file is downloaded from the File server. The file format is specified in TS 32.584.

D. CM file download status indication: the HNB indicates success or failure of the CM file download to the TR-069 manager. The success case means all downloaded parameters are installed / configured in the HNB. The failure case means none of the downloaded parameters is installed / configured in the HNB. Possible reasons are: one or more downloaded parameters are considered illegal or invalid, the downloaded file was corrupted.

The mechanisms by which the CM file is installed on the File server and the corresponding URL is built and provided to the TR-069 manager are not specified in this document.

5.3.2 HNB configuration management using RPC Set Parameter Value method (Mandatory)

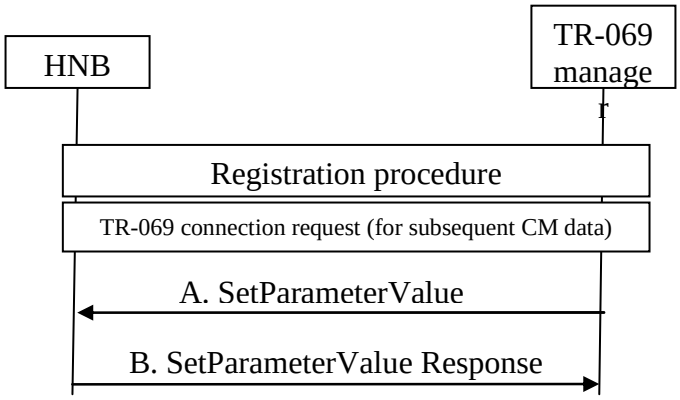

Figure 5.3.2-1

Following the HNB registration procedure or subsequently when the TR-069 manager decides to update CM data (in this case the TR-069 manager needs to issue a connection request to the HNB), the following sequence of exchange takes place

A. The TR-069 manager calls a SetParameterValue RPC on the HNB with the following parameters:

- Parameter List: the set of parameter names and corresponding values

B. indicates the status of the SetParameterValue RPC (success or failure)

5.4 HNB De-Provisioning (Mandatory)

The TR-069 manager must provide the ability for the operator to de-provision a HNB (e.g. if the subscriber ends his subscription).

Subsequent requests from the HNB shall not lead to the registration process described in clause 5.2 until the operator allows it.

De-provisioning may involve other operations which are not in the scope of this document...

There are two possible ways to de-provision a HNB:

- Use of FactoryReset RPC method (optional in TR-069)
- SetParameterValue to reset all or a set of HNB parameters

If the FactoryReset RPC method is used, the HNB must initiate the factory reset procedure only after successful completion of the session.

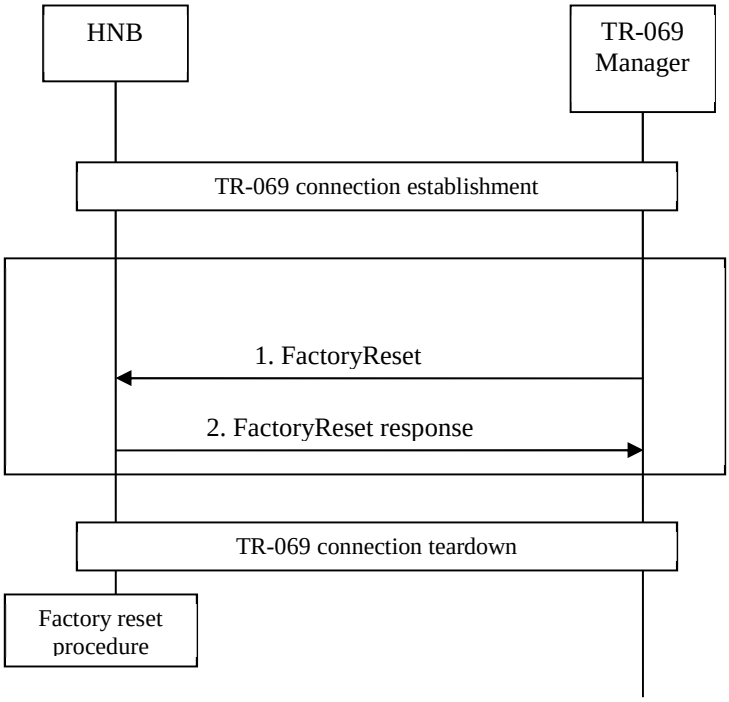

Figure 5.4-1: HNB de-provisioning using FactoryReset RPC method

Figure 5.4-2 provides the procedure flows for HNB deregistration using SetParameterValue. The process consists in reinitializing all or a set of parameters in the data model. The set of parameters to be reinitialized is operator policy dependent.

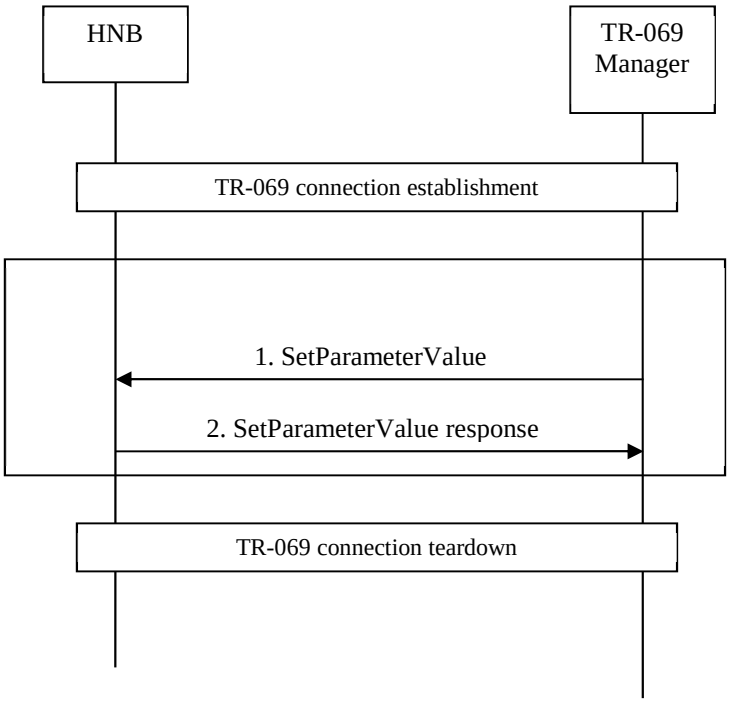

Figure 5.4-2: HNB de-provisioning using SetParameterValue method

5.5 Alarm Reporting (Mandatory)

5.5.1 Alarm Reporting Mechanism Configuration (Mandatory)

This procedure allows TR-069 Manager to use SetParameterValues method to determine by which alarm attributes of the HNB alarms shall be selected out and reported to TR-069 Manager. The alarms shall be selected out by perceived severity, alarm type, etc.

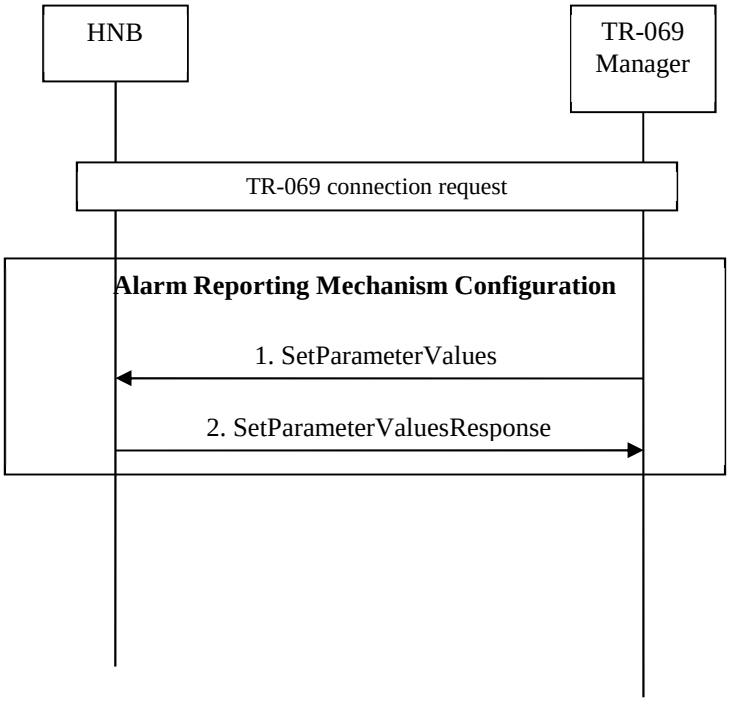

Figure 5.5.1-1: Alarm Reporting Mechanism Configuration

A TR-069 connection is requested to be established before the procedure.

1. TR-069 Manager initiates alarm reporting mechanism configuration by using SetParameterValues. The parameters determined in SetParameterValues are referring to TS 32.582 [10].

2. HNB responses to TR-069 Manager to confirm alarm reporting mechanism by SetParameterValues Response. If the response message returns an error code, then the procedure ends up with failure.

The detail procedure of SetParameterValues refer to TR-069 Amendment 2 [5] A.3.2.1

5.5.2 Alarm Reporting Procedure (by RPC method) (Mandatory)

When the alarms occur, the HNB report alarms to the TR-069 Manager according to the predefined alarm reporting mechanism.

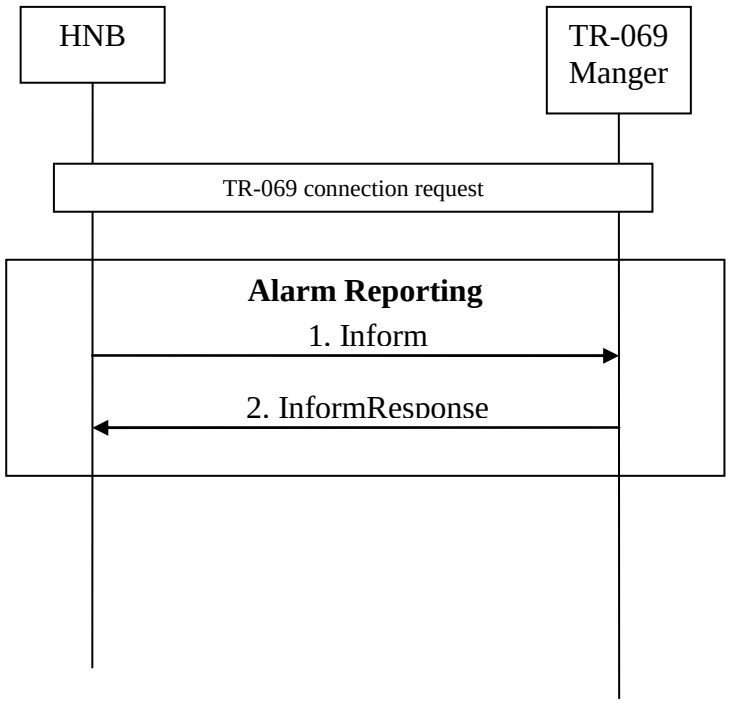

Figure 5.5.2-1: Alarm Reporting Procedure Flow

A TR-069 connection is requested to be established before the procedure.

1. HNB reports the alarm directly to TR-069 Manager by using Inform method when the raised alarm keeps in line with alarm reporting mechanism.

2. When TR-069 Manager receives the alarm, it responses to HNB with InformResponse.

The detail procedure of Inform refer to TR-069 Amendment 2 [5] A.3.3.1

For Inform method to report the HNB alarms, active notifications shall be reported to TR-069 Manager immediately, passive notifications shall be reported in the next session established with TR-069 Manager.

5.6 PM File Upload (Mandatory)

5.6.1 PM File Upload Period Set Procedure (Mandatory)

In the PM file upload procedure flow, TR-069 Manager uses SetParameterValues method to set the period a HNB for PM file uploading of HNB. The HNB then uploads PM file to the File Server periodically. When the periodic upload enable parameter is set to disabled, HNB shall not upload PM file any more.

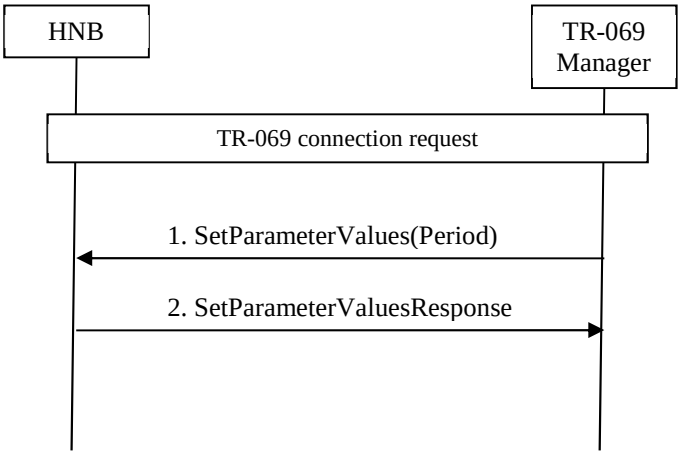

Figure 5.6.1-1: PM File Upload Period Set procedure flow

A TR-069 connection is requested to be established before the procedure.

1. TR-069 Manager initiates PM file upload period set procedure flow by using SetParameterValues to set the period of PM file uploading.
2. HNB responses to TR-069 Manager to confirm the setting by SetParameterValuesRessponse. If the response message returns an error code, then the procedure ends up with failure.

The detail procedure of SetParameterValues refer to TR-069 Amendment 2 [5] A.3.2.1

5.6.2 PM File Uploading Procedure (Mandatory)

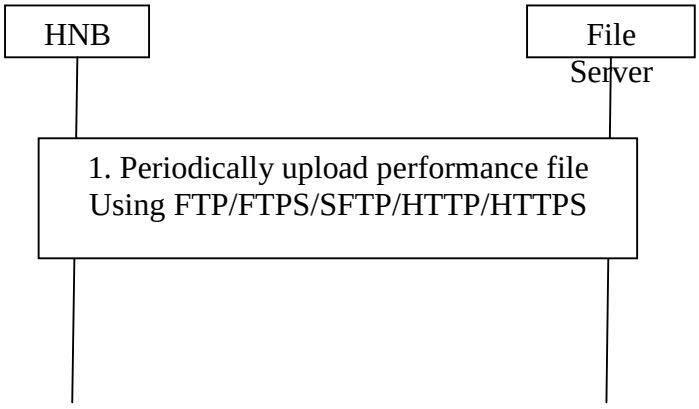

Figure 5.6.2-1: PM file uploading procedure flow

1. HNB uploads the PM file to File Server (by use of upload method) periodically according to period parameter. The upload method may be one selected from FTP/ FTPS/SFTP/HTTP/HTTPS. The location of File Server is determined by TR-069 Manager.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Mar 2009	SP-43	SP-090069	--	--	Presentation to SA for information and approval	1.0.0	8.0.0
Jun 2009	SP-44	SP-090295	001	--	Clarify the HNB Configuration Management (CM) procedure flow via file download	8.0.0	9.0.0
Sep 2009	SP-45	SP-090539	003	--	Precise the meaning of HNB CM procedure flow via file download	9.0.0	9.1.0
Dec-2009	SP-46	SP-090723	005	--	Correction of errors in clause number reference, figure number reference, and figure numbering	9.1.0	9.2.0
2011-03	-	-	-	-	Update to Rel-10 version (MCC)	9.2.0	10.0.0
2011-06	SP-52	SP-110288	006	2	Correction of procedure flows for HNB non-IPsec usage - alignment with 33.320	10.0.0	10.1.0
2011-09	SP-53	SP-110533	010	1	Align the HNB-GW discovery procedure with flow diagram	10.1.0	10.2.0
2011-09	SP-53	SP-110532	012	1	Add the root CA certificate pre-configuration to the discovery procedures	10.1.0	10.2.0
2012-09	-	-	-	-	Update to Rel-11 version (MCC)	10.2.0	**11.0.0**
2014-10	-	-	-	-	Update to Rel-12 version (MCC)	11.0.0	**12.0.0**
2016-01	-	-	-	-	Update to Rel-13 version (MCC)	12.0.0	**13.0.0**
2017-04	SA#75	-	-	-	Promotion to Release 14 without technical change	13.0.0	**14.0.0**
2018-06	-	-	-	-	Update to Rel-15 version (MCC)	14.0.0	**15.0.0**
2020-07	-	-	-	-	Update to Rel-16 version (MCC)	15.0.0	**16.0.0**
2022-04	-	-	-	-	Update to Rel-17 version (MCC)	16.0.0	**17.0.0**
2024-04	-	-	-	-	Update to Rel-18 version (MCC)	17.0.0	**18.0.0**

History

Document history		
V18.0.0	May 2024	Publication