ETSI TS 133 320 V9.0.0 (2010-02)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
LTE;
Security of Home Node B (HNB) / Home evolved Node B (HeNB)
(3GPP TS 33.320 version 9.0.0 Release 9)

Reference

DTS/TSGS-0333320v900

Keywords

LTE, SECURITY, 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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

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

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.

1 Scope

This document specifies the security architecture for the H(e)NB subsystem. This includes security requirements on Home Node Bs, Home eNode Bs, and other H(e)NB-associated network nodes (e.g. SeGW and H(e)MS), as well as the procedures and features which are provided to meet those requirements.

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 32.583: “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)”.

[3] IETF RFC 4187: “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”.

[4] IETF RFC 4306: “Internet Key Exchange (IKEv2) Protocol”.

[5] IETF RFC 4301: “Security Architecture for the Internet Protocol”.

[6] IETF RFC 4739: “Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2 Protocol”, Nov 2006.

[7] 3GPP TS 33.310: “Network Domain Security (NDS); Authentication Framework (AF)”.

[8] 3GPP TS 23.003: “Numbering, addressing and identification”.

[9] 3GPP TS 33.210: “3G security; Network Domain Security (NDS); IP network layer security”.

[10] 3GPP TS 33.234: “3G security; Wireless Local Area Network (WLAN) interworking security”.

[11] 3GPP TS 32.593: “Telecommunication management; Procedure flows for Type 1 interface H(e)NB to H(e)NB Management System (H(e)MS)”.

[12] GPP TS 25.467: “UTRAN architecture for 3G Home Node B (HNB); Stage 2”.

[13] 3GPP TS 24.008: “Mobile radio interface Layer 3 specification; Core network protocols; Stage 3”.

[14] 3GPP TS 24.301: “Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3”.

[15] The Broadband Forum TR-069: “CPE WAN Management Protocol v1.1”, Issue 1 Amendment 2, December 2007.

[16] IETF RFC 4346: “The Transport Layer Security (TLS) Protocol Version 1.1”.

[17] IETF RFC 5246: “The Transport Layer Security (TLS) Protocol Version 1.2”.

[18] ETSI ES 282 004 (V1.1.1): Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN functional architecture; Network Attachment Sub-System (NASS), 2006.

[19] ETSI ES 283 035 (V1.1.1): "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol",,2006.

[20] 3GPP TS 33.102: “3G security; Security architecture”

[21] 3GPP TS 33.401: “3GPP System Architecture Evolution (SAE): Security architecture”

[22] IETF RFC 2560: “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”

[23] Open Mobile Alliance OMA-WAP-OCSP V1.0: "Online Certificate Status Protocol Mobile Profile". URL: http://www.openmobilealliance.org/

[24] IETF RFC 4806: “Online Certificate Status Protocol (OCSP) Extensions to IKEv2”

[25] IETF RFC 4366: “Transport Layer Security (TLS) Extensions”

[26] IETF RFC 5280:” Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”

3 Definitions and abbreviations

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].

CSG:A closed subscriber group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN of but having restricted access (“CSG cells”)

Hosting party: the party hosting the H(e)NB and having a contract with the PLMN operator.

Security Gateway: Element at the edge of the core network terminating security association(s) for the backhaul link between H(e)NB and core network.

3.2 Abbreviations

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

AAA	Authentication, Authorization, and Accounting
ACS	Auto-Configuration Server
AKA	Authentication and Key Agreement
ASME	Access Security Management Entity
CA	Certification Authority
CPE	Customer Premises Equipment
CSG	Closed Subscriber Group
DHCP	Dynamic Host Configure Protocol
DPD	Dead Peer Detection
eNB	Evolved Node-B
EAP	Extensible Authentication Protocol
EPS	Evolved Packet System
ESP	Encapsulating Security Payload

E-UTRAN	Evolved UTRAN
FQDN	Fully Qualified Domain Name
GNSS	Global Navigation Satellite System
H(e)NB	Home NodeB or Home eNodeB
H(e)NB-GW	Home (e)NodeB Gateway
H(e)MS	Home NodeB Management or Home eNodeB Management System
HeMS	Home eNodeB Management System
HeNB	Home eNodeB
HMS	Home NodeB Management System
HNB	Home NodeB
HP	Hosting Party
HPM	HP Module
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
LTE	Long Term Evolution
MME	Mobility Management Entity
MSK	Master Session Key
NAI	Network Access Identifier
NAS	Non-Access Stratum
NAT	Network Address Translation
PKI	Public Key Infrastructure
SA	Security Association
SeGW	Security Gateway
TLS	Transport Layer Security
TrE	Trusted Environment
UICC	Universal Integrated Circuit Card
UP	User plane
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
UMTS	Universal Mobile Telecommunications System
UTRAN	Universal Terrestrial Radio Access Network

4 Overview of Security Architecture and Requirements

4.1 System architecture of H(e)NB

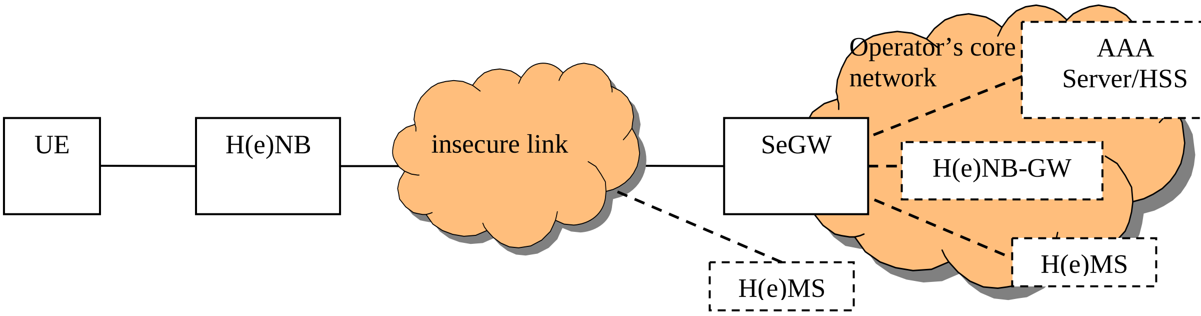

Figure 4.1.1: System Architecture of H(e)NB

Description system architecture:

- Air interface between UE and H(e)NB should be backwards compatible air interface in UTRAN or E-UTRAN;
- H(e)NB access operator’s core network via a Security Gateway. The backhaul between H(e)NB and SeGW may be insecure.
- Security Gateway represent operator’s core network to perform mutual authentication with H(e)NB.

- AAA server authenticates the hosting party based on the authentication information retrieved from HSS when hosting party authentication is performed.

- Security tunnel is established between H(e)NB and Security Gateway to protect information transmitted in backhaul link. IPsec use for this security tunnel is mandatory to implement but optional to use based on an operator policy. If the operator chooses not to use IPsec, the interface between the H(e)NB and SeGW shall be secured with a mechanism that provides layer 2 security for confidentiality and integrity protection of communications. This mechanism then shall also bind this secure communications to device authentication and optional HPM authentication.

Editor's Note: The consistency of the above statement with the rest of the present document needs to be checked further carefully. According to IETF RFCs, IKEv2 and IPsec ESP must always be used jointly. However, there is a draft in IETF in the early stage on separating IKE and IPSec.

NOTE: The details of this layer 2 security mechanism and the binding are out of scope of this standard.

- HNB-GW performs the mandatory access control and HNB performs the optional access control in case non-CSG capable UEs or non-CSG capable HNBs. SeGW and HNB-GW are logically separate entities within operator’s network. If the SeGW and the HNB-GW are not integrated, then the interface between the HNB-GW and the SeGW may be protected using NDS/IP [9].

- HeNB-GW is optional to deploy. If HeNB-GW is deployed, then SeGW may be integrated into HeNB GW. If the SeGW and the HeNB-GW are not integrated, then the interface between the HeNB-GW and the SeGW may be protected using NDS/IP [9].

- H(e)MS, H(e)NB-GW, or MME performs location verification of H(e)NB [12].

- Secure communication is required to H(e)NB Management System (H(e)MS).

4.2 Network Elements

4.2.1 H(e)NB

The H(e)NB is a network element that connects User Equipment via its radio interface to the operator’s core network. The backhaul link to the operator’s core network is a broadband connection. A H(e)NB is typically deployed in customers’ premises.

NOTE: The term H(e)NB refers to both Home NodeB (HNB) and Home eNodeB (HeNB), when both are meant without distinction.

4.2.2 Security Gateway (SeGW)

The SeGW is a network element at the border of the operator’s core network. After successful mutual authentication between the H(e)NB and the SeGW, the SeGW connects the H(e)NB to the operator’s core network. Any connection between the H(e)NB and the core network is tunnelled through the SeGW.

4.2.3 H(e)NB Management System (H(e)MS)

The H(e)MS is a management server that configures the H(e)NB according to the operator’s policy. H(e)MS is also capable of installing software updates on the H(e)NB. The H(e)MS server may be located inside the operator’s core network (accessible on the MNO Intranet) or outside of it (accessible on the public Internet).

The HMS is specified in TS 32.583 [2].

The HeMS is specified in TS 32.593 [11].

4.2.4 UE

UE is a standard user equipment for UMTS (for HNB) or LTE (for HeNB).

4.2.5 H(e)NB Gateway (H(e)NB-GW) and MME

H(e)NB-GW serves as a concentrator for control plane traffic to/from multiple H(e)NBs. The H(e)NB-GW and the SeGW may be co-located. The HeNB-GW is optional, while the HNB-GW is mandatory. In the absence of a HeNB-GW, the HeNB is directly connected to the MME via the SeGW.

4.2.6 AAA Server and HSS

HSS stores the subscription data and authentication information of the H(e)NBs. When hosting party authentication is required, AAA server authenticates the hosting party based on the authentication information retrieved from HSS.

4.2.7 SGSN/MSC/VLR

4.3 Interfaces (Reference Points)

Editor's Note: Are we going to specify new interface designators, or are we describing the interfaces with the designators as used for the functions e.g. carried inside a secure tunnel?

4.3.1 Backhaul Link

The backhaul link used between H(e)NB and SeGW provides a secure tunnel carrying both the user plane data and the control plane data that are transmitted between the H(e)NB and network elements in the core network.

H(e)MS traffic is also tunnelled through this secure backhaul link, if the H(e)MS is accessible on the MNO Intranet.

The backhaul link may also carry other data between H(e)NB and core network, e.g. time protocol traffic.

4.3.2 H(e)MS Interface

The H(e)MS Interface between the H(e)NB and the H(e)MS server shall provide a secure connection carrying configuration data., SW updates and additional data, e.g. location information.

4.3.3 Interface between SeGW and AAA Server, AAA Server and HSS

The interface between the SeGW and AAA Server provides a secure connection carrying authentication, authorization, and related information.

The interface between AAA Server and HSS provides a secure connection for the retrieval of authentication vectors (e.g. for hosting party authentication) and retrieval of H(e)NB access-related information for HPM.

4.4 Security Requirements and Principles

4.4.1 Operation

The requirements on operation are:

- Only algorithms of adequate cryptographic strength shall be used for authentication and protection of confidentiality and integrity.
- Modifications of Hosting Party controlled information by the operator shall only be allowed with the permission of the Hosting Party.
- The extent of Hosting Party controllable information shall be controlled by the operator.
- IMSIs of users connected to H(e)NB shall not be revealed to the Hosting Party of the H(e)NB.

4.4.2 Requirements on H(e)NB

The requirements on the H(e)NB are:

- The integrity of the H(e)NB shall be validated before any connection into the core network is established.
- The H(e)NB shall be authenticated by the SeGW based on a globally unique and permanent H(e)NB identity.
- The H(e)NB shall authenticate the SeGW.
- Optionally the hosting party of the H(e)NB may be authenticated.
- If hosting party authentication is used, the H(e)NB shall shut down its air interface and disconnect from the operator's core network on removal of the HPM which was used for authentication towards the MNO.
- The H(e)NB shall authenticate the H(e)MS, if the H(e)MS is accessed on the public Internet.
- The H(e)NB shall be authenticated by the H(e)MS using the same identity as for authentication to the SeGW, if the H(e)MS is accessed on the public Internet.
- The configuration and the software of the H(e)NB shall only be updated in a secure way, i.e. the integrity of the configuration data including the licensed radio parameters and the integrity of the software updates must be verified.
- Sensitive data including cryptographic keys, authentication credentials, user information, user plane data and control plane data shall not be accessible at the H(e)NB in plaintext to unauthorized access.
- The time base of the H(e)NB shall be synchronized to the core network.
- The location of the H(e)NB shall be reliably transferred to the network.
- The H(e)NB shall be capable of filtering unauthenticated traffic received from the access network. Operator policy shall control which types of unauthenticated traffic are filtered.
- All security requirements of the eNB secure environment of TS 33.401 [21] clause 5.3 shall apply to the HeNB.

  Security measures to establish this secure environment shall be assured by the TrE (subclause 5.1.2) where they fall under the capability of the TrE.

4.4.3 Requirements on SeGW

The requirements on the SeGW are:

- The SeGW shall be authenticated by the H(e)NB using a SeGW certificate. The SeGW certificate shall be signed by a CA trusted by the operator.
- The SeGW shall authenticate the H(e)NB based on H(e)NB certificate.
- The SeGW may authenticate the hosting party of the H(e)NB in cooperation with the AAA server using EAP-AKA [3].
- The SeGW shall allow the H(e)NB access to the core network only after successful completion of all required authentications.
- Any unauthenticated traffic from the H(e)NB shall be filtered out at the SeGW.

4.4.4 Requirements on H(e)MS

The requirements on the H(e)MS are:

- The H(e)MS shall be authenticated by the H(e)NB if the H(e)MS is accessible on the public Internet and may be authenticated by H(e)NB if the H(e)MS is accessible on the MNO Intranet using a H(e)MS certificate. The H(e)MS certificate shall be provided by a MNO trusted CA.

- The H(e)MS shall authenticate the identity of the H(e)NB if the H(e)MS is accessible on the public Internet and may authenticate the identity of the H(e)NB if the H(e)MS is accessible on the MNO Intranet, using a H(e)NB certificate. This identity shall be the same as used during backhaul link establishment (cf. sub-clause 4.4.5 of this document).
- If the H(e)MS is accessible on the MNO Intranet and the mutual authentication between H(e)MS and H(e)NB is not performed the identity of H(e)NB has to be transferred over the H(e)MS link.

NOTE 1: In case of H(e)MS accessible on the MNO intranet there may be an additional secure end-to-end tunnel between H(e)NB and H(e)MS carried inside the secure backhaul link.

NOTE 2: Mutual authentication between H(e)MS and H(e)NB may not be necessary due to mutual authentication between H(e)NB and SeGW.

4.4.5 Requirements on Backhaul Link

The requirements on the backhaul link are:

- The establishment of the secure backhaul link shall be based on IKEv2 [4] comprising the required authentications as given in subclauses 4.4.2 and 4.4.3 of this document.
- The backhaul link shall provide integrity protection of the transmitted data. It may provide confidentiality protection of the transmitted data, depending on operator option.
- The security solution for the backhaul link shall be based on IPsec ESP tunnel mode [9].
- Any connection between the H(e)NB and the core network shall be tunnelled through the Backhaul Link.
- The security solution for the backhaul link shall be compatible with common network address and port translation variations and support firewall traversal.

4.4.6 Requirements on H(e)MS Link

The requirements on the H(e)MS link are:

- The establishment of the secure H(e)MS link shall be based on the authentication principles as given in subclauses 4.4.2 and 4.4.4 of this document.
- The H(e)MS link shall provide integrity protection of the transmitted data. It may provide confidentiality protection of the transmitted data, depending on operator option.

5 Security Features

5.1 Secure Storage and Execution

5.1.1 Hosting Party Module

The Hosting Party authentication shall be based on a Hosting Party Module. The Hosting Party Module (HPM) is a physical entity distinct from the H(e)NB physical equipment, dedicated to the identification and authentication of the Hosting Party towards the MNO. The HPM shall have the following features:

- The HPM shall be a tamper resistant environment and shall contain the credentials used to authenticate the Hosting Party.
- The HPM shall be bound to the Hosting Party (e.g. by contractual agreement between Hosting Party and MNO) and supplied by the MNO to the Hosting Party.
- The HPM shall be removable from the H(e)NB and it shall be possible for a Hosting Party to change the H(e)NB device by inserting the HPM in the new H(e)NB.

The HPM is provided by means of a UICC.

5.1.2 Trusted Environment (TrE)

5.1.2.1 General

The Trusted Environment (TrE) shall be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data.

All data produced through execution of functions within the TrE shall be unknowable to unauthorized external entities.

The TrE shall be built from an irremovable, HW-based root of trust by way of a secure boot process, which shall occur whenever a H(e)NB is turned on or goes through a hard reset. The root of trust shall be physically bound to the H(e)NB. The secure boot process shall include checks of the integrity of the TrE performed by the root of trust. Only successfully verified components shall be loaded or started. The TrE , after having been successfully started, shall proceed to verify other components of the H(e)NB (e.g. operating system and further programs) that are necessary for trusted operation of the H(e)NB.

The TrE shall perform sensitive functions (such as storing private keys and providing cryptographic calculations using those private keys) needed to perform H(e)NB device integrity check (cf. clause 6.1) and device validation as specifically described in clauses 7.1 and 8.3.2.2.

The TrE shall perform sensitive functions (such as storing private keys and providing cryptographic calculations using those private keys) needed for H(e)NB device authentication with the operator network, as specifically described in clauses 7.2 and 8.3.

5.2 Device Mutual Authentication

The device mutual authentication is mandatory for H(e)NB.

Device mutual authentication shall be performed using a H(e)NB certificate. The credentials and critical security functions for device authentication shall be protected inside a TrE.

The device mutual authentication shall be securely bound to device integrity validation. This procedure, when successful, leads to mutual authentication between the H(e)NB and the SeGW.

The certificate-based device authentication shall have the following parts:

- The H(e)NB shall be provisioned with a device certificate. This device certificate allows the authentication of the H(e)NB by the SeGW (and thus the operator network). The device certificate shall be provided by the operator, manufacturer, vendor of the H(e)NB, or by another party trusted by the operator.
- A globally unique, Fully Qualified Domain Name (FQDN) formatted identifier shall be used for certificate based device authentication.
- The H(e)NB may check the revocation status of certificates using OCSP.
- The SeGW may check the revocation status of certificates using CRLs or OCSP.

5.3 Hosting Party Mutual Authentication

The hosting party mutual authentication is optionally performed by the operator’s network following successful device mutual authentication.

An EAP-AKA based method [3] shall be used for hosting party authentication. When Hosting Party Authentication is used, both device and hosting party authentication must be completed successfully before a secure tunnel to the operator network can be established.

The authentication of the hosting party is based on credentials contained in a separate Hosting Party Module (HPM) in H(e)NB, and in the MNO HLR/HSS.

The EAP-AKA based hosting party authentication shall have the following parts:

- An AKA credential shall be stored in HPM enabling to use EAP-AKA. The SeGW is acting as EAP authenticator and forwards the EAP protocol messages to the AAA server to retrieve an authentication vector from AuC via HSS/HLR.
- A globally unique identifier in the format of an IMSI shall be used for EAP-AKA based authentication. These IMSIs shall be marked in HLR/HSS as used for H(e)NBs, e.g. by allocating dedicated ranges or by adding specific attributes to avoid misuse of these IMSIs for ordinary UEs.

NOTE: The implementation of the related HLR/HSS entry is out of scope of this document.

5.4 Other security features

The communication between time server and H(e)NB shall be provided with adequate protection.

Access control shall be performed in the HNB-GW and optionally in HNB in case of non-CSG capable UEs or non-CSG capable HNBs.

In case of CSG capable UEs and CSG capable H(e)NBs, the SGSN/MSC/VLR shall perform access control for UE for accessing HNB and the MME shall perform access control for HeNB.as described in [13] and [14]

The H(e)MS, H(e)NB-GW or MME shall perform H(e)NB location verification,

NOTE: Location verification is needed to satisfy various security, regulatory and operational requirements of operators.

6 Security Procedures in H(e)NB

6.1 Device Integrity Check

6.1.1 Device Integrity Check Procedure

The H(e)NB and TrE shall perform a device integrity check upon booting and before connecting to the core network and/or to the H(e)MS. The device integrity check shall be based on one or more trusted reference value(s) and the TrE. The following requirements shall apply:

- The TrE shall boot securely according to section 5.1.2.1.
- The integrity of a component is verified by comparing the result of a measurement (typically a cryptographic hash) of the component to the trusted reference value. If these values agree, the component is successfully verified and can be started.
- For each of the component integrity checks, the TrE shall retrieve the corresponding trusted reference value from secure memory.
- The TrE shall check the integrity of all components necessary for trusted operation of the device. Any individual component shall be started only if its integrity check is successful.
- The integrity of the device is verified if all components necessary for trusted operation of the device are verified.

6.1.2 Protection of Trusted Reference Value(s)

- The TrE shall securely store all trusted reference values at all times.
- The TrE shall detect un-authorized modifications of the trusted reference values necessary for trusted operation of the device.

6.2 Binding of HPM ID and Device ID

6.3 Measures for Clock Protection

6.3.1 Clock Synchronization Security Mechanisms for H(e)NB

The H(e)NB requires time synchronization with a time server. The H(e)NB shall support receiving time synchronisation messages over the secure backhaul link between H(e)NB and the SeGW.

Optionally other secure clock servers may be used, which do not use the secure backhaul link. In this case the communication between these clock server(s) and H(e)NB shall be secured.

NOTE 1: How to secure communication between clock servers and H(e)NB outside the secure backhaul link is out of scope of the present document.

The availability of the correct current time is important for certificate validation and thus for the establishment of secure links (IKEv2 and/or TLS). This results in the following requirements:

- The H(e)NB shall be equipped with a clock.
- Upon the H(e)NB connecting to the CN, the clock shall be synchronized with the secured time server.
- During normal operation of the H(e)NB, the clock shall be re-synchronized with the secured time signal from the network at least every 48 hours.

The following requirements on local time arise from certificate handling, applying to operation of the H(e)NB before the secure backhaul link or the secure H(e)MS connection is established and thus before secured clock information is available from the clock server:

- The last time at which the H(e)NB was active before the current power-up shall be recorded and saved in the TrE.
- Upon restoration of power of the H(e)NB, the clock shall resume counting from the last saved time. If a continuously running clock exists, the clock may resume counting from the later of the current time of the clock and the last saved time

NOTE 2: Usage of the current time of the clock upon restoration of power of the H(e)NB assumes that the clock starts at its own power-up at some point in time which does not lie in the future. The start time could be at a fixed date, e.g. the epoch 1970-01-01. Otherwise the H(e)NB may falsely interpret a certificate as expired, if the start time of the clock lies after expiry time of the certificates.

NOTE 3: If a HeNB clock erroneously received a time lying sufficiently far in the future, the validation of the SeGW's or the H(e)MS's certificate will fail and the H(e)NB will be unable to connect to the operator's network. No specific solution to this scenario is given; a common solution for problems with the H(e)NB authentication might be considered in the future.

7 Security Procedures between H(e)NB and SeGW

7.1 Device Validation

The H(e)NB shall support a device validation method where the device implicitly indicates its validity to the SeGW or H(e)MS by successful execution of device authentication. To achieve this, the following requirement applies:

- If the device integrity check according to clause 6.1 failed, the TrE shall not give access to the sensitive functions using the private key needed for H(e)NB device authentication with the SeGW.

7.2 Device Authentication

7.2.1 General

Device authentication of the H(e)NB shall be securely bound by the TrE to the device validation of the H(e)NB platform.

Device authentication of H(e)NB shall be based on device certificate for H(e)NB and network certificate for the core.

IKEv2 with certificates used for authentication shall be run between H(e)NB and SeGW to mutually authenticate the H(e)NB and the SeGW.

7.2.2 SeGW and Device Mutual Authentication Procedure

Device authentication shall be performed using IKEv2 with public key signature based authentication with certificates, as specified in RFC 4306 [4]. The H(e)NB device shall authenticate itself to the SeGW with a certificate based on the globally unique and permanent H(e)NB identity, signed by an operator authorized entity. The SeGW shall authenticate itself to the H(e)NB using a certificate signed by an operator trusted CA. The H(e)NB shall verify the SeGW identity by checking the subjectAltName field of the SeGW certificate against the name of the SeGW used by the H(e)NB to connect to the SeGW.

NOTE 1: If DNS is available, the SeGW's name is the FQDN used to resolve its IP address; otherwise it is the IP address of the SeGW.

The H(e)NB may check the revocation status of the SeGW certificate using OCSP as specified in [22] and [23]. Support for OCSP is optional for the operator network. The H(e)NB should support OCSP.

NOTE 2: It is strongly recommended to support OCSP in the H(e)NB, as this feature may become mandatory for H(e)NB in future releases.

The OCSP communication between H(e)NB and OCSP server may use the in-band signaling of certificate revocation status in IKEv2 according to RFC 4806 [24], through which the SeGW can include an OCSP response within IKEv2. Support for this extension to IKEv2 in H(e)NB and SeGW is optional.

The SeGW may check the revocation status of the H(e)NB certificate using CRLs according to TS 33.310 [7] or OCSP as specified in [22] and [23].

The SeGW shall implement support for either CRL checking or OCSP or both. The locations of the CRL Server and OCSP Responder may be in the operator's network or provided by the manufacturer/vendor. Neither the operator nor the manufacturer is required to provide a CRL Server or an OCSP Responder. For the case when the operator provides a CRL Server or OCSP Responder, the manufacturer shall forward revocation data to the operator. The interface to forward revocation data is out of scope of the present document.

If the H(e)NB certificate contains CRL or OCSP server information (cf. sub-clause 7.2.5.2), then the SeGW may contact this server for revocation information.

NOTE 3: A CRL or OCSP server located at manufacturer of H(e)NB allows distribution of revocation information by the manufacturer directly. To use such revocation information, normally the SeGW needs a CRL or OCSP client capable to reach the public Internet to contact these servers.

Validity check of H(e)NB certificates in SeGW shall be configurable by the operator, i.e. whether to use CRLs, OCSP or both and whether to use operator CRL or OCSP server, manufacturer CRL or OCSP server, or more than one of them.

The H(e)NB’s TrE shall be used to provide the following critical security functions supporting the IKEv2 and certificate processes:.

- The H(e)NB’s identity shall be stored in the TrE and shall not be modifiable.
- The H(e)NB’s private key shall be stored in the TrE and shall not be exposed outside of the TrE.
- The root certificate used to verify the signatures on the SeGW certificate shall be stored in the H(e)NB’s TrE and shall be writable by authorized access only. The verification process for signatures shall be performed by the H(e)NB’s TrE.
- The H(e)NB’s TrE shall be used to compute the AUTH payload used during the IKE_AUTH request message exchanges.

NOTE 4: Autonomous validation is performed during secure start-up and performs validation of the H(e)NB. As IKEv2 allows the inclusion of information data into Notify Payload, information regarding the trustworthy state of the H(e)NB may be carried in the Notify Payload (see Annex A.1) during IKEv2 procedures from the H(e)NB to the SeGW.Notify Payload within IKEv2's IKE_AUTH message is protected by IKEv2 SK and AUTH. In addition, the Notify Payload, as constructed by the TrE, should include a nonce and should be cryptographically signed by the TrE.

Editor’s Note: Replay protection within the Notify Payload is FFS.

7.2.3 H(e)NB/IKEv2 Processing Requirements for SeGW Certificates

The H(e)NB/IKEv2 processing requirements for SeGW certificates shall be as follows:

1. The SeGW shall not send certificate paths containing more than four certificates.
2. The H(e)NB shall be able to process SeGW certificate paths containing up to four certificates. The SeGW certificate and the intermediate CA certificates for the SeGW shall be obtained from the IKEv2 CERT payload. The certificates of the trusted root CA shall be obtained from the TrE of the H(e)NB.
3. The H(e)NB shall check the validity time of the SeGW certificates, and reject certificates that are either not yet valid or that are expired.

4. In case the H(e)NB is configured to check the certificate revocation status of the SeGW certificate, and it receives no valid OCSP response, the H(e)NB shall abort the IKEv2 protocol.

NOTE 1: The execution of this check does not depend on the existence of an OCSP server information in the SeGW certificate, if OCSP extension according to RFC 4806 [24] is used.

NOTE 2: A H(e)NB may want to check the revocation status of the SeGW certificate, but it may not have access to the OCSP server until the IPSec tunnel is established. In this case, after the tunnel is successfully established and before user data is transmitted in the tunnel, the H(e)NB sends an OCSP request message to the OCSP responder. When the H(e)NB receives the OCSP response, it checks the certificate status. If the certificate of SeGW is valid, the H(e)NB will allow user data to be transmitted to the SeGW in the tunnel. If the certificate is not valid, the H(e)NB may terminate the tunnel that just was established.

7.2.4 SeGW/IKEv2 Processing Requirements for H(e)NB Certificates

The SeGW/IKEv2 processing requirements for H(e)NB certificates shall be as follows:

1. The H(e)NB shall not send certificate paths containing more than four certificates.

2. The SeGW shall be able to process H(e)NB certificate paths containing up to four certificates. The H(e)NB certificate and the intermediate CA certificates for the H(e)NB shall be obtained from the IKEv2 CERT payload. The trusted root CA shall be obtained from a SeGW local store of trusted CA certificates.

3. The SeGW shall check the validity time of the H(e)NB certificates, and reject certificates that are either not yet valid or that are expired.

4. The SeGW shall check the certificate revocation status if configured by local policy.

NOTE: The mere existence of a CRL or OCSP server information in the H(e)NB certificate does not mandate the SeGW to perform certificate status checking.

7.2.5 Security Profiles

7.2.5.1 Profile for IKEv2

The H(e)NB and the SeGW shall conform to the profile of IKEv2 as specified in clause 5.4.2 of TS 33.210 [9] with the exception that the use of pre-shared secrets for authentication is not supported.

The following additional requirements on certificate based IKEv2 authentication for the IKE_INIT_SA and IKE_AUTH exchanges shall be applied:

- The use of RSA signatures for authentication shall be supported.

- The H(e)NB shall include its identity in the IDi payload of the first IKE_AUTH request.

- The H(e)NB identity in the IDi payload may be used for policy checks.

- Initiating/responding end entities are required to send certificate requests in the IKE_INIT_SA exchange for the responder and in the IKE_AUTH exchange for the initiator.

- The messages for the IKE_AUTH exchanges shall include a certificate or certificate chain providing evidence that the key used to compute a digital signature belongs to the identity in the ID payload.

- The certificates in the certificate payload shall be encoded as type 4 (X.509 Certificate – Signature).

7.2.5.2 IKEv2 Certificate Profile

7.2.5.2.1 IKEv2 Entity Certificates

The H(e)NB and SeGW certificates shall both conform to the requirements set out in clauses 6.1.1 and 6.1.3 of TS 33.310 [7] with the following additions and exceptions:

- The H(e)NB certificate shall be signed by an entity that is authorized by the operator, e.g. the manufacturer or the vendor.
- The H(e)NB certificate shall carry the H(e)NB identity in FQDN format in the subjectAltName. This identity shall be the same as the identity in the IDi payload of the first IKE_AUTH request.
- If the manufacturer or vendor provides a CRL or OCSP server, the H(e)NB certificate shall carry the CRL distribution point as specified in TS 33.310 [7] or the OCSP server information (AIA extension) as specified in RFC5280 [26] and RFC 2560 [22].

NOTE: Server information for CRL and/or OCSP servers deployed in operator network may be configured in SeGW.

- If the operator provides an OCSP server, the SeGW certificate shall carry the OCSP server information as specified in RFC 2560 [22]. This OCSP server information is not mandatory, if OCSP extension according to RFC 4806 [24] is used.

Editor's Note: The H(e)NB identity should be specified by CT4 as "HNB unique identity" in a new sub-clause of clause 4 in TS 23.003 [8]. Once this is done, this editor's note should be replaced by a reference to this new sub-clause.

7.2.5.2.2 IKEv2 CA Certificates

IKEv2 CA certificates shall conform to the requirements set out for NE CA certificates in clauses 6.1.1, and 6.1.4b of TS 33.310 [7].

NOTE: This requirement implies that there is no restriction in the issuer name for both H(e)NB CA certificates and SeGW CA certificates.

7.3 Hosting Party Authentication

Device Authentication may optionally be followed with an EAP-AKA-based hosting party authentication exchange. The IKEv2 certificate-based mutual authentication is executed according to IETF RFC 4306 [4] as specified in 7.2, extended by IKEv2's multiple authentication procedure defined in IETF RFC 4739 [6].

The IKEv2 EAP-AKA authentication will follow the TS 33.234 [10] specification.

The H(e)NB's HPM must be used to provide critical security functions supporting the EAP-AKA authentication processes.

- The secret key (K) used for HP authentication shall be stored in the HPM.
- The HPM is responsible for computing the RES and AUTN parameters for the EAP-AKA based hosting party authentication.

7.4 IPsec Tunnel Establishment

The H(e)NB shall use IKEv2 protocol to set up at least one IPsec tunnel to protect the traffic with SeGW, i.e. a pair of unidirectional SAs between H(e)NB and SeGW. All signalling, user, and management plane traffic over the interface between H(e)NB and SeGW shall be sent through an IPsec ESP tunnel (with NAT-T UDP encapsulation as necessary) that is established as a result of the authentication procedure.

The H(e)NB shall initiate the creation of the SA i.e. it shall act as initiator in the Traffic Selector negotiation. Upon H(e)NB's request, the SeGW should allocate IP address to the H(e)NB after successful authentication.

The H(e)NB and SeGW shall use the IKEv2 mechanisms for detection of NAT, UDP encapsulation for NAT Traversal, H(e)NB initiated NAT keep-alive, IKEv2 SA and IPsec SA rekeying, and Dead Peer Detection (DPD).

During setup of the tunnel, the H(e)NB shall include a list of supported ESP authentication transforms and ESP encryption transforms as part of the IKEv2 signalling. The SeGW shall select an ESP authentication transform and an ESP encryption transform conforming to clause 5.3 of TS 33.210 [9], and shall signal this to the H(e)NB.

7.5 Device Authorization

Optionally an AAA server may be used to verify the authorization of the H(e)NB to connect to the operator's network based on the authenticated device identity extracted from the H(e)NB certificate. This authorization check is separate from and in addition to the revocation status check via OCSP or CRL.

NOTE: If OCSP is used, the result of the authorization check may be included in the certificate revocation check described in section 7.2.2 by having the OCSP responder provide a certificate status of "good" as in RFC 2560 [22] only when the certificate has not been revoked and the device is authorized to connect to the operator's network. If either of these conditions is false, the OCSP responder should provide a certificate status of "revoked".

8 Security Aspects of H(e)NB Management

8.1 Location Verification

8.1.1 General

Operators require assurance of the H(e)NB location to satisfy various security, regulatory and operational requirements. The H(e)MS and/or H(e)NB-GW/MME (referred to in this section as the "verifying node") shall perform location verification. It shall be possible for the verifying node to obtain one or more of the following information which may be used to perform location verification:

- the public IP address of the broadband access device provided by the H(e)NB
- the IP address and/or access line location identifier provided by broadband access provider
- information of macro-cells surrounding the H(e)NB provided by the H(e)NB
- geo-coordinates provided by a GNSS receiver embedded into the H(e)NB

Different deployment scenarios and H(e)NB configurations will influence the availability, accuracy and reliability of these types of location information.

8.1.2 IP Address provided by H(e)NB

A H(e)NB is normally connected to the IP network via some access device (e.g. DSL modem, cable modem, home router, etc.). If the H(e)NB is capable of acquiring the public IP address of the access device, it shall be able to provide this IP address to the verifying node.

8.1.3 IP Address and/or access line location identifier provided by broadband access provider

A H(e)NB is normally connected to the IP network via some access device (e.g. DSL modem, cable modem, home router, etc.) This device will have an IP address and/or access line location assigned by the broadband access provider. The broadband access provider may, subject to regulatory approval, be able to provide the verifying node with this information based on the solution in [18] and [19]. An example information flow of location verification based on access line identifier is provided in Annex B.

NOTE: The verifying node must receive the IP address as used in the NASS. This may require either that the verifying node be located directly at the edge of the NASS, or that the NASS uses public IP addresses without NAT or NAPT to Internet.

8.1.4 Surrounding macro-cell information provided by H(e)NB

If the H(e)NB has the capability to receive transmissions from surrounding macro-cells, it shall be capable of providing information on the identity of any such macro-cells to the verifying node.

NOTE: A report that no macro-cells can be detected may be of use in determining that the H(e)NB has been moved to an unauthorized location.

8.1.5 GNSS information provided by H(e)NB

If the H(e)NB has the capability to receive GNSS transmissions, it shall be capable of sending GNSS determined location information to the verifying node. To be able to determine H(e)NB location based on an internal GNSS, a H(e)NB must be equipped with a GNSS receiver and be installed in a location where GNSS satellites can be acquired.

8.1.6 Requirements

The verifying node shall be capable of requesting one or more of the types of location information listed in section 8.1.1.

It shall be possible to configure how often the verifying node requests location information, and what information types are requested.

It shall be possible to configure policies to control how the verifying node evaluates the received location information in order to perform location verification.

NOTE: The details of these policies are out of scope of this specification.

The verifying node may perform location verification using information provided by the H(e)NB. This information may be provided automatically and/or upon request.

It shall be possible for the verifying node to use ancillary information to perform location verification such as geo-coordinates of surrounding macrocells, postal address of H(e)NB as claimed by H(e)NB hosting party, IP address location information, etc.

It shall be possible for the verifying node to perform location verification both before and after switching on the H(e)NB radio.

Depending on the result of location verification, the verifying node shall take one or more of the following actions: raise an alarm, permit the H(e)NB to radiate or prevent the H(e)NB from radiating.

According to operator policy, an operating H(e)NB which is ordered to cease radiating may do so immediately, or it may wait until any calls in progress have been completed before it complies with the order and ceases radiating. It shall not allow new calls to be established during this waiting period.

8.2 Access Control Mechanisms for H(e)NB

8.2.1 Non-CSG Method

The ACL (Access Control List) based access control mechanism for a non CSG capable UE accessing the HNB is handled in [12]. The ACL shall be securely stored in and integrity protected in the HNB if the HNB performs access control.

8.2.2 CSG Method

The CSG based access control mechanism for a CSG capable UE accessing the H(e)NB is handled in [12],[13] and [14].

Editor’s Note: This may need to be coordinated with work being done in SA2 and/or RAN3.

8.3 Protection of H(e)MS traffic between HMS and H(e)NB

8.3.1 Connection to H(e)MS accessible on MNO Intranet

In case that the H(e)MS is accessible on MNO Intranet, H(e)MS traffic shall be protected through the support of one of the two security mechanisms determined by the Network Operator’s Security Policies:

- H(e)MS traffic is protected in hop-by-hop way. H(e)MS traffic is protected by IPsec tunnel between H(e)NB and SeGW. Network security mechanisms (cf. clause 7 of this document) shall be used to protect H(e)MS traffic between SeGW and H(e)MS when the path from SeGW to H(e)MS is considered as insecure.
- H(e)MS traffic is protected by the IPsec Tunnel between H(e)NB and SeGW. And TLS tunnel also shall be utilized within the IPsec Tunnel for additional end-to-end security.

When TLS is performed between H(e)NB and H(e)MS, mutual authentication between H(e)NB and H(e)MS shall be based on device certificate for the H(e)NB and network certificate for the H(e)MS. H(e)NB and H(e)MS may check the validity of the certificates as given in sub-clause 8.3.2.1 .

8.3.2 Connection to H(e)MS accessible on public Internet

8.3.2.1 General

In case that the H(e)MS is accessible on the public Internet, the H(e)MS is exposed to attackers located in insecure network. H(e)MS traffic shall be protected by TLS tunnel established between H(e)NB and H(e)MS. In this case, mutual authentication between H(e)NB and H(e)MS shall be based on device certificate for the H(e)NB and network certificate for the H(e)MS. The H(e)NB shall verify the H(e)MS identity by checking the subjectAltName field of the H(e)MS certificate against the name of the H(e)MS.

NOTE 1: If DNS is available, the H(e)MS's name is the FQDN used to resolve its IP address; otherwise it is the IP address of the H(e)MS.

The H(e)NB may check the revocation status of the H(e)MS certificate using OCSP as specified in [22] and [23]. Support for OCSP is optional for the operator network. The H(e)NB should support OCSP.

NOTE 2: It is strongly recommended to support OCSP in the H(e)NB, as this feature may become mandatory for H(e)NB in future releases.

The OCSP communication between H(e)NB and OCSP server may use the in-band signaling of certificate revocation status in TLS according to RFC 4366 [25]. Support for this extension to TLS in H(e)NB and H(e)MS is optional.

The H(e)MS may check the revocation status of the H(e)NB certificate using CRLs according to TS 33.310 [7] or OCSP as specified in [22] and [23].

The H(e)MS shall implement support for either CRL checking or OCSP or both. The locations of the CRL Server and OCSP Responder may be in the operator's network or provided by the manufacturer/vendor. Neither the operator nor the manufacturer is required to provide a CRL Server or an OCSP Responder. For the case when the operator provides a CRL Server or OCSP Responder, the manufacturer shall forward revocation data to the operator. The interface to forward revocation data is out of scope of the present document.

If the H(e)NB certificate contains CRL or OCSP server information (cf. sub-clause 8.3.3.1), then the H(e)MS may contact this server for revocation information.

NOTE 3: A CRL or OCSP server located at manufacturer of H(e)NB allows distribution of revocation information by the manufacturer directly. To use such revocation information, normally the H(e)MS needs a CRL or OCSP client capable to reach the public Internet to contact these servers.

Validity check of H(e)NB certificates in H(e)MS shall be configurable by the operator, i.e. whether to use CRLs, OCSP or both and whether to use operator CRL or OCSP server, manufacturer CRL or OCSP server, or more than one of them.

8.3.2.2 Device Validation

The H(e)NB shall support a device validation method whereby the device implicitly indicates its validity to the H(e)MS by successful execution of device authentication. To achieve this, the following requirement applies:

- If the device integrity check according to clause 6.1 failed, the TrE shall not give access to the sensitive functions using the private key needed for H(e)NB device authentication with the H(e)MS.

8.3.3 TLS certificate profile

8.3.3.1 TLS entity certificates

The H(e)NB and H(e)MS certificates for use with TLS shall both conform to the requirements set out in clauses 6.1.1 and 6.1.3a of TS 33.310 [7] with the following additions and exceptions:

- The H(e)NB certificate shall be signed by an entity that is authorized by the operator, e.g. the manufacturer or the vendor.
- The H(e)NB certificate shall carry the H(e)NB identity in FQDN format in both the subjectAltName extension of type dNSName and in the common name field.
- If the manufacturer or vendor provides a CRL or OCSP server, the H(e)NB certificate shall carry the CRL distribution point as specified in TS 33.310 [7] or the OCSP server information (AIA extension) as specified in RFC 5280 [26] and RFC 2560 [22].

NOTE 1: Server information for CRL and/or OCSP servers deployed in operator network may be configured in H(e)MS.

Editor's Note: The H(e)NB identity should be specified by CT4 as "HNB unique identity" in a new sub-clause of clause 4 in TS 23.003 [8]. Once this is done, this editor's note should be replaced by a reference to this new sub-clause.

- The H(e)MS certificate shall carry the identity of the H(e)MS in FQDN format in both the subjectAltName extension of type dNSName and in the common name field.

NOTE 2: The reason for carrying the identities in the common name field is compatibility.

- If an OCSP server is provided for the H(e)MS certificates, the H(e)MS certificate shall carry the OCSP server information as specified in RFC 2560 [22]. This OCSP server information is not mandatory, if OCSP extension to TLS according to RFC 4366 [25] is used.

NOTE 3: In general, it is possible to use a TLS client certificate in accordance with this specification also for IKEv2, if key exchange algorithm and used key length for both TLS and IKEv2 are chosen identically.

8.3.3.2 TLS CA certificates

TLS CA certificates shall conform to the requirements set out in clauses 6.1.1 and 6.1.4a of TS 33.310 [7] with the exception that there is no restriction in the issuer name.

8.3.4 TR-069 protocol profile

For the management of the H(e)NB by the H(e)MS, the CPE WAN Management Protocol TR-069 [15] shall be used with the following restrictions and extensions:

- SSL 3.0 shall not be used as it is outdated.
- At least TLS 1.1 [16] shall be supported. TLS 1.2 [17] should be supported.
- Shared-secret-based authentication between H(e)NB acting as CPE and H(e)MS acting as ACS shall not be allowed. Only certificate-based authentication shall be allowed.
- The use of TLS to transport the CPE WAN Management Protocol shall be mandatory in case that the H(e)MS is accessible on public internet or when TLS is used within the IPsec tunnel.
- The H(e)MS URI shall be specified as an HTTPS URL in case that the H(e)MS is accessible on public internet or when TLS is used within the IPsec tunnel.
- The support of TLS cipher suite RSA_WITH_AES_128_CBC_SHA shall be mandatory.
- Only TLS cipher suites listed in TLS 1.2 [17] shall be used. Ciphersuites with RC4 shall not be used. The support of TLS cipher suite RSA_WITH_RC4_128_SHA shall not be mandatory
- The H(e)NB acting as CPE shall not be obliged to wait until it has accurate absolute time before it contacts the H(e)MS acting as ACS.

NOTE 1: The term "absolute time" refers to UTC and its use is consistent with its definition and use in the sections on "Use of SSL/TLS and TCP and on Data Types" in TR-069 [15].

- If the H(e)NB contacts the H(e)MS without having the accurate absolute time, it shall not ignore components of the H(e)MS certificate that involve absolute time.

- The support for H(e)NB authentication using client-side (CPE side) certificates shall be mandatory.
- The H(e)NB acting as CPE shall be authenticated to the H(e)MS by the globally unique H(e)NB identity contained in the H(e)NB certificate in case that mutual authentication between H(e)NB and H(e)MS is performed. The exact format of the TLS client certificate is specified in clause 8.3.3.1.

NOTE 2: This profile is intended to be consistent with the TLS profile in Annex E of TS 33.310 [7].

8.4 Protection of SW Download

The H(e)NB shall utilize the established TR-069 method to download software from the H(e)MS or a server directed to by the H(e)MS according to TR-069 Version 1 Amendment 2 [15]. The following requirements are added for security:

- The file shall use the signed package format according to TR-069 [15].

NOTE 1: Depending on the link to H(e)MS, transport security is provided by the secure link according to clauses 4.3.1 (when H(e)MS is in operator network) or 4.3.2 (when H(e)MS is in public Internet).

- The SignedData object in the signed package shall contain at least one signature provided by a software signing entity, with certificate issued by an operator trusted CA.
- The TrE shall use a public key issued by an operator trusted CA to verify the software signing entity certificate and the signature(s) in the SignedData object. All root certificates used for this purpose shall be stored in the TrE.

Editor's Note: Use of the more current CMS (Cryptographic Message Syntax) in RFC 3852 and other enhancements to PKCS#7 is for FFS.

- The signed package shall also contain the trusted reference values needed for the software integrity checks performed during secure boot.

NOTE 2: TR-069 [15] supports multiple signatures which can be used for the purpose of supporting different hash algorithms.

If the digest authentication fails, the H(e)NB shall not install the software.

Editor's Note: Requirements for reporting failures to an external entity or entities and/or performing internal logging are FFS.

9 Security Aspects of Emergency Call Handling

The H(e)NB and/or the H(e)NB-GW shall support security handling of Emergency call as specified in TS 25.467[12], TS 33.102 [20] and TS 33.401 [21].

Emergency call shall be allowed by the H(e)NB and/or operator's core network entities (e.g. H(e)NB-GW) regardless of whether UE can pass access control as specified in section 8.2.

In case of non CSG UEs or non CSG HNBs, after Emergency call is finished, the context (as described in [12]) extablished between the HNB and operator's core network entities for UEs who can not get access over the HNB shall be released to prevent the UE from accessing non-emergency services.

Editor's Note: RAN2 and SA1 emergency call handling alignment verification is still needed.

Annex A (informative): Authentication Call-flows

A.1 Device Authentication Call-flow Example

Certificate based mutual authentication between the H(e)NB and the core network is specified in clause 7.2. As example the call flow between the H(e)NB and the SeGW is shown in Figure A.1. This example illustrates an autonomous device integrity check followed by initiation of device authentication.

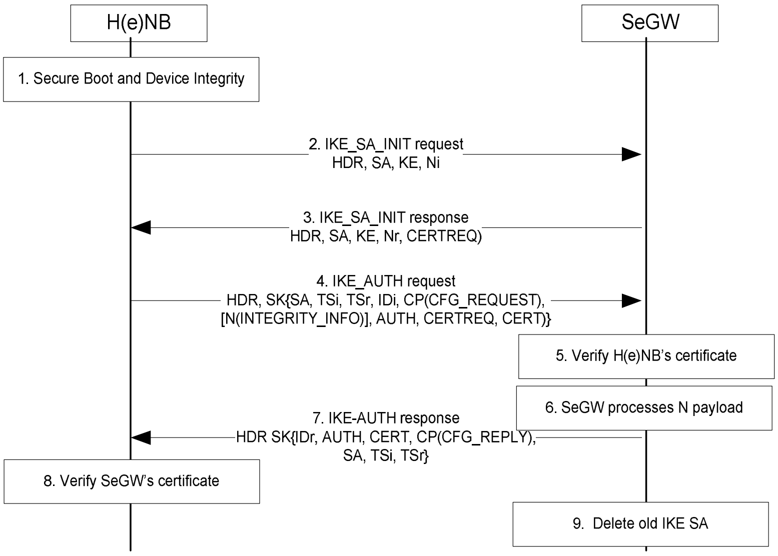
H(e)NB
SeGW
1. Secure Boot and Device Integrity
2. IKE_SA_INIT request
HDR, SA, KE, Ni
3. IKE_SA_INIT response
HDR, SA, KE, Nr, CERTREQ)
4. IKE_AUTH request
HDR, SK{SA, TSi, TSr, IDi, CP(CFG_REQUEST),
[N(INTEGRITY_INFO)], AUTH, CERTREQ, CERT)}
5. Verify H(e)NB's certificate
6. SeGW processes N payload
7. IKE-AUTH response
HDR SK{IDr, AUTH, CERT, CP(CFG_REPLY),
SA, TSi, TSr}
8. Verify SeGW's certificate
9. Delete old IKE SA

Figure A.1: Certificate-based authentication with device integrity

1. TrE brings H(e)NB to secure boot and performs device integrity check of H(e)NB.

NOTE 1: If the device integrity check fails the following procedure is not executed.

2. Following successful device integrity check, the H(e)NB sends an IKE_SA_INIT request to the SeGW.

3. The SeGW sends IKE_SA_INIT response, requesting a certificate from the H(e)NB.

4. The H(e)NB sends its identity in the IDi payload in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. Optionally a user profile may be selected based on the H(e)NB's identity presented in the IDi payload and the authentication type indication in the user profile may be used to enforce the choice of authentication (device only or combined device and HP). The H(e)NB sends the AUTH payload and its own certificate, and also requests a certificate from the SeGW. Configuration payload is carried in this message if the H(e)NB's remote IP address should be configured dynamically. H(e)NB optionally includes a Notify Payload containing integrity information of H(e)NB with a Notification Type of INTEGRITY_INFO in the IKE_AUTH request. Computation of the AUTH parameter is performed within the H(e)NB's TrE. If configured to check the validity of the SeGW certificate the H(e)NB retrieves SeGW certificate status information from the OCSP responder. Alternatively the H(e)NB may add an OCSP request to the IKE message.

NOTE 2: Inclusion of the Notify Payload and further usage of data transferred in this payload is not part of autonomous validation.

5. The SeGW checks the correctness of the AUTH received from the H(e)NB and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The SeGW verifies the certificate received from the H(e)NB. The SeGW may check the validity of the certificates using CRL or OCSP. If the H(e)NB request

contained an OCSP request, or if the SeGW is configured to provide its certification revocation status to the H(e)NB, the SeGW retrieves SeGW certificate status information from the OCSP server, or uses a valid cached response if one is available

6. The SeGW processes the N payload of the IKE_AUTH request based on local policy of the operator.

NOTE 3: SeGW may choose to retain the information carried in the N payload for statistical analysis, send the information to a FIGS (Fraud Information Gathering System) for fraud detection, or send the information to a validation entity for validation.

7. The SeGW sends its identity in the IDr payload, the AUTH parameter and its certificate to the H(e)NB together with the configuration payload, security associations, and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates. The Remote IP address is assigned in the configuration payload (CFG_REPLY), if the H(e)NB requested for a Remote IP address through the CFG_REQUEST. If the SeGW has SeGW certificate status information available, this information is added to the IKE response to H(e)NB.

8. The H(e)NB verifies the SeGW certificate with its stored root certificate. The root certificate for the SeGW certificate shall be stored in the TrE. The H(e)NB checks that the SeGW identity as contained in the SeGW certificate equals the SeGW identity as provided to H(e)NB by initial configuration or by H(e)MS. The H(e)NB checks the validity of the SeGW certificates using the OCSP response if configured to do so.

9. If the SeGW detects that an old IKE SA for that H(e)NB already exists, it will delete the IKE SA and send the H(e)NB an INFORMATIONAL exchange with a Delete payload in order to delete the old IKE SA in H(e)NB.

NOTE 4: If the Notify Payload is used to convey integrity information, then an available values in the Private Use Status Types range of Notification Type values in IKEv2 may be used.

Editor's Note: In case the integrity information payload carries security information, the security issues have to be studied.

A.2 Combined Device and HP Authentication Call-flow Example

The certificate based mutual authentication between the H(e)NB and the core network, followed by an EAP-AKA-based HP authentication exchange between the H(e)NB/HPM and the AAA server, is specified in clause 7.2. As example the call flow between the H(e)NB, SeGW and AAA server is shown in Figure A.2. This example illustrates an autonomous device integrity check followed by initiation of combined device and HP authentication.

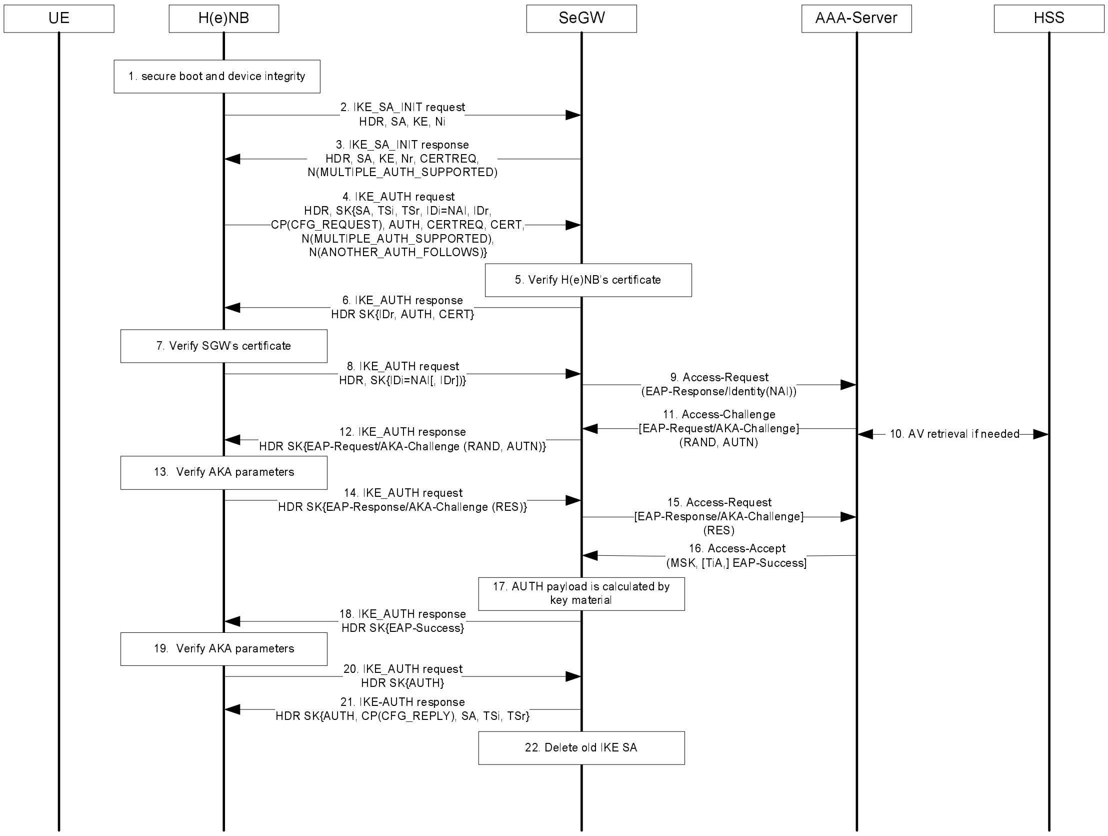
UE
H(e)NB
SeGW
AAA-Server
HSS
1. secure boot and device integrity
2. IKE_SA_INIT request
HDR, SA, KE, Ni
3. IKE_SA_INIT response
HDR, SA, KE, Nr, CERTREQ,
N(MULTIPLE_AUTH_SUPPORTED)
4. IKE_AUTH request
HDR, SK{SA, TSi, TSr, IDi=NAI, IDr,
CP(CFG_REQUEST), AUTH, CERTREQ, CERT,
N(MULTIPLE_AUTH_SUPPORTED),
N(ANOTHER_AUTH_FOLLOWS)}
5. Verify H(e)NB's certificate
6. IKE_AUTH response
HDR SK{IDr, AUTH, CERT}
7. Verify SGW's certificate
8. IKE_AUTH request
HDR, SK{IDi=NAI[, IDr])}
9. Access-Request
(EAP-Response/Identity(NAI))
11. Access-Challenge
[EAP-Request/AKA-Challenge]
(RAND, AUTN)
10. AV retrieval if needed
12. IKE_AUTH response
HDR SK{EAP-Request/AKA-Challenge (RAND, AUTN)}
13. Verify AKA parameters
14. IKE_AUTH request
HDR SK{EAP-Response/AKA-Challenge (RES)}
15. Access-Request
[EAP-Response/AKA-Challenge]
(RES)
16. Access-Accept
(MSK, [TiA,] EAP-Success]
17. AUTH payload is calculated by
key material
18. IKE_AUTH response
HDR SK{EAP-Success}
19. Verify AKA parameters
20. IKE_AUTH request
HDR SK{AUTH}
21. IKE-AUTH response
HDR SK{AUTH, CP(CFG_REPLY), SA, TSi, TSr}
22. Delete old IKE SA

Figure A.2: Combined certificate and EAP-AKA-based authentication

1. TrE brings H(e)NB to secure boot and performs device integrity check of H(e)NB.

NOTE: If the device integrity check fails the following procedure is not executed.

2. Following successful device integrity check, the H(e)NB sends an IKE_SA_INIT request to the SeGW.

3. The SeGW sends IKE_SA_INIT response, requesting a certificate from the H(e)NB. The SeGW indicates that it support Multiple Authentication by including the MULTIPLE_AUTH_SUPPORTED payload.

4. The H(e)NB inserts its identity in the IDi payload in this first message of the IKE_AUTH phase, computes the AUTH parameter within its TrE, and begins negotiation of child security associations. The authentication type indication in user profile which is selected selected by H(e)NB's identity presented in the IDi payload may be used and enforce the choice of authentication (device only or combined device and HP). The H(e)NB then sends IKE_AUTH request with the AUTH payload, its own certificate, and also requests a certificate from the SeGW. Configuration payload is carried in this message if the H(e)NB's remote IP address should be configured dynamically. The H(e)NB indicates that it support Multiple Authentication and that it wants to do a second authentication by including the MULTIPLE_AUTH_SUPPORTED and ANOTHER_AUTH_FOLLOWS attributes. If configured to check the validity of the SeGW certificate the H(e)NB retrieves SeGW certificate status information from the OCSP responder. Alternatively the H(e)NB may add an OCSP request to the IKE message.

5. The SeGW checks the correctness of the AUTH received from the H(e)NB and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The SeGW verifies the certificate received from the H(e)NB. The SeGW may check the validity of the certificates using CRL or OCSP. If the H(e)NB request contained an OCSP request, or if the SeGW is configured to provide its certification revocation status to the H(e)NB, the SeGW retrieves SeGW certificate status information from the OCSP server, or uses a valid cached response if one is available.

6. The SeGW sends IKE_AUTH response with its identity in the IDr payload, the AUTH parameter and its certificate to the H(e)NB. If the SeGW has SeGW certificate status information available, this information is added to the IKE response to H(e)NB.

7. The H(e)NB verifies the SeGW certificate with its stored root certificate. The root certificate for the SeGW certificate shall be stored in the TrE. The H(e)NB checks that the SeGW identity as contained in the SeGW certificate equals the SeGW identity as provided to H(e)NB by initial configuration or by H(e)MS. The H(e)NB checks the validity of the SeGW certificates using the OCSP response if configured to do so.

8. The H(e)NB sends another IKE_AUTH request message with the HP's identity in the IDi payload and the AUTH payload omitted to inform the SeGW that the H(e)NB want to perform EAP authentication.

9. The SeGW sends the Authentication Request message with an empty EAP AVP to the 3GPP AAA Server, containing the identity received in IKE_AUTH request message received in step 8.

10. The AAA Server shall fetch the subscription data and authentication vectors from HSS/HLR.

11. The AAA Server initiates the authentication challenge.

12. The SeGW sends IKE_AUTH response to H(e)NB. The EAP message received from the AAA Server (EAP-Request/AKA-Challenge) is included in order to start the EAP procedure over IKEv2.

13. The H(e)NB processes the EAP challenge message and uses the HPM for verification of the AUTN and generating the RES parameters. Optionally, processing of the whole EAP challenge message, including verification of the received MAC with the newly derived keying material may be performed within the H(e)NB's HPM.

14. The H(e)NB sends the IKE_AUTH request with the EAP-Response/AKA-Challenge to the SeGW.

15. The SeGW forwards the EAP-Response/AKA-Challenge message to the AAA Server.

16. When all checks are successful, the AAA Server sends the Authentication Answer including an EAP success and the key material to the SeGW. This key material should consist of the MSK generated during the authentication process.

17. The MSK should be used by the SeGW to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages.

18. The EAP Success message is forwarded to the H(e)NB over IKEv2.

19. IKE_AUTH response with the H(e)NB should take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. Computation of the AUTH parameter is performed within the H(e)NB's HPM.

20. IKE_AUTH request with the AUTH parameter is sent to the SeGW.

21. The SeGW checks the correctness of the AUTH received from the H(e)NB and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The SeGW should send the assigned Remote IP address in the configuration payload (CFG_REPLY), if the H(e)NB requested for a Remote IP address through the CFG_REQUEST. Then the IKE_AUTH response with AUTH parameter is sent to the H(e)NB together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

22. If the SeGW detects that an old IKE SA for that H(e)NB already exists, it will delete the IKE SA and send the H(e)NB an INFORMATIONAL exchange with a Delete payload in order to delete the old IKE SA in H(e)NB.

Annex B (informative): Location Verification Examples

B.1 Example of Location verification based on IP address and line identifier in NASS

The NASS (Network Attachment Subsystem) standard in TISPAN [18] has defined the interface through which the mobile core network is able to query the geographic location information based on the IP address. The network-based database can be the CLF (connectivity Session Location and Repository Function) element . The CLF registers the following information provided by the NACF (network access configuration function), and make them relevant: the IP address located to the fixed access point, the network location information, and geography location information. The CLF provides e2 interface for service layer entity. The reference document [19] specifies e2 interface based on Diameter protocol.

NOTE 1: The verifying node must receive the IP address as used in the NASS. This may require either that the verifying node be located directly at the edge of the NASS, or that the NASS uses public IP addresses without NAT or NAPT to Internet.

The entity used to query CLF is located in the verifying node.

The contract location exists in the verifying node already before the location verification process can be performed. The contract location can be defined by the operator when H(e)NB service is subscribed to the network.

The location authentication procedure consists of the following steps:

a) H(e)NB sends request message to the verifying node, carrying its IP address in this message.

b) According to the IP address, the verifying node queries the CLF to obtain the access line location identifier.

c) Verifying node authenticates whether the access line location identifier stored in the verifying node (i.e. the legal contract location) corresponds to the location identifier it retrieves from the CLF based on IP address obtained from the H(e)NB. If it is the same, this means that the H(e)NB location has not been changed.

d) Other procedures, e.g. provisioning of configuration parameters from the verifying node to the H(e)NB, can be performed only after successful location verification of the H(e)NB by the verifying node.

NOTE 2: Storage of the location information in the verifying node as a subscription profile is preferable.

NOTE 3 : The above procedure provides an effective method to query the CLF according the H(e)NB's IP address. If the CLF is not available to the mobile operator, similar methods using the broadband connection information can be implemented.

Annex C:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2009-09	SA#45	SP-090527	--	--	Presentation to SA for information	--	1.0.0
2009-12	SA#46	SP-090825	--	--	Presentation to SA for approval	1.0.0	2.0.0
2009-12	SA#46	--	--	--	Publication of SA approved version	2.0.0	9.0.0

History

Document history		
V9.0.0	February 2010	Publication